

# **ESET Endpoint Antivirus**

## Vodič za korisnike

[Kliknite ovdje za prikazivanje verzije mrežne pomoći dokumenta](#)



Autorska prava ©2023 tvrtke ESET, spol. s r.o.

ESET Endpoint Antivirus razvila je tvrtka ESET, spol. s r.o.

Za više informacija posjetite <https://www.eset.com>.

Sva prava pridržana. Nijedan dio ove dokumentacije ne smije se reproducirati, pohranjivati u sustavu za dohvaćanje ili prenositi u bilo kojem obliku ili na bilo koji način, elektronički, mehanički, fotokopiranjem, snimanjem, skeniranjem ili na drugi način bez dopuštenja autora u pisanim oblicima.

ESET, spol. s r.o. zadržava pravo promijeniti bilo koji od opisanih softvera aplikacije bez prethodne najave.

Tehnička podrška: <https://support.eset.com>

REV. 19.03.2023.

<b>1 ESET Endpoint Antivirus 8</b>	1
<b>1.1 Koje su novosti u ovoj verziji?</b>	2
<b>1.2 Sistemske preduvjeti</b>	3
1.2 Podržani jezici	4
<b>1.3 Prevencija</b>	5
<b>1.4 Stranice pomoći</b>	6
<b>2 Dokumentacija za daljinski upravljane krajne točke</b>	7
<b>2.1 Uvod u ESET PROTECT</b>	8
<b>2.2 Uvod u ESET PROTECT Cloud</b>	9
<b>2.3 Postavke zaštićene lozinkom</b>	10
<b>2.4 Što su pravila</b>	11
2.4 Spajanje pravila	11
<b>2.5 Kako funkciraju zastavice</b>	12
<b>3 Samostalno korištenje programa ESET Endpoint Antivirus</b>	13
<b>3.1 Metoda instalacije</b>	13
3.1 Instalacija pomoću programa ESET AV Remover	14
3.1 ESET AV Remover	14
3.1 Deinstalacija pomoću programa ESET AV Remover završila je s pogreškom	17
3.1 Instalacija (.exe)	17
3.1 Promjena instalacijske mape (.exe)	19
3.1 Instalacija (.msi)	20
3.1 Napredna instalacija (.msi)	22
3.1 Instalacija putem naredbenog retka	23
3.1 Instalacija pomoću GPO-a ili SCCM-a	27
3.1 Nadogradnja na noviju verziju	28
3.1 Automatska nadogradnja programa koji radi prema starom standardu	29
3.1 Nadogradnje za potrebe sigurnosti i stabilnosti	30
3.1 Uobičajene teškoće prilikom instalacije	30
3.1 Aktivacija nije uspjela	30
<b>3.2 Aktivacija proizvoda</b>	31
<b>3.3 Skeniranje računala</b>	31
<b>3.4 Vodič za početnike</b>	31
3.4 Korisničko sučelje	31
3.4 Podešavanje aktualizacije	35
<b>4 Rad s programom ESET Endpoint Antivirus</b>	36
<b>4.1 Računalo</b>	38
4.1 Modul detekcije	40
4.1 Napredne opcije modula detekcije	45
4.1 Otkrivena je infiltracija	45
4.1 Zajednička lokalna predmemorija	47
4.1 rezidentna zaštita	47
4.1 Provjera rezidentne zaštite	49
4.1 Kada treba izmijeniti konfiguraciju rezidentne zaštite	49
4.1 Što ako rezidentna zaštita ne funkcioniра	49
4.1 Skeniranje računala	50
4.1 Pokretač prilagođenog skeniranja	52
4.1 Napredak skeniranja	54
4.1 Dnevnik skeniranja računala	55
4.1 Skeniranja za zlonamjerne softvere	56
4.1 Skeniranje u stanju mirovanja	56

4.1 Profili skeniranja .....	57
4.1 Ciljevi skeniranja .....	57
4.1 Napredne mogućnosti skeniranja .....	58
4.1 Kontrola uređaja .....	59
4.1 Uređivač pravila kontrole uređaja .....	59
4.1 Otkriveni uređaji .....	60
4.1 Grupe uređaja .....	61
4.1 Dodavanje pravila kontrole uređaja .....	62
4.1 Sistem za sprečavanje upada (HIPS) .....	64
4.1 HIPS interaktivni prozor .....	66
4.1 Otkriveno je moguće ponašanje ransomwarea .....	67
4.1 HIPS upravljanje pravilima .....	68
4.1 Postavke HIPS pravila .....	68
4.1 HIPS napredno podešavanje .....	71
4.1 Upravljački programi koji se uvijek smiju učitati .....	71
4.1 Način rada za prezentacije .....	71
4.1 Skeniranje pri pokretanju .....	72
4.1 Automatska provjera pokretačke datoteke .....	72
4.1 Zaštita dokumenata .....	73
4.1 Izuzeci .....	73
4.1 Izuzeci radi poboljšanja performansi .....	74
4.1 Dodavanje ili uređivanje izuzetka radi poboljšanja performansi .....	75
4.1 Format izuzetaka puta .....	76
4.1 Izuzeci detekcija poznatih prijetnji .....	77
4.1 Dodavanje ili uređivanje izuzetih detekcija poznatih prijetnji .....	80
4.1 Čarobnjak za stvaranje izuzetih detekcija poznatih prijetnji .....	81
4.1 Izuzeci (7.1 i stariji) .....	81
4.1 Izuzeti procesi .....	82
4.1 Dodavanje ili uređivanje izuzetih procesa .....	83
4.1 Izuzeci iz HIPS-a .....	83
4.1 ThreatSense parametri .....	83
4.1 Razine čišćenja .....	87
4.1 Datotečne ekstenzije izuzete od skeniranja .....	88
4.1 Dodatni ThreatSense parametri .....	89
<b>4.2 Mreža .....</b>	<b>89</b>
4.2 Zaštita od mrežnog napada .....	90
4.2 Napredne opcije filtriranja .....	90
4.2 Pravila IDS-a .....	92
4.2 Blokirana je potencijalna prijetnja .....	93
4.2 Otklanjanje poteškoća mrežne zaštite .....	93
4.2 Popis privremeno blokiranih IP adresa .....	94
<b>4.3 Web i e-pošta .....</b>	<b>94</b>
4.3 Filtriranje protokola .....	95
4.3 Izuzete aplikacije .....	96
4.3 Izuzete IP adrese .....	97
4.3 SSL/TLS .....	97
4.3 Certifikati .....	99
4.3 Šifrirani mrežni promet .....	99
4.3 Popis poznatih certifikata .....	100
4.3 Popis filtriranih SSL/TLS aplikacija .....	100
4.3 zaštita klijenta e-pošte .....	101

4.3 Protokoli e-pošte .....	103
4.3 Upozorenja i obavijesti e-pošte .....	104
4.3 Integracija s klijentima e-pošte .....	105
4.3 Alatna traka za Microsoft Outlook .....	105
4.3 Alatna traka za Outlook Express i Windows Mail .....	105
4.3 Dijaloški okvir s potvrdom .....	106
4.3 Ponovno skeniranje poruka .....	106
4.3 zaštita web pristupa .....	106
4.3 Napredno podešavanje zaštite web pristupa .....	108
4.3 Web protokoli .....	109
4.3 Upravljanje URL adresama .....	109
4.3 Popis URL adresa .....	110
4.3 Stvaranje novog popisa URL adresa .....	111
4.3 Kako dodati URL masku .....	112
4.3 Anti-phishing zaštita .....	112
<b>4.4 Aktualizacija programa .....</b>	<b>114</b>
4.4 Podešavanje aktualizacije .....	117
4.4 Vraćanje aktualizacije .....	120
4.4 Nadogradnja programskih komponenti .....	122
4.4 Opcije veze .....	122
4.4 Aktualizacijski mirror .....	124
4.4 HTTP server i SSL za mirror .....	126
4.4 Aktualizacija s mirrora .....	126
4.4 Otklanjanje poteškoća s mirror aktualizacijom .....	128
4.4 Stvaranje aktualizacijskih zadataka .....	129
<b>4.5 Alati .....</b>	<b>129</b>
4.5 Dnevnići .....	130
4.5 Filtriranje dnevnika .....	133
4.5 Konfiguracija zapisivanja .....	134
4.5 Dnevnići provjera .....	135
4.5 Planer .....	136
4.5 Nadzor aktivnosti .....	139
4.5 ESET SysInspector .....	140
4.5 Zaštita na bazi clouda .....	141
4.5 Filtar izuzetaka za zaštitu na bazi clouda .....	144
4.5 Procesi koji se izvršavaju .....	145
4.5 Sigurnosno izvješće .....	146
4.5 ESET SysRescue Live .....	148
4.5 Slanje uzorka na analizu .....	148
4.5 Odabir uzorka za analizu - Sumnjiva datoteka .....	149
4.5 Odabir uzorka za analizu - Sumnjiva web stranica .....	149
4.5 Odabir uzorka za analizu - Neispravno identificirana datoteka .....	149
4.5 Odabir uzorka za analizu - Neispravno identificirana web stranica .....	150
4.5 Odabir uzorka za analizu - Ostalo .....	150
4.5 Obavijesti .....	150
4.5 Obavijesti aplikacije .....	151
4.5 Obavijesti na radnoj površini .....	152
4.5 Obavijesti e-poštom .....	153
4.5 Prilagodba obavijesti .....	155
4.5 Karantena .....	155
4.5 Podešavanje proxy servera .....	157

4.5 Vremensko razdoblje .....	159
4.5 Nadogradnja sustava Microsoft Windows .....	159
4.5 Interval provjere licence .....	160
<b>4.6 Korisničko sučelje .....</b>	<b>160</b>
4.6 Elementi korisničkog sučelja .....	161
4.6 Statusi aplikacije .....	162
4.6 Podešavanje pristupa .....	163
4.6 Lozinka za napredno podešavanje .....	164
4.6 Upozorenja i okviri s porukama .....	164
4.6 Interaktivna upozorenja .....	166
4.6 Poruke za potvrdu .....	167
4.6 Pogreška zbog sukoba naprednih postavki .....	168
4.6 Izmjenjivi mediji .....	168
4.6 Potrebno je ponovno pokretanje .....	170
4.6 Preporučuje se ponovno pokretanje .....	171
4.6 Ikona trake sustava .....	173
4.6 Kontekstni izbornik .....	174
4.6 Pomoć i podrška .....	174
4.6 O programu ESET Endpoint Antivirus .....	175
4.6 Slanje podataka o sistemskoj konfiguraciji .....	176
4.6 Tehnička podrška .....	176
4.6 Upravljanje profilima .....	177
4.6 Tipkovnički prečaci .....	178
4.6 Dijagnostika .....	178
4.6 Skener naredbenog retka .....	179
4.6 ESET CMD .....	182
4.6 Otkrivanje stanja mirovanja .....	184
4.6 Uvoz i izvoz postavki .....	184
4.6 Vrati sve postavke na standardne .....	185
4.6 Želite li vratiti sve postavke u ovom odjeljku .....	185
4.6 Pogreška prilikom spremanja konfiguracije .....	185
4.6 Daljinsko praćenje i upravljanje .....	186
4.6 ERMM naredbeni redak .....	187
4.6 Popis ERMM JSON naredbi .....	188
4.6 nabavi zaštitu-status .....	189
4.6 nabavi aplikaciju-informacije .....	190
4.6 nabavi licencu-informacije .....	192
4.6 nabavi dnevниke .....	192
4.6 nabavi aktivaciju-status .....	193
4.6 nabavi skeniranje-informacije .....	194
4.6 nabavi konfiguraciju .....	195
4.6 preuzmi aktualizaciju-status .....	196
4.6 pokreni skeniranje .....	197
4.6 pokreni aktivaciju .....	197
4.6 pokreni deaktivaciju .....	198
4.6 pokreni aktualizaciju .....	199
4.6 postavi konfiguraciju .....	199
<b>5 Najčešća pitanja .....</b>	<b>200</b>
<b>5.1 Aktualizacija programa ESET Endpoint Antivirus .....</b>	<b>201</b>
<b>5.2 Aktivacija programa ESET Endpoint Antivirus .....</b>	<b>201</b>
5.2 Unos Licenčnog ključa prilikom aktivacije .....	202

5.2 Prijava u ESET Business Account korisnički račun .....	202
5.2 Upotreba podataka o staroj licenci za aktivaciju novijeg ESET-ova sigurnosnog programa .....	203
<b>5.3 Uklanjanje virusa s računala .....</b>	<b>203</b>
<b>5.4 Stvaranje novog zadatka u Planeru .....</b>	<b>203</b>
5.4 Zakazivanje tjednog skeniranja računala .....	204
<b>5.5 Povezivanje programa ESET Endpoint Antivirus s alatom ESET PROTECT .....</b>	<b>205</b>
5.5 Korištenje načina nadjačavanja .....	205
5.5 Primjena preporučenog pravila za program ESET Endpoint Antivirus .....	206
<b>5.6 Konfiguiriranje mirrora .....</b>	<b>209</b>
<b>5.7 Kako nadograditi na Windows 10 s proizvodom ESET Endpoint Antivirus .....</b>	<b>209</b>
<b>5.8 Kako aktivirati daljinsko praćenje i upravljanje .....</b>	<b>210</b>
<b>5.9 Kako blokirati preuzimanje specifičnih vrsti datoteka s interneta .....</b>	<b>212</b>
<b>5.10 Kako minimizirati korisničko sučelje programa ESET Endpoint Antivirus .....</b>	<b>213</b>
<b>6 Lisenčni ugovor za krajnjeg korisnika .....</b>	<b>214</b>
<b>7 Pravila privatnosti .....</b>	<b>220</b>

# ESET Endpoint Antivirus 8

ESET Endpoint Antivirus 8 predstavlja novi pristup potpuno integriranoj zaštiti računala. Najnovija verzija sustava za skeniranje ThreatSense® brzo i precizno čuva sigurnost vašeg računala. Rezultat je pametan sustav koji neprekidno vodi računa o napadima i zlonamjernom softveru koji bi mogao ugroziti vaše računalo.

ESET Endpoint Antivirus 8 potpuno je sigurnosno rješenje nastalo dugoročnim nastojanjima da se maksimalna zaštita kombinira s minimalnim utjecajem na sustav. Napredne tehnologije koje se temelje na umjetnoj inteligenciji mogu proaktivno eliminirati infiltraciju [virusima](#), spywareom, virusom trojan, crvima, adwareom, rootkitima i drugim [internetskim napadima](#), pri čemu nema negativnog utjecaja na rad vašeg sustava i računala.

Program ESET Endpoint Antivirus 8 prvenstveno je osmišljen za upotrebu na radnim stanicama u manjim poslovnim okruženjima.

U odjeljku [Samostalna upotreba programa ESET Endpoint Antivirus](#) možete pronaći teme pomoći podijeljene u nekoliko poglavlja i potpoglavlja koja vam mogu pružiti kontekst i olakšati snalaženje, uključujući [Preuzimanje](#), [Instalaciju](#) i [Aktivaciju](#).

[7 prvenstveno je osmišljen za korištenje na radnim stanicama u malim tvrtkama. Upotreba programa ESET Endpoint Antivirus s programom ESET PROTECT](#) u poslovnom okruženju omogućuje vam jednostavno upravljanje klijentskim radnim stanicama, primjenu smjernica i pravila, nadzor otkrivanja i daljinsko konfiguriranje klijenata s bilo kojeg umreženog računala.

Ovo poglavlje bavi se [najčešćim pitanjima](#) i problemima s kojima se možete susresti.

## Značajke i prednosti

<b>Redizajnirano korisničko sučelje</b>	Korisničko sučelje u ovoj verziji značajno je redizajnirano i pojednostavljeno na temelju rezultata testa upotrebljivosti. Cjelokupan tekst i obavijesti grafičkog korisničkog sučelja pomno su pregledani pa sučelje sada pruža podršku i za pisma koja se pišu zdesna nalijevo, poput hebrejskog i arapskog. Pomoć na mreži sad je integrirana u ESET Endpoint Antivirus i pruža sadržaj podrške koji se dinamički nadograđuje.
<b>Antivirus i antispyware</b>	Proaktivno otkriva i čisti veći broj poznatih i nepoznatih virusa, <a href="#">crva</a> , <a href="#">trojanaca</a> i <a href="#">rootkita</a> . Napredna heuristička tehnologija upozorava čak i na potpuno nepoznat zlonamjerni softver, štiteći vas od prijetnji i neutralizirajući ih prije nego uspiju prouzročiti bilo kakvu štetu. Zaštita web pristupa i <a href="#">Anti-Phishing</a> zaštita vrši se nadgledanjem komunikacije između internetskih preglednika i udaljenih servera (uključujući SSL). Zaštita klijenta e-pošte omogućuje nadzor komunikacije e-poštom koja se prima putem protokola POP3(S) i IMAP(S).
<b>Redovite nadogradnje</b>	Redovita nadogradnja modula za otkrivanje virusa (prethodno zvanog „baza podataka virusnih potpisa“) i programskih modula najbolji je način za osiguravanje maksimalnog stupnja zaštite na računalu.
<b>ESET LiveGrid® (reputacija utemeljena na Cloud tehnologiji)</b>	Reputaciju procesa koji se izvršavaju i datoteka možete provjeriti izravno iz programa ESET Endpoint Antivirus.

<b>Daljinsko upravljanje</b>	ESET PROTECT ili ESET Security Management Center omogućuje upravljanje ESET-ovim programima na radnim stanicama, serverima i mobilnim uređajima u umreženom okruženju s jedne središnje lokacije. Uporabom ESET Security Management Center web konzole (ESMC web konzole) možete instalirati ESET-ova rješenja, upravljati zadacima, nametati sigurnosna pravila, nadgledati stanje sustava i brzo rješavati probleme ili prijetnje na udaljenim računalima.
<b>Zaštita od mrežnog napada</b>	Analizira sadržaj mrežnog prometa i štiti od mrežnih napada. Blokira se sav promet koji se smatra štetnim.
<b>Kontrola weba (samo ESET Endpoint Security)</b>	Web kontrola omogućuje blokiranje web stranica s potencijalno uvredljivim sadržajima. Osim toga, poslodavci ili sistemski administratori mogu zabraniti pristup do 27 unaprijed definiranih kategorija web stranica i više od 140 podkategorija.

## Koje su novosti u ovoj verziji?

ESET Endpoint Antivirus 8 je objavljen i [dostupan je za preuzimanje](#).

### WMI i skeniranje cijelog registra

- unapređenje skeniranja registra koje može otkriti i eliminirati zločudne reference ili opasan sadržaj bilo gdje u registru ili WMI repozitoriju
- pregled može potrajati neko vrijeme; ove objekte skeniranja potrebno je odabrati za sva skeniranja na zahtjev, čak i za profil "dubinskog" skeniranja

### Mikro nadogradnja programskih komponenti (nadogradnja funkcija)

- [pametno rješenje](#) za svođenje održavanja ESET Endpoint Antivirus na minimum
- MicroPCU može tjednima čekati ponovno pokretanje sustava
- ne provodi ponovnu instalaciju programa uz sve nedostatke kao što je odjava iz sustava tijekom procesa, uključujući prijenos konfiguracije
- preuzima manje podataka (diferencijalna nadogradnja)
- uključuje prijateljski podsjetnik ili podsjetnik koji korisnik može lako isključiti i kompatibilan je s upravljanim mrežama

### Nadogradnje za potrebe sigurnosti i stabilnosti

- [nadogradnje za potrebe sigurnosti i stabilnosti](#) automatski će se distribuirati podržanim verzijama (7.x i novije), koje sadrže samo bitne izmjene koje će se zabilježiti u dnevnicima značajnih promjena uz potpunu transparentnost

Ova nadogradnja pruža razne ispravke pogreški i poboljšanja performansi.

---

Dodatne informacije i snimke zaslona povezane s novim funkcijama programa ESET Endpoint Antivirus potražite u

sljedećem članku ESET-ove baze znanja:

- [Što je novo u ESET Endpoint Antivirus 8?](#)

## Sistemski preuvjeti

Za rad programa ESET Endpoint Antivirus bez prekida sustav mora zadovoljiti sljedeće hardverske i softverske uvjete (standardne postavke proizvoda):

### Podržani procesori

Intel ili AMD procesor, 32-bitni (x86) sa skupom uputa SSE2 ili 64-bitni (x64), 1 GHz ili više

### Operacijski sustavi

Microsoft® Windows® 10

Microsoft® Windows® 8.1

Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 s najnovijim nadogradnjama sustava Windows (barem [KB4474419](#) i [KB4490628](#))

Windows XP i Windows Vista više [nisu podržani](#).

 Pobrinite se da je vaš operacijski sustav nadograđen.

### Ostalo

- Ispunjeni su sistemski preuvjeti operacijskog sustava i drugog softvera koji je instaliran na računalu
- 0,3 GB slobodne sistemske memorije (pogledajte Napomenu 1)
- 1 GB slobodnog diskovnog prostora (pogledajte Napomenu 2)
- Minimalna razlučivost zaslona 1024x768
- Internetska veza ili veza putem lokalne mreže s izvorom (pogledajte Napomenu 3) nadogradnji programa
- Dva antivirusna programa koja su istovremeno pokrenuta na jednom uređaju uzrokuju neizbjježne sukobe upotrebe resursa sustava, kao što je usporavanje sustava zbog kojeg on postaje neupotrebljiv

Iako je možda moguće instalirati i pokrenuti program na sustavima koji ne podržavaju navedene preuvjete, preporučujemo prethodnu provedbu testa upotrebljivosti na temelju izvedbenih zahtjeva.

- (1):** Program može upotrebljavati više memorije ako bi ona inače bila neiskorištena na vrlo zaraženom računalu ili prilikom uvoza velikih popisa podataka u program (npr. popisi pouzdanih URL-ova).
- (2):** Diskovni prostor koji je potreban za preuzimanje instalacijskog programa, instalaciju proizvoda i pohranu kopije instalacijskog paketa u programskim podacima kao i sigurnosnih kopija nadogradnji proizvoda u sklopu podrške za značajku vraćanja. Proizvod može upotrijebiti više diskovnog prostora u slučaju različitih postavki (npr. kada se pohranjuje više verzija sigurnosne kopije nadogradnji proizvoda, kod ispisa memorije ili čuvanja vrlo velikog broja zapisa dnevnika) ili na zaraženom računalu (npr. zbog značajke karantene). Preporučujemo vam da održavate dovoljno slobodnog diskovnog prostora da biste omogućili provedbu nadogradnje operacijskog sustava i proizvoda tvrtke ESET.
- (3):** Premda to ne preporučujemo, program se može nadograditi ručno putem izmjenjivog medija.

## Podržani jezici

Program ESET Endpoint Antivirus dostupan je za instalaciju i preuzimanje na sljedećim jezicima.

Jezik	Kod jezika	LCID
Engleski (Sjedinjene Američke Države)	en-US	1033
Arapski (Egipat)	ar-EG	3073
Bugarski	bg-BG	1026
Kineski pojednostavljeni	zh-CN	2052
Kineski tradicionalni	zh-TW	1028
Hrvatski	hr-HR	1050
Češki	cs-CZ	1029
Estonski	et-EE	1061
Finski	fi-FI	1035
Francuski (Francuska)	fr-FR	1036
Francuski (Kanada)	fr-CA	3084
Njemački (Njemačka)	de-DE	1031
Grčki	el-GR	1032
*Hebrejski	he-IL	1037
Mađarski	hu-HU	1038
*Indonezijski	id-ID	1057
Talijanski	it-IT	1040
Japanski	ja-JP	1041
Kazaški	kk-KZ	1087
Korejski	ko-KR	1042
*Letonski	lv-LV	1062
Litavski	lt-LT	1063
Nederlands	nl-NL	1043
Norveški	nn-NO	1044
Poljski	pl-PL	1045
Portugalski, brazилски	pt-BR	1046
Rumunjski	ro-RO	1048

Jezik	Kod jezika	LCID
Ruski	ru-RU	1049
Španjolski (Čile)	es-CL	13322
Španjolski (Španjolska)	es-ES	3082
Švedski (Švedska)	sv-SE	1053
Slovački	sk-SK	1051
Slovenski	sl-SI	1060
Tajski	th-TH	1054
Turski	tr-TR	1055
Ukrajinski (Ukrajina)	uk-UA	1058
*Vijetnamski	vi-VN	1066

\* Program ESET Endpoint Antivirus dostupan je na ovom jeziku, no online korisnički vodič nije dostupan (bit će preusmjereni na engleski verziju).

Za promjenu jezika ovog online korisničkog vodiča pogledajte okvir za odabir jezika (u gornjem desnom kutu).

## Prevencija

Prilikom rada na računalu i osobito prilikom pretraživanja interneta imajte na umu da nijedan antivirusni sustav na svijetu ne može potpuno otkloniti opasnost od [raznih prijetnji](#) i [udaljenih napada](#). Za maksimalnu zaštitu i ugodan rad ključno je da antivirusni sustav ispravno upotrebljavate i pridržavate se nekoliko korisnih pravila:

### Redovito preuzimajte aktualizacije

Prema statistici sustava ESET LiveGrid® svakog se dana pojavljuje tisuće novih, jedinstvenih infiltracija koje njihovi autori stvaraju s ciljem zaobilaženja postojećih sigurnosnih mjera i ostvarivanja zarade nauštrb ostalih korisnika. Stručnjaci u laboratoriju za viruse tvrtke ESET svakodnevno analiziraju te prijetnje te pripremaju i izdaju aktualizacije radi stalnog poboljšavanja zaštite korisnika. Da bi se postigla najveća učinkovitost tih nadogradnji, važno ih je ispravno konfigurirati u sustavu. Dodatne informacije o konfiguriranju aktualizacija potražite u poglavljiju [Podešavanje aktualizacije](#).

### Preuzimajte sigurnosne zakrpe

Autori zlonamjernog softvera često koriste razne slabe točke sustava radi učinkovitijeg širenja zlonamjernog koda. Imajući to na umu, proizvođači softvera pomno nadziru pojavu bilo kakvih slabih točaka u svojim aplikacijama te redovito stvaraju i objavljaju sigurnosne aktualizacije za uklanjanje potencijalnih prijetnji. Važno je da takve sigurnosne aktualizacije preuzmete odmah nakon objavljivanja. Microsoft Windows i web preglednici poput sustava Internet Explorer primjeri su programa za koje se redovno objavljaju sigurnosne aktualizacije.

### Sigurnosno kopiranje važnih podataka

Autore zlonamjernog softvera obično nije briga za potrebe korisnika, a aktivnost njihovih zlonamjernih programa često dovodi do potpunog kvara operacijskog sustava i gubitka važnih podataka. Važno je da redovito sigurnosno kopirate važne i povjerljive podatke na neki vanjski medij za pohranu, kao što je DVD ili vanjski tvrdi disk. Takve će mjere opreza uvelike pojednostaviti i ubrzati oporavak podataka u slučaju pada sustava.

## **Redovito skeniranjem provjeravajte postojanje virusa na računalu**

Modul rezidentne zaštite bavi se otkrivanjem većeg broja poznatih i nepoznatih virusa, crva, trojanaca i rootkita. To znači da će svaki put kad pristupite nekoj datoteci ili je otvorite ona biti pretražena radi otkrivanja zlonamjerne aktivnosti. Preporučujemo da pokrenete potpuno skeniranje računala barem jednom mjesечно jer se potpisi zlonamjernog softvera mogu razlikovati, a modul za otkrivanje virusa se aktualizira svakodnevno.

## **Pridržavajte se osnovnih pravila sigurnosti**

Najkorisnije i najučinkovitije pravilo jest – uvijek biti na oprezu. Danas mnoge infiltracije za izvršenje i distribuciju trebaju intervenciju korisnika. Ako ste oprezni prilikom otvaranja novih datoteka, uštedjet ćete vrijeme i trud potreban za čišćenje infiltracija. Evo nekih korisnih smjernica:

- Nemojte posjećivati sumnjive web stranice s višestrukim skočnim prozorima i blještavim oglasima.
- Budite oprezni prilikom instaliranja besplatnih programa, paketa za kodiranje itd. Koristite samo sigurne programe i posjećujte samo sigurne web stranice.
- Budite oprezni prilikom otvaranja privitaka e-pošte, osobito onih uz masovno poslane poruke i poruke od nepoznatih pošiljatelja.
- Nemojte koristiti administratorski račun za svakodnevni rad na računalu.

## **Stranice pomoći**

Dobrodošli u datoteke pomoći programa ESET Endpoint Antivirus. Ovdje navedene informacije upoznat će vas s proizvodom i učiniti vaš rad na računalu sigurnijim.

### **Početak korištenja**

Prije nego što se počnete služiti programom ESET Endpoint Antivirus, imajte na umu da naš program [mogu upotrebljavati korisnici povezani putem programa ESET Security Management Center](#) ili se on može upotrebljavati [samostalno](#). Preporučujemo i da se upoznate s raznim [vrstama otkrivenih prijetnji i daljinskih napada](#) s kojima se možete susresti prilikom upotrebe računala.

Pogledajte [nove funkcije](#) kako biste upoznali funkcije uvedene u ovoj verziji programa ESET Endpoint Antivirus. Pripremili smo i vodič za podešavanje i prilagodbu osnovnih postavki programa ESET Endpoint Antivirus.

### **Korištenje stranica pomoći programa ESET Endpoint Antivirus**

Teme pomoći podijeljene su na nekoliko poglavlja i potpoglavlja kako bi se pružio kontekst i olakšalo snalaženje. Povezane informacije možete pronaći jednostavnim pregledavanjem strukture stranica pomoći.

Pritisnite tipku **F1** da biste saznali dodatne informacije o svakom prozoru u programu. Prikazat će se stranica pomoći povezana s trenutno otvorenim prozorom.

Stranice pomoći možete pretraživati putem ključne riječi ili unosom riječi ili izraza. Razlika između te dvije metode je u tome da se ključna riječ može logički povezati sa stranicama pomoći koje ne sadrže dotičnu ključnu riječ u tekstu. Pretraživanjem prema riječima i izrazima pregledava se sadržaj svih stranica i prikazuju samo one koje sadrže traženu riječ ili izraz.

U svrhu dosljednosti i radi sprečavanja zabune, terminologija koja se upotrebljava u ovom priručniku temelji se na nazivima parametara programa ESET Endpoint Antivirus. Također upotrebljavamo jedinstven skup simbola za naglašavanje tema od posebnog interesa ili značaja.

**i** Napomena je kratko opažanje. Premda ih možete preskočiti, napomene vam mogu pružiti vrijedne informacije, kao što su posebne značajke ili veza na povezanu temu.

**!** Ovaj naslov zahtijeva vašu pažnju i ne preporučujemo njegovo preskakanje. Obično pruža važne informacije koje nisu od kritične važnosti.

**!** Ove informacije zahtijevaju dodatnu pažnju i oprez. Upozorenja su navedena kako bi vas spriječila da napravite potencijalno štetne pogreške. Tekst u zagradama upozorenja pročitajte s razumijevanjem jer se odnosi na vrlo osjetljive postavke sustava ili određene rizike.

**✓** To je primjer upotrebe ili praktični primjer koji vam pruža pomoć u razumijevanju načina na koji se određene funkcije mogu upotrebljavati.

Konvencija	Značenje
<b>Podebljan tekst</b>	Nazivi stavki sučelja kao što su okviri i gumbi opcija.
<i>Kosa slova</i>	Rezervirana mjesta za informacije koje pružate. Na primjer, naziv datoteke ili put znači da morate upisati stvarni put ili naziv datoteke.
<i>Courier New</i>	Uzorci koda ili naredbe.
<u>Hiperveza</u>	Omogućuje brz i jednostavan pristup temama na koje se unakrsno referira ili vanjskoj web-lokaciji. Hiperveze su plave boje i mogu biti podcrtane.
<code>%ProgramFiles%</code>	Direktorij sustava Windows u koji se pohranjuju programi instalirani na sustavu Windows.

**Mrežna pomoć** primarni je izvor sadržaja za pomoć. Najnovija verzija mrežne pomoći prikazat će se automatski kada imate internetsku vezu koja radi.

## Dokumentacija za daljinski upravljane krajnje točke

ESET-ovim poslovnim programima i programom ESET Endpoint Antivirus može se daljinski upravljati na klijentskim radnim stanicama, serverima i mobilnim uređajima u umreženom okruženju s jedne središnje lokacije. Administratori sustava s više od 10 klijentskih radnih stanica mogli bi instalirati jedan od ESET-ovih alata za daljinsko upravljanje radi instalacije ESET-ovih rješenja, upravljanja zadacima, nametanja [sigurnosnih pravila](#), nadgledanja statusa sustava i brzog rješavanja problema ili prijetnji na udaljenim računalima s jedne središnje lokacije.

## ESET-ovi alati za daljinsko upravljanje

Programom ESET Endpoint Antivirus možete upravljati daljinski ili pomoću alata ESET Security Management Center ili ESET Cloud Administrator.

- [Uvod u ESET PROTECT](#)
- [Uvod u ESET PROTECT Cloud](#)

## Alati trećih strana za daljinsko upravljanje

- [Daljinsko praćenje i upravljanje \(RMM\)](#)

## Najbolje prakse

- [Povežite sve krajnje točke na kojima se nalazi program ESET Endpoint Antivirus uz pomoć programa ESET PROTECT](#)
- Zaštitite [postavke naprednog podešavanja](#) na povezanim klijentskim računalima da biste spriječili neovlaštene izmjene
- Primijenite [preporučeno pravilo](#) da biste nametnuli dostupne sigurnosne funkcije
- [Smanjenje korisničkog sučelja](#) – za smanjenje ili ograničenje korisničke interakcije s programom ESET Endpoint Antivirus

## Vodiči

- [Korištenje načina nadjačavanja](#)
- [Instalacija programa ESET Endpoint Antivirus pomoću GPO-a ili SCCM-a](#)

## Uvod u ESET PROTECT

ESET PROTECT omogućuje upravljanje ESET-ovim programima na radnim stanicama, serverima i mobilnim uređajima u umreženom okruženju s jedne središnje lokacije.

Upotrebom web konzole ESET PROTECT možete instalirati ESET-ova rješenja, upravljati zadacima, nametati sigurnosna pravila, nadgledati status sustava i brzo rješavati probleme ili prijetnje na udaljenim računalima. Isto tako pogledajte [pregled arhitektturnih elemenata i elemenata infrastrukture za ESET PROTECT](#), [Početak korištenja web konzole ESET PROTECT](#) i [Podržana okruženja za dodjeljivanje radne površine](#).

ESET PROTECT se sastoji od sljedećih komponenti:

- [ESET PROTECT Server](#) – ESET PROTECT server može se instalirati na Windows i Linux serverima, a dostupan je i kao virtualni uređaj. On komunicira s agentima te prikuplja i sprema podatke o aplikaciji u bazu podataka.
- [ESET PROTECT Web konzola](#) – ESET PROTECT primarno je sučelje koje omogućuje upravljanje klijentskim računalima u vašoj okolini. Prikazuje pregled statusa klijenata u mreži i omogućuje daljinsku instalaciju rješenja tvrtke ESET na neupravljenim računalima. Nakon što instalirate ESET PROTECT server (server), možete pristupiti web konzoli s pomoću svojeg web preglednika. Ako odlučite omogućiti pristup web serveru putem interneta, možete upotrebljavati ESET PROTECT s bilo koje lokacije i ili uređaja s internetskom vezom.
- [ESET Management Agent](#) – ESET Management agent omogućava komunikaciju između ESET PROTECT servera i klijentskih računala. Agent morate instalirati na klijentsko računalo kako bi se mogla uspostaviti komunikacija između tog računala i ESET PROTECT servera. Budući da je smješten na klijentskom računalu i može pohraniti više sigurnosnih scenarija, korištenje ESET Management agenta znatno skraćuje vrijeme reakcije na nove prijetnje. Upotrebom ESET PROTECT web konzole možete [instalirati ESET Management agent](#) na neupravljana računala identificirana putem servisa Active Directory ili ESET [RD Senzora](#). Također po potrebi možete [ručno instalirati ESET Management agent](#) na klijentska računala.
- [Rogue Detection Sensor](#) – ESET PROTECT Rogue Detection (RD) Sensor otkriva neupravljana računala prisutna u vašoj mreži i šalje informacije o njima na ESET PROTECT server. To omogućuje jednostavno dodavanje novih klijentskih računala u vašu zaštićenu mrežu. RD Sensor pamti računala koja su otkrivena i neće

slati iste informacije dvaput.

- [Apache HTTP Proxy](#) – servis koji se može upotrebljavati u kombinaciji s programom ESET PROTECT za sljedeće:

ODistribuciju nadogradnji na klijentska računala i instalacijskih paketa na ESET Management agent.

OProsljeđivanje komunikacije od ESET Management agenata do ESET PROTECT servera.

- [Mobile Device Connector](#) – komponenta koja omogućava upravljanje mobilnim uređajima s pomoću programa ESET PROTECT i pritom vam dopušta upravljanje mobilnim uređajima (Android i iOS) i primjenu programa ESET Endpoint Security za Android.
- [ESET PROTECT Virtualni uređaj \(VA\)](#) – ESET PROTECT VA namijenjen je za korisnike koji žele upotrebljavati program ESET PROTECT u virtualiziranom okruženju.
- [ESET PROTECT Virtual Agent Host](#) – komponenta programa ESET PROTECT koja virtualizira subjekte agenta da bi omogućila upravljanje virtualnim računalima bez agenta. Ovo rješenje aktivira automatizaciju, iskorištavanje dinamičkih grupa i istu razinu upravljanja zadacima kao i ESET Management agent na fizičkim računalima. Virtualni agent prikuplja informacije s virtualnih računala i šalje ih ESET PROTECT serveru.
- [Mirror alat](#) – mirror alat potreban je za izvanmrežne nadogradnje modula. Ako klijentska računala nemaju internetsku vezu, možete upotrijebiti mirror alat za preuzimanje datoteka za nadogradnju s ESET-ovih servera za nadogradnju i pohraniti ih lokalno.
- [ESET Remote Deployment Tool](#) – ovaj alat omogućuje instalaciju cjelovitih paketa stvorenih na <%PRODUCT%> web konzoli. Predstavlja praktičan način za distribuciju ESET Management agenta s ESET-ovim programom na računala putem mreže.
- [ESET Business Account](#) – novi portal za licenciranje ESET-ovih poslovnih programa omogućuje vam upravljanje licencama. Pogledajte odjeljak [ESET Business Account](#) ovoga dokumenta da biste pronašli upute za aktivaciju programa ili potražite više informacija o uporabi programa ESET Business Account u [Vodiču za korisnike programa](#) ESET Business Account. Ako već imate korisničko ime i lozinku koje je izdala tvrtka ESET i koje želite pretvoriti u licenčni ključ, pogledajte odjeljak [Pretvaranje podataka o naslijedenoj licenci](#).
- [ESET Enterprise Inspector](#) – sveobuhvatni sustav za otkrivanje i odgovor sigurnosnog programa koji uključuje funkcije kao što su: otkrivanje incidenata, upravljanje incidentima i odgovor na incidente, prikupljanje podataka, pokazatelji otkrivanja kompromisa, otkrivanje anomalija, otkrivanje ponašanja i kršenja pravila.

Služite se web konzolom ESET PROTECT da biste instalirali ESET-ova rješenja, upravljali zadacima, nametali [sigurnosna pravila](#), nadgledali status sustava i brzo rješavali probleme ili prijetnje na udaljenim računalima.

 Dodatne informacije potražite u odjeljku [Mrežna pomoć za ESET PROTECT](#).

## Uvod u ESET PROTECT Cloud

ESET PROTECT Cloud omogućuje vam upravljanje ESET-ovim programima na radnim stanicama i serverima u umreženom okruženju iz jedne središnje lokacije, bez preduvjeta posjedovanja fizičkog ili virtualnog servera kao za ESET PROTECT ili ESMC. Pomoću (ESET PROTECT Cloud web konzole) možete instalirati ESET-ova rješenja, upravljati zadacima, provoditi sigurnosna pravila, pratiti status sustava i brzo reagirati na probleme ili prijetnje na udaljenim računalima.

- [Pročitajte više o ovome u online korisničkom vodiču za ESET PROTECT Cloud](#)

## Postavke zaštićene lozinkom

Kako bi pružio maksimalnu zaštitu vašem sustavu, program ESET Endpoint Antivirus mora se pravilno konfigurirati. Svaka nestručna promjena ili postavka može dovesti do smanjenja sigurnosti i razine zaštite klijenta. Da bi ograničio pristup korisnika naprednim postavkama, administrator može zaštititi postavke lozinkom.

Administrator može stvoriti pravilo da bi lozinkom zaštitio postavke naprednog podešavanja programa ESET Endpoint Antivirus na povezanim klijentskim računalima. Za stvaranje novoga pravila učinite sljedeće:

1. U ESET PROTECT web konzoli ili u ESMC web konzoli kliknite **Pravila** u glavnom izborniku s lijeve strane.
2. Kliknite "**Novo pravilo**".
3. Odredite naziv svom novom pravilu i, ako želite, dodajte mu kratak opis. Kliknite gumb "**Dalje**".
4. Na popisu programa odaberite "**ESET Endpoint za Windows**".
5. Kliknite **Korisničko sučelje** u popisu **Postavke** i proširite **Podešavanje pristupa**.
6. Ovisno o verziji programa ESET Endpoint Antivirus, kliknite traku klizača da biste aktivirali **Lozinku za zaštitu postavki**. Imajte na umu da verzija 7 ESET-ovih Endpoint programa pruža poboljšanu zaštitu. Ako imate i verziju 7 i verziju 6 Endpoint programa na mreži, preporučujemo da stvorite dva zasebna pravila s različitim lozinkama za svaku verziju.
7. U skočnom prozoru stvorite novu lozinku, potvrdite je i kliknite "**U redu**". Kliknite "**Dalje**".
8. Dodijelite pravila klijentima. Kliknite **Dodijeli** i odaberite računala ili grupe računala koje ćete zaštititi lozinkom. Kliknite **U redu** za potvrdu.
9. Provjerite jesu li sva željena klijentska računala na popisu objekata i kliknite "**Dalje**".
10. Pregledajte postavke pravila u sažetku i kliknite "**Završi**" da biste spremili novo pravilo.

The screenshot shows the 'New Policy' configuration screen in the ESET Security Management Center. The left sidebar includes links for Dashboard, Computers, Threats, Reports, Client Tasks, Installers, Policies (selected), Computer Users, Notifications, Status Overview, and More. The main content area is titled 'New Policy' under 'Policies > New Policy'. On the left, a navigation bar has 'Basic' and 'Settings' selected. The right side contains several configuration sections: 'DETECTION ENGINE' (Update, Network Protection, Web and Email, Device Control, Tools), 'USER INTERFACE' (Customization, Override Mode), and 'USER INTERFACE ELEMENTS' (Alerts and Notifications, Access Setup). Under 'USER INTERFACE ELEMENTS', there are sections for 'PASSWORD SETTINGS FOR VERSION 6 AND BELOW' and 'PASSWORD SETTINGS FOR VERSION 7 AND ABOVE', each with various configuration options like 'Password protect' and 'Set password' settings, and checkboxes for requiring administrator rights.

## Što su pravila

Administrator može proslijediti određene konfiguracije ESET-ovim programima koji se pokreću na klijentskim računalima uz pomoć pravila s ESET PROTECT web konzole ili ESMC web konzole. Pravila se mogu primjenjivati izravno na pojedinačna računala ili grupe računala. Također možete dodijeliti više pravila jednom računalu ili grupi.

Korisnik mora imati sljedeća dopuštenja za stvaranje novoga pravila: razinu dopuštenja "čitanje" kako bi čitao popis pravila, razinu dopuštenja "upotreba" kako bi dodjeljivao pravila ciljanim računalima te razinu dopuštenja "pisanje" kako bi stvarao, mijenjao ili uređivao pravila.

Pravila se primjenjuju redoslijedom kojim su raspoređene statičke grupe. To ne vrijedi za dinamičke grupe u kojima se pravila prvo primjenjuju na podređene dinamičke grupe. Time se omogućuje da se pravila s većim učinkom primijene na vrh stabla grupe, a specifična pravila na podgrupe. Upotrebom [zastavica](#) korisnik programa ESET Endpoint Antivirus s pristupom grupama smještenima visoko na stablu može nadjačati pravila nižih grupa. Algoritam je objašnjen u odjeljku [Mrežna pomoć za ESET PROTECT](#).

**i** Preporučuje se dodjeljivanje generičkih pravila (npr. pravila za server za nadogradnju) grupama koje su na višoj razini stabla grupe. Specifična pravila (npr. postavke za kontrolu uređaja) trebaju se dodijeliti niže na stablu grupe. Niže pravilo obično nadjačava postavke viših pravila nakon spajanja (osim ako je drugačije definirano [zastavicama pravila](#)).

## Spajanje pravila

Pravilo koje se primjenjuje na klijent obično je rezultat spajanja više pravila u jedno konačno pravilo. Pravila se spajaju jedno po jedno. Prilikom spajanja pravila općenito vrijedi da novije pravilo uvijek zamjenjuje postavke starijeg pravila. Da biste promijenili takvo ponašanje, upotrijebite [zastavice za pravila](#) (dostupne za svaku

postavku).

Prilikom stvaranja pravila primijetit ćete da neke postavke imaju dodatna pravila (zamjena / dodavanje na kraj / dodavanje na početak) koja možete konfigurirati.

- **Zamjena** – zamjenjuje se cijeli popis, dodaju nove vrijednosti i uklanjuju sve prethodne.
- **Dodavanje na kraj** – stavke se dodaju na dno popisa koji se trenutačno primjenjuje (mora biti drugo pravilo, lokalni popis uvijek će se prebrisati).
- **Dodavanje na početak** – stavke se dodaju na vrh popisa (lokalni će se popis prebrisati).

ESET Endpoint Antivirus podržava spajanje lokalnih postavki s udaljenim pravilima na posve nov način. Ako je postavka popis (primjerice, popis blokiranih web stranica), a daljinsko je pravilo u sukobu s postojećom lokalnom postavkom, daljinsko je pravilo briše. Možete odlučiti kako kombinirati lokalne i daljinske popise odabirom različitih pravila spajanja za:

- Postavke spajanja za daljinska pravila.
- Spajanje daljinskih i lokalnih pravila – lokalne postavke s nastalim daljinskim pravilom.

Za više informacija o spajanju pravila slijedite upute iz online korisničkog priručnika za [ESET PROTECT](#) i pogledajte [primjer](#).

## Kako funkcioniraju zastavice

Pravilo koje se primjenjuje na klijentsko računalo obično je rezultat spajanja više pravila u jedno konačno pravilo. Prilikom spajanja pravila možete prilagoditi očekivano ponašanje konačnog pravila na temelju redoslijeda primijenjenih pravila upotrebom zastavica pravila. Zastavice određuju kako će pravilo postupati s određenom postavkom.

Za svaku postavku možete odabrati jednu od sljedećih zastavica:

<b>Nemoj primijeniti</b>	Nemoj primjeniti – nijedna postavka s ovom zastavicom ne postavlja se pravilom. Budući da se postavka ne postavlja pravilom, može se promijeniti drugim pravilima primijenjenima naknadno.
<b>Primijeni</b>	Primijeni – postavke sa zastavicom " <b>Primijeni</b> " primijenit će se na klijentsko računalo. Međutim, prilikom spajanja pravila mogu se prebrisati drugim pravilima primijenjenima naknadno. Kada se pravilo pošalje klijentskom računalu s postavkama označenima ovom zastavicom, te će postavke promijeniti lokalnu konfiguraciju klijentskog računala. Budući da postavka nije prisilno primijenjena, može se promijeniti drugim pravilima primijenjenima naknadno.
<b>Obavezno primijeni</b>	Obavezno primijeni – postavke sa zastavicom " <b>Obavezno primijeni</b> " imaju prioritet i ne mogu se prebrisati nijednim drugim pravilom primijenjenim naknadno (čak i ako ono ima zastavicu " <b>Obavezno primijeni</b> "). Time se osigurava da druga pravila primjenjena naknadno neće moći promijeniti ovu postavku tijekom spajanja. Kada se pravilo pošalje klijentskom računalu s postavkama označenima ovom zastavicom, te će postavke promijeniti lokalnu konfiguraciju klijentskog računala.

**Scenarij:** administrator želi omogućiti korisniku Johnu da stvara ili uređuje pravila u svojoj glavnoj grupi i da vidi sva pravila koja stvori administrator, uključujući pravila koja imaju zastavice "Obavezno primjeni". Administrator želi omogućiti Johnu da vidi sva pravila, no ne i da uređuje postojeća pravila koja stvori administrator. John može stvarati ili uređivati pravila samo u svojoj glavnoj grupi naziva San Diego.

Rješenje: administrator mora slijediti ove korake:

#### Stvaranje prilagođenih statičkih grupa i skupova dopuštenja

1. Stvorite novu [statičku grupu](#) naziva *San Diego*.
2. Stvorite novi [skup dopuštenja](#) naziva *Pravilo – Sve John* s pristupom statičkoj grupi *Sve* i razinom dopuštenja "čitanje" za "**Pravila**".
3. Stvorite novi [skup dopuštenja](#) naziva *Pravilo John* s pristupom statičkoj grupi *San Diego* i pristupom razini dopuštenja "pisanje" za **grupu i računala i pravila**. Taj skup dopuštenja omogućuje Johnu stvaranje ili uređivanje pravila u njegovoj glavnoj grupi *San Diego*.
4. Stvorite novog [korisnika](#) Johna pa u odjeljku "**Skupovi dopuštenja**" odaberite *Pravilo – Sve John* i *Pravilo John*.



#### Stvaranje pravila

5. Stvorite novo [pravilo Sve – aktiviraj firewall](#), proširite odjeljak **Postavke**, odaberite "ESET Endpoint za Windows", idite na "Osobni firewall" > "Osnovno" i primijenite sve postavke zastavicom "Obavezno primjeni". Proširite odjeljak "Dodjela" i odaberite statičku grupu *Sve*.
6. Stvorite novo [pravilo Johnova grupa – aktiviraj firewall](#), proširite odjeljak "Podešavanje", odaberite ESET Endpoint za Windows, idite na "Osobni firewall" > "Osnovno" i primijenite sve postavke zastavicom "Primjeni". Proširite odjeljak "Dodjela" i odaberite statičku grupu *San Diego*.

#### Rezultat

Prvo će se primijeniti pravila koja stvori administrator jer su na postavke pravila primjenjene zastavice "Obavezno primjeni". Postavke s primijenjenom zastavicom "Obavezno primjeni" imaju prioritet i ne mogu se prebrisati drugim pravilom primijenjenim naknadno. Pravila koja stvori korisnik John primjenit će se nakon pravila koja stvori administrator.

Idite na "**Više > Grupe > San Diego**" da biste vidjeli konačan redoslijed pravila. Odaberite računalo i odaberite "**Prikaži pojedinosti**". U odjeljku "**Konfiguracija**" kliknite "**Primjenjena pravila**".

## Samostalno korištenje programa ESET Endpoint Antivirus

Ovaj dio korisničkog priručnika namijenjen je korisnicima koji [koriste ESET Endpoint Antivirus](#) bez programa ESET PROTECT, ESET Security Management Center ili ESET PROTECT Cloud. Svaka je značajka i funkcija programa ESET Endpoint Antivirus u potpunosti dostupna ovisno o pravima računa korisnika.

## Metoda instalacije

Postoji nekoliko metoda za instalaciju verzije 8.x programa ESET Endpoint Antivirus na klijentske radne stanice, osim ako daljinski ne [instalirate program ESET Endpoint Antivirus na klijentske radne stanice pomoću programa ESET PROTECT, ESET Security Management Center ili ESET PROTECT Cloud](#).

- [Instalirajte ili nadogradite ESET Endpoint Antivirus na verziju 6.6.x](#)

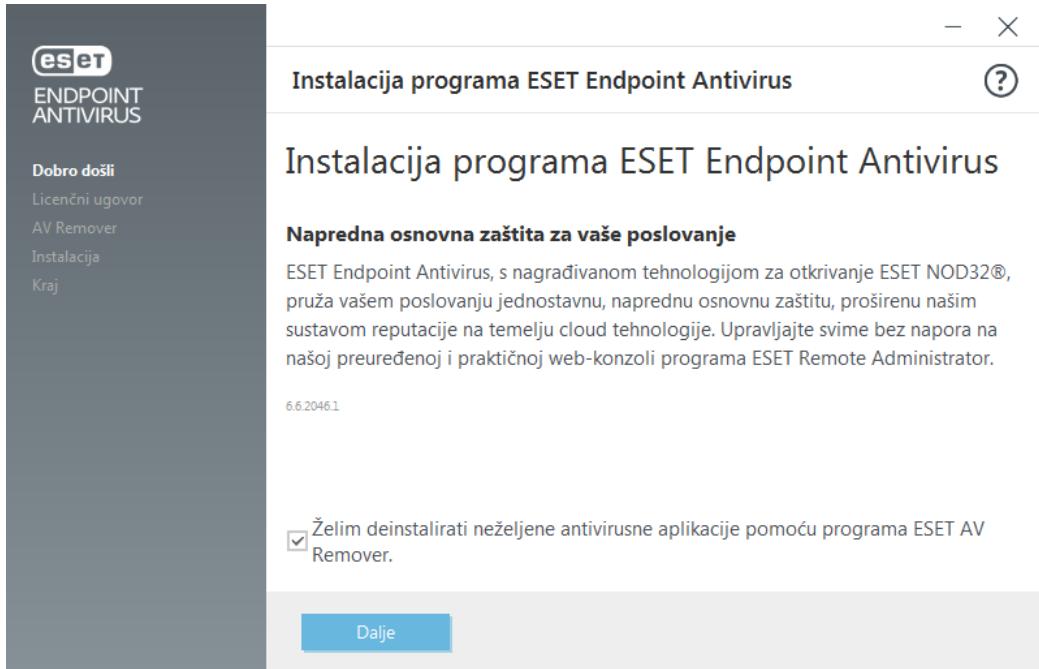
Metoda	Svrha	Link za preuzimanje
<a href="#">Instalacija pomoću programa ESET AV Remover</a>	Alat ESET AV Remover pomoći će vam da uklonite gotovo sve antivirusne programe prethodno instalirane na sustavu prije nego što nastavite instalaciju.	<a href="#">Preuzmi 64-bitni</a> <a href="#">Preuzmi 32-bitni</a>
<a href="#">Instalacija (.exe)</a>	Instalacijski postupak bez alata ESET AV Remover.	N/A

Metoda	Svrha	Link za preuzimanje
<a href="#">Instalacija (.msi)</a>	U poslovnim okruženjima, instalacijski program .msi preferirani je instalacijski paket. To je prvenstveno zbog izvanmrežnih i daljinskih instalacija koje se koriste raznim alatima, kao što je ESET Security Management Center.	<a href="#">Preuzmi 64-bitni</a> <a href="#">Preuzmi 32-bitni</a>
<a href="#">Instalacija putem naredbenog retka</a>	ESET Endpoint Antivirus može se instalirati lokalno upotrebom naredbenog retka ili na daljinu upotrebom zadatka klijenta iz programa ESET PROTECT ili ESET Security Management Center.	N/A
<a href="#">Instalacija pomoću GPO-a ili SCCM-a</a>	Upotrijebite alate za upravljanje poput GPO-a ili SCCM-a da biste instalirali ESET Management Agent i program ESET Endpoint Antivirus na klijentske radne stanice.	N/A
<a href="#">Instalacija pomoću RMM alata</a>	ESET-ovi DEM dodaci alata za daljinsko praćenje i upravljanje (RMM) omogućuju instalaciju programa ESET Endpoint Antivirus na klijentske radne stanice.	N/A

Program ESET Endpoint Antivirus [dostupan je na više od 30 jezika](#).

## Instalacija pomoću programa ESET AV Remover

Prije nego nastavite instalacijski postupak, važno je da deinstalirate sve sigurnosne aplikacije koje su već prisutne na računalu. Odaberite potvrđni okvir pored mogućnosti **Želim deinstalirati neželjene antivirusne aplikacije pomoću programa ESET AV Remover** kako bi program ESET AV Remover skenirao vaš sustav i uklonio sve podržane sigurnosne aplikacije. Ostavite potvrđni okvir neoznačen i kliknite **Nastavi** da biste instalirali program ESET Endpoint Antivirus bez pokretanja programa ESET AV Remover.

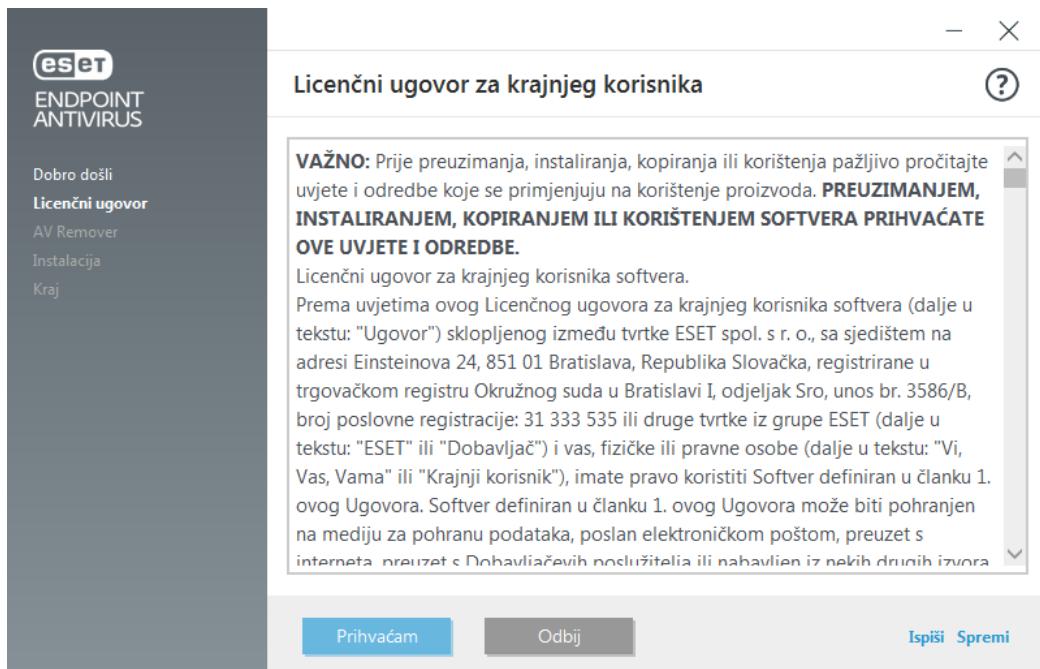


## ESET AV Remover

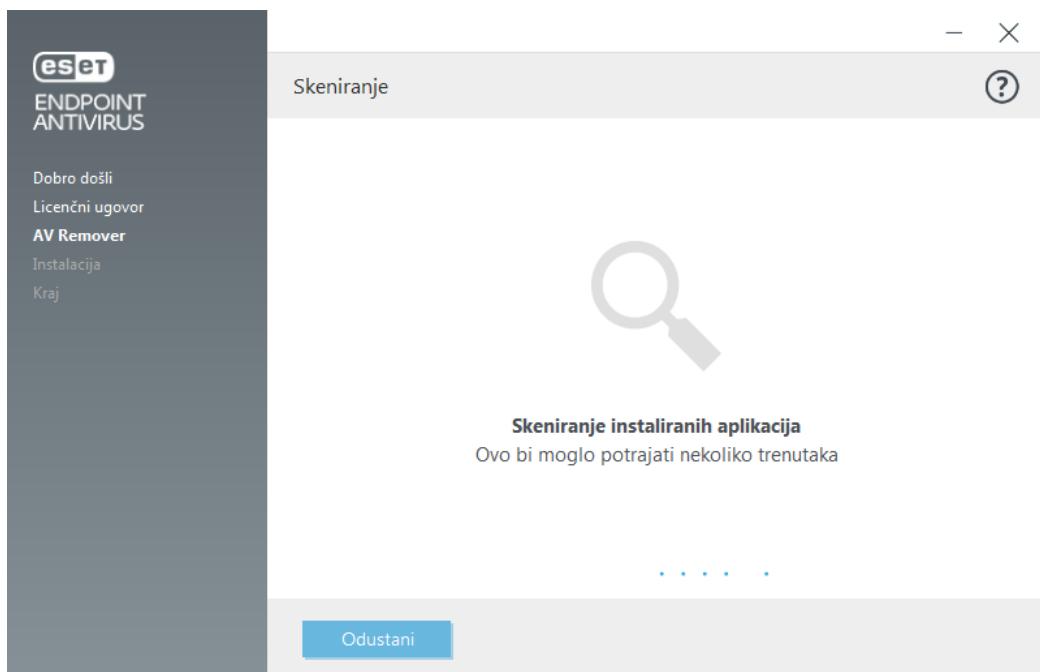
ESET AV Remover alat je koji će vam pomoći da uklonite gotovo sve antivirusne programe prethodno instalirane na sustavu. Slijedite upute u nastavku kako biste uklonili postojeći antivirusni program pomoću programa ESET AV Remover:

1. Da biste vidjeli popis antivirusnih programa koje program ESET AV Remover može ukloniti, [pogledajte članak iz ESET-ove baze znanja](#).

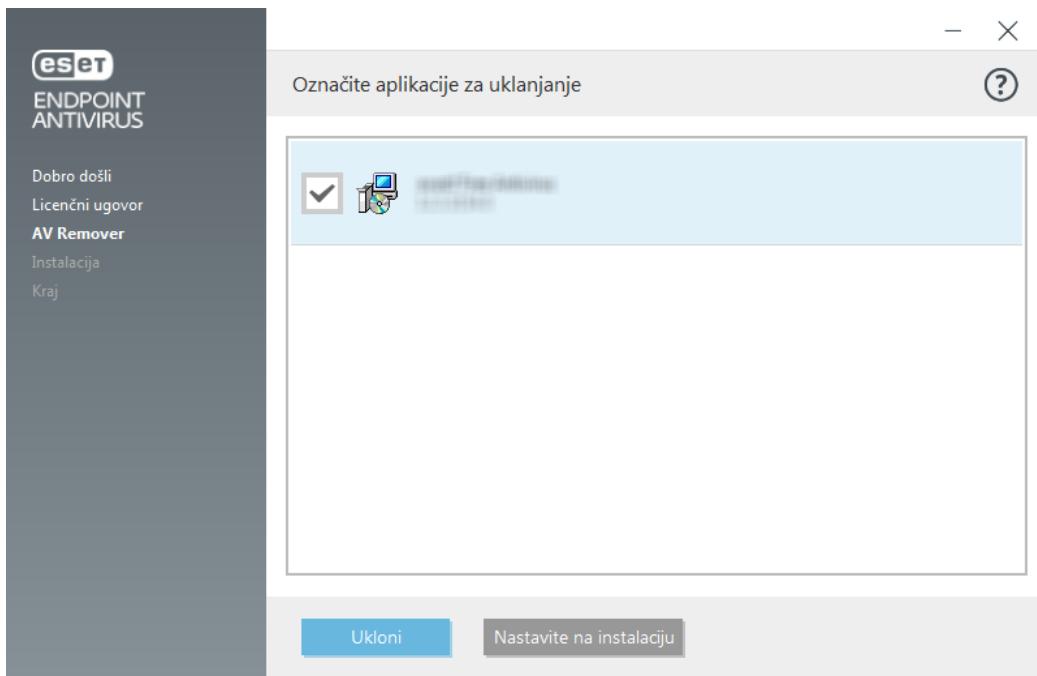
2. Pročitajte Licenčni ugovor za krajnjeg korisnika i kliknite **Prihvati** da biste prihvatili uvjete. Ako kliknete **Odbij**, instalacija programa ESET Endpoint Antivirus nastavit će se bez uklanjanja postojećih sigurnosnih aplikacija s računala.



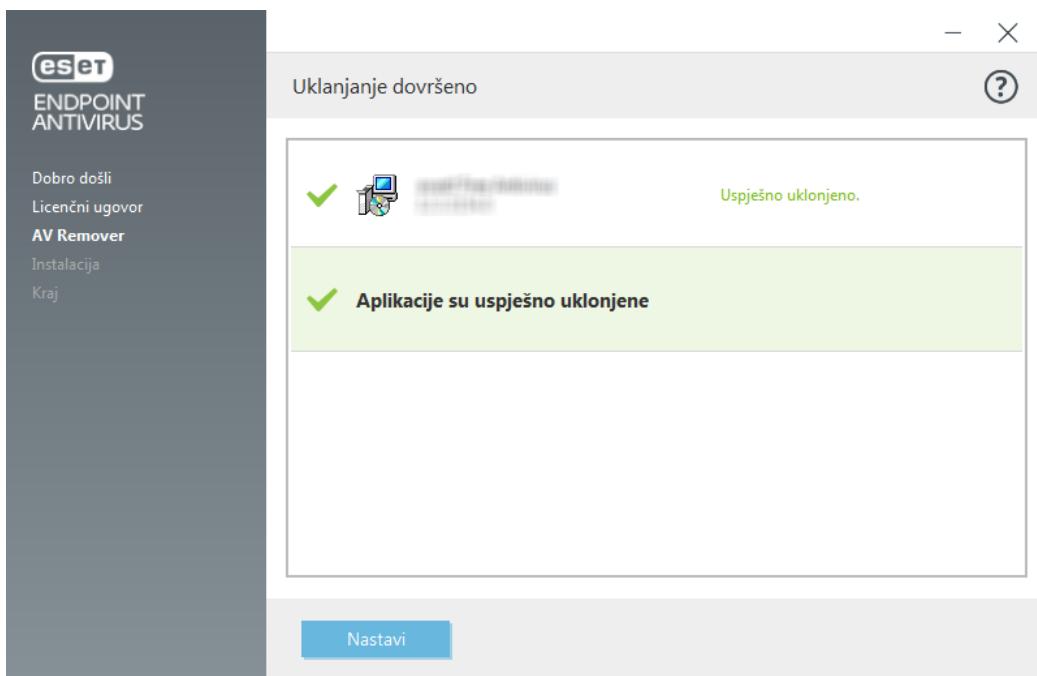
3. ESET AV Remover započet će pretraživanje vašeg sustava kako bi pronašao antivirusni softver.



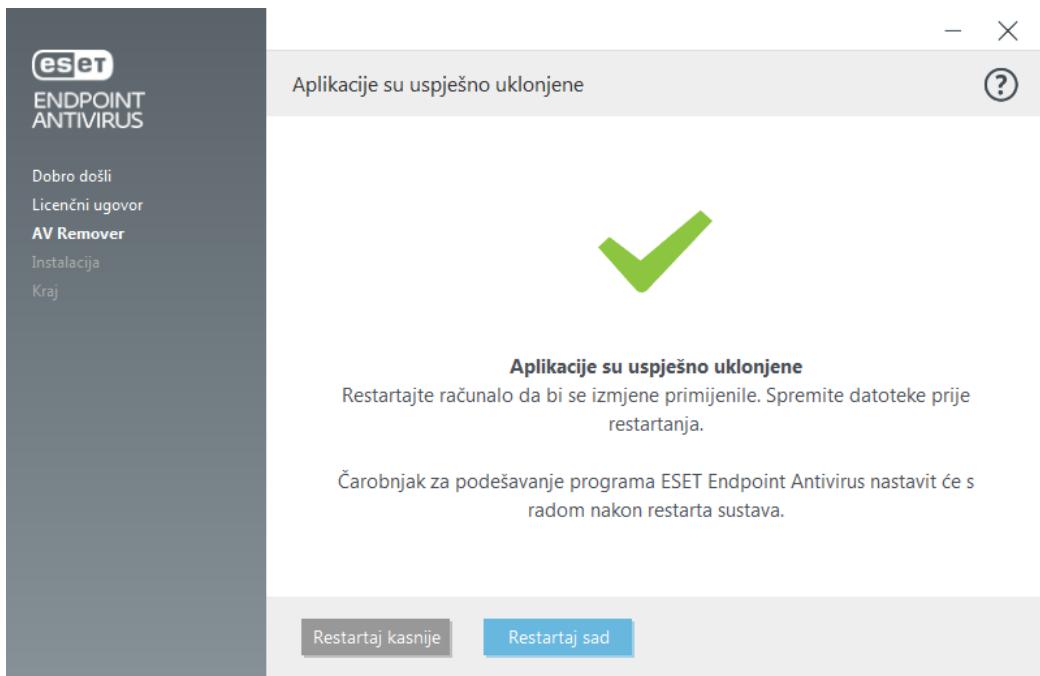
4. Odaberite bilo koju od antivirusnih aplikacija na popisu i kliknite **Ukloni**. Uklanjanje bi moglo potrajati nekoliko trenutaka.



5. Ako je uklanjanje bilo uspješno, kliknite **Nastavi**.



6. Restartajte računalo kako bi se primijenile postavke i nastavite instalaciju programa ESET Endpoint Antivirus.  
Ako je deinstalacija bila neuspješna, pogledajte odjeljak [Deinstalacija pomoću programa ESET AV Remover završila je s pogreškom](#) u ovom vodiču.



## Deinstalacija pomoću programa ESET AV Remover završila je s pogreškom

Ako nije moguće ukloniti antivirusni program pomoću programa ESET AV Remover, dobit ćete obavijest da ESET AV Remover možda ne podržava aplikaciju koju pokušavate ukloniti. Posjetite stranicu s [popisom podržanih proizvoda](#) ili [programima za deinstalaciju uobičajenog antivirusnog softvera za sustav Windows](#) u ESET-ovoj bazi znanja da biste saznali može li se taj specifični program ukloniti.

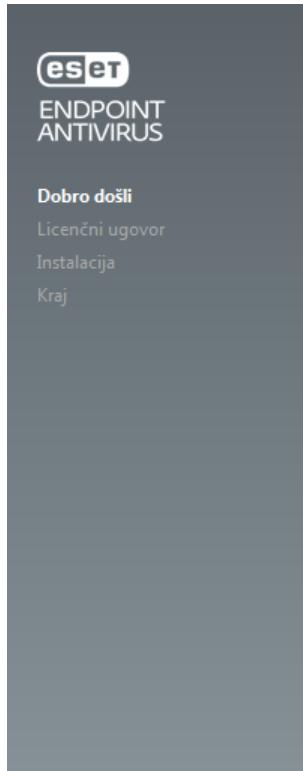
Ako deinstalacija sigurnosnog programa nije uspjela ili je neka od njegovih komponenti deinstalirana djelomično, pojavit će se uputa "**Ponovno pokreni i ponovno skeniraj**". Potvrdite kontrolu korisničkog računa (UAC) nakon pokretanja sustava i nastavite s postupkom skeniranja i deinstalacije.

Po potrebi kontaktirajte [ESET-ovu korisničku službu](#) kako biste joj poslali zahtjev za podršku, a pritom će vam biti potrebna datoteka **AppRemover.log** kako biste pomogli tehničarima tvrtke ESET. Datoteka **AppRemover.log** nalazi se u mapi **eset**. Idite na **%TEMP%** u programu Windows Explorer da biste pristupili toj mapi. ESET-ova korisnička služba brzo će vam odgovoriti i pomoći da pronađete rješenje.

## Instalacija (.exe)

Kada pokrenete instalacijski program .exe, čarobnjak za instalaciju provest će vas kroz instalacijski postupak.

**!** Provjerite nije li na računalu instaliran još neki antivirusni program. Ako su na jednom računalu instalirana dva ili više antivirusnih programa, mogli bi se međusobno sukobljavati. Ako su na računalu instalirani još neki antivirusni programi, preporučujemo da ih deinstalirate. Pogledajte naš [članak baze znanja](#) (dostupan na engleskom i nekoliko drugih jezika).



## Instalacija programa ESET Endpoint Antivirus

### Napredna osnovna zaštita za vaše poslovanje

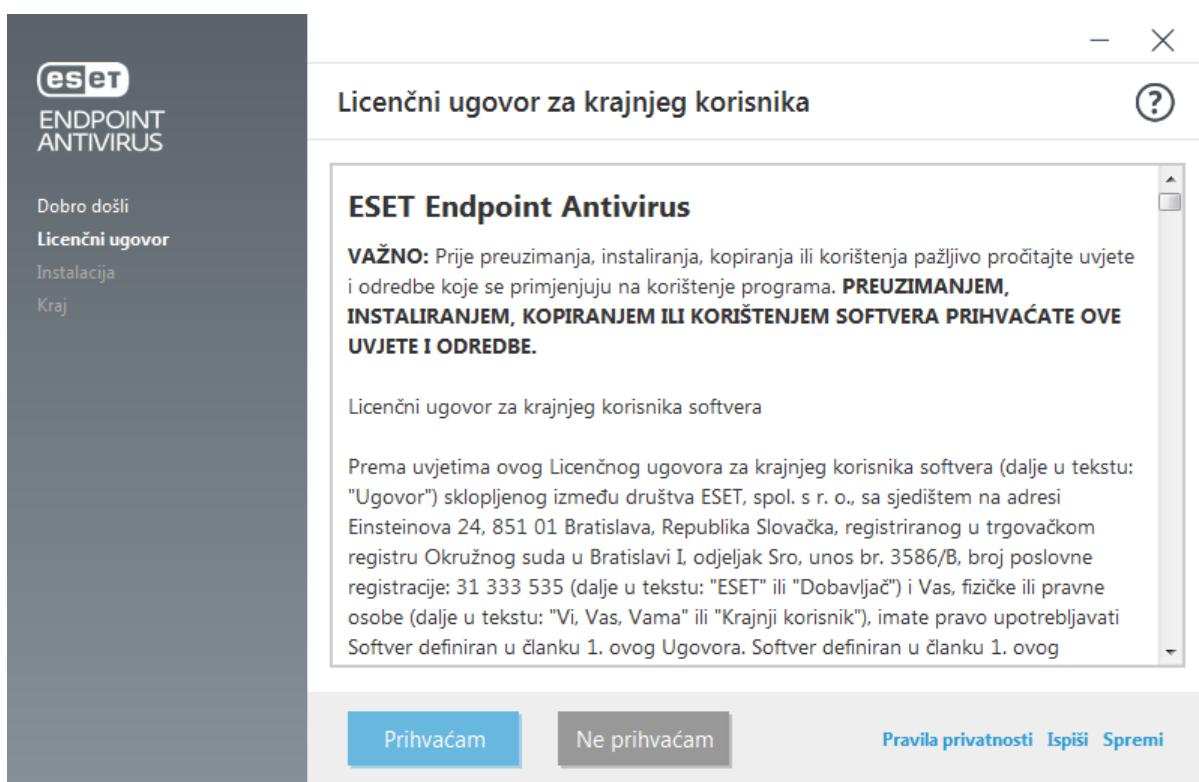
ESET Endpoint Antivirus, s nagrađivanom tehnologijom za otkrivanje ESET NOD32®, pruža vašem poslovanju jednostavnu, naprednu osnovnu zaštitu, proširenu našim sustavom reputacije na temelju cloud tehnologije. Upravlajte svime bez napora na našoj preuređenoj i praktičnoj web-konzoli programa ESET Remote Administrator.

7.0.2074.0

Dalje

Hrvatski

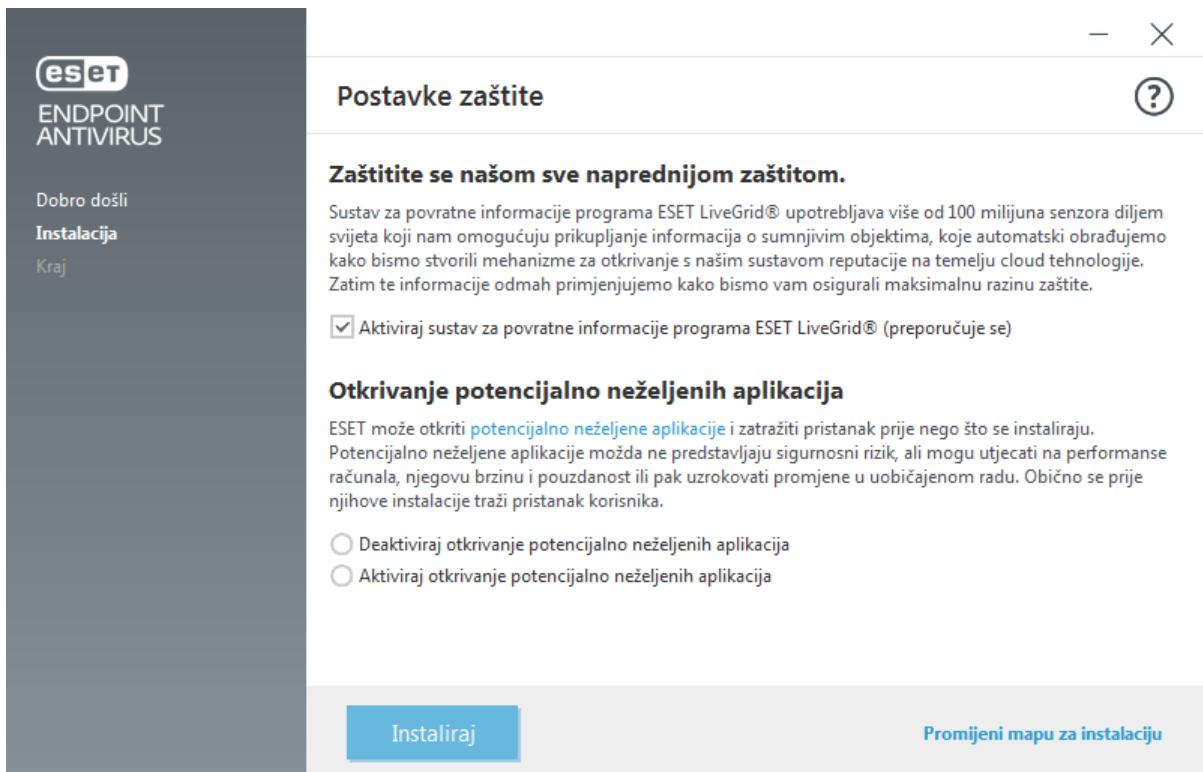
1. Pročitajte Lisenčni ugovor za krajnjeg korisnika i kliknite **Prihvaćam** da biste prihvatili uvjete Lisenčnog ugovora za krajnjeg korisnika. Kliknite **Dalje** nakon što prihvate uvjete kako biste nastavili instalaciju.



2. Odaberite hoćete li aktivirati sustav za povratne informacije [ESET LiveGrid®](#). ESET LiveGrid® osigurava da tvrtka ESET odmah i neprekidno bude obaviještena o novim infiltracijama radi pružanja bolje zaštite svojim korisnicima. Sustav dopušta slanje novih prijetnji u Laboratorij tvrtke ESET za otkrivanje virusa, gdje se one analiziraju, obrađuju i dodaju u modul detekcije.

3. Sljedeći je korak postupka instalacije konfiguiriranje otkrivanja potencijalno nepoželjnih aplikacija. Pojedinosti potražite u poglavlju [Potencijalno nepoželjne aplikacije](#).

4. Završni korak je potvrda instalacije klikom na **Instaliraj**. Program ESET Endpoint Antivirus možete instalirati u određenu mapu tako da kliknete **Promijeni mapu za instalaciju**. Nakon završetka instalacije od vas će se zatražiti da [aktivirate program ESET Endpoint Antivirus](#).



## Promjena instalacijske mape (.exe)

Nakon što odaberete preferencu otkrivanja potencijalno nepoželjnih aplikacija i kliknete "**Promjena instalacijske mape**", od vas će se zatražiti da odaberete lokaciju za instalacijsku ESET Endpoint Antivirus mapu. Prema standardnim postavkama program se instalira u sljedeću mapu:

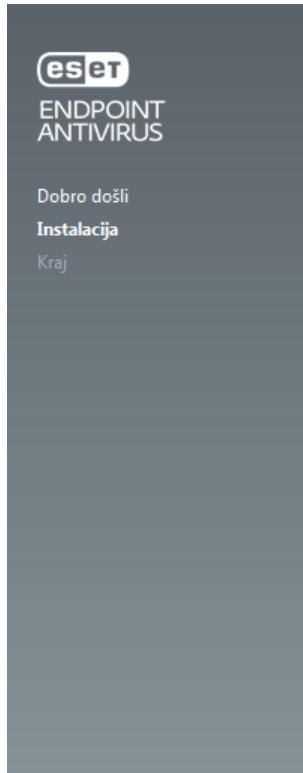
*C:\Program Files\ESET\ESET Security\*

Možete odrediti lokaciju za programske module i podatke. Prema standardnim se postavkama program instalira u sljedeće mape:

*C:\Program Files\ESET\ESET Security\Modules\*

*C:\ProgramData\ESET\ESET Security\*

Kliknite "**Pregledaj**" da biste promijenili lokaciju (ne preporučuje se).



Kliknite "Dalje" i zatim "Instaliraj" da biste započeli instalaciju.

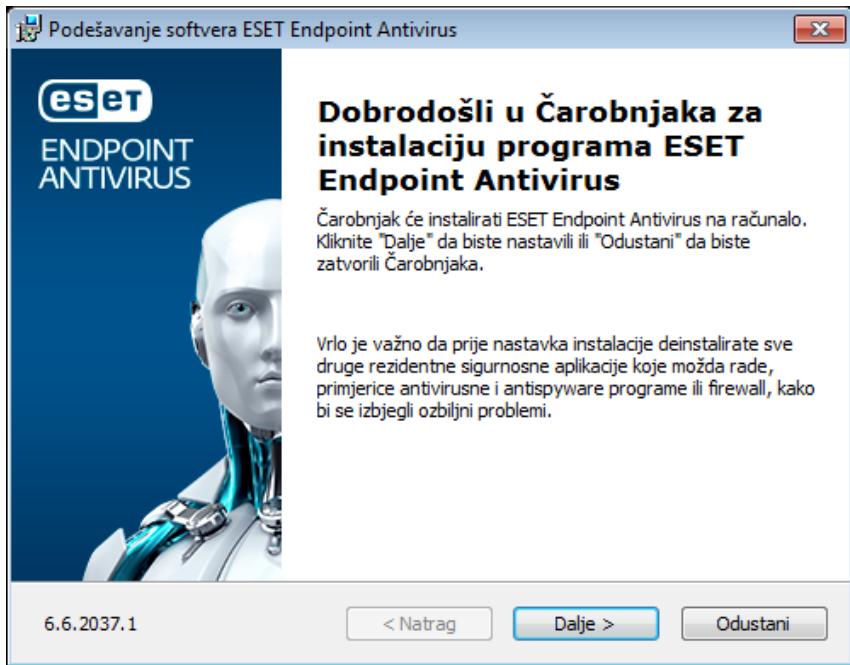
## Instalacija (.msi)

Kada pokrenete instalacijski program .msi, čarobnjak za instalaciju provest će vas kroz instalacijski postupak.

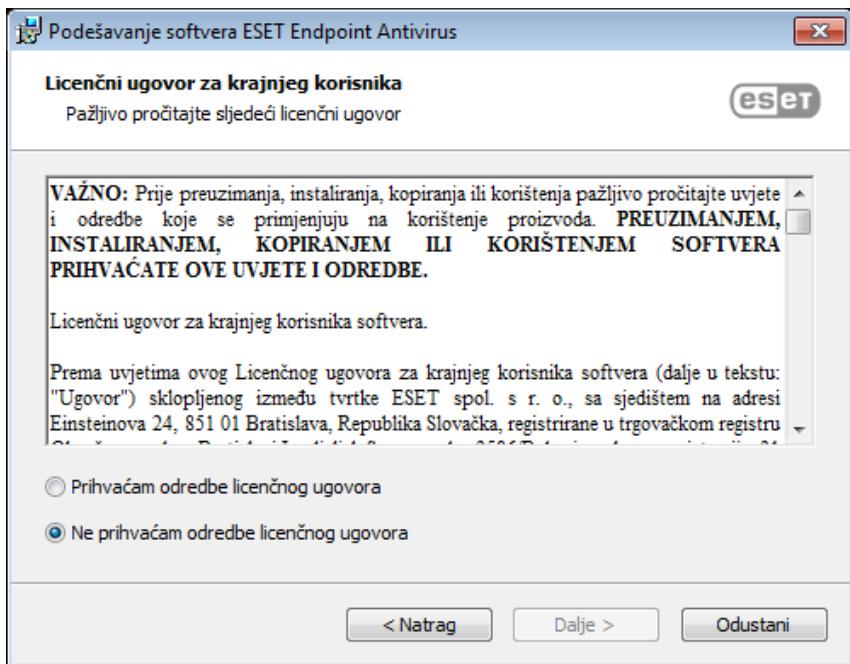
U poslovnim okruženjima, instalacijski program .msi preferirani je instalacijski paket. To je prvenstveno ✓ zbog izvanmrežnih i daljinskih instalacija koje se koriste raznim alatima, kao što je ESET Security Management Center.

Provjerite nije li na računalu instaliran još neki antivirusni program. Ako su na jednom računalu instalirana dva ili više antivirusnih programa, mogli bi se međusobno sukobljavati. Ako su na računalu instalirani još neki antivirusni programi, preporučujemo da ih deinstalirate. Pogledajte naš [članak baze znanja](#) (dostupan na engleskom i nekoliko drugih jezika).

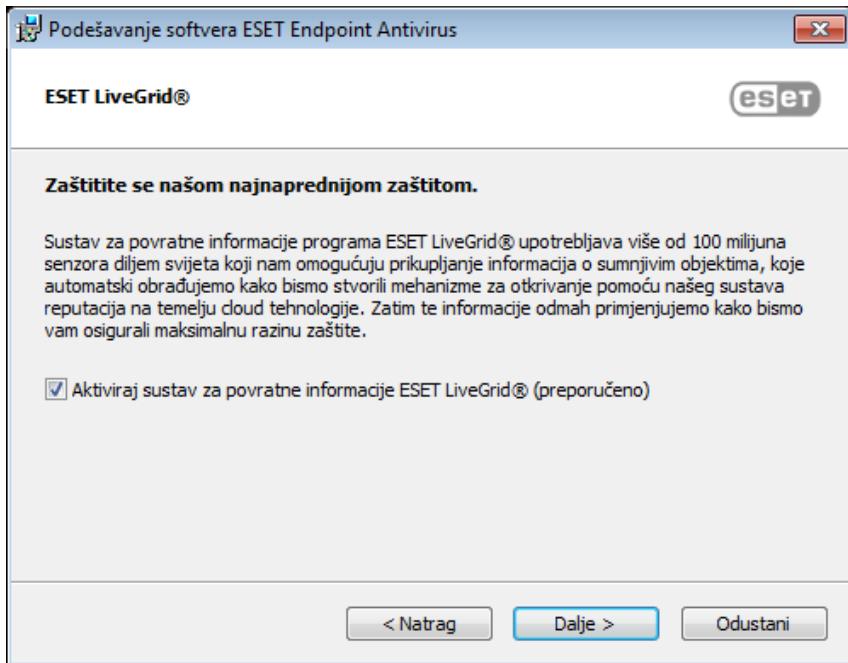
1. Odaberite željeni jezik i kliknite **Sljedeće**.



2. Pročitajte Licenčni ugovor za krajnjeg korisnika i kliknite **Prihvaćam uvjete licenčnog ugovora** da biste prihvatili uvjete Licenčnog ugovora za krajnjeg korisnika. Kliknite **Dalje** nakon što prihvate uvjete kako biste nastavili instalaciju.

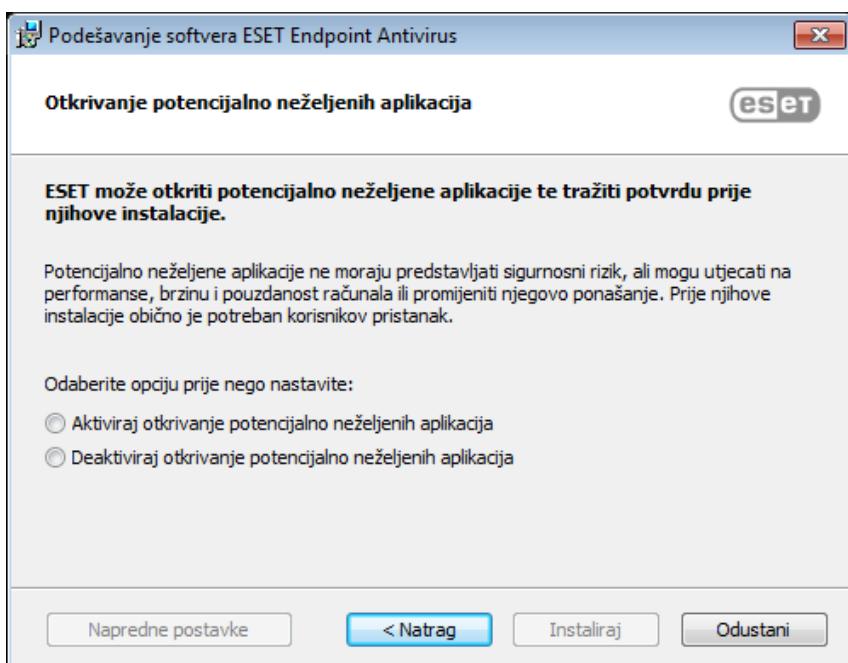


3. Odaberite svoje preferencije za sustav za povratne informacije [ESET LiveGrid®](#). ESET LiveGrid® osigurava da tvrtka ESET odmah i neprekidno bude obaviještena o novim infiltracijama radi pružanja bolje zaštite svojim korisnicima. Sustav dopušta slanje novih prijetnji u Laboratorij tvrtke ESET za otkrivanje virusa, gdje se one analiziraju, obrađuju i dodaju u modul detekcije.



4. Sljedeći je korak postupka instalacije konfiguriranje otkrivanja potencijalno nepoželjnih aplikacija. Pojedinosti potražite u poglavlju [Potencijalno nepoželjne aplikacije](#).

Kliknite **Napredne postavke** ako želite nastaviti s [Naprednom instalacijom \(.msi\)](#).



5. Završni je korak potvrda instalacije klikom na **Instaliraj**. Nakon završetka instalacije, od vas će se zatražiti da aktivirate program [ESET Endpoint Antivirus](#).

## Napredna instalacija (.msi)

Napredna instalacija omogućuje vam prilagodbu raznih parametara instalacije koji nisu dostupni prilikom izvršavanja uobičajene instalacije.

5. Nakon odabira preferencije otkrivanja [Potencijalno nepoželjnih aplikacija](#) te klikom stavke **Napredne**

**postavke**, od vas će se zatražiti da odaberete lokaciju za instalaciju programa ESET Endpoint Antivirus. Prema standardnim postavkama program se instalira u sljedeću mapu:

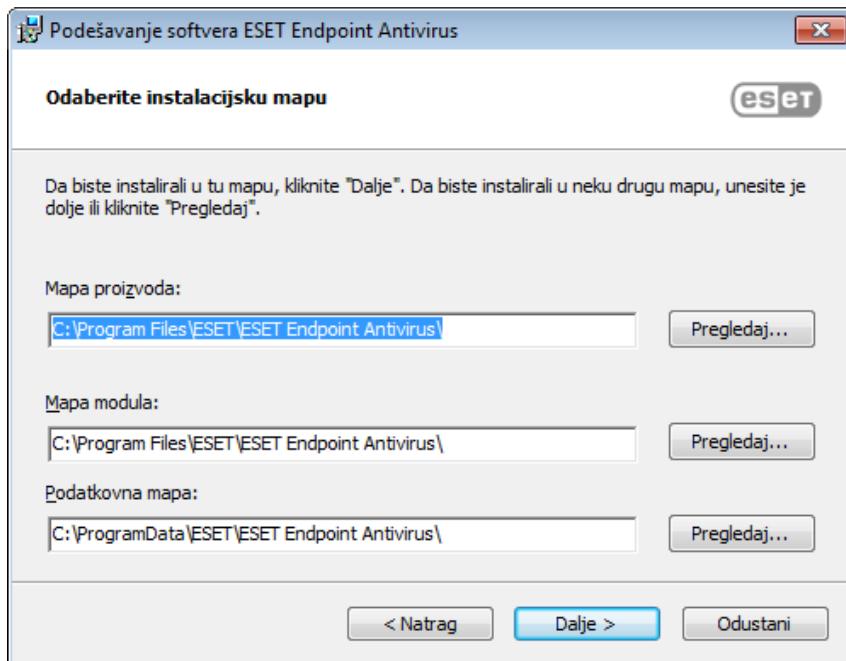
*C:\Program Files\ESET\ESET Security\*

Možete odrediti lokaciju za programske module i podatke. Prema standardnim se postavkama program instalira u sljedeće mape:

*C:\Program Files\ESET\ESET Security\Modules\*

*C:\ProgramData\ESET\ESET Security\*

Kliknite "Pregledaj" da biste promijenili lokaciju (ne preporučuje se).



7. Završni je korak potvrda instalacije klikom na **Instaliraj**.

## Instalacija putem naredbenog retka

Program ESET Endpoint Antivirus možete instalirati lokalno putem naredbenog retka ili možete upotrijebiti ESET PROTECT ili ESET Security Management Center da biste ga instalirali daljinski.

### Podržani parametri

#### APPDIR=<path>

- Put – valjani put do direktorija
- Direktorij za instalaciju aplikacije.

#### APPDATADIR=<path>

- Put – valjani put do direktorija
- Direktorij za instalaciju podataka aplikacije.

## **MODULEDIR=<path>**

- Put – valjani put do direktorija
- Direktorij za instalaciju modula.

## **ADDLOCAL=<list>**

- Instalacija komponente – popis neobaveznih značajki za lokalnu instalaciju.
- Upotreba s ESET-ovim .msi paketima: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Za više informacija o svojstvu **ADDLOCAL** pogledajte  
<http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx>

## **ADDEXCLUDE=<list>**

- Na popisu ADDEXCLUDE zarezom su odvojeni svi nazivi funkcija koje se neće instalirati i služi kao zamjena za zastarjeli popis REMOVE.
- Prilikom odabira funkcije koja se neće instalirati, na popis morate eksplicitno uključiti cijeli put (tj. put sa svim podfunkcijama) i povezanim nevidljivim funkcijama.
- Upotreba s ESET-ovim .msi paketima: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

 **ADDEXCLUDE** ne može se upotrebljavati uz **ADDLOCAL**.

U [dokumentaciji](#) za upotrijebljenu verziju **msiexec** potražite odgovarajuće parametre naredbenog retka.

## **Pravila**

- Popis **ADDLOCAL** jest popis svih naziva značajki koje će se instalirati, a koje su odvojene zarezima.
- Kod odabira značajke za instalaciju cijeli put (sve nadređene značajke) mora biti eksplicitno uključen na popis.
- Pogledajte dodatna pravila za ispravnu upotrebu.

## **Komponente i funkcije**

 Instalacija komponenti pomoću parametara ADDLOCAL/ADDEXCLUDE neće funkcionirati uz ESET Endpoint Antivirus.

Funkcije se dijele u 4 kategorije:

- **Obavezno** – funkcija će se uvijek instalirati.
- **Nije obavezno** – odabir funkcije može se poništiti kako se ona ne bi instalirala.
- **Nevidljivo** – logična značajka obavezna za funkcioniranje ostalih značajki

- **Rezervirano mjesto** – značajka bez utjecaja na proizvod, ali mora se navesti s podznačjkama

U nastavku je naveden skup funkcija programa ESET Endpoint Antivirus:

Opis	Naziv značajke	Nadređena stavka funkcije	Prisutnost
Osnovne programske komponente	Computer		Rezervirano mjesto
Modul detekcije	Antivirus	Computer	Obavezno
Modul detekcije / skeniranje zlonamjernih programa	Scan	Computer	Obavezno
Modul detekcije / rezidentna zaštita sistemskih datoteka	RealtimeProtection	Computer	Obavezno
Modul detekcije / skeniranje zlonamjernih programa / zaštita dokumenata	DocumentProtection	Antivirus	Nije obavezno
Kontrola uređaja	DeviceControl	Computer	Nije obavezno
Mrežna zaštita	Network		Rezervirano mjesto
Mrežna zaštita / firewall	Firewall	Network	Nije obavezno
Mrežna zaštita / zaštita od mrežnog napada / ...	IdsAndBotnetProtection	Network	Nije obavezno
Zaštićeni preglednik	OnlinePaymentProtection	WebAndEmail	Nije obavezno
Web i e-pošta	WebAndEmail		Rezervirano mjesto
Web i e-pošta / filtriranje protokola	ProtocolFiltering	WebAndEmail	Nevidljivo
Web i e-pošta / Zaštita web pristupa	WebAccessProtection	WebAndEmail	Nije obavezno
Web i e-pošta / Zaštita klijenta e-pošte	EmailClientProtection	WebAndEmail	Nije obavezno
Web i e-pošta / zaštita klijenta e-pošte / klijenti e-pošte	MailPlugins	EmailClientProtection	Nevidljivo
Web i e-pošta / Zaštita klijenta e-pošte / Antispam zaštita	Antispam	EmailClientProtection	Nije obavezno
Web i e-pošta / Kontrola weba	WebControl	WebAndEmail	Nije obavezno
Alati / ESET RMM	Rmm		Nije obavezno
Nadogradnja / profili / mirror za nadogradnju	UpdateMirror		Nije obavezno
<a href="#">Dodatak za ESET Enterprise Inspector</a>	EnterpriseInspector		Nevidljivo

Skup grupnih funkcija:

Opis	Naziv značajke	Prisutnost značajke
Sve obavezne funkcije	_Base	Nevidljivo
Sve dostupne funkcije	ALL	Nevidljivo

## Dodatna pravila

- Ako je bilo koja funkcija iz skupine **WebAndEmail** odabrana za instalaciju, na popis je potrebno uključiti i nevidljivu funkciju **ProtocolFiltering**.
- U nazivima svih funkcija razlikuju se mala i velika slova. Primjerice, UpdateMirror nije isto što i UPDATEMIRROR.

## Popis konfiguracijskih svojstava

Svojstvo	Vrijednost	Funkcija
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – deaktivirano 1 – aktivirano	<a href="#">Otkrivena potencijalno nepoželjna aplikacija</a>
CFG_LIVEGRID_ENABLED=	<a href="#">Pogledajte u nastavku</a>	Pogledajte <a href="#">LiveGrid svojstvo</a> u nastavku
FIRSTSCAN_ENABLE=	0 – deaktivirano 1 – aktivirano	Zakažite i pokrenite <a href="#">skeniranje računala</a> nakon instalacije
CFG_PROXY_ENABLED=	0 – deaktivirano 1 – aktivirano	Postavke proxy servera postavke servera
CFG_PROXY_ADDRESS=	<ip>	IP adresa proxy servera
CFG_PROXY_PORT=	<port>	Broj porta proxy servera
CFG_PROXY_USERNAME=	<username>	Korisničko ime za autorizaciju.
CFG_PROXY_PASSWORD=	<password>	Lozinka za Provjera autentičnosti
ACTIVATION_DATA=	<a href="#">Pogledajte u nastavku</a>	Aktivacija programa, licenčni ključ ili datoteka izvanmrežne licence
ACTIVATION_DLG_SUPPRESS=	0 – deaktivirano 1 – aktivirano	Kada je vrijednost postavljena na „1“, ne prikazuj <a href="#">prozor za aktivaciju programa</a> nakon prvog pokretanja
ADMINCFG=	<path>	Put do <a href="#">izvezene XML konfiguracije</a> (standardna vrijednost <i>cfg.xml</i> )

### [LiveGrid®](#) svojstvo

Prilikom instalacije programa ESET Endpoint Antivirus uz opciju **CFG\_LIVEGRID\_ENABLED**, program će se ponašati na sljedeći način nakon instalacije:

Funkcija	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
<b>Reputacijski sustav ESET LiveGrid®</b>	Uključeno	Uključeno
<b>Sustav za povratne informacije programa ESET LiveGrid®</b>	Isključeno	Uključeno
<b>Pošalji anonimnu statistiku</b>	Isključeno	Uključeno

### Svojstvo ACTIVATION\_DATA

Format	Metoda
ACTIVATION_DATA=key : AAAA-BBBB-CCCC-DDDD-EEEE	<a href="#">Aktivacija pomoću ESET-ova licenčnog ključa</a> (potrebna je aktivna veza s internetom)

Format	Metoda
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.1f	<a href="#">Aktivacija pomoću datoteke izvanmrežne licence</a>

## Svojstva jezika

Jezik programa ESET Endpoint Antivirus (morate navesti oba svojstva).

Svojstvo	Vrijednost
PRODUCT_LANG=	LCID šifra (ID regionalnih postavki), primjerice 1033 za engleski (Sjedinjene Američke Države); pogledajte <a href="#">popis kodova jezika</a> .
PRODUCT_LANG_CODE=	LCID oznaka (naziv jezične kulture) malim slovima, primjerice en-us za engleski – Sjedinjene Američke Države; pogledajte <a href="#">popis kodova jezika</a> .

## Primjeri instalacije putem naredbenog retka

- ! Obavezno pročitajte [Licenčni ugovor za krajnjeg korisnika](#) i provjerite imate li administratorske ovlasti prije pokretanja instalacije.
- ✓ Izuzmite odjeljak **NetworkProtection** iz instalacije (morate isto tako navesti sve podređene funkcije):  
`msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection`
- ✓ Ako želite da se program ESET Endpoint Antivirus automatski konfigurira nakon instalacije, možete navesti osnovne konfiguracijske parametre u instalacijskoj naredbi.  
✓ Instalirajte program ESET Endpoint Antivirus uz aktiviranESET LiveGrid®:  
`msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1`
- ✓ Instalirajte u drugu mapu za instalaciju aplikacije umjesto [standardne mape](#).  
`msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\`
- ✓ Instalirajte i aktivirajte program ESET Endpoint Antivirus pomoću ESET-ova licenčnog ključa.  
`msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`
- ✓ Neprimjetna instalacija s detaljnim vođenjem dnevnika (korisno za otklanjanje poteškoća) i RMM samo s obaveznim komponentama:  
`msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm`
- ✓ Nametnuta neprimjetna instalacija na [definiranom jeziku](#).  
`msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us`

## Opcije naredbenog retka nakon instalacije

- [ESET CMD](#) – uvezite .xml konfiguracijsku datoteku ili uključite/isključite sigurnosnu funkciju
- [Skener naredbenog retka](#) – pokrenite skeniranje računala iz naredbenog retka

## Instalacija pomoću GPO-a ili SCCM-a

Osim [izravne instalacije programa ESET Endpoint Antivirus na klijentsku radnu stanicu](#) ili [daljinske instalacije pomoću zadatka servera u programu ESMC](#), možete ga instalirati i upotrebom alata za upravljanje kao što je

objekt pravila grupe (GPO) ili programa Software Center Configuration Manager (SCCM), Symantec Altiris ili Puppet.

## Upravljano (preporučeno)

Za upravljanu računalu najprije je potrebno instalirati ESET Management Agent, a zatim instalirati program ESET Endpoint Antivirus putem programa ESET Security Management Center (ESMC). ESMC mora biti instaliran na vašoj mreži.

1. Preuzmite [zasebni instalacijski program](#) za ESET Management Agent.
2. [Pripremite GPO/SCCM skriptu za daljinsku instalaciju.](#)
3. Instalirajte ESET Management Agent pomoću alata GPO ili SCCM.
4. Provjerite jesu li [klijentska računala](#) dodana u ESMC.
5. [Instalirajte i aktivirajte program ESET Endpoint Antivirus na klijentskim računalima.](#)

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

-  • [Instalirajte ESET Management Agent putem alata SCCM ili GPO](#)  
• [Instalirajte ESET Management Agent putem objekta pravila grupe \(GPO\)](#)

[??](#)

## Nadogradnja na noviju verziju

Nove verzije programa ESET Endpoint Antivirus izdaju se radi implementacije poboljšanja ili popravka problema koji se ne mogu ukloniti automatskom nadogradnjom modula programa.

Nadogradnja na noviju verziju može se postići na nekoliko načina:

1. Automatski, pomoću programa ESET PROTECT, ESET Security Management Center (ESMC) ili ESET PROTECT Cloud. Verzijom 8 programa ESET Endpoint Antivirus ne možete upravljati pomoću programa ESET Remote Administrator.
2. Automatski, [pomoću GPO-a ili SCCM-a.](#)
3. Automatski putem aktualizacije programa.  
Budući da se nadogradnja programa šalje svim korisnicima i može utjecati na pojedine konfiguracije sustava, izdaje se tek nakon dugoročnog testiranja sa svim mogućim konfiguracijama sustava kako bi se osigurala funkcionalnost. Ako trebate nadograditi na noviju verziju odmah nakon njenog izdavanja, upotrijebite jedan od načina u nastavku.  
Provjerite jeste li aktivirali **Način rada nadogradnje** u opciji **Napredno podešavanje (F5) > Nadogradnja > Profili > Nadogradnja programske komponente.**
4. Ručno preuzimanjem i [instaliranjem nove verzije](#) preko prethodne.

## Preporučeni scenariji nadogradnje

### Upravljam ili želim upravljati svojim ESET programima na daljinu

Ako upravljate s više od 10 ESET-ovih sigurnosnih programa, razmislite o upravljanju nadogradnjama pomoću programa ESET PROTECT, ESET PROTECT Cloud ili ESMC.

Pregledajte sljedeću dokumentaciju:

- [ESET PROTECT | Nadogradnja ESET-ovog softvera putem zadatka klijenta](#)
- [ESET PROTECT | Vodič za mala do srednja poduzeća koja upravljaju s najviše 250 ESET-ovih sigurnosnih programa za Windows](#)
- [Uvod u ESET PROTECT Cloud](#)

### Ručna nadogradnja na klijentskoj radnoj stanici

Nemojte instalirati verziju 8 preko verzije 4.x ni preko starije/nefunkcionalne verzije programa ESET Endpoint Antivirus 5.x ili 6.x.

Ako planirate upravljati nadogradnjama ručno na pojedinačnim klijentskim radnim stanicama:

1. Provjerite je li vaš operacijski sustav [podržan](#) Windows Vista i Windows XP nije podržan u verziji.
2. Preuzmite i [instalirajte noviju verziju](#) preko prethodne.

Ako želite maksimalno povećati šanse za uspješnu nadogradnju na [najnoviju verziju 8.x](#), izvršite nadogradnju s jedne od sljedećih verzija programa ESET Endpoint Antivirus:

- 5.0.2272.x
- 6.5.2132.x
- 7.3.2044.x

U suprotnom najprije deinstalirajte program ESET Endpoint Antivirus. Za dodatne informacije o nadogradnji programa ESET Endpoint Antivirus na klijentskoj radnoj stanici pročitajte sljedeći [članak ESET-ove baze znanja](#).

## Automatska nadogradnja programa koji radi prema starom standardu

Vaša verzija ESET-ovog programa više nije podržana, stoga je program nadograđen na najnoviju verziju.

#### [Uobičajene teškoće prilikom instalacije](#)

 Svaka nova verzija ESET-ovih programa sadrži mnoge ispravke pogrešaka i poboljšanja. Postojeći korisnici s valjanom licencom za ESET-ov program mogu besplatno nadograditi na najnoviju verziju istog programa.

Da biste dovršili instalaciju:

1. Kliknite **Prihvati i nastavi** kako biste prihvatali [Licenčni ugovor za krajnjeg korisnika](#) i [Pravila privatnosti](#). Ako se ne slažete s Licenčnim ugovorom za krajnjeg korisnika, kliknite **Deinstaliraj**. Nije moguće vratiti se na prethodnu verziju.
2. Kliknite **Dopusti sve i nastavi** da biste dopustili [Sustav za povratne informacije programa ESET LiveGrid®](#) ili kliknite **Nastavi** ako ne želite sudjelovati.

3. Nakon aktivacije novog ESET-ovog programa pomoću licenčnog ključa prikazat će se početna stranica. Ako nije moguće pronaći vaše podatke o licenci, nastavite s novom probnom licencom. Ako licenca koju ste upotrebljavali za prethodni program nije valjana, [aktivirajte ESET-ov program](#).

4. Za dovršetak instalacije potrebno je ponovno pokrenuti uređaj.

## Nadogradnje za potrebe sigurnosti i stabilnosti

Nadogradnja programa ESET Endpoint Antivirus važan je dio osiguranja potpune zaštite od zločudnih kodova. Svaka nova verzija programa ESET Endpoint Antivirus sadržava brojna poboljšanja i ispravke pogrešaka. Preporučujemo povremenu nadogradnju programa ESET Endpoint Antivirus kako bi se spriječila sigurnosna ranjivost i prijetnje. ESET Endpoint Antivirus nalazi se u određenoj fazi životnog ciklusa programa, kao i svi ostali ESET-ovi programi. Pročitajte više o [pravilima kraja života \(poslovni programi\)](#).

Dodatne informacije o promjenama programa ESET Endpoint Antivirus pročitajte u sljedećem članku u [ESET-ovoj bazi znanja](#).

 Automatske nadogradnje osiguravaju maksimalnu sigurnost i stabilnost programa. Nadogradnje koje služe sigurnosti i stabilnosti ne mogu se deaktivirati.

## Uobičajene teškoće prilikom instalacije

Ako se tijekom instalacije pojave poteškoće, pogledajte naš popis [uobičajenih pogrešaka prilikom instalacije i rješenja](#) da biste pronašli rješenje problema.

## Aktivacija nije uspjela

Najčešći mogući scenariji u slučaju neuspješne aktivacije programa ESET Endpoint Antivirus navedeni su u nastavku:

- Licenčni ključ već se upotrebljava
- Licenčni ključ nije valjan. Pogreška obrasca za aktivaciju proizvoda
- Dodatne informacije nužne za aktivaciju nedostaju ili su nevaljane
- Komunikacija s bazom podataka za aktivaciju nije uspjela. Pričekajte 15 minuta i ponovno pokušajte s aktivacijom
- Nema veze s ESET-ovim serverima za aktivaciju ili je veza deaktivirana

Provjerite jeste li unijeli ispravan licenčni ključ ili priložili izvanmrežnu licencu i pokušajte ponovo aktivirati.

Ako aktivacija ne uspije, naš paket za dobrodošlicu provest će vas kroz česta pitanja, pogreške i probleme povezane s aktivacijom i licencama (dostupan na engleskom i više drugih jezika).

- [Pokretanje postupka otklanjanja poteškoća za aktivaciju ESET-ova programa](#)

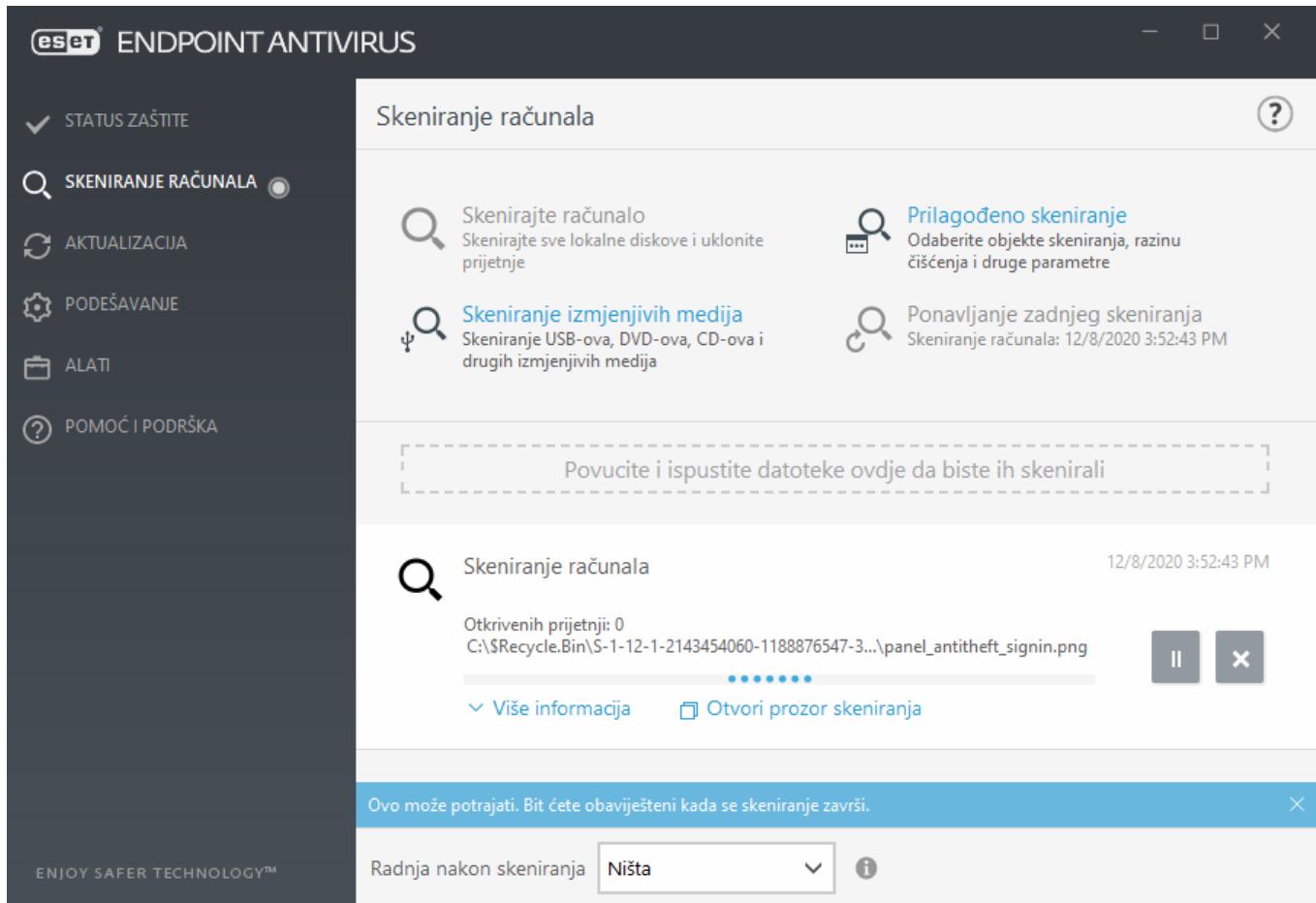
# Aktivacija proizvoda

Po završetku instalacije od vas će se zatražiti da aktivirate proizvod.

Odaberite jedan od dostupnih načina za aktivaciju ESET Endpoint Antivirus. Dodatne informacije potražite u odjeljku [Kako aktivirati ESET Endpoint Antivirus](#).

## Skeniranje računala

Preporučujemo da izvršite redovita skeniranja računala ili isplanirate [redovito skeniranje](#) za provjeru prijetnji. U glavnom prozoru programa kliknite **Skeniranje računala** i nakon toga **Smart skeniranje**. Više informacija o skeniranjima računala potražite u odjeljku [Skeniranje računala](#).



## Vodič za početnike

U ovom poglavlju pronaći ćete uvod u program ESET Endpoint Antivirus i njegove osnovne postavke.

## Korisničko sučelje

Glavni programski prozor programa ESET Endpoint Antivirus podijeljen je u dva glavna odjeljka. Primarni prozor s desne strane prikazuje informacije koje odgovaraju mogućnosti odabranoj na glavnom izborniku s lijeve strane.

Slijedi opis mogućnosti na glavnom izborniku:

**Status zaštite** – Pruga informacije o statusu zaštite programa ESET Endpoint Antivirus.

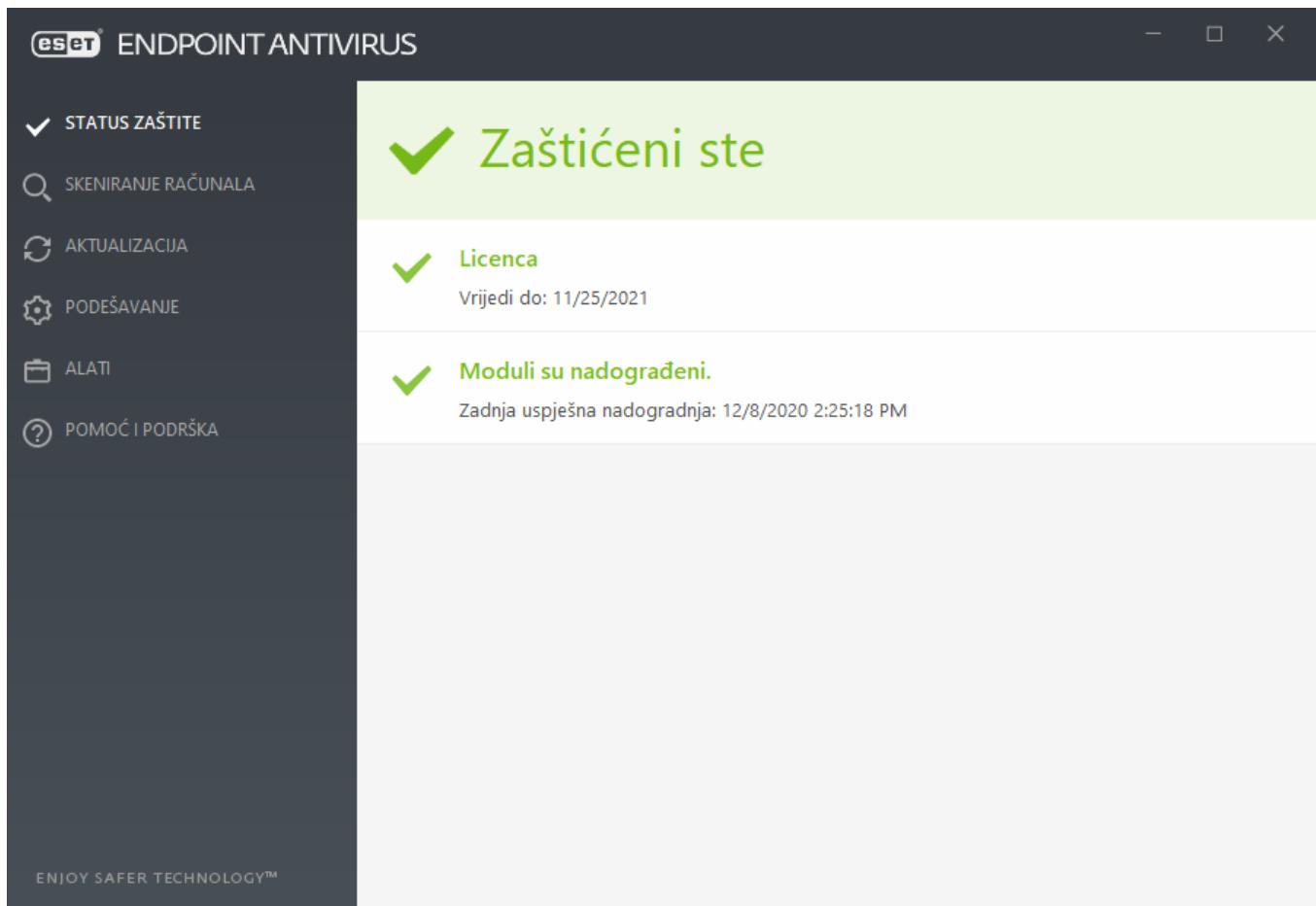
**Skeniranje računala** – Ta opcija omogućuje konfiguriranje i pokretanje smart skeniranja, prilagođenog skeniranja ili skeniranja izmjenjivih medija. Možete još i ponoviti posljednje izvršeno skeniranje.

**Nadogradnja** – Prikazuje informacije o modulu detekcije i omogućava ručnu provjeru nadogradnji.

**Podešavanje** – Označite ovu opciju za podešavanje računala ili weba i e-pošte.

**Alati** – Omogućuje pristup dnevnicima, statistici zaštite, nadzoru aktivnosti, pokrenutim procesima, planeru, karanteni, ESET SysInspector i ESET SysRescue za stvaranje CD-a za oporavak. Možete i poslati uzorak za analizu.

**Pomoć i podrška** – Omogućuje pristup datotekama za pomoć, [ESET-ovoj bazi znanja](#) i web stranici tvrtke ESET. Dostupni su i linkovi za otvaranje zahtjeva za tehničku podršku, alati za podršku te informacije o aktivaciji programa.

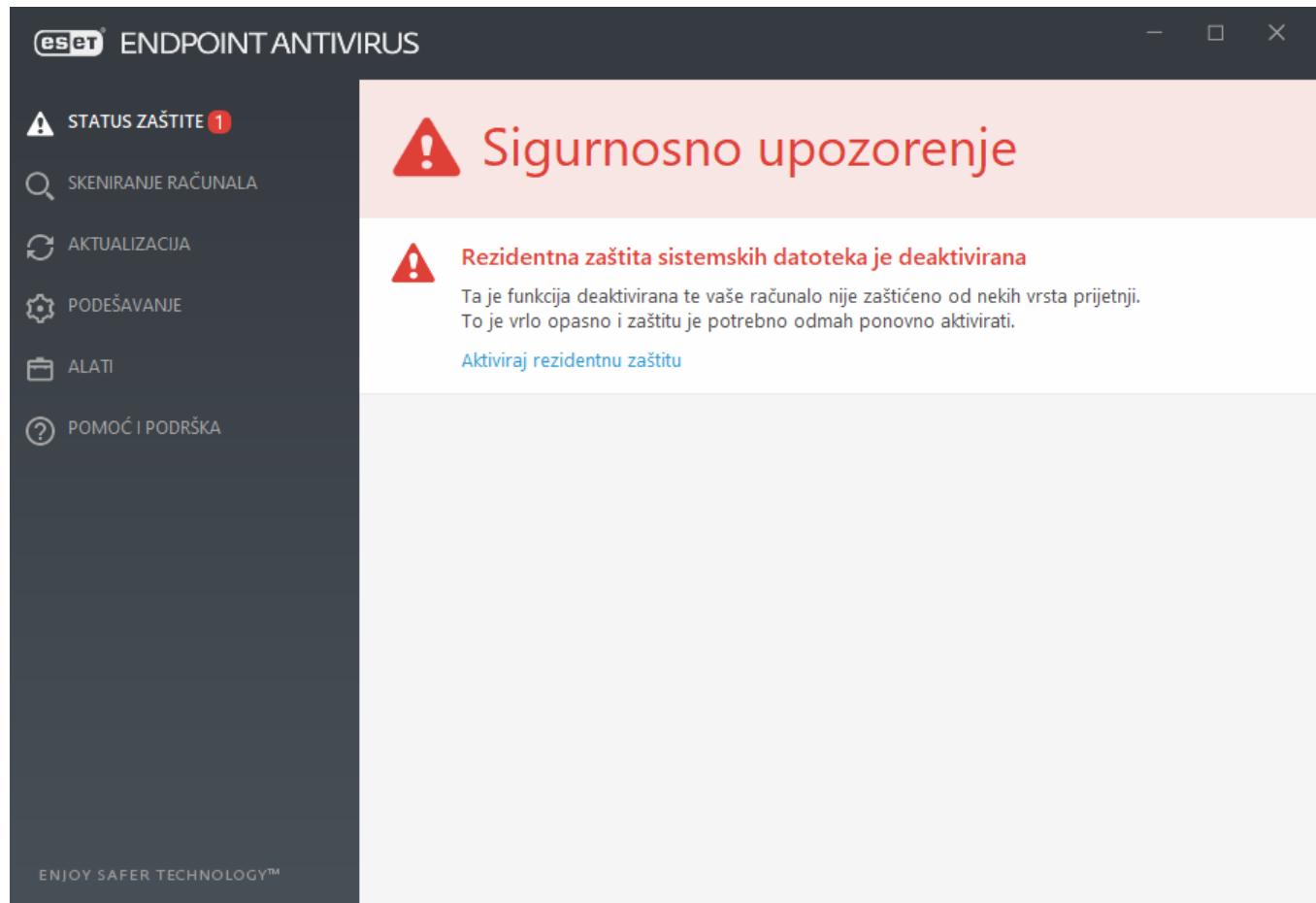


U zaslonu **Status zaštite** nalaze se informacije o sigurnosti i trenutnoj razini zaštite vašeg računala. Zeleni status **Maksimalna zaštita** znači da je osigurana maksimalna zaštita.

Prozor sa statusom prikazuje i najčešće korištene značajke u programu ESET Endpoint Antivirus te informacije o zadnjoj aktualizaciji.

## Što učiniti ako program ne radi ispravno?

Pokraj svih modula programa koji su u potpunosti funkcionalni prikazat će se zelena potvrDNA kvačica. Ako je potrebno obratiti pozornost na modul, prikazuje se crveni uskličnik ili narančasta ikona s obavijesti. Dodatne informacije o modulu, uključujući i naše preporuke o tome kako vratiti sve funkcije, prikazane su u gornjem dijelu prozora. Da biste promijenili status modula, na glavnom izborniku kliknite **Podešavanje** i kliknite željeni modul.



Ikona crvenog uskličnika (!) pokazuje da nije osigurana maksimalna zaštita vašeg računala. Do te vrste obavijesti može doći u sljedećim situacijama:

- **Antivirusna i antispyware zaštita je pauzirana** – kliknite **Pokreni sve module antivirusne i antispyware zaštite** da biste ponovno aktivirali antivirusnu i antispyware zaštitu u oknu **Status zaštite** ili **Aktiviraj antivirusnu i antispyware zaštitu** u oknu **Podešavanje** u glavnom programskom prozoru.
- Antivirusna je zaštita deaktivirana – pokretanje virusnog skenera nije uspjelo. Većina modula programa ESET Endpoint Antivirus neće ispravno raditi.
- **Antiphishing zaštita ne funkcionira** – funkcija ne funkcionira jer ostali potrebni moduli programa nisu aktivni.
- **Zastario je modul detekcije** – ta će se pogreška pojaviti nakon nekoliko neuspješnih pokušaja nadogradnje modula detekcije (prethodno baze podataka virusnih potpisa). Preporučujemo da provjerite postavke nadogradnje. Najčešći je uzrok ove pogreške neispravan unos [podataka za autentikaciju](#) ili neispravna konfiguracija [postavki povezivanja](#).
- **Program nije aktiviran ili je licenca istekla** – to označava crvena ikona statusa zaštite. Program se ne može

nadograditi nakon što licenca istekne. Preporučujemo da pratite upute u prozoru upozorenja i obnovite svoju licencu.

- **Deaktiviran je sustav za sprečavanje upada (HIPS)** – Ovaj se problem javlja kada se HIPS deaktivira u Naprednom podešavanju. Računalo nije zaštićeno od nekih vrsta prijetnji i potrebno je ponovno aktivirati zaštitu klikom opcije **Aktiviraj HIPS**.
- **ESET LiveGrid® je deaktiviran** – Ovaj se problem javlja kada se ESET LiveGrid® deaktivira u Naprednom podešavanju.
- **Nisu zakazane redovne aktualizacije** – ESET Endpoint Antivirus neće provjeravati ili primati važne aktualizacije osim ako ne zakažete aktualizacijski zadatak.
- **Anti-Stealth je deaktiviran** – Kliknite **Aktiviraj Anti-Stealth** da biste ponovno aktivirali ovu funkciju.
- **Blokiran pristup mreži** – prikazuje se kad se pokrene zadatak klijenta **Izolacija računala s mreže** na ovoj radnoj stanici iz programa ESMC. Obratite se svom administratoru sustava za više informacija.
- **Pauzirana je rezidentna zaštita** – korisnik je deaktivirao rezidentnu zaštitu. Vaše računalo nije zaštićeno od prijetnji. Kliknite Aktiviraj rezidentnu zaštitu da biste ponovno aktivirali tu funkciju.



Narančasti znak „i“ označava da morate pripaziti na nekritičan problem u programu tvrtke ESET. Mogući su razlozi:

- **Zaštita web pristupa deaktivirana je** – kliknite sigurnosnu obavijest da biste ponovno aktivirali zaštitu web pristupa i zatim kliknite **Aktiviraj zaštitu web pristupa**.
- **Vaša će licenca uskoro isteći** – To označava ikona statusa zaštite s uskličnikom. Nakon isteka licence program se neće moći nadograditi i ikona statusa zaštite postat će crvena.
- **Antispam zaštita je pauzirana** – Kliknite **Aktiviraj antispam zaštitu** da biste ponovno aktivirali ovu funkciju.
- **Web kontrola je pauzirana** – Kliknite **Aktiviraj kontrolu weba da biste ponovno aktivirali ovu funkciju**.
- **Aktivno je nadjačavanje pravila** – Konfiguracija koja je postavljena pravilom privremeno je nadjačana, možda dok se ne dovrši otklanjanje poteškoća. Postavke pravila može nadjačati samo ovlašteni korisnik. Više informacija potražite u odjeljku [Korištenje načina nadjačavanja](#).
- **Kontrola uređaja je pauzirana** – Kliknite **Aktiviraj kontrolu uređaja** da biste ponovno aktivirali ovu funkciju.

Za poboljšanje vidljivosti statusa u programima u prvom okviru programa ESET Endpoint Antivirus pogledajte odjeljak [Statusi aplikacije](#).

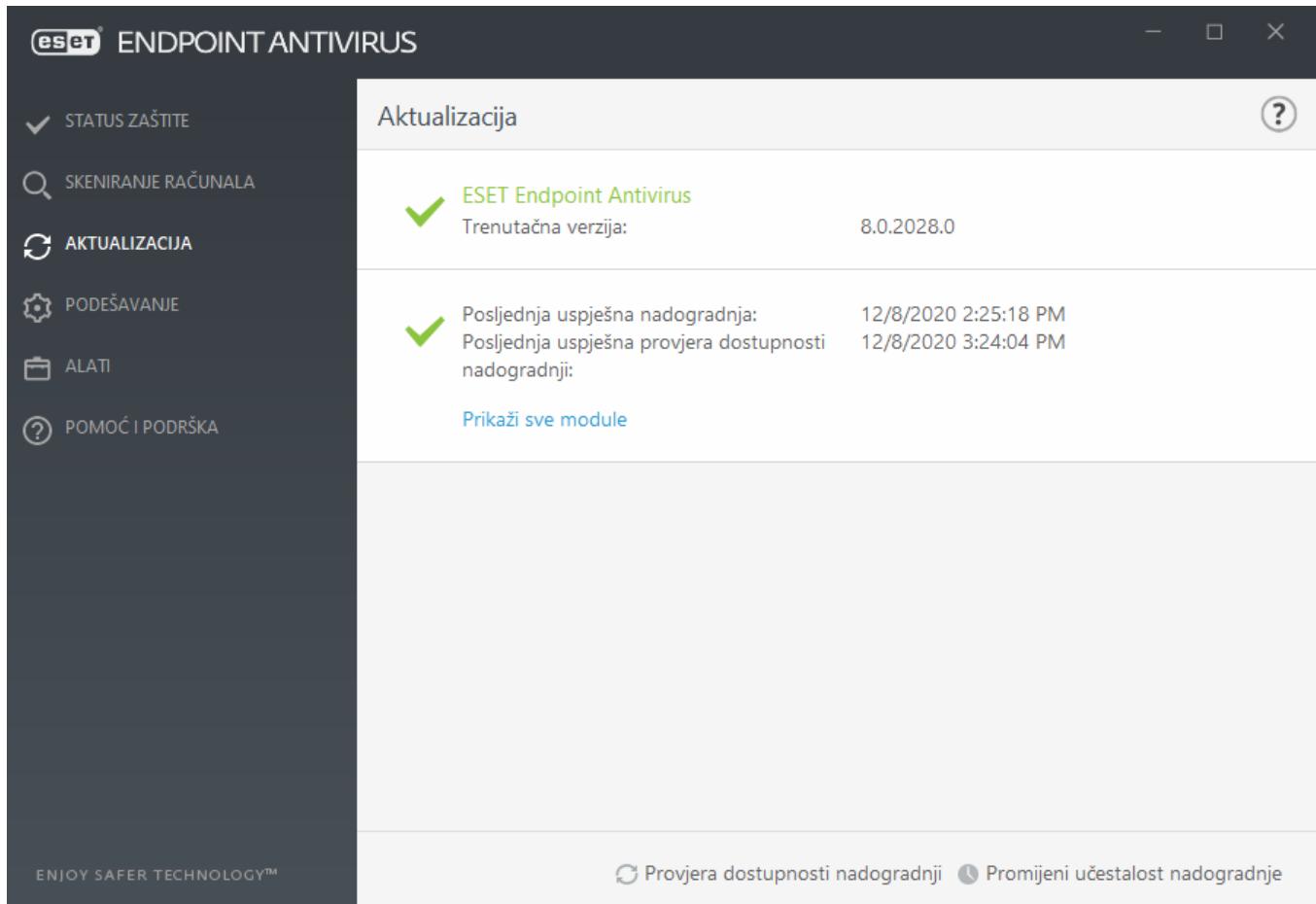
Ako problem ne možete riješiti s pomoću predloženih rješenja, kliknite stavku **Pomoć i podrška** da biste pristupili datotekama pomoći ili pretražili [ESET-ovu bazu znanja](#). Ako vam je i nakon toga potrebna pomoć, možete poslati zahtjev za podršku. ESET-ova tehnička podrška brzo će odgovoriti na vaša pitanja i pomoći vam da pronađete rješenje.

Ako se status odnosi na funkciju koja je blokirana ESMC ili ESET PROTECT pravilom, na link se neće moći kliknuti.

# Podešavanje aktualizacije

Nadogradnja modula važan je dio održavanja potpune zaštite od zlonamjernog koda. Obratite posebnu pozornost na njihovu konfiguraciju i rad. U glavnom izborniku odaberite **Nadogradnja > Potraži nadogradnje** da biste potražili noviju nadogradnju modula.

Ako niste unijeli **ključ licence**, nećete moći primati nove aktualizacije i od vas će se zatražiti da aktivirate proizvod.



Prozor naprednog podešavanja (kliknite stavku **Podešavanje > Napredno podešavanje u glavnom izborniku** ili pritisnite **F5** na tipkovnici) sadrži dodatne opcije nadogradnje. Da biste konfiguirirali opcije napredne nadogradnje kao što su način nadogradnje, pristup proxy servera, LAN veze i postavke izrade kopija modula detekcije, kliknite **Nadogradnja** u stablu Napredno podešavanje.

- Ako imate probleme s nadogradnjom, kliknite **Očisti** da biste izbrisali privremenu predmemoriju nadogradnje.

- Opcija **Odaberite automatski** u izborniku **Profilii > Nadogradnje > Nadogradnje modula** aktivirana je prema standardnim postavkama. Ako upotrebljavate ESET-ov server za nadogradnju, preporučujemo da ostavite odabranu standardnu opciju.
- Ako ne želite da se prikazuje obavijest o uspješnoj nadogradnji na traci sustava u donjem desnom kutu zaslona, proširite izbornik **Profilii > Nadogradnje**, kliknite **Uredi** pokraj **Odaberite obavijesti o primljenim nadogradnjama** i podesite potvrđne okvire za obavijest **Modul detekcije uspješno je nadograđen**.

Radi optimalne funkcionalnosti važno je automatski aktualizirati program. To je moguće samo ako je točan **ključ licence** unesen pod **Pomoć i podrška > Aktiviraj proizvod**.

Ako nakon instalacije niste unijeli **Ključ licence**, možete to učiniti u bilo kojem trenutku. Detaljne informacije o aktivaciji potražite u poglavljiju [Aktivacija programa ESET Endpoint Antivirus](#) i u prozor **Detalji o licenci** unesite podatke dobivene sa sigurnosnim proizvodom tvrtke ESET.

## Rad s programom ESET Endpoint Antivirus

Mogućnostima podešavanja programa ESET Endpoint Antivirus prilagođava se razina zaštite računala, weba i e-pošte.

Prilikom stvaranja pravila u ESET PROTECT web konzoli ili ESET Security Management Center web konzoli možete odabrati zastavicu za svaku postavku. Postavke sa zastavicom "Obavezno primjeni" imaju prioritet i ne može ih prebrisati novije pravilo (čak i kada novo pravilo ima zastavicu "Obavezno primjeni"). Tako se osigurava da se ta postavka ne promjeni (npr. da je ne promijeni korisnik ili novija pravila tijekom spajanja). Dodatne informacije potražite u [odjeljku Zastavice u Mrežnoj pomoći za ESET PROTECT](#).

STATUS ZAŠTITE

SKENIRANJE RAČUNALA

AKTUALIZACIJA

PODEŠAVANJE

ALATI

POMOĆ I PODRŠKA

ENJOY SAFER TECHNOLOGY™

Podešavanje

Računalo  
Sve su funkcije zaštite računala aktivne.

Mreža  
Sve su funkcije mrežne zaštite aktivne.

Web i e-pošta  
Sve su funkcije internetske zaštite aktivne.

Uvoz ili izvoz postavki Napredno podešavanje

Izbornik **Podešavanje** sadrži sljedeće odjeljke:

- **Računalo**
- **Mreža**
- **Web i e-pošta**

Odjeljak Računalo omogućuje aktiviranje ili deaktiviranje sljedećih komponenti:

- **Rezidentna zaštita sistemskih datoteka** – U svim se datotekama skeniranjem provjerava postojanje zlonamjernog koda u trenutku njihova otvaranja, stvaranja ili pokretanja.
- **Kontrola uređaja** – Omogućuje automatsku [kontrolu](#) uređaja (CD/DVD/USB/...). Ovaj modul omogućuje blokiranje ili prilagođavanje dodatnih filtera/dopuštenja i određuje način na koji korisnik pristupa određenom uređaju i radi s njim.
- **Sustav za sprečavanje upada (HIPS)** – Sustav [HIPS](#) nadzire događaje koji se događaju unutar operacijskog sustava i reagira na njih u skladu s prilagođenim skupom pravila.
- **Napredni skener memorije** – radi zajedno sa zaštitom od zloupotrebe na ojačavanju zaštite od zlonamjernog softvera koji je osmišljen tako da skrivanjem i/ili šifriranjem izbjegava da ga otkriju proizvodi za zaštitu od zlonamjernog softvera. Prema standardnim postavkama napredni je skener memorije aktiviran. Više o toj vrsti zaštite pročitajte u [rječniku](#).

- **Sprječavanje ranjivosti** – Osmišljeno je za ojačavanje zaštite često zloupotrebjavanih vrsta aplikacija kao što su web preglednici, PDF čitači, klijenti e-pošte i komponente sustava MS Office. Sprječavanje ranjivosti aktivirano je prema standardnim postavkama. Pročitajte više o ovoj vrsti zaštite u [rječniku](#).

- **Zaštita od ransomwarea** – dodatan sloj zaštite koji djeluje kao dio funkcije HIPS. Sustav reputacije ESET LiveGrid® mora biti aktiviran da bi zaštita od ransomwarea djelovala. [Više o toj vrsti zaštite pročitajte ovdje](#).

- **Način rada za prezentacije** – Funkcija za korisnike koji softver žele koristiti bez prekida, ne žele biti ometani skočnim prozorima te žele smanjiti korištenje CPU-a. Nakon aktivacije [Načina rada za prezentacije](#) primit ćete poruku upozorenja (mogući sigurnosni rizik) i glavni će prozor postati narančast.

Odjeljak **Mrežna zaštita** omogućuje konfiguraciju značajki Zaštita od mrežnog napada (IDS) i [Zaštita od botneta](#).

Podešavanje zaštite **weba i e-pošte** omogućuje vam aktiviranje ili deaktiviranje sljedećih komponenti:

- **Zaštita web pristupa** – Ako se aktivira ova postavka, sav promet putem HTTP-a ili HTTPS-a skenira se za zlonamjerni softver.
- **Zaštita klijenta e-pošte** – Omogućuje nadzor komunikacije e-poštom koja se prima putem protokola POP3 i IMAP.
- **Antiphishing zaštita** – Štiti vas od pokušaja pribavljanja lozinki, bankovnih i drugih osjetljivih podataka s neovlaštenih web stranica koje se prikazuju kao legitimne.

Da biste privremeno deaktivirali pojedinačne module, pritisnite zelenu oznaku pored željenog modula. Imajte na umu da to može umanjiti zaštitu vašeg računala.

Da biste ponovno aktivirali zaštitu ili deaktiviranu sigurnosnu komponentu, kliknite crvenu oznaku da bi se komponenta ponovno aktivirala.

Kada se primjeni ESET PROTECT/ESMC/ERA pravilo, vidjet ćete ikonu za zaključavanje pokraj odgovarajuće komponente. Pravilo koje primjeni ESET Security Management Center ili ESET PROTECT može lokalno nadjačati prijavljeni korisnik (npr. administrator) nakon autorizacije. Dodatne informacije potražite u [mrežnoj pomoći za ESET PROTECT](#).

Tako će se sve deaktivirane mjere zaštite ponovno aktivirati nakon restarta računala.

Ako želite pristupiti detaljnim postavkama neke sigurnosne komponente, kliknite znak zupčanika pored bilo koje komponente.

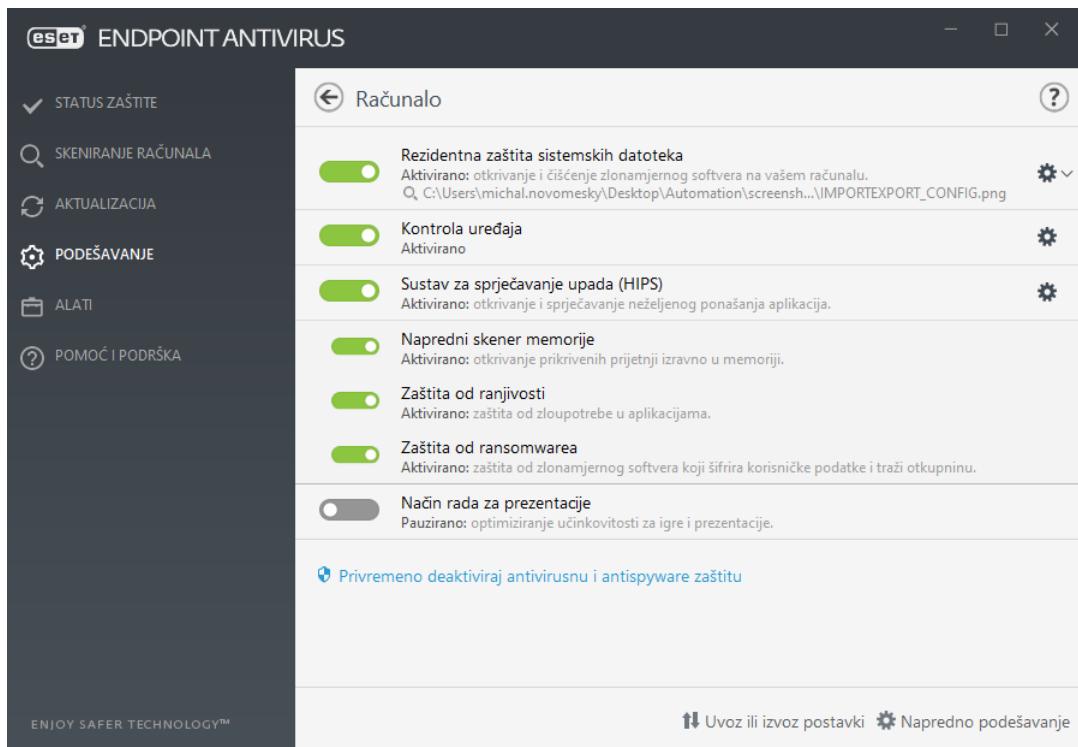
Postoje dodatne mogućnosti na dnu prozora podešavanja. Za učitavanje parametara podešavanja s pomoću .xml/ konfiguracijske datoteke ili spremanje trenutačnih parametara podešavanja u konfiguracijsku datoteku, upotrijebite mogućnost **Uvoz ili izvoz postavki**. Dodatne informacije potražite u odjeljku [Uvoz ili izvoz postavki](#).

Za prikaz detalja mogućnosti kliknite **Napredno podešavanje** ili pritisnite **F5**.

## Računalo

Modul **Računalo** možete pronaći u oknu **Podešavanje > Računalo**. Prikazuje pregled svih zaštitnih modula opisanih u [prethodnom poglavljju](#). U ovom odjeljku dostupne su sljedeće postavke:

Kliknite zupčanik  pokraj stavke **Rezidentna zaštita sistemskih datoteka** i kliknite **Uredi izuzetke** da biste otvorili prozor Podešavanje izuzetaka koji vam omogućuje da izuzmete datoteke i mape od skeniranja. Da biste otvorili napredno podešavanje **Rezidentne zaštite sistemskih datoteka**, kliknite **Konfiguriraj**.



Odjeljak **Računalo** omogućuje aktiviranje ili deaktiviranje sljedećih komponenti:

- **Rezidentna zaštita** – U svim se datotekama skeniranjem provjerava postojanje zlonamjernog koda u trenutku njihova otvaranja, stvaranja ili pokretanja na računalu.
- **Kontrola uređaja** – Omogućuje automatsku [kontrolu](#) uređaja (CD/DVD/USB/...). Ovaj modul omogućuje blokiranje ili prilagođavanje dodatnih filtera/dopuštenja i određuje način na koji korisnik pristupa određenom uređaju i radi s njim.
- **Sustav za sprečavanje upada (HIPS)** – Sustav [HIPS](#) nadzire događaje koji se događaju unutar operacijskog sustava i reagira na njih u skladu s prilagođenim skupom pravila.
- **Napredni skener memorije** – radi zajedno sa zaštitom od zloupotrebe na ojačavanju zaštite od zlonamjernog softvera koji je osmišljen tako da skrivanjem i/ili šifriranjem izbjegava da ga otkriju proizvodi za zaštitu od zlonamjernog softvera. Prema standardnim postavkama napredni je skener memorije aktiviran. Više o toj vrsti zaštite pročitajte u [rječniku](#).
- **Sprečavanje ranjivosti** – Osmišljeno je za ojačavanje zaštite često zloupotrebljavanih vrsta aplikacija kao što su web preglednici, PDF čitači, klijenti e-pošte i komponente sustava MS Office. Sprječavanje ranjivosti aktivirano je prema standardnim postavkama. Pročitajte više o ovoj vrsti zaštite u [rječniku](#).
- **Zaštita od ransomwarea** – dodatan sloj zaštite koji djeluje kao dio funkcije HIPS. Sustav reputacije ESET LiveGrid® mora biti aktiviran da bi zaštita od ransomwarea djelovala. [Više o toj vrsti zaštite pročitajte ovdje](#).
- **Način rada za prezentacije** – Funkcija za korisnike koji softver žele koristiti bez prekida, ne žele biti ometani skočnim prozorima te žele smanjiti korištenje CPU-a. Nakon aktivacije [Načina rada za prezentacije](#) primit ćete poruku upozorenja (mogući sigurnosni rizik) i glavni će prozor postati narančast.

**Pauziraj antivirus i antispyware zaštitu** – Svaki put kada privremeno onemogućite antivirus i antispyware zaštitu, možete odabrati vremensko razdoblje za koje želite da odabrane komponente budu deaktivirane s pomoću padajućeg izbornika i zatim kliknite **Primijeni** da biste onemogućili sigurnosnu komponentu. Za ponovno aktiviranje zaštite kliknite **Aktiviraj antivirusnu i antispyware zaštitu**.

## Modul detekcije

Modul detekcije štiti sustav od zlonamjernih napada nadziranjem datoteka, e-pošte i internetske komunikacije. Primjerice, ako se otkrije objekt klasificiran kao zlonamjerni program, započet će ispravljanje. Modul detekcije može ga eliminirati prvo blokiranjem, a zatim čišćenjem, brisanjem ili premještanjem u karantenu.

Da biste detaljno konfigurirali postavke modula detekcije, kliknite **Napredno podešavanje** ili pritisnite **F5**.

U ovom odjeljku:

- [Kategorije rezidentne zaštite i zaštite na temelju strojnog učenja](#)
- [Skeniranja za zlonamjerne softvere](#)
- [Podešavanje izvješćivanja](#)
- [Podešavanje zaštite](#)
- [Najbolje prakse](#)

**i** Počevši od verzije 7.2, odjeljak modula detekcije više nema potvrđne okvire za uključivanje/isključivanje [kao verzija 7.1 i starije](#). Gumbi za uključivanje/isključivanje zamjenjeni su s četiri praga - agresivni, uravnoteženi, oprezni i isključeni.

## Kategorije rezidentne zaštite i zaštite na temelju strojnog učenja

**Rezidentna zaštita i zaštita na temelju strojnog učenja** za sve module za zaštitu (na primjer, rezidentna zaštita sistemskih datoteka, zaštita web pristupa...) omogućuje vam konfiguriranje razina izvještavanja i zaštite sljedećih kategorija:

- **Zlonamjerni programi** – Računalni virus dio je zlonamjernog koda koji je dodan na početak ili na kraj postojećih datoteka na vašem računalu. Međutim, pojam „virus“ često se pogrešno upotrebljava, a točniji bi termin bio „zlonamjerni program“. Zlonamjerni programi otkrivaju se uz pomoć modula detekcije u kombinaciji s komponentom strojnog učenja.

Više o tim vrstama aplikacija pročitajte u [rječniku](#).

- **Potencijalno nepoželjne aplikacije**– Grayware ili potencijalno neželjene aplikacije (PUA) široka su kategorija softvera čija namjera nije nedvosmisleno zlonamjerna poput drugih vrsta zlonamjernih programa, kao što su virusi ili trojanci. Međutim, takvi programi mogu instalirati dodatne neželjene programe, promijeniti rad digitalnog uređaja ili provesti aktivnosti koje korisnik nije dopustio ili koje ne očekuje.

Više o tim vrstama aplikacija pročitajte u [rječniku](#).

- **Potencijalno nesigurne aplikacije** – Naziv je koji se odnosi na komercijalan, legitiman softver koji sadrži mogućnost zloupotrebe. Primjeri potencijalno nesigurnih aplikacija (PUA) obuhvaćaju alate za daljinski pristup, aplikacije za probijanje lozinki i keyloggere (programe koji zapisuju svaki korisnikov pritisak tipke). Više o tim vrstama aplikacija pročitajte u [rječniku](#).

- **Sumnjive aplikacije** obuhvaćaju programe komprimirane pomoću [arhivatora](#) ili protektora. Takve vrste protektora često iskorištavaju autori zlonamjernog softvera kako bi izbjegli da ih se otkrije.

The screenshot shows the ESET Endpoint Antivirus interface. At the top, there's a navigation bar with the ESET logo and tabs for 'MODUL DETEKCIJE', 'REZIDENTNA ZAŠTITA I ZAŠTITA NA TEMELJU STROJNOG UČENJA', 'NADOGRADNJA', 'MREŽNA ZAŠTITA', 'WEB I E-POŠTA', 'KONTROLA UREĐAJA', 'ALATI', and 'KORISNIČKO SUČELJE'. Below the navigation bar, the 'REZIDENTNA ZAŠTITA I ZAŠTITA NA TEMELJU STROJNOG UČENJA' section is expanded, showing various detection modules like 'Zlonamjerni softver', 'Prijavljivanje', 'Zaštita', 'Potencijalno nepoželjne aplikacije', 'Prijavljivanje', 'Zaštita', 'Sumnjive aplikacije', 'Prijavljivanje', 'Zaštita', 'Potencijalno nesigurne aplikacije', 'Prijavljivanje', and 'Zaštita'. Each module has four radio buttons for 'Agresivno', 'Uravnot...', 'Oprezno', and 'Isključeno', with 'Uravnot...' selected for most. There are also 'i' icons next to each module. At the bottom, there are buttons for 'Standardno', 'U redu', and 'Odustani'.

**i** Napredno strojno učenje sada je sastavni dio modula detekcije kao napredni sloj zaštite kojim se poboljšava otkrivanje prijetnji na temelju strojnog učenja. Više o ovoj vrsti zaštite potražite u [rječniku](#).

## Skeniranja za zlonamjerne softvere

Postavke skenera mogu se konfigurirati zasebno za rezidentni skener i [skener na zahtjev](#). Prema standardnim postavkama, omogućena je opcija **Upotrijebi postavke rezidentne zaštite**. Kad je omogućena, relevantne postavke skeniranja na zahtjev preuzimaju se iz odjeljka **Rezidentna zaštita i zaštita na temelju strojnog učenja**.

## Podešavanje izvješćivanja

U slučaju detekcije prijetnje (npr. prijetnja je pronađena i klasificirana kao zlonamjerni program), informacije će se zabilježiti u [Dnevniku otkrivenih prijetnji](#) i pojavit će se [obavijesti na radnoj površini](#) ako je tako konfigurirano u programu ESET Endpoint Antivirus.

Prag za prijavljivanje konfiguriran je za svaku kategoriju (dalje u tekstu „KATEGORIJA”):

- 1.Zlonamjerni programi
- 2.Potencijalno nepoželjne aplikacije
- 3.Potencijalno nesigurne
- 4.Sumnjive aplikacije

Izvještavanje putem modula detekcije, uključujući komponentu strojnog učenja. Moguće je postaviti viši prag za prijavljivanje od trenutačnog [praga](#) zaštite. Ove postavke ne utječu na blokiranje, [čišćenje](#) ni uklanjanje [objekata](#).

Prije promjene praga (ili razine) za KATEGORIJU izvještavanje pročitajte sljedeće:

Prag	Objašnjenje
<b>Agresivno</b>	Prijavljanje KATEGORIJE konfiguirirano je na najveću osjetljivost. Prijavljuje se više otkrivenih prijetnji. Postavka <b>Agresivno</b> može pogrešno prepoznati objekte kao KATEGORIJU.
<b>Uravnoteženo</b>	Prijavljanje KATEGORIJE konfiguirirano je kao uravnoteženo. Ova postavka je optimizirana kako bi se uravnotežili rezultati i stopa otkrivanja prijetnji i broj pogrešno prijavljenih objekata.
<b>Oprezno</b>	Prijavljanje KATEGORIJE konfiguirirano je za smanjenje pogrešno prepoznatih objekata na najmanju mjeru uz održavanje dovoljne razine zaštite. Objekti se prijavljuju samo kada postoji visoka vjerojatnost da je riječ o prijetnji i kada ponašanje objekta odgovara ponašanju KATEGORIJE.
<b>Isključeno</b>	Prijavljanje KATEGORIJE nije aktivno, a ova se vrsta prijetnje ne pronalazi, prijavljuje niti čisti. Stoga se ovom postavkom deaktivira zaštita protiv ove vrste prijetnje. Opcija Isključeno nije dostupna za prijavljivanje zlonamjernih programa i standardna je vrijednost za potencijalno nesigurne aplikacije.

### [Dostupnost modula za zaštitu programa ESET Endpoint Antivirus](#)

Dostupnost (aktivirana ili deaktivirana) modula za zaštitu za odabrani prag KATEGORIJE jest sljedeći:

	Agresivno	Uravnoteženo	Oprezno	Isključeno**
Modul naprednog strojnog učenja*	✓ (agresivni način)	✓ (konzervativni način)	X	X
Modul detekcije	✓	✓	✓	X
Ostali moduli za zaštitu	✓	✓	✓	X

\* Dostupno u verziji programa ESET Endpoint Antivirus 7.2 i novijima.

\*\* Nije preporučeno

### [Određivanje verzije programa, modula programa i datuma podverzije](#)

1. Kliknite **Pomoć i podrška > O programu ESET Endpoint Antivirus**.

2. Na zaslonu **O programu**, prvi redak teksta prikazuje broj verzije vašeg ESET programa.

3. Kliknite **Instaliraj komponente** da biste pristupili informacijama o određenim modulima.

## Osnovne bilješke

Nekoliko osnovnih bilješki za postavljanje odgovarajućeg praga za vaše okruženje:

- Prag **Uravnoteženo** preporučuje se za većinu postavki.
- Prag **Oprezno** predstavlja usporedivu razinu zaštite od prethodnih verzija programa ESET Endpoint Antivirus (7.1 i starije). Preporučuje se za okruženja gdje je prioritet da sigurnosni softver smanji broj lažno identificiranih objekata.
- Što je viši prag za izvještavanje, viša je stopa otkrivanja, ali i šanse da će se objekt lažno prepoznati.
- Iz perspektive stvarnog svijeta, ne postoji jamstvo 100 %-tne stope otkrivanja prijetnji, kao ni 0 %-tne šanse da se izbjegne pogrešna kategorizacija čistih objekata kao zlonamjernih programa.
- [Redovito ažurirajte program ESET Endpoint Antivirus i njegove module](#) kako bi se maksimalno povećala ravnoteža između performansi i učinkovitosti stopa otkrivanja prijetnji i broja pogrešno prijavljenih objekata.

## Podešavanje zaštite

Ako je objekt klasificiran kao KATEGORIJA prijavljen, program blokira objekt i potom ga [uklanja](#), briše ili prebacuje u [Karantenu](#).

Prije promjene praga (ili razine) za KATEGORIJU zaštite pročitajte sljedeće:

Prag	Objašnjenje
<b>Agresivno</b>	Blokiraju se prijavljene otkrivene prijetnje agresivne razine (ili prijetnje niže razine) i pokreće se automatsko ispravljanje (npr. čišćenje). Ova postavka se preporučuje kada su sva računala skenirana uz postavke na agresivnoj razini i kada su pogrešno prijavljeni objekti dodani u izuzete otkrivene prijetnje.
<b>Uravnoteženo</b>	Blokiraju se prijavljene otkrivene prijetnje uravnotežene razine (ili prijetnje niže razine) i pokreće se automatsko ispravljanje (npr. čišćenje).
<b>Oprezno</b>	Blokiraju se prijavljene otkrivene prijetnje na opreznoj razini rada i pokreće se automatsko ispravljanje prijetnji (npr. čišćenje).
<b>Isključeno</b>	Ovo je korisno za prepoznavanje i izuzimanje pogrešno prijavljenih objekata. Opcija Isključeno nije dostupna za zaštitu od zlonamjernih programa i standardna je vrijednost za potencijalno nesigurne aplikacije.

 [Tablica konverzije pravila programa ESET PROTECT za ESET Endpoint Antivirus 7.1 i starije verzije](#)

Od programa ESET PROTECT uređivač pravila za postavke skenera više ne sadrži opcije za uključivanje/isključivanje za pojedine KATEGORIJE. U tablici u nastavku navedena je konverzija između praga zaštite i završnog stanja [programu ESET Endpoint Antivirus 7.1 i starijim verzijama](#).

Stanje praga za KATEGORIJU	Agresivno	Uravnoteženo	Oprezno	Isključeno
Primijenjeno prebacivanje KATEGORIJE	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Pri nadogradnji s verzije 7.1 i starijih na verziju 7.2 i novije, novo stanje praga bit će sljedeće:

Prebacivanje kategorije prije nadogradnje	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Novi prag za KATEGORIJE nakon nadogradnje		Uravnoteženo	Isključeno

## Najbolje prakse

### NEUPRAVLJANO (radna stanica pojedinačnog klijenta)

Zadržite standardne preporučene vrijednosti kakve jesu.

### UPRAVLJANO OKRUŽENJE

Ove se postavke obično primjenjuju na radne stanice pomoću [pravila](#).

#### 1. Početna faza

Ova faza može potrajati do jednog tjedna.

- Postavite sve pragove za **Prijavljivanje** na **Uravnoteženo**.  
**NAPOMENA:** ako je potrebno, postavite ih na **Agresivno**.
- Postavite ili zadržite **Zaštitu** od zlonamjernih programa na razini **Uravnoteženo**.
- Postavite **Zaštitu** za druge KATEGORIJE na **Oprezno**.  
**NAPOMENA:** U ovoj se fazi ne preporučuje postavljanje praga **Zaštite** na **Agresivno** jer će se ispraviti sve otkrivene prijetnje, uključujući one koje su lažno prijavljene.
- Odredite lažno prijavljene objekte u [Dnevniku otkrivenih prijetnji](#) i prvo ih dodajte [Izuzecima detekcija poznatih prijetnji](#).

#### 2. Faza prijelaza

- Provedite „fazu produkcije“ na nekim radnim stanicama kao test (ne za sve radne stanice na mreži).

#### 3. Faza produkcije

- Postavite sve pragove **Zaštite** na **Uravnoteženo**.
- Prilikom daljinskog upravljanja upotrijebite odgovarajuće [unaprijed definirano pravilo](#) za antivirus za program ESET Endpoint Antivirus.
- Prag zaštite **Agresivno** može se postaviti ako su potrebne najveće stope otkrivanja prijetnji i ako su prihvaćeni lažno prepoznati objekti.
- Provjerite [Dnevnik otkrivenih prijetnji](#) ili izvješća programa ESET PROTECT kako biste pronašli moguće prijetnje koje nedostaju.

# Napredne opcije modula detekcije

**Tehnologija Anti-Stealth** sofisticiran je sustav prepoznavanja opasnih programa poput [rootkita](#) koji se mogu sakriti od operacijskog sustava. To znači da ih nije moguće otkriti primjenom uobičajenih tehnika testiranja.

**Aktiviraj napredno skeniranje putem AMSI-ja** – Alat Microsoft Antimalware Scan Interface koji omogućuje razvojnim inženjerima aplikacije obranu od novog zlonamjernog softvera (samo za Windows 10).

## Otkrivena je infiltracija

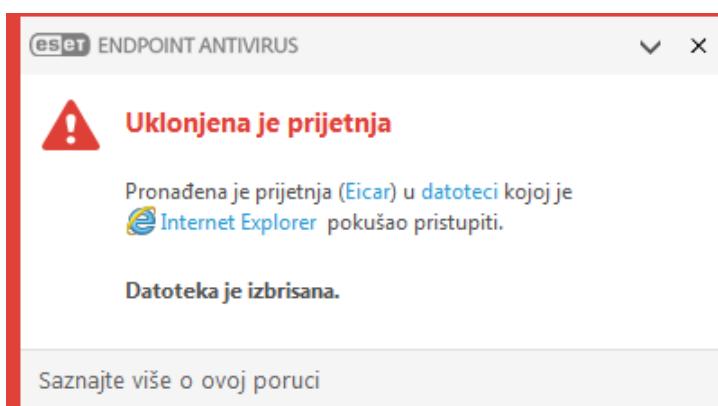
Infiltracije mogu doći do sustava iz raznih izvora: s [web stranica](#), iz zajednički korištenih mapa, putem e-pošte ili s [izmjenjivih uređaja](#) (USB-ova, vanjskih diskova, CD-ova, DVD-ova, itd.).

## Standardno ponašanje

Kao općeniti primjer načina na koji ESET Endpoint Antivirus postupa s infiltracijama, infiltracije se mogu otkriti korištenjem značajki:

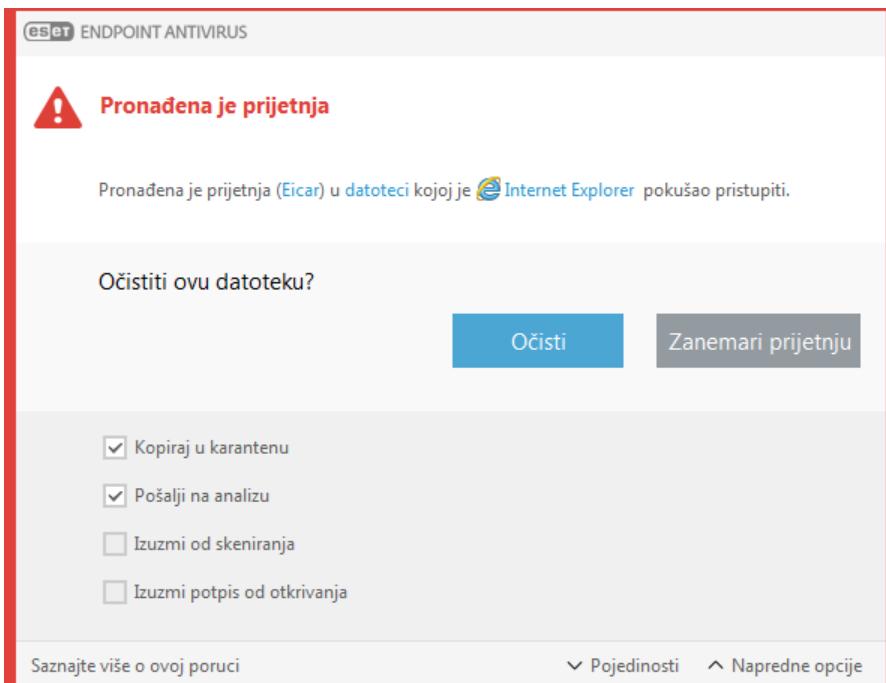
- [režidentna zaštita](#)
- [zaštita web pristupa](#)
- [zaštita klijenta e-pošte](#)
- [Skeniranje računala na zahtjev](#)

Svaka funkcija koristi standardnu razinu čišćenja i pokušat će očistiti datoteku i premjestiti je u [karantenu](#) ili prekinuti vezu. U području obavijesti u donjem desnom kutu zaslona prikazuje se prozor obavijesti. Detaljne informacije o otkrivenim/izbrisanim objektima potražite u opciji [Dnevnići](#). Dodatne informacije o razinama čišćenja i ponašanju potražite u odjeljku [Čišćenje](#).



## Čišćenje i brisanje

Ako za rezidentnu zaštitu nije unaprijed definirana akcija koju treba poduzeti, prikazat će se prozor upozorenja u kojem se od korisnika traži da odabere jednu od mogućnosti. Obično su dostupne mogućnosti **Očisti**, **Izbriši** i **Bez akcije**. Ne preporučuje se odabir mogućnosti **Bez akcije** jer će na taj način zaražene datoteke ostati neočišćene. Iznimka su jedino datoteke za koje ste sigurni da su bezopasne i da su otkrivene pogreškom.



Primjenite čišćenje ako je datoteku napao virus koji je pridodao zlonamjerni kôd uz datoteku. U tom slučaju prvo pokušajte očistiti zaraženu datoteku da biste je vratili u izvorno stanje. Ako se datoteka sastoji isključivo od zlonamjernog koda, bit će izbrisana.

Ako je zaražena datoteka „zaključana“ ili je koristi neki sistemski proces, obično se briše tek po prestanku zauzeća (najčešće nakon ponovnog pokretanja sustava).

## Vraćanje iz karantene

Karanteni se može pristupiti iz glavnog prozora programa ESET Endpoint Antivirus klikom na **Alati > Karantena**.

Datoteke u karanteni također se mogu vratiti na izvornu lokaciju:

- U tu svrhu upotrijebite funkciju **Vrati**, koja je dostupna iz kontekstnog izbornika tako da desnom tipkom miša kliknete određenu datoteku u karanteni.
- Ako je datoteka označena kao [potencijalno neželjena aplikacija](#), aktivirana je opcija **Vrati i izuzmi od skeniranja**. Također pogledajte odjeljak [Izuzeci](#).
- Kontekstni izbornik također pruža opciju **Vrati na**, koja vam omogućuje vraćanje datoteke na lokaciju koja nije ista kao lokacija s koje je datoteka obrisana.
- Funkcija vraćanja nije dostupna u nekim slučajevima, na primjer, za datoteke koje se nalaze na zajedničkoj mreži samo za čitanje.

## Višestruke prijetnje

Ako neke zaražene datoteke nisu očišćene tijekom skeniranja računala (ili je [Razina čišćenja](#) postavljena na **Bez čišćenja**), prikazuje se prozor upozorenja s upitom o odabiru radnje za te datoteke.

## Brisanje datoteka u arhivama

U standardnom načinu čišćenja cijela se arhiva briše samo ako su sve datoteke u toj arhivi zaražene. Drugim riječima, arhive se ne brišu ako sadrže i bezopasne čiste datoteke. Budite oprezni prilikom skeniranja potpunim čišćenjem – potpuno čišćenje briše svaku arhivu koja sadrži najmanje jednu zaraženu datoteku, bez obzira na status ostalih datoteka u arhivi.

Ako računalo pokazuje znakove zaraze zlonamjernim softverom, na primjer sporije radi, često se "zamrzava" itd., preporučujemo sljedeće:

- Otvorite program ESET Endpoint Antivirus i kliknite Skeniranje računala;
- Kliknite **Smart skeniranje** (dodatne informacije potražite u odjelu [Skeniranje računala](#));
- Nakon završetka skeniranja pogledajte u dnevniku koliko je skeniranih, zaraženih i očišćenih datoteka.

Ako želite skenirati samo određeni dio diska, kliknite **Prilagođeno skeniranje** i odaberite ciljeve u kojima će se skeniranjem provjeriti postojanje virusa.

## Zajednička lokalna predmemorija

Zajednička lokalna predmemorija može poboljšati performanse u izoliranim okruženjima (na primjer, virtualna računala) eliminiranjem dvostrukog skeniranja na mreži. Tako se osigurava da će se svaka datoteka skenirati samo jednom i pohraniti u zajedničku predmemoriju.

Prvo se treba instalirati i konfigurirati ESET Shared Local Cache.

- [Preuzmite ESET Shared Local Cache](#).
- Više informacija potražite u [mrežnoj pomoći za ESET Shared Local Cache](#).

Aktivirajte **Opciju predmemoriranja** da biste spremili informacije o skeniranjima datoteka i mapa na mreži u ESET Shared Local Cache. Ako pokrenete novo skeniranje, ESET Endpoint Antivirus će potražiti skenirane datoteke u ESET Shared Local Cache. Ako se datoteke podudaraju, bit će izuzete od skeniranja.

Podešavanje za **Server predmemorije** sadrži sljedeće:

- **Naziv hosta** – Naziv ili IP adresa računala na kojem se nalazi ESET Shared Local Cache.
- **Port** – Broj porta koji se upotrebljava za komunikaciju (isto kao što je postavljeno pod ESET Shared Local Cache).
- **Lozinka** – Navedite lozinku za ESET Shared Local Cache ako je potrebno.

## rezidentna zaštita

Rezidentna zaštita sistemskih datoteka kontrolira zlonamjeran kod u svim datotekama u sustavu kada se otvore, stvore ili pokrenu.

The screenshot shows the 'Napredno podešavanje' (Advanced Settings) screen of the ESET Endpoint Antivirus software. On the left, a sidebar lists several modules: 'MODUL DETEKCIJE' (2), 'Rezidentna zaštita sistemskih datoteka', 'Zaštita potpomognuta cloudom', 'Skeniranje zlonamjernog softvera', 'HIPS' (2), 'NADOGRADNJA' (2), 'MREŽNA ZAŠTITA', 'WEB I E-POŠTA' (3), 'KONTROLA UREĐAJA' (2), 'ALATI' (3), and 'KORISNIČKO SUČELJE' (1). The main panel is titled 'OSNOVNO' and contains the following sections:

- Aktiviraj rezidentnu zaštitu sistemskih datoteka**: A toggle switch is set to 'On' (indicated by a blue checkmark).
- MEDIJI ZA SKENIRANJE**: Three checkboxes are checked:
  - Lokalni pogoni
  - Izmjenjivi mediji
  - Mrežni pogoni
- SKENIRAJ PRI SLJEDEĆEM**: Four checkboxes are checked:
  - Otvaranje datoteke
  - Stvaranje datoteke
  - Pokretanje datoteke
  - Pristup boot sektoru izmjenjivih medija
- IZUZETI PROCESI**: Buttons for 'Standardno' (selected), 'U redu', and 'Odustani'.

Prema standardnim postavkama rezidentna zaštita sistemskih datoteka pokreće se prilikom pokretanja sustava i omogućuje neometano skeniranje. Ne preporučujemo deaktiviranje opcija **Aktiviraj rezidentnu zaštitu sistemskih datoteka** u odjeljku **Napredno podešavanje** pod stavkom **Modul detekcije > Rezidentna zaštita sistemskih datoteka > Osnovno**.

## Mediji za skeniranje

Prema standardnim postavkama skeniraju se sve vrste medija radi otkrivanja potencijalnih prijetnji:

- **Lokalni pogoni** – skenira sve tvrde diskove sustava te fiksne tvrde pogone (primjer: *C:\*, *D:\*).
- **Izmjenjivi mediji** – skenira CD-ove/DVD-ove, USB medije, memorijske kartice itd.
- **Mrežni pogoni** – skenira sve mapirane mrežne pogone (primjer: *H:\* kao `\|store04`) ili mrežne pogone s izravnim pristupom (primjer: `\|store08`).

Promjenu tih standardnih postavki preporučujemo samo u iznimnim slučajevima, primjerice ako nadzor određenog medija značajno usporava prijenos podataka.

## Skeniraj pri

Prema standardnim postavkama sve se datoteke skeniraju prilikom otvaranja, stvaranja ili izvršavanja. Preporučujemo da zadržite standardne postavke zato što osiguravaju maksimalnu razinu rezidentne zaštite računala:

- **Otvaranje datoteke** – Skenira prilikom otvaranja datoteke.

- **Stvaranje datoteke** – Skenira stvorenu ili izmijenjenu datoteku.
- **Pokretanje datoteke** – Skenira kad se datoteka izvršava ili pokreće.
- **Pristup boot sektoru izmjenjivih medija** – kada se u uređaj umetnu izmjenjivi mediji koji sadrže boot sektor, on se odmah skenira. Ova opcija ne omogućuje skeniranje datoteka izmjenjivih medija. Skeniranje datoteka izmjenjivih medija se nalazi u odjeljku **Mediji za skeniranje > Izmjenjivi mediji**. Da bi opcija **Pristup boot sektoru izmjenjivih medija** ispravno radila, ostavite opciju **Boot sektori / UEFI** aktiviranu u ThreatSense parametrima.

**Procesi koji će se izuzeti od skeniranja** – pročitajte više o ovoj vrsti izuzetka u poglavlju [Izuzeti procesi](#).

Rezidentna zaštita provjerava sve vrste medija, a pokreću je različiti događaji u sustavu, poput pristupa datoteci. Pomoću metoda za otkrivanje u tehnologiji ThreatSense (opisane su u odjeljku [Podešavanje parametara sustava ThreatSense](#)) rezidentna zaštita može se konfigurirati tako da s novostvorenim datotekama postupa drugačije nego s postojećim datotekama. Primjerice, možete konfigurirati rezidentnu zaštitu da detaljnije nadzire novostvorene datoteke.

Radi postizanja minimalnog utjecaja na sustav pri upotrebi rezidentne zaštite već skenirane datoteke ne skeniraju se ponovno (osim ako su izmijenjene). Datoteke se ponovno skeniraju odmah nakon svake aktualizacije modula za otkrivanje. To se ponašanje konfigurira s pomoću opcije **Smart optimizacija**. Ako je **Smart optimizacija** deaktivirana, sve se datoteke skeniraju u trenutku kada im se pristupa. Da biste promijenili tu postavku, pritisnite **F5** i otvorite Napredno podešavanje da bi se otvorio prozor **Modul za otkrivanje > Rezidentna zaštita**. Kliknite **ThreatSense parametri > Ostalo** i odaberite ili poništite odabir opcije **Aktiviraj Smart optimizaciju**.

## Provjera rezidentne zaštite

Da biste provjerili funkcioniranje rezidentne zaštite i njeno otkrivanje virusa, upotrijebite probnu datoteku s adrese eicar.com. Ta probna datoteka je bezopasna i mogu je otkriti svi antivirusni programi. Datoteku je stvorila tvrtka EICAR (European Institute for Computer Antivirus Research – Europski institut za istraživanje zaštite od računalnih virusa) u svrhu testiranja funkcionalnosti antivirusnih programa.

Datoteka se može preuzeti s adrese <http://www.eicar.org/download/eicar.com>.

Nakon što unesete ovaj URL u svoj preglednik, trebali biste vidjeti poruku da je prijetnja uklonjena.

## Kada treba izmijeniti konfiguraciju rezidentne zaštite

Rezidentna zaštita najvažnija je komponenta za održavanje sigurnog sustava. Stoga oprezno mijenjajte njezine parametre. Preporučujemo vam da te parametre mijenjate samo u specifičnim slučajevima.

Nakon instalacije programa ESET Endpoint Antivirus sve postavke optimizirane su tako da se korisnicima pruži maksimalna razina zaštite sustava. Da biste vratili standardne postavke, kliknite  uz svaku karticu u prozoru (**Napredno podešavanje > Modul za otkrivanje > Rezidentna zaštita**).

## Što ako rezidentna zaštita ne funkcioniра

U ovom se poglavlju opisuju problemi do kojih može doći pri upotrebi rezidentne zaštite te načini njihova rješavanja.

## Rezidentna zaštita je deaktivirana

Ako korisnik nehotice deaktivira rezidentnu zaštitu, treba je ponovno aktivirati. Da biste ponovno aktivirali rezidentnu zaštitu, idite na **Podešavanje** u glavnom prozoru programa i kliknite **Zaštita računala > Rezidentna zaštita sistemskih datoteka**.

Ako se rezidentna zaštita ne pokrene prilikom pokretanja sustava, vjerojatno je deaktivirana mogućnost **Aktiviraj rezidentnu zaštitu**. Kako biste bili sigurni da je ta opcija aktivirana, idite na **Napredno podešavanje (F5)** i kliknite **Modul za otkrivanje > Rezidentna zaštita**.

## Ako rezidentna zaštita ne otkriva ni ne čisti infiltracije

Provjerite nije li na računalu instaliran još neki antivirusni program. Ako su istodobno instalirana dva antivirusna programa, moguće je da će se međusobno sukobljavati. Preporučujemo da prije instalacije programa ESET deinstalirate sve druge antivirusne programe.

## Rezidentna zaštita se ne pokreće

Ako se rezidentna zaštita ne pokrene prilikom pokretanja sustava (a opcija **Aktiviraj rezidentnu zaštitu sistemskih datoteka** je aktivirana), možda je došlo do sukoba s drugim programima. Obratite se ESET-ovoj tehničkoj podršci za pomoć pri rješavanju ovog problema. Stvaranje SysInspector dnevnika i njegovo slanje ESET-ovoj tehničkoj podršci na analizu može pomoći riješiti problem. Za više informacije pročitajte sljedeći [članak ESET-ove baze znanja](#).

## Skeniranje računala

Skener na zahtjev važan je dio programa ESET Endpoint Antivirus. Koristi se za skeniranje datoteka i mapa na računalu. Sa sigurnosne točke gledišta ključno je da se računalo ne skenira samo kada posumnjate na zarazu, već redovito kao dio rutinskih mjera zaštite. Preporučujemo da redovito izvršavate dubinska skeniranja sustava (primjerice, jednom mjesечно) da biste otkrili moguće viruse koje nije otkrila [Rezidentna zaštita](#). To se može dogoditi ako je u tom trenutku rezidentna zaštita bila deaktivirana, ako je modul za otkrivanje virusa bio zastario ili ako datoteka nije otkrivena kao virus kad je spremljena na disk.

The screenshot shows the ESET Endpoint Antivirus application window. On the left sidebar, there are several menu items: STATUS ZAŠTITE, SKENIRANJE RAČUNALA (selected), AKTUALIZACIJA, PODEŠAVANJE, ALATI, and POMOĆ I PODRŠKA. The main content area is titled 'Skeniranje računala'. It displays two scan options: 'Skenirajte računalo' (Scan computer) and 'Skeniranje izmjenjivih medija' (Scan removable media). Below these is a dashed box with the placeholder text 'Povucite i ispustite datoteke ovdje da biste ih skenirali' (Drag and drop files here to scan them). A specific scan task is listed: 'Skeniranje računala' from 12/8/2020 3:52:43 PM, which has found 0 threats. There are buttons for pausing and stopping the scan. At the bottom, a message says 'Ovo može potrajati. Bit će obaviješteni kada se skeniranje završi.' (This may take time. You will be notified when scanning is complete.) and a dropdown menu for 'Radnja nakon skeniranja' (Action after scan) set to 'Ništa' (Nothing).

Dostupne su dvije vrste **Skeniranja računala**. **Skeniraj računalo** brzo skenira sustav bez potrebe za detaljnom konfiguracijom parametara skeniranja. **Prilagođeno skeniranje** omogućuje odabir bilo kojeg prethodno definiranog profila skeniranja i definiranje određenih ciljeva skeniranja.

Dodatne informacije o procesu skeniranja potražite u poglavlju [Napredak skeniranja](#).

## **Skenirajte svoje računalo**

Smart skeniranje omogućuje brzo pokretanje skeniranja računala i čišćenje zaraženih datoteka bez potrebe za korisničkom intervencijom. Prednost je Smart skeniranja to što je jednostavan za upotrebu i ne zahtijeva detaljnu konfiguraciju skeniranja. Smart skeniranje provjerava sve datoteke na lokalnim pogonima te automatski briše otkrivene infiltracije. Razina čišćenja automatski se postavlja na standardnu vrijednost. Dodatne informacije o vrstama čišćenja potražite u odjeljku [Čišćenje](#).

## **Prilagođeno skeniranje**

Prilagođeno skeniranje optimalno je rješenje ako želite zadati parametre kao što su ciljevi i metode skeniranja. Prednost je prilagođenog skeniranja mogućnost detaljnog konfiguiranja parametara. Konfiguracije možete spremiti u korisnički definirane profile koji mogu biti korisni ako se skeniranje opetovano izvodi s istim parametrima.

Da biste odabrali ciljeve skeniranja, odaberite **Skeniranje računala > Prilagođeno skeniranje** i odaberite mogućnost s padajućeg izbornika **Ciljevi skeniranja**, ili odaberite određene ciljeve skeniranja sa strukture stabla. Cilj skeniranja može se preciznije navesti unosom puta do mape ili datoteka koje želite uključiti. Ako vas zanima samo skeniranje sustava bez dodatnih akcija čišćenja, odaberite mogućnost **Skeniraj bez čišćenja**. Prilikom skeniranja možete odabrati jednu od tri razine čišćenja klikom na **Podešavanje > ThreatSense parametri >**

## Čišćenje.

Prilagođeno skeniranje računala prikladno je za napredne korisnike s iskustvom u korištenju antivirusnih programa.

Također možete upotrijebiti funkciju **Skeniranje povlačenjem i ispuštanjem** za ručno skeniranje datoteke ili mape tako da kliknete datoteku ili mapu, pomaknete pokazivač miša na označeno područje uz pritisnutu tipku miša, a zatim je ispustite. Nakon toga aplikacija se premješta u prvi plan.

## **Skeniranje izmjenjivih medija**

Slično opciji „**Skenirajte svoje računalo**“ – omogućuje brzo pokretanje skeniranja izmjenjivih medija (npr. CD/DVD/USB) koji su trenutačno priključeni na računalo. To može biti korisno kada na računalo priključujete USB flash pogon i želite ga skenirati radi otkrivanja zlonamjernog softvera i ostalih mogućih prijetnji.

Tu vrsta skeniranja možete pokrenuti i tako da kliknete **Prilagođeno skeniranje**, odaberete značajku **Izmjenjivi mediji** s padajućeg izbornika **Ciljevi skeniranja** i zatim kliknete **Skeniraj**.

## **Ponavljanje zadnjeg skeniranja**

Omogućuje brzo pokretanje prijašnjeg skeniranja upotrebom istih postavki pomoću kojih je izvedeno.

U padajućem izborniku **Radnja nakon skeniranja** možete odabrati **Bez radnje**, **Isključivanje računala**, **Ponovno pokreni** ili **Ponovno pokreni po potrebi**. Dostupnost radnji **Mirovanje** ili **Hibernacija** ovisi o postavkama uštede energije i stanja mirovanja operacijskog sustava ili mogućnostima stolnog/prijenosnog računala. Odabrana radnja započet će nakon završetka svih pokrenutih skeniranja. Ako odaberete **Isključivanje računala**, prikazat će se prozor s upitom za potvrdu isključivanja s istekom vremena od 30 sekundi (kliknite **Odustani** za deaktivaciju zatraženog isključivanja). Pojedinosti potražite u odjeljku [Napredne mogućnosti skeniranja](#).

 Preporučujemo da skenirate računalo barem jednom mjesечно. Skeniranje se može konfigurirati kao planirani zadatak u odjeljku **Alati > Planer**. [Kako zakazati tjedno skeniranje računala?](#)

## **Pokretač prilagođenog skeniranja**

Ako želite skenirati samo određeni cilj, možete upotrijebiti prilagođeno skeniranje tako da kliknete na stavku **Skeniranje računala > Prilagođeno skeniranje** i odaberete mogućnost s padajućeg izbornika  > **Ciljevi skeniranja** ili odaberete određene ciljeve sa (stablaste) strukture mape.

Prozor za podešavanje ciljeva skeniranja omogućuje definiranje objekata (memorija, pogona, sektora, datoteka i mapa) koji se skeniraju radi pronalaženja infiltracija.

Padajući izbornik **Ciljevi skeniranja** omogućuje odabir ciljeva skeniranja.

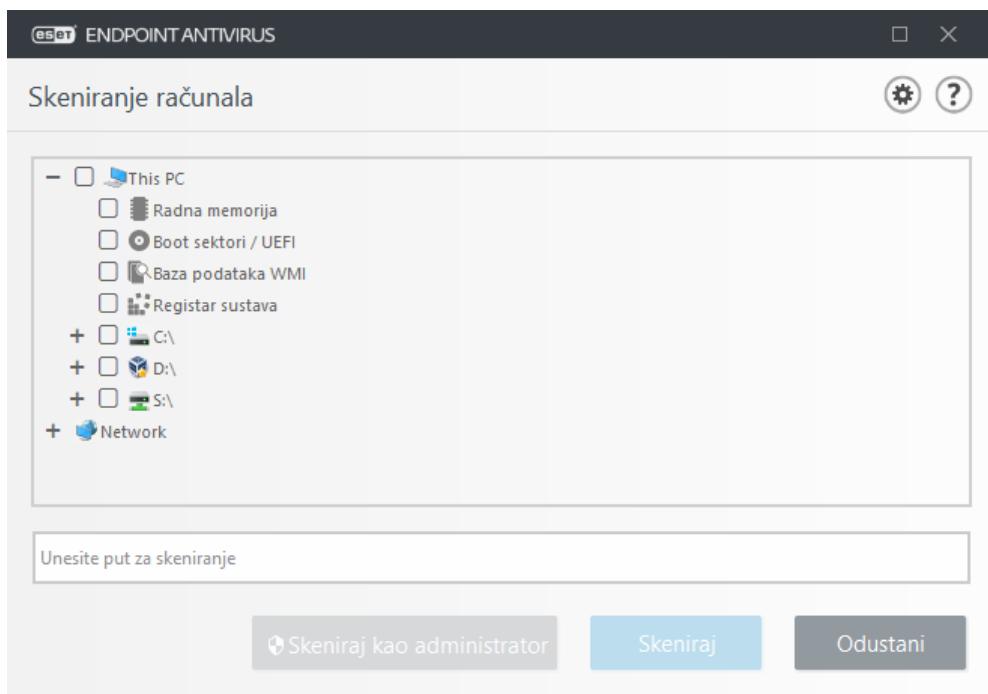
- **Prema postavkama profila** – Odabire ciljeve postavljene u odabranom profilu skeniranja.
- **Izmjenjivi mediji** – Odabire disketne pogone, USB uređaje za pohranu podataka, CD/DVD uređaje.
- **Lokalni pogoni** – Odabire sve sistemske tvrde diskove.

- **Mrežni pogoni** – Odabire sve mapirane mrežne pogone.
- **Prilagođeni odabir** – Poništava sve prethodne odabire.

Struktura mape (stablo) također sadrži specifične ciljeve skeniranja.

- **Radna memorija** – Skenira sve procese i podatke koje trenutačno koristi radna memorija.
- **Boot sektori / UEFI** – Skenira boot sektore i UEFI da bi se otkrila prisutnost zlonamjernih programa. Više o UEFI skeneru pronađite u [rječniku](#).
- **Baza podataka WMI** – Skenira cijelu bazu podataka Windows Management Instrumentation WMI, sva polja naziva, sve instance klase i sva svojstva. Traži reference na zaražene datoteke ili zlonamjerne programe ugrađene kao podatke.
- **Sistemski registar** – Skenira cijeli sistemski registar, sve ključeve i potključeve. Traži reference na zaražene datoteke ili zlonamjerne programe ugrađene kao podatke. Prilikom brisanja prijetnji referenca ostaje u registru kako bi se osiguralo da se ne izgube važni podaci.

Da biste brzo došli do objekta skeniranja ili dodali ciljnu mapu ili jednu ili više datoteka, unesite ciljnu mapu u prazno polje ispod popisa mapa.



Zaražene se stavke ne čiste automatski. Skeniranje bez čišćenja može se upotrebljavati za pregled trenutačnog statusa zaštite. Osim toga možete odabrati jednu od tri razine čišćenja ako kliknete **Napredno podešavanje > Modul za otkrivanje > Skeniranje na zahtjev > ThreatSense parametri > Čišćenje**. Ako želite samo skenirati sustav bez dodatnih radnji čišćenja, odaberite **Skeniraj bez čišćenja**. Povijest skeniranja spremi se u dnevnik skeniranja.

Ako odaberete **Zanemari iznimke** datoteke s ekstenzijama koje su prije bile izuzete od skeniranja sada će se skenirati bez iznimke.

S padajućeg izbornika **Profil skeniranja** možete odabrati profil koji ćete upotrebljavati za skeniranje odabranih objekata. Standardni je profil **Smart skeniranje**. Postoje još tri unaprijed definirana profila skeniranja: **Skeniranje iz kontekstnog izbornika**, **Dubinsko skeniranje** i **Skeniranje računala**. Ovi profili skeniranja upotrebljavaju različite

[ThreatSense parametre](#). Dostupne opcije opisane su pod **Napredno podešavanje > Modul detekcije > Skeniranje zlonamjernih programa > Skeniranje na zahtjev > ThreatSense parametri**.

Kliknite **Skeniraj** da biste izvršili skeniranje s prilagođenim parametrima koje ste postavili.

Mogućnost **Skeniraj kao administrator** omogućuje vam skeniranje s administratorskog računa. Kliknite tu mogućnost ako trenutno prijavljeni korisnik nema dovoljno prava za pristup odgovarajućim datotekama koje treba skenirati. Napominjemo da taj gumb nije dostupan ako trenutačno prijavljeni korisnik ne može zakazivati operacije kontrole korisničkih računa kao administrator.

**i** Kada se skeniranje dovrši, možete vidjeti dnevnik skeniranja računala klikom na mogućnost [Prikaži dnevnik](#).

## Napredak skeniranja

Prozor napretka skeniranja pokazuje status trenutnog skeniranja i informacije o broju datoteka u kojima je pronađen zlonamjerni kôd.

Skeniranje računala ?

Pronađeno prijetnji: 0  
C:\Documents and Settings\John\AppData\Local\Temporary Internet Files\Con...\\4iCv6KVjbNBYIgoC1CzjvmyL[1].woff

8/22/2018 7:13:25 AM || X

Manje informacija

Korisnik: John-PC\John  
Skeniranih objekata: %s  
Trajanje: 0:00:30

C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\c3a84c6dd0bf0eb5da5d84a4742f6f35\_a110f29a-833e-446a-bfdb-195863cabae - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\dc558a410ecc71a25c9884a937c89d6e\_a110f29a-833e-446a-bfdb-195863cabae - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\ef73ed1b2f5151d2486bcc4721be893\_a110f29a-833e-446a-bfdb-195863cabae - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Crypto\RSA\MachineKeys\f080183c2cf12a3df6bc1a8a14723fdb\_a110f29a-833e-446a-bfdb-195863cabae - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Diagnosis\DownloadedSettings\telemetry.ASM-WindowsDefault.json - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Diagnosis\DownloadedSettings\utc.app.json - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Diagnosis\events00.rbs - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Diagnosis\events01.rbs - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Diagnosis\events10.rbs - nije moguće otvoriti [4]  
C:\Documents and Settings\All Users\Microsoft\Diagnosis\events11.rbs - nije moguće otvoriti [4]

Listaj dnevnik skeniranja Zatvori

**i** Normalno je da se neke datoteke, kao što su datoteke zaštićene lozinkom ili datoteke koje isključivo koristi sustav (obično *pagefile.sys* i određeni dnevnići), ne mogu skenirati.

**Napredak skeniranja** – Na traci napretka prikazuju se paralelni postotak već skeniranih objekata i onih koji čekaju da budu skenirani. Status napretka skeniranja određuje se iz ukupnog broja objekata obuhvaćenih skeniranjem.

**Objekt** – Naziv objekta koji se trenutno skenira i njegovo mjesto.

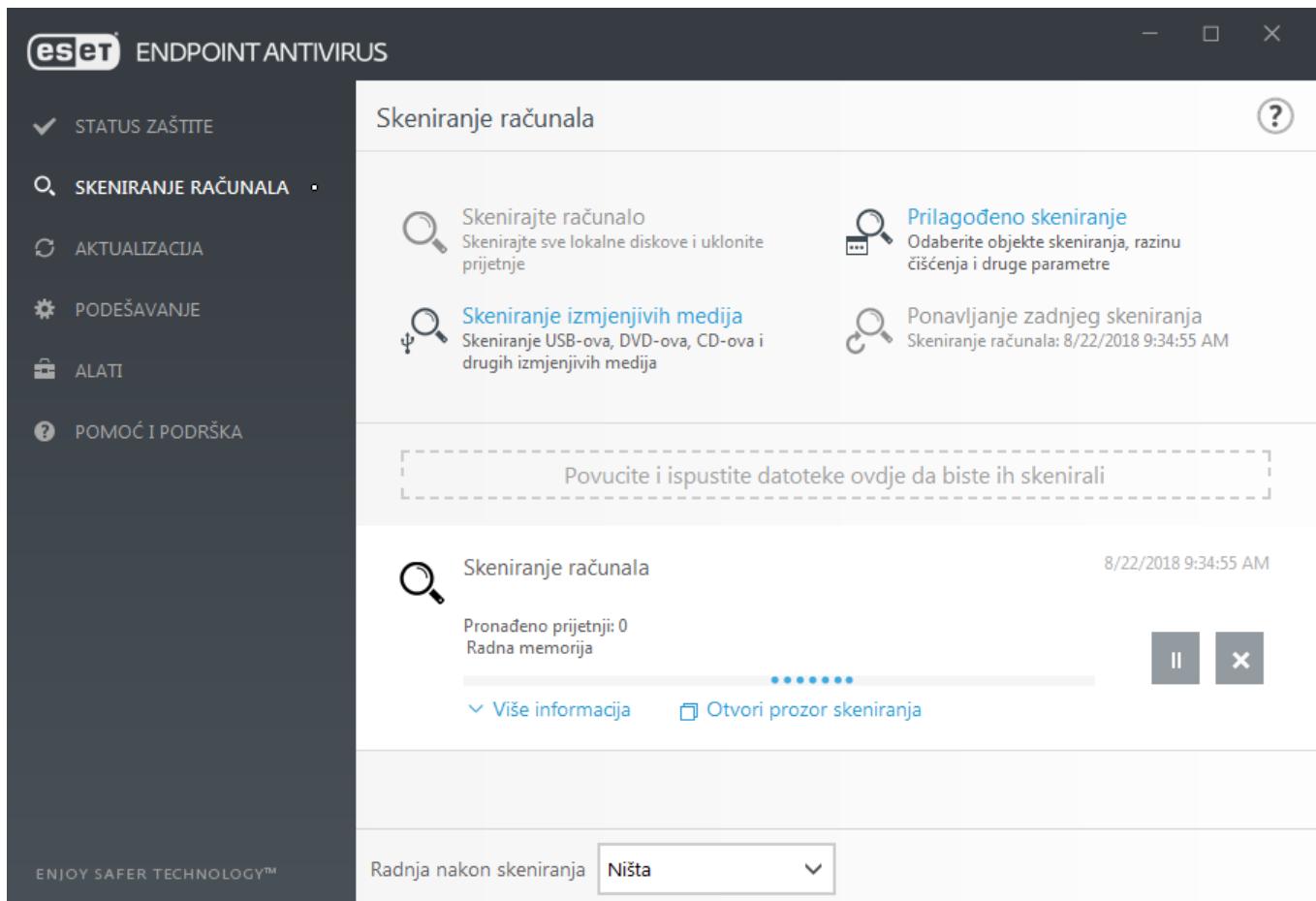
**Pronađene prijetnje** – Prikazuje ukupan broj prijetnji pronađenih tijekom skeniranja.

**Pauza** – Pauzira skeniranje.

**Nastavi** – Ta je opcija vidljiva kada je napredak skeniranja pauziran. Kliknite **Nastavi** za nastavak skeniranja.

**Zaustavljanje** – Zaustavlja skeniranje.

**Listaj dnevnik skeniranja** – Ako je ta opcija aktivirana, dnevnik skeniranja automatski će se listati kako se dodaju novi unosi da bi bili vidljivi najnoviji unosi.



## Dnevnik skeniranja računala

Dnevnik skeniranja računala pruža vam općenite informacije o skeniranju kao što su:

- Datum i vrijeme skeniranja
- Skenirani diskovi, mape i datoteke
- Broj skeniranih objekata
- Broj pronađenih prijetnji
- Vrijeme dovršetka
- Ukupno vrijeme skeniranja

# Skeniranja za zlonamjerne softvere

Odjeljak **Skeniranje zlonamjernih programa** dostupan je u izborniku Napredno podešavanje. Pritisnite tipku **F5**, kliknite **Modul detekcije > Skeniranje zlonamjernih programa** i navest će vam se opcije za odabir parametara skeniranja. Ovaj odjeljak sadrži sljedeće opcije:

- **Odabrani profil** – Određeni skup parametara koje upotrebljava skener na zahtjev.  
Da biste stvorili novi profil, kliknite Uredi pored stavke Popis profila. Više pojedinosti potražite u odjeljku [Profil skeniranja](#).
- **Zaštita na zahtjev i na temelju strojnog učenja** – Pogledajte [modul detekcije \(7.2 i noviji\)](#).
- **Ciljevi skeniranja** – Ako samo želite skenirati određeni cilj, možete kliknuti **Uredi** pored **Ciljevi skeniranja** i odabrati opciju iz padajućeg izbornika ili odabrati određene ciljeve iz strukture mapa (stablaste strukture).  
Pojedinosti potražite u odjeljku [Ciljevi skeniranja](#).
- Podešavanje parametara sustava **ThreatSense** – U tom odjeljku nalaze se opcije Naprednog podešavanja, kao što su datotečne ekstenzije koje želite kontrolirati, korištene metode otkrivanja itd. Kliknite da biste otvorili karticu s naprednim mogućnostima skeniranja.

## Skeniranje u stanju mirovanja

Skener u stanju mirovanja može se aktivirati u **Naprednom podešavanju** pod stavkom **Modul detekcije > Skeniranje zlonamjernih programa > Skeniranje u stanju mirovanja**.

### Skeniranje u stanju mirovanja

Postavite prekidač uz stavku **Aktiviraj skeniranje u stanju mirovanja** u položaj **Uključeno** da biste aktivirali ovu funkciju. Kad se računalo nalazi u stanju mirovanja, na svim lokalnim pogonima provodi se tiho skeniranje računala.

Prema standardnim postavkama skener za stanje mirovanja ne radi kada se računalo (prijenosno računalo) napaja iz baterije. Ovu postavku možete zaobići odabirom potvrdnog okvira uz stavku **Pokreni čak i ako se računalo napaja putem baterije** u Naprednom podešavanju.

Uključite prekidač **Aktiviraj zapisivanje** u naprednom podešavanju da biste vidjeli rezultate skeniranja računala u odjeljku [Dnevnići](#) (u glavnom prozoru programa kliknite **Alati > Dnevnići** i odaberite **Skeniranje računala** s padajućeg izbornika **Dnevnik**).

### Otkrivanje stanja mirovanja

U odjeljku [Pokretači otkrivanja stanja mirovanja](#) naći ćete puni popis uvjeta koje je potrebno zadovoljiti da bi se pokrenuo skener u stanju mirovanja.

Kliknite [Podešavanje parametara modula ThreatSense](#) ako želite izmijeniti više parametara skeniranja (npr. metode otkrivanja) za skeniranje u stanju mirovanja.

# Profil skeniranja

U programu ESET Endpoint Antivirus postoje četiri unaprijed definirana profila skeniranja:

- **Smart skeniranje** – ovo je standardni napredni profil skeniranja. Profil Smart skeniranja upotrebljava tehnologiju Smart optimizacije koja isključuje datoteke za koje je tijekom prethodnog skeniranja utvrđeno da su čiste, a od tog skeniranja nisu izmijenjene. To omogućuje kraće vrijeme skeniranja s minimalnim utjecajem na sigurnost sustava.
- **Skeniranje iz kontekstnog izbornika** – iz kontekstnog izbornika možete započeti skeniranje bilo koje datoteke na zahtjev. Profil skeniranja iz kontekstnog izbornika omogućuje vam da definirate konfiguraciju skeniranja koja će se upotrebljavati kada pokrenete skeniranje na ovaj način.
- **Dubinsko skeniranje** – profil dubinskog skeniranja standardno ne upotrebljava Smart optimizaciju, tako da nijedna datoteka nije isključena iz skeniranja pomoću ovog profila.
- **Skeniranje računala** – ovo je standardni profil koji se upotrebljava za standardno skeniranje računala.

Vaši preferirani parametri skeniranja mogu se spremiti za buduća skeniranja. Preporučujemo da stvorite drugi profil (s različitim ciljevima i metodama skeniranja te ostalim parametrima) za svako redovito korišteno skeniranje.

Za stvaranje novog profila otvorite prozor naprednog podešavanja (F5) i kliknite **Modul za otkrivanje > Skeniranja zlonamjernog softvera > Skeniranje na zahtjev > Popis profila**. Prozor **Upravljanje profilima** sadrži padajući izbornik **Odabrani profil** s postojećim profilima skeniranja i mogućnošću stvaranja novog. Pomoć pri stvaranju profila skeniranja koji odgovara vašim potrebama potražite u odjeljku [Podešavanje parametara sustava ThreatSense](#) za opis svakog parametra podešavanja skeniranja.

Prepostavimo da želite stvoriti vlastiti profil skeniranja i djelomično vam odgovara konfiguracija **Skenirajte svoje računalo**, no ne želite skenirati [runtime arhivatore](#) ni [potencijalno nesigurne aplikacije](#) te želite **i** primjeniti **Potpuno čišćenje**. Unesite naziv novog profila u prozoru **Upravljanje profilima** i kliknite **Dodaj**. Odaberite novi profil iz padajućeg izbornika **Odabrani profil** i prilagodite preostale parametre kako vam odgovara te kliknite **U redu** da biste spremili novi profil.

## Ciljevi skeniranja

Prozor za podešavanje ciljeva skeniranja omogućuje definiranje objekata (memorija, pogona, sektora, datoteka i mapa) koji se skeniraju radi pronalaženja infiltracija.

Padajući izbornik **Ciljevi skeniranja** omogućuje odabir ciljeva skeniranja.

- **Prema postavkama profila** – Odabire ciljeve postavljene u odabranom profilu skeniranja.
- **Izmjenjivi mediji** – Odabire disketne pogone, USB uređaje za pohranu podataka, CD/DVD uređaje.
- **Lokalni pogoni** – Odabire sve sistemske tvrde diskove.
- **Mrežni pogoni** – Odabire sve mapirane mrežne pogone.
- **Prilagođeni odabir** – Poništava sve prethodne odabire.

Struktura mape (stablo) također sadrži specifične ciljeve skeniranja.

- **Radna memorija** – Skenira sve procese i podatke koje trenutačno koristi radna memorija.
- **Boot sektori / UEFI** – Skenira boot sektore i UEFI da bi se otkrila prisutnost zlonamjernih programa. Više o UEFI skeneru pronađite u [rječniku](#).
- **Baza podataka WMI** – Skenira cijelu bazu podataka Windows Management Instrumentation WMI, sva polja naziva, sve instance klase i sva svojstva. Traži reference na zaražene datoteke ili zlonamjerne programe ugrađene kao podatke.
- **Sistemski registar** – Skenira cijeli sistemski registar, sve ključeve i potključeve. Traži reference na zaražene datoteke ili zlonamjerne programe ugrađene kao podatke. Prilikom brisanja prijetnji referenca ostaje u registru kako bi se osiguralo da se ne izgube važni podaci.

Da biste brzo došli do objekta skeniranja ili dodali ciljnu mapu ili jednu ili više datoteka, unesite ciljnu mapu u prazno polje ispod popisa mapa.

## Napredne mogućnosti skeniranja

U ovom prozoru možete odrediti napredne mogućnosti za planirani zadatak skeniranja računala. Putem padajućeg izbornika možete postaviti automatsko izvršenje akcije kada završi skeniranje:

- **Isključi** – Kada skeniranje završi, računalo se isključuje.
- **Ponovno pokreni** – Zatvara sve otvorene programe i restarta računalo kada završi skeniranje.
- **Ponovno pokreni prema potrebi** – zatvara sve otvorene programe i ponovno pokreće računalo ako skeniranje to zatraži.
- **Spavanje** – Sprema vašu sesiju i stavlja računalo u privremeno stanje u kojem troši malo energije kako biste brzo mogli nastaviti s radom.
- **Hibernacija** – Prebacuje sve što radi na sistemskoj memoriji (RAM) u posebnu datoteku na tvrdom disku. Računalo se isključuje, ali će se prilikom sljedećeg pokretanja vratiti u svoje posljednje stanje prije isključenja.
- **Bez radnje** – Kada skeniranje završi, neće se izvršiti nijedna radnja.

**i** Napominjemo da računalo u mirovanju i dalje radi. Dok radi na bateriju, njegove osnovne funkcije i dalje rade i vaše računalo i dalje troši električnu energiju. Da bi vam baterija dulje trajala, primjerice prilikom odlaska izvan ureda, preporučujemo upotrebu opcije hibernacije.

Odaberite mogućnost **Korisnik ne može odustati od radnje** kako biste korisnicima koji nemaju posebne ovlasti onemogućili prekidanje radnji nakon skeniranja.

Odaberite mogućnost **Korisnik može pauzirati skeniranje na (min)** ako želite odabranom i ograničenom broju korisnika omogućiti pauziranje skeniranja računala na određeno vremensko razdoblje.

Pogledajte i poglavlje [Napredak skeniranja](#).

# Kontrola uređaja

ESET Endpoint Antivirus omogućuje automatski nadzor nad uređajima (CD/DVD/USB/...). Taj modul omogućuje blokiranje ili prilagođavanje dodatnih filtara/ovlaštenja i odabir načina na koji korisnik pristupa određenom uređaju i radi s njim. To može biti korisno ako administrator računala želi korisnicima zabraniti upotrebu uređaja na kojima se nalazi nedopušten sadržaj.

## Podržani vanjski uređaji:

- Pohrana na disku (HDD, izmjenjivi USB disk)
- CD/DVD
- USB pisač
- FireWire Spremiste
- Bluetooth uređaj
- Čitač pametnih kartica
- Uređaj za obradu slike
- Modem
- LPT/COM port
- Prijenosni uređaj
- Sve vrste uređaja

Mogućnosti podešavanja kontrole uređaja mogu se izmijeniti pod **Napredno podešavanje (F5) > Kontrola uređaja**.

Odabirom potvrdnog okvira uz stavku **Aktiviraj kontrolu uređaja** aktivira se funkcija kontrole uređaja u programu ESET Endpoint Antivirus; morat ćete ponovno pokrenuti računalo da bi ova promjena stupila na snagu. Nakon što se kontrola uređaja aktivira, **pravila** će postati aktivna, što će omogućiti otvaranje prozora [Uređivač pravila](#).

Ako se umetne uređaj koji blokira postojeće pravilo, prikazat će se prozor obavijesti i pristup uređaju bit će zabranjen.

## Uređivač pravila kontrole uređaja

Prozor **Uređivač pravila kontrole uređaja** prikazuje postojeća pravila i omogućuje preciznu kontrolu vanjskih uređaja koje korisnici povezuju s računalom. Pogledajte i [Dodavanje pravila kontrole uređaja](#).



Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

- [Dodavanje i izmjena pravila kontrole uređaja ESET-ovim sigurnosnim programima](#)

Pravila

Naziv	Aktivirano	Vrsta	Opis	Radnja	Korisnici	Ozbiljnost	Vrem...
Block USB for User	<input checked="" type="checkbox"/>	Čvrsti disk		Blokiraj	Sve	Sve	Sve
Rule	<input checked="" type="checkbox"/>	Bluetooth ur...		Čitanje/pisa...	Sve	Sve	Sve

Dodaj    Uredi    Izbrisati    Kopiraj    Ispuni    ↑ ↓ ↑ ↓

U redu    Odustani

Moguće je dopustiti ili blokirati određene uređaje po korisniku ili korisničkoj grupi ili na temelju nekih dodatnih parametara koje je moguće odrediti u konfiguraciji pravila. Popis pravila sadrži nekoliko opisa pravila poput naziva, vrste vanjskog uređaja, akcije koju treba poduzeti nakon povezivanja vanjskog uređaja s računalom i zapisivanja ozbiljnosti.

Kliknite **Dodaj** ili **Uredi** da biste upravljali pravilom. Poništite potvrđni okvir **Aktivirano** pored pravila koje želite deaktivirati do sljedeće upotrebe. Ako pravila želite trajno izbrisati, odaberite jedno ili više pravila i kliknite **Izbrisati**.

**Kopiraj** – Stvara novo pravilo s unaprijed definiranim mogućnostima koje se koriste za drugo odabranou pravilo.

Kliknite mogućnost **Ispuni** da biste automatski unijeli parametre uređaja izmjenjivih medija povezanih s računalom.

Pravila su na popisu poredana prema prioritetu pa su pravila višeg prioriteta bliže vrhu popisa. Pravila se mogu pomaknuti klikom ↑ ↓ ↑ ↓ **Vrh/Gore/Dolje/Dno** i mogu se pomaknuti pojedinačno ili u grupama.

Dnevnik kontrole uređaja bilježi sve slučajeve uključivanja kontrole uređaja. Unosi u dnevniku mogu se pregledati u glavnom prozoru programa ESET Endpoint Antivirus pod **Alati > Dnevnići**.

## Otkriveni uređaji

Klikom na gumb **Ispuni** prikazat će se svi trenutačno povezani uređaji i sljedeće informacije o njima: vrsta uređaja, informacije o proizvođaču uređaja, model i serijski broj (ako je dostupan).

Ako odaberete uređaj (s popisa otkrivenih uređaja) i kliknete **U redu**, prikazat će se prozor uređivača pravila s unaprijed definiranim informacijama (sve se postavke mogu prilagođavati).

# Grupe uređaja

 Uređaj povezan s vašim računalom može predstavljati sigurnosni rizik.

Prozor grupe uređaja podijeljen je u dva dijela. U desnom dijelu prozora nalazi se popis uređaja koji pripadaju dotičnoj grupi, a u lijevom dijelu nalaze se stvorene grupe. Odaberite grupu s popisom uređaja koje želite prikazati u desnom oknu.

Kada otvorite prozor grupe uređaja i odaberete grupu, možete dodavati uređaje na popis ili ih uklanjati s popisa. Drugi način dodavanja uređaja u grupu jest uvoz iz datoteke. Umjesto toga, možete kliknuti gumb **Ispuni** i popis svih uređaja povezanih na vaše računalo prikazat će se u prozoru **Otkriveni uređaji**. Odaberite uređaj s ispunjenog popisa da biste ga dodali u grupu klikom na gumb **U redu**.

## Kontrolni elementi

**Dodaj** – Možete dodati grupu tako da unesete njezin naziv ili možete dodati uređaj u postojeću grupu (opcionalno možete navesti detalje kao što su naziv proizvođača, model i serijski broj) ovisno o tome na kojem ste dijelu prozora kliknuli gumb.

**Uredi** – Ova opcija omogućuje izmjenu naziva odabrane grupe ili parametara uređaja (prodavač, model, serijski broj).

**Izbriši** – Briše odabranu grupu ili uređaj, ovisno o tome u kojem ste dijelu prozora kliknuli gumb.

**Uvezi** – Uvozi popis uređaja iz tekstne datoteke. Za uvoz uređaja iz tekstne datoteke potreban je ispravan format:

- Svaki uređaj počinje u novom retku.
- **Dobavljač, Model i Serijski broj** moraju biti navedeni za svaki uređaj i odvojeni zarezom.

Slijedi primjer sadržaja tekstne datoteke:

 Kingston, DT 101 G2, 001CCE0DGRFC0371  
04081-0009432, USB2.0 HD WebCam, 20090101

**Izvezi** – Izvozi popis uređaja u datoteku.

Klikom na gumb **Ispuni** prikazat će se svi trenutačno povezani uređaji i sljedeće informacije o njima: vrsta uređaja, informacije o proizvođaču uređaja, model i serijski broj (ako je dostupan).

Kada završite s prilagodbom, kliknite **U redu**. Kliknite **Odustani** ako želite zatvoriti prozor **Grupe uređaja** bez spremanja promjena.

 Možete stvoriti više grupa uređaja na koje će se primijeniti različita pravila. Isto tako, možete stvoriti samo jednu grupu uređaja na koje će se primijeniti pravilo s akcijom **Čitaj/piši** ili **Samo čitaj**. Tako će svi uređaji koje kontrola uređaja ne prepoznaje biti blokirani prilikom povezivanja na vaše računalo.

Napominjemo da sve akcije (dopuštenja) nisu dostupne za sve vrste uređaja. Ako se radi o uređaju za pohranu, dostupne su sve četiri akcije. Za uređaje koji nisu za pohranu postoje samo tri akcije (npr. akcija **Samo za čitanje** nije dostupna za Bluetooth, što znači da je Bluetooth uređaje moguće samo dopustiti, blokirati ili upozoriti).

# Dodavanje pravila kontrole uređaja

Pravilo kontrole uređaja određuje akciju koja će se poduzeti kada se uređaj koji zadovoljava kriterije pravila priključi na računalo.

Uredi pravilo

Naziv	Rule
Pravilo aktivirano	<input checked="" type="checkbox"/>
Primjeni	Sve
Vrsta uređaja	Bluetooth uređaj
Dozvoljena radnja	Čitanje/pisanje
Vrsta uvjeta	Uredaj
Dobavljač	
Model	
Serijski broj	
Događaji koji će se bilježiti u dnevnik	Sve
Popis korisnika	Uredi
Obavijesti korisnika	<input checked="" type="checkbox"/>

**U redu**

Unesite opis pravila u polje **Naziv** radi bolje identifikacije. Odabir potvrđnog okvira uz značajku **Pravilo aktivirano** deaktivira ili aktivira to pravilo; to može biti korisno ako ne želite trajno izbrisati pravilo.

**Primjeni tijekom** – omogućuje vam da primijenite stvoreno pravilo tijekom određenog vremena. Iz padajućeg izbornika odaberite stvoreno vremensko razdoblje. Više informacija potražite [u vremenskim razdobljima](#).

## Vrsta uređaja

Odaberite vrstu vanjskog uređaja s padajućeg izbornika (Pohrana na disku/Prijenosni uređaj/Bluetooth/FireWire/...). Informacije o vrsti uređaja preuzimaju se iz operacijskog sustava i mogu se vidjeti u upravitelju uređaja sustava ako je uređaj priključen na računalo. Uređaji za pohranu obuhvaćaju vanjske diskove ili konvencionalne čitače memorijskih kartica povezane putem USB-a ili sučelja FireWire. Čitači pametnih kartica obuhvaćaju čitače pametnih kartica s ugrađenim električnim integriranim krugom, kao što su SIM kartice ili kartice za autorizaciju. Primjeri su uređaja za obradu slike skeneri i kamere. Budući da ti uređaji daju samo informacije o svojim akcijama, bez informacija o korisnicima, mogu se samo globalno blokirati.

**i** Funkcija popisa korisnika nije dostupna za vrstu modema. Pravilo će se primijeniti na sve korisnike i izbrisat će se trenutačan popis korisnika.

## Akcija

Pristup uređajima koji nisu za pohranu može biti dopušten ili blokiran. Za razliku od toga, pravila za uređaje za pohranu dopuštaju odabir jednog od sljedećih prava:

- **Čitaj/Piši** – Dopustit će se potpuni pristup uređaju.
- **Blokiraj** – Pristup uređaju će se blokirati.
- **Samo za čitanje** – Dopustit će se samo čitanje s uređaja.
- **Upozori** – Ako odaberete ovu opciju, korisnik će svaki put prilikom priključivanja uređaja primiti obavijest je li uređaj dopušten/blokiran i stvorit će se zapis u dnevniku. Uređaji neće ostati upamćeni, a obavijest će se prikazati i prilikom sljedećih pokušaja priključivanja istog uređaja.

Napominjemo da sve akcije (dopuštenja) nisu dostupne za sve vrste uređaja. Ako se radi o uređaju za pohranu, dostupne su sve četiri akcije. Za uređaje koji nisu za pohranu postoje samo tri akcije (npr. akcija **Samo za čitanje** nije dostupna za Bluetooth, što znači da je Bluetooth uređaje moguće samo dopustiti, blokirati ili upozoriti).

## Vrsta uvjeta

Odaberite **Grupa uređaja ili Uređaj**.

Pomoći ostalih parametara navedenih u nastavku pravila se mogu detaljno konfigurirati i prilagoditi uređajima. Nijedan parametar ne razlikuje velika i mala slova:

- **Proizvođač** – filtriraj prema nazivu proizvođača ili ID-u.
- **Model** – Naziv uređaja.
- **Serijski broj** – Vanjski uređaji obično imaju vlastite serijske brojeve. U slučaju CD-a/DVD-a to je serijski broj danog medija, a ne CD pogona.

**i** Ako ovi parametri nisu definirani, pravilo će pri određivanju podudaranja ignorirati ta polja. Parametri filtriranja u svim tekstnim poljima osjetljivi su na velika i mala slova te nisu dopušteni zamjenski znakovi (\*, ?).

**i** Da biste prikazali informacije o nekom uređaju, stvorite pravilo za tu vrstu uređaja, priključite uređaj na računalo i zatim provjerite detalje uređaja u [dnevniku kontrole uređaja](#).

## Minimalna opširnost zapisivanja

- **Uvijek** – Zapisuje sve događaje u dnevnik.
- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa.
- **Informativno** – Zapisuju se sve informativne poruke, uključujući poruke o uspešnoj nadogradnji, te svi prethodno navedeni zapisi.
- **Upozorenje** – Zapisuju se kritične pogreške i poruke s upozorenjima te se šalju na ERA Server.
- **Ništa** – neće se stvoriti dnevničici.

Moguće je ograničiti pravila na određene korisnike ili grupe korisnika tako da ih dodate na **Popis korisnika**:

- **Dodaj** – otvara **Vrste objekata**: korisnici ili grupe koji vam omogućuje odabir željenih korisnika.
- **Ukloni** – Uklanja odabranog korisnika iz filtra.

**i** Svi se uređaji ne mogu filtrirati prema korisničkim pravilima (primjerice, uređaji za obradu slike ne daju informacije o korisnicima, već samo o njihovim radnjama).

## Sistem za sprečavanje upada (HIPS)

**!** Samo bi iskusan korisnik trebao mijenjati HIPS postavke. Neispravno konfiguiranje HIPS postavki može uzrokovati nestabilnost sustava.

**Sistem za sprečavanje upada (HIPS)** štiti vaš sustav od zlonamjernog softvera i svake neželjene aktivnosti koja ima negativan učinak na sigurnost vašeg računala. HIPS koristi naprednu analizu ponašanja u kombinaciji s mogućnostima otkrivanja prijetnji u sklopu mrežnog filtriranja za nadzor procesa koji se izvršavaju, datoteka i ključeva registra. HIPS nije isto što i rezidentna zaštita, a nije ni firewall; on nadzire samo one procese koji se izvršavaju unutar operacijskog sustava.

HIPS postavke možete pronaći pod **Naprednim podešavanjem (F5) > Modul detekcije > HIPS > Osnovno**. Stanje HIPS-a (aktivirano/deaktivirano) prikazuje se u glavnom prozoru programa ESET Endpoint Antivirus, u oknu **Podešavanje > Računalo**.

The screenshot shows the 'Napredno podešavanje' (Advanced Settings) window of the ESET Endpoint Antivirus. On the left, there's a sidebar with navigation links: MODUL DETEKCIJE (selected), OSNOVNO, NADODRŽANJA, MREŽNA ZAŠTITA, WEB I E-POŠTA, KONTROLA UREĐAJA, ALATI, and KORISNIČKO SUČELJE. The main area has a search bar and a help icon. The 'OSNOVNO' tab is selected, showing the following settings:

Setting	Status	Action
Aktiviraj HIPS	Enabled (checkmark)	
Aktiviraj samozaštitu	Disabled (unchecked)	
Aktiviraj zaštićeni servis	Enabled (checkmark)	
Aktiviraj napredni skener memorije	Enabled (checkmark)	
Aktiviraj Sprječavanje ranjivosti	Enabled (checkmark)	

Below this are sections for 'DUBINSKI PREGLED PONAŠANJA' and 'ZAŠTITA OD RANSOMWAREA', each with a single setting and a 'Uredi' (Edit) button. At the bottom, there's a 'POSTAVKE HIPS-A' section with a 'Standardno' button, a blue 'U redu' (Ready) button, and a grey 'Odustani' (Cancel) button.

## Osnovno

**Aktiviraj HIPS** – HIPS je aktiviran prema standardnim postavkama u programu ESET Endpoint Antivirus. Isključivanjem HIPS-a deaktivirat će se i ostale funkcije HIPS-a, kao što je Sprječavanje ranjivosti.

**Aktiviraj samozaštitu** – ESET Endpoint Antivirus upotrebljava ugrađenu tehnologiju **samozaštite** kao dio HIPS-a da bi spriječio da zlonamjerni programi uzrokuju kvar vaše antivirusne i antispyware zaštite ili da je deaktiviraju. Samozaštita štiti ključne procese sustava i ESET-ove procese, ključeve registra i datoteke od neovlaštene upotrebe. ESET Management agent također je zaštićen ako se instalira.

**Aktiviraj zaštićeni servis** – omogućuje zaštitu za ESET-ovu uslugu (ekrn.exe). Kada je ova opcija aktivirana, usluga se pokreće kao zaštićeni proces sustava Windows radi obrane od napada zlonamjernih programa. Ova je opcija dostupna u sustavima Windows 8.1 i Windows 10.

**Aktiviraj napredni skener memorije** – Radi zajedno sa sprječavanjem ranjivosti radi bolje zaštite od zlonamjernih programa koji su osmišljeni tako da skrivanjem i šifriranjem izbjegavaju da ih otkriju programi za zaštitu od zlonamjernih programa. Napredni skener memorije aktiviran je prema standardnim postavkama. Pročitajte više o ovoj vrsti zaštite u [rječniku](#).

**Aktiviraj zaštitu od zloupotrebe** – Osmišljena je za ojačavanje zaštite često zloupotreblijavanih vrsta aplikacija kao što su web preglednici, PDF čitači, klijenti e-pošte i komponente sustava MS Office. Prema standardnim postavkama zaštita od zloupotrebe je aktivirana. Više o toj vrsti zaštite pročitajte u [rječniku](#).

## Dubinski pregled ponašanja

**Aktiviraj dubinski pregled ponašanja** – dodatan sloj zaštite u sklopu funkcije HIPS. Ova ekstenzija HIPS-a analizira ponašanje svih programa pokrenutih na računalu i upozorava vas ako je ponašanje nekog procesa zločudno.

[Izuzeci iz HIPS-ova dubinskog pregleda ponašanja](#) omogućuju izuzimanje procesa od analize. Da bi se osiguralo skeniranje mogućih prijetnji u svim procesima, preporučujemo stvaranje izuzetaka samo kada je to apsolutno nužno.

## Zaštita od ransomwarea

**Zaštita od ransomwarea** dodatni je sloj zaštite koji djeluje kao dio funkcije HIPS. Reputacijski sustav ESET LiveGrid® mora biti aktiviran da bi zaštita od ransomwarea djelovala. Više o toj vrsti zaštite [pročitajte ovdje](#).

**Aktiviraj Način rada za provjeru** – sve što otkrije Zaštita od ransomwarea neće se automatski blokirati, no [zapisat će se u dnevnik uz naznačenu ozbiljnost upozorenja](#) i poslat će se upravljačkoj konzoli s oznakom „NAČIN RADA ZA PROVJERU“. Administrator može izuzeti takvu otkrivenu prijetnju da bi se spriječilo daljnje otkrivanje ili je ostaviti aktivnom, što znači da će se blokirati i ukloniti nakon završetka Načina rada za provjeru. Aktivacija ili deaktivacija Načina rada za provjeru isto će se tako zapisivati u dnevnik programa ESET Endpoint Antivirus. Ova je opcija dostupna samo u uređivaču konfiguracije pravila u programima ESET PROTECT ili ESMC.

## Postavke HIPS-a

**Način filtriranja** može se izvesti na jedan od sljedećih načina:

Način filtriranja	Opis
<b>Automatski način rada</b>	Operacije su aktivirane, uz iznimku onih koje su blokirane putem unaprijed definiranih pravila koja štite vaš sustav.
<b>Pametni način rada</b>	Korisnik će biti obaviješten samo o vrlo sumnjivim događajima.
<b>Interaktivni način</b>	Korisnik će dobiti upit da potvrdi operacije.
<b>Način rada na temelju pravila</b>	blokira sve operacije koje nisu definirane određenim pravilom koje ih dopušta.
<b>Način rada za učenje</b>	Operacije su aktivirane i pravilo se stvara nakon svake operacije. Pravila stvorena u ovom načinu rada mogu se prikazati u <b>Uređivač HIPS pravila</b> , ali je njihov prioritet niži od prioriteta ručno stvorenih pravila ili pravila koja su stvorena u automatskom načinu rada. Ako s padajućeg izbornika <b>načina filtriranja</b> odaberete <b>način rada za učenje</b> , postavka <b>Način rada za učenje završava</b> za će postati dostupna. Odaberite vremensko razdoblje u kojem će način rada za učenje biti aktiviran, a maksimalno dostupno trajanje iznosi 14 dana. Po isteku unesenog trajanja od vas će biti zatraženo da uredite pravila stvorena pomoću značajke HIPS dok je bila u načinu rada za učenje. Još možete odabrat i drugi način filtriranja ili odgoditi donošenje odluke i nastaviti koristiti način rada za učenje.

**Način rada postavljen nakon isteka načina rada za učenje** – Odaberite način filtriranja koji će se upotrebljavati nakon što istekne način rada za učenje. Nakon isteka, opcija **Pitaj korisnika** zahtijeva administratorske ovlasti da bi provela promjenu u načinu filtriranja u HIPS-u.

HIPS sustav nadzire događaje unutar operacijskog sustava i reagira u skladu s pravilima koja su slična pravilima koja upotrebljava firewall. Kliknite **Uredi** pored opcije **Pravila** da biste otvorili uređivač **HIPS pravila**. U prozoru HIPS pravila možete odabrat, dodati, urediti ili ukloniti pravila. Pojedinosti o stvaranju pravila i HIPS operacijama možete pronaći u odjeljku [Uređivanje HIPS pravila](#).

## HIPS interaktivni prozor

HIPS prozor obavijesti dopušta stvaranje pravila na temelju novih radnji koje HIPS otkrije te zatim definiranje uvjeta pod kojima se ta radnja može dopustiti ili zabraniti.

Pravila koja su stvorena u prozoru obavijesti smatraju se jednakima pravilima koja su ručno stvorena. Pravilo stvoreno u prozoru obavijesti može biti manje određeno od pravila koje je pokrenulo taj prozor. To znači da nakon stvaranja pravila u prozoru ista operacija može pokrenuti isti prozor. Više informacija potražite u odjeljku [Prioritet za HIPS pravila](#).

Ako je standardna radnja pravila postavljena na **Pitaj svaki put**, prilikom svakog pokretanja tog pravila prikazuje se prozor. Možete zabraniti ili dopustiti operaciju pomoću stavki **Zabrani** ili **Dopusti**. Ako u zadanom vremenu ne odaberete radnju, nova se radnja odabire na temelju pravila.

**Nakon odabira mogućnosti Zapamti do zatvaranja aplikacije** dotična radnja (**Dopusti/Zabrani**) koristit će se sve dok se ne promijene pravila ili način filtriranja, nadogradi modul HIPS ili ponovno pokrene sustav. Poslije svake od tih triju radnji privremena se pravila brišu.

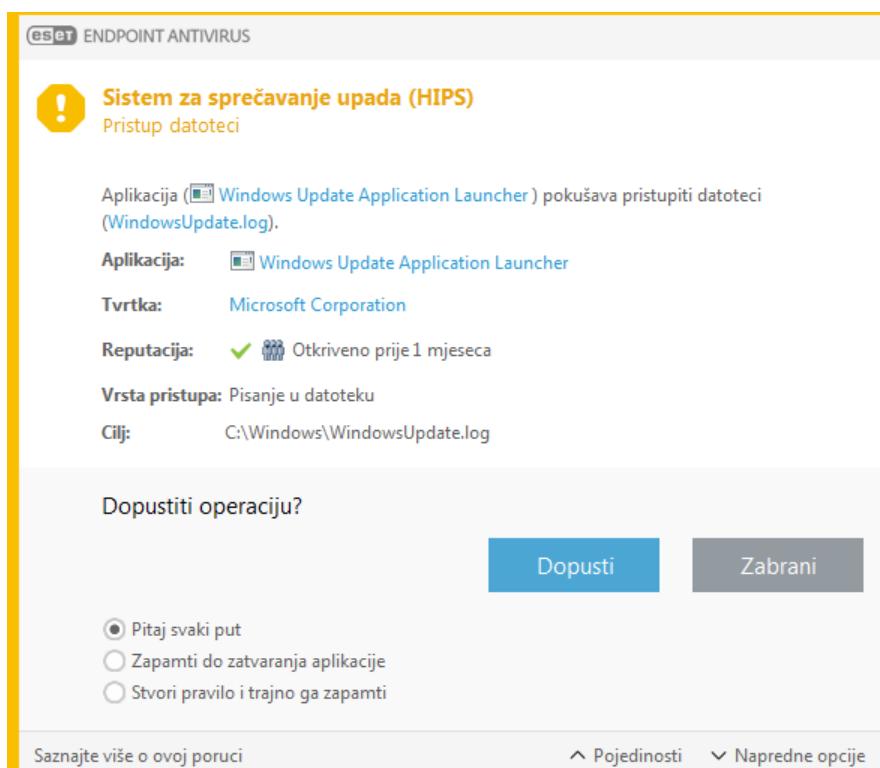
Opcija **Stvori pravilo i trajno ga zapamti** stvorit će novo HIPS pravilo koje se kasnije može mijenjati u odjeljku [HIPS upravljanje pravilima](#) (potrebne administratorske ovlasti).

Kliknite **Pojedinosti** na dnu da biste vidjeli koja aplikacija pokreće operaciju, kakva je reputacija datoteke ili za kakvu se operaciju traži dopuštenje ili zabrana.

Postavkama za detaljnije parametre pravila možete pristupiti tako da kliknete **Napredne opcije**. Opcije u nastavku bit će dostupne ako odaberete **Stvori pravilo i trajno ga zapamti**:

- **Stvori pravilo valjano samo za ovu aplikaciju** – Ako odznačite ovaj potvrđni okvir, pravilo će se stvoriti za sve izvorne aplikacije.
- **Samo za operaciju** – Odaberite operacije pravila za datoteku/aplikaciju/registar. [Pogledajte opise svih HIPS operacija](#).
- **Samo za objekt** – odaberite objekte pravila za datoteku/aplikaciju/registar.

**!** Da biste zaustavili pojavljivanje obavijesti, promijenite način filtriranja na **Automatski način rada u Naprednom podešavanju (F5) > Modul detekcije > HIPS > Osnovno**.



## Otkriveno je moguće ponašanje ransomwarea

Ovaj će se interaktivni prozor pojaviti kad se otkrije ponašanje potencijalnog ransomwarea. Možete zabraniti ili dopustiti operaciju pomoću stavki **Zabrani** ili **Dopusti**.

Kliknite **Pojedinosti** za prikaz određenih parametara otkrivanja. U ovom su vam prozoru dostupne opcije **Pošalji na analizu** ili **Izuzmi od skeniranja**.

**!** ESET LiveGrid® mora biti aktiviran kako bi [zaštita od ransomwarea](#) ispravno radila.

# HIPS upravljanje pravilima

Ovo je popis korisnički definiranih i automatski dodanih pravila u HIPS sustavu. Pojedinosti o stvaranju pravila i HIPS operacijama možete pronaći u poglavlju o [Postavkama HIPS pravila](#). Također pogledajte [Opći princip HIPS-a](#).

## Stupci

**Pravilo** – Korisnički definiran ili automatski odabran naziv pravila.

**Aktivirano** – Deaktivirajte ovu označku ako želite održati pravilo na popisu, ali ne i primijeniti ga.

**Radnja** – Pravilo određuje radnju – **Dopusti**, **Blokiraj** ili **Pitaj** – koja bi se trebala izvršiti ako su uvjeti odgovarajući.

**Izvori** – Pravilo će se koristiti samo ako događaj pokrenu aplikacije.

**Objekti** – Pravilo će se koristiti samo ako je operacija povezana s određenom datotekom, aplikacijom ili unosom u registar.

**Razina ozbiljnosti za vođenje dnevnika** – Ako aktivirate ovu opciju, informacije o ovom pravilu bit će zapisane u [HIPS dnevnik](#).

**Obavijesti** – U donjem desnom kutu prikazat će se mala skočna obavijest ako se pokrene događaj.

## Kontrolni elementi

**Dodaj** – Stvara novo pravilo.

**Uredi** – Omogućuje vam uređivanje odabranih unosa.

**Izbriši** – Uklanja odabrane unose.

## Prioriteti za HIPS pravila

Ne postoje opcije za podešavanje razine prioriteta HIPS pravila pomoću gumba vrh/dno.

- Sva pravila koja stvorite imaju isti prioritet
- Što je pravilo određenje, prioritet je viši (na primjer, pravilo za određenu aplikaciju ima viši prioritet od pravila za sve aplikacije)
- HIPS interno sadrži pravila višeg prioriteta kojima ne možete pristupiti (na primjer, ne možete nadjačati pravila definirana za Samozaštitu)
- Neće se primijeniti pravilo koje stvorite, a koje može zamrznuti operacijski sustav (imat će najniži prioritet)

## Postavke HIPS pravila

Najprije pogledajte [upravljanje HIPS pravilima](#).

**Naziv pravila** – Korisnički definiran ili automatski odabran naziv pravila.

**Radnja** – Specificira radnju – Dopusti, Blokiraj ili Pitaj – koja će se provesti ako se zadovolje uvjeti.

**Operacije na koje se pravilo odnosi** – Morate odabratи vrstu operacije na koje ћe se pravilo primijeniti. Pravilo ћe se koristiti samo za tu vrstu operacije i za odabrani cilj.

**Aktivirano** – Poništite odabir ovog potvrđnog okvira ako pravilo želite zadržati na popisu, no ne želite ga koristiti.

**Razina ozbiljnosti za vođenje dnevnika** – Ako aktivirate ovu opciju, informacije o ovom pravilu bit ћe zapisane u [HIPS dnevnik](#).

**Obavijesti korisnika** – U donjem desnom kutu prikazat ћe se mali skočni prozor ako se pokrene događaj.

Pravilo se sastoji od tri dijela koji opisuju uvjete koji pokreću to pravilo:

**Izvorne aplikacije** – Pravilo ћe se upotrebljavati samo ako je događaj pokrenula ova aplikacija/aplikacije. S padajućeg izbornika odaberite **Specifične aplikacije** i kliknite **Dodaj** ako želite dodati nove datoteke ili s padajućeg izbornika odaberite **Sve aplikacije** ako želite dodati sve aplikacije.

**Ciljne datoteke** – Pravilo ћe se upotrebljavati samo ako se operacija odnosi na taj objekt. S padajućeg izbornika odaberite **Specifične datoteke** i kliknite **Dodaj** ako želite dodati nove datoteke ili mape ili s padajućeg izbornika odaberite **Sve datoteke** ako želite dodati sve datoteke.

**Aplikacije** – Pravilo ћe se koristiti samo ako se operacija odnosi na taj objekt. S padajućeg izbornika odaberite **specifične aplikacije** i kliknite **Dodaj** ako želite dodati nove datoteke ili mape ili s padajućeg izbornika odaberite **sve aplikacije** ako želite dodati sve aplikacije.

**Unosi u registar** – Pravilo ћe se koristiti samo ako se operacija odnosi na taj objekt. S padajućeg izbornika odaberite **specifične unose** i kliknite **Dodaj** ako želite dodati nove datoteke ili mape ili s padajućeg izbornika odaberite **svi unosi** ako želite dodati sve aplikacije.

**i** Neke operacije specifičnih pravila koje su unaprijed definirane značajkom HIPS ne mogu se blokirati i dopuštene su prema standardnim postavkama. Nadalje, HIPS ne nadzire sve operacije sustava. HIPS nadzire operacije koje se mogu smatrati nesigurnima.

**i** Pri navođenju puta C:\example utječe na radnje sa samom mapom, a C:\example\*.\* utječe na datoteke u mapi.

## Operacije aplikacija

- Ukloni pogreške druge aplikacije** – Prilaganje programa za uklanjanje pogrešaka u proces. Tijekom uklanjanja pogrešaka aplikacije mnoge pojedinosti tog ponašanja mogu se pregledati i izmijeniti te se može pristupiti podacima.
- Presretni događaje iz druge aplikacije** – Izvorna aplikacija pokušava uhvatiti događaje koji su usmjereni na određenu aplikaciju (na primjer, keylogger koji pokušava zabilježiti događaje preglednika).
- Zatvori/obustavi drugu aplikaciju** – Obustava, nastavak ili zatvaranje procesa (izravan pristup moguć iz značajke Process Explorer ili okna Procesi).
- Pokreni novu aplikaciju** – Pokretanje novih aplikacija ili procesa.
- Preinači stanje druge aplikacije** – Izvorna aplikacija pokušava zapisivati u memoriju ciljanih aplikacija ili u

njihovo ime pokrenuti kôd. Ta funkcija može biti korisna za zaštitu ključne aplikacije koje se mogu konfigurirati kao ciljne aplikacije u pravilu koje blokira korištenje te operacije.

**i** Nije moguće presretanje operacija procesa na 64-bitnoj verziji sustava Windows XP.

## Operacije registra

- **Preinači postavke pokretanja** – Bilo koja promjena postavki koja definira koje će se aplikacije pokrenuti prilikom pokretanja sustava Windows. One se mogu pronaći ako se, na primjer, potraži ključ Run u registru sustava Windows.
- **Izбриши iz registra** – Brisanje ključa registra ili njegove vrijednosti.
- **Promijeni naziv ključa registra** – Mjenja naziv ključeva registra.
- **Izmijeni registar** – Stvaranje novih vrijednosti ključeva registra, promjena postojećih vrijednosti, premještanje podataka na stablu baze podataka ili postavljanje korisničkih ili grupnih prava za ključeve registra.

### Upotreba zamjenskih znakova u pravilima

Zvjezdica u pravilima može se upotrijebiti isključivo za zamjenu određenog ključa, npr.

"HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\\*\Start". Ostali načini upotrebe zamjenskih znakova nisu podržani.

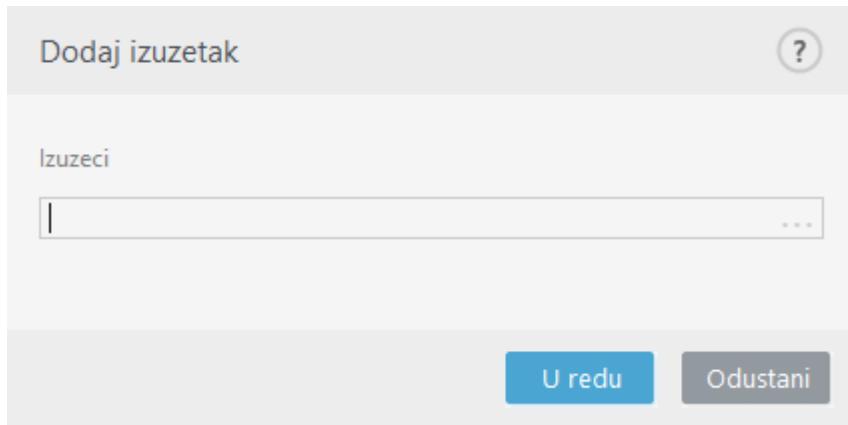
### **i** Stvaranje pravila koja se odnose na ključ HKEY\_CURRENT\_USER

Ovaj je ključ samo link za odgovarajući potključ HKEY\_USERS koji je specifičan za korisnika koji se identificira SID-om (sigurnim identifikatorom). Da bi se stvorilo pravilo samo za trenutačnog korisnika, umjesto upotrebe puta do HKEY\_CURRENT\_USER upotrijebite put do HKEY\_USERS%\%SID%. Za SID možete upotrijebiti zvjezdicu da bi se pravilo primijenilo na sve korisnike.

**A** Ako stvorite preopćenito pravilo, prikazat će se upozorenje za tu vrstu pravila.

U sljedećem primjeru pokazat ćemo kako ograničiti neželjeno ponašanje određene aplikacije:

- 1.Unesite naziv pravila i odaberite **Blokiraj** (ili **Pitaj** ako želite odabrati kasnije) s padajućeg izbornika **Radnja**.
- 2.Aktivirajte potvrđni okvir **Obavijesti korisnika** da bi se pri svakoj primjeni pravila prikazala obavijest.
- 3.Odaberite barem jednu operaciju u odjeljku **Operacije koje utječu na sljedeće objekte** na koje će se primjenjivati pravilo.
- 4.Kliknite **Dalje**.
- 5.U prozoru **Izvorene aplikacije** na padajućem izborniku odaberite **Određene aplikacije** kako biste novo pravilo primijenili na sve aplikacije koje pokušavaju izvršiti bilo koju od odabranih operacija aplikacije na aplikacijama koje ste odredili.
- 6.Kliknite **Dodaj** i zatim ... da biste odabrali put do određene aplikacije i zatim pritisnite **U redu**. Dodajte više aplikacija ako želite.  
Na primjer: *C:\Program Files (x86)\Untrusted application\application.exe*
- 7.Odaberite operaciju **Pisanje u datoteku**.
- 8.Odaberite **Sve datoteke** u padajućem izborniku. Time ćete blokirati sve pokušaje aplikacija odabranih u prethodnom koraku da pišu u bilo koje datoteke.
- 9.Kliknite **Završi** da biste spremili novo pravilo.



## HIPS napredno podešavanje

Sljedeće mogućnosti korisne su za uklanjanje pogrešaka i analizu ponašanja aplikacije:

**Upravljački programi uvijek se smiju učitati** – Odabrani se upravljački programi uvijek smiju učitati, neovisno o konfiguiranom filterskom načinu, osim ako su izričito blokirani korisničkim pravilom.

**Zabilježi sve blokirane operacije** – Sve blokirane operacije zapisat će se u HIPS dnevnik.

**Obavijesti prilikom promjena u aplikacijama pokretanja** – Prikazuje obavijest na radnoj površini prilikom svakog dodavanja ili uklanjanja aplikacije iz pokretanja sustava.

## Upravljački programi koji se uvijek smiju učitati

Upravljački programi s ovog popisa uvijek se smiju učitati, neovisno o HIPS filterskom načinu, osim ako su izričito blokirani korisničkim pravilom.

**Dodaj** – Dodaje novi upravljački pogon.

**Uredi** – Uređuje odabrani upravljački pogon.

**Ukloni** – Uklanja upravljački pogon s popisa.

**Poništi** – Ponovno učitava skup upravljačkih programa sustava.

**i** Kliknite **Ponovno postavi** ako ne želite uključiti upravljačke programe koje ste dodali ručno. To može biti korisno ako ste dodali nekoliko upravljačkih programa i ne možete ih ručno izbrisati s popisa.

## Način rada za prezentacije

Način rada za prezentacije značajka je za korisnike koji softver žele koristiti bez prekida, ne žele biti ometani skočnim prozorima te žele smanjiti korištenje CPU-a. Način rada za prezentacije može se koristiti i tijekom prezentacija koje se ne smiju prekidati antivirusnim aktivnostima. Kad je omogućen, način deaktivira sve skočne prozore i ne pokreće planirane zadatke. Zaštita sustava i dalje se izvodi u pozadini, no ne zahtijeva nikakvu aktivnost korisnika.

Kliknite **Podešavanje > Računalo**, a zatim kliknite prekidač uz **Način rada za prezentacije kako biste ručno**

omogućili način rada za prezentacije. U Naprednom podešavanju (F5) kliknite **Alati > Način rada za prezentacije**, a zatim kliknite prekidač uz **Automatski aktiviraj način rada za prezentacije prilikom izvršavanja aplikacija preko cijelog zaslona** kako bi ESET Endpoint Antivirus automatski uključio način rada za prezentacije kada se pokrenu aplikacije preko cijelog zaslona. Aktiviranje načina rada za prezentacije predstavlja mogući sigurnosni rizik pa će ikona statusa zaštite na programskoj traci postati narančasta i prikazat će se upozorenje. To upozorenje vidjet ćete i u glavnom prozoru programa u kojem će stavka **Način rada za prezentacije je aktiviran** biti označena narančastom bojom.

Kada odaberete mogućnost **Automatski aktiviraj način rada za prezentacije prilikom izvršavanja aplikacija preko cijelog zaslona**, način rada za prezentacije pokrenut će se svaki put kada pokrenete aplikaciju na cijelom zaslonu i automatski će se prekinuti nakon što zatvorite aplikaciju. To je osobito korisno za pokretanje načina rada za prezentacije odmah nakon pokretanja igre, otvaranja aplikacije na cijelom zaslonu ili pokretanja prezentacije.

Možete odabrati i stavku **Automatski deaktiviraj način rada za prezentacije nakon** da biste definirali nakon koliko će se minuta način rada za prezentacije automatski deaktivirati.

## Skeniranje pri pokretanju

Prema standardnoj postavci, automatska provjera datoteka pri pokretanju sustava izvršit će se prilikom pokretanja sustava i tijekom aktualizacije modula. To skeniranje ovisi o mogućnosti [Konfiguracija i zadaci planera](#).

Mogućnosti skeniranja pri pokretanju spadaju pod zadatak planera **Provjera datoteke za pokretanje sustava**. Da biste promijenili postavke skeniranja pri pokretanju, u odjelu **Alati > Planer** kliknite stavku **Automatska provjera pokretačke datoteke**, a zatim kliknite **Uredi**. U zadnjem koraku prikazat će se prozor [Automatska provjera pokretačkih datoteka](#) (dodatne pojedinosti potražite u sljedećem poglavljju).

Detaljne upute o stvaranju i upravljanju zadacima planera potražite u odjelu [Stvaranje novih zadataka](#).

## Automatska provjera pokretačke datoteke

Pri stvaranju planiranog zadatka Provjera datoteke za pokretanje sustava imate nekoliko mogućnosti za prilagodbu sljedećih parametara:

Na padajućem izborniku **Cilj skeniranja** navedena je dubina skeniranja datoteka koje se pokreću prilikom pokretanja sustava na temelju tajnog i složenog algoritma. Datoteke su sortirane silazno prema sljedećim kriterijima:

- **Sve registrirane datoteke** (najviše datoteka za skeniranje)
- **Rijetko korištene datoteke**
- **Redovito korištene datoteke**
- **Često korištene datoteke**
- **Samo najčešće korištene datoteke** (najmanje datoteka za skeniranja)

Obuhvaćene su i dvije određene grupe:

- **Datoteke pokrenute prije prijave korisnika** – Sadrži datoteke s mjesta kojima je moguće pristupiti bez

prijave korisnika (obuhvaća gotovo sva mesta za pokretanje kao što su servisi, pomoćni objekti preglednika, obavijesti procesa Winlogon, stavke planera sustava Windows, poznati dll-ovi itd).

- **Datoteke pokrenute nakon prijave korisnika** – Sadrži datoteke s mesta kojima je moguće pristupiti samo nakon prijave korisnika (obuhvaća datoteke koje su pokrenute samo za određenog korisnika, obično datoteke u direktoriju `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

Popis datoteka koje treba skenirati fiksan je za svaku spomenutu grupu.

**Prioritet provjere** – Razina prioriteta pomoću koje se određuje kada započeti skeniranje:

- **Dok miruje** – zadatak će se izvršiti samo kad sustav miruje.
- **Najniža** – kad je opterećenje sustava najniže moguće,
- **Niže** – kada je opterećenje sustava nisko,
- **Uobičajeno** – kada je opterećenje sustava uobičajeno.

## Zaštita dokumenata

Značajka Zaštita dokumenata skenira dokumente sustava Microsoft Office prije otvaranja, kao i datoteke koje automatski preuzima preglednik Internet Explorer, kao što su Microsoft ActiveX elementi. Zaštita dokumenta osigurava dodatni sloj zaštite rezidentnoj zaštiti i može se deaktivirati radi poboljšanja učinkovitosti u sustavima koji ne upravljaju velikim brojem dokumenata sustava Microsoft Office.

Da biste aktivirali zaštitu dokumenata, otvorite prozor **Napredno podešavanje** (pritisnite F5) > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Zaštita dokumenata** i kliknite **Aktiviranje zaštite dokumenata**.



Tu funkciju aktiviraju aplikacije koje upotrebljavaju Microsoft Antivirus API (npr. sustav Microsoft Office 2000 i novije verzije ili preglednik Microsoft Internet Explorer 5.0 i novije verzije).

## Izuzeci

**Izuzeci** vam omogućuju izuzimanje [objekata](#) od modula detekcije. Da bi se osiguralo skeniranje svih objekata, preporučujemo stvaranje izuzetaka samo kada je to apsolutno nužno. Međutim, postoje situacije kada ćete morati izuzeti objekt i, primjerice, skenirati velike unose u bazi podataka koji bi računalo usporili tijekom skeniranja ili softver čije skeniranje dovodi do sukoba.

[Izuzeci radi poboljšanja performansi](#) omogućuju vam izuzimanje datoteka i mapa od skeniranja. Izuzeci radi poboljšanja performansi korisni su za izuzimanje skeniranja aplikacija za igranje na razini datoteke ili kada uzrokuju nenormalno ponašanje sustava ili radi poboljšanja performansi.

[Izuzeci detekcija poznatih prijetnji](#) omogućuju vam izuzimanje objekata iz čišćenja pomoću naziva prijetnje, puta ili hasha. Izuzeci detekcija poznatih prijetnji ne izuzimaju datoteke i mape iz skeniranja kao Izuzetke radi poboljšanja performansi. Izuzeci detekcija poznatih prijetnji izuzimaju objekte samo kada ih otkrije modul detekcije i kad se na popisu izuzetaka nalazi odgovarajuće pravilo.

Kod [izuzetaka u verziji 7.1 i starijim verzijama](#) Izuzeci radi poboljšanja performansi i Izuzeci detekcija poznatih prijetnji spojeni su u jedno.

Ne smiju se pomiješati s drugim vrstama izuzetaka:

- [Izuzeci procesa](#) – Sve operacije s datotekama pripisane izuzetim procesima aplikacija izuzimaju se iz skeniranja (možda će biti potrebno poboljšanje brzine sigurnosnog kopiranja i dostupnosti usluge).
- [Izuzete ekstenzije datoteka](#)
- [Izuzeci iz HIPS-a](#)
- [Filtar izuzetaka za zaštitu na bazi clouda](#)

## Izuzeci radi poboljšanja performansi

Izuzeci radi poboljšanja performansi omogućuju vam izuzimanje datoteka i mapa od skeniranja.

Da bi se osiguralo traženje prijetnji u svim objektima, preporučujemo stvaranje izuzetaka radi poboljšanja performansi samo kada je to apsolutno nužno. Međutim, postoje situacije kada ćete morati izuzeti objekt, primjerice, velike unose u bazi podataka koji bi računalo usporili tijekom skeniranja ili softver čije skeniranje dovodi do sukoba.

Datoteke i mape koje će se izuzeti iz skeniranja možete dodati na popis izuzetaka putem stavke **Napredno podešavanje (F5) > Modul detekcije > Izuzeci > Izuzeci radi poboljšanja performansi > Uredi**.

Da biste [izuzeli objekt](#) (put: datoteka ili mapa) iz skeniranja, kliknite **Dodaj** i unesite odgovarajući put ili ga odaberite u stablastoj strukturi.

Izuzeci radi poboljšanja performansi

Izuzmi put	Komentar
C:\Backup\*	
C:\pagefile.sys	

Dodaj Uredi Izbrisati Uvezi Izvezi Odustani

**i** Modul za **rezidentnu zaštitu** ili modul za **skeniranje računala** neće otkriti prijetnju u datoteci ako datoteka zadovoljava kriterije za izuzimanje od skeniranja.

## Kontrolni elementi

- **Dodaj** – dodajte novu stavku za izuzimanje objekata od skeniranja.
- **Uredi** – Omogućuje vam uređivanje odabranih unosa.
- **Ukloni** – uklanja odabrane unose (CTRL + klik za odabir više unosa).
- **Uvezi/izvezi** – uvoz i izvoz izuzetaka radi poboljšanja performansi korisni su ako trebate izraditi sigurnosnu kopiju trenutačnih izuzetaka da biste ih mogli upotrebljavati kasnije. Opcija izvoza postavki je praktična i za korisnike u neupravljenim okruženjima koji žele upotrebljavati svoju preferiranu konfiguraciju na više sustava – oni mogu jednostavno uvesti .txt datoteku za prijenos tih postavki.  
[Prikaz primjera formata datoteke za uvoz/izvoz](#)

```
# {"product": "endpoint", "version": "7.2.2055", "path": "plugins.01000600.settings.PerformanceExclusions", "columns": ["Path", "Description"]}
```

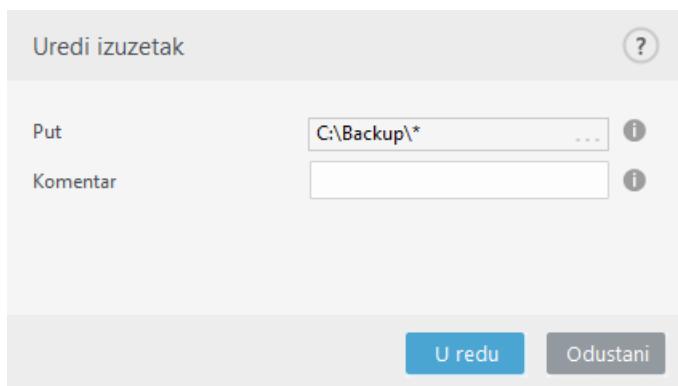
C:\Backup\\*,custom comment

C:\pagefile.sys

## Dodavanje ili uređivanje izuzetka radi poboljšanja performansi

U ovom dijaloškom prozoru izuzima se određeni put (datoteka ili mapa) za ovo računalo.

**i** Odaberite odgovarajući put tako da kliknete ... u polju Put.  
Kada unosite ručno, više [primjera formata izuzetaka](#) nalazi se u nastavku.



---

Možete upotrijebiti zamjenske znakove da biste izuzeli grupu datoteka. Upitnik (?) predstavlja jedan znak, a zvjezdica (\*) znakovni niz od nula ili više znakova.

- Ako želite izuzeti sve datoteke i podmape u mapi, upišite put do mape i upotrijebite masku \*.
- Ako želite izuzeti samo datoteke s ekstenzijom doc, upotrijebite masku \*.doc.
- Ako se naziv izvršne datoteke sastoji od određenog broja znakova (koji se međusobno razlikuju) i sigurni ste samo u prvi znak (primjerice "D"), upotrijebite sljedeći format:  
*D????.exe* (upitnici zamjenjuju znakove koji nedostaju ili znakove koji su nepoznati)

Primjeri:

- ✓ • *C:\Tools\\** – Put mora završiti obrnutom kosom crtom (\) i zvjezdicom (\*) da bi se naznačilo da se radi o mapi te da će se sav sadržaj u mapi (datoteke i podmape) izuzeti.
- *C:\Tools\\*.\** – Isto ponašanje kao *C:\Tools\\**
- *C:\Tools* – Mapa *Tools* neće biti izuzeta. Iz perspektive skenera, *Tools* može biti i naziv datoteke.
- *C:\Tools\\*.dat* – Izuzet će se .dat datoteke u mapi *Tools*.
- *C:\Tools\sg.dat* – Izuzet će se ova specifična datoteka koja se nalazi na točno tom putu.

Za definiranje izuzetaka od skeniranja možete upotrijebiti varijable sustava, primjerice %PROGRAMFILES%.

- Da biste izuzeli mapu Programske datoteke pomoću ove varijable sustava, upotrijebite put %PROGRAMFILES%\\* (zapamtite dodati obrnutu kosu crtu I zvjezdicu na kraju puta) prilikom dodavanja izuzetaka.
- Da biste izuzeli sve datoteke i mape u podmapi %PROGRAMFILES%, upotrijebite put %PROGRAMFILES%\Excluded\_Directory\\*

#### Proširivanje popisa podržanih varijabla sustava

Sljedeće se varijable mogu upotrebljavati u formatu izuzetaka puta:

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Varijable sustava specifične za korisnika (primjerice %TEMP% ili %USERPROFILE%) ili varijable okruženja (primjerice %PATH%) nisu podržane.

Upotreba zamjenskih znakova u sredini puta (na primjer, *C:\Tools\\*\Data\file.dat*) može funkcionirati, ali nije službeno podržana za izuzetke radi poboljšanja performansi. Pročitajte sljedeći [članak iz baze znanja](#) za više informacija.

Nema ograničenja upotrebe zamjenskih znakova usred puta kad upotrebljavate [izuzetke detekcija poznatih prijetnji](#).

Redoslijed izuzimanja:

- Ne postoje opcije za podešavanje razine prioriteta izuzetaka pomoću gumba vrh/dno.
- ✓ • Kada se prvo primjenjivo pravilo podudara sa skenerom, drugo se primjenjivo pravilo neće procjenjivati.
- Što je manje pravila, to će performanse skeniranja biti bolje.
- Izbjegavajte stvaranje istovremenih pravila.

## Format izuzetaka puta

Možete upotrijebiti zamjenske znakove da biste izuzeli grupu datoteka. Upitnik (?) predstavlja jedan znak, a zvjezdica (\*) znakovni niz od nula ili više znakova.

- Ako želite izuzeti sve datoteke i podmape u mapi, upišite put do mape i upotrijebite masku \*.
- Ako želite izuzeti samo datoteke s ekstenzijom doc, upotrijebite masku \*.doc.
- Ako se naziv izvršne datoteke sastoji od određenog broja znakova (koji se međusobno razlikuju) i sigurni ste samo u prvi znak (primjerice "D"), upotrijebite sljedeći format:  
*D????.exe* (upitnici zamjenjuju znakove koji nedostaju ili znakove koji su nepoznati)

Primjeri:

- C:\Tools\\* – Put mora završiti obrnutom kosom crtom (\) i zvjezdicom (\*) da bi se naznačilo da se radi o mapi te da će se sav sadržaj u mapi (datoteke i podmape) izuzeti.
- C:\Tools\\*.\* – Isto ponašanje kao C:\Tools\\*.
- C:\Tools – Mapa Tools neće biti izuzeta. Iz perspektive skenera, Tools može biti i naziv datoteke.
- C:\Tools\\*.dat – Izuzet će se .dat datoteke u mapi Tools.
- C:\Tools\sg.dat – Izuzet će se ova specifična datoteka koja se nalazi na točno tom putu.

Za definiranje izuzetaka od skeniranja možete upotrijebiti varijable sustava, primjerice %PROGRAMFILES%.

- Da biste izuzeli mapu Programske datoteke pomoću ove varijable sustava, upotrijebite put %PROGRAMFILES%\\* (zapamtite dodati obrnutu kosu crtu I zvjezdicu na kraju puta) prilikom dodavanja izuzetaka.
- Da biste izuzeli sve datoteke i mape u podmapi %PROGRAMFILES%, upotrijebite put %PROGRAMFILES%\Excluded\_Directory\\*

#### [Proširivanje popisa podržanih varijabla sustava](#)

Sljedeće se varijable mogu upotrebljavati u formatu izuzetaka puta:

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Varijable sustava specifične za korisnika (primjerice %TEMP% ili %USERPROFILE%) ili varijable okruženja (primjerice %PATH%) nisu podržane.

## Izuzeci detekcija poznatih prijetnji

Izuzeci detekcija poznatih prijetnji omogućuju vam da izuzmete objekte iz [čišćenja](#) filtriranjem naziva prijetnje, puta objekta ili hasha.

Izuzeci detekcija poznatih prijetnji ne izuzimaju datoteke i mape iz skeniranja kao [Izuzetke radi poboljšanja performansi](#). Izuzeci detekcija poznatih prijetnji izuzimaju objekte samo kada ih otkrije modul detekcije i kad se na popisu izuzetaka nalazi odgovarajuće pravilo.

Na (pogledajte prvi red na slici u nastavku), kad se objekt otkrije kao Win32/Adware.Optmedia i otkrivena je datoteka C:\Recovery\file.exe. U drugom redu svaka datoteka koja ima odgovarajući hash SHA-1 uvijek će biti izuzeta, bez obzira na naziv prijetnje.

Izuzeci detekcija poznatih prijetnji

Kriteriji za objekte	Izuzmi otkrivanje	Komentar
C:\Recovery\*.* 2723cb8ca015209528d3fbddcaa801124f4f40ad4	Win32/Adware.Optmedia <i>Sve otkrivene prijetnje</i>	SuperApi.exe

**Dodaj** **Uredi** **Izbriši** **Uvezi** **Izvezi**

**U redu** **Odustani**

Kako bi se osiguralo otkrivanje svih prijetnji, preporučujemo stvaranje izuzetih otkrivenih prijetnji samo kada je to nužno.

Datoteke i mape možete dodati na popis izuzetaka putem stavke **Napredno podešavanje (F5) > Modul detekcije > Izuzeci > Izuzeci detekcija poznatih prijetnji > Uredi**.

Da biste [izuzeli objekt \(prema nazivu prijetnje ili hashu\)](#) od čišćenja, kliknite **Dodaj**.

Izuzetak prema nazivu prijetnje za [potencijalno nepoželjne aplikacije](#) i [potencijalno nesigurne aplikacije](#) može se stvoriti i na sljedeće načine:

- U prozoru s upozorenjem koji prikazuje prijetnju (kliknite **Prikaži napredne opcije**, a zatim odaberite **Izuzmi od otkrivanja**).
- U kontekstnom izborniku dnevnika odaberite [Čarobnjak za stvaranje izuzetih detekcija poznatih prijetnji](#).
- Kliknite na **Alati > Karantena**, a potom desnom tipkom miša kliknite datoteku u karanteni te odaberite stavku **Vrati i izuzmi od skeniranja** u kontekstnom izborniku.

## Kriteriji za objekte koji su izuzete otkrivene prijetnje

- **Put** – Ograničavanje izuzetih otkrivenih prijetnji na određeni put (ili više njih).
- **Naziv prijetnje** – ako je pored izuzete datoteke naziv [prijetnje](#), to znači da datoteka nije izuzeta u potpunosti, već samo za tu prijetnju. Ako ta datoteka kasnije bude zaražena nekom drugom vrstom zlonamjernog programa, to će se otkriti.
- **Hash** – izuzima datoteku na temelju navedenog hasha SHA-1, bez obzira na vrstu, lokaciju, naziv ili ekstenziju datoteke.

## Kontrolni elementi

- **Dodaj** – dodajte novu stavku za izuzimanje objekata od čišćenja.
- **Uredi** – Omogućuje vam uređivanje odabralih unosa.
- **Ukloni** – uklanja odabrane unose (CTRL + klik za odabir više unosa).
- **Uvezi/izvezi** – uvoz i izvoz izuzetih prijetnji korisni su ako trebate izraditi sigurnosnu kopiju trenutačnih izuzetaka da biste ih mogli upotrebljavati kasnije. Opcija izvoza postavki je praktična i za korisnike u neupravljenim okruženjima koji žele upotrebljavati svoju preferiranu konfiguraciju na više sustava – oni mogu jednostavno uvesti .txt datoteku za prijenos tih postavki.

[Prikaz primjera formata datoteke za uvoz/izvoz](#)

```
# {"product": "endpoint", "version": "7.2.2055", "path": "Settings.ExclusionsManagement.DetectionExclusions", "columns": ["Id", "Path", "ThreatName", "Description", "FileHash"]}
```

```
4c59cd02-357c-4b20-a0ac-  
ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF
```

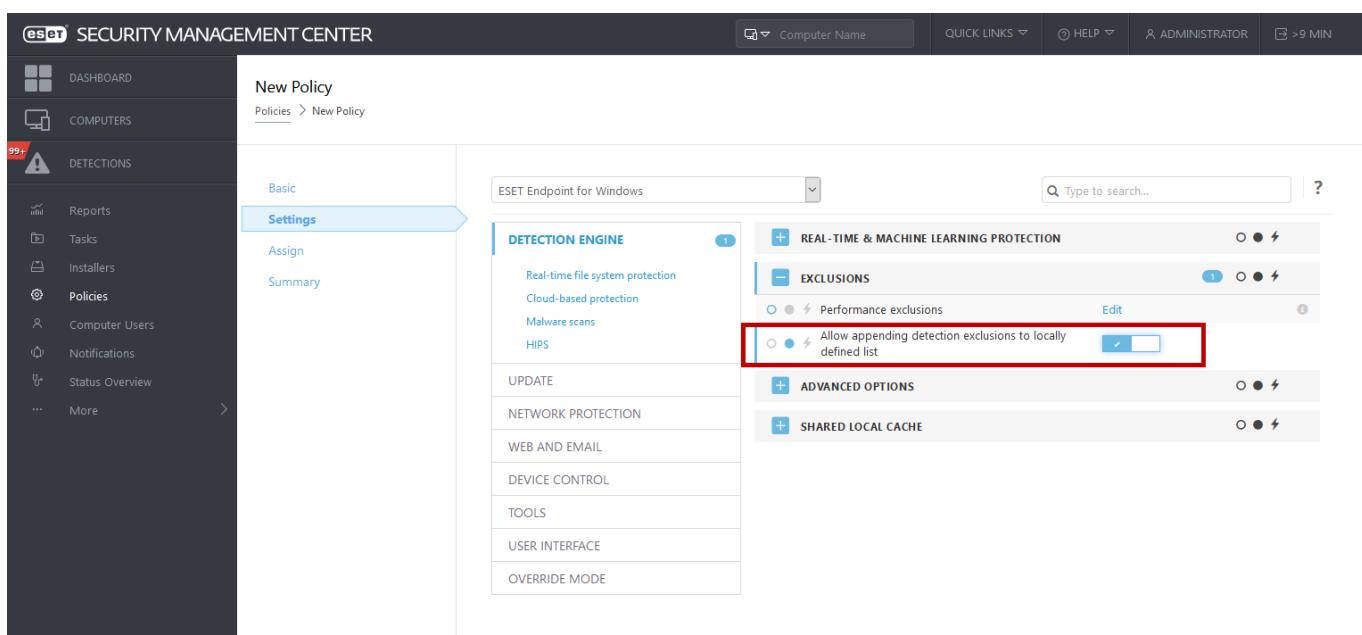
```
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,,
```

## Podešavanje izuzetih otkrivenih prijetnji u programu ESET PROTECT

ESMC 7.1 i ESET PROTECT 8.0 sadrži [novog čarobnjaka za upravljanje izuzecima detekcija poznatih prijetnji](#) – stvorite izuzetak detekcije poznatih prijetnji i primijenite ga na više računala/grupa.

### Moguće nadjačavanje izuzetih otkrivenih prijetnji iz programa ESET PROTECT

Kada postoji lokalni popis izuzetih otkrivenih prijetnji, administrator mora primijeniti pravilo pomoću opcije **Dopusti dodavanje izuzetih otkrivenih prijetnji na lokalno definirane popise**. Nakon toga, dodavanje izuzetih otkrivenih prijetnji iz programa ESET PROTECT radit će kako je predviđeno.

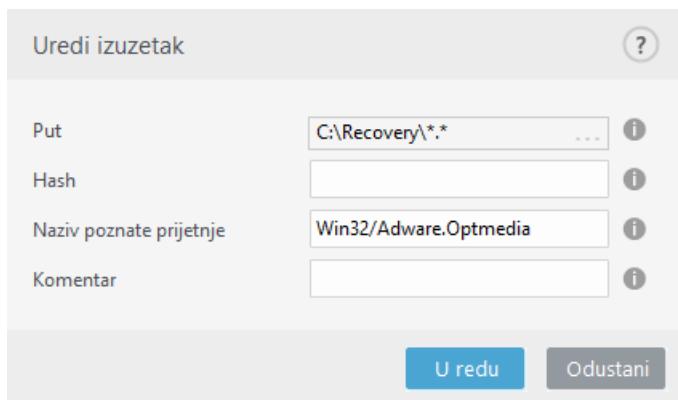


# Dodavanje ili uređivanje izuzetih detekcija poznatih prijetnji

## Izuzmi otkrivanje

Potrebno je navesti valjani naziv ESET-ove prijetnje. Za valjani naziv prijetnje pogledajte [dnevnike](#) i odaberite **Otkrivene prijetnje** putem padajućeg izbornika dnevnika. To je korisno kada ESET Endpoint Antivirus kao prijetnju otkriva [neispravno identificirani uzorak](#). Izuzimanje stvarnih infiltracija vrlo je opasno, pa možete izuzeti samo zahvaćene datoteke/mape tako da kliknete ... u polju **Maska puta** i/ili ih samo privremeno izuzeti. Izuzeci se primjenjuju i na [potencijalno nepoželjne aplikacije](#), potencijalno nesigurne aplikacije i sumnjive aplikacije.

Također pogledajte [Format izuzetaka puta](#).



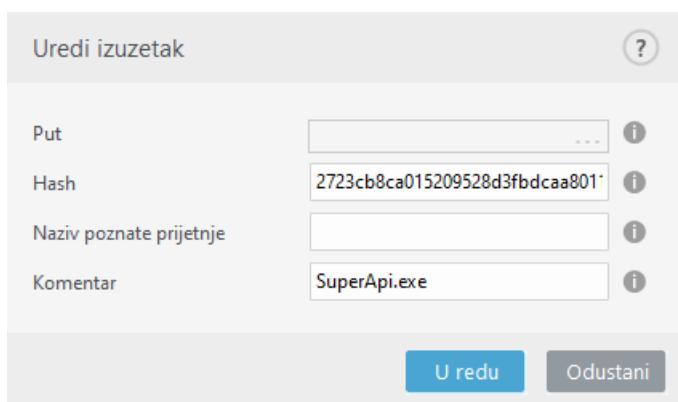
Put	C:\Recovery\*.*	...	i
Hash			i
Naziv poznate prijetnje	Win32/Adware.Optmedia		i
Komentar			i

**U redu** **Odustani**

Pogledajte [primjer izuzetih detekcija poznatih prijetnji](#) u nastavku.

## Izuzmi hash

Izuzima datoteku na temelju navedenog hasha SHA-1, bez obzira na vrstu, lokaciju, naziv ili ekstenziju datoteke.



Put		...	i
Hash	2723cb8ca015209528d3fbdcdaa801		i
Naziv poznate prijetnje			i
Komentar	SuperApi.exe		i

**U redu** **Odustani**

Da biste izuzeli određenu prijetnju prema nazivu, unesite valjani naziv otkrivene prijetnje:  
*Win32/Adware.Optmedia*

Kada izuzimate otkrivenu prijetnju iz prozora upozorenja programa ESET Endpoint Antivirus, možete

✓ upotrijebiti i sljedeći format:

*@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt  
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan  
@NAME=Win32/Bagle.D@TYPE=worm*

---

## Kontrolni elementi

- **Dodaj** – Izuzima objekte od otkrivanja.
- **Uredi** – Omogućuje vam uređivanje odabralih unosa.
- **Ukloni** – uklanja odabrane unose (CTRL + klik za odabir više unosa).

## Čarobnjak za stvaranje izuzetih detekcija poznatih prijetnji

Izuzeta detekcija poznatih prijetnji također se može stvoriti u kontekstnom izborniku [Dnevnići](#) (nije dostupno za detekciju zlonamjernih programa):

1. U glavnom prozoru programa kliknite **Alati > Dnevnići**.
2. Kliknite desnom tipkom miša prijetnju u **Dnevniku prijetnji**.
3. Kliknite **Stvori izuzetak**.

Za izuzimanje jedne ili više prijetnji na temelju **Kriterija izuzetka** kliknite **Promjeni kriterije**:

- **Točne datoteke** – Izuzimanje datoteka prema hashu SHA-1.
- **Prijetnja** – Izuzimanje datoteka prema nazivu prijetnje.
- **Put + prijetnja** – Izuzimanje datoteka prema nazivu i putu prijetnje, uključujući naziv datoteke (npr. `file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe`).

Preporučena opcija unaprijed je odabrana na temelju prijetnje.

Dodatno možete dodati **Komentar** prije nego što kliknete na **Stvori izuzetak**.

## Izuzeci (7.1 i stariji)

Kod izuzetaka u verziji 7.1 i starijim verzijama [Izuzeci radi poboljšanja performansi](#) i [Izuzeci detekcija poznatih prijetnji](#) spojeni su u jedno.



Vrsta	Pojedinosti
Put: Opis:	C:\Backup\*.*
Put: Opis:	C:\pagefile.sys
Prijetnja: Put: Opis:	@NAME=Win32/Advare.Optmedia C:\Recovery\*.*
Ključ: Opis:	678C1422DE867141B947EA700E8A2D6114AFAE97 SuperApi.exe

**Dodaj** **Uredi** **Izbriši** **Spremi** **Odustani**

## Izuzeti procesi

Funkcija Izuzeti procesi omogućuje vam da izuzmete procese aplikacija iz Rezidentne zaštite sistemskih datoteka. Za poboljšanje brzine sigurnosnog kopiranja, cjelevitosti procesa i dostupnosti usluge tijekom sigurnosnog kopiranja upotrebljavaju se neke tehnike za koje je poznato da dolaze u sukob sa zaštitom od zlonamjernih programa na razini datoteka. Slični problemi mogu se pojaviti kada pokušavate uživo migrirati virtualna računala. Jedini je učinkovit način da izbjegnete obje situacije da deaktivirate softver za zaštitu od zlonamjernih programa. Izuzimanjem određenih procesa (primjerice procesa rješenja za sigurnosno kopiranje), sve operacije s datotekama pripisane takvim izuzetim procesima zanemaruju se i smatraju se sigurnima, stoga se smanjuje ometanje procesa sigurnosnog kopiranja. Preporučujemo da budete oprezni kada stvarate izuzetke – alat za sigurnosno kopiranje koji je izuzet može pristupiti zaraženim datotekama bez pokretanja upozorenja, zbog čega su proširena dopuštenja dopuštena samo u modulu rezidentne zaštite.

Izuzeti procesi pomažu smanjiti rizik od potencijalnih sukoba i poboljšati performanse izuzetih aplikacija, što u konačnici ima pozitivan učinak na ukupne performanse i stabilnost operacijskog sustava. Izuzimanjem procesa/aplikacije izuzima se njihova izvršna datoteka (.exe).

Možete dodati izvršne datoteke na popis izuzetih procesa u **Naprednom podešavanju (F5) > Modul detekcije > Rezidentna zaštita sistemskih datoteka > Izuzeti procesi**.

Ova je značajka osmišljena tako da izuzima alate za sigurnosno kopiranje. Izuzimanje procesa alata za sigurnosno kopiranje od skeniranja ne samo da osigurava stabilnost sustava, već ne utječe ni na učinkovitost sigurnosnog kopiranja jer se sigurnosno kopiranje ne usporava dok je u tijeku.

**Kliknite Uredi** da biste otvorili prozor za upravljanje **izuzetim procesima**, gdje možete [dodati izuzetke](#) i pretraživati izvršne datoteke (na primjer *Backup-tool.exe*), koje će biti izuzete od skeniranja. Čim se datoteka .exe doda izuzecima, ESET Endpoint Antivirus više ne prati aktivnost tog procesa i ne provodi se skeniranje operacija s datotekama tog procesa.

**Ako ne upotrebljavate funkciju pretraživanja kada birate izvršnu datoteku procesa, trebate ručno unijeti cijeli put do izvršne datoteke.** U suprotnom izuzetak neće ispravno funkcionirati i [HIPS](#) može prijaviti pogreške.

Također možete **Urediti** postojeće procese ili ih **Ukloniti** iz izuzetaka.

**i** [Zaštita web pristupa](#) ne uzima u obzir ovakav izuzetak, stoga ako izuzmete izvršnu datoteku svojeg web preglednika, preuzete datoteke i dalje će se skenirati. Na taj se način i dalje može otkriti infiltracija. Ovaj slučaj služi samo kao primjer, ne preporučujemo stvaranje izuzetaka za web preglednike.

## Dodavanje ili uređivanje izuzetih procesa

Ovaj dijaloški prozor omogućava **dodavanje** procesa izuzetih od modula detekcije. Izuzeti procesi pomažu smanjiti rizik od potencijalnih sukoba i poboljšati performanse izuzetih aplikacija, što u konačnici ima pozitivan učinak na ukupne performanse i stabilnost operacijskog sustava. Izuzimanje procesa/aplikacije znači izuzimanje njihove izvršne datoteke (.exe).

Odaberite put datoteke izuzete aplikacijetako da kliknete na ... (na primjer *C:\Program*

*Files\Firefox\Firefox.exe*). NEMOJTE upisati naziv aplikacije.

✓ Čim se datoteka .exe doda izuzecima, ESET Endpoint Antivirus više ne prati aktivnost tog procesa i ne provodi se skeniranje operacija s datotekama tog procesa.

⚠ Ako ne upotrebljavate funkciju pretraživanja kada birate izvršnu datoteku procesa, trebate ručno unijeti cijeli put do izvršne datoteke. U suprotnom izuzetak neće ispravno funkcionirati i [HIPS](#) može prijaviti pogreške.

Također možete **Urediti** postojeće procese ili ih **Ukloniti** iz izuzetaka.

## Izuzeci iz HIPS-a

Izuzeci omogućavaju izuzimanje procesa iz HIPS-ova dubinskog pregleda ponašanja.

Da biste izuzeli objekt, kliknite **Dodaj** i unesite put do objekta ili ga odaberite u stablastoj strukturi. Također možete **uređivati** ili **ukloniti** odabrane unose.

**i** Pogledajte poglavlje [Izuzeci](#).

## ThreatSense parameteri

ThreatSense se sastoji od mnogo složenih metoda otkrivanja prijetnji. To je proaktivna tehnologija, što znači da omogućuje zaštitu u ranom stadiju širenja nove prijetnje. Koristi kombinaciju analize koda, emulacije koda, generičkih potpisa i virusnih potpisa, koji zajedno uvelike poboljšavaju sigurnost sustava. Sustav skeniranja može kontrolirati nekoliko podatkovnih tokova istodobno, čime pruža maksimalnu učinkovitost i stopu otkrivanja. Tehnologija ThreatSense uspješno eliminira i rootkite.

Mogućnosti podešavanja tehnologije ThreatSense omogućuju vam određivanje nekoliko parametara skeniranja:

- Vrste datoteka i datotečnih ekstenzija koje treba skenirati
- Kombinacija različitih metoda otkrivanja
- razina čišćenja itd.

Da biste otvorili prozor za podešavanje, kliknite **ThreatSense parameteri** u prozoru Napredno podešavanje za svaki modul koji koristi tehnologiju ThreatSense (pogledajte niže). Za različite scenarije sigurnosti moglo bi biti potrebne različite konfiguracije. ThreatSense je moguće pojedinačno konfigurirati za sljedeće zaštitne module:

- rezidentna zaštita
- Skeniranje u stanju mirovanja
- Skeniranje pri pokretanju
- Zaštita dokumenata
- zaštita klijenta e-pošte
- zaštita web pristupa
- Skeniranje računala

The screenshot shows the 'Napredno podešavanje' (Advanced Settings) window of the ESET Endpoint Antivirus interface. On the left, a sidebar lists various modules: MODUL DETEKCIJE (2), Rezidentna zaštita sistemskih datoteka, Zaštita potpomognuta cloudom, Skeniranje zlonamjernog softvera, HIPS (2), NADOGRADNJA (1), MREŽNA ZAŠTITA, WEB I E-POŠTA (3), KONTROLA UREĐAJA (2), ALATI (3), and KORISNIČKO SUČELJE (1). The main panel is titled 'OSNOVNO' and contains a section for 'THREATSENSE PARAMETRI'. Under 'OBJEKTI SKENIRANJA', 'Boot sektori / UEFI' has a checked checkbox. Under 'OPCIJE SKENIRANJA', 'Heuristika' has a checked checkbox. In the bottom right corner, there is a note: 'U ovom će načinu rada program automatski pokušati očistiti ili izbrisati sve zaražene datoteke. Ukoliko nije moguće izvesti niti jednu radnju, a korisnik je prijavljen, prikazat će se prozor s upozorenjem s popisom dostupnih akcija. Prozor s upozorenjem prikazat će se i ako akcija ne uspije.' Below this note are three buttons: 'Standardno' (gray), 'U redu' (blue), and 'Odustani' (gray).

Parametri sustava ThreatSense optimizirani su za svaki modul, a njihova izmjena može znatno utjecati na rad cjelokupnog sustava. Promjena parametara kako bi se uvijek skenirali runtime arhivatori ili aktiviranje napredne heuristike u modulu za rezidentnu zaštitu, na primjer, može dovesti do usporavanja sustava (obično se tim metodama skeniraju samo novostvorene datoteke). Stoga vam preporučujemo da osim skeniranja računala ni za koji modul ne mijenjate standardne parametre sustava ThreatSense.

## Objekti za skeniranje

U ovom odjeljku možete definirati koje će se računalne komponente i datoteke skenirati radi otkrivanja

infiltracija.

**Radna memorija** – Skenira prijetnje koje napadaju radnu memoriju sustava.

**Boot sektori / UEFI** – Skenira boot sektore da bi se otkrila prisutnost zlonamjernih programa u glavnom boot zapisu. [Više o UEFI-ju pročitajte u rječniku](#).

**Datoteke e-pošte** – Program podržava sljedeće ekstenzije: DBX (Outlook Express) i EML.

**Arhive** – Program podržava sljedeće ekstenzije: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE i mnoge druge.

**Samoraspakirajuće arhive** – Samoraspakirajuće arhive (SFX) arhive su koje se same mogu raspakirati.

**Runtime arhivatori** – Runtime arhivatori (za razliku od standardnih arhiva) nakon pokretanja se raspakiraju u memoriji. Uz standardne statične arhivatore (UPX, yoda, ASPack, FSG itd.), skener zahvaljujući emulaciji koda podržava i mnoge druge vrste arhivatora.

## Mogućnosti skeniranja

Odaberite postupke koji će se koristiti za skeniranje sustava radi otkrivanja infiltracija. Na raspolaganju su sljedeće mogućnosti:

**Heuristika** – Heuristika je algoritam pomoću kojega se analizira (zlonamjerna) aktivnost programa. Glavna prednost ove tehnologije je sposobnost identifikacije zlonamjernog softvera koji nije postao ili nije bio poznat prethodnoj verziji modula za otkrivanje virusa. Mana joj je (vrlo mala) mogućnost lažnih uzbuna.

**Napredna heuristika / DNA potpisi** – Napredna se heuristika sastoji od jedinstvenog heurističkog algoritma razvijenog u tvrtki ESET, koji je optimiziran za prepoznavanje računalnih crva i trojanskog softvera, a napisan je u programskim jezicima visoke razine. Korištenje napredne heuristike uvelike povećava sposobnosti programa tvrtke ESET u otkrivanju prijetnji. Pomoću potpisa moguće je pouzdano otkriti i prepoznati virus. Koristeći sustav automatske nadogradnje novi potpisi dostupni su u roku od nekoliko sati od otkrivanja prijetnje. Mana je potpisa to što se pomoću njih otkrivaju samo poznati virusi (ili njihove malo izmijenjene verzije).

## Čišćenje

[Postavke čišćenja](#) određuju funkcioniranje programa ESET Endpoint Antivirus prilikom čišćenja objekata.

## Izuzeci

Ekstenzija je dio naziva datoteke iza točke. Ekstenzija definira vrstu i sadržaj datoteke. Ovaj odjeljak podešavanja parametara sustava ThreatSense omogućuje definiranje vrsta datoteka za skeniranje.

## Ostalo

Prilikom konfiguiranja podešavanja parametara sustava ThreatSense za skeniranje računala na zahtjev u odjeljku **Ostalo** dostupne su i sljedeće mogućnosti:

**Skeniraj alternativne protokole podataka (ADS)** – Alternativni protoci podataka koje koristi datotečni sustav NTFS pridruživanja su datoteka i mapa nevidljiva običnim tehnikama skeniranja. Mnoge infiltracije pokušavaju izbjegći otkrivanje tako što se prikazuju kao alternativni protoci podataka.

**Pokreni pozadinska skeniranja s niskim prioritetom** – Svaki slijed skeniranja troši izvjesnu količinu sistemskih resursa. Ako radite s programima koji obilato koriste sistemske resurse, možete aktivirati pozadinsko skeniranje

niskog prioriteta da biste resurse sačuvali za ostale aplikacije.

**Zabilježi sve objekte** – [Dnevnik skeniranja](#) pokazat će sve skenirane datoteke u samoraspakirajućim arhivama, čak i one koje nisu zaražene (može se generirati mnogo podataka dnevnika skeniranja i povećati veličina dnevnika skeniranja).

**Omogući SMART optimizaciju** – Kada je aktivirana SMART optimizacija, koriste se optimalne postavke da bi se osigurala najučinkovitija razina skeniranja te da bi se skeniranje izvršavalo najvećom mogućom brzinom. Različiti moduli zaštite vrše pametno skeniranje pri čemu koriste različite metode skeniranja i primjenjuju ih na različite vrste datoteka. Ako je Smart optimizacija deaktivirana, prilikom skeniranja koriste se samo korisnički definirane postavke u jezgri programa ThreatSense za određene module.

**Sačuvaj vremensku oznaku zadnjeg pristupa** – Odaberite ovu opciju ako želite sačuvati vrijeme zadnjeg pristupa skeniranim datotekama umjesto njihove nadogradnje (npr. za korištenje sa sustavima sigurnosnog kopiranja).

## **Ograničenja**

Odjeljak Ograničenja omogućuje određivanje maksimalne veličine objekata i razina ugnježđenih arhiva za skeniranje:

### **Postavke objekta**

**Maksimalna veličina objekta** – Definira maksimalnu veličinu objekata za skeniranje. Dani antivirusni modul skenirat će samo objekte manje od zadane veličine. Na promjenu te mogućnosti trebali bi se ograničiti samo napredni korisnici koji imaju određene razloge da od skeniranja izuzmu veće objekte. Standardna vrijednost: neograničeno.

**Maksimalno vrijeme skeniranja za objekt (u sekundama)** – Definira maksimalnu vremensku vrijednost za skeniranje datoteka u spremišnom objektu (kao što je RAR/ZIP arhiva ili e-poruka s više privitaka). Ova postavka se ne odnosi na samostalne datoteke. Ako je unesena korisnički definirana vrijednost i to vrijeme je proteklo, skeniranje će se zaustaviti što je prije moguće, neovisno o tome je li skeniranje svih datoteka u spremišnom objektu dovršeno.

U slučaju arhive s velikim datotekama, skeniranje će se zaustaviti tek nakon što se raspakira datoteka iz arhive (na primjer, kada je korisnički definirana varijabla 3 sekunde, ali raspakiravanje datoteke traje 5 sekundi). Ostale datoteke u arhivi se neće skenirati kada to vrijeme istekne.

Da biste ograničili vrijeme skeniranja, uključujući za veće arhive, upotrijebite opcije **Maksimalna veličina objekta** i **Maksimalna veličina datoteke u arhivi** (ne preporučuje se zbog mogućih sigurnosnih rizika). Standardna vrijednost: neograničeno.

### **Podešavanje skeniranja arhive**

**Razina ugnježđenja arhive** – Određuje maksimalnu dubinu skeniranja arhiva. Standardna vrijednost: 10.

**Maksimalna veličina datoteke u arhivi** – Ova opcija omogućuje vam da odredite maksimalnu veličinu (raspakiranih) datoteka sadržanih u arhivama koje želite skenirati. Standardna vrijednost: neograničeno.

**i** Ne preporučujemo da mijenjate standardne vrijednosti jer u normalnim okolnostima nema razloga za to.

# Razine čišćenja

Da biste pristupili postavkama razina čišćenja za željeni zaštitni modul, proširite **ThreatSense parametre** (primjerice, **Rezidentnu zaštitu sistemskih datoteka**) i zatim kliknite **Čišćenje**.

Rezidentna zaštita i ostali zaštitni moduli imaju sljedeće razine ispravljanja (odnosno čišćenja).

## Ispravljanje u programu ESET Endpoint Antivirus 8

Razina čišćenja	Opis
<b>Uvijek ispravi prijetnju</b>	Pokušaj uklanjanja otkrivene prijetnje prilikom čišćenja objekata bez intervencije krajnjeg korisnika. U rijetkim slučajevima (npr. u slučaju sistemskih datoteka) kada se otkrivena prijetnja ne može ispraviti, prijavljeni objekt ostavlja se na izvornoj lokaciji. Preporučena standardna postavka je <b>Uvijek ispravi prijetnju</b> u <a href="#">upravljanom okruženju</a> .
<b>Ispravi otkrivenu prijetnju ako je sigurna, u suprotnom je zadrži</b>	Pokušaj ispravljanja otkrivene prijetnje prilikom čišćenja <a href="#">objekata</a> bez intervencije krajnjeg korisnika. U nekim slučajevima (npr. u slučaju sistemskih datoteka ili arhiva koji sadrže i čiste i zaražene datoteke), ako se otkrivena prijetnja ne može ispraviti, prijavljeni se objekt ostavlja na izvornoj lokaciji.
<b>Ispravi otkrivenu prijetnju ako je sigurna, u suprotnom postavi pitanje</b>	Pokušaj ispravljanja otkrivene prijetnje prilikom čišćenja objekata. Ako se u nekim slučajevima ne izvrši nikakva radnja, krajnjem korisniku prikazuje se interaktivno upozorenje i potrebno je odabrati radnju za ispravljanje (npr. uklanjanje ili zanemarivanje). Ova se postavka preporučuje u većini slučajeva.
<b>Uvijek pitaj krajnjeg korisnika</b>	Tijekom čišćenja objekata krajnjem korisniku se prikazuje interaktivno upozorenje i potrebno je odabrati radnju za ispravljanje (npr. uklanjanje ili zanemarivanje). Ta razina namijenjena je naprednjim korisnicima koji znaju koje korake treba poduzeti u slučaju prijetnje.

## Napredno podešavanje



## MODUL DETEKCIJE 2

## Rezidentna zaštita sistemskih datoteka

Zaštita potpomognuta cloudom

Skeniranje zlonamjernog softvera

## HIPS 2

## NADOGRADNJA 1

## MREŽNA ZAŠTITA

## WEB I E-POŠTA 3

## KONTROLA UREĐAJA 2

## ALATI 3

## KORISNIČKO SUČELJE 1

## OSNOVNO

## THREATSENSE PARAMETRI

## OBJEKTI SKENIRANJA

Boot sektori / UEFI



Runtime arhivatori



## OPCIJE SKENIRANJA

Heuristika



Napredna heuristika / DNA potpis



## ČIŠĆENJE

Razina čišćenja

Ispravi zarazu ako je to sigurno... ▾



U ovom će načinu rada program automatski pokušati očistiti ili izbrisati sve zaražene datoteke. Ukoliko nije moguće izvesti niti jednu radnju, a korisnik je prijavljen, prikazat će se prozor s upozorenjem s popisom dostupnih akcija. Prozor s upozorenjem prikazat će se i ako akcija ne uspije.

Standardno

U redu

Odustani

## Datotečne ekstenzije izuzete od skeniranja

Ekstenzija je dio naziva datoteke iza točke. Ekstenzija definira vrstu i sadržaj datoteke. Ovaj odjeljak podešavanja parametara sustava ThreatSense omogućuje definiranje vrsta datoteka za skeniranje.

**i** Ne smiju se pomiješati s drugim vrstama [izuzetaka](#).

Prema standardnim se postavkama skeniraju sve datoteke. Svaka se ekstenzija može dodati na popis datoteka izuzetih od skeniranja.

Isključivanje datoteka ponekad je potrebno ako skeniranje određenih vrsta datoteka ometa ispravan rad programa koji koriste te ekstenzije. Ako, primjerice, koristite MS Exchange Server, možda bi bilo dobro da iz pregleda izuzmete ekstenzije .edb, .eml i .tmp.

Za dodavanje nove ekstenzije na popis kliknite **Dodaj**. Upišite ekstenziju u prazno polje (na primjer tmp) i kliknite **U redu**. Kad odaberete **Unesite višestruke vrijednosti**, možete dodati više datotečnih ekstenzija odvojenih crtama, zarezima ili točka-zarezima (na primjer, odaberite **Točka-zarez** iz padajućeg izbornika kao razdjelnik i upišite edb;eml;tmp). Možete upotrijebiti poseban simbol ? (upitnik). Upitnik zamjenjuje bilo koji simbol (na primjer, ?db).

**i** da biste vidjeli točnu ekstenziju (ako je ima) datoteke u operacijskom sustavu Windows, morate poništiti mogućnost **Sakrij datotečne nastavke za poznate vrste datoteka** na **Upravljačkoj ploči > Mogućnosti mapa > Prikaz** (kartica) i primijeniti tu promjenu.

# Dodatni ThreatSense parametri

**Dodatni ThreatSense parametri za novostvorene i preinačene datoteke** – Vjerovatnost zaraze novostvorenih ili preinačenih datoteka razmijerno je viša nego kod postojećih datoteka. Iz tog razloga program provjerava te datoteke pomoću dodatnih parametara skeniranja. Uz uobičajene metode skeniranja na temelju potpisa, koristi se i napredna heuristika, koja može otkriti nove prijetnje prije objave aktualizacije modula za otkrivanje virusa. Uz novostvorene datoteke skeniraju se i samoraspakirajuće datoteke (.sfx) te runtime arhivatori (interni sažete izvršne datoteke). Standardno se arhive skeniraju do desetog stupnja grijevanja, a provjeravaju se bez obzira na njihovu veličinu. Da biste izmijenili postavke skeniranja arhive, deaktivirajte **Standardne postavke skeniranja arhive**.

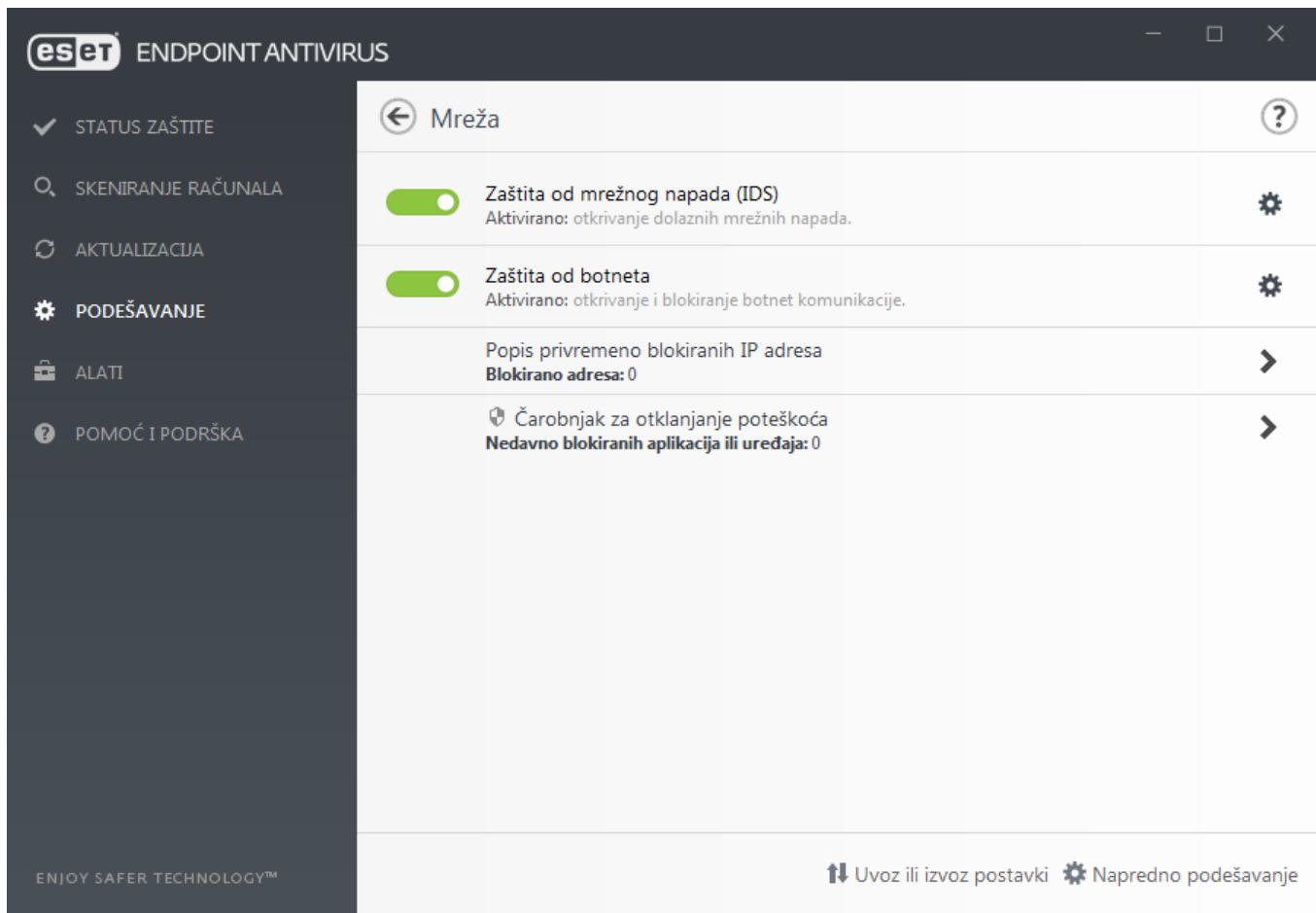
Dodatne informacije o mogućnostima Runtime arhivatori, Samoraspakirajuće arhive i Napredna heuristika potražite u odjeljku [Podešavanje ThreatSense parametara](#).

**Dodatni ThreatSense parametri za pokrenute datoteke** – Standardno se pri pokretanju datoteka upotrebljava [Napredna heuristika](#). Preporučujemo da, dok je ta mogućnost aktivirana, budu aktivirane i mogućnosti [Smart optimizacija](#) i ESET LiveGrid® kako se ne bi narušile performanse sustava.

## Mreža

Odjeljak **Mreža** omogućava brz pristup sljedećim komponentama ili postavkama u izborniku **Napredno podešavanje**:

- **Zaštita od mrežnog napada (IDS)** – Analizira sadržaj mrežnog prometa i štiti od mrežnih napada. Blokira se sav promet koji se smatra štetnim. ESET Endpoint Antivirus obavijestit će vas kada se povežete s nezaštićenom bežičnom mrežom ili s mrežom sa slabom zaštitom.
- **Zaštita od botneta** – Brzo i točno identificira zlonamjerni softver u sustavu. Da biste deaktivirali zaštitu od botneta na određeno vremensko razdoblje, kliknite  (nije preporučeno).
- **Popis privremeno blokiranih IP adresa** – prikazuje popis IP adresa koje su prepoznate kao izvori napada i dodane na popis blokiranih adresa radi sprečavanja povezivanja na određeno razdoblje. Za više informacija kliknite ovu opciju i pritisnite F1.
- **Čarobnjak za otklanjanje poteškoća** – Pomaže vam u rješavanju problema s povezivanjem uzrokovanih ESET firewallom. Detaljne informacije potražite u odjeljku [Čarobnjak za otklanjanje poteškoća](#).



## Zaštita od mrežnog napada

**Zaštita od mrežnog napada (IDS)** – Analizira sadržaj mrežnog prometa i štiti od mrežnih napada. Blokira se sav promet koji se smatra štetnim.

**Aktiviraj zaštitu od botneta** – Otkriva i blokira komunikaciju sa zločudnim naredbama i kontrolnim serverima na temelju tipičnih obrazaca kada je računalo zaraženo i bot pokušava komunicirati. [Pročitajte više o zaštiti od botneta u rječniku](#).

**Pravila IDS-a** – Ta opcija omogućuje vam konfiguriranje naprednih funkcija filtriranja radi otkrivanja raznih vrsta mogućih napada na vaše računalo.

## Napredne opcije filtriranja

Odjeljak Zaštita od mrežnog napada omogućuje konfiguraciju naprednih opcija filtriranja radi otkrivanja nekoliko vrsta napada i ranjivosti koje mogu ciljati na vaše računalo.

**i** U nekim slučajevima nećete primiti obavijest o prijetnjama u vezi s blokiranim komunikacijama. Pogledajte odjeljak [Vođenje dnevnika i stvaranje pravila ili iznimki iz dnevnika](#) za upute o prikazu svih blokiranih komunikacija u dnevniku firewalla.

**!** Dostupnost određenih opcija u odjeljku Napredno podešavanje (**F5**) > **Mrežna zaštita > Zaštita od mrežnog napada** može se razlikovati ovisno o vrsti ili verziji ESET-ova sigurnosnog programa i modula firewalla, kao i o verziji operacijskog sustava. Neke od njih mogu biti dostupne samo za program ESET Endpoint Security.

## **- Otkrivanje upada**

- **Protokol SMB** – Otkriva i blokira razne sigurnosne probleme u SMB protokolu, odnosno:
  - **Otkrivanje napada lažnim izazovom za autentikaciju servera** – Ova opcija štiti od napada koji koriste lažni izazov tijekom autorizacije radi dohvaćanja korisničkih podataka.
  - **Otkrivanje izbjegavanja IDS-a tijekom otvaranja kanala s imenom** – Otkrivanje poznatih tehnika izbjegavanja za otvaranje MSRPCS cijevi s imenom u SMB protokolu.
  - **Otkrivanje CVE** (Common Vulnerabilities and Exposures) – Primjenjene metode otkrivanja raznih napada, oblika, sigurnosnih rupa i manevra preko SMB protokola. Pogledajte [CVE web stranicu na adresi cve.mitre.org](#) i potražite detaljnije informacije o CVE identifikatorima (CVE-ovi).
- **RPC protokol** – Otkriva i blokira razne CVE-ove u udaljenom sustavu poziva razvijenom za Distribuirano računalno okruženje (DCE).
- **Protokol RDP** – Otkriva i blokira razine CVE-ove u RDP protokolu (pogledajte iznad).
- **Blokiraj nesigurne adrese nakon otkrivanja napada** – IP adrese koje su prepoznate kao izvori napada dodaju se popisu spam adresa radi sprečavanja povezivanja na određeno razdoblje.
- **Prikaži obavijest nakon otkrivanja napada** – Uključuje obavijest na programskoj traci koja se nalazi u donjem desnom kutu zaslona.
- **Prikaži obavijest i za nadolazeće napade na sigurnosne rupe** – Prikazuje upozorenja u slučaju otkrivanja napada na sigurnosne rupe ili pokušaja prodiranja prijetnje u sustav.

## **- Provjera paketa**

- **Dopusti dolaznu vezu za zajedničke mreže u SMB protokolu** – Zajedničke mreže odnose se ovdje na standardne zajedničke mreže koje dijele particije tvrdog diska (*C\$, D\$*, ...) u sustavu zajedno s mapom sustava (*ADMIN\$\*). Deaktiviranje veze sa zajedničkim mrežama trebalo bi smanjiti mnoge sigurnosne rizike. Primjerice, crv Conficker vrši napade "dictionary attack" kako bi uspostavio vezu sa zajedničkim mrežama.
- **Zabrani stare (nepodržane) SMB dijalekte** – Odbija se SMB sesija sa starim SMB dijalektom koji IDS ne podržava. Suvremeni operacijski sustavi Windows podržavaju stare SMB dijalekte zahvaljujući unazadnoj kompatibilnosti sa starim operacijskim sustavima kao što je Windows 95. Napadač može koristiti stari dijalekt u SMB sesiji kako bi izbjegao provjeru prometa. Zabranite stare SMB dijalekte ako računalo ne treba zajednički koristiti datoteke (ili SMB komunikaciju općenito) s računalom koje koristi staru verziju sustava Windows.
- **Zabrani SMB sesije bez povećane sigurnosti** – Povećana sigurnost može se koristiti tijekom pregovaranja SMB sesije kako bi se osigurao mehanizam autentikacije koji je sigurniji od autentikacije izazovom/odgovorom LAN upravitelja (LM). LM shema smatra se slabom i ne preporučuje se za upotrebu.
- **Dopusti komunikaciju sa servisom Security Account Manager** – Više informacija o ovom servisu pogledajte ovdje [\[MS-SAM\]](#).
- **Dopusti komunikaciju sa servisom Local Security Authority** – Više informacija o ovom servisu pogledajte ovdje [\[MS-LSAD\]](#) i ovdje [\[MS-LSAT\]](#).
- **Dopusti komunikaciju sa servisom Remote Registry** – Više informacija o ovom servisu pogledajte ovdje [\[MS-RRP\]](#).
- **Dopusti komunikaciju sa servisom Service Control Manager** – Više informacija o ovom servisu pogledajte

ovdje [\[MS-SCMR\]](#).

- **Dopusti komunikaciju sa servisom Server** – Više informacija o ovom servisu pogledajte ovdje [\[MS-SRVS\]](#).
- **Dopusti komunikaciju s drugim servisima** – Microsoftova implementacija mehanizma DCE RPC. Osim toga, Microsoftova implementacija mehanizma DCE RPC. Osim toga, MSRPC može za prijenos (ncacn\_np transport) koristiti cijevi s nazivom koje su prenesene u protokol SMB (zajedničko korištenje mrežnih datoteka). MSRPC servisi nude sučelja za udaljeno pristupanje i upravljanje prozorima. Otkriveno je i iskorišteno "in the wild" nekoliko sigurnosnih slabosti u sustavu Windows MSRPC (crv Conficker, crv Sasser...). Deaktivirajte komunikaciju s MSRPC servisima koja vam nije potrebna kako biste umanjili mnoge sigurnosne rizike (kao što je udaljeno izvršavanje koda ili napad uskraćivanjem usluge).

## Pravila IDS-a

U nekim situacijama [usluga otkrivanja upada \(IDS\)](#) može otkriti komunikaciju između routera ili drugih unutarnjih uređaja za umrežavanje kao potencijalni napad. Primjerice, poznatu sigurnu adresu možete dodati u Adrese izuzete iz zone IDS-a da biste zaobišli IDS.

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

- i**
- [Stvaranje pravila IDS-a o klijentskim radnim stanicama u programu ESET Endpoint Antivirus \(8.x\)](#)
  - [Izrada pravila IDS-a za klijentske radne stanice u programu ESET PROTECT \(8.x\)](#)

## Stupci

- **Prijetnja** – vrsta prijetnje.
- **Aplikacija** – Odaberite put datoteke izuzete aplikacijetako da kliknete na ... (na primjer C:\Program Files\Firefox\Firefox.exe). NEMOJTE upisati naziv aplikacije.
- **Udaljeni IP** – Popis udaljenih IPv4 ili IPv6 adresa / raspona / podmreža. Višestruke adrese potrebno je odvojiti zarezima.
- **Blokiraj** – Svaki sistemski proces ima svoje standardno ponašanje i dodijeljenu radnju (blokiranje ili dopuštanje). Da biste nadjačali standardno ponašanje za program ESET Endpoint Antivirus, putem padajućeg izbornika možete odabrati želite li blokirali ili dopustiti.
- **Obavijesti** – Odaberite Da za prikaz [Obavijesti na radnoj površini](#) na računalu. Odaberite Ne ako ne želite obavijesti na radnoj površini. Dostupne su vrijednosti Standardno/Da/Ne.
- **Dnevnik** – Odaberite Da za zapisivanje događaja u dnevničku knjigu programa [ESET Endpoint Antivirus](#). Odaberite Ne ako ne želite zapisivati događaje u dnevnik. Dostupne su vrijednosti Standardno/Da/Ne.

Izuzeci kartica prikazat će se ako administrator [stvori izuzetke IDS-a u ESET PROTECT web konzoli](#). Izuzeci IDS-a mogu sadržavati samo dopuštajuća pravila i procjenjuju se prije pravila IDS-a.

## Upravljanje pravilima IDS-a

- **Dodaj** – kliknite da biste stvorili novo pravilo IDS-a.
- **Uredi** – kliknite da biste uredili postojeće pravilo IDS-a.

- **Ukloni** – označite i kliknite ako želite ukloniti postojeću iznimku s popisa pravila IDS-a.
- **Vrh/Gore/Dolje/Dno** – omogućuje vam podešavanje razine prioriteta pravila (iznimke se procjenjuju od vrha prema dnu).

Želite prikazati obavijest i prikupiti dnevnik svaki put kada se događaj pojavi:

- 1.Kliknite **Dodaj** da biste dodali novo pravilo IDS-a.
- 2.Odaberite određeno upozorenje iz padajućeg izbornika **Prijetnja**.
- 3.Kliknite ... i odaberite put datoteke aplikacije na koju želite da se primjenjuje obavijest.
- 4.Ostavite postavku **Standardno** u padajućem izborniku **Blokiraj**. Time će se preuzeti standardna radnja koju primjenjuje ESET Endpoint Antivirus.
- 5.Postavite padajuće izbornike **Obavijesti i Dnevnik** na **Da**.
- 6.Kliknite **U redu** da biste spremili ovu obavijest.

Ako želite ukloniti učestale obavijesti za vrstu prijetnje za koju smatrate da nije prijetnja:

- 1.Kliknite **Dodaj** da biste dodali novu IDS iznimku.
- 2.Odaberite određeno upozorenje iz padajućeg izbornika **Prijetnja**, na primjer **SMB sesija bez sigurnosnih ekstenzija**.
- 3.Odaberite **Ulaz** iz padajućeg izbornika smjera u slučaju da potječe od dolazne komunikacije.
- 4.Postavite padajući izbornik **Obavijesti** na **Ne**.
- 5.Postavite padajući izbornik **Dnevnik** na **Da**.
- 6.Ostavite stavku **Aplikacija** praznom.
- 7.Ako komunikacija ne dolazi s određene IP adrese, ostavite stavku **Udaljene IP adrese** praznom.
- 8.Kliknite **U redu** da biste spremili ovu obavijest.

## Blokirana je potencijalna prijetnja

Do ove situacije može doći kada neka aplikacija na vašem računalu pokušava prenijeti zlonamjerni promet drugome računalu na mreži iskorištavanjem sigurnosne rupe ili ako netko pokuša skenirati portove na vašoj mreži.

**Prijetnja** – Naziv prijetnje.

**Izvor** – Mrežna adresa izvora.

**Objekt** – Mrežna adresa objekta.

**Prestani blokirati** – stvara pravilo IDS-a za potencijalnu prijetnju s postavkama za dopuštanje komunikacije.

**Nastavi blokirati** – blokira otkrivenu prijetnju. Da biste stvorili pravilo IDS-a s postavkama za blokiranje komunikacije za navedenu prijetnju, odaberite opciju **Nemoj me ponovno obavijestiti**.

- i** Informacije prikazane u prozoru obavijesti mogu se razlikovati ovisno o vrsti otkrivene prijetnje.  
Više informacija o prijetnjama i drugim povezanim pojmovima potražite u odjeljku [Vrste udaljenih napada](#) ili [Vrste otkrivenih prijetnji](#).

## Otklanjanje poteškoća mrežne zaštite

Čarobnjak za otklanjanje poteškoća pomaže vam riješiti probleme s povezivanjem koje je uzrokovao ESET firewall. Na padajućem izborniku odaberite vremensko razdoblje tijekom kojeg je komunikacija bila blokirana. Popis

nedavno blokiranih komunikacija daje vam uvid u vrstu aplikacije ili uređaja te u reputaciju i ukupan broj aplikacija i uređaja blokiranih tijekom tog razdoblja. Za dodatne informacije o blokiranoj komunikaciji kliknite stavku **Detalji**. U sljedećem koraku trebate deblokirati aplikaciju ili uređaj s kojim imate teškoće u povezivanju.

Kada kliknete **Deblokiraj**, komunikacija koja je bila blokirana sada će biti dopuštena. Ako i dalje imate poteškoće s aplikacijom, ili vaš uređaj ne radi prema očekivanjima, kliknite **Aplikacija i dalje ne radi** pa će sve komunikacije koje su prije bile blokirane sada biti dopuštene. Ako problem i dalje postoji, ponovno pokrenite računalo.

Kliknite **Prikaži promjene** da biste vidjeli pravila koja je stvorio čarobnjak.

Kliknite **Deblokiraj** sljedeće da biste riješili komunikacijske poteškoće s drugim uređajem ili aplikacijom.

## Popis privremeno blokiranih IP adresa

Da biste vidjeli IP adrese koje su prepoznate kao izvori napada i dodane popisu nepoželjnih IP adresa radi blokiranja povezivanja na određeno razdoblje, iz programa ESET Endpoint Antivirus idite u **Podešavanje > Mrežna zaštita > Popis privremeno blokiranih IP adresa**. Privremeno blokirane IP adrese blokirane su na 1 sat.

### Stupci

**IP adresa** – Prikazuje IP adresu koja je blokirana.

**Razlog za blokiranje** – Prikazuje vrstu napada s dane adrese koja je spriječena (npr. napad skeniranjem TCP porta).

**Istek vremena** – Prikazuje vrijeme i datum do kada će adresa biti na popisu blokiranih adresa.

### Kontrolni elementi

**Ukloni** – Kliknite ovu opciju da biste uklonili adresu s popisa blokiranih adresa prije isteka vremena.

**Ukloni sve** – Kliknite ovu opciju da biste odmah uklonili sve adrese s popisa blokiranih adresa.

**Dodaj iznimku** – Kliknite ovu opciju da biste dodali firewall iznimku u IDS filtriranje.

## Web i e-pošta

Konfiguraciju weba i e-pošte možete pronaći u prozoru **Podešavanje > Web i e-pošta**. S tog mesta možete pristupiti detaljnijim postavkama programa.

The screenshot shows the ESET Endpoint Antivirus application window. On the left is a dark sidebar with icons for Status zaštite, Skeniranje računala, Aktualizacija, Podešavanje, Alati, and Pomoći i podrška. Below the sidebar is the text 'ENJOY SAFER TECHNOLOGY™'. The main area has a light background and contains the following information:

- Web i e-pošta** (with a back arrow icon)
- Zaštita web pristupa**: Aktivirano (green switch). Description: Otkrivanje i blokiranje web stranica sa zlonamjernim sadržajem. Gear icon for configuration.
- Zaštita klijenta e-pošte**: Aktivirano (green switch). Description: Skeniranje primljenih poruka e-pošte i slanje putem klijenta za e-poštu. Gear icon for configuration.
- Anti-Phishing zaštita**: Aktivirano (green switch). Description: Otkrivanje i blokiranje web stranica prijevara i phishinga. Gear icon for configuration.

At the bottom right of the main area are two buttons: 'Uvoz ili izvoz postavki' with a gear icon and 'Napredno podešavanje' with a gear icon.

Povezivost s internetom standardna je značajka osobnih računala. Nažalost, internet je postao glavni medij za prijenos zlonamjernog koda. Zbog toga je iznimno važno dobro razmisliti o postavkama [Zaštite web pristupa](#).

[Zaštita klijenta e-pošte](#) omogućuje nadzor komunikacije e-poštom koja se prima putem protokola POP3(S) i IMAP(S). Uz dodatni program za vaš klijent e-pošte, ESET Endpoint Antivirus omogućuje nadzor sve komunikacije iz klijenta e-pošte.

[Antiphishing zaštita](#) još je jedan sloj zaštite koji omogućuje povećanu razinu zaštite od nelegitimnih web stranica koje pokušavaju pridobiti lozinke i ostale osjetljive podatke. Antiphishing zaštita može se naći u oknu Podešenja pod Web i e-pošta. Za više informacija pogledajte članak [Antiphishing zaštita](#).

Možete deaktivirati modul web/antiphishing zaštite na neko vrijeme klikom stavke .

## Filtriranje protokola

Antivirusnu zaštitu za aplikacijske protokole daje modul za skeniranje ThreatSense u koji su integrirane sve napredne tehnike skeniranja zlonamjernih programa. Filtriranje protokola funkcioniра automatski, neovisno o web pregledniku ili klijentu e-pošte koji se koriste. Za uređivanje šifriranih (SSL) postavki idite na **Napredno podešavanje (F5) > Web i e-pošta > SSL/TLS**.

**Omogući filtriranje sadržaja protokola aplikacije** – Može se koristiti za deaktivaciju filtriranja protokola. Napominjemo da brojne komponente programa ESET Endpoint Antivirus (zaštita web pristupa, zaštita protokola za e-poštu, antiphishing zaštita, kontrola weba) ovisno o tome i neće raditi bez toga.

**Izuzete aplikacije** – Omogućuje vam izuzimanje specifičnih aplikacija od filtriranja protokola. Korisno kada

filtriranje protokola uzrokuje probleme u kompatibilnosti.

**Izuzete IP adrese** – Omogućuje vam izuzimanje specifičnih udaljenih adresa od filtriranja protokola. Korisno kada filtriranje protokola uzrokuje probleme u kompatibilnosti.

**IPv4 adrese i maska:**

- **192.168.0.10** – Time se dodaje IP adresa pojedinačnog računala na koje treba primijeniti pravilo.
- **192.168.0.1 do 192.168.0.99** – Unesite početnu i završnu IP adresu da biste odredili IP raspon (nekoliko računala) na koja se pravilo treba primijeniti.
- Podmreža (grupa računala) definira se putem IP adrese i maske. Na primjer, **255.255.255.0** je mrežna maska za prefiks **192.168.1.0/24**, što znači raspon adresa od **192.168.1.1** do **192.168.1.254**.

**IPv6 adresa i maska:**

- **2001:718:1c01:16:214:22ff:fec9:ca5** – IPv6 adresa pojedinačnog računala na koje treba primijeniti pravilo.
- **2002:c0a8:6301:1::1/64** – IPv6 adresa s prefiksom dužine 64 bita, što znači **2002:c0a8:6301:0001:0000:0000:0000 do 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff**

## Izuzete aplikacije

Da biste komunikaciju određenih aplikacija koje su svjesne mreže isključili iz filtriranja sadržaja, dodajte ih na ovaj popis. HTTP/POP3/IMAP komunikacija odabranih aplikacija neće se provjeravati da bi se pronašle prijetnje.

Preporučamo da ovo koristite u slučajevima gdje aplikacije ne rade ispravno dok je uključeno filtriranje protokola.

Aplikacije i servisi na koje utječe filtriranje protokola automatski će se prikazati nakon što kliknete mogućnost **Dodaj**.

**Uredi** – Uređivanje odabranih unosa na popisu.

**Ukloni** – Uklanjanje odabranih unosa s popisa.

Izuzete aplikacije

C:\Windows\System32\svchost.exe	C:\Program Files\Notepad++\notepad++.exe
---------------------------------	--

**Dodaj** **Uredi** **Izbriši** **Uvezi** **Izvezi**

**U redu** **Odustani**

## Izuzete IP adrese

IP adrese na ovom popisu izuzet će se iz filtriranja sadržaja protokola. HTTP/POP3/IMAP komunikacija s/na odabrane adrese neće se provjeravati da bi se pronašle prijetnje. Preporučujemo da tu mogućnost koristite samo za pouzdane adrese.

**Dodaj** – Kliknite ovu opciju da biste dodali IP adresu / raspon adresa / podmrežu udaljene točke na koju će se pravilo primijeniti.

**Uredi** – Uređivanje odabralih unosa na popisu.

**Ukloni** – Uklanjanje odabralih unosa s popisa.

## SSL/TLS

ESET Endpoint Antivirus može provjeriti prijetnje u komunikaciji koje koriste SSL protokol. Možete koristiti različite načine skeniranja za pregled komunikacije s SSL zaštitom uz pouzdane certifikate, nepoznate certifikate ili certifikate koji su isključeni iz provjere komunikacije s SSL zaštitom.

**Aktiviraj filtriranje SSL/TLS protokola** – filtriranje protokola aktivirano je prema standardnim postavkama.

Možete deaktivirati filtriranje SSL/TLS protokola u izborniku **Napredno podešavanje > Web i e-pošta > SSL/TLS** ili putem pravila. Ako je filtriranje protokola deaktivirano, program neće skenirati komunikaciju putem SSL protokola.

**Način filtriranj SSL/TLS protokola** dostupan je u sljedećim mogućnostima:

Način filtriranja	Opis
<b>Automatski način rada</b>	Standardni način rada skenirat će samo odgovarajuće aplikacije kao što su web preglednici i klijenti e-pošte. Možete ga zaobići odabirom aplikacija za koje će se njihova komunikacija skenirati.

Način filtriranja	Opis
<b>Interaktivni način</b>	Ako unesete novu web stranicu s SSL- zaštitom (s nepoznatim certifikatom), prikazat će se <a href="#">prozor za odabir radnje</a> . Taj način rada omogućuje vam stvaranje popisa SSL certifikata / aplikacija koji će se izuzeti od skeniranja.
<b>Način rada prema zadanim pravilima</b>	Odaberite ovu opciju da biste skenirali svu komunikaciju s SSL zaštitom osim komunikacije koja je zaštićena certifikatima izuzetima od provjere. Ako se uspostavi nova komunikacija koja koristi nepoznati potpisani certifikat, nećete primiti obavijest i komunikacija će se automatski filtrirati. Kada pristupite serveru s nepouzdanim certifikatom koji ste sami označili kao pouzdan (nalazi se na popisu pouzdanih certifikata), komunikacija se sa serverom dopušta i sadržaj se komunikacijskog kanala filtrira.

**Popis aplikacija filtriranih SSL/TLS aplikacija** može se upotrebljavati za prilagodbu ponašanja programa ESET Endpoint Antivirus za određene aplikacije.

**Popis poznatih certifikata** omogućuje vam da prilagodite ponašanje programa ESET Endpoint Antivirus za određene SSL certifikate.

**Izuzmi komunikaciju s pouzdanim domenama** – Kad se opcija aktivira, komunikacija s pouzdanim domenama bit će izuzeta od provjere. Povjerljivost domena određuje ugrađeni popis pouzdanih stavki.

**Blokiraj šifriranu komunikaciju koja koristi zastarjeli protokol SSL v2** – Automatski će se blokirati komunikacija koja koristi stariju verziju SSL protokola.

**i** Adrese se neće filtrirati ako je aktivirana postavka **Izuzmi komunikaciju s pouzdanim domenama** i ako se domena smatra pouzdanom.

## Verifikacijski (root) certifikat

**Root certifikat** – Da bi SSL komunikacija ispravno radila u vašim preglednicima/klijentima e-pošte, važno je da root certifikat za ESET dodate na popis poznatih root certifikata (izdavača). Stoga treba aktivirati mogućnost **Dodaj verifikacijski (root) certifikat u poznate preglednike**. Odaberite tu mogućnost da biste ESET-ov verifikacijski (root) certifikat automatski pridodali poznatim preglednicima (npr. Opera, Firefox). Taj se certifikat automatski pridodaje preglednicima koji koriste pohranu sistemskih certifikata (npr. Internet Explorer).

Da biste certifikat primijenili na preglednike koji nisu podržani, kliknite **Pregled certifikata > Detalji > Kopiraj u datoteku**, a zatim ga ručno uvezite u preglednik.

## Valjanost certifikata

**Ako nije moguće utvrditi pouzdanost certifikata** – u nekim slučajevima certifikat web stranice nije moguće provjeriti s pomoću pouzdanog izvora root certifikata (TRCA). To znači da je certifikat netko potpisao (na primjer, administrator web servera ili manje tvrtke) te postavljanje tog certifikata kao pouzdanog ne predstavlja uvijek rizik. Većina velikih tvrtki (kao što su banke) upotrebljava certifikat s TRCA potpisom. Ako je odabrana opcija **Pitaj o valjanosti certifikata** (standardna postavka), od korisnika će se zatražiti da odabere radnju koja će se provesti prilikom uspostavljanja šifrirane komunikacije. Možete odabrati opciju **Blokiraj komunikaciju koja upotrebljava certifikat** da bi se svaki put prekinule šifrirane veze s web stranicama koje upotrebljavaju certifikate koji nisu provjereni.

**Ako je certifikat oštećen** – to znači da je certifikat neispravno potpisano ili oštećeno. U tom slučaju preporučujemo da opcija **Blokiraj komunikaciju koja upotrebljava certifikat** ostane odabранa. Ako se

odabere opcija **Pitaj o valjanosti certifikata**, od korisnika će se zatražiti da odabere radnju koja će se provesti prilikom uspostavljanja šifrirane komunikacije.

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

- [Obavijesti o certifikatima u ESET-ovim programima](#)
- [Prilikom posjećivanja web stranica prikazuje se "Šifrirani mrežni promet: certifikat nije vjerodostojan"](#)

## Certifikati

Da bi SSL komunikacija ispravno radila u vašim preglednicima/klijentima e-pošte, važno je da verifikacijski (root) certifikat za ESET dodate na popis poznatih verifikacijskih (root) certifikata (izdavača). Stoga treba aktivirati mogućnost **Dodaj verifikacijski (root) certifikat u poznate preglednike**. Odaberite tu mogućnost da biste ESET-ov verifikacijski (root) certifikat automatski pridodali poznatim preglednicima (npr. Opera, Firefox). Taj se certifikat automatski pridaje preglednicima koji koriste pohranu sistemskih certifikata (npr. Internet Explorer). Da biste certifikat primjenili na preglednike koji nisu podržani, kliknite **Pregled certifikata > Detalji > Kopiraj u datoteku**, a zatim ga ručno uvezite u preglednik.

U nekim slučajevima certifikat se ne može provjeriti putem vjerodostojnog izvora verifikacijskog (root) certifikata (npr. VeriSign). To znači da je certifikat netko samopotpisao (npr. administrator web servera ili manje tvrtke) te postavljanje tog certifikata kao pouzdanog ne predstavlja uvijek rizik. Većina velikih tvrtki (npr. banke) koristi certifikat s TRCA potpisom. Ako je odabrana mogućnost **Pitaj o valjanosti certifikata** (standardna postavka), korisniku će se prikazati odzivnik za odabir radnje koja će se poduzeti prilikom uspostavljanja šifrirane komunikacije. Prikazat će se dijaloški okvir za odabir radnje u kojem certifikat možete označiti kao pouzdan ili izuzet. Ako se certifikat ne nalazi na TRCA popisu, prozor će biti crven. Ako se certifikat nalazi na TRCA popisu, prozor će biti zelen.

Možete odabrati mogućnost **Blokiraj komunikaciju koja koristi certifikat** da bi se svaki put prekinula šifrirana veza s web stranicom koja koristi certifikat koji nije provjeren.

Ako je certifikat nevaljan ili oštećen, znači da je istekao ili nije ispravno samopotpisani. U tom slučaju preporučujemo da blokirate komunikaciju koja koristi taj certifikat.

## Šifrirani mrežni promet

Ako je računalo konfiguirano za SSL skeniranje protokola, prikazuje se dijaloški okvir s upitom o dalnjim akcijama u sljedeće dvije situacije:

Prvo, ako web stranica upotrebljava certifikat koji se ne može potvrditi ili neispravan certifikat, a ESET Endpoint Antivirus je konfiguriran da u takvim slučajevima pita korisnika (prema standardnim postavkama odabrana je opcija "da" za certifikate koji se ne mogu potvrditi i "ne" za neispravne certifikate), otvorit će se prozor u kojem će se zatražiti da **dopustite ili blokirate** vezu. Ako se certifikat ne nalazi u spremištu Trusted Root Certification Authorities store (TRCA), smatra se da nije vjerodostojan.

Drugo, ako je mogućnost **Način filtriranja SSL protokola** postavljena na **Interaktivni način**, otvorit će se dijaloški okvir za svaku web stranicu u kojem će se od vas zatražiti da odaberete mogućnost **Skeniraj** ili **Ignoriraj** za promet. Neke aplikacije provjeravaju je li njihov SSL promet promijenjen i je li ga netko pregledavao pa u takvim slučajevima ESET Endpoint Antivirus mora **ignorirati** taj promet da bi aplikacija nastavila raditi.

- Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
- [Obavijesti o certifikatima u ESET-ovim programima](#)
  - [Prilikom posjećivanja web stranica prikazuje se "Šifrirani mrežni promet: certifikat nije vjerodostojan"](#)

U oba slučaja korisnik može odabrati upamćivanje odabrane akcije. Spremljene akcije pohranjuju se na [Popisu poznatih certifikata](#).

## Popis poznatih certifikata

**Popis poznatih certifikata** može se koristiti za prilagodbu ponašanja programa ESET Endpoint Antivirus za određene SSL certifikate i pamćenje odabrane akcije ako je odabrana mogućnost **Interaktivni način rada** u odjelu **Način filtriranja SSL/TLS protokola**. Popis se može pregledavati i uređivati u izborniku **Napredno podešavanje** (F5) > **Web i e-pošta** > **SSL/TLS** > **Popis poznatih certifikata**.

Prozor **Popis poznatih certifikata** sastoji se od:

### Stupci

**Naziv** – Naziv certifikata.

**Izdavač certifikata** – Naziv izdavača certifikata.

**Primatelj certifikata** – Polje primatelja identificira entitet koji je povezan s javnim ključem spremlijenim u polje javnog ključa primatelja.

**Pristup** – odaberite **Dopusti** ili **Blokiraj kao Radnju pristupa** da biste dopustili/blokirali komunikaciju zaštićenu ovim certifikatom neovisno o pouzdanosti. Odaberite **Automatski** kako biste dopustili pouzdane certifikate i dobili upit za nepouzdane. Odaberite **Pitaj** kako bi program uvijek pitao korisnika što učiniti.

**Skeniranje** – Odaberite **Skeniraj** ili **Ignoriraj** kao **Radnju skeniranja** kako biste skenirali ili ignorirali komunikaciju zaštićenu ovim certifikatom. Odaberite **Automatski** za skeniranje u automatskom načinu rada i upit u interaktivnom načinu rada. Odaberite **Pitaj** kako bi program uvijek pitao korisnika što učiniti.

### Kontrolni elementi

**Dodaj** – Certifikat se može ručno učitati kao datoteka s ekstenzijom **.cer**, **.crt** ili **.pem**. Kliknite **Datoteka** da biste učitali lokalni certifikat ili kliknite **URL** da biste odredili lokaciju certifikata na mreži.

**Uredi** – Odaberite certifikat koji želite konfigurirati i kliknite **Uredi**.

**Izbrisí** – Odaberite certifikat koji želite izbrisati i kliknite **Ukloni**.

**U redu/Otkaži** – Kliknite **U redu** ako želite spremiti promjene ili **Odustani** da biste izašli bez spremanja.

## Popis filtriranih SSL/TLS aplikacija

**Popis filtriranih SSL/TLS aplikacija** može se koristiti za prilagodbu ponašanja programa ESET Endpoint Antivirus za određene aplikacije i pamćenje odabranih radnji ako je odabrana mogućnost **Interaktivni način rada** u odjelu **Način filtriranja SSL/TLS protokola**. Popis se može pregledavati i uređivati u izborniku **Napredno podešavanje** (F5) > **Web i e-pošta** > **SSL/TLS** > **Popis filtriranih SSL/TLS aplikacija**.

Prozor **Popis filtriranih SSL/TLS aplikacija** sastoji se od sljedećeg:

## Stupci

### Aplikacija – Naziv aplikacije.

**Radnja skeniranja** – Odaberite **Skeniraj** ili **Zanemari** da biste skenirali ili ignorirali komunikaciju. Odaberite **Automatski** za skeniranje u automatskom načinu rada i upit u interaktivnom načinu rada. Odaberite **Pitaj** kako bi program uvijek pitao korisnika što učiniti.

## Kontrolni elementi

**Dodaj** – Dodajte filtriranu aplikaciju.

**Uredi** – Odaberite certifikat koji želite konfigurirati i kliknite **Uredi**.

**Izbriši** – Odaberite certifikat koji želite izbrisati i kliknite **Ukloni**.

**U redu/Otkaži** – Kliknite **U redu** ako želite spremiti promjene ili **Odustani** ako želite izaći bez spremanja.

## zaštita klijenta e-pošte

Integracija programa ESET Endpoint Antivirus s klijentom e-pošte povećava razinu aktivne zaštite od zlonamjernog koda u porukama e-pošte. Ako je vaš klijent e-pošte podržan, ta se integracija može aktivirati u programu ESET Endpoint Antivirus. Nakon integracije u klijent e-pošte alatna traka programa ESET Endpoint Antivirus umeće se izravno u klijent e-pošte za učinkovitiju zaštitu e-pošte. Postavke integracije nalaze se u odjeljku **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita klijenta e-pošte** > **Klijenti e-pošte**.

The screenshot shows the 'Klijenti e-pošte' (Clients) configuration screen in the ESET Endpoint Antivirus software. On the left, there's a sidebar with navigation links: MODUL DETEKCIJE (2), NADOGRADNJA (2), MREŽNA ZAŠTITA, WEB I E-POŠTA (3), Zaštita klijenta e-pošte (4), KONTROLA UREĐAJA (2), ALATI (3), and KORISNIČKO SUČELJE (1). The main area has a title 'Klijenti e-pošte'. Under 'INTEGRACIJA S KLJIENTIMA E-POŠTE', there are four checkboxes: 'Integriraj u Microsoft Outlook' (checked), 'Integriraj u Outlook Express / Windows Mail' (checked), 'Integriraj u Windows Live Mail' (checked), and 'Isključi provjeru pri promjeni sadržaja ulazne pošte' (unchecked). Below that is a section titled 'E-POŠTA ZA SKENIRANJE' with four checkboxes: 'Aktiviraj zaštitu e-pošte klijentskim programskim dodacima' (checked), 'Primljene poruke e-pošte' (checked), 'Poslane poruke e-pošte' (checked), and 'Pročitane poruke e-pošte' (checked). At the bottom, there's a 'RADNJA KOJU TREBA PROVESTI NA PORUKAMA E-POŠTE S PRIJETNJAMA' section with a dropdown menu set to 'Premiesti poruku e-pošte u m...', a 'U redu' button with a shield icon, and an 'Odustani' button.

## Integracija s klijentima e-pošte

Trenutačno su, između ostalih, podržani sljedeći klijenti e-pošte: [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) i [Windows Live Mail](#). Zaštita e-pošte funkcioniра као додатак за те програме. Главна је предност додатка то да он не овиси о протоколу који се користи. Када кlijent e-pošte прими шифрирану поруку, она се дешифрира и шалје скенеру вируса. Потпуни попис подрžаних klijenata e-pošte и njihovih verzija потражите у слjedećем [članku ESET-ove baze znanja](#).

Укључите опцију **Deaktiviraj provjeru pri promjeni sadržaja ulazne pošte** ако примјетите да sustav функционира спорије када дохваћа поруке e-pošte.

## E-pošta za skeniranje

**Aktiviraj zaštitu e-pošte klijentskim dodacima** – Када је деактивирана, искључена је заштита klijentskim podacima за e-poštu.

**Primljene poruke e-pošte** – провјерава primljene poruke e-pošte када је омогућено.

**Poslane poruke e-pošte** – провјерава poslane poruke e-pošte када је омогућено.

**Pročitane poruke e-pošte** – провјерава pročitane poruke e-pošte када је омогућено.

**i** Preporučujemo да активирате опцију **Aktiviraj zaštitu e-pošte klijentskim dodacima**. Чак и ако интеграција nije активирана или функционална, значјака [Filtriranje protokola](#) (IMAP/IMAPS и POP3/POP3S) sveједно штити комуникацију e-poштом.

## Akcija koju treba izvesti na zaraženoj poruci e-pošte

**Bez radnje** – ako je aktivirana ova opcija, program će prepoznavati zaražene privitke, ali neće poduzimati nikakve radnje na e-pošti.

**Izbriši poruku e-pošte** – Program će obavještavati korisnika o infiltracijama i izbrisati poruku.

**Premjesti poruku e-pošte u mapu s izbrisanim stavkama** – Zaražene poruke e-pošte automatski će se premjestiti u mapu Izbrisane stavke.

**Premjesti poruku e-pošte u mapu** – Zaražene poruke e-pošte automatski će se premjestiti u navedenu mapu.

**Mapa** – Odredite prilagođenu mapu u koju želite premjestiti zaražene poruke e-pošte nakon što se otkriju.

**Ponovi skeniranje nakon nadogradnje** – ponovno skenira zaražene poruke e-pošte nakon nadogradnje modula detekcije kada je omogućeno.

**Prihvati rezultate skeniranja iz ostalih modula** – omogućuje modulu zaštite e-pošte da upotrebljava rezultate skeniranja primljene od drugih modula zaštite umjesto ponovnog skeniranja.

## Protokoli e-pošte

IMAP i POP3 su najčešće korišteni protokoli za primanje e-pošte u aplikacijama klijenata e-pošte. Internet Message Access Protocol (IMAP) još je jedan internetski protokol za dohvat e-pošte. IMAP ima određene prednosti u odnosu na POP3, npr. višestruki klijenti mogu se istovremeno povezati s istim poštanskim sandučićem i održavati informacije o stanju poruke, primjerice je li poruka pročitana, je li na nju odgovoren ili je izbrisana. Modul zaštite koji omogućuje tu kontrolu automatski se pokreće prilikom pokretanja sustava i ostaje aktivan u memoriji.

ESET Endpoint Antivirus omogućuje zaštitu tih protokola neovisno o korištenom klijentu e-pošte i bez potrebe za ponovnom konfiguracijom klijenta e-pošte. Prema standardnim postavkama sva se komunikacija putem protokola POP3 i IMAP skenira, neovisno o standardnim brojevima portova protokola POP3/IMAP.

Protokol MAPI nije skeniran. Međutim, komunikacija s Microsoft Exchange serverom može se skenirati integracijskim modulom u klijentima e-pošte kao što je Microsoft Outlook.

Preporučujemo da aktivirate opciju **Aktiviraj zaštitu e-pošte filtriranjem protokola**. Da biste konfiguirali provjeru protokola IMAP/IMAPS i POP3/POP3S, idite na Napredno podešavanje > **Web i e-pošta > Zaštita klijenta e-pošte > Protokoli e-pošte**.

ESET Endpoint Antivirus podržava i skeniranje protokola IMAPS (585, 993) i POP3S (995) koji koriste šifrirani kanal za prijenos informacija između servera i klijenata. ESET Endpoint Antivirus provjerava komunikaciju koja koristi protokole SSL (Secure Socket Layer) i TLS (Transport Layer Security). Program skenira samo promet e-pošte na portovima definiranim u opciji **Portovi koje koristi protokol IMAPS/POP3S**, neovisno o verziji operacijskog sustava. Prema potrebi se mogu dodati i drugi komunikacijski portovi. Višestruke brojeve portova potrebno je razgraničiti zarezima.

Šifrirana komunikacija bit će skenirana prema standardnoj postavci. Da biste prikazali podešavanje skenera, idite na SSL/TLS u odjeljku Napredno podešavanje, kliknite **Web i e-pošta > SSL/TLS** i aktivirajte opciju **Aktiviraj filtriranje SSL/TLS protokola**.

The screenshot shows the ESET Endpoint Antivirus interface. On the left, a sidebar lists several modules: MODUL DETEKCIJE (2), NADOGRADNJA (2), MREŽNA ZAŠTITA, WEB I E-POŠTA (3), Zaštita klijenta e-pošte (4), KONTROLA UREĐAJA (2), ALATI (3), and KORISNIČKO SUČELJE (1). The main panel is titled 'Napredno podešavanje' and focuses on 'Zaštita klijenta e-pošte'. It includes sections for 'Klijenti e-pošte' and 'Protokoli e-pošte'. Under 'Protokoli e-pošte', there is a checkbox for 'Aktiviraj zaštitu e-pošte filtriranjem protokola'. Below this are sections for 'PODEŠAVANJE IMAP SKENERA' and 'PODEŠAVANJE IMAPS SKENERA', each with a checkbox for 'Aktiviraj provjeru IMAP protokola'. The 'IMAPS SKENERA' section also includes a field for 'Portovi koje koristi IMAPS protokol' with the value '585, 993'. At the bottom are buttons for 'Standardno', 'U redu' (with a shield icon), and 'Odustani'.

## Upozorenja i obavijesti e-pošte

Mogućnosti za tu funkciju dostupne su pod stavkom **Napredno podešavanje > Web i e-pošta > Zaštita klijenta e-pošte Upozorenja i obavijesti**.

Nakon provjere, poruci e-pošte može se dodati obavijest s rezultatima skeniranja. Možete odabrati opciju **Dodaj oznake primljenim i pročitanim porukama e-pošte** ili **Dodaj oznake poslanim porukama e-pošte**. Imajte na umu da se u rijetkim slučajevima oznake mogu izostaviti u problematičnim HTML porukama ili ako ih zlonamjerni programi krivotvore. Oznake se mogu dodati primljenoj i pročitanoj e-pošti, poslanoj e-pošti ili objema. Dostupne su sljedeće opcije:

- **Nikad** – Neće se dodavati nikakve obavijesti uz poruke.
- **Kada se otkrije prijetnja** – Kao provjerene će se označavati samo one poruke koje sadrže zlonamjerni softver (standardna postavka).
- **Za svu e-poštu kada se skenira** – Program će dodati oznake svim skeniranim porukama e-pošte.

**Ažuriraj naslov poslane e-pošte** – deaktivirajte ovo ako ne želite da zaštita e-pošte u predmet zaražene poruke e-pošte dodaje upozorenje o virusu. Ova funkcija omogućuje jednostavno filtriranje zaražene e-pošte na temelju naslova (ako to podržava program za e-poštu). Ona povećava i vjerodostojnost primatelja te, ako se otkrije infiltracija, daje važne informacije o razini prijetnje dane poruke e-pošte ili pošiljatelja.

**Tekst koji se dodaje u naslov zaražene poruke e-pošte** – Uredite predložak ako želite promijeniti format prefiksa koji se dodaje predmetu zaražene poruke e-pošte. Ova funkcija zamjenit će predmet poruke "Hello" u sljedeći format: "[prijetnja %DETECTIONNAME%] Hello". Varijabla %DETECTIONNAME% predstavlja otkrivenu prijetnju.

# Integracija s klijentima e-pošte

Trenutačno su, između ostalih, podržani sljedeći klijenti e-pošte: [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) i Windows Live Mail. Zaštita e-pošte funkcioniра kao dodatak za te programe. Glavna je prednost dodatka to da on ne ovisi o protokolu koji se koristi. Kada klijent e-pošte primi šifriranu poruku, ona se dešifrira i šalje skeneru virusa. Potpuni popis podržanih klijenata e-pošte i njihovih verzija potražite u sljedećem [članku ESET-ove baze znanja](#).

## Alatna traka za Microsoft Outlook

Zaštita programa Microsoft Outlook radi kao dodatni modul. Nakon instalacije programa ESET Endpoint Antivirus ova alatna traka na kojoj se nalazi mogućnosti antivirusne/ zaštite dodaje se programu Microsoft Outlook:

**ESET Endpoint Antivirus** – Ako kliknete ikonu, otvorit će se glavni prozor programa ESET Endpoint Antivirus.

**Ponovno skeniraj poruke** – Omogućuje ručno pokretanje provjere e-pošte. Možete odrediti koje poruke želite skenirati te ponovno pokrenuti skeniranje primljene e-pošte. Dodatne informacije potražite u odjeljku [Zaštita klijenta e-pošte](#).

**Podešavanje skenera** – Prikazuje opcije podešavanja [zaštite klijenta e-pošte](#).

## Alatna traka za Outlook Express i Windows Mail

Zaštita programa Outlook Express i Windows Mail radi kao dodatni modul. Nakon instalacije programa ESET Endpoint Antivirus ova alatna traka na kojoj se nalazi mogućnosti antivirusne/ zaštite dodaje se programu Outlook Express ili Windows Mail:

**ESET Endpoint Antivirus** – Ako kliknete ikonu, otvorit će se glavni prozor programa ESET Endpoint Antivirus.

**Ponovno skeniraj poruke** – Omogućuje ručno pokretanje provjere e-pošte. Možete odrediti koje poruke želite skenirati te ponovno pokrenuti skeniranje primljene e-pošte. Dodatne informacije potražite u odjeljku [Zaštita klijenta e-pošte](#).

**Podešavanje skenera** – Prikazuje opcije podešavanja [zaštite klijenta e-pošte](#).

## Korisničko sučelje

**Prilagodba izgleda** – Izgled alatne trake može se promijeniti za vaš klijent e-pošte. Poništite mogućnost prilagodbe izgleda neovisno o parametrima programa e-pošte.

**Prikaži tekst** – Prikazuje opise ikona.

**Tekst udesno** – Opisi opcija pomicu se s dna na desnu stranu ikona.

**Veličine ikone** – Prikazuje velike ikone za mogućnosti izbornika.

# Dijaloški okvir s potvrdom

Ta obavijest služi kao potvrda da korisnik zaista želi izvršiti odabranu akciju čime bi se trebale eliminirati moguće pogreške.

S druge strane, dijaloški okvir nudi i mogućnost deaktiviranja potvrda.

## Ponovno skeniranje poruka

Antivirusna alatna traka sustava ESET Endpoint Antivirus integrirana u klijente e-pošte korisnicima omogućuje da navedu nekoliko mogućnosti provjere poruka e-pošte. Mogućnost **Ponovno skeniraj poruke** nudi dva načina skeniranja:

**Sve poruke u trenutačnoj mapi** – Skenira poruke u mapi koja je trenutačno prikazana.

**Samo odabrane poruke** – Skenira samo one poruke koje je korisnik označio.

Potvrdni okvir **Ponovno skeniraj već skenirane poruke** korisniku nudi mogućnost pokretanja novog skeniranja poruka koje su ranije već skenirane.

## Zaštita web pristupa

Povezivost s internetom standardna je značajka osobnih računala. Nažalost, postala je i glavni medij za prijenos zlonamjernog koda. Zaštita web pristupa vrši se nadgledanjem komunikacije između internetskih preglednika i udaljenih servera te je u skladu s pravilima o HTTP-u (Hypertext Transfer Protocol, protokol prijenosa hiperteksta) i HTTPS-u (šifrirana komunikacija).

Pristup web stranicama za koje se zna da sadrže zlonamjerni sadržaj blokira se prije preuzimanja sadržaja. Sustav za skeniranje ThreatSense skenira sve ostale web stranice nakon njihovog učitavanja i blokira ih ako otkrije zlonamjerni sadržaj. Zaštita web pristupa nudi dvije razine zaštite, blokiranje prema popisu spam adresa i blokiranje prema sadržaju.

Preporučujemo da obavezno aktivirate mogućnost Zaštita web pristupa. Toj mogućnosti može se pristupiti u glavnom prozoru programa ESET Endpoint Antivirus odlaskom na stavku **Podešavanje > Internetska zaštita > Zaštita web pristupa**.

**ESET ENDPOINT ANTIVIRUS**

STATUS ZAŠTITE

SKENIRANJE RAČUNALA

AKTUALIZACIJA

PODEŠAVANJE

ALATI

POMOĆ I PODRŠKA

ENJOY SAFER TECHNOLOGY™

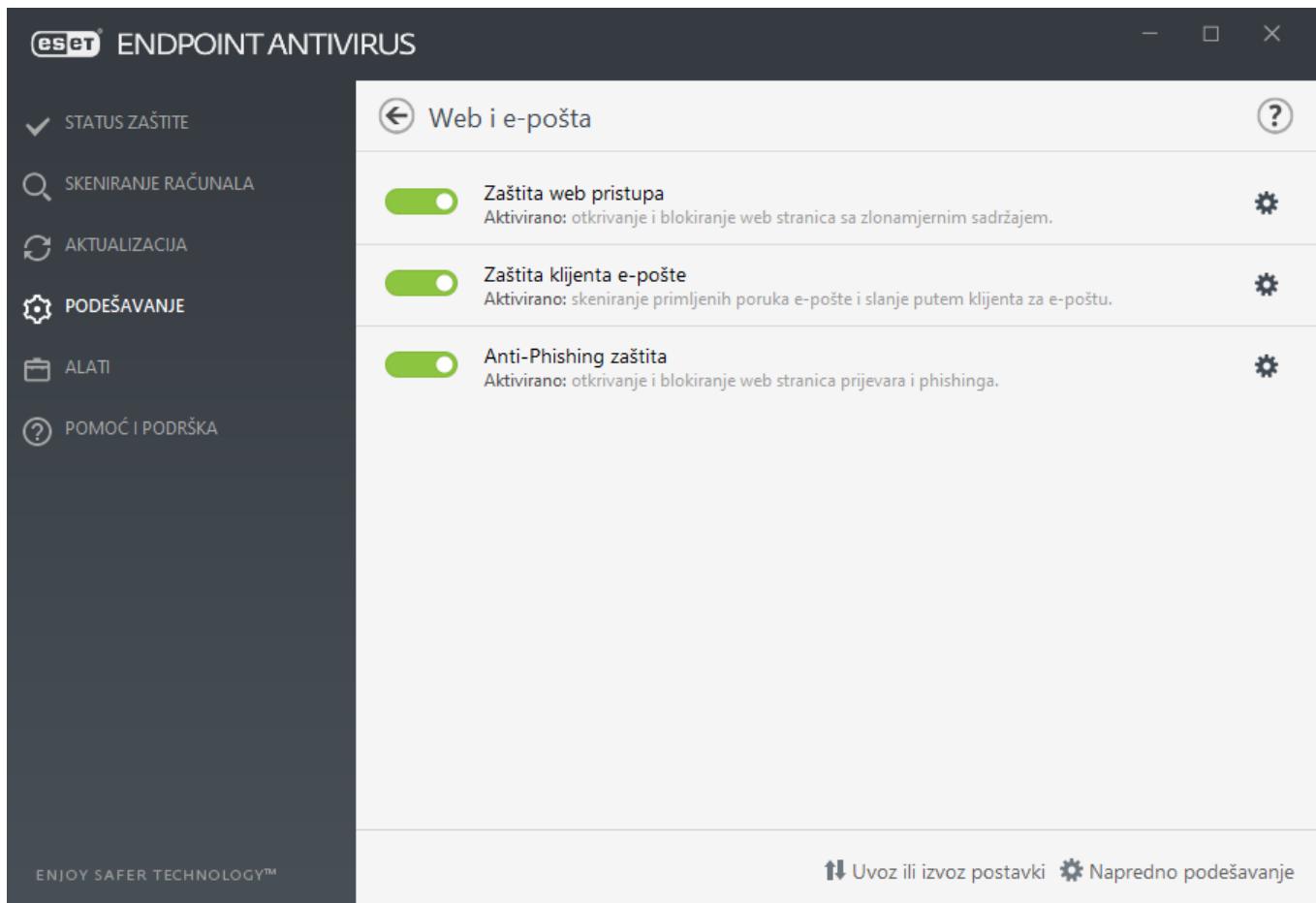
Web i e-pošta

Zaštita web pristupa  
Aktivirano: otkrivanje i blokiranje web stranica sa zlonamjernim sadržajem.

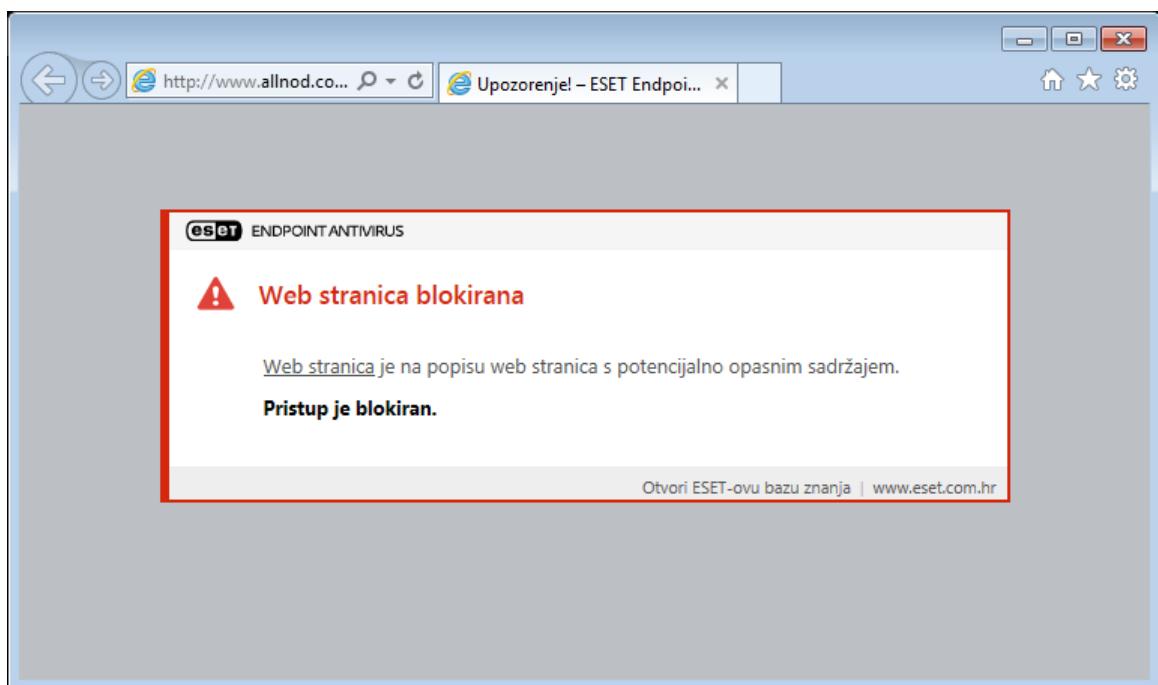
Zaštita klijenta e-pošte  
Aktivirano: skeniranje primljenih poruka e-pošte i slanje putem klijenta za e-poštu.

Anti-Phishing zaštita  
Aktivirano: otkrivanje i blokiranje web stranica prijevara i phishinga.

Uvoz ili izvoz postavki | Napredno podešavanje



Zaštita web pristupa prikazat će sljedeću poruku u vašem pregledniku kad je web stranica blokirana:



Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

- [Deblokirajte sigurnu stranicu na pojedinačnoj radnoj stanici u programu ESET Endpoint Antivirus](#)
- [Deblokirajte sigurnu stranicu na krajnja točki pomoću ESET Security Management Center](#)

Sljedeće su mogućnosti dostupne pod **Napredno podešavanje (F5) > Web i e-pošta > Zaštita web pristupa**:

- **Osnovno** – Za aktivaciju ili deaktivaciju ove funkcije u Naprednom podešavanju.
- **Web protokoli** – omogućuje konfiguriranje nadzora standardnih protokola koje koristi većina internetskih preglednika.
- **Upravljanje URL adresama** – omogućuje navođenje URL adresa koje želite blokirati, dopustiti ili izuzeti od provjere.
- **ThreatSense parametri** – Napredno podešavanje virusnog skenera omogućuje vam konfiguriranje postavki poput vrsta objekata za skeniranje (e-pošta, arhive itd.), metoda otkrivanja za zaštitu web pristupa itd.

Napredno podešavanje

MODUL DETEKCIJE 2

NADOGRADNJA 2

MREŽNA ZAŠTITA

WEB I E-POŠTA 3

Zaštita klijenta e-pošte 4

**Zaštita web pristupa**

Anti-Phishing zaštita

KONTROLA UREĐAJA 2

ALATI 2

KORISNIČKO SUČELJE 1

OSNOVNO

Aktiviraj zaštitu web pristupa

Aktiviraj napredno skeniranje skripta preglednika

WEB PROTOKOLI

UPRAVLJANJE URL ADRESAMA

THREATSENSE PARAMETRI

Standardno

U redu

Odustani

## Napredno podešavanje zaštite web pristupa

Sljedeće su opcije dostupne pod **Napredno podešavanje (F5) > Web i e-pošta > Zaštita web pristupa > Osnovno**:

**Aktiviraj zaštitu web pristupa** – Nakon deaktivacije te opcije [zaštita web pristupa](#) i [anti-phishing zaštita](#) neće raditi.

**Aktiviraj napredno skeniranje skripta preglednika** – Nakon aktivacije modul detekcije pregledat će sve programe JavaScript koje pokrenu internetski preglednici.

**i** Preporučujemo da obavezno ostavite aktiviranu mogućnost Zaštita web pristupa.

# Web protokoli

ESET Endpoint Antivirus prema standardnim je postavkama konfiguriran za nadzor HTTP protokola, koji koristi većina internetskih preglednika.

## Podešavanje HTTP skenera

HTTP promet uvijek se nadzire na svim portovima za sve aplikacije.

## Podešavanje HTTPS skenera

ESET Endpoint Antivirus podržava provjeru HTTPS protokola. HTTPS komunikacija koristi šifrirani kanal za prijenos informacija između servera i klijenta. ESET Endpoint Antivirus provjerava komunikaciju pomoću protokola SSL (Secure Socket Layer) i TLS (Transport Layer Security). Program skenira promet samo na portovima (443, 0-65535) definiranim pod **Portovi koje koristi HTTPS protokol**, neovisno o verziji operacijskog sustava.

Šifrirana komunikacija bit će skenirana prema standardnoj postavci. Da biste prikazali podešavanje skenera, idite na [SSL/TLS](#) u odjeljku Napredno podešavanje, kliknite **Web i e-pošta > SSL/TLS** i aktivirajte opciju **Aktiviraj filtriranje SSL/TLS protokola**.

## Upravljanje URL adresama

U odjeljku za upravljanje URL adresama omogućeno je navođenje HTTP adresa koje želite blokirati, omogućiti ili izuzeti od skeniranja.

Opcija [\*\*Aktiviraj filtriranje SSL/TLS protokola\*\*](#) mora biti označena ako želite filtrirati HTTPS adrese uz HTTP web stranice. U suprotnom će se dodati samo domene posjećenih HTTPS stranica, ali ne i puna URL adresa.

Web stranice s **popisa blokiranih adresa** neće biti dostupne, osim ako su uključene na **popis dopuštenih adresa**. Web stranice s **popisa adresa izuzetnih iz skeniranja sadržaja** bit će dostupne bez skeniranja za zlonamjernim kodom.

Ako želite blokirati sve HTTP adrese osim adresa prisutnih na aktivnom **popisu dopuštenih adresa**, dodajte \* na aktivni **popis blokiranih adresa**.

Na tim popisima moguća je upotreba posebnih simbola \* (zvjezdica) i ? (upitnik). Zvjezdica zamjenjuje bilo koji niz znakova, a upitnik zamjenjuje bilo koji pojedini znak. Osobitu pozornost treba obratiti prilikom određivanja izuzetih adresa jer bi popis trebao sadržavati samo pouzdane i sigurne adrese. Treba obratiti pozornost i na to da se simboli \* i ? pravilno koriste na popisu. Pogledajte [Dodavanje HTTP adrese / maske domene](#) kako biste saznali kako sigurno uskladiti čitavu domenu zajedno sa svim poddomenama. Da biste aktivirali popis, odaberite mogućnost **Aktivan popis**. Ako želite primiti obavijest kada upišete adresu s trenutačnog popisa, aktivirajte mogućnost **Obavijesti prilikom primjene**.

**i** Upravljanje URL adresama omogućava i blokiranje ili dopuštanje otvaranja posebnih vrsta datoteka tijekom pregledavanja weba. Na primjer, ako ne želite dopustiti otvaranje izvršnih datoteka, na padajućem izborniku odaberite popis na kojem želite blokirati te datoteke, a zatim unesite masku "\*\*.exe".

**i** Adrese se neće filtrirati ako je aktivirana postavka **Web i e-pošta > SSL/TLS > Izuzmi komunikaciju s pouzdanim domenama** i ako se domena smatra pouzdanom.

Popis adresa

Naziv popisa	Vrste adresa	Opis popisa
Popis dopuštenih adresa	Dopušteno	
Popis blokiranih adresa	Blokirano	
Popis adresa izuzetih od skeniranja sadržaja	Pronađeni zlonamjerni p...	

Dodaj Uredi Izbrisí Uvezi Izvezi

Dodajte zamjenski znak (\*) na popis blokiranih adresa da biste blokirali sve URL-ove osim onih koji se nalaze na popisu dopuštenih adresa.

U redu Odustani

## Kontrolni elementi

**Dodaj** – Stvara novi popis uz one koji su prethodno definirani. To može biti posebno korisno ako želite logički podijeliti različite skupine adresa. Primjerice, jedan popis blokiranih adresa može sadržavati adrese vanjskog javnog popisa spam adresa, a drugi može sadržavati vaš osobni popis spam adresa, čime je lakše ažurirati vanjski popis dok vaš ostaje netaknut.

**Uredi** – Uređuje postojeće popise. Upotrijebite da biste dodali ili uklonili adrese.

**Izbriši** – Briše postojeće popise. To je dostupno samo za popise stvorene stavkom **Dodaj**, ne i za standardne.

## Popis URL adresa

U ovom odjeljku možete zadati popis HTTP adresa koje će biti blokirane, dopuštene ili izuzete iz provjere.

Prema standardnim postavkama dostupna su sljedeća tri popisa:

- **Popis adresa koje su izuzete od provjere** – Za adrese s ovog popisa neće se izvršiti provjera zlonamjernog koda.
- **Popis dopuštenih adresa** – Ako je aktivirana značajka Dopusti pristup samo HTTP adresama s popisa dopuštenih adresa, a popis blokiranih adresa sadrži \* (univerzalni znak), korisniku će biti dopušten pristup samo adresama koje je naveo na tom popisu. Adrese s popisa bit će dopuštene čak i ako se nalaze na popisu blokiranih adresa.
- **Popis blokiranih adresa** – Korisnik neće moći pristupati adresama s popisa ako iste nisu na popisu dopuštenih adresa.

Kliknite **Dodaj** da biste stvorili novi popis. Kliknite **Izbriši** da biste izbrisali odabrane popise.

Popis adresa

Naziv popisa	Vrste adresa	Opis popisa
Popis dopuštenih adresa	Dopušteno	
Popis blokiranih adresa	Blokirano	
Popis adresa izuzetih od skeniranja sadržaja	Pronađeni zlonamjerni p...	

Dodaj Uredi Izbriši Uvezi Izvezi

Dodajte zamjenski znak (\*) na popis blokiranih adresa da biste blokirali sve URL-ove osim onih koji se nalaze na popisu dopuštenih adresa.

U redu Odustani

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

- [Deblokirajte sigurnu stranicu na pojedinačnoj radnoj stanici u programu ESET Endpoint Antivirus](#)
- [Deblokirajte sigurnu stranicu na krajnja točki pomoću ESET Security Management Center](#)

Više informacija potražite u odjeljku [Upravljanje URL adresama](#).

## Stvaranje novog popisa URL adresa

Ovaj odjeljak omogućuje određivanje popisa URL adresa/maski koje će biti blokirane, dopuštene ili izuzete od provjere.

Prilikom stvaranja novog popisa za konfiguriranje su dostupne sljedeće mogućnosti:

**Vrsta popisa adresa** – Dostupne su tri prethodno definirane vrste popisa:

- **Popis adresa izuzetih iz provjere** – Provjera zlonamjernog koda ne izvršava se ni za jednu adresu dodanu na popis.
- **Popis blokiranih adresa** – Korisnik neće moći pristupiti adresama navedenim na tom popisu.
- **Dopušteno** – Ako je vaše pravilo konfiguirano za upotrebu ove funkcije i ako se zamjenski znak (\*) doda na vaš popis, moći ćete pristupiti adresama s ovog popisa, čak i ako se te adrese nalaze i na popisu blokiranih adresa.

**Naziv popisa** – Navedite naziv popisa. Ovo polje neće biti dostupno ako uređujete jedan od triju prethodno definiranih popisa.

**Opis popisa** – Upišite kratki opis popisa (neobavezno). Ovo će polje biti nedostupno ako uređujete jedan od triju prethodno definiranih popisa.

**Popis je aktivran** – Odaberite traku klizača da biste aktivirali popis.

**Obavijesti pri primjeni** – Odaberite traku klizača ako želite biti obaviješteni kada se popis koristi za procjenu HTTP stranice koju ste posjetili. Primjerice, bit ćete obaviješteni kada je web stranica blokirana ili dopuštena zato jer se

web stranica nalazi na popisu blokiranih ili dopuštenih adresa. Obavijest će prikazati naziv popisa za popis koji navede web stranica.

**Opseg vođenja dnevnika** – odaberite opseg vođenja dnevnika iz padajućeg izbornika. Zapise koji sadrže Upozorenja o opsegu može prikupiti ESMC ili ESET PROTECT.

## Kontrolni elementi

**Dodaj** – Služi za dodavanje URL adrese na popis (moguće je unos više vrijednosti sa separatorom).

**Uredi** – Uređuje postojeće adrese na popisu. Ta je mogućnost dostupna samo za adrese stvorene putem mogućnosti **Dodaj**.

**Ukloni** – Briše postojeće adrese s popisa. Ta je opcija dostupna samo za adrese stvorene putem opcije **Dodaj**.

**Uvezi** – Služi za uvoz datoteke s URL adresama (vrijednosti morate odvojiti prijelomom retka, na primjer \*.txt s kodiranjem UTF-8).

## Kako dodati URL masku

Prije unosa željene adrese / maske domene pogledajte upute u ovom dijaloškom okviru.

Program ESET Endpoint Antivirus korisnicima omogućuje blokiranje pristupa određenim web stranicama i sprečavanje prikazivanja njihova sadržaja u web pregledniku. Korisnicima uz to omogućuje da definiraju adrese koje se izuzimaju iz provjere. Ako nije poznat cijeli naziv udaljenog servera ili korisnik želi obuhvatiti čitavu skupinu udaljenih servera, za identifikaciju takve skupine mogu se koristiti tzv. maske. Maske sadrže simbole „?” i „\*”:

- ? zamjenjuje bilo koji znak
- \* zamjenjuje tekstualni znakovni niz.

Primjerice, znakovni niz \*.c?m obuhvaća sve adrese kojima zadnji dio počinje slovom c, završava slovom m i sadrži nepoznat znak između njih (.com, .cam itd.).

S nizom koji započinje s “\*.” postupa se na poseban način ako se koristi na početku naziva domene. Kao prvo, u tom slučaju zamjenski znak \* ne odgovara znaku kose crte ('/'). To je tako kako bi se spriječilo zaobilazeњe maske, primjerice, maska \*.domena.com neće se podudarati s http://bilokojadomena.com/bilokojiput#.domena.com (taj se nastavak može pridružiti bilo kojem URL-u bez učinka na preuzimanje). A kao drugo, u tom posebnom slučaju “\*.” znači isto kao prazan niz. To je tako kako bi se omogućilo uskladišvanje čitave domene zajedno sa svim poddomenama pomoći jedne maske. Primjerice, maska \*.domena.com podudara se i s http://domena.com. Korištenje maske \*domena.com bilo bi netočno jer bi se podudaralo i s http://drugadomena.com.

## Anti-phishing zaštita

Pojam phishing odnosi se na protuzakonitu aktivnost koja koristi tehnike društvenog inženjeringu (manipuliranje korisnicima radi stjecanja povjerljivih informacija). Phishing se često koristi za ostvarivanje pristupa tajnim podacima kao što su brojevi bankovnih računa, PIN kodovi itd. Više o toj aktivnosti pročitajte u [rječniku](#). ESET Endpoint Antivirus podržava antiphishing zaštitu, pa je moguća blokada web stranica za koje se zna da distribuiraju takvu vrstu sadržaja.

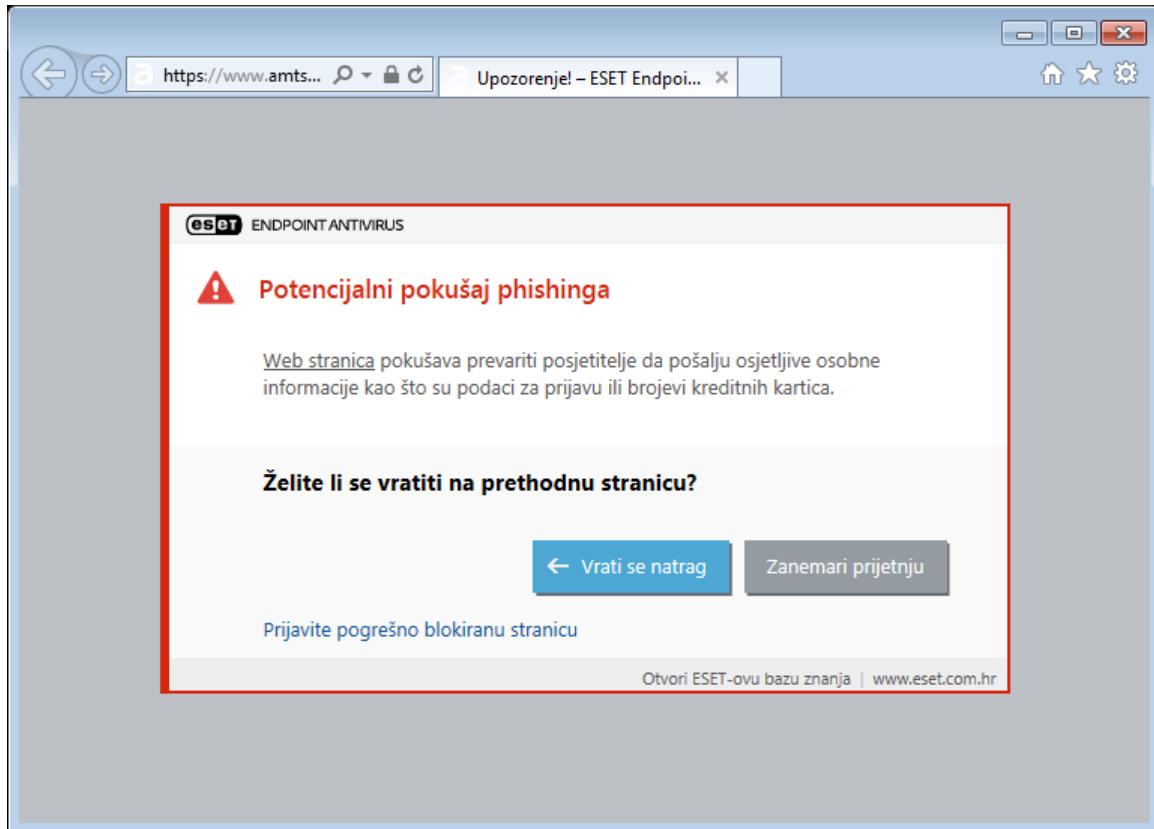
Preporučujemo da obavezno aktivirate Antiphishing u programu ESET Endpoint Antivirus. Da biste to učinili,

otvorite **Napredno podešavanje** (F5) i idite do stavke **Web i e-pošta > Anti-phishing zaštita**.

Pogledajte [članak u našoj bazi znanja](#) kako biste saznali više o antiphishing zaštiti u programu ESET Endpoint Antivirus.

## Pristupanje web stranici za phishing

Kada pristupite web stranici za phishing, u web pregledniku prikazat će se sljedeći dijaloški okvir. Ako i dalje želite pristupiti web stranici, kliknite **Produži do stranice** (ne preporučuje se).



**i** Potencijalne web stranice za phishing koje su stavljenе na popis pouzdanih adresa prema standardnim postavkama će nestati nakon nekoliko sati. Da biste trajno dopustili web stranicu, upotrijebite alat [Upravljanje URL adresama](#). U odjeljku **Napredno podešavanje** (F5) otvorite mogućnosti **Web i e-pošta > Zaštita web pristupa > Upravljanje URL adresama > Popis adresa**, kliknite **Uredi** i na popis dodajte web stranicu koju želite uređiti.

## Prijava stranice za phishing

Veza [Priavi](#) omogućuje vam da prijavite phishing/zlonamjernu web stranicu tvrtki ESET radi analize.

**i** Prije slanja web stranice u ESET provjerite je li zadovoljen neki od sljedećih kriterija:

- web stranica uopće nije otkrivena,
- web stranica je neispravno otkrivena kao prijetnja. U tom slučaju možete [prijaviti neispravno identificiranu stranicu za phishing](#).

Web stranicu možete poslati i e-poštom. Pošaljite poruku e-pošte na adresu [samples@eset.com](mailto:samples@eset.com). Napominjemo da predmet poruke mora sadržavati opis, a sama poruka što više informacija o web stranici (primjerice, informacije o web stranici preko koje ste došli do nje, kako ste čuli za tu web stranicu itd.).

# Aktualizacija programa

Redovita nadogradnja programa ESET Endpoint Antivirus najbolji je način za osiguranje maksimalne razine sigurnosti na računalu. Modul nadogradnje osigurava da je program uvijek ažuriran na dva načina, nadogradnjom modula detekcije i nadogradnjom komponenti sustava. Nadogradnje su automatske prema standardnim postavkama kada je program aktiviran.

Klikom na **Aktualizacija** u glavnom prozoru programa možete provjeriti status trenutne aktualizacije uključujući datum i vrijeme zadnje uspješne aktualizacije i je li aktualizacija potrebna. Također možete kliknuti link **Prikaži sve module** kako biste otvorili popis instaliranih modula i provjerili verziju i posljednju aktualizaciju modula.

Osim toga, dostupna je i opcija ručnog pokretanja procesa aktualizacije, **Potraži aktualizacije**. Aktualizacije modula za otkrivanje virusa i programskih komponenti važan su dio održavanja potpune zaštite od zlonamjernog koda. Obratite pozornost na njihovu konfiguraciju i rad. Ako tijekom instalacije niste unijeli detalje licence, licenčni ključ možete unijeti prilikom aktualizacije klikom na mogućnost **Aktiviraj program** kako biste pristupili aktualacijskim serverima tvrtke ESET.

Ako aktivirate program ESET Endpoint Antivirus pomoću datoteke izvanmrežne licence bez korisničkog imena i lozinke te pokušate izvršiti nadogradnju, crvena informacija **Nadogradnja modula nije uspjela** signalizira da možete preuzeti nadogradnje samo s mirrora.



Licenčni ključ isporučuje tvrtka ESET nakon kupnje programa ESET Endpoint Antivirus.

The screenshot shows the ESET Endpoint Antivirus interface. On the left is a dark sidebar with icons for 'STATUS ZAŠTITE' (checkmark), 'SKENIRANJE RAČUNALA' (magnifying glass), 'AKTUALIZACIJA' (refresh), 'PODEŠAVANJE' (gear), 'ALATI' (briefcase), and 'POMOĆ I PODRŠKA' (question mark). The main window has a title bar 'eset ENDPOINT ANTIVIRUS'. The central area is titled 'Aktualizacija'. It displays information about the update status of the 'ESET Endpoint Antivirus' module. The module is listed with a green checkmark, current version '8.0.2028.0', and the date '12/8/2020 2:25:18 PM'. Below this, it shows the last successful update was on '12/8/2020 3:24:04 PM'. At the bottom of the central pane is a blue link 'Prikaži sve module'. At the very bottom of the window, there are two small status indicators: a circular arrow with the text 'Provjera dostupnosti nadogradnji' and a clock with the text 'Promijeni učestalost nadogradnje'.

**Trenutačna verzija** – Broj verzije programa ESET Endpoint Antivirus.

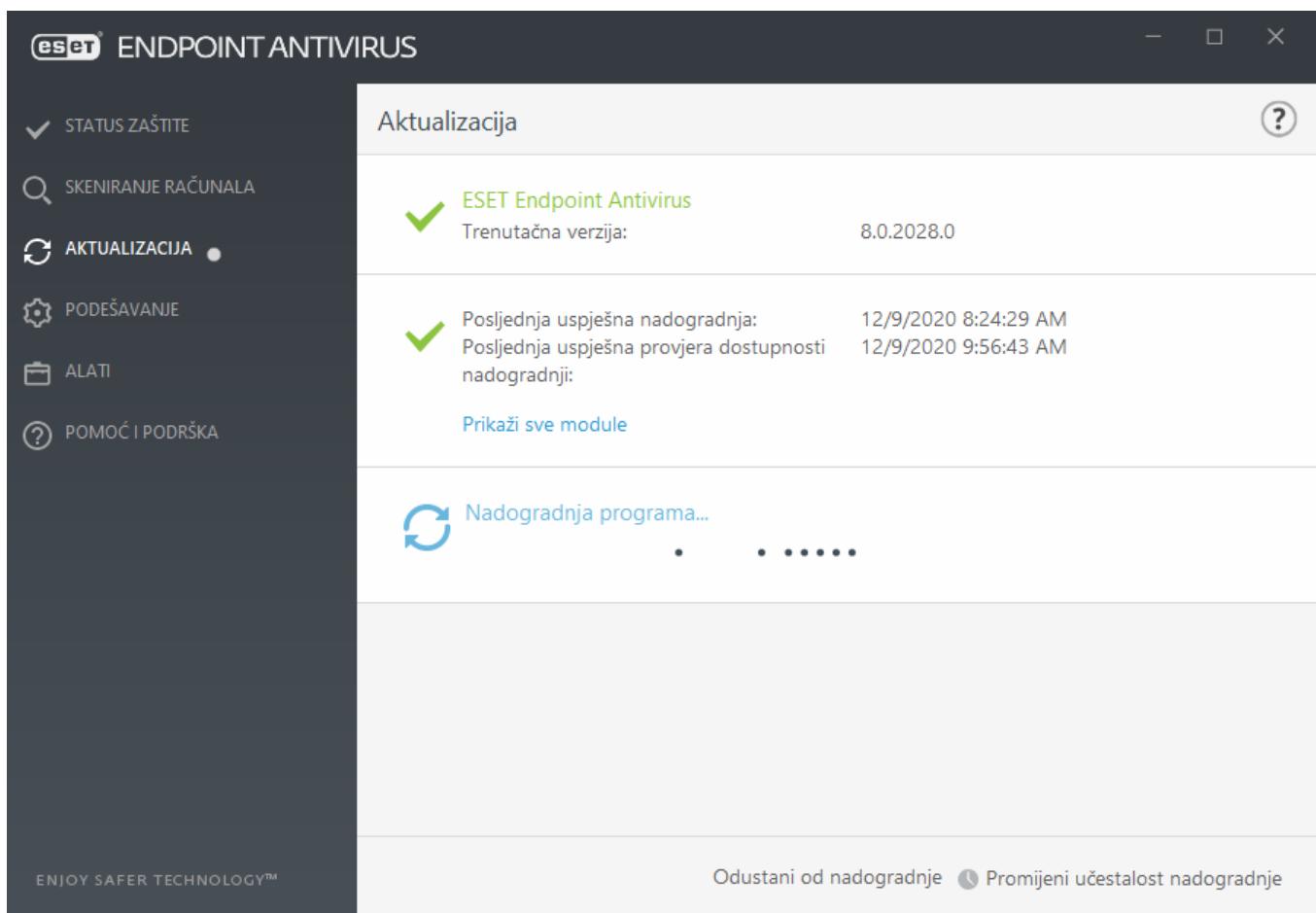
**Posljednja uspješna nadogradnja** – Datum i vrijeme posljednje uspješne nadogradnje. Pobrinite se da se odnosi na nedavan datum, što znači da modul za otkrivanje virusa nije zastario.

**Posljednja uspješna provjera dostupnosti nadogradnji** – Datum i vrijeme posljednjeg uspješnog pokušaja nadogradnje modula.

**Prikaži sve module** – Kliknite link kako biste otvorili popis instaliranih modula i provjerite verziju i posljednju aktualizaciju modula.

## Proces aktualizacije

Nakon klika opcije **Potraži aktualizacije** pokreće se postupak preuzimanja. Prikazat će se traka napretka i preostalo vrijeme za preuzimanje. Da biste prekinuli aktualizaciju, kliknite **Odustani od aktualizacije**.



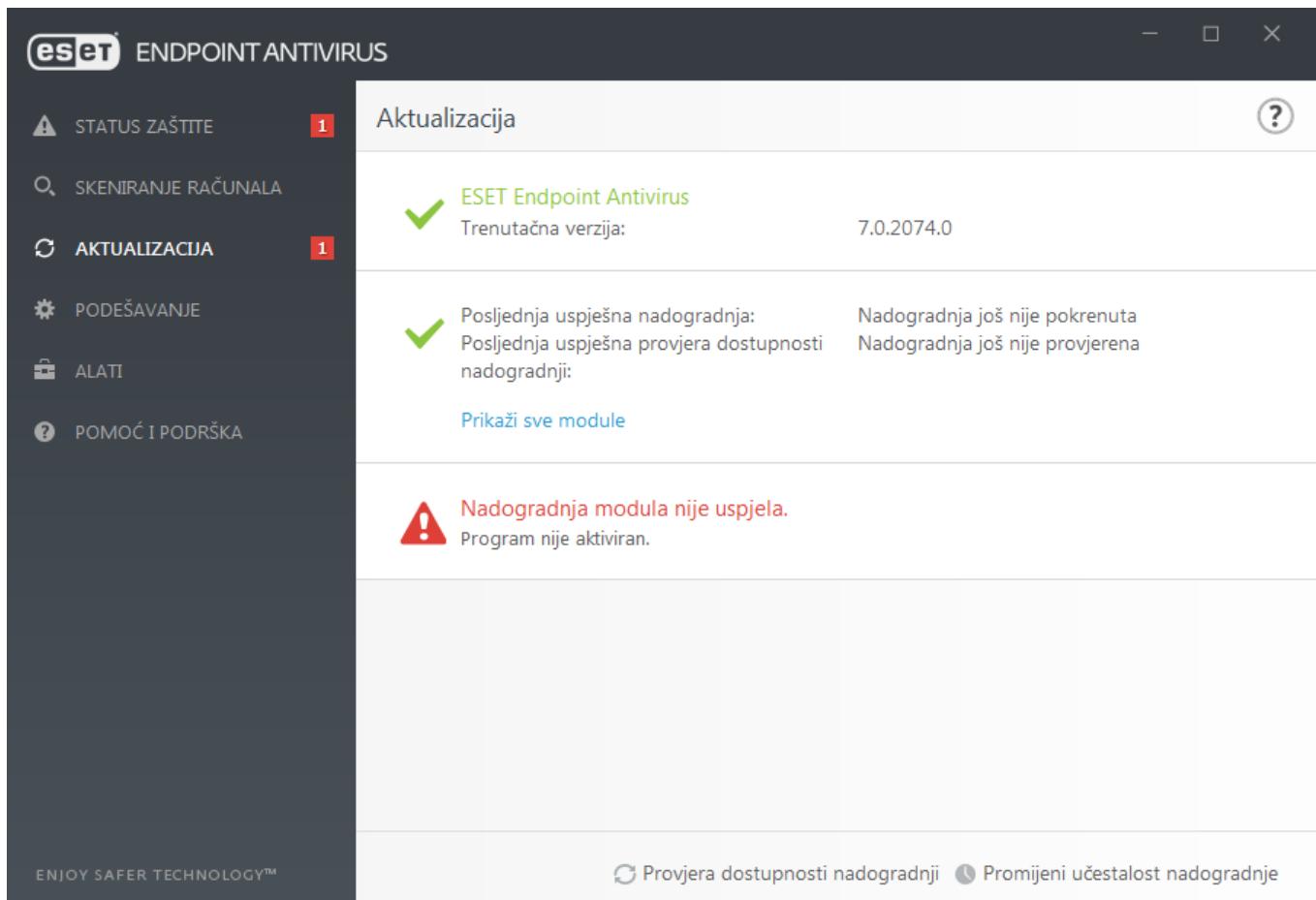
**!** U normalnim okolnostima modul se nadograđuje nekoliko puta dnevno. Ako to nije slučaj, program je zastario i izloženiji je zarazama. Čim prije nadogradite module.

**Modul detekcije je zastario** – ova pogreška pojavit će se nakon nekoliko neuspješnih pokušaja nadogradnje modula. Preporučujemo da provjerite postavke nadogradnje. Najčešći je uzrok ove pogreške neispravan unos podataka za prijavu ili neispravna konfiguracija [postavki povezivanja](#).

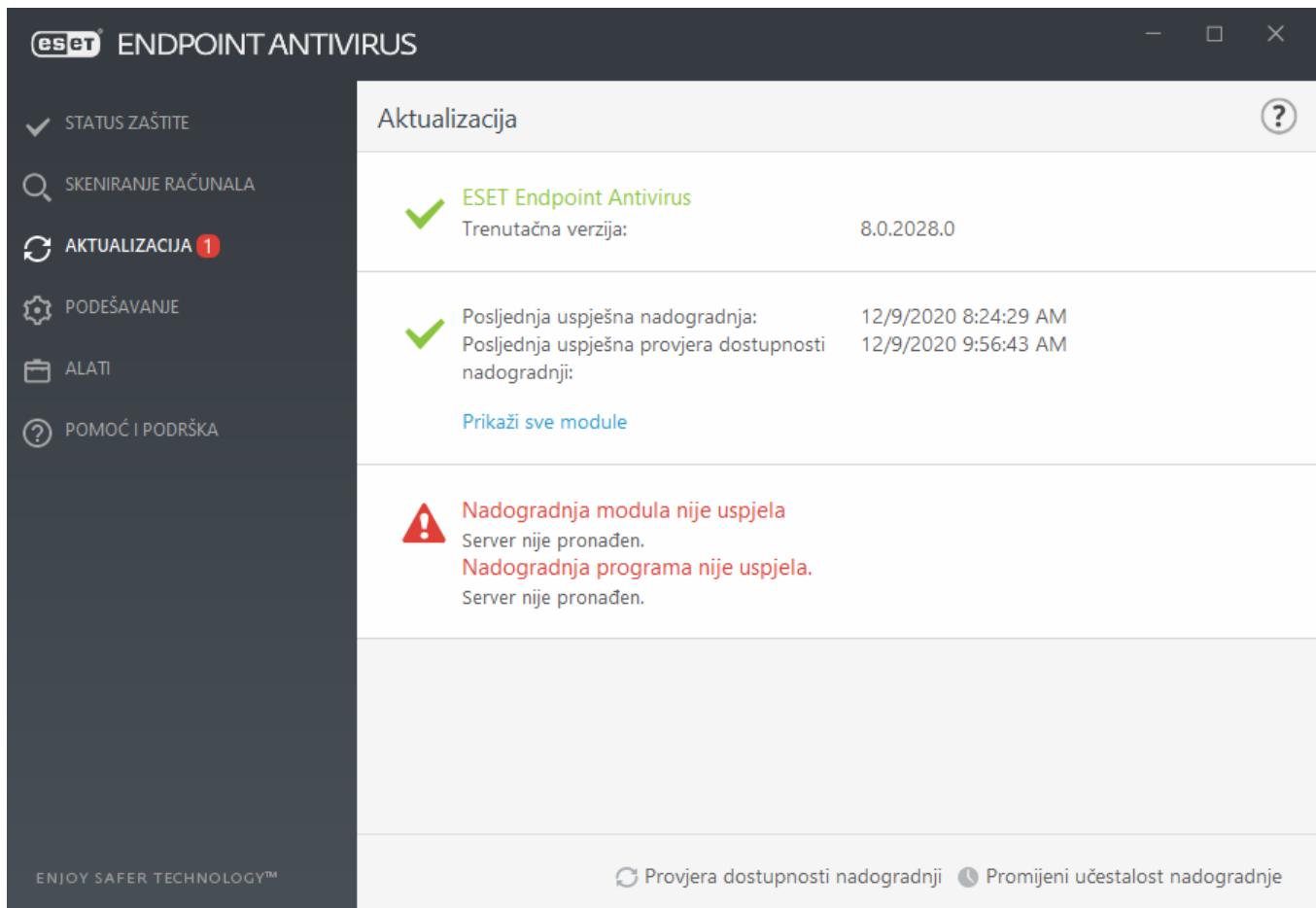
Prethodna obavijest odnosi se na sljedeće dvije poruke **Nadogradnja modula nije uspjela** o neuspješnim nadogradnjama:

- Neispravna licenca** – U podešavanju nadogradnje unesen je pogrešan licenčni ključ. Preporučujemo provjeru podataka za autorizaciju. U prozoru naprednog podešavanja (kliknite **Podešavanje** u glavnom

izborniku i zatim kliknite **Napredno podešavanje** ili na tipkovnici pritisnite F5) dostupne su dodatne opcije nadogradnje. Na glavnom izborniku kliknite mogućnost **Pomoć i podrška > Promijeni licencu** da biste unijeli novi licenčni ključ.



**2. Došlo je do pogreške tijekom preuzimanja datoteke za aktualizaciju** – Mogući uzrok pogreške su [Postavke internetske veze](#). Preporučujemo da provjerite vezu s internetom (primjerice, otvaranjem nekih web stranica u web pregledniku). Ako se web stranica ne otvori, vjerojatno nije uspostavljena internetska veza ili na računalu postoje problemi s povezivošću. Ako nemate aktivnu internetsku vezu, provjerite to kod svoga davatelja internetskih usluga (ISP).



**i** Dodatne informacije potražite u ovom [članku ESET-ove baze znanja](#).

## Podešavanje aktualizacije

Mogućnosti podešavanja aktualizacije dostupne su na stablu **Napredno podešavanje** (F5) u odjeljku **Aktualizacija**. U ovom odjeljku navode se informacije o izvoru aktualizacije, na primjer aktualizacijski serveri i podaci za autorizaciju za te servere.

**!** Da bi se aktualizacije pravilno preuzele, važno je pravilno navesti sve parametre. Ako koristite firewall, provjerite je li programu tvrtke ESET dopuštena komunikacija s internetom (npr. komunikacija putem HTTPS-a).

### - Osnovno

Profil nadogradnje koji se trenutačno upotrebljava prikazuje se u padajućem izborniku **Odaberite standardni profil nadogradnje**.

Da biste stvorili novi profil, pogledajte odjeljak [Profili](#).

**Konfiguriraj obavijesti o nadogradnjama** – kliknite gumb **Uredi** da biste odabrali koje se [obavijesti aplikacije](#) prikazuju. Možete odabrati između opcija **Prikaži** na radnoj površini i/ili **Pošalji e-poštom**.

Ako imate poteškoća prilikom preuzimanja nadogradnji modula, kliknite **Očisti** pored stavke **Očisti predmemoriju nadogradnje** da biste izbrisali privremene datoteke/predmemoriju nadogradnje.

# Upozorenja o zastarjelom modulu za otkrivanje virusa

**Automatski postavi maksimalnu starost modula detekcije** – Omogućuje postavljanje maksimalnog vremena (u danima) nakon kojeg će se modul za otkrivanje prijaviti kao zastario. Standardna vrijednost **maksimalne starosti modula detekcije (u danima)** iznosi 7 dana.

## Povrat na prethodno stanje modula

Ako sumnjate da je nova aktualizacija modula za otkrivanje i/ili modula programa nestabilna ili oštećena, možete se [vratiti na prethodnu verziju](#) i na određeno vremensko razdoblje deaktivirati aktualizacije.

Napredno podešavanje

MODUL DETEKCIJE 2

NADOGRADNJA 2

MREŽNA ZAŠTITA

WEB I E-POŠTA 3

KONTROLA UREĐAJA 2

ALATI 3

KORISNIČKO SUČELJE 1

**OSNOVNO**

Odaberite standardni profil nadogradnje

Automatska zamjena profila

Konfiguriraj obavijesti o nadogradnjama

Očisti predmemoriju nadogradnje

**UPOZORENJA O ZASTARJELOSTI ALATA MODULA DETEKCIJE**

Ova postavka određuje maksimalnu dopuštenu starost alata modula detekcije prije nego što se počne smatrati zastarjelim i prije nego što se pojavi upozorenje.

Automatski postavi maksimalnu starost modula detekcije

Maksimalna starost modula detekcije (u danima)

**POVRAT NA PRETHODNO STANJE MODULA**

Stvorji snimke modula

Broj lokalno spremljenih snimki

Standardno

U redu

Odustani

## - Profili

Aktualizacijske profile moguće je stvoriti za različite konfiguracije aktualizacije i zadatke. Stvaranje aktualizacijskih profila posebno je korisno za mobilne korisnike kojima je potreban alternativni profil za internetske veze čija se svojstva redovito mijenjaju.

Padajući izbornik **Odaberi profil za uređivanje** prikazuje trenutačno odabrani profil te je prema standardnim postavkama postavljen na **Moj profil**.

Da biste stvorili novi profil, kliknite **Uredi** uz **Popis profila**, a zatim unesite vlastiti **Naziv profila** te kliknite **Dodaj**.

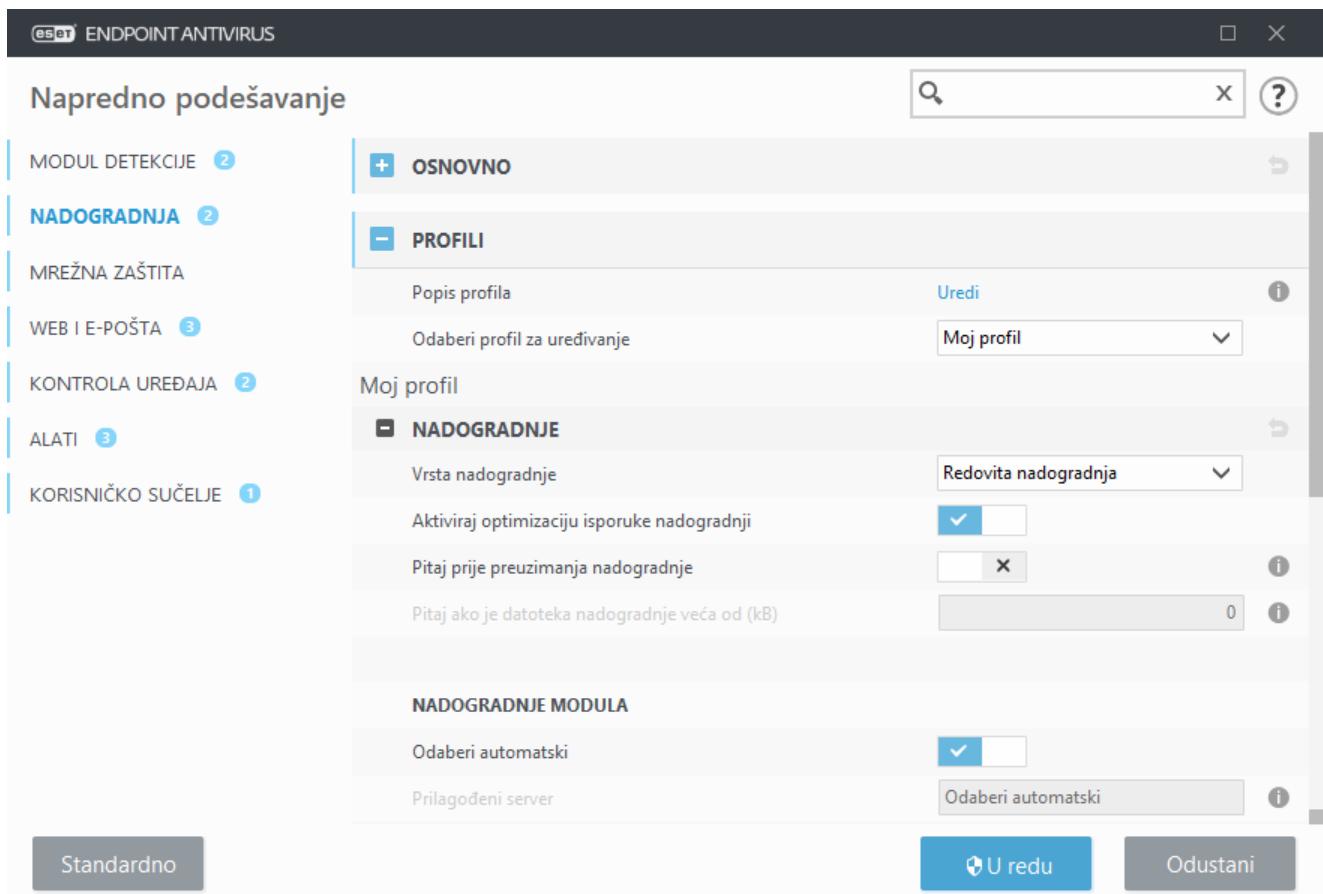
## Nadogradnje

Prema standardnim postavkama Vrsta aktualizacije postavljena je na Redovita aktualizacija kako bi se osiguralo automatsko preuzimanje aktualizacijskih datoteka s ESET servera s najmanjim mrežnim prometom. Probni način

rada (mogućnost Probni način rada) obuhvaća aktualizacije koje su prošle interno testiranje i koje će uskoro biti općenito dostupne. Ako aktivirate probni način rada, imat ćete pristup najnovijim metodama otkrivanja i popravcima. Međutim, probni način rada možda neće biti dovoljno stabilan cijelo vrijeme i NE PREPORUČUJE se njegovo korištenje na proizvodnim serverima i radnim stanicama gdje se traži maksimalna dostupnost i stabilnost. Odgođena aktualizacija omogućuje aktualizaciju s posebnih aktualizacijskih servera koji sadrže nove verzije baze podataka virusa s odgodom od barem X sati, (tj. baze podataka testirane su u stvarnom okruženju i smatraju se stabilnima).

**Aktiviraj optimizaciju isporuke nadogradnji** – Kad je ova opcija aktivirana, datoteke nadogradnje mogu se preuzeti iz CDN (mreže za isporuku sadržaja). Ako deaktivirate ovu postavku, može doći do prekida preuzimanja kada su namjenski ESET serveri za nadogradnju preopterećeni. Deaktivacija može biti korisna kad je firewall ograničen samo na pristupanje [IP adresama ESET servera za nadogradnju](#) ili kad spajanje s uslugama CDN ne radi.

**Pitaj prije preuzimanja nadogradnje** – program će prikazati obavijest u kojoj možete potvrditi ili odbiti preuzimanja datoteka nadogradnje. Ako je datoteka za nadogradnju veća od vrijednosti navedene u polju Pitaj ako je datoteka za nadogradnju veća od (kB), program će prikazati upit za potvrdu. Ako je veličina datoteke za nadogradnju postavljena na 0 kB, program će uvijek prikazati upit za potvrdu.



## Nadogradnje modula

Opcija **Odaberi automatski** postavljena je prema standardnim postavkama. Opcija **Prilagođeni server** mjesto je na kojem se pohranjuju aktualizacije. Ako upotrebljavate ESET server za nadogradnju, preporučujemo da ostavite odabranu standardnu opciju.

**Aktiviraj češće nadogradnje potpisa za otkrivanje** – Potpisi za otkrivanje bit će nadograđivani u kraćim intervalima. Deaktivacija ove postavke može negativno utjecati na stopu otkrivanja.

**Dopustite nadogradnje modula s izmjenjivog medija** – omogućuje nadogradnju s izmjenjivog medija ako sadrži stvoreni mirror. Kada je odabrana opcija Automatski, nadogradnja će se pokrenuti u pozadini. Ako želite da se

prikažu dijaloški okviri za nadogradnju, odaberite stavku Uvijek pitaj.

Kada koristite lokalni HTTP server, poznat i kao mirror, server za nadogradnju treba postaviti na sljedeći način:  
`http://naziv_računala_ili_njegova_IP_adresa:2221`

Kada koristite lokalni HTTP server i SSL – server za nadogradnju treba postaviti na sljedeći način:  
`https://naziv_računala_ili_njegova_IP_adresa:2221`

Kada koristite lokalnu zajedničku mapu – server za nadogradnju treba postaviti na sljedeći način:  
`\|naziv_računala_ili_njegova_IP_adresa\zajednička_mapa`

 Broj porta HTTP servera naveden u prethodnim primjerima ovisi o tome koji port osluškuje vaš HTTP/HTTPS server.

## Nadogradnja programske komponente

Pogledajte [Nadogradnju programske komponente](#).

## Opcije veze

Pogledajte [Opcije veze](#).

## Aktualizacijski mirror

Pogledajte [Mirror za nadogradnju](#).

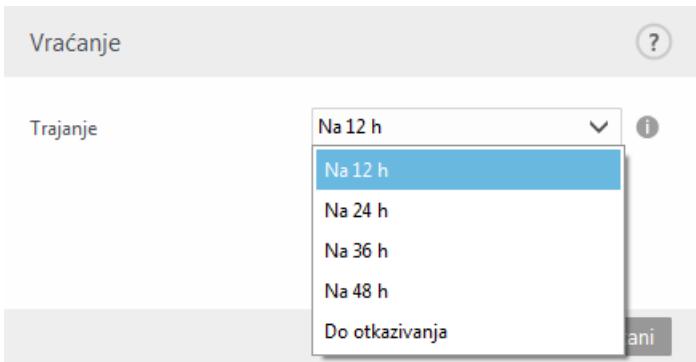
# Vraćanje aktualizacije

Ako sumnjate da je nova nadogradnja modula detekcije nestabilna ili oštećena ili da su moduli programa nestabilni ili oštećeni, možete ih vratiti na prethodnu verziju i privremeno deaktivirati nadogradnje. Možete i aktivirati nadogradnje koje ste prethodno deaktivirali i odgodili na neograničeno vrijeme.

ESET Endpoint Antivirus bilježi snimke modula detekcije i modula programa za upotrebu s funkcijom vraćanja na prethodno stanje. Da biste stvorili snimke baze podataka virusa, funkcija **Stvari snimke modula** mora ostati aktivirana. Kada je aktivirana funkcija **Stvari snimke modula**, prva snimka stvara se tijekom prve nadogradnje. Sljedeća se stvara nakon 48 sati. U polju **Broj lokalno spremljenih snimki** naveden je broj spremljenih snimki modula detekcije.

 Kada se dosegne maksimalna količina snimki (na primjer, tri), najstarija snimka zamjenjuje se novom svakih 48 sati. ESET Endpoint Antivirus vraća modul detekcije i verzije nadogradnji modula programa na najstariju snimku.

Morate odabrati vremenski interval u padajućem izborniku **Trajanje** ako kliknete **Vraćanje na prethodno stanje** (**Napredno podešavanje** (F5) > **Nadogradnja** > **Osnovno** > **Povrat na prethodno stanje modula**).



Odaberite stavku **Do otkazivanja** da biste redovne aktualizacije odgodili na neograničeno vrijeme, sve dok ručno ne vratite funkciju aktualizacije. Ne preporučujemo odabir te mogućnosti jer predstavlja mogući sigurnosni rizik.

Ako se vrši vraćanje na prethodno stanje, gumb **Vrati na prethodno stanje** pretvara se u **Dopusti nadogradnje**. Tijekom vremenskog intervala odabranog iz padajućeg izbornika **Obustava nadogradnji** nisu dopuštene nadogradnje. Verzija modula detekcije vraćena je na najstariju dostupnu verziju i spremljena je kao snimka u datotečni sustav lokalnog računala.

Recimo da je broj 22700 najnovija verzija modula detekcije, a verzije 22698 i 22696 spremljene su kao snimke modula detekcije. Verzija 22697 nije dostupna. U ovom primjeru računalo je bilo isključeno tijekom nadogradnje verzije 22697 i pojavila se novija nadogradnja prije nego što je preuzeta verzija 22697. Ako je polje **Broj lokalno pohranjenih snimaka** postavljeno na 2 i kliknete **Vraćanje na prethodno stanje**, modul detekcije (uključujući module programa) bit će vraćen na verziju broj 22696. Taj postupak može potrajati. Provjerite je li verzija modula detekcije vraćena na stariju na zaslonu [Nadogradnja](#).

# Nadogradnja programskih komponenti

Kartica **Način nadogradnje** sadrži mogućnosti vezane uz nadogradnju programskih komponenti. Program vam omogućuje da unaprijed definirate njegovo ponašanje kada postane dostupna nova nadogradnja neke programske komponente.

Nadogradnje programskih komponenti uvode nove značajke ili mijenjaju one koje već postoje u prethodnim verzijama. Moguće ih je izvršiti automatski bez korisničke intervencije, ali korisnik može odabrat da ga se o tome obavijesti. Nakon instalacije nadogradnje programske komponente mogao bi biti potreban restart računala.

U padajućem izborniku **Način rada nadogradnje** dostupne su tri opcije:

- **Pitaj prije nadogradnje** – Standardna opcija za računala kojima se ne upravlja. Prikazat će se odzivnik za potvrdu ili odbijanje nadogradnje programskih komponenti kada ona bude dostupna.
- **Uvijek nadogradi programske komponente** – Time će se nadogradnje programskih komponenti automatski preuzimati i instalirati. Imajte na umu da će možda biti potrebno ponovno pokrenuti računalo.
- **Nemoj nikad nadograditi programske komponente** – Time se programske komponente uopće neće nadograditi. Ta je mogućnost praktična za serverske instalacije jer se serveri obično restartaju samo radi održavanja.

Prema standardnim postavkama nadogradnje programskih komponenti preuzimaju se sa servera ESET Repozitorija. U velikim okruženjima ili okruženjima izvan mreže promet se može distribuirati radi omogućavanja unutarnjeg predmemoriranja datoteka programskih komponenti.

## [Određivanje prilagođenog servera za nadogradnje programskih komponenti](#)

1.Odredite put do nadogradnje programskih komponenti u polju **Prilagođeni server**.

To može biti HTTP(S) link, put zajedničke mreže u SMB protokolu i put lokalnog diska ili izmjenjivog medija. Za mrežne pogone upotrijebite UNC umjesto slova mapiranog pogona.

2.Ostavite polja **Korisničko ime** i **Lozinka** praznima ako nisu obavezna.

Ako su obavezna, odredite odgovarajuće korisničke podatke za HTTP prijavu na prilagođeni web server.

3.Potvrdite promjene i provjerite postoji li nadogradnja programskih komponenti pomoću standardne nadogradnje programa ESET Endpoint Antivirus.

 Odabir najprikladnije mogućnosti ovisi o radnoj stanici na kojoj se te postavke primjenjuju. Imajte na umu da postoje razlike između radnih stanica i servera, npr. automatskim ponovnim pokretanjem servera nakon nadogradnje programa moguće je nanijeti ozbiljnu štetu.

## Opcije veze

Da biste pristupili opcijama podešavanja proxy servera za određeni profil nadogradnje, kliknite **Nadogradnja** na stablu **Napredno podešavanje** (F5) i zatim kliknite **Profilii > Nadogradnje > Opcije povezivanja**.

## Proxy server

Kliknite padajući izbornik **Način rada proxy servera** i odaberite jednu od sljedećih triju opcija:

- Nemoj koristiti proxy server
- Veza putem proxy servera
- Koristi globalne postavke proxy servera

Odaberite mogućnost **Koristi globalne postavke proxy servera** za upotrebu mogućnosti konfiguracije proxy servera koje su već definirane u ogranku stabla naprednog podešavanja **Alati > Proxy server**.

Mogućnost **Nemoj koristiti proxy server** odaberite da biste odredili da se za nadogradnju programa ESET Endpoint Antivirus ne koristi proxy server.

Mogućnost **Veza putem proxy servera** treba se odabratи ako:

- Drugačiji proxy server od onog definiranog pod Alati > **Proxy server** upotrebljava se za nadogradnju programa ESET Endpoint Antivirus. U ovoj konfiguraciji, informacije za novi proxy trebale bi biti određene pod adresom **proxy servera**, komunikacijskim **portom** (3128 prema standardnim postavkama) te prema potrebi, **korisničkim imenom i lozinkom** za proxy server.
- Postavke proxy servera nisu postavljene globalno, no program ESET Endpoint Antivirus povezat će se s proxy serverom radi nadogradnje.
- Vaše računalo povezano je na internet putem proxy servera. Postavke se preuzimaju iz Internet Explorera tijekom instalacije programa, no ako se promijene (npr. ako promijenite davatelja internetskih usluga), provjerite jesu li postavke za proxy ispravne u ovom prozoru. Program se inače neće moći povezati sa serverima za nadogradnje.

Standardna je postavka za proxy server **Koristi globalne postavke proxy servera**.

**Upotrijebi izravnu vezu ako nije dostupan proxy** – Ako nije dostupan, proxy će se zaobići tijekom nadogradnje.

## Zajedničke mreže Windowsa

Pri aktualizaciji s lokalnog servera s operacijskim sustavom Windows NT, autorizacija je prema standardnim postavkama obavezna za svaku mrežnu vezu.

Za konfiguriranje takvog računa na padajućem izborniku odaberite **Poveži se s LAN-om kao:**

- **Sistemski račun (standardno)**,
- **Trenutačni korisnik**,
- **Određeni korisnik**.

Izaberite mogućnost **Sistemski račun (standardno)** da biste za autorizaciju koristili sistemski račun. Ako u glavnom odjeljku podešavanja aktualizacije nisu uneseni podaci za autorizaciju, obično nema nikakvog procesa autorizacije.

Da biste bili sigurni da će program autorizirati pomoću trenutno prijavljenog korisničkog računa, odaberite **Trenutni korisnik**. Nedostatak je tog rješenja taj što se program neće moći povezivati s aktualacijskim serverom ako trenutno nije prijavljen nijedan korisnik.

Ako želite da program za autorizaciju koristi račun nekog točno određenog korisnika, odaberite **Određeni**

**korisnik.** Tu metodu primijenite kada ne uspije povezivanje putem standardnog sistemskog računa. Imajte na umu da određeni korisnički račun mora imati pristup direktoriju s aktualizacijskim datotekama na lokalnom serveru. U suprotnome program neće moći uspostaviti vezu i preuzeti aktualizacije.

Postavke **korisničkog imena** i **lozinke** nisu obavezne.

Kada su odabранe mogućnosti **Trenutni korisnik** ili **Određeni korisnik**, postoji mogućnost pogreške prilikom promjene identiteta programa na željenog korisnika. Preporučujemo da u glavni odjeljak podešavanja aktualizacije unesete podatke za autorizaciju LAN-a. U tom odjeljku podešavanja aktualizacije podatke za autorizaciju trebalo bi unijeti na sljedeći način: *naziv\_domene\korisnik* (ako se radi o radnoj grupi, unesite *naziv\_radnegrupe\naziv*) i lozinka. Pri aktualizaciji s HTTP verzije lokalnog servera nije potrebna nikakva autorizacija.

Odaberite opciju Nakon nadogradnje **prekini vezu** sa serverom da biste prinudno raskinuli vezu ako ona ostane aktivna nakon preuzimanja nadogradnje.

## Aktualizacijski mirror

ESET Endpoint Antivirus omogućuje stvaranje kopija aktualizacijskih datoteka koje se mogu koristiti za aktualizaciju drugih radnih stanica u mreži. Korištenje „mirrorra”, kopije aktualizacijskih datoteka u lokalnoj mreži, praktično je jer se aktualizacijske datoteke ne moraju više puta preuzimati s proizvođačeva servera za nadogradnju te ih odatle ne mora preuzeti svaka radna stanica. One se preuzimaju centralizirano na lokalni mirror server, a zatim se distribuiraju svim radnim stanicama, čime se izbjegava mogući rizik od zagušenja mrežnog prometa. Aktualizacijom klijentskih radnih stanica s mirrora optimizira se opterećenje mreže i štedi propusnost internetske veze.

Kako biste smanjili internetski promet na mrežama na kojima se ESET PROTECT upotrebljava za upravljanje velikim brojem klijenata, preporučujemo da koristite Apache HTTP proxy umjesto da konfigurirate klijent kao mirror. Apache HTTP proxy može se instalirati s programom ESET PROTECT putem cjelovitog instalacijskog programa ili kao samostalna komponenta. Više informacija i razlike između Apache HTTP proxyja, mirror alata i izravne povezivosti potražite na [stranici online pomoći za ESET PROTECT](#).

Opcije konfiguriranja za lokalni mirror server dostupne su u Naprednom podešavanju pod **Nadogradnja**. Da biste pristupili tom odjeljku, pritisnite **F5** da biste otvorili Napredno podešavanje, kliknite **Nadogradnja > Profili** i odaberite karticu **Mirror za nadogradnju**.

## Napredno podešavanje

MODUL DETEKCIJE 1

**NADOGRADNJA** 4

MREŽNA ZAŠTITA

WEB I E-POŠTA 3

KONTROLA UREĐAJA 1

ALATI 2

KORISNIČKO SUČELJE 1

Stvori mirror za nadogradnju



x



### PRISTUP DATOTEKAMA ZA NADOGRADNU

Mapa za pohranu

C:\ProgramData\ESET\ESET Smart Security Premium\mirror

Očisti

Aktiviraj HTTP server



Korisničko ime



Lozinka



### NADOGRADNJA PROGRAMSKIH KOMPONENTI

Datoteke

[Uredi](#)

Automatski nadograđi komponente



Nadograđi komponente sada

[Nadogradnja](#)

**HTTP SERVER**

**OPCIJE VEZE**

[U redu](#)

[Odustani](#)

Standardno

Da biste stvorili mirror na klijentskom računalu, aktivirajte mogućnost **Stvori aktualizacijski mirror**. Aktivacijom te mogućnosti aktiviraju se druge mogućnosti konfiguracije mirrora kao što su način pristupa aktualizacijskim datotekama i aktualizacijski put do mirror datoteka.

## Pristup aktualizacijskim datotekama

**Omogući aktualizaciju putem internog HTTP servera** – Ako je aktivirana, ova opcija omogućuje [pristup aktualizacijskim datotekama preko HTTP-a](#) bez unosa korisničkih podataka.

Načini pristupanja mirror serveru detaljno su opisani u odjeljku [Aktualizacija s mirrora](#). Mirror je moguće konfigurirati na dva osnovna načina – mapa s datotekama za nadogradnju može biti zajednička mrežna mapa ili klijenti mogu pristupati mirroru na HTTP serveru.

Mapa namijenjena pohrani aktualizacijskih datoteka za mirror definira se u odjeljku **Mapa za mirror**. Za odabir druge mape kliknite **Očisti** da biste izbrisali unaprijed odabrano mapu C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror i kliknite **Uredi** da biste pronašli mapu na lokalnom računalu ili zajedničku mrežnu mapu. Ako je za navedenu mapu potrebna autorizacija, u polja **Korisničko ime** i **Lozinka** potrebno je unijeti podatke za autorizaciju. Ako se odabrana odredišna mapa nalazi na mrežnom disku s verzijama operacijskog sustava Windows NT, 2000 ili XP, korisnik čije se korisničko ime i lozinka navedu mora imati prava pisanja za odabrano mapu. Korisničko ime i lozinku treba unijeti u obliku *Domena/Korisnik* ili *Radna grupa/Korisnik*. Ne zaboravite unijeti odgovarajuće lozinke.

## Nadogradnja programskih komponenti

**Datoteke** – prilikom konfiguriranja mirrora možete zadati jezik aktualizacije za preuzimanje. Odabранe jezike mora podržavati mirror server koji je konfiguirao korisnik.

**Automatski nadogradi komponente** – Omogućuje instaliranje novih funkcija i nadograđivanje postojećih. Nadogradnju je moguće izvršiti automatski bez korisničke intervencije, ali korisnik može odabrat da ga se o tome obavijesti. Nakon instalacije nadogradnje programske komponente moglo bi biti potrebno ponovno pokretanje računala.

**Nadogradi komponente odmah** – Nadograđuje vaše programske komponente na najnoviju verziju.

## HTTP server i SSL za mirror

U odjeljku **HTTP server** na kartici **Mirror** možete odrediti **port servera** putem kojeg će HTTP server osluškivati te vrstu **autentikacije** koju će koristiti. Prema standardnim postavkama port servera postavljen je na **2221**.

**Autentikacija** – Definira način autentikacije koji se koristi za pristup datotekama za nadogradnju. Na raspolaganju su sljedeće mogućnosti: **Ništa**, **Osnovno** i **NTLM**. Da biste koristili base64 šifriranje s osnovnom autorizacijom putem korisničkog imena i lozinke, odaberite **Osnovno**. Mogućnost **NTLM** nudi šifriranje pomoću sigurne metode šifriranja. Za autorizaciju koristi se radna stanica koju je stvorio korisnik i na kojoj se zajednički koriste aktualizacijske datoteke. Standardna je postavka **Ništa**, a omogućuje pristup aktualizacijskim datotekama bez potrebe za autorizacijom.

**i** Podaci za prijavu kao što su **korisničko ime** i **lozinka** namijenjeni su isključivo pristupanju mirror HTTP serveru. Ispunite ta polja samo ako su korisničko ime i lozinka obavezni.

Ako želite pokrenuti HTTP server s podrškom za HTTPS (SSL), dodajte svoju **Datoteku lanca certifikata** ili generirajte samopotpisani certifikat. Dostupne su sljedeće **vrste certifikata**: ASN, PEM i PFX. Za dodatnu zaštitu pri preuzimanju aktualizacijskih datoteka možete koristiti HTTPS protokol. Uz taj protokol gotovo je nemoguće pratiti prijenos podataka i podatke za prijavu. Opcija **Vrsta privatnog ključa** prema standardnim je postavkama postavljena na **Integrirano** (i zato je prema zadanim postavkama opcija **Datoteka privatnog ključa** deaktivirana). To znači da je privatni ključ dio odabrane datoteke lanca certifikata.

### Samopotpisani certifikati za HTTPS mirror

**!** Ako upotrebljavate HTTPS mirror server, morate uvesti njegov certifikat u pouzdano root spremište na svim klijentskim računalima. Pogledajte [Instaliranje pouzdanog root certifikata](#) u Windowsu.

## Aktualizacija s mirora

Postoje dva osnovna načina za konfiguriranje mirora koji je zapravo repozitorij s kojeg klijenti mogu preuzimati aktualizacijske datoteke. Mapa s aktualizacijskim datotekama može biti zajednička mrežna mapa ili na HTTP serveru.

### Pristup mirroru putem internog HTTP servera

To je standardna konfiguracija, određena u unaprijed definiranoj konfiguraciji programa. Da biste omogućili pristup mirroru s pomoću HTTP servera, idite na "**Napredno podešavanje**" > "**Nadogradnja**" > "**Profil**" > „**Mirror za nadogradnju**“ i odaberite "**Stvori mirror za nadogradnju**".

U odjeljku **HTTP server** na kartici **Mirror** možete odrediti **port servera** putem kojeg će HTTP server osluškivati te vrstu **autentikacije** koju će koristiti. Prema standardnim postavkama port servera postavljen je na **2221**.

**Autentikacija** – Definira način autentikacije koji se koristi za pristup datotekama za nadogradnju. Na raspolaganju su sljedeće mogućnosti: **Ništa**, **Osnovno** i **NTLM**. Da biste koristili base64 šifriranje s osnovnom autorizacijom putem korisničkog imena i lozinke, odaberite **Osnovno**. Mogućnost **NTLM** nudi šifriranje pomoću sigurne metode šifriranja. Za autorizaciju koristi se radna stanica koju je stvorio korisnik i na kojoj se zajednički koriste aktualizacijske datoteke. Standardna je postavka **Ništa**, a omogućuje pristup aktualizacijskim datotekama bez potrebe za autorizacijom.

**A** Ako želite dopustiti pristup aktualizacijskim datotekama putem HTTP servera, mapa mirrora mora se nalaziti na istom računalu na kojem se nalazi i instanca programa ESET Endpoint Antivirus koja je stvara.

**i** Pogreška **Neispravno korisničko ime/lozinka** pojavit će se u oknu Aktualizacija u glavnom izborniku nakon nekoliko neuspješnih pokušaja aktualizacije modula za otkrivanje virusa s mirrora. Preporučujemo vam da idete do odjeljka **Napredno podešavanje > Aktualizacija > Profili > Mirror za nadogradnju** i provjerite korisničko ime i lozinku. Najčešći je razlog pojavljivanja te pogreške unos pogrešnih podataka za autorizaciju.

Nakon konfiguriranja mirror servera morate dodati novi aktualizacijski server na klijentske radne stanice. Da biste to učinili, slijedite ove korake:

- Pristupite **naprednom podešavanju** (F5) i kliknite **Nadogradnja > Profili > Nadogradnje > Nadogradnje modula**.
- Deaktivirajte odabir mogućnosti **Odaberite automatski** i dodajte novi poslužitelj **u polje Aktualizacijski server** u jednom od sljedećih formata:  
*http://IP\_adresa\_servera:2221*  
*https://IP\_adresa\_servera:2221* (ako se koristi SSL)

## Pristup mirroru putem zajedničkih mrežnih mjesta

Najprije treba stvoriti zajedničku mapu na lokalnom ili mrežnom uređaju. Kada stvarate mapu za mirror, potrebno je omogućiti pristup za „pisanje“ za korisnika koji će spremiti aktualizirane datoteke u mapu i pristup za „čitanje“ za korisnika koji će aktualizirati ESET Endpoint Antivirus iz mape mirror.

Zatim konfigurirajte pristup mirroru tako da na kartici **Napredno podešavanje > Nadogradnja > Profili > Mirror za nadogradnju** deaktivirate opciju **Aktiviraj HTTP server**. Ta je opcija prema standardnim postavkama aktivirana u instalacijskom paketu programa.

Ako se zajednička mapa nalazi na nekom drugom računalu u mreži, morate unijeti podatke za prijavu za pristup tom drugom računalu. Za unos podataka za prijavu otvorite ESET Endpoint Antivirus **Napredno podešavanje** (F5) i kliknite **Nadogradnja > Profili > Nadogradnje > Opcije povezivanja > Zajedničke mreže Windowsa > Poveži se s LAN-om kao**. Ta je postavka ista kao i za nadogradnju, kao što je opisano u odjeljku [Poveži se s LAN-om kao](#).

Za pristup mapi mirrora to se mora učiniti s istoga računa koji je upotrijebljen za prijavu na računalo na kojemu je stvoren mirror. Ako se računalo nalazi u domeni, treba se upotrijebiti korisničko ime "domain\user". Ako računalo nije u domeni, treba upotrijebiti "IP\_address\_of\_your\_server\user" ili "hostname\user".

Nakon završetka konfiguracije mirrora, nastavite na radnim stanicama i postavite **||UNC|PATH** kao aktualizacijski server slijedeći korake u nastavku:

- 1.Otvorite ESET Endpoint Antivirus **Napredno podešavanje** i kliknite **Aktualizacija > Profili > Osnovno**.
- 2.Deaktivirajte odabir opcije **Odaberite automatski** pored **Nadogradnji modula** i dodajte novi server u polju

**Server za nadogradnju** koristeći se formatom **||UNC|PATH**.

**i** Radi pravilnog funkcioniranja put do mape mirrora potrebno je odrediti kao UNC put. Aktualizacije s mapiranih pogona možda neće raditi.

### Stvaranje mirrora pomoću mirror alata

Struktura mapa koju stvara mirror alat razlikuje se od onoga što čini mirror Endpoint programa. Svaka mapa sadržava datoteke za nadogradnju za skupinu programa. U postavkama nadogradnje programa koji se služi mirrorom morate navesti cijeli put do točne mape.

Primjerice, da biste s mirrora nadogradili ESET PROTECT, postavite [server za nadogradnju](#) na sljedeću adresu (prema osnovnoj lokaciji HTTP servera):

[http://your\\_server\\_address/mirror/eset\\_upd/era6](http://your_server_address/mirror/eset_upd/era6)

U zadnjem se odjeljku nalaze postavke za upravljanje programskim komponentama (PCU-ovima). Prema standardnim se postavkama preuzete komponente programa pripremaju za kopiranje u lokalni mirror. Ako je aktivirana mogućnost **Nadogradnja programskih komponenti**, nije potrebno kliknuti **Nadograđi** jer se datoteke automatski kopiraju na lokalni mirror kada postanu dostupne. Dodatne informacije o aktualizaciji programskih komponenti potražite u odjeljku [Način aktualizacije](#).

## Otklanjanje poteškoća s mirror aktualizacijom

U većini su slučajeva problemi tijekom aktualizacije s mirror servera izazvani neispravnim određivanjem mogućnosti mape za mirror, neispravnim podacima za autorizaciju pri pristupu mapi za mirror, neispravnom konfiguracijom na lokalnim radnim stanicama koje pokušavaju preuzeti aktualizacijske datoteke s mirrora ili kombinacijom navedenih razloga. Slijedi pregled najčešćih problema koji se mogu pojaviti tijekom aktualizacije s mirrora.

**ESET Endpoint Antivirus prijavljuje pogrešku pri povezivanju s mirror serverom** – Taj je problem vjerojatno prouzročilo neispravno određivanje aktualizacijskog servera (mrežnog puta do mape za mirror) s kojega lokalne radne stanice preuzimaju nadogradnje. Da biste provjerili mapu, u sustavu Windows kliknite **Start**, zatim **Pokreni**, unesite naziv mape pa kliknite **U redu**. Trebao bi se prikazati sadržaj mape.

**ESET Endpoint Antivirus zahtijeva korisničko ime i lozinku** – Problem se vjerojatno pojavio zbog neispravnog unosa podataka za autentikaciju (korisničkog imena i lozinke) u odjeljku nadogradnje. Korisničko ime i lozinka služe za omogućivanje pristupa aktualizacijskom serveru s kojega se program aktualizira. Provjerite jesu li podaci za autorizaciju točni i jesu li uneseni u pravilnom obliku. Na primjer, Domena/Korisničko ime ili Radna stanica/Korisničko ime te odgovarajuće lozinke. Ako je mirror server dostupan „svima”, imajte na umu da to ne znači da je svim korisnicima omogućen pristup. Pod pojmom „svi” ne podrazumijeva se bilo koji neovlašteni korisnik, već se podrazumijeva da mapi mogu pristupiti svi korisnici domene. Zbog toga je, čak i ako mapi mogu pristupiti „svi”, u odjeljak podešavanja nadogradnje potrebno unijeti korisničko ime i lozinku.

**ESET Endpoint Antivirus prijavljuje pogrešku pri povezivanju s mirror serverom** – Na portu definiranom za pristup HTTP verziji mirrora blokirana je komunikacija.

**ESET Endpoint Antivirus prijavljuje pogrešku prilikom preuzimanja datoteka za nadogradnju** – taj je problem vjerojatno uzrokovalo neispravno određivanje servera za nadogradnju (mrežnog puta do mape za mirror) s kojega lokalne radne stanice preuzimaju nadogradnje.

# Stvaranje aktualizacijskih zadataka

Aktualizacije se mogu ručno pokrenuti klikom opcije **Potraži aktualizacije** u primarnom prozoru koji se prikaže nakon što kliknete **Aktualizacija** u glavnom izborniku.

Aktualizacije je moguće pokretati i kao zakazane zadatke. Da biste konfigurirali planirani zadatak, kliknite **Alati > Planer**. Prema standardnim se postavkama u programu ESET Endpoint Antivirus aktiviraju sljedeći zadaci:

- **Redovna automatska aktualizacija**
- **Automatska aktualizacija po uspostavi modemske veze**
- **Automatska aktualizacija po prijavi korisnika**

Svaki aktualizacijski zadatak moguće je izmijeniti u skladu s vašim potrebama. Osim standardnih aktualizacijskih zadataka možete stvarati i nove aktualizacijske zadatke s korisnički definiranom konfiguracijom. Detalje o stvaranju i konfiguriranju aktualizacijskih zadataka potražite u odjeljku [Planer](#).

## Alati

Izbornik **Alati** sadrži module koji pojednostavuju administriranje programa i nude dodatne mogućnosti naprednim korisnicima.

Taj izbornik sadrži sljedeće alate:

- [Dnevnići](#)
- [Sigurnosno izvješće](#) (za računala kojima se ne upravlja)
- [Procesi koji se izvršavaju](#) (ako je ESET LiveGrid® aktiviran u programu ESET Endpoint Antivirus)
- [Nadzor aktivnosti](#)
- [Planer](#)
- [ESET SysInspector](#)
- [ESET SysRescue Live](#) – Preusmjerava vas na stranicu ESET SysRescue Live, gdje možete preuzeti sliku CD-a/DVD-a za ESET SysRescue Live .iso.
- [Karantena](#)
- [Slanje uzorka na analizu](#) – Omogućuje slanje sumnjive datoteke na analizu u Laboratorij za istraživanje tvrtke ESET (možda neće biti dostupno ovisno o konfiguraciji za ESET LiveGrid®).

The screenshot shows the main window of ESET Endpoint Antivirus. On the left sidebar, there are several icons and labels: STATUS ZAŠTITE (checkmark), SKENIRANJE RAČUNALA (magnifying glass), AKTUALIZACIJA (refresh), PODEŠAVANJE (gear), ALATI (briefcase), and POMOĆ I PODRŠKA (question mark). The main content area is titled "Alati". It contains a grid of tools: "Dnevnički" (Daily log) with a brief description; "Pokrenuti procesi" (Running processes) with a description mentioning ESET LiveGrid®; "Sigurnosno izvješće" (Security report) with a brief description; "Nadzor aktivnosti" (Activity monitoring) with a brief description; "ESET SysInspector" (with a disk icon) with a brief description; "Planer" (with a clock icon) with a brief description; "ESET SysRescue Live" (with a plus sign icon) with a brief description; "Slanje datoteke na analizu" (with a test tube icon) with a brief description; and "Karantena" (with a biohazard icon) with a brief description.

## Dnevnički

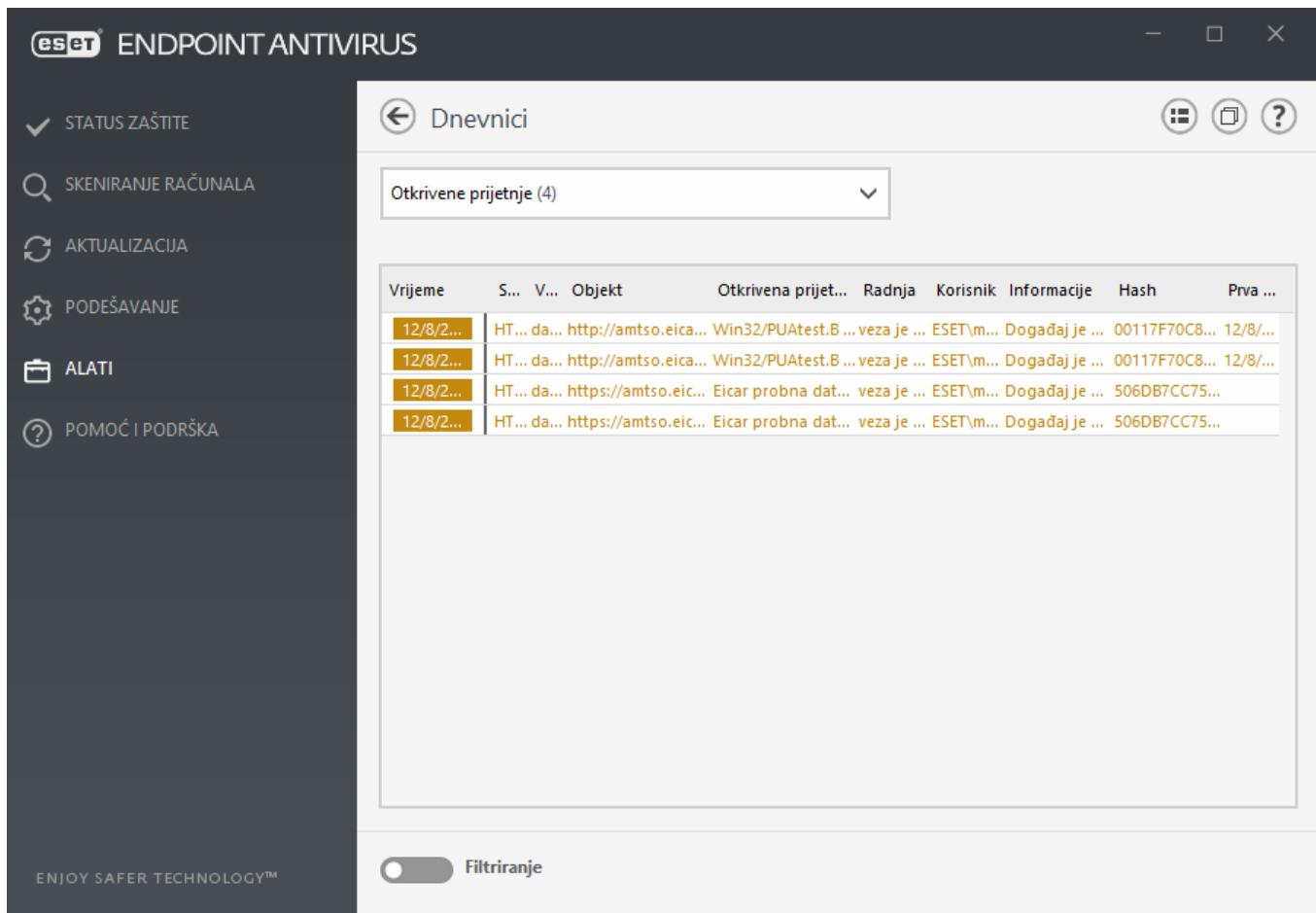
Dnevnički sadrže informacije o svim važnim događajima u programu koji su se pojavili i pružaju pregled otkrivenih prijetnji. Dnevnički su ključan alat za analizu sustava, otkrivanje prijetnji te otklanjanje poteškoća. Zapisivanje se izvodi aktivno u pozadini bez korisničke intervencije. Podaci se bilježe na temelju trenutnih postavki opsega zapisivanja. Prikaz tekstualnih poruka i dnevnika moguće je izravno iz okruženja programa ESET Endpoint Antivirus. Moguće je i arhiviranje dnevnika.

Dnevnicima se pristupa iz glavnog prozora programa klikom na **Alati > Dnevnički**. Odaberite željenu vrstu dnevnika s padajućeg izbornika **Dnevnik**. Dostupni su sljedeći dnevnici:

- Otkrivene prijetnje** – Ovaj dnevnik pruža detaljne informacije o otkrivenim prijetnjama i infiltracijama koje su otkrili moduli programa ESET Endpoint Antivirus. Ove informacije obuhvaćaju vrijeme i mjesto otkrivanja, naziv otkrivanja, izvršenu radnju te ime korisnika prijavljenog u trenutku otkrivanja prijetnje. Dvokliknite bilo koju stavku dnevnika da biste prikazali detalje u zasebnom prozoru. Neočišćene infiltracije uvijek su označene crvenim tekstom na svjetlocrvenoj pozadini, a očišćene infiltracije označene su žutim tekstom na bijeloj pozadini. Neočišćene potencijalno nepoželjne aplikacije ili potencijalno nesigurne aplikacije označene su žutim tekstom na bijeloj pozadini.
- Događaji** – sve važne radnje koje je obavio ESET Endpoint Antivirus zabilježene su u dnevniku događaja. Dnevnik događaja sadrži informacije o događajima i pogreškama do kojih je došlo u programu. Namijenjen je za pomoć administratorima sustava i korisnicima za rješavanje problema. Te informacije često mogu olakšati iznalaženje rješenja za problem koji se pojavio u programu.
- Skeniranje računala** – U ovom se prozoru prikazuju svi rezultati skeniranja. Svaki redak odgovara jednom

izvršenom procesu skeniranja računala. Na popisu izvršenih skeniranja bit će prikazana i nedovršena skeniranja (prekinuta od strane korisnika). Dvokliknite bilo koju stavku za prikaz detalja dotičnog skeniranja.

- **Blokirane datoteke** – sadrži zapise o blokiranim datotekama kojima se nije moglo pristupiti tijekom povezanosti s programom ESET Enterprise Inspector. Protokol prikazuje razlog i izvorni modul koji je blokira datoteku, kao i aplikaciju korisnika koji ju je pokrenuo. Za više informacija pogledajte [mrežni korisnički priručnik za ESET Enterprise Inspector](#).
- **Poslane datoteke** – Sadrži zapise datoteka koje su poslane sustavu ESET LiveGrid® ili [ESET Dynamic Threat Defense](#) na analizu.
- **Dnevni provjere** – svaki dnevnik sadrži podatke o datumu i vremenu promjene, vrsti promjene, opisu, izvoru i korisniku. Pogledajte odjeljak [Dnevni provjere](#) za više detalja.
- **HIPS** – Sadrži zapise određenih pravila označenih za zapisivanje. Protokol prikazuje aplikaciju koja je pozvala operaciju, rezultat (je li pravilo bilo dopušteno ili zabranjeno) i naziv stvorenog pravila.
- **Mrežna zaštita** – Dnevnik firewalla prikazuje sve udaljene napade koje je otkrila [Zaštita od mrežnog napada](#). Tu možete pronaći informacije o svim napadima na vaše računalo. U stupcu Događaj nalazi se popis otkrivenih napada. Stupac Izbor sadrži dodatne informacije o napadaču. Stupac Protokol otkriva komunikacijski protokol korišten u napadu. Analiza dnevnika firewalla može vam pomoći da na vrijeme otkrijete pokušaje infiltracije kako biste spriječili svaki pokušaj neovlaštenog pristupa sustavu. Dodatne pojedinosti o određenim mrežnim napadima potražite u odjeljku [IDS i napredne mogućnosti](#).
- **Filtrirane web stranice** – Taj je popis koristan kada želite pregledati popis web stranica koje je blokirala [Zaštita web pristupa](#). U tim dnevnicima možete vidjeti vrijeme, URL, korisnika i aplikaciju koja je stvorila vezu s određenom web stranicom.
- **Kontrola uređaja** – Sadrži zapise izmjenjivih medija ili uređaja koji su priključeni na računalo. U dnevnik se zapisuju samo uređaji s postavljenim pravilom kontrole uređaja. Ako pravilo ne odgovara priključenom uređaju, neće se stvoriti stavka dnevnika za priključeni uređaj. Tu možete vidjeti i pojedinosti kao što su vrsta uređaja, serijski broj, naziv proizvođača i veličina medija (ako je dostupno).



Odaberite sadržaj bilo kojeg dnevnika i pritisnite **Ctrl + C** kako biste ga kopirali u međuspremnik. Držite **Ctrl + Shift** kako biste odabrali više unosa.

Kliknite  **Filtriranje** da biste otvorili prozor [Filtriranje dnevnika](#) u kojem možete definirati kriterije za filtriranje.

Desnom tipkom miša kliknite određeni zapis kako biste otvorili kontekstni izbornik. Sljedeće mogućnosti dostupne su u kontekstnom izborniku:

- **Prikaži** – Prikazuje detaljne informacije o odabranom dnevniku u novom prozoru.
- **Filtriraj iste zapise** – Nakon aktiviranja tog filtra vidjet ćete samo zapise iste vrste (dijagnostika, upozorenja...).
- **Filtriraj** – Nakon što kliknete tu opciju, otvorit će se prozor [Filtriranje dnevnika](#) u kojem možete definirati kriterije za određene stavke u dnevniku.
- **Aktiviraj filter** – Aktivira postavke filtra.
- **Deaktiviraj filter** – Poništava sve postavke filtra (kao što je gore opisano).
- **Kopiraj / Kopiraj sve** – Kopira informacije o svim zapisima u prozoru.
- **Izbriši / Izbriši sve** – Briše odabrane zapise ili sve prikazane zapise – ova radnja zahtijeva administratorske ovlasti.
- **Izvezi** – Izvozi informacije o zapisima u XML obliku.

- **Izvezi sve** – Izvozi informacije o svim zapisima u XML obliku.
- **Pronađi / Pronađi sljedeće / Pronađi prethodno** – nakon što kliknete ovu opciju, prozor Filtriranje dnevnika omogućit će vam da definirate kriterije za filtriranje da biste istaknuli određeni unos.
- **Stvori izuzetak** – Stvorite novi [izuzetak za detekciju pomoću čarobnjaka](#) (nije dostupno za detekciju zlonamjernog softvera).

## Filtriranje dnevnika

Kliknite  **Filtriranje** na kartici **Alati > Dnevnići** za određivanje kriterija za filtriranje.

Funkcija filtriranja dnevnika pomoći će vam da pronađete informacije koje tražite, posebice kada imate mnogo zapisova. Omogućuje vam sužavanje zapisova dnevnika, na primjer ako tražite određenu vrstu događaja, status ili vremensko razdoblje. Možete filtrirati zapisove dnevnika navođenjem određenih opcija pretraživanja; u prozoru Dnevnika prikazat će se samo relevantni zapisovi (prema navedenim opcijama pretraživanja).

Upišite ključnu riječ koju tražite u polje **Pronađi tekst**. Upotrijebite padajući izbornik **Traži u stupcima** kako biste suzili svoje pretraživanje. Odaberite jedan ili više zapisova iz padajućeg izbornika **Vrste zapisova dnevnika**. Odredite **Vremensko razdoblje** iz kojeg želite prikazati rezultate. Također možete upotrijebiti dodatne opcije pretraživanja, kao što su **Traži samo cijele riječi** ili **Osjetljivo na velika i mala slova**.

### Pronađi tekst

Upišite niz teksta (rijec ili dio riječi). Prikazat će se samo zapisovi koji sadrže taj niz. Ostali zapisovi bit će izostavljeni.

### Traži u stupcima

Odaberite stupce koji će se uzeti u obzir prilikom pretraživanja. Možete označiti jedan stupac ili više njih za pretraživanje.

### Vrste zapisova

Odaberite jednu vrstu zapisova dnevnika ili više njih u padajućem izborniku:

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa te svi prethodno navedeni zapisovi.
- **Informativno** – Zapisuju se sve informativne poruke, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisovi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke s upozorenjima.
- **Pogreške** – Zapisuju se pogreške kao što je „Pogreška preuzimanja datoteke“ i kritične pogreške.
- **Kritično** – Zapisuju se samo kritične pogreške (pogreška pri pokretanju antivirusne zaštite).

### Vremensko razdoblje

Definirajte vremensko razdoblje od kojeg želite prikazati rezultate.

- **Nije određeno** (standardno) – Ne pretražuje unutar vremenskog razdoblja, već pretražuje čitav dnevnik.
- **Prošli dan**
- **Zadnje viđen**
- **Prošli mjesec**

- **Vremensko razdoblje** – Možete navesti točno vremensko razdoblje (Od: i Do:) da biste filtrirali samo zapise iz određenog vremenskog razdoblja.

## Traži samo cijele riječi

Upotrijebite potvrđni okvir ako želite tražiti čitave riječi kako biste dobili preciznije rezultate.

## Osjetljivo na velika i mala slova

**Aktivirajte** ovu opciju ako vam je važno da se velika i mala slova razlikuju tijekom filtriranja. Nakon što konfigurirate opcije filtriranja/pretraživanja, kliknite **U redu** da biste prikazali filtrirane zapise dnevnika ili **Pronađi** da biste započeli pretraživanje. Dnevnički se pretražuju od vrha prema dnu, počevši od trenutačnog položaja (zapis koji je istaknut). Pretraživanje se zaustavlja kada se pronađe prvi odgovarajući zapis. Pritisnite **F3** da biste tražili sljedeći zapis ili kliknite desnom tipkom miša i odaberite **Pronađi** da biste suzili opcije pretraživanja.

# Konfiguracija zapisivanja

Konfiguraciji zapisivanja u programu ESET Endpoint Antivirus može se pristupiti s glavnog prozora programa. Kliknite **Podešavanje > Napredno podešavanje > Alati > Dnevnički**. Odjeljak dnevnika koristi se za definiranje načina upravljanja dnevnicima. Da bi oslobodio prostor na tvrdom disku, program automatski briše starije zapise. Za dnevnike možete definirati sljedeće mogućnosti:

**Minimalni opseg vođenja dnevnika** – Tu se određuje minimalni opseg podataka za događaje koji se zapisuju u dnevnik.

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguiranje programa te svi prethodno navedeni zapisi.
- **Informativno** – Zapisuju se sve informativne poruke, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke s upozorenjima.
- **Pogreške** – Zapisuju se pogreške kao što je „Pogreška preuzimanja datoteke“ i kritične pogreške.
- **Kritično** – Zapisuju se samo kritične pogreške (pogreška pri pokretanju antivirusne zaštite, itd.).



Kada odaberete razinu opsega **dijagnostike**, zapisat će se sve blokirane veze.

Unosi u dnevniku koji su stariji od broja dana definiranog u polju **Automatski izbriši zapise starije od (dana)** automatski će se izbrisati.

**Automatski optimiziraj dnevničke** – Kada je ova opcija aktivirana, dnevnički će se automatski defragmentirati ako je postotak fragmentacije viši od vrijednosti naznačene u polju **Ako broj nekorištenih zapisa premašuje (%)**.

Kliknite **Optimiziraj** za pokretanje defragmentiranja dnevnika. Uklanjaju se svi prazni unosi u dnevnik kako bi se poboljšala radna svojstva i brzina obrade. To poboljšanje primjećuje se osobito ako dnevnički sadrže velik broj unosa.

Mogućnost **Aktiviraj tekstualni protokol** omogućuje pohranu dnevnika u drugom formatu, zasebno od [dnevnika](#):

- **Ciljani direktorij** – Odaberite direktorij u kojem će se pohraniti dnevnički (odnosi se samo na Tekst/CSV). Možete kopirati put ili odabrati drugi direktorij klikom na **Očisti**. Svaki odjeljak dnevnika ima vlastitu datoteku s unaprijed definiranim nazivom datoteke (primjerice, *virlog.txt* za odjeljak **Otkrivena prijetnje** u dnevniku ako želite koristiti običan format tekstualne datoteke za pohranu dnevnika).
- **Vrsta** – ako odaberete format datoteke **Tekst**, dnevnički će se pohraniti u tekstualnoj datoteci i podaci će se razdvojiti na kartice. Isto se primjenjuje za podatke odvojene zarezom u **CSV** datoteci. Ako odaberete **Događaj**, dnevnički će se umjesto u datoteku pohranjivati u dnevnik Windows Event (može se pregledati uz pomoć programa Event Viewer na upravljačkoj ploči).
- **Izbriši sve dnevnički** – briše sve pohranjene dnevničke koji su trenutačno odabrani u padajućem izborniku **Vrsta**. Prikazat će se obavijest o uspješnom brisanju dnevnika.

**Aktiviraj praćenje konfiguracijskih promjena u dnevniku provjere** – informira vas o svakoj promjeni konfiguracije. Pogledajte odjeljak [Dnevnički provjere](#) za više informacija.

**i** Kako biste pomogli u bržem rješavanju problema, tvrtka ESET od vas može zatražiti dnevničke s vašeg računala. ESET Log Collector omogućuje lako prikupljanje potrebnih informacija. Dodatne informacije o alatu ESET Log Collector potražite u [članku u ESET-ovoj bazi znanja](#).

## Dnevnički provjere

U korporativnom okruženju obično postoji više korisnika s definiranim pravima pristupa konfiguraciji krajnjih točaka. Preinaka konfiguracije programa može dramatično utjecati na rad programa i zato je vrlo važno da administratori prate promjene koje korisnici izvršavaju da bi brzo prepoznali i riješili problem te spriječili pojavu istog ili sličnih problema u budućnosti.

Dnevnik provjere nova je vrsta vođenja dnevnika u programu ESET Endpoint Antivirus verzije 7.1 i rješenje je za prepoznavanje izvora problema. Dnevnik provjere prati promjene u konfiguraciji ili stanju zaštite i stvara snimke za kasniju upotrebu.

Da biste vidjeli **Dnevnik provjere**, kliknite **Alati** u glavnom izborniku te kliknite **Dnevnički** i odaberite **Dnevnički provjere** iz padajućeg izbornika.

Dnevnik provjere sadrži sljedeće podatke:

- Vrijeme – kada je promjena provedena
- Vrsta – koja je vrsta postavke ili funkcije promijenjena
- Opis – što se točno promijenilo, koji dio postavke se promijenio i broj promijenjenih postavki
- Izvor – gdje se nalazi izvor promjene
- Korisnik – tko je napravio promjenu

Vrijeme	Vrsta	Opis	Izvor	Korisnik
12/8/2020 ...	Funkcija je pro...	Botnet je promijenio stanje s Neaktivno na Aktivno.	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Zaštita od mrežnog napada (IDS) je promijen...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Antiphishing je promijenio stanje s Neaktivno...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Antiphishing je promijenio stanje s Aktivno n...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Antiphishing je promijenio stanje s Neaktivno...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Zaštita od mrežnog napada (IDS) je promijen...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Kontrola uređaja je promijenio stanje s Neakti...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Zaštita dokumenata je promijenio stanje s Ne...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Rezidentna zaštita sistemskih datoteka je pro...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Anti-Ransomware je promijenio stanje s Neaktiv...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Sprečavanje ranjivosti je promijenio stanje s ...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Napredni skener memorije je promijenio stanj...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	HIPS je promijenio stanje s Neaktivno na Aktiv...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Botnet je promijenio stanje s Neaktivno na Ak...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Zaštita od mrežnog napada (IDS) je promijen...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Antiphishing je promijenio stanje s Neaktivno...	SUSTAV	NT AUTHORITY\SYSTEM
12/8/2020 ...	Funkcija je pro...	Antiphishing je promijenio stanje s Aktivno n...	SUSTAV	NT AUTHORITY\SYSTEM

U prozoru Dnevniči desnom tipkom miša kliknite bilo koju vrstu dnevnika provjere s **promijenjenim postavkama** i odaberite **Pokaži promjene** iz kontekstnog izbornika za prikaz detaljnih podataka o provedenoj promjeni. Osim toga možete vratiti promjenu postavke tako da kliknete **Vrati** u kontekstnom izborniku (nije dostupno za programe kojima se upravlja pomoću programa ESMC ili ESET PROTECT). Ako odaberete **Obrisí sve** u kontekstnom izborniku, stvorit će se dnevnik s podacima o toj radnji.

Ako je aktivirana opcija **Automatski optimiziraj dnevničke** u izborniku **Napredno podešavanje > Alati > Dnevniči**, dnevničke provjere automatski će se defragmentirati kao ostali dnevnički.

Ako je aktivirana opcija **Automatski obriši zapise starije od (u danima)** u izborniku **Napredno podešavanje > Alati > Dnevniči**, dnevničke provjere stariji od navedenog broja dana automatski će se obrisati.

## Planer

Planer upravlja planiranim zadacima s unaprijed definiranom konfiguracijom i svojstvima i pokreće ih.

Planeru se može pristupiti iz glavnog programskog prozora programa ESET Endpoint Antivirus klikom na **Alati > Planer**. Planer sadrži popis svih planiranih zadataka i njihova konfiguracijska svojstva, primjerice unaprijed definirani datum i vrijeme te profil skeniranja koji se koristi.

Planer služi za planiranje sljedećih zadataka: aktualizacije modula za otkrivanje virusa, zadataka skeniranja, provjera datoteke pokretanja sustava i održavanje dnevnika. Možete dodavati i brisati zadatake izravno iz glavnog prozora Planera (klikom na gumb **Dodaj zadatak** ili **Izbriši** koji se nalaze u donjem dijelu). Kliknite desnom tipkom miša na bilo koji zadatak u Planeru da biste izvršili sljedeće akcije: prikazali detaljne informacije, odmah izvršili zadatak, dodali novi zadatak ili izbrisali postojeći. Potvrđnim okvirima na početku svakog unosa aktivirajte ili

deaktivirajte zadatke.

Prema standardnim postavkama **Planer** prikazuje sljedeće planirane zadatke:

- **Održavanje dnevnika**
- **Redovna automatska aktualizacija**
- **Automatska aktualizacija po uspostavi modemske veze**
- **Automatska aktualizacija po prijavi korisnika**
- **Automatska provjera pokretačkih datoteka** (nakon prijave korisnika)
- **Automatska provjera datoteke pokretanja** (nakon uspješne aktualizacije modula)

Da biste uredili konfiguraciju postojećeg zakazanog zadatka (standardnu ili korisnički definiranu), desnom tipkom miša kliknite zadatak i kliknite **Uredi** ili odaberite zadatak koji želite izmijeniti pa kliknite gumb **Uredi**.

The screenshot shows the ESET Endpoint Antivirus software interface. On the left, there's a sidebar with icons for Status zaštite, Skeniranje računala, Aktualizacija, podešavanje, Alati, and Pomoć i podrška. The main area is titled 'Planer' and displays a table of scheduled tasks. The columns are: Zadatak, Naziv, Okidači, Sljedeće pokretanje, and Zadnje pokretanje. The tasks listed are:

Zadatak	Naziv	Okidači	Sljedeće pokretanje	Zadnje pokretanje
<input checked="" type="checkbox"/>	Održavanje dnev...	Održavanje dnevnika	Zadatak će se pokren...	12/9/2020 2:00:00 AM
<input checked="" type="checkbox"/>	Nadogradnja	Redovita automatska ...	Zadatak će se pokren...	12/8/2020 4:23:58 PM
<input checked="" type="checkbox"/>	Nadogradnja	Automatska nadogra...	Modemska veza s inte...	Pri događaju
<input type="checkbox"/>	Nadogradnja	Automatska nadogra...	Prijava korisnika (najv...	Pri događaju
<input checked="" type="checkbox"/>	Provjera datoteke...	Provjera datoteka koj...	Prijava korisnika Zada...	Pri događaju
<input checked="" type="checkbox"/>	Provjera datoteke...	Provjera datoteka koj...	Uspješna nadogradnj...	Pri događaju

At the bottom, there are buttons for Dodavanje zadatka, Uredi, Izbrisati, and Standardno.

## Dodavanje novog zadatka

1. Kliknite **Dodaj zadatak** na dnu prozora.
2. Unesite naziv zadatka.
3. Odaberite željeni zadatak iz padajućeg izbornika:

- **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
- **Održavanje dnevnika** – Dnevniči sadrže i zaostatke već izbrisanih zapisa. Taj zadatak redovito optimizira zapise u dnevnicima radi učinkovitijeg rada.
- **Provjera datoteke za pokretanje sustava** – Provjerava datoteke kojima je dopušteno pokretanje prilikom pokretanja sustava ili prijave.
- **Stvori snimku statusa računala** – Stvara snimku računala pomoću programa ESET SysInspector – prikuplja detaljne informacije o komponentama sustava (primjerice upravljačkim programima, aplikacijama) i procjenjuje razinu rizika za svaku komponentu.
- **Skeniranje računala na zahtjev** – Izvodi skeniranje datoteka i mapa na računalu.
- **Aktualizacija** – Planira zadatak aktualizacije aktualizacijom modula za otkrivanje virusa i programskih modula.

4. Uključite prekidač **Aktiviraj** ako želite aktivirati zadatak (možete to učiniti kasnije odabirom potvrđnog okvira na popisu planiranih zadataka), a zatim kliknite **Sljedeće** i odaberite jednu od vremenskih mogućnosti:

- **Jednom** – Zadatak će se izvršiti na unaprijed definirani datum i vrijeme.
- **Opetovano** – Zadatak će se izvršavati u navedenim vremenskim intervalima.
- **Svakodnevno** – Zadatak će se izvršavati opetovano svakog dana u isto vrijeme.
- **Tjedno** – Zadatak će se izvršiti na određeni dan i u određeno vrijeme.
- **Pri događaju** – Zadatak će se izvršiti kod određenog događaja.

5. Odaberite mogućnost **Nemoj izvršavati zadatak ako računalo koristi bateriju** da biste minimizirali korištenje sistemskih resursa dok prijenosno računalo koristi bateriju. Zadatak će se izvršiti na datum i vrijeme zadani u poljima **Izvršavanje zadataka**. Ako se zadatak nije mogao izvršiti u unaprijed definirano vrijeme, možete navesti kada će se ponovno izvršiti odabirom sljedećih mogućnosti:

- **U sljedećem zakazanom terminu**
- **Što prije**
- **Odmah, ako vrijeme proteklo od zadnjeg izvršavanja premašuje određenu vrijednost** (interval se može definirati putem okvira za listanje **Vrijeme od zadnjeg izvršavanja**)

Možete pregledati planirane zadatke desnim klikom i odabirom **Prikaži detalje zadatka**.

**Naziv zadatka**

Automatska aktualizacija po prijavi korisnika

**Vrsta zadatka**

Aktualizacija

**Izvrši zadatak**

Prijava korisnika (najviše jednom u/na sat)

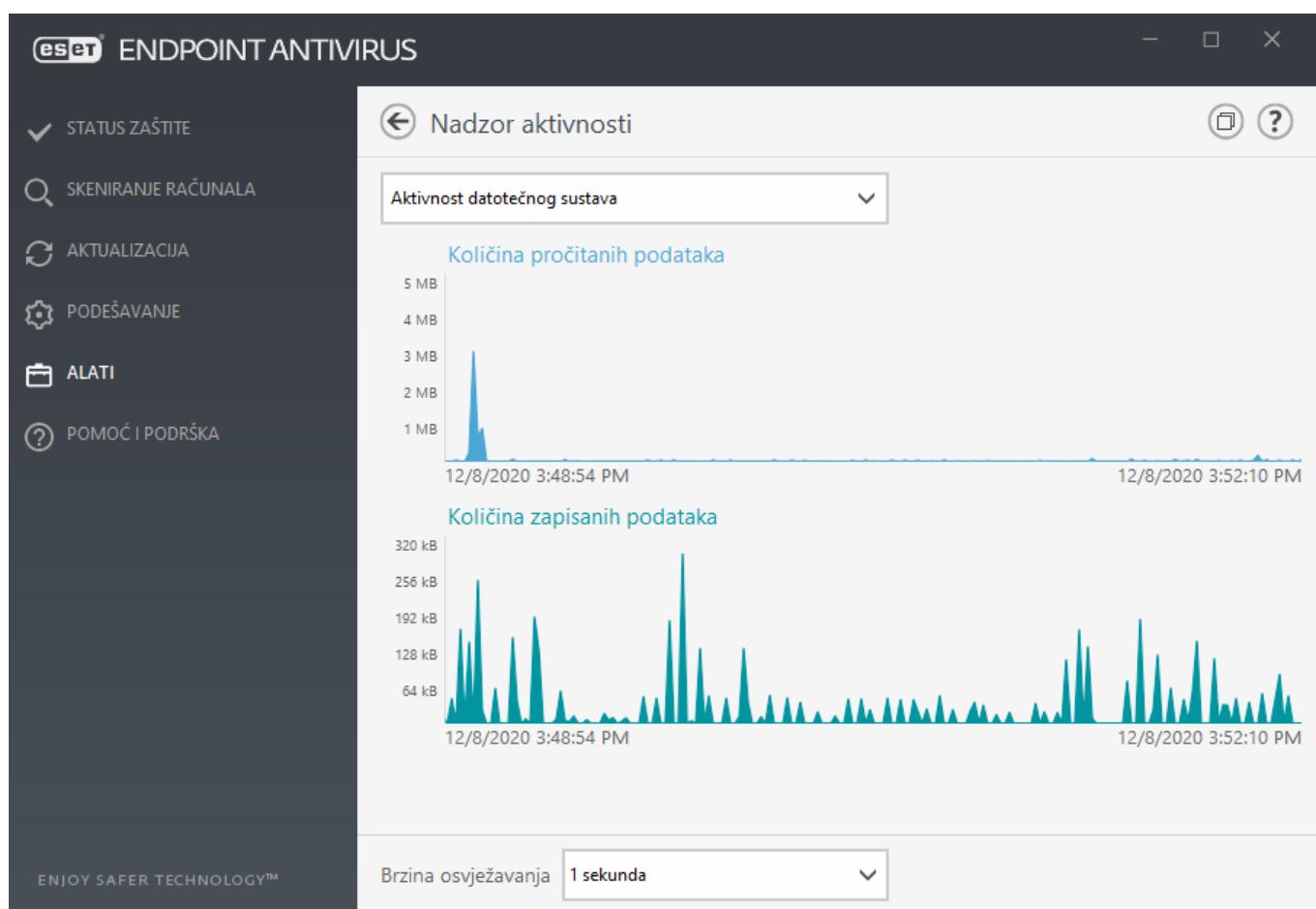
Akcija koju treba poduzeti ako se zadatak ne izvrši u zadano vrijeme

U sljedećem zakazanom terminu

[U redu](#)

## Nadzor aktivnosti

Da biste trenutačnu **Aktivnost datotečnog sustava** vidjeli u obliku grafa, kliknite **Alati > Nadzor aktivnosti**. Pri dnu grafikona nalazi se vremenska crta na kojoj je zapisana aktivnost datotečnog sustava u stvarnom vremenu na osnovi odabranog vremenskog raspona. Da biste promijenili vremenski raspon, odaberite nešto s padajućeg izbornika **Brzina osvježavanja**.



Na raspolaganju su sljedeće mogućnosti:

- **Korak: 1 sekunda** – Graf se osvježava svake sekunde, a vremenska crta pokriva posljednjih 10 minuta.
- **Korak: 1 minuta (zadnja 24 sata)** – Graf se osvježava svake minute, a vremenska crta pokriva posljednja 24 sata.
- **Korak: 1 sat (zadnji mjesec)** – Graf se osvježava svakog sata, a vremenska crta pokriva posljednjih mjesec dana.
- **Korak: 1 sat (odabrani mjesec)** – Graf se osvježava svakog sata, a vremenska crta pokriva posljednjih X odabralih mjeseci.

Vertikalna os grafikona **Aktivnost datotečnog sustava** predstavlja količinu pročitanih podataka (plava boja) i zapisanih podataka (tirkizna boja). Obje vrijednosti izražene su u KB (kilobajtima) / MB / GB. Prijeđete li mišem preko pročitanih ili napisanih podataka u kazalu ispod grafikona, na grafikonu će se prikazati podaci samo za jednu od tih aktivnosti.

## ESET SysInspector

[ESET SysInspector](#) aplikacija je koja temeljito pregledava računalo i prikuplja detaljne informacije o komponentama sustava kao što su upravljački programi i aplikacije, mrežne veze ili važni unosi u registar te ocjenjuje razinu rizika svake komponente. Te informacije mogu olakšati određivanje uzroka sumnjivog ponašanja sustava do kojeg može doći zbog nekompatibilnosti softvera ili hardvera ili zbog zaraze zlonamjernim programom. [Pogledajte i online korisnički priručnik za ESET SysInspector.](#)

U prozoru alata SysInspector prikazuju se sljedeći podaci o stvorenim dnevnicima:

- **Vrijeme** – Vrijeme stvaranja dnevnika.
- **Komentar** – Kratki komentar.
- **Korisnik** – Ime korisnika koji je stvorio dnevnik.
- **Status** – Status stvaranja dnevnika.

Na raspolaganju su sljedeće akcije:

- **Prikaži** – Otvara stvoreni dnevnik. Možete i desnom tipkom miša kliknuti dotični dnevnik i odabratи mogućnost **Prikaži** na kontekstnom izborniku.
- **Usporeди** – uspoređuje dva postojeća dnevnika.
- **Stvori** – Stvara novi dnevnik. Pričekajte da značajka ESET SysInspector završi s radom (za status dnevnika prikazat će se **Stvoren**) prije nego pokušate pristupiti dnevniku.
- **Izbriši** – Briše odabrane dnevниke s popisa.

Ako odaberete jedan ili više dnevnika, na kontekstnom izborniku bit će dostupne sljedeće stavke:

- **Prikaži** – Otvara odabrani dnevnik u ESET SysInspector (ista funkcija kao i dvoklik dnevnika).
- **Usporeди** – uspoređuje dva postojeća dnevnika.

- **Stvori** – Stvara novi dnevnik. Pričekajte da značajka ESET SysInspector završi s radom (za status dnevnika prikazat će se **Stvoren**) prije nego pokušate pristupiti dnevniku.
- **Obriši** – Briše odabrani dnevnik.
- **Izbriši sve** – Briše sve dnevниke.
- **Izvezi** – Izvozi dnevnik u .xml datoteku ili komprimiranu .xml datoteku.

## Zaštita na bazi clouda

ESET LiveGrid® (konstruiran na temelju naprednog sustava ranog upozorenja ESET ThreatSense.Net) prikuplja podatke koje šalju korisnici ESET-ovih programa diljem svijeta i prosljeđuje ih u Laboratorij za istraživanje tvrtke ESET. Pružanjem sumnjivih uzoraka i metapodataka "from the wild" (iz opće upotrebe) ESET LiveGrid® omogućuje nam da brzo reagiramo na potrebe svojih korisnika i da održimo ESET-ovu sposobnost reagiranja na najnovije prijetnje.

Postoje tri opcije:

### Opcija 1: aktivacija sustava reputacije ESET LiveGrid®

Sustav reputacije ESET LiveGrid® omogućuje stvaranje popisa pouzdanih i nepoželjnih adresa na temelju cloud tehnologije.

Provjerite reputaciju [pokrenutih procesa](#) i datoteka izravno iz sučelja programa ili kontekstnog izbornika uz dodatne informacije koje su dostupne u sustavu ESET LiveGrid®.

### Opcija 2: aktivacija sustava za povratne informacije ESET LiveGrid®

Uz sustav reputacije ESET LiveGrid®, sustav za povratne informacije ESET LiveGrid® prikupljat će informacije o vašem računalu koje se odnose na nove pronađene prijetnje. Te informacije mogu obuhvaćati uzorak ili kopiju datoteke u kojoj se pojavila prijetnja, put do te datoteke, naziv datoteke, datum i vrijeme, proces u kojem se prijetnja pojavila na računalu i informacije o operacijskom sustavu računala.

Prema standardnim je postavkama sustav ESET Endpoint Antivirus konfiguriran tako da šalje sumnjive datoteke na detaljnu analizu u laboratorij tvrtke ESET za otkrivanje virusa. Datoteke s ekstenzijama kao što su *.doc* ili *.xls* uvijek se isključuju. Ako postoje određene datoteke koje vi ili vaša tvrtka ne želite slati, možete dodati i njihove ekstenzije.

### Opcija 3: neaktiviranje sustava ESET LiveGrid®

Funkcionalnost softvera ostat će ista, ali u nekim slučajevima ESET Endpoint Antivirus možda će na nove prijetnje reagirati brže od nadogradnje baze podataka virusnih potpisa kada je aktiviran ESET LiveGrid®.

**i** Pročitajte više o sustavu ESET LiveGrid® u [rječniku](#).  
Pogledajte naše [ilustrirane upute](#) dostupne na engleskom i na još nekoliko jezika za aktiviranje i deaktiviranje sustava ESET LiveGrid® u programu ESET Endpoint Antivirus.

## Konfiguracija zaštite utemeljene na clodu u naprednom podešavanju

Za pristup postavkama za ESET LiveGrid® pritisnite **F5** da biste ušli u napredno podešavanje i proširite stavku **Modul detekcije > Zaštita na bazi clouda**.

**Aktiviraj sustav reputacije ESET LiveGrid® (preporučeno)** – sustav reputacije ESET LiveGrid® poboljšava učinkovitost ESET-ovih rješenja za zaštitu od zlonamjernog softvera uspoređujući skenirane datoteke s bazom podataka popisa pouzdanih i nepouzdanih adresa u clodu.

**Aktiviraj sustav za povratne informacije ESET LiveGrid®** – Šalje laboratoriju tvrtke ESET za istraživanje relevantne podatke (opisane u odjeljku **Slanje uzorka** u nastavku) uz izvješća o padu sustava i statistiku radi daljne analize.

**Aktiviraj ESET Dynamic Threat Defense** (nije vidljivo u programu ESET Endpoint Antivirus) – ESET Dynamic Threat Defense ESET-ov je plaćeni servis. Njegova je svrha dodati sloj zaštite koji je posebno osmišljen za ublažavanje novonastalih prijetnji. Sumnjive datoteke automatski se šalju u ESET-ov cloud. U clodu ih analiziraju naši [napredni moduli detekcije zlonamjernih programa](#). Korisnik koji je pružio uzorak primit će izvješće o ponašanju sa sažetkom ponašanja promatranog uzorka.

**Pošalji izvješća o padu sustava i dijagnostičke podatke** – Pošaljite dijagnostičke podatke povezane sa sustavom ESET LiveGrid® kao što su izvješća o padu sustava i slike stanja memorije modula. Preporučujemo da ostane aktiviran kako bi pomogao tvrtki ESET u dijagnostici problema, poboljšavanju programa i osiguravanju bolje zaštite krajnjih korisnika.

**Pošalji anonimnu statistiku** – Dopustite tvrtki ESET da prikupi informacije o novootkrivenim prijetnjama kao što su naziv prijetnje, datum i vrijeme otkrivanja, način otkrivanja i povezani metapodaci, verzija programa i konfiguracija, uključujući informacije o vašem sustavu.

**E-pošta za kontakt (nije obavezno)** – Vaša adresa e-pošte za kontakt može se uključiti uz sumnjive datoteke i može se koristiti ako za analizu budu potrebne dodatne informacije. Imajte na umu da vam ESET neće slati odgovor ako ne budu potrebne dodatne informacije.

## Napredno podešavanje

 X ?
MODUL DETEKCIJE 2

Rezidentna zaštita sistemskih datoteka

## Zaštita potpomognuta cloudom

Skeniranje zlonamjernog softvera

HIPS 2NADOGRADNJA 2

## MREŽNA ZAŠTITA

WEB I E-POŠTA 3KONTROLA UREĐAJA 2ALATI 3KORISNIČKO SUČELJE 1

## ZAŠTITA POTPOMOZNUTA CLOUDOM

Aktiviraj ESET LiveGrid® sustav reputacije (preporučeno)

i

Aktiviraj sustav za povratne informacije programa ESET LiveGrid®

i

Pošalji izvješća o padu sustava i dijagnostičke podatke

i

Pošalji anonimnu statistiku

i

Adresa e-pošte za kontakt (nije obavezno)

i

## + SLANJE UZORAKA

Standardno

U redu

Odustani

## Slanje uzoraka

**Ručno slanje uzoraka** – aktivira opciju ručnog slanja uzorka ESET-u iz kontekstnog izbornika, opcije [Karantena](#) ili opcije [Alati > Slanje uzorka na analizu](#).

## Automatsko slanje otkrivenih uzoraka

Odaberite vrstu uzorka koji će se slati tvrtki ESET na analizu i poboljšajte buduće otkrivanje prijetnji. Dostupne su sljedeće opcije:

- **Svi otkriveni uzorci** – svi [objekti](#) koje otkrije [modul detekcije](#) (uključujući potencijalno nepoželjne aplikacije kada je to aktivirano u postavkama skenera).
- **Svi uzorci osim dokumenata** – Svi otkriveni objekti osim [dokumenata](#) (pogledajte u nastavku).
- **Ne šalji** – Otkriveni objekti neće se poslati tvrtki ESET.

## Automatsko slanje sumnjivih uzoraka

I ovi će se uzorci poslati tvrtki ESET u slučaju da ih modul detekcije nije otkrio. Na primjer, uzorci koji gotovo nisu otkriveni ili uzorci koji jedan od [modula zaštite](#) programa ESET Endpoint Antivirus smatra sumnjivima ili nejasnima.

- **Izvršne datoteke** – Uključuje datoteke poput .exe, .dll, .sys.
- **Arhive** – Uključuje vrste datoteka poput .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

- **Skripte** – Uključuje vrste datoteka poput .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Ostalo** – Uključuje vrste datoteka poput .jar, .reg, .msi, .sfw, .lnk.
- **Moguće neželjene poruke e-pošte** – Time će se omogućiti slanje mogućih neželjenih dijelova ili cijelovitih neželjenih poruka e-pošte s privicima tvrtki ESET radi daljnje analize. Aktiviranjem ove opcije poboljšava se globalno otkrivanje neželjene pošte, kao i buduće otkrivanje vaše neželjene pošte.
- **Dokumenti** – Uključuje dokumente programa Microsoft Office ili PDF s aktivnim sadržajem ili bez njega.

■ [Proširivanje popisa svih obuhvaćenih vrsta datoteka dokumenata](#)

ACCDB, ACCDT, DOC, DOC\_OLD, DOC\_XML, DOCM, DOCX, DWFX, EPS, IWORK\_NUMBERS, IWORK\_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2\_ENCRYPTED, OLE2\_MACRO, OLE2\_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT\_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD\_XML, WPC, WPS, XLS, XLS\_XML, XLSB, XLSM, XLSX, XPS

### Izuzeci

[Filtar izuzetaka](#) omogućuje vam da izuzmete određene datoteke/mape od slanja (primjerice, možete izuzeti datoteke koje mogu sadržavati povjerljive informacije, kao što su dokumenti ili proračunske tablice). Datoteke s popisa nikada se neće slati u laboratorije tvrtke ESET na analizu, čak ni ako sadrže sumnjiv kod. Najčešće vrste datoteka izostavljaju se prema standardnim postavkama (.doc itd.). Ako želite, na popis izuzetih datoteka možete dodati druge datoteke.

✓ Da biste izuzeli datoteke preuzete s web stranice download.domain.com, idite na **Napredno podešavanje > Zaštita na bazi clouda > Slanje uzoraka > Izuzeci** i dodajte izuzetak .download.domain.com.

## ESET Dynamic Threat Defense

Za aktiviranje servisa ESET Dynamic Threat Defense na klijentskom računalu pomoću ESET PROTECT web konzole pogledajte [EDTD konfiguraciju za ESET Endpoint Antivirus](#).

---

Ako ste ranije koristili sustav ESET LiveGrid® i deaktivirali ste ga, možda još uvijek ima paketa podataka koje treba poslati. Ti će se paketi slati tvrtki ESET čak i nakon deaktivacije. Nakon što sve trenutačne informacije budu poslane novi se paketi neće stvarati.

## Filtar izuzetaka za zaštitu na bazi clouda

Filtar izuzetaka omogućuje vam izuzimanje određenih datoteka ili mapa od slanja. Datoteke s popisa nikada se neće slati u laboratorije tvrtke ESET na analizu, čak i ako sadrže sumnjiv kod. Česte se vrste datoteka (kao što je .doc itd.) izostavljaju prema standardnim postavkama.

ℹ Ova je značajka korisna za izuzimanje datoteka koje mogu sadržavati povjerljive informacije, kao što su dokumenti ili proračunske tablice.

✓ Da biste izuzeli datoteke preuzete s web stranice download.domain.com, idite na **Napredno podešavanje > Zaštita na bazi clouda > Slanje uzoraka > Izuzeci** i dodajte izuzetak .download.domain.com.

# Procesi koji se izvršavaju

Procesi koji se izvršavaju prikazuju programe i procese pokrenute na računalu i ESET se odmah i neprekidno obavlještava o novim infiltracijama. ESET Endpoint Antivirus pruža detaljne informacije o procesima koji se izvršavaju kako bi zaštitio korisnike pomoću tehnologije [ESET LiveGrid®](#).

The screenshot shows the ESET Endpoint Antivirus interface. On the left, there's a sidebar with icons for Status zaštite, Skeniranje računala, Aktualizacija, Podešavanje, Alati, and Pomoć i podrška. Below that is the slogan 'ENJOY SAFER TECHNOLOGY™'. The main window title is 'Pokrenuti procesi'. It contains a message: 'U ovom prozoru prikazan je popis odabranih datoteka s dodatnim informacijama iz sustava ESET LiveGrid®. Za svaku je naznačena reputacija, broj korisnika i vrijeme prvo otvaranja.' A table lists running processes:

Reputacija	Proces	PID	Broj korisnika	Vrijeme otkr...	Naziv aplikacije
██████	smss.exe	352	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	csrss.exe	476	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	wininit.exe	552	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	winlogon.exe	644	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	services.exe	664	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	lsass.exe	672	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	svchost.exe	804	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	fontdrvhost.exe	812	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	dwm.exe	388	██████████	prije 1 mjeseca	Microsoft® Windows® Op...
██████	vboxservice.exe	1564	██████████	prije 1 godine	Oracle VM VirtualBox Guest...

Below the table, detailed information for the first process (smss.exe) is shown:

Put:	c:\windows\system32\smss.exe
Veličina:	152.3 kB
Opis:	Windows Session Manager
Tvrtka:	Microsoft Corporation
Verzija:	10.0.19041.1 (WinBuild.160101.0800)
Program:	Microsoft® Windows® Operating System
Stvoreno dana:	10/23/2020 5:42:13 PM
Izmjenjeno dana:	10/23/2020 5:42:13 PM

[Sakrij detalje](#)

**Reputacija** – u većini slučajeva ESET Endpoint Antivirus i tehnologija ESET LiveGrid® dodjeljuju razine rizika objektima (datotekama, procesima, ključevima registra itd.) s pomoću niza heurističkih pravila koja provjeravaju značajke svakog objekta i zatim procjenjuju moguću zlonamjernu aktivnost. Prema tim heurističkim pravilima objektima se dodjeljuje razina reputacije od 9 – najbolja reputacija (zeleno) do 0 – najgora reputacija (crveno).

**Proces** – Naziv slike programa ili procesa koji je trenutačno pokrenut na vašem računalu. Također možete upotrijebiti Windows Upravitelj zadataka za pregled svih procesa koji se izvršavaju na računalu. Upravitelj zadataka možete otvoriti tako da desnom tipkom miša kliknete prazno područje na programskoj traci i nakon toga kliknete Upravitelj zadataka, ili možete pritisnuti **Ctrl+Shift+Esc** na tipkovnici.

**PID** – To je ID procesa koji su pokrenuti u operacijskim sustavima Windows.

**i** Poznate aplikacije označene zeleno definitivno su čiste (nalaze se na popisu pouzdanih adresa) i neće biti skenirane, čime se povećava brzina skeniranja računala na zahtjev ili rezidentne zaštite sistemskih datoteka na računalu.

**Broj korisnika** – Broj korisnika koji koriste danu aplikaciju. Te podatke prikuplja tehnologija ESET LiveGrid®.

**Vrijeme otkrivanja** – Vremensko razdoblje koje je proteklo otkada je tehnologija ESET LiveGrid® otkrila aplikaciju.

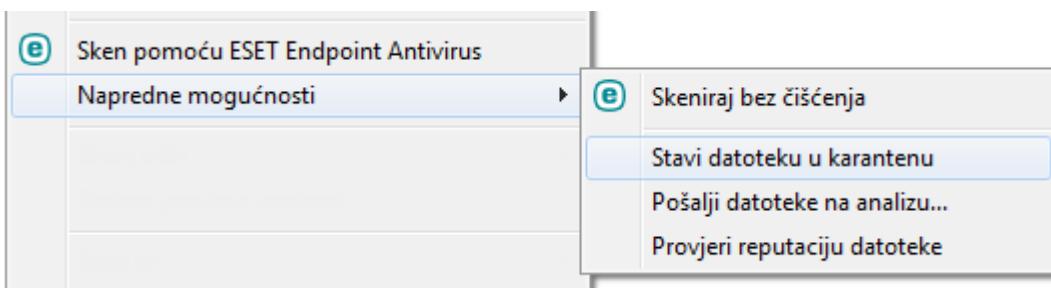
Kada je aplikacija označena kao aplikacija sigurnosne razine Nepoznato (narančasto), možda nije riječ o zlonamjernom softveru. Obično je samo riječ o novijoj aplikaciji. Ako za neku datoteku niste sigurni, možete **i poslati datoteku na analizu** u laboratorij tvrtke ESET za otkrivanje virusa. Ako se ispostavi da je datoteka zlonamjerna aplikacija, njezino otkrivanje dodat će se jednoj od sljedećih aktualizacija modula za otkrivanje virusa.

**Naziv aplikacije** – Zadani naziv programa ili procesa.

Klikom na određenu aplikaciju na dnu, prikazat će se sljedeće informacije pri dnu prozora:

- **Put** – Lokacija aplikacije na vašem računalu.
- **Veličina** – Veličina datoteke u kB (kilobajtima) ili MB (megabajtima).
- **Opis** – Značajke datoteke temeljem opisa iz operacijskog sustava.
- **Tvrtka** – Naziv proizvođača ili procesa aplikacije.
- **Verzija** – informacije od izdavača aplikacije.
- **Program** – Naziv aplikacije i/ili poslovni naziv.
- **Stvoreno dana** – Datum i vrijeme kada je aplikacija stvorena.
- **Promijenjeno** – datum i vrijeme kada je aplikacija promijenjena.

**i** Reputacija se može provjeriti i za datoteke koje ne djeluju kao programi/procesi koji se izvršavaju – označite datoteke koje želite provjeriti, kliknite ih desnom tipkom miša i iz [kontekstnog izbornika](#) odaberite **Napredne mogućnosti > Provjeri reputaciju datoteka pomoću sustava ESET LiveGrid®**.



## Sigurnosno izvješće

Ova funkcija pruža pregled statistika za sljedeće kategorije:

**Blokirane web stranice** – Prikazuje broj blokiranih web stranica (URL-ovi koji su na popisu potencijalno neželjenih aplikacija, phishing, hakirani router, IP ili certifikat).

**Otkriveni objekti zaražene e-pošte** – Prikazuje broj zaraženih [objekata](#) e-pošte koji su otkriveni.

**Otkrivene potencijalno nepoželjne aplikacije** – prikazuje broj [potencijalno nepoželjnih aplikacija](#) (PUA).

**Pregledani dokumenti** – Prikazuje broj skeniranih objekata dokumenata.

**Skenirane aplikacije** – Prikazuje broj skeniranih izvršnih objekata.

**Skenirani ostali objekti** – Prikazuje broj ostalih skeniranih objekata.

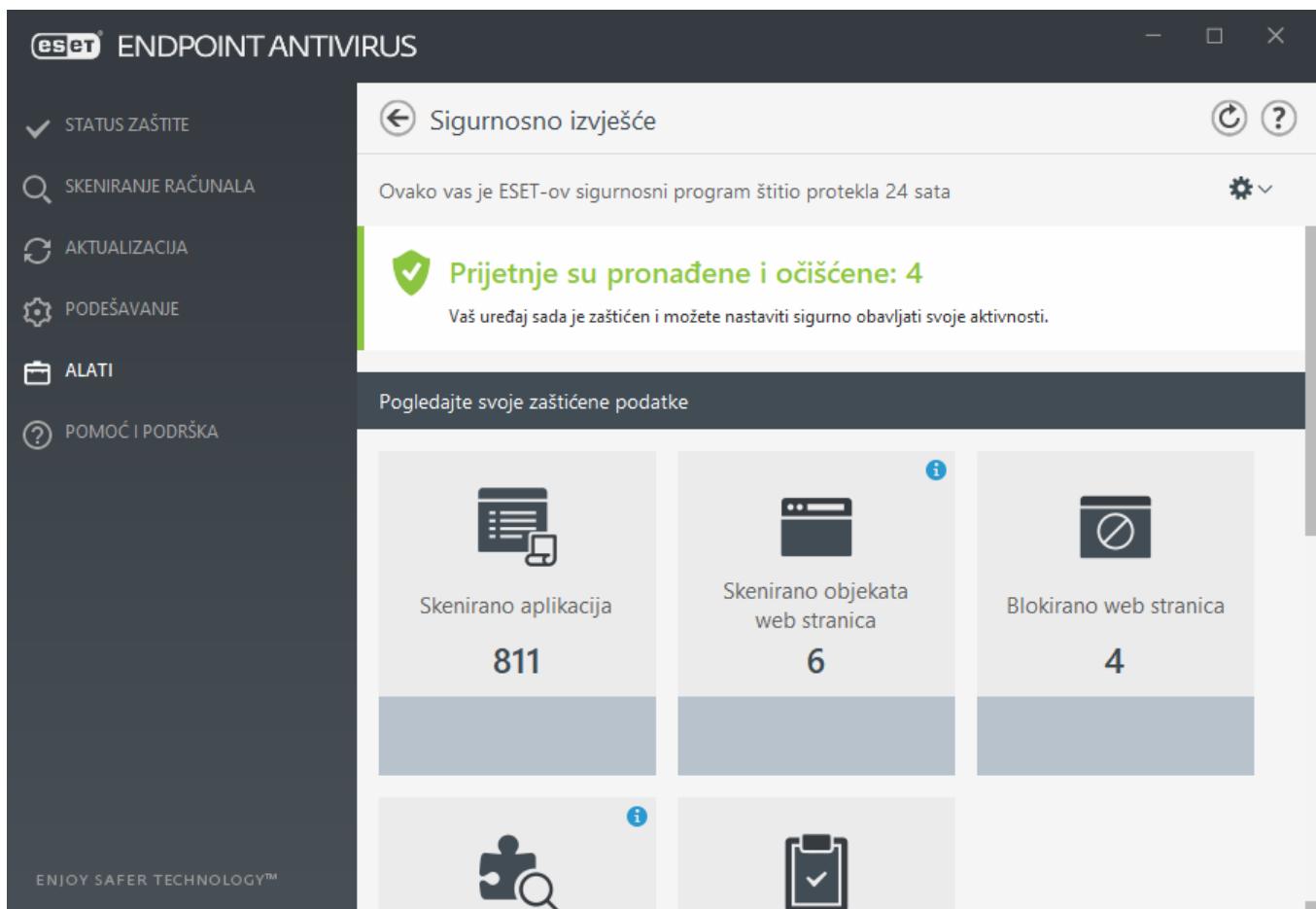
**Pregledani objekti web stranica** – Prikazuje broj skeniranih objekata web stranica.

**Skenirani objekti e-pošte** – prikazuje broj skeniranih objekata e-pošte.

Redoslijed ovih kategorija temelji se na numeričkoj vrijednosti od najviše prema najnižoj. Kategorije s nultom vrijednošću nisu prikazane. Kliknite **Prikaži više** za proširivanje i prikaz skrivenih kategorija.

Ispod kategorija možete vidjeti trenutnu situaciju s virusima na karti svijeta. Prisutnost virusa u svakoj zemlji označena je bojom (što je boja tamnija, to je veći broj virusa). Zemlje za koje nema podataka zasivljene su. Ako prijeđete mišem iznad zemlje, prikazat će se podaci za tu zemlju. Možete odabrati određeni kontinent i on će se automatski zumirati.

Ako kliknete zupčanik  u gornjem desnom kutu, možete **aktivirati/deaktivirati obavijesti sigurnosnog izvješća** ili odabrati hoće li se prikazivati podaci za zadnjih 30 dana ili za razdoblje otkada je program aktiviran. Ako je ESET Endpoint Antivirus instaliran manje od 30 dana, moguće je odabrati samo broj dana nakon instalacije. Razdoblje od 30 dana postavljeno je kao standardno.



**Poništi podatke** izbrisat će sve statistike i ukloniti postojeće podatke iz sigurnosnog izvješća. Ovu je radnju potrebno potvrditi, osim u slučaju kada ste odznačili opciju **Pitaj prije poništavanja statistike** u **Napredno podešavanje > Korisničko sučelje > Upozorenja i okviri s porukama > Poruke za potvrdu**.

# ESET SysRescue Live

ESET SysRescue Live besplatni je uslužni alat koji omogućuje stvaranje CD-a/DVD-a ili USB pogona za pokretanje i oporavak. Možete pokrenuti zaraženo računalo s odabranog medija za oporavak kako biste skenirali zlonamjerne programe i očistili zaražene datoteke.

Glavna je prednost programa ESET SysRescue Live to što se pokreće neovisno o glavnom operacijskom sustavu, ali ima izravan pristup disku i datotečnom sustavu. Zahvaljujući tome, moguće je ukloniti prijetnje koje se u normalnim radnim uvjetima ne bi mogle izbrisati (na primjer, kada je pokrenut operacijski sustav itd.).

- [Online pomoć za ESET SysRescue Live](#)

## Slanje uzorka na analizu

Ako na računalu pronađete sumnjivu datoteku ili na internetu pronađete sumnjivu web stranicu, možete ih poslati na analizu u Laboratorij za istraživanje tvrtke ESET (možda neće biti dostupno ovisno o konfiguraciji za ESET LiveGrid®).

Nemojte slati uzorak ako ne ispunjava barem jedan od sljedećih kriterija:

- Uzorak uopće nije otkriven ESET-ovim programom.
- Uzorak je neispravno otkriven kao prijetnja.
- Ne prihvaćamo osobne datoteke (za koje biste htjeli da ih ESET skenira u potrazi za zlonamjernim programima) kao uzorke (Laboratorij za istraživanje tvrtke ESET ne provodi skeniranja na zahtjev korisnika).
- Upotrijebite opisni redak naslova i priložite što je moguće više informacija o datoteci (npr. snimka zaslona ili web stranica s koje ste je preuzeli).

Slanje uzorka omogućuje vam da pošaljete datoteku ili web stranicu ESET-u radi analize jednom od sljedećih metoda:

1. Upotrijebite prozor za slanje uzorka koji se nalazi u izborniku **Alati > Slanje uzorka na analizu**.
2. Datoteku možete poslati i e-poštom. Ako želite upotrijebiti tu mogućnost, datoteku zapakirajte s pomoću programa WinRAR/ZIP, arhivsku datoteku zaštitite lozinkom "infected" i pošaljite je na adresu [samples@eset.com](mailto:samples@eset.com).
3. Prijavljanje spam sadržaja ili neispravno identificiranog spam sadržaja, pročitajte [članak ESET-ove baze znanja](#).

Dok je otvorena stavka **Odabir uzorka za analizu**, u padajućem izborniku **Razlog za slanje uzorka** odaberite opis koji najbolje odgovara vašoj poruci:

- [Sumnjiva datoteka](#)
- [Sumnjiva stranica](#) (web stranica koja je zaražena bilo kojim zlonamjernim softverom),
- [Neispravno identificirana datoteka](#) (datoteka koja je otkrivena kao zaražena, ali zapravo nije),
- [Neispravno identificirana web stranica](#)
- [Ostalo](#)

**Datoteka/Stranica** – Put do datoteke ili web stranice koju želite poslati.

**Adresa e-pošte za kontakt** – adresa e-pošte za kontakt šalje se u ESET zajedno sa sumnjivim datotekama, a može se upotrijebiti za komunikaciju u slučaju potrebe za dodatnim informacijama za analizu. Unos adrese e-pošte za kontakt nije obavezan. Odaberite **Pošalji anonimno** da bi polje ostalo prazno.

**i** Ako ne budu potrebne dodatne informacije, ESET vam neće poslati odgovor. Naši serveri svakodnevno primaju desetke tisuća datoteka, pa ne možemo odgovoriti na sve poruke.

Ako se pokaže da je uzorak ustvari zlonamjerna aplikacija ili web stranica, njegovo će se otkrivanje dodati u jednu od sljedećih ESET-ovih nadogradnji.

## Odabir uzorka za analizu – Sumnjiva datoteka

**Primjećeni znakovi i simptomi zaraze zlonamjernim softverom** – Unesite opis ponašanja sumnjive datoteke na svojem računalu.

**Porijeklo datoteke (URL adresa ili dobavljač)** – Unesite porijeklo (izvor) datoteke i kako ste došli do nje.

**Napomene i dodatne informacije** – Ovdje možete unijeti dodatne informacije ili opis koji će nam pomoći pri identifikaciji sumnjive datoteke.

**i** Prvi je parametar – **Primjećeni znakovi i simptomi zaraze zlonamjernim softverom** – obavezan, no navođenje dodatnih informacija našim će laboratorijima uvelike pomoći pri identifikaciji uzorka.

## Odabir uzorka za analizu – Sumnjiva web stranica

Odaberite jednu od sljedećih mogućnosti s padajućeg izbornika **Što nije u redu s web stranicom**:

- **Zaraženo** – Web stranica koja sadrži viruse ili drugi zlonamjerni softver koji se distribuiru raznim metodama.
- **Phishing** – Phishing se često koristi za ostvarivanje pristupa tajnim podacima kao što su brojevi bankovnih računa, PIN kodovi itd. Više o toj vrsti napada pročitajte u [rječniku](#).
- **Prijevara** – Web stranica čiji je sadržaj lažan ili obmanjujuć, posebno u svrhu ostvarivanja brze zarade.
- Odaberite **Ostalo** ako se iznad spomenute mogućnosti ne odnose na web stranicu koju želite poslati.

**Napomene i dodatne informacije** – Tu možete unijeti dodatne informacije ili opis koji će nam pomoći pri analizi sumnjive web stranice.

## Odabir uzorka za analizu – Neispravno identificirana datoteka

Od vas tražimo da pošaljete datoteke koje su identificirane kao zaražene, no zapravo to nisu kako bismo poboljšali svoj antivirusni i antispyware modul te pomogli drugima da ostanu zaštićeni. Do neispravne identifikacije (NI) može doći kada uzorak datoteke odgovara uzorku koji se nalazi u modulu detekcije.

**Naziv i verzija aplikacije** – Naslov i verzija programa (npr. broj, drugo ime ili kodno ime).

**Porijeklo datoteke (URL adresa ili dobavljač)** – Unesite porijeklo (izvor) datoteke i zabilježite kako ste došli do nje.

**Svrha aplikacija** – Općeniti opis aplikacije, vrsta aplikacije (npr. preglednik, multimedijijski reproduktor...) i njena funkcionalnost.

**Napomene i dodatne informacije** – Ovdje možete unijeti dodatne informacije ili opis koji će nam pomoći pri obradi sumnjive datoteke.

**i** prva tri parametra obavezna su za identifikaciju legitimnih aplikacija i njihovo razlikovanje od zlonamjernog koda. Navođenjem dodatnih informacija našim ćete laboratorijima uvelike pomoći pri identifikaciji i obradi uzorka.

## Odabir uzorka za analizu – Neispravno identificirana web stranica

Od vas tražimo da pošaljete web stranice koje su identificirane kao zaražene ili kao stranice za prijevaru ili phishing, no zapravo to nisu. Neispravno identificirane stranice (FP-ovi) mogu se pojaviti kad uzorak datoteke odgovara istom uzorku sadržanom u modulu za otkrivanje virusa. Pošaljite nam takve web stranice da bismo poboljšali svoj antivirusni i antiphishing modul te pomogli drugima da ostanu zaštićeni.

**Napomene i dodatne informacije** – ovdje možete unijeti dodatne informacije ili opise koji će nam pomoći pri obradi sumnjive web stranice.

## Odabir uzorka za analizu – Ostalo

Taj obrazac koristite ako se datoteka ne može definirati kao **Sumnjiva datoteka** ni kao **Neispravna identifikacija**.

**Razlog slanja datoteke** – Unesite detaljan opis i razlog slanja datoteke.

## Obavijesti

Da biste upravljali načinom na koji program ESET Endpoint Antivirus obavještava korisnika o događajima, idite na **Napredno podešavanje (F5) > Alati > Obavijesti**. U ovom konfiguracijskom prozoru možete postaviti sljedeće vrste obavijesti:

- **Obavijesti aplikacije** – prikazuju se izravno u glavnom prozoru programa.
- **Obavijesti na radnoj površini** – obavijest na radnoj površini prikazuje se kao mali skočni prozor pokraj programske trake sustava.
- **Obavijesti e-poštom** – obavijesti e-poštom šalju se na određenu adresu e-pošte.
- **Prilagodba obavijesti** – možete dodati prilagođenu poruku, npr. za obavijest na radnoj površini.

U odjeljku **Osnovno** upotrijebite odgovarajući prekidač da biste podesili sljedeće stavke:

Prekidač	Standardno	Opis
Prikaži obavijesti na radnoj površini	<input checked="" type="checkbox"/>	Deaktivirajte da biste sakrili skočne obavijesti pokraj programske trake sustava. Preporučujemo da ne deaktivirate ovu opciju da biste mogli primati obavijesti programa o novim događajima.
Ne prikazuj obavijesti prilikom...	<input checked="" type="checkbox"/>	Aktivirajte opciju <b>Ne prikazuj obavijesti prilikom pokretanja aplikacija preko cijelog zaslona</b> da biste sakrili sve neaktivne obavijesti.
Prikaži obavijesti sigurnosnih izvješća	<input type="checkbox"/>	Aktivirajte da biste primili obavijest kada se stvori nova verzija <a href="#">sigurnosnog izvješća</a> (dostupno samo ako se njome ne upravlja uz pomoć programa ESET Security Management Center).
Prikaži obavijest o uspješnoj nadogradnji	<input type="checkbox"/>	Aktivirajte da biste primili obavijest kada se nadograde komponente i moduli detekcije programa.
Pošalji obavijest o događaju e-poštom	<input type="checkbox"/>	Aktivirajte da biste primali <a href="#">obavijesti e-poštom</a> .

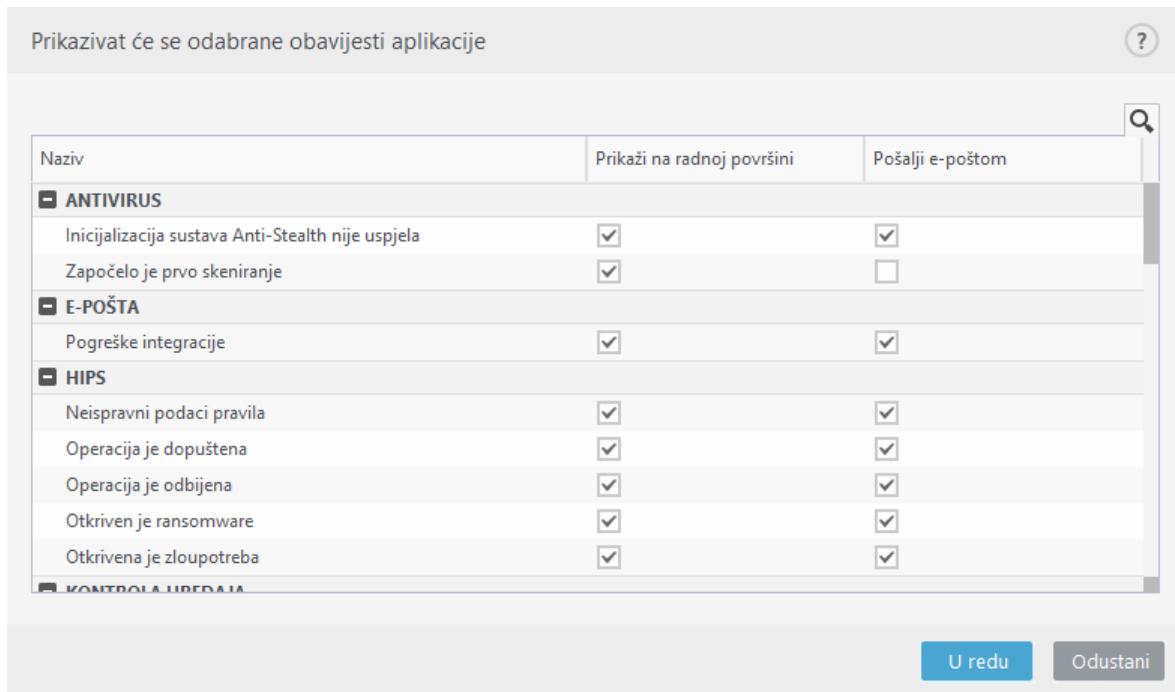
Da biste aktivirali ili deaktivirali određene [obavijesti aplikacije](#), kliknite gumb **Uredi** pokraj stavke **Obavijesti aplikacije**.

## Obavijesti aplikacije

Da biste podešili vidljivost obavijesti aplikacije (koje se prikazuju u donjem desnom kutu zaslona), idite na izbornik **Alati > Obavijesti > Osnovno > Obavijesti aplikacije** u stablu Napredno podešavanje programa ESET Endpoint Antivirus.

Popis obavijesti podijeljen je u tri stupca. Nazivi obavijesti sortirani su prema kategorijama u prvom stupcu. Da

biste promijenili način na koji vas program obavještava o novim događajima aplikacija, odaberite potvrđne okvire **Prikaži na radnoj površini** i **Pošalji e-poštom**.



Naziv	Prikaži na radnoj površini	Pošalji e-poštom
<b>ANTIVIRUS</b>		
Inicijalizacija sustava Anti-Stealth nije uspjela	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Započelo je prvo skeniranje	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>E-POŠTA</b>		
Pogreške integracije	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>HIPS</b>		
Neispravni podaci pravila	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operacija je dopuštena	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Operacija je odbijena	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Otkriven je ransomware	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Otkrivena je zloupotreba	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Da biste postavili opće postavke za obavijesti na radnoj površini, primjerice, koliko će se dugo prikazivati poruka ili minimalni opseg događaja za prikaz, pogledajte stavku [Obavijesti na radnoj površini](#) u izborniku **Napredno podešavanje > Alati > Obavijesti**.

Da biste postavili format poruka e-pošte i konfigurirali postavke SMTP servera, pogledajte stavku [Obavijesti e-poštom](#) u izborniku **Napredno podešavanje > Alati > Obavijesti**.

**Ako želite postaviti obavijesti Datoteka analizirana i Datoteka nije analizirana tijekom upotrebe programa ESET Dynamic Threat Defense, [Proaktivna zaštita](#) mora biti postavljena na Blokiranje pokretanja do primanja rezultata analize.**

## Obavijesti na radnoj površini

Obavijest na radnoj površini prikazuje se kao mali skočni prozor pokraj programske trake sustava. Prema standardnim postavkama prikazuje se na 10 sekundi, a zatim postupno nestaje. To je glavni način na koji program ESET Endpoint Antivirus obavještava korisnika o uspješnim nadogradnjama programa, novim povezanim uređajima, dovršetku skeniranja virusa ili novim pronađenim prijetnjama.

Odjeljak **Obavijesti na radnoj površini** omogućava prilagodbu ponašanja skočnih obavijesti. Mogu se postaviti sljedeći atributi:

**Trajanje** – postavlja se trajanje vidljivosti poruke obavijesti. Vrijednost mora biti u rasponu od 3 do 30 sekundi.

**Prozirnost** – postavlja se postotak prozirnosti poruke obavijesti. Podržani je raspon od 0 (nema prozirnosti) do 80 (vrlo visoka prozirnost).

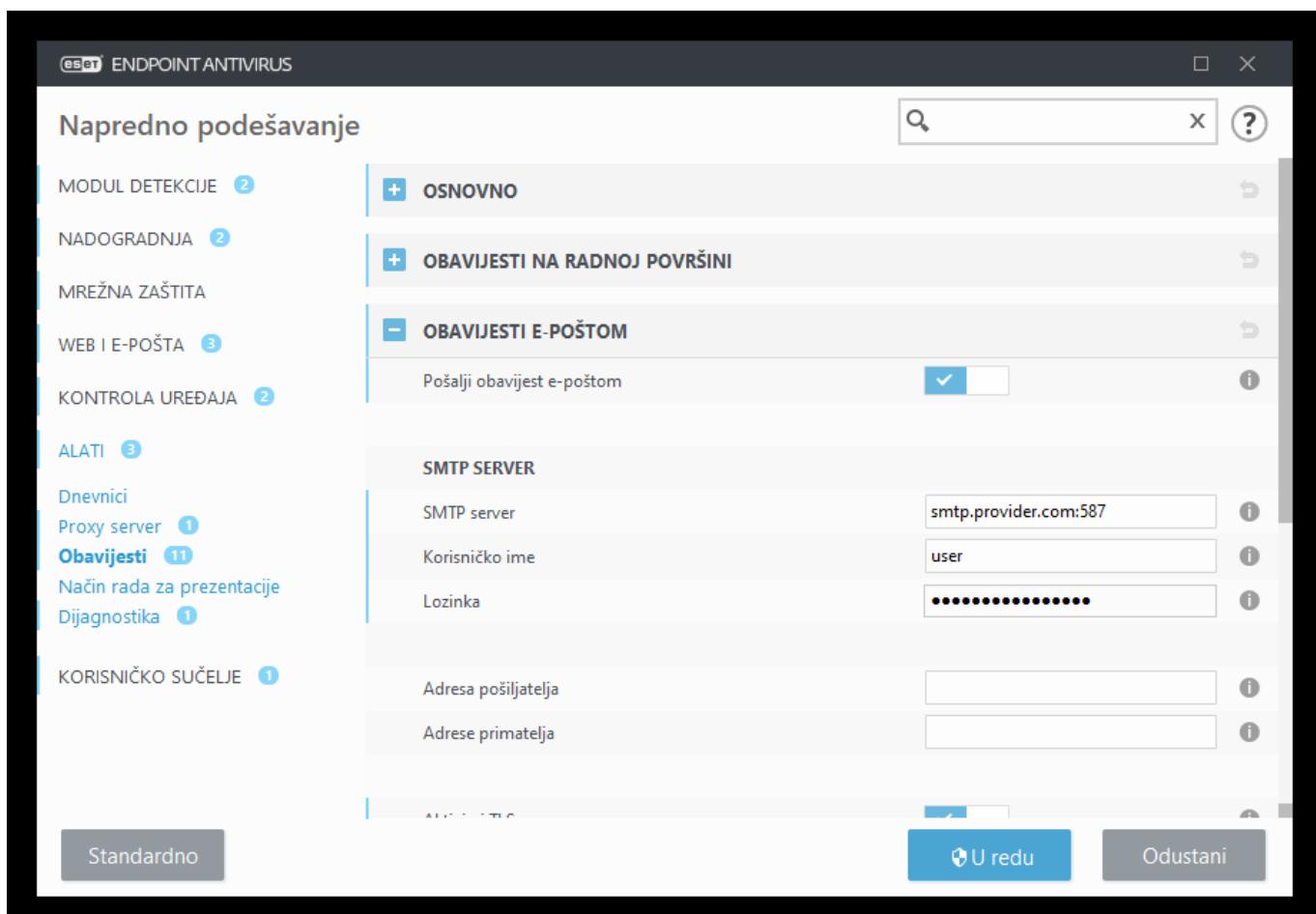
**Minimalni opseg zapisa događaja za prikaz** – u padajućem izborniku možete odabrati početnu razinu ozbiljnosti obavijesti koje će se prikazivati:

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguiranje programa te svi prethodno navedeni zapisi.
- **Informacije** – Zapisuju se sve informativne poruke kao što su nestandardni mrežni događaji, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke upozorenja (antistealth tehnologija ne radi ispravno ili aktualizacija nije uspjela).
- **Pogreške** – Zapisuju se pogreške (zaštita dokumenata nije pokrenuta) i kritične pogreške.
- **Kritično** – Zapisuju se samo kritične pogreške pri pokretanju antivirusne zaštite ili ako je sustav zaražen.

**U sustavu s više korisnika prikazuj obavijesti na zaslonu ovog korisnika** – unesite pune nazine računa korisnika kojima je dopušteno primati obavijesti na radnoj površini. Primjerice, ako upotrebljavate računalo i za račune koji nisu administratorski, a želite primati obavijesti o novim događajima programa.

## Obavijesti e-poštom

ESET Endpoint Antivirus podržava slanje obavijesti e-poštom ako se pojavi događaj s odabranom razinom opširnosti podataka. U odjeljku **Osnovno** omogućite stavku **Pošalji obavijesti o događaju e-poštom** da biste aktivirali obavijesti e-poštom.



## SMTP server

**SMTP server** – SMTP server koji se upotrebljava za slanje obavijesti (npr. *smtp.provider.com:587*, prethodno definirani port je 25).



Program ESET Endpoint Antivirus podržava SMTP servere s TLS šifriranjem.

**Korisničko ime i lozinka** – Ako SMTP zahtjeva autorizaciju, ova se polja trebaju popuniti ispravnim korisničkim imenom i lozinkom kako bi se moglo pristupiti SMTP serveru.

**Adresa pošiljatelja** – U tom se polju navodi adresa pošiljatelja koja se prikazuje u zaglavlju poruka e-pošte s obavijestima.

**Adresa primatelja** – U ovom polju navode se adrese primatelja koje će biti prikazana u zaglavlju obavijesti e-poštom. Upotrijebite točku sa zarezom „;” da biste odvojili više adresa e-pošte.

**Aktiviraj TLS** – Aktivira slanje upozorenja i poruka obavijesti koje podržavaju TLS šifriranje.

## Postavke e-pošte

Na padajućem izborniku **Minimalna opširnost za obavijesti** možete odabrati početnu razinu ozbiljnosti za obavijesti.

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa te svi prethodno navedeni zapisi.
- **Informacije** – Zapisuju se sve informativne poruke kao što su nestandardni mrežni događaji, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke upozorenja (antistealth tehnologija ne radi ispravno ili aktualizacija nije uspjela).
- **Pogreške** – Zapisuju se pogreške (zaštita dokumenata nije pokrenuta) i kritične pogreške.
- **Kritično** – Zapisuju se samo kritične pogreške pri pokretanju antivirusne zaštite ili ako je sustav zaražen.

**Pošalji svaku obavijest u zasebnoj poruci e-pošte** – Kada je ova opcija aktivirana, primatelj prima novu poruku e-pošte za svaku obavijest. To može dovesti do primitka velikog broja poruka e-pošte u kratkom vremenskom razdoblju.

**Interval nakon kojeg će biti poslana obavijest e-poštom (min)** – Interval u minutama nakon kojeg će nove obavijesti biti poslane e-poštom. Ako ovu vrijednost postavite na 0, obavijesti će biti odmah poslane.

## Oblik poruke

Komunikacija između programa i udaljenog korisnika ili administratora sustava odvija se putem e-pošte ili poruka u LAN-u (putem servisa za razmjenu poruka sustava Windows). Standardni oblik za poruke upozorenja i obavijesti optimalan je za većinu situacija. U nekim četvrtinama možda morati promijeniti oblik poruka o događajima.

**Oblik poruka o događaju** – Format poruka o događaju koje su prikazane na udaljenim računalima.

**Oblik poruka s upozorenjem o prijetnji** – Upozorenja o prijetnji i poruke s obavijestima imaju unaprijed

definirani standardni oblik. Preporučujemo da ne mijenjate taj oblik. No u određenim čete slučajevima (ako, primjerice, radite s automatiziranim sustavom za obradu e-pošte) možda morati promijeniti oblik poruka.

**Charset** – Pretvara poruku e-pošte u ANSI kodiranje znakova na temelju regionalnih postavki sustava Windows (npr. windows-1250, Unicode (UTF-8), ACSII 7-bit ili japanski (ISO-2022-JP)). Zbog toga će "á" biti promijenjeno u "a", a nepoznati simbol u "?".

**Koristi Quoted-printable kodiranje znakova** – Izvor poruke e-pošte bit će kodiran u oblik Quoted-printable (QP) koji koristi ASCII znakove i može ispravno e-poštom prenijeti posebne znakove u 8-bitnom obliku (čččžđ).

Ključne riječi (nizovi odvojeni znakovima %) u poruci zamjenjuju se stvarnim podacima koji se odnose na to upozorenje. Dostupne su sljedeće ključne riječi:

- **%TimeStamp%** – datum i vrijeme događaja
- **%Scanner%** – modul o kojem je riječ
- **%ComputerName%** – naziv računala na kojem se pojavilo upozorenje
- **%ProgramName%** – program koji je generirao upozorenje
- **%InfectedObject%** – naziv zaražene datoteke, poruke itd.
- **%VirusName%** – identifikacija zaraze
- **%Action%** – radnja koja se poduzima nakon infiltracije
- **%ErrorDescription%** – opis događaja koji nije izazvan virusom

Ključne riječi **%InfectedObject%** i **%VirusName%** koriste se samo u porukama s upozorenjima o prijetnjama, a **%ErrorDescription%** se koristi samo u porukama o događajima.

## Prilagodba obavijesti

U ovom prozoru možete prilagoditi poruke iz obavijesti.

**Tekst standardne obavijesti** – Standardna poruka koja se prikazuje u podnožju obavijesti.

## Prijetnje

Ako želite da obavijesti o zlonamjernom softveru ostanu na zaslonu sve dok ih ručno ne zatvorite, aktivirajte mogućnost **Nemoj automatski zatvarati obavijesti o zlonamjernom softveru**.

Za korištenje prilagođenih poruka obavijesti deaktivirajte **Koristi standardnu poruku** i unesite vlastitu poruku u polje **Poruka obavijesti za prijetnju**.

## Karantena

Glavna funkcija karantene je sigurna pohrana prijavljenih objekata (kao što su zlonamjerni programi, zaražene datoteke ili potencijalno nepoželjne aplikacije).

Karanteni se može pristupiti iz glavnog prozora programa ESET Endpoint Antivirus klikom na **Alati > Karantena**.

Datoteke pohranjene u mapi karantene mogu se pregledati u tablici koja prikazuje:

- datum i vrijeme karantene,
- put do izvorne lokacije datoteke,
- njezinu veličinu u bajtovima,
- razlog (na primjer, objekt koji je dodao korisnik),
- broj prijetnji (na primjer, duplikati prijetnji iste datoteke ili arhiva koja sadrži višestruke infiltracije).

- [Na daljinu upravljam karantenom na klijentskim radnim stanicama](#)

Vrijeme	Naziv objekta	Velič...	Razlog	Broj	Korisnički račun
12/8/2020 2:...	http://amtso.eicar.org/Potenti...	32.5 kB	Win32/PUAtest.B ... 2	2	ESET\michal.novomesky
12/8/2020 2:...	https://amtso.eicar.org/eicar.c...	70 B	Eicar file pengujian 6	6	ESET\michal.novomesky

## Stavljanje datoteke u karantenu

ESET Endpoint Antivirus automatski stavlja obrisane datoteke u karantenu (ako niste onemogućili ovu opciju u [prozoru s upozorenjima](#)).

Dodatne datoteke treba staviti u karantenu:

- ako se ne mogu izbrisati,
- ako ih nije sigurno ili preporučljivo obrisati,
- ako ih ESET Endpoint Antivirus pogrešno otkrije,

d.ili ako se datoteka ponaša sumnjivo, ali je [skener](#) ne otkrije.

Imate više opcija za stavljanje datoteke u karantenu:

a.upotrijebite funkciju povlačenja i ispuštanja za ručno stavljanje datoteke u karantenu tako da kliknete datoteku, pomaknete pokazivač miša na označeno područje uz pritisnutu tipku miša, a zatim je ispustite. Nakon toga se aplikacija prebacuje u prvi plan.

b.Kliknite **Prebaci u karantenu** iz glavnog prozora programa.

c.U tu svrhu se također može upotrebljavati kontekstni izbornik; desnom tipkom miša kliknite prozor **Karantena** i odaberite **Karantena**.

## Vraćanje iz karantene

Datoteke u karanteni također se mogu vratiti na izvornu lokaciju:

- U tu svrhu upotrijebite funkciju **Vrati**, koja je dostupna iz kontekstnog izbornika tako da desnom tipkom miša kliknete određenu datoteku u karanteni.
- Ako je datoteka označena kao [potencijalno neželjena aplikacija](#), aktivirana je opcija **Vrati i izuzmi od skeniranja**. Također pogledajte odjeljak [Izuzeci](#).
- Kontekstni izbornik također pruža opciju **Vrati na**, koja vam omogućuje vraćanje datoteke na lokaciju koja nije ista kao lokacija s koje je datoteka obrisana.
- Funkcija vraćanja nije dostupna u nekim slučajevima, na primjer, za datoteke koje se nalaze na zajedničkoj mreži samo za čitanje.

## Brisanje iz karantene

Kliknite desnom tipkom miša na odabranu stavku i odaberite **Izbriši iz karantene** ili odaberite stavku koju želite izbrisati i pritisnite **Izbriši** na tipkovnici. Možete odabrati i više stavki odjednom i sve ih izbrisati. Izbrisane stavke trajno će se ukloniti s uređaja i iz karantene.

## Slanje datoteke iz karantene

Ako ste u karantenu stavili sumnjivu datoteku koju program nije otkrio ili ako je datoteka neispravno procijenjena kao zaražena (npr. heurističkom analizom koda) i stavljen u karantenu, [pošaljite uzorak na analizu u Laboratorij](#) [za istraživanje tvrtke ESET](#). Da biste poslali datoteku, kliknite je desnom tipkom miša i u kontekstnom izborniku odaberite **Pošalji na analizu**.

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

- [Upravljanje karantenom u programu ESET PROTECT \(8.x\)](#)
- [ESET-ov program obavijestio me o prijetnji – što trebam učiniti?](#)

## Podešavanje proxy servera

U velikim lokalnim mrežama (LAN-ovima) veza računala s internetom može se ostvariti posredstvom proxy servera. Da bi se koristila ta konfiguracija, moraju biti definirane sljedeće postavke. U suprotnom se program neće

moći automatski aktualizirati. U programu ESET Endpoint Antivirus proxy server može se postaviti u dva različita odjeljka stabla naprednog podešavanja.

Postavke proxy servera mogu se prvo konfigurirati u **Naprednom podešavanju** pod **Alati > Proxy server**.

Određivanjem proxy servera na toj razini definiraju se globalne postavke proxy servera za cijeli program ESET Endpoint Antivirus. Parametre koji se tu nalaze koristit će svi moduli kojima je potrebna internetska veza.

Da biste odredili postavke proxy servera za tu razinu, odaberite potvrđni okvir **Koristi proxy server** i zatim unesite adresu proxy servera u polje **Proxy server**, zajedno s brojem **porta** proxy servera.

Ako je za komunikaciju s proxy serverom potrebna prijava, odaberite potvrđni okvir **Proxy server zahtjeva prijavu** i u odgovarajuća polja unesite valjano **korisničko ime** i **lozinku**. Kliknite **Otkrij proxy server** da biste automatski prepoznali i ispunili postavke proxy servera. Kopirat će se parametri navedeni u internetskim opcijama preglednika Internet Explorer ili Google Chrome.

**i** Korisničko ime i lozinku morate ručno unijeti u postavke **proxy servera**.

**Upotrijebi izravnu vezu ako nije dostupan proxy** – ako je ESET Endpoint Antivirus konfiguriran za povezivanje putem proxyja, a proxy nije dostupan, program ESET Endpoint Antivirus zaobići će ga i komunicirati izravno s ESET-ovim serverima.

Postavke proxy servera moguće je uspostaviti i putem naprednog podešavanja nadogradnje (**Napredno podešavanje > Nadogradnja > Profili > Nadogradnje > Opcije povezivanja** odabirom opcije **Veza putem proxy servera** s padajućeg izbornika **Proxy način rada**). Ta postavka primjenjuje se na dani profil nadogradnje i preporučuje se za prijenosna računala koja često s udaljenih lokacija primaju nadogradnje modula za otkrivanje. Dodatne informacije o toj postavci potražite u odjeljku [Napredno podešavanje nadogradnje](#).

The screenshot shows the 'Napredno podešavanje' (Advanced Settings) window. On the left, a sidebar lists various modules: MODUL DETEKCIJE (1), NADOGRADNJA (4), MREŽNA ZAŠTITA, WEB I E-POŠTA (3), KONTROLA UREĐAJA (1), ALATI (3), and KORISNIČKO SUČELJE (1). The 'ALATI' section is expanded, showing 'Dnevnički', 'Proxy server' (selected, with 1 notification), 'Obavijesti e-poštom' (3), 'Način rada za prezentacije', and 'Dijagnostika'. The main panel is titled 'PROXY SERVER' and contains the following fields:

- 'Koristi proxy server': checked (indicated by a blue checkmark icon).
- 'Proxy server': empty input field.
- 'Port': input field containing '3128'.
- 'Proxy server zahtjeva prijavu': unchecked (indicated by a grey 'X' icon).
- 'Korisničko ime': empty input field.
- 'Lozinka': empty input field.
- 'Otkrij proxy server': button with a blue outline.
- 'Upotrijebi izravnu vezu ako nije dostupan proxy': checked (indicated by a blue checkmark icon).

At the bottom, there are three buttons: 'Standardno' (grey), 'U redu' (blue with a gear icon), and 'Odustani' (grey).

# Vremensko razdoblje

Vremenska razdoblja mogu se stvarati i zatim dodjeljivati pravilima za **kontrolu uređaja**. Postavka **vremenskih razdoblja** nalazi se pod "**Napredno podešavanje**" > "**Alati**". Ova opcija omogućuje vam definiranje najčešćih vremenskih razdoblja (npr. radno vrijeme, vikend itd.) i njihovu jednostavnu ponovnu upotrebu bez ponovnog definiranja vremenskih raspona za svako pravilo. Vremensko razdoblje primjenjivo je za svaku relevantnu vrstu pravila koje podržava kontrolu utemeljenu na vremenu.

Naziv	Opis
Work time	Weekdays 8:00-17:00
Off-work	Evenings & weekends

Dodaj    Uredi    Izbriši

U redu    Odustani

Za stvaranje vremenskog razdoblja učinite sljedeće:

- 1.Kliknite "**Uredi**" > "**Dodaj**".
- 2.Unesite naziv i **opis** vremenskog razdoblja i kliknite "**Dodaj**".
- 3.Navedite dan i vrijeme početka/završetka za vremensko razdoblje ili odaberite "**Cijeli dan**".
- 4.Kliknite "**U redu**" za potvrdu.

Jedno vremensko razdoblje može se definirati s jednim ili više vremenskih raspona na temelju dana i vremena. Kada se vremensko razdoblje stvori, prikazat će se u padajućem izborniku "**Primjeni tijekom**" u [prozoru uređivača pravila kontrole uređaja](#).

## Nadogradnja sustava Microsoft Windows

Mogućnost nadogradnje sustava Windows važan je element za zaštitu korisnika od zlonamjernog softvera. Iz tog razloga izuzetno je važno nadogradnje sustava Microsoft Windows instalirati čim one postanu dostupne. ESET Endpoint Antivirus vas obavještava o nadogradnjama koje nedostaju u skladu s razinom koju definirate. Dostupne su sljedeće razine:

- **Nema nadogradnji** – Neće se navoditi nadogradnje sustava za preuzimanje.

- **Dodatne nadogradnje** – Za preuzimanje će biti ponuđene nadgradnje koje imaju oznaku niskog i višeg prioriteta.
- **Preporučene nadogradnje** – Za preuzimanje će biti ponuđene nadgradnje koje imaju oznaku uobičajenog i višeg prioriteta.
- **Važne nadogradnje** – Za preuzimanje će biti ponuđene nadgradnje koje imaju oznaku visokog i višeg prioriteta.
- **Kritične nadogradnje** – Samo će kritične nadgradnje biti ponuđene za preuzimanje.

Kliknite **U redu** da biste spremili promjene. Prozor za nadogradnje sustava prikazat će se nakon verifikacije statusa putem servera za nadogradnju. Prema tome, informacije o nadogradnji sustava možda neće biti dostupne odmah po spremanju promjena.

## Interval provjere licence

ESET Endpoint Antivirus se mora automatski povezivati s ESET-ovim serverima. Da biste promijenili tu postavku, idite u odjeljak **Napredno podešavanje (F5) > Alati > Licenca**. Prema standardnim postavkama **interval provjere** postavljen je na **Automatski** i ESET-ov server licenci provjerava program nekoliko puta u satu. U slučaju povećanog mrežnog prometa promijenite postavke na **Ograničeno** da biste smanjili preopterećenje. Kada je odabrana opcija **Ograničeno**, ESET Endpoint Antivirus provjerava server licenci samo jednom dnevno ili prilikom ponovnog pokretanja računala.

Ako je **interval provjere** postavljen na **Ograničeno**, može potrajati do jedan dan prije nego što se sve promjene u vezi s licencom koje se izvrše putem programa ESET Business Account /ESET MSP Administrator primijene na postavke programa ESET Endpoint Antivirus.

## Korisničko sučelje

Odjeljak **Korisničko sučelje** omogućuje vam konfiguriranje ponašanja grafičkog korisničkog sučelja programa (GUI-ja).

Pomoću alata [Elementi korisničkog sučelja](#) možete prilagoditi vizualni izgled programa i efekte koji se koriste.

Da biste omogućili maksimalnu sigurnost softvera za zaštitu, možete spriječiti neovlaštene promjene pomoću alata [Podešavanje pristupa](#).

Konfiguiranjem opcija [Upozorenja i okviri s porukama](#) i [Obavijesti](#) možete promijeniti ponašanje upozorenja o otkrivenim prijetnjama i sistemskih obavijesti. Možete ih prilagoditi vlastitim potrebama.

Ako ne želite prikazati neke obavijesti, one će biti prikazane u području **Elementi korisničkog sučelja > Statusi aplikacija**. Tamo možete provjeriti njihov status ili spriječiti njihovo prikazivanje.

[Integracija kontekstnog izbornika](#) prikazuje se kada desnom tipkom miša kliknete odabrani objekt. Taj alat koristite da biste upravljačke elemente programa ESET Endpoint Antivirus integrirali u kontekstni izbornik.

[Način rada za prezentacije](#) koristan je za korisnike koji žele raditi s aplikacijom, a da ih pritom ne prekidaju skočni prozori, planirani zadaci i bilo koje komponente koje bi mogle opteretiti procesor i RAM.

Također pogledajte [Kako minimizirati korisničko sučelje programa ESET Endpoint Antivirus](#) (korisno za upravljanja okruženja).

## Elementi korisničkog sučelja

Mogućnosti konfiguriranja korisničkog sučelja u programu ESET Endpoint Antivirus omogućuju vam da radno okruženje prilagodite svojim potrebama. Te mogućnosti konfiguriranja dostupne su u ogranku **Korisničko sučelje** > **Elementi korisničkog sučelja** na stablu Napredno podešavanje programa ESET Endpoint Antivirus.

U odjeljku **Elementi korisničkog sučelja** možete prilagoditi radno okruženje. S pomoću padajućeg izbornika **Način rada za pokretanje** odaberite neki od sljedećih načina rada za pokretanje grafičkog korisničkog sučelja (GUI-ja):

**Sve** – Prikazat će se cijeli GUI.

**Minimalno** – GUI radi, ali korisniku se prikazuju samo obavijesti.

**Ručno** – GUI se ne pokreće automatski pri prijavi. Svaki ga korisnik može ručno pokrenuti.

**Tiho** – neće se prikazivati obavijesti ni upozorenja. GUI može pokrenuti samo administrator. Ovaj način rada koristan je za upravljanja okruženja ili situacije u kojima trebate sačuvati resurse sustava.

**i** Ako napravite restart računala dok je odabran minimalni način rada za pokretanje GUI-ja, obavijesti će se prikazati, ali ne i grafičko sučelje. Za vraćanje na način punog korisničkog sučelja pokrenite GUI iz izbornika Start u **Svi programi** > **ESET** > ESET Endpoint Antivirus kao administrator, ili to možete učiniti putem programa ESET Security Management Center s pomoću [pravila](#).

Ako želite deaktivirati uvodni prozor programa ESET Endpoint Antivirus, poništite odabir **Prikaži uvodni prozor pri pokretanju programa**.

Ako želite da se program ESET Endpoint Antivirus oglasi zvučnim signalom u slučaju važnih događaja tijekom skeniranja, na primjer kada se otkrije prijetnja ili kada se skeniranje završi, odaberite **Koristi zvučni signal**.

**Integriraj u kontekstni izbornik** – Integrirajte kontrolne elemente programa ESET Endpoint Antivirus u kontekstni izbornik.

### Statusi

**Statusi aplikacije** – kliknite gumb **Uredi** da biste upravljali statusima (deaktivirali ih) koji su prikazani u oknu **Status zaštite** u glavnom izborniku.

## Informacije o licenci

**Prikaži informacije o licenci** – Kada je ova opcija deaktivirana, informacije o licenci na zaslonu **Status zaštite** i **Pomoć i podrška** neće biti prikazane.

**Prikaži poruke i obavijesti u vezi s licencem** – Kada je ova opcija deaktivirana, obavijesti i poruke prikazat će se samo kada licenca istekne.

**i** Postavke podataka o licenci primjenjuju se, ali nisu dostupne za proizvod ESET Endpoint Antivirus aktiviran pomoću MSP licence.

Napredno podešavanje

- MODUL DETEKCIJE 2
- NADOGRADNJA 2
- MREŽNA ZAŠTITA
- WEB I E-POŠTA 3
- KONTROLA UREĐAJA 2
- ALATI 3
- KORISNIČKO SUČELJE 1**

**ELEMENTI KORISNIČKOG SUČELJA**

Prikaz sučelja prilikom pokretanja	Kompletan
Prikazuje se kompletno grafičko korisničko sučelje.	
Prikaži uvodni prozor pri pokretanju programa	<input checked="" type="checkbox"/>
Koristi zvučni signal	<input checked="" type="checkbox"/>
Integriraj u kontekstni izbornik	<input checked="" type="checkbox"/>

**STATUSI**

Status aplikacije	<a href="#">Uredi</a>
-------------------	-----------------------

**PODACI LICENCE**

Prikaži podatke licence	<input checked="" type="checkbox"/>
Prikaži poruke i obavijesti u vezi s licencem	<input checked="" type="checkbox"/>

Standardno U redu Odustani

## Statusi aplikacije

Da biste podešili statuse u sklopu programa, u prvom prozoru programa ESET Endpoint Antivirus idite na **Korisničko sučelje > Elementi korisničkog sučelja > Statusi aplikacije** u stablu Napredno podešavanje programa ESET Endpoint Antivirus.

Prikazivat će se odabrani statusi aplikacija

Naziv	Prikaži
<b>ANTI-PHISHING ZAŠTITA</b>	
Anti-Phishing zaštita je deaktivirana	<input checked="" type="checkbox"/>
Anti-Phishing zaštita je pauzirana	<input checked="" type="checkbox"/>
Anti-Phishing zaštita ne funkcioniра	<input checked="" type="checkbox"/>
<b>ANTIVIRUS</b>	
Anti-Stealth je deaktiviran	<input checked="" type="checkbox"/>
Anti-Stealth ne funkcioniра	<input checked="" type="checkbox"/>
Antivirusna i antispyware zaštita je pauzirana	<input checked="" type="checkbox"/>
Antivirusna zaštita ne funkcioniра	<input checked="" type="checkbox"/>
Rezidentna zaštita sistemskih datoteka je deaktivirana	<input checked="" type="checkbox"/>
Rezidentna zaštita sistemskih datoteka je pauzirana	<input checked="" type="checkbox"/>

U redu Odustani

Aktivirajte ili deaktivirajte koji će se statusi aplikacija prikazivati, na primjer, kada želite pauzirati antivirusnu i antispyware zaštitu ili aktivirati način rada za prezentacije. Status aplikacije prikazivat će se i ako program nije aktiviran ili je istekla licenca. Ta postavka može se promijeniti pomoću pravila programa [ESET Security Management Center](#).

## Podešavanje pristupa

Da bi se postigla maksimalna sigurnost sustava, program ESET Endpoint Antivirus mora biti pravilno konfiguriran. Svaka neovlaštena promjena može dovesti do gubitka važnih podataka. Da bi se izbjegle neovlaštene preinake, parametre podešavanja programa ESET Endpoint Antivirus moguće je zaštititi lozinkom.

### Upravljana okruženja

Administrator može stvoriti pravilo da bi lozinkom zaštitio postavke programa ESET Endpoint Antivirus na povezanim klijentskim računalima. Za stvaranje novog pravila pogledajte [Postavke zaštićene lozinkom](#).

### Neupravljano

Postavke konfiguracije za zaštitu lozinkom nalaze se u odjeljku **Napredno podešavanje** (F5) pod stavkom **Korisničko sučelje > Podešavanje pristupa**.

The screenshot shows the 'Napredno podešavanje' (Advanced Settings) screen. On the left, there's a sidebar with categories: MODUL DETEKCIJE (2), NADOGRADNJA (2), MREŽNA ZAŠTITA, WEB I E-POŠTA (3), KONTROLA UREĐAJA (2), ALATI (3), and KORISNIČKO SUČELJE (1). The main area has sections: ELEMENTI KORISNIČKOG SUČELJA, UPOZORENJA I OKVIRI S PORUKAMA, and PODEŠAVANJE PRISTUPA. Under PODEŠAVANJE PRISTUPA, there's a sub-section 'Zaštita postavki lozinkom' with a 'Postavi' button. At the bottom, there are buttons for 'Standardno', 'U redu' (with a shield icon), and 'Odustani'.

**Zaštita postavki lozinkom** – Odaberite za unos postavki lozinke. Kliknite da biste otvorili prozor za podešavanje lozinke.

Da biste postavili ili promijenili lozinku za zaštitu parametara podešavanja, kliknite **Postavi**.

# Lozinka za napredno podešavanje

Da biste zaštitali parametre podešavanja programa ESET Endpoint Antivirus i izbjegli neželjene preinake, morate postaviti novu lozinku.

## Upravljana okruženja

Administrator može stvoriti pravilo da bi lozinkom zaštitio postavke programa ESET Endpoint Antivirus na povezanim klijentskim računalima. Za stvaranje novog pravila pogledajte [Postavke zaštićene lozinkom](#).

## Neupravljano

Ako želite promijeniti postojeću lozinku:

1. Utipkajte staru lozinku u polje **Stara lozinka**.
2. Unesite novu lozinku u polja **Nova lozinka** i **Potvrda nove lozinke**.
3. Kliknite **U redu**.

Ta lozinka morat će se unijeti prilikom budućih preinaka programa ESET Endpoint Antivirus.

Ako zaboravite lozinku, moguće je vratiti pristup naprednim postavkama.

- [Vratite pristup uz pomoć metode „Vrati lozinku“ \(u verziji 7.1 i novijima\)](#)
- [Vratite pristup uz pomoć ESET-ova alata za otključavanje \(u verziji 7.0 i starijima\)](#)

---

[Pročitajte više informacija ako ste zaboravili licenčni ključ koji je izdala tvrtka ESET](#), datum isteka licence ili druge podatke o licenci za ESET Endpoint Antivirus.

## Upozorenja i okviri s porukama

**Tražite informacije o čestim upozorenjima i obavijestima?**

- [Pronađena je prijetnja](#)
  - [Adresa je blokirana](#)
  - [Program nije aktiviran](#)
  - [Dostupna je nadogradnja](#)
-  Informacije o nadogradnji nisu dosljedne
- [Otklanjanje poteškoća za poruku "Nadogradnja modula nije uspjela"](#)
  - ['Oštećena datoteka' ili 'Preimenovanje datoteke nije uspjelo'](#)
  - [Odbijen certifikat web stranice](#)
  - [Blokirana je mrežna prijetnja](#)

Odjeljak **Upozorenja i okviri s porukama** pod **Korisničko sučelje** omogućuje vam konfiguriranje načina na koji ESET Endpoint Antivirus upravlja prijetnjama kada korisnik treba donijeti odluku (na primjer, potencijalne web stranice za phishing).

Napredno podešavanje

MODUL DETEKCIJE (2)

NADODGRADNJA (2)

MREŽNA ZAŠTITA

WEB I E-POŠTA (3)

KONTROLA UREĐAJA (2)

ALATI (3)

KORISNIČKO SUČELJE (1)

ELEMENTI KORISNIČKOG SUČELJA

UPOZORENJA I OKVIRI S PORUKAMA

INTERAKTIVNA UPOZORENJA

Prikaži interaktivna upozorenja

Popis interaktivnih upozorenja [Uredi](#)

Kada odaberete "Pitaj korisnika" za bilo koje interaktivno upozorenje, lokalni korisnik s administratorskim ovlastima može odabrati radnju koja će se primijeniti kada se javi to interaktivno upozorenje. [Saznajte više...](#)

OKVIRI S PORUKAMA

Automatski zatvori okvire s porukama

Trajanje (u sekundama) 120

Poruke za potvrdu [Uredi](#)

PODEŠAVANJE PRISTUPA

Standardno

[U redu](#)

Odustani

## Interaktivna upozorenja

Prozori s interaktivnim upozorenjima prikazuju se ako se otkrije prijetnja ili ako je potrebna intervencija korisnika.

### Prikaži interaktivna upozorenja

ESET Endpoint Antivirus verzija 7.2 ili novija:

- Za korisnike kojima se ne upravlja preporučujemo da se ova opcija ostavi u standardnoj postavci (aktivirano).
- Za korisnike kojima se upravlja ova postavka treba ostati aktivirana te odaberite unaprijed definiranu radnju za korisnika na [popisu interaktivnih upozorenja](#).

Deaktiviranje opcije **Prikaži interaktivna upozorenja** sakrit će sve prozore upozorenja i dijaloške okvire u pregledniku. Unaprijed definirana standardna radnja odabrat će se automatski (na primjer, blokirat će se „Potencijalne web stranice za phishing“).

ESET Endpoint Antivirus verzija 7.1 ili starija:

Naziv ove postavke jest **Prikaži upozorenja** i nije moguće prilagoditi unaprijed definirane radnje za određene prozore s interaktivnim upozorenjima.

### Obavijesti na radnoj površini

[Obavijesti na radnoj površini](#) i oblačići sa savjetima samo su informativne prirode i ne zahtijevaju intervenciju korisnika. Odjeljak **Obavijesti na radnoj površini** premješten je u odjeljak **Alati > Obavijesti** u odjeljku Napredno podešavanje (u verziji 7.1 i novijima).

## Otvori s porukama

Da bi se skočni prozori s porukama automatski zatvarali nakon određenog vremenskog razdoblja, odaberite mogućnost **Automatski zatvori okvire s porukama**. Ako se ne zatvore ručno, prozori upozorenja automatski će se zatvoriti nakon isteka navedenog vremenskog razdoblja.

**Poruke za potvrdu** – Prikazuje [popis poruka za potvrdu](#) na kojem možete odabrati hoće li se iste prikazivati ili ne.

## Interaktivna upozorenja

U ovom je odjeljku istaknuto nekoliko prozora s interaktivnom upozorenjima koja će ESET Endpoint Antivirus prikazati prije provođenja bilo koje radnje.

Da bi se podesilo ponašanje interaktivnih upozorenja koja se mogu konfigurirati, idite na **Korisničko sučelje > Upozorenja i otvori s porukama > Popis interaktivnih upozorenja** programa ESET Endpoint Antivirus u stablu za napredno podešavanje i kliknite **Uredi**.

**i** Korisno za upravljanja okruženja gdje administrator svugdje može poništiti odabir opcije **Pitaj korisnika** i odabrati unaprijed definiranu radnju kad se prikažu prozori s interaktivnim upozorenjima.  
Također pogledajte [status aplikacije](#) unutar programa.

Naziv	Pitaj korisnika	Radnja se primjenjuje kada se ne prikaz...
<b>IZMJENJIVI MEDIJI</b>		
Otkriven je novi uređaj	<input checked="" type="checkbox"/>	Prikaz opcija skeniranja
<b>MREŽNA ZAŠTITA</b>		
Blokiran pristup mreži	<input checked="" type="checkbox"/>	Ništa
Blokirana je mrežna komunikacija	<input checked="" type="checkbox"/>	Blokiraj
Blokirana je mrežna prijetnja	<input checked="" type="checkbox"/>	Blokiraj
<b>NADOGRADNJA</b>		
Dostupna je nadogradnja	<input checked="" type="checkbox"/>	Ništa
<b>RAČUNALO</b>		

Provjerite ostale odjeljke pomoći u kojima se navodi određeni prozor s interaktivnim upozorenjem:

### Izmjenjivi mediji

- [Otkriven je novi uređaj](#)

### Zaštićeni preglednik

- [Dopusti nastavak u standardnom pregledniku](#)

## Mrežna zaštita

- [Blokiran pristup mreži](#) prikazuje se kad se pokrene zadatak klijenta **Izolacija računala s mreže** na ovoj radnoj stanici iz programa ESET PROTECT.
- [Blokirana je mrežna komunikacija](#)
- [Blokirana je mrežna prijetnja](#)

## Upozorenja web preglednika

- [Pronađen je potencijalno neželjen sadržaj](#)
- [Web stranica blokirana zbog phishinga](#)

## Računalo

Zbog prisutnosti ovih upozorenja korisničko sučelje prijeći će u narančastu boju:

- [Ponovno pokreni računalo \(obavezno\)](#)
- [Ponovno pokreni računalo \(preporučeno\)](#)

**i** Interaktivna upozorenja ne sadrže interaktivne prozore modula detekcije, HIPS-a ni firewalla jer se njihovo ponašanje može pojedinačno konfigurirati u određenoj funkciji.

## Poruke za potvrdu

Da biste podesili poruke za potvrdu idite na **Korisničko sučelje > Upozorenja i okviri s porukama > Poruke za potvrdu** u stablu Napredno podešavanje programa ESET Endpoint Antivirus i kliknite **Uredi**.

Prikazat će se odabrane poruke

<input checked="" type="checkbox"/> Pitaj prije brisanja dnevnika ESET SysInspectora
<input checked="" type="checkbox"/> Pitaj prije brisanja objekta iz karantene
<input checked="" type="checkbox"/> Pitaj prije brisanja statistike
<input checked="" type="checkbox"/> Pitaj prije brisanja svih dnevnika ESET SysInspectora
<input type="checkbox"/> Pitaj prije odbacivanja postavki u naprednom podešavanju
<input checked="" type="checkbox"/> Pitaj prije ostavljanja neuklonjenih prijetnji u upozorenjima
<input checked="" type="checkbox"/> Pitaj prije pokretanja zakazanog zadatka u planeru
<input checked="" type="checkbox"/> Pitaj prije uklanjanja svih zapisa dnevnika
<input checked="" type="checkbox"/> Pitaj prije uklanjanja zakazanog zadatka u planeru
<input checked="" type="checkbox"/> Pitaj prije uklanjanja zapisa iz dnevnika
<input checked="" type="checkbox"/> Pitaj prije vraćanja objekata iz karantene

U redu Odustani

U ovom se dijaloškom prozoru prikazuju poruke za potvrdu koje program ESET Endpoint Antivirus prikazuje prije provođenja bilo kakve akcije. Da biste dopustili prikaz neke poruke za potvrdu ili je deaktivirali, odaberite ili poništite odabir potvrdnog okvira pored nje.

Saznajte više o određenoj funkciji povezanoj s porukama za potvrdu:

- [Pitaj prije brisanja dnevnika ESET SysInspectora](#)
- [Pitaj prije brisanja svih dnevnika ESET SysInspectora](#)
- [Pitaj prije brisanja objekta iz karantene](#)
- Pitaj prije odbacivanja postavki u naprednom podešavanju
- [Pitaj prije ostavljanja neuklonjenih prijetnji u upozorenjima](#)
- [Pitaj prije uklanjanja zapisa iz dnevnika](#)
- [Pitaj prije uklanjanja zakazanog zadatka u planeru](#)
- [Pitaj prije uklanjanja svih zapisa dnevnika](#)
- [Pitaj prije brisanja statistike](#)
- [Pitaj prije vraćanja objekata iz karantene](#)
- [Pitaj prije vraćanja objekata iz karantene i izuzimanja iz skeniranja](#)
- [Pitaj prije pokretanja zakazanog zadatka u planeru](#)
- [Prikaži potvrđne dijaloške okvire za Outlook Express i Windows Mail](#)
- [Prikaži potvrđne dijaloške okvire za Windows Live Mail](#)
- [Prikaži potvrđne dijaloške okvire za Outlook](#)

## Pogreška zbog sukoba naprednih postavki

Do ove pogreške može doći ako neka komponenta (npr. HIPS) i korisnik stvore pravila u interaktivnom načinu rada ili načinu rada za učenje istovremeno.



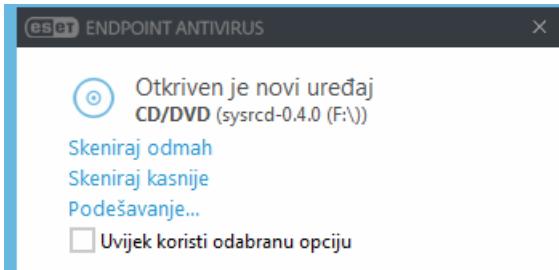
Preporučujemo da promijenite način filtriranja u standardni **Automatski način rada** ako želite sami stvarati svoja pravila. Pročitajte više o [HIPS-u i HIPS načinima filtriranja](#).

## Izmjenjivi mediji

ESET Endpoint Antivirus pruža automatsko skeniranje izmjenjivih medija (CD/DVD/USB/...) prilikom umetanja u računalo. To može biti korisno ako administrator računala želi korisnicima zabraniti uporabu izmjenjivih medija na kojima se nalazi nedopušten sadržaj.

Nakon umetanja izmjenjivog medija i podešavanja opcije **Prikaz opcija skeniranja** u programu ESET Endpoint

Antivirus, prikazuje se sljedeći prozor:



Opcije za ovaj prozor:

- **Skeniraj odmah** – Pokreće skeniranje izmjenjivih medija.
- **Skeniraj kasnije** – Skenira izmjenjive medije uz odgodu.
- **Podešavanje** – Otvara odjeljak **Napredno podešavanje**.
- **Uvijek koristi odabrano opciju** – Ako je odabrana ova opcija, ista će se radnja izvršiti i kada se izmjenjivi medij umetne i drugi put.

Osim toga, ESET Endpoint Antivirus sadrži funkciju kontrole uređaja, koja pruža mogućnost definiranja pravila za korištenje vanjskih uređaja na određenom računalu. Dodatne pojedinosti o kontroli uređaja možete pronaći u odjeljku [Kontrola uređaja](#).

## ESET Endpoint Antivirus 7.2 i noviji

Da biste pristupili postavkama za skeniranje izmjenjivih medija, otvorite Napredno podešavanje (**F5**) > **Korisničko sučelje** > **Upozorenja i okviri s porukama** > **Interaktivna upozorenja** > **Popis interaktivnih upozorenja** > **Uredi** > **Otkriven je novi uređaj**.

Ako nije odabrana opcija **Pitaj korisnika**, odaberite željenu radnju nakon umetanja izmjenjivog medija u računalo:

- **Ne skeniraj** – Neće se provesti nikakva radnja i prozor **Prepoznat je novi uređaj** neće se otvoriti.
- **Automatsko skeniranje uređaja** – Provest će se skeniranje računala za umetnuti izmjenjivi medij.
- **Prikaz opcija skeniranja** – otvara odjeljak za podešavanje opcije **Interaktivna upozorenja**.

## ESET Endpoint Antivirus 7.1 i stariji

Otvorite Napredno podešavanje (**F5**) > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Izmjenjivi mediji** da biste pristupili postavkama skeniranja izmjenjivih medija.

**Radnja koju treba napraviti nakon umetanja izmjenjivih medija** – Odaberite standardnu radnju koja će se provesti kada se dostupan izmjenjivi medijski uređaj umetne u računalo (CD/DVD/USB). Odaberite željenu radnju nakon umetanja izmjenjivog medija u računalo:

- **Ne skeniraj** – Neće se provesti nikakva radnja i prozor **Prepoznat je novi uređaj** neće se otvoriti.
- **Automatsko skeniranje uređaja** – Provest će se skeniranje računala za umetnuti izmjenjivi medij.

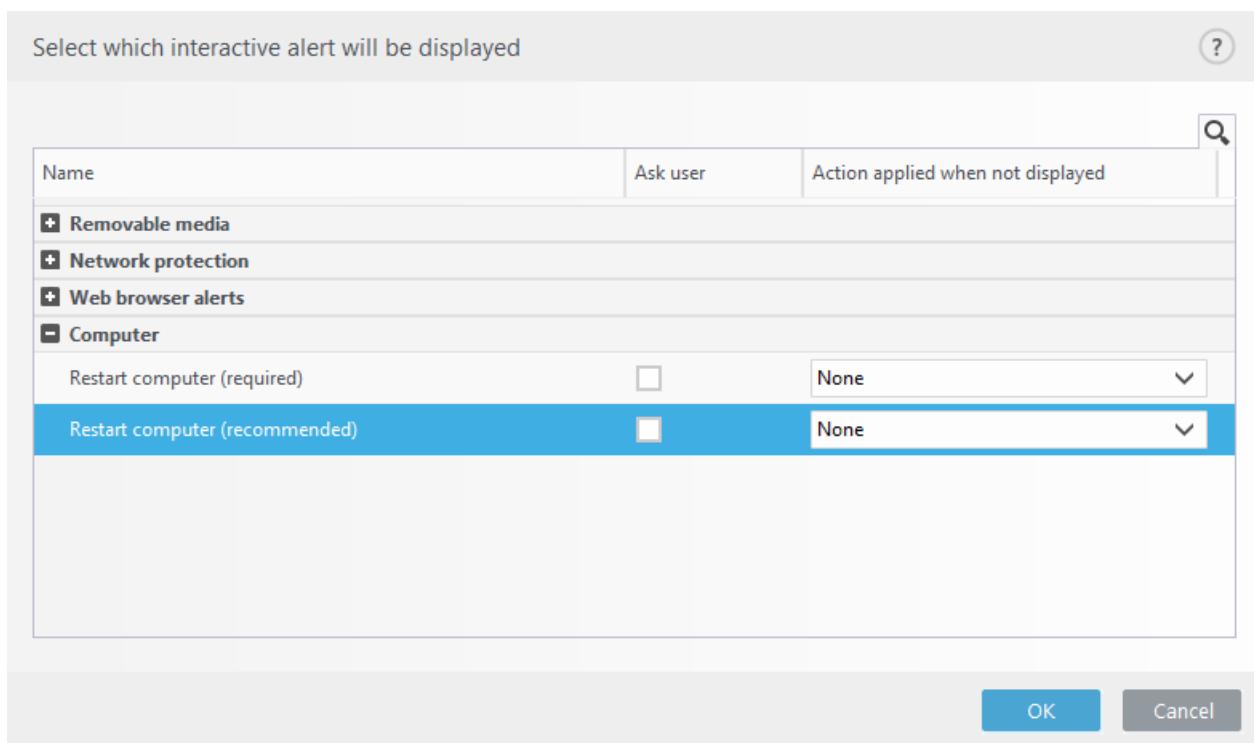
- Prikaz mogućnosti skeniranja – Otvara odjeljak podešavanja izmjenjivih medija.

## Potrebno je ponovno pokretanje

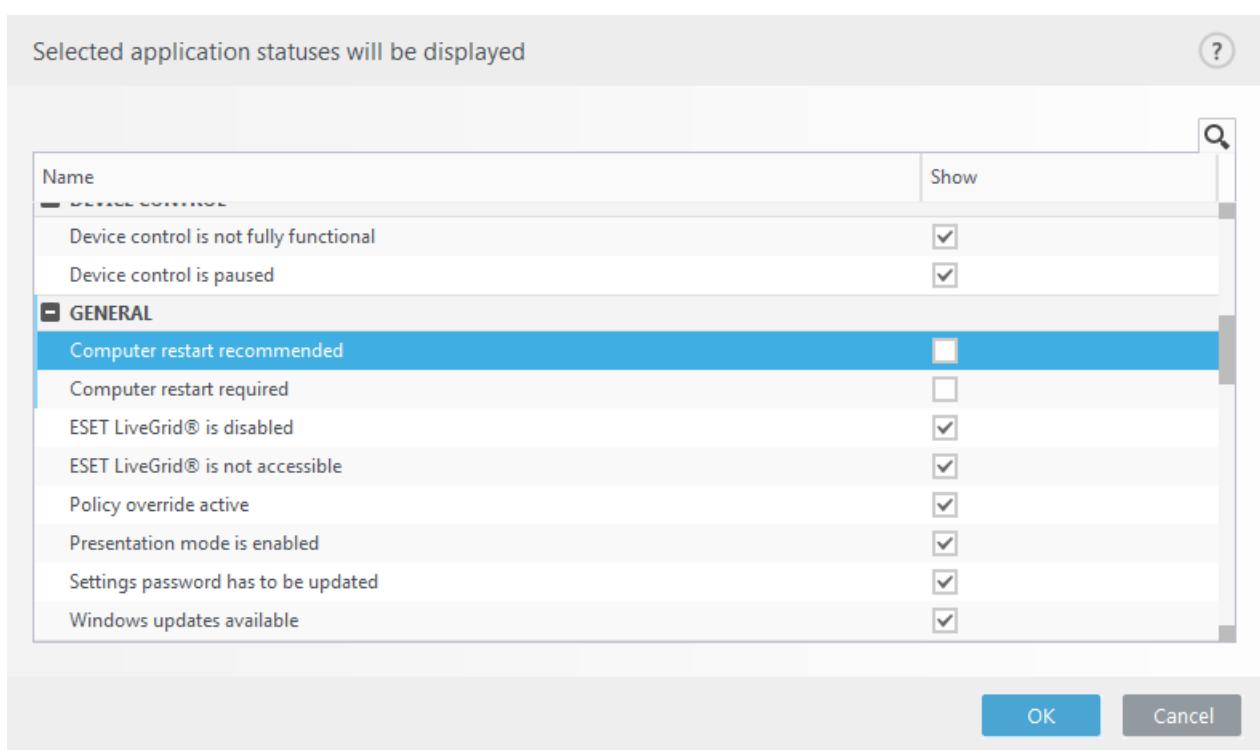
Ako krajnji uređaji primaju crveno upozorenje „Potrebno je ponovno pokretanje”, možete onemogućiti prikazivanje upozorenja.

Da biste deaktivirali upozorenje „Potrebno je ponovno pokretanje” ili „Preporučuje se ponovno pokretanje”, pratite korake u nastavku:

1. Pritisnite tipku **F5** da biste pristupili odjeljku Napredno podešavanje i proširili odjeljak **Upozorenja i okviri s porukama**.
2. Kliknite **Uredi** pored **Popisa interaktivnih upozorenja**. U odjeljku **Računalo** odznačite okvire pored odjeljaka **Ponovno pokreni računalo (obavezno)** i **Ponovno pokreni računalo (preporučeno)**.



3. Kliknite **U redu** za spremanje promjena u oba otvorena prozora.
4. Upozorenja se više neće prikazivati na krajnjem uređaju.
5. (nije obavezno) Da biste deaktivirali status aplikacije u glavnom prozoru programa ESET Endpoint Antivirus, u prozoru Status aplikacija odznačite okvire pored odjeljaka **Potrebno je ponovno pokretanje računala** i **Preporučuje se ponovno pokretanje računala**.



## Preporučuje se ponovno pokretanje

Ako krajnji uređaji primaju žuto upozorenje „Preporučuje se ponovno pokretanje”, možete onemogućiti prikazivanje upozorenja.

Da biste deaktivirali upozorenje „Potrebno je ponovno pokretanje” ili „Preporučuje se ponovno pokretanje”, pratite korake u nastavku:

1. Pritisnite tipku **F5** da biste pristupili odjeljku Napredno podešavanje i proširili odjeljak **Upozorenja i okviri s porukama**.
2. Kliknite **Uredi** pored **Popisa interaktivnih upozorenja**. U odjeljku **Računalo** odznačite okvire pored odjeljaka **Ponovno pokreni računalo (obavezno)** i **Ponovno pokreni računalo (preporučeno)**.

Select which interactive alert will be displayed

Name	Ask user	Action applied when not displayed
<b>+ Removable media</b>	<input type="checkbox"/>	<input type="button" value="None"/>
<b>+ Network protection</b>	<input type="checkbox"/>	<input type="button" value="None"/>
<b>+ Web browser alerts</b>	<input type="checkbox"/>	<input type="button" value="None"/>
<b>- Computer</b>		
Restart computer (required)	<input type="checkbox"/>	<input type="button" value="None"/>
Restart computer (recommended)	<input type="checkbox"/>	<input type="button" value="None"/>

**OK**    **Cancel**

3. Kliknite **U redu** za spremanje promjena u oba otvorena prozora.
4. Upozorenja se više neće prikazivati na krajnjem uređaju.
5. (nije obavezno) Da biste deaktivirali status aplikacije u glavnom prozoru programa ESET Endpoint Antivirus, u prozoru [Status aplikacija](#) odznačite okvire pored odjeljaka **Potrebno je ponovno pokretanje računala i Preporučuje se ponovno pokretanje računala**.

Selected application statuses will be displayed

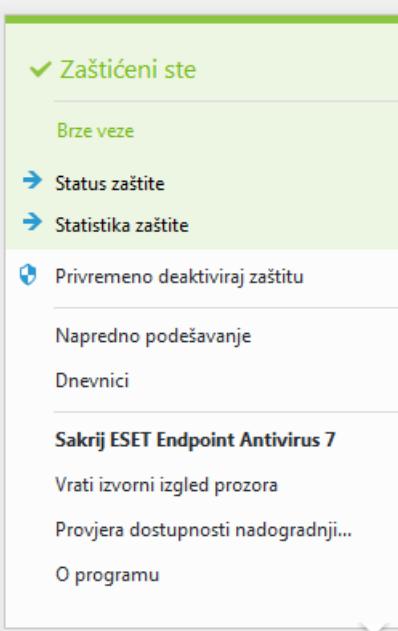
Name	Show
<b>- DEVICE CONTROL</b>	
Device control is not fully functional	<input checked="" type="checkbox"/>
Device control is paused	<input checked="" type="checkbox"/>
<b>- GENERAL</b>	
Computer restart recommended	<input type="checkbox"/>
Computer restart required	<input type="checkbox"/>
ESET LiveGrid® is disabled	<input checked="" type="checkbox"/>
ESET LiveGrid® is not accessible	<input checked="" type="checkbox"/>
Policy override active	<input checked="" type="checkbox"/>
Presentation mode is enabled	<input checked="" type="checkbox"/>
Settings password has to be updated	<input checked="" type="checkbox"/>
Windows updates available	<input checked="" type="checkbox"/>

**OK**    **Cancel**

# Ikona trake sustava

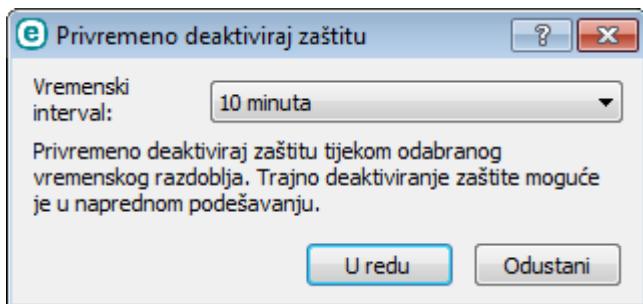
Neke od najvažnijih mogućnosti i značajki podešavanja dostupne su kada desnom tipkom miša kliknete ikonu trake sustava .

 Da biste pristupili izborniku ikone trake sustava, provjerite je li način pokretanja funkcije [Elementi korisničkog sučelja](#) postavljen na Potpuno.



**Pauziraj zaštitu** – Prikazuje upit za potvrdu kojim se deaktivira [Modul detekcije](#), koji štiti od napada kontrolirajući komunikaciju datoteka, weba i e-pošte.

Padajući izbornik **Vremensko razdoblje** predstavlja vremensko razdoblje tijekom kojeg će zaštita biti deaktivirana.



**Napredno podešavanje** – odaberite ovu opciju da biste ušli u stablo **Napredno podešavanje**. Naprednom podešavanju možete pristupiti i pritiskanjem tipke F5 ili odlaskom na **Podešavanje > Napredno podešavanje**.

**Dnevnnici** – [Dnevnnici](#) sadrže informacije o svim važnim događajima u programu koji su se pojavili i pružaju pregled otkrivenih prijetnji.

**Otvori program ESET Endpoint Antivirus** – Otvara glavni prozor programa ESET Endpoint Antivirus s ikone trake.

**Poništi raspored prozora** – Vraća prozor programa ESET Endpoint Antivirus na standardnu veličinu i položaj na

zaslonu.

**Provjera dostupnosti nadogradnji** – Pokreće nadogradnju programskih modula kako bi se osigurala vaša razina zaštite od zlonamjernog koda.

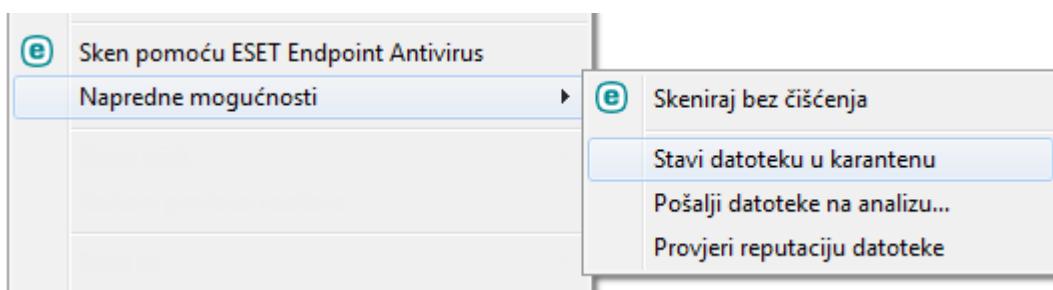
**O programu** – Pruža informacije o sustavu, detalje o instaliranoj verziji programa ESET Endpoint Antivirus i instaliranim modulima programa, kao i datum isteka valjanosti vaše licence. Informacije o operacijskom sustavu i sistemskim resursima nalaze se na dnu stranice.

## Kontekstni izbornik

Kontekstni izbornik prikazuje se kada desnom tipkom miša kliknete neki objekt (datoteku). Izbornik prikazuje sve akcije koje se mogu izvesti na objektu.

Upravljački elementi programa ESET Endpoint Antivirus mogu se integrirati u kontekstni izbornik. Mogućnosti podešavanja za tu funkciju dostupne su na stablu Napredno podešavanje pod **Korisničko sučelje > Elementi korisničkog sučelja**.

**Integriraj u kontekstni izbornik** – Integrirajte kontrolne elemente programa ESET Endpoint Antivirus u kontekstni izbornik.



## Pomoć i podrška

ESET Endpoint Antivirus sadrži alate za otklanjanje poteškoća i informacije za podršku koje će vam pomoći u rješavanju problema koji se mogu pojaviti.

### Instalirani program

- **O programu ESET Endpoint Antivirus** – Prikazuje informacije o vašoj kopiji programa [ESET Endpoint Antivirus](#).
- [\*\*Otklanjanje poteškoća s programom\*\*](#) – kliknite ovaj link da biste pronašli rješenja za najčešće probleme.
- [\*\*Otklanjanje poteškoća s licencom\*\*](#) – kliknite ovaj link da biste pronašli rješenja za probleme s aktivacijom ili promjenom licence.
- [\*\*Promjena licence\*\*](#) – Kliknite za pokretanje aktivacijskog prozora i aktivaciju programa.

### Stranica pomoći – Kliknite ovaj link da biste pokrenuli stranicu pomoći programa ESET Endpoint Antivirus.



## Tehnička podrška

- **Zatražite podršku** – ako ne možete pronaći odgovor na svoj problem, možete upotrijebiti ovaj obrazac koji se nalazi na web stranici tvrtke ESET da biste se brzo obratili odjelu za tehničku podršku. Na temelju vaših postavki, prozor [Pošalji podatke o konfiguraciji sustava](#) će se prikazati prije ispunjavanja web obrasca.
- **Detalji za tehničku podršku** – Kada vam se prikaže odzivnik, možete kopirati i poslati informacije tehničkoj podršci tvrtke ESET (na primjer naziv programa, verziju programa, operacijski sustav i vrstu procesora).
- **ESET Log Collector** – Veza na članak iz [ESET-ove baze znanja](#) na kojem možete preuzeti uslužni alat ESET Log Collector, aplikaciju koja automatski prikuplja informacije i dnevниke s računala i omogućuje brže rješavanje problema. Za više informacija pogledajte mrežni korisnički priručnik za [ESET Log Collector](#).
- Aktivirajte [Napredno vođenje dnevnika](#) za izradu naprednih dnevnika za sve dostupne funkcije kako biste pomogli programerima u dijagnozi i rješavanju problema. Minimalna opširnost vođenja dnevnika postavljena je na razinu Dijagnostičko. Napredno vođenje dnevnika automatski će biti deaktivirano nakon dva sata, osim ako ga ne zaustavite ranije klikom na Zaustavi napredno vođenje dnevnika. Nakon što se izrade svi dnevnići, prikazat će se prozor obavijesti koji pruža izravan pristup mapi Dijagnostike s izrađenim dnevnicima.



**Baza znanja** – [ESET-ova baza znanja](#) sadrži odgovore na najčešće postavljana pitanja kao i preporučena rješenja za razne probleme. Stručnjaci tehničke podrške tvrtke ESET redovito nadograđuju bazu znanja, što je čini najpotpunijim alatom za rješavanje raznih problema.

## O programu ESET Endpoint Antivirus

U ovom se prozoru navode detalji o instaliranoj verziji programa ESET Endpoint Antivirus, vašem operacijskom sustavu i resursima sustava.

Da biste vidjeli informacije o popisu instaliranih modula programa i njihovim verzijama, kliknite **Instalirane komponente**. Informacije o modulima možete kopirati u međuspremnik tako da kliknete **Kopiraj**. To može biti korisno prilikom otklanjanja poteškoća ili kontaktiranja s tehničkom podrškom.

The screenshot shows the ESET Endpoint Antivirus application window. On the left sidebar, there are several icons and labels: 'STATUS ZAŠTITE' (checkmark), 'SKENIRANJE RAČUNALA' (magnifying glass), 'AKTUALIZACIJA' (refresh), 'PODEŠAVANJE' (gear), 'ALATI' (briefcase), and 'POMOĆ I PODRŠKA' (question mark). The main content area has a title 'O programu' with a back arrow icon. It displays the following information:

- ESET Endpoint Antivirus™, verzija 8.0.2028.0**
- Nova generacija tehnologije NOD32.
- Autorska prava © 1992-2020 ESET, spol. s r.o. Sva prava pridržana.
- Ovaj je program zaštićen američkim patentom br. US 8.943.592.

Below this, there are two blue links:

- Licenčni ugovor za krajnjeg korisnika
- Pravila privatnosti

Underneath these links, the following user details are shown:

- Korisničko ime: ESET\michal.novomesky
- Naziv računala: DESKTOP-DDGGG57
- Naziv mjesta: DESKTOP-DDGGG57-1

A blue button labeled 'Instalirane komponente' is visible at the bottom of this section. At the very bottom of the main content area, a warning message is displayed in a grey box:

**Upozorenje:** ovaj je program zaštićen autorskim pravima i međunarodnim sporazumima. Strogo se zabranjuje kopiranje ili distribucija na bilo koji način, djelomično ili u cijelosti, bez izričitog dopuštenja tvrtke ESET, spol. s r.o., što u suprotnom može dovesti do međunarodnog kaznenog progona u punoj mjeri dozvoljenoj zakonom. ESET, logotip ESET, ESET Endpoint Antivirus, LiveGrid, logotip LiveGrid i SysInspector zaštitni su ili registrirani zaštitni znakovi tvrtke ESET, spol. s r.o. u Europskoj uniji i/ili drugim zemljama. Svi drugi zaštitni znakovi vlasništvo su njihovih pojedinih vlasnika.

## Slanje podataka o sistemsкој konfigurацији

Radi pružanja što brže i preciznije pomoći, tvrtki ESET potrebne su informacije o konfiguraciji programa ESET Endpoint Antivirus, detaljne informacije o sustavu i procesima koji se izvršavaju ([dnevnik značajke ESET SysInspector](#)) te podaci iz registra. ESET te podatke koristi isključivo za osiguranje tehničke podrške za korisnike.

Prilikom slanja web obrasca tvrtki ESET bit će poslani podaci o konfiguraciji vašeg sustava. Odaberite mogućnost **Uvijek pošalji ove podatke** ako želite da ova radnja ostane upamćena za ovaj proces. Za slanje obrasca bez ikakvih podataka kliknite **Nemoj slati podatke** i obratite se tehničkoj podršci tvrtke ESET putem web obrasca za podršku.

Ovu postavku možete konfigurirati i u odjelu **Napredno podešavanje > Alati > Dijagnostika > Tehnička podrška**.

**i** Ako odlučite poslati sistemske podatke, morate ispuniti i poslati web obrazac jer u protivnom vaš zahtjev neće biti stvoren i sistemski podaci bit će izgubljeni.

## Tehnička podrška

### Obratite se tehničkoj podršci

**Zatražite podršku** – ako ne možete pronaći odgovor na svoj problem, možete upotrijebiti ovaj obrazac koji se nalazi na web stranici tvrtke ESET da biste se brzo obratili ESET-ovoj tehničkoj podršci. Na temelju vaših postavki, prozor [Pošalji podatke o konfiguraciji sustava](#) prikazat će se prije ispunjavanja web obrasca.

## Potražite informacije za tehničku podršku

**Detalji za tehničku podršku** – kada vam se prikaže upit, možete kopirati i poslati informacije ESET-ovoj tehničkoj podršci (kao što su detalji o licenci, naziv programa, verzija programa, operacijski sustav i podaci o računalu).

**ESET Log Collector** – Veza na članak iz [ESET-ove baze znanja](#) na kojem možete preuzeti uslužni alat ESET Log Collector, aplikaciju koja automatski prikuplja informacije i dnevниke s računala i omogućuje brže rješavanje problema. Za više informacija pogledajte mrežni korisnički priručnik za [ESET Log Collector](#).

Aktivirajte [Napredno vođenje dnevnika](#) za izradu naprednih dnevnika za sve dostupne funkcije kako biste pomogli programerima u dijagnozi i rješavanju problema. Minimalna opširnost vođenja dnevnika postavljena je na razinu **Dijagnostičko**. Napredno vođenje dnevnika automatski će biti deaktivirano nakon dva sata, osim ako ga ne zaustavite ranije klikom na **Zaustavi napredno vođenje dnevnika**. Nakon što se izrade svi dnevnići, prikazat će se prozor obavijesti koji pruža izravan pristup mapi Dijagnostike s izrađenim dnevnicima.

## Upravljanje profilima

Upravljanje profilima koristi se na dva mesta u programu ESET Endpoint Antivirus – u odjeljku **Skeniranje računala na zahtjev** i u odjeljku **Aktualizacija**.

### skeniranje računala na zahtjev

Vaši preferirani parametri skeniranja mogu se spremiti za buduća skeniranja. Preporučujemo da stvorite drugi profil (s različitim ciljevima i metodama skeniranja te ostalim parametrima) za svako redovito korišteno skeniranje.

Da biste stvorili novi profil, otvorite prozor Napredno podešavanje (F5) i kliknite **Antivirus > Skeniranje računala na zahtjev**, a zatim **Uredi uz Popis profila**. Padajući izbornik **Aktualizacijski profil** prikazuje postojeće profile skeniranja. Pomoć pri stvaranju profila skeniranja koji odgovara vašim potrebama potražite u odjeljku [Podešavanje parametara sustava ThreatSense](#) za opis svakog parametra podešavanja skeniranja.

Prepostavimo da želite stvoriti vlastiti profil skeniranja i djelomično vam odgovara konfiguracija **Skenirajte svoje računalo**, no ne želite skenirati [runtime arhivatore](#) ni [potencijalno nesigurne aplikacije](#) te želite **i** primjeniti **Potpuno čišćenje**. Unesite naziv novog profila u prozoru **Upravljanje profilima** i kliknite **Dodaj**. Odaberite novi profil iz padajućeg izbornika **Odabrani profil** i prilagodite preostale parametre kako vam odgovara te kliknite **U redu** da biste spremili novi profil.

### Nadogradnja

Uređivač profila u odjeljku za podešavanje aktualizacije korisnicima omogućuje stvaranje novih aktualizacijskih profila. Stvarajte i koristite vlastite prilagođene profile (koji se razlikuju od standardnog predloška **Moj profil**) samo ako na računalu koristite više različitih načina povezivanja s aktualizacijskim serverima.

Na primjer, prijenosno računalo koje se obično povezuje s lokalnim serverom (mirrorom) u lokalnoj mreži, ali koje u slučaju prekida veze s lokalnom mrežom (tijekom, primjerice, poslovnog puta) preuzima aktualizacije izravno s aktualizacijskog servera tvrtke ESET, može koristiti dva profila: jedan za povezivanje s lokalnim serverom, a drugi za povezivanje sa serverima tvrtke ESET. Nakon konfiguracije tih profila idite na **Alati > Planer** i uredite parametre aktualizacijskog zadatka. Odredite jedan profil kao primarni, a drugi kao sekundarni.

Profil za nadogradnju – Profil za nadogradnju koji se trenutačno koristi. Da biste ga promijenili, odaberite neki profil s padajućeg izbornika.

Popis profila – Stvorite nove ili uklonite postojeće profile za nadogradnju.

## Tipkovnički prečaci

Za bolju navigaciju u programu ESET Endpoint Antivirus možete upotrebljavati sljedeće tipkovničke prečace:

Tipkovnički prečaci	Poduzeta radnja
F1	otvara stranice pomoći
F5	otvara Napredno podešavanje
Up/Down	navigacija kroz stavke programa
TAB	pomiče pokazivač u prozoru
Esc	zatvara aktivni dijaloški prozor
Ctrl+U	prikazuje informacije o licenci za ESET i vašem računalu (Detalji za tehničku podršku)
Ctrl+R	vraća prozor programa na standardnu veličinu i položaj na zaslonu

## Dijagnostika

Dijagnostika omogućuje stvaranje slike stanja memorije u slučaju pada aplikacija za ESET procese (primjerice, ekrn). Ako dođe do pada aplikacije, generira se slika stanja memorije. To razvojnim programerima može pomoći ukloniti poteškoće i riješiti razne ESET Endpoint Antivirus probleme.

Kliknite padajući izbornik pored stavke **Vrsta slike stanja memorije** i odaberite jednu od tri dostupne opcije:

- Odaberite **Deaktiviraj** da biste deaktivirali funkciju.
- **Mini** – Bilježi najmanji skup korisnih informacija pomoći kojih bi se mogao prepoznati razlog neočekivanog pada aplikacije. Takva datoteka dumpa može biti korisna ako je prostor ograničen, no budući da sadrži ograničene informacije, pogreške koje nisu izravno uzrokovane nizom koji je bio pokrenut u vrijeme kada se problem pojavio možda se neće moći otkriti analizom takve datoteke.
- **Kompletan** – Bilježi cjelokupan sadržaj sistemske memorije kada aplikacija neočekivano prestane s radom. Dump cijele memorije može sadržavati podatke iz procesa koji su bili pokrenuti prilikom prikupljanja dumpa memorije.

**Ciljani direktorij** – Direktorij u kojem će se tijekom pada sustava generirati sliku stanja memorije.

**Otvori mapu dijagnostike** – Kliknite **Otvori** da biste otvorili ovaj direktorij u *novom prozoru Windows explorer*.

**Stvari dijagnostički dump** – kliknite **Stvari** da biste stvorili dijagnostičke datoteke slike stanja memorije u **ciljnom direktoriju**.

## Napredno vođenje dnevnika

**Aktiviraj napredno vođenje dnevnika skenera računala** – Bilježi sve događaje koji se dogode tijekom skeniranja

datoteka i mapa pomoću skeniranja računala ili rezidentne zaštite sistemskih datoteka.

**Aktiviraj napredno vođenje dnevnika kontrole uređaja** – Bilježi sve događaje koji se dogode u kontroli uređaja. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s kontrolom uređaja.

**Aktiviraj napredno vođenje dnevnika zaštite dokumenata** – bilježi sve događaje koji se dogode u zaštiti dokumenata kako bi se omogućilo dijagnosticiranje i rješavanje problema.

**Aktiviraj napredno vođenje dnevnika jezgre** – bilježi sve događaje koji se dogode na usluzi ESET Kernel (ekrn) radi dijagnostike i rješavanja problema (dostupno u verziji 7.2 i novijima).

**Aktiviraj napredno vođenje dnevnika licenciranja** – bilježi svu komunikaciju programa s ESET-ovim aktivacijskim i ESET Business Account serverima.

**Aktiviraj praćenje memorije** – Zapisivanje svih događaja koji će razvojnim inženjerima pomoći u dijagnosticiranju curenja memorije.

**Aktiviraj napredno vođenje dnevnika mrežne zaštite** – Bilježi sve mrežne podatke koji prolaze kroz firewall u PCAP formatu kako bi se razvojnim programerima pomoglo u dijagnozi i popravku problema povezanih s firewallom.

**Aktiviraj napredno vođenje dnevnika operacijskog sustava** – Prikupljat će se dodatne informacije o operacijskom sustavu kao što su pokrenuti procesi, aktivnost procesora, operacije diska. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s ESET-ovim programom koji radi na vašem operacijskom sustavu.

**Aktiviraj napredno vođenje dnevnika filtriranja protokola** – Bilježi sve mrežne podatke koji prolaze kroz modul za filtriranje protokola u PCAP formatu kako bi se razvojnim programerima pomoglo u dijagnostici i otklanjanju problema povezanih s filtriranjem protokola.

**Aktiviraj napredno vođenje dnevnika rezidentne zaštite sistemskih datoteka** – bilježi sve događaje koji se događaju u rezidentnoj zaštiti sistemskih datoteka da bi se omogućilo dijagnosticiranje i rješavanje problema.

**Aktiviraj napredno vođenje dnevnika modula za nadogradnju** – Bilježi sve događaje do kojih dolazi tijekom nadogradnje. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s modulom za nadogradnju.

## Lokacija dnevnika

*C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics\*

## Skener naredbenog retka

Modul za antivirusnu zaštitu programa ESET Endpoint Antivirus moguće je pokrenuti iz naredbenog retka – ručno (pomoću naredbe „ecls“) ili pomoću skupne datoteke („bat“).

Upotreba ESET skenera iz naredbenog retka:

```
ecls [OPTIONS...] FILES..
```

Kada se skeniranje na zahtjev pokreće iz naredbenog retka, potrebno je koristiti sljedeće parametre:

## Mogućnosti

/base-dir=MAPA	učitaj module iz MAPE
/quar-dir=MAPA	MAPA karantene
/exclude=MASKA	izuzmi iz skeniranja datoteke koje odgovaraju MASKI
/subdir	skeniraj podmape (standardno)
/no-subdir	ne skeniraj podmape
/max-subdir-level=RAZINA	maksimalna podrazina mapa unutar mapa za skeniranje
/symlink	slijedi simboličke veze (standardno)
/no-symlink	preskoči simboličke veze
/ads	skeniraj ADS-ove (standardno)
/no-ads	ne skeniraj ADS-ove
/log-file=DATOTEKA	zapiši izlaz u DATOTEKU
/log-rewrite	prebriši izlaznu datoteku (standardno – dopuni)
/log-console	zapiši izlaz u konzolu (standardno)
/no-log-console	ne zapisuj izlaz u konzolu
/log-all	zapiši i čiste datoteke
/no-log-all	ne zapisuj čiste datoteke (standardno)
/aind	prikaži indikator aktivnosti
/auto	automatski skeniraj i očisti sve lokalne diskove

## Mogućnosti skenera

/files	skeniraj datoteke (standardno)
/no-files	ne skeniraj datoteke
/memory	skeniraj memoriju
/boots	skeniraj boot sektore
/no-boots	ne skeniraj boot sektore (standardno)
/arch	skeniraj arhive (standardno)
/no-arch	ne skeniraj arhive
/max-obj-size=VELIČINA	skeniraj samo datoteke manje od VELIČINE u megabajtima (standardno 0 = neograničeno)
/max-arch-level=RAZINA	maksimalna podrazina arhiva unutar arhiva (ugniježđene arhive) za skeniranje
/scan-timeout=OGRANIČENJE	skeniraj arhive najviše do OGRANIČENJA u sekundama
/max-arch-size=VELIČINA	skeniraj samo datoteke u arhivi ako su manje od VELIČINE (standardno 0 = neograničeno)
/max-sfx-size=VELIČINA	skeniraj samo datoteke u samoraspakirajućim arhivama ako su manje od VELIČINE u megabajtima (standardno 0 = neograničeno)
/mail	skeniraj datoteke e-pošte (standardno)
/no-mail	ne skeniraj datoteke e-pošte
/mailbox	skeniraj poštanske sandučiće (standardno)

/no-mailbox	ne skeniraj poštanske sandučiće
/sfx	skeniraj samoraspakirajuće arhive (standardno)
/no-sfx	ne skeniraj samoraspakirajuće arhive
/rtp	skeniraj runtime arhivatore (standardno)
/no-rtp	ne skeniraj runtime arhivatore
/unsafe	skeniraj potencijalno nesigurne aplikacije
/no-unsafe	ne skeniraj potencijalno nesigurne aplikacije (standardno)
/unwanted	skeniraj potencijalno neželjene aplikacije
/no-unwanted	ne skeniraj potencijalno neželjene aplikacije (standardno)
/suspicious	skeniraj sumnjive aplikacije (standardno)
/no-suspicious	ne skeniraj sumnjive aplikacije
/pattern	koristi potpise (standardno)
/no-pattern	ne koristi potpise
/heur	aktiviraj heurstiku (standardno)
/no-heur	deaktiviraj heurstiku
/adv-heur	aktiviraj naprednu heurstiku (standardno)
/no-adv-heur	deaktiviraj naprednu heurstiku
/ext-exclude=EKSTENZIJE	izuzmi iz skeniranja EKSTENZIJE datoteka razgraničene dvotočkom
/clean-mode=NAČIN	<p>koristi NAČIN čišćenja za zaražene objekte</p> <p>Na raspolaganju su sljedeće mogućnosti:</p> <ul style="list-style-type: none"> <li>• <b>none</b> (standardno) – Automatsko čišćenje neće se izvršiti.</li> <li>• <b>standard</b> – ecls.exe automatski će pokušati očistiti ili izbrisati zaražene datoteke.</li> <li>• <b>strict (strog)</b> – ecls.exe automatski će pokušati očistiti ili izbrisati zaražene datoteke bez intervencije korisnika (neće se prikazati odzivnik prije brisanja datoteka).</li> <li>• <b>rigorous (rigorozno)</b> – ecls.exe će izbrisati datoteke bez pokušaja čišćenja, neovisno o tome o kakvim se datotekama radi.</li> <li>• <b>delete (brisanje)</b> – ecls.exe će izbrisati datoteke bez pokušaja čišćenja, ali neće izbrisati osjetljive datoteke poput onih sustava Windows.</li> </ul>
/quarantine	kopiraj zaražene datoteke (ako su očišćene) u karantenu (dopunjuje akciju koja se izvršava prilikom čišćenja)
/no-quarantine	ne kopiraj zaražene datoteke u karantenu

## Općenite mogućnosti:

/help	prikaži pomoć i izađi
/version	prikaži informacije o verziji i izađi
/preserve-time	sačuvaj vremensku oznaku zadnjeg pristupa

## Izlazni kodovi

0	nisu pronađene prijetnje
1	prijetnje su pronađene i očišćene

10	neke datoteke nisu se mogle skenirati (možda su prijetnje)
50	pronađena je prijetnja
100	pogreška

 Izlazni kodovi veći od 100 znače da datoteka nije skenirana pa bi stoga mogla biti zaražena.

## ESET CMD

Ovom se funkcijom aktiviraju napredne ecmd naredbe. Omogućuje vam izvoz i uvoz postavki upotrebom naredbenog retka (ecmd.exe). Dosad je bilo moguće izvoziti postavke samo uporabom [GUI-ja](#). ESET Endpoint Antivirus konfiguracija se može izvesti u datoteci .xml.xml.

Kada aktivirate ESET CMD, dostupne su dvije metode autorizacije:

- **Ništa** – nema autorizacije. Ne preporučujemo ovu metodu jer omogućuje uvoz svih nepotpisanih konfiguracija, što predstavlja potencijalni rizik.
- **Lozinka naprednog podešavanja** – potrebna je lozinka za uvoz konfiguracije iz datoteke .xml, ta datoteka mora biti potpisana (pogledajte potpisivanje konfiguracijske datoteke .xml u nastavku). Lozinka navedena u [Podešavanju pristupa](#) mora se navesti kako bi bilo moguće uesti novu konfiguraciju. Ako podešavanje pristupa nije aktivirano, lozinka ne odgovara ili konfiguracijska datoteka .xml nije potpisana, konfiguracija se neće uesti.

Kad se aktivira ESET CMD, možete upotrijebiti naredbeni redak za uvoz ili izvoz konfiguracija ESET Endpoint Antivirus. To možete učiniti ručno ili možete stvoriti skriptu radi automatizacije postupka.

 Da biste se mogli koristiti naprednim ecmd naredbama, morate ih pokrenuti s administratorskim ovlastima ili otvoriti naredbeni redak sustava Windows (cmd) opcijom **Pokreni kao administrator**. U protivnom ćete primiti poruku **Error executing command**. Isto tako, kada izvozite konfiguraciju, mora postojati odredišna mapa. Naredba izvoza i dalje radi kad se postavka ESET CMD isključi.

 Napredne ecmd naredbe mogu se pokrenuti samo lokalno. Izvršavanje zadatka klijenta **Izvrši naredbu** upotrebom ESET PROTECT-e ili ESMC-e neće raditi.

Naredba izvoza postavki:  
ecmd /getcfg c:\config\settings.xml



Naredba uvoza postavki:  
ecmd /setcfg c:\config\settings.xml

Potpisivanje konfiguracijske datoteke .xml:

1. Preuzmite izvršnu datoteku [XmlSignTool](#).
2. Otvorite naredbeni redak sustava Windows (cmd) opcijom **Pokreni kao administrator**.
3. Idite na lokaciju gdje je spremljena datoteka xmldsigntool.exe
4. Izvršite naredbu da biste potpisali konfiguracijsku datoteku .xml, upotreba: xmldsigntool /version 1|2 <xml\_file\_path>

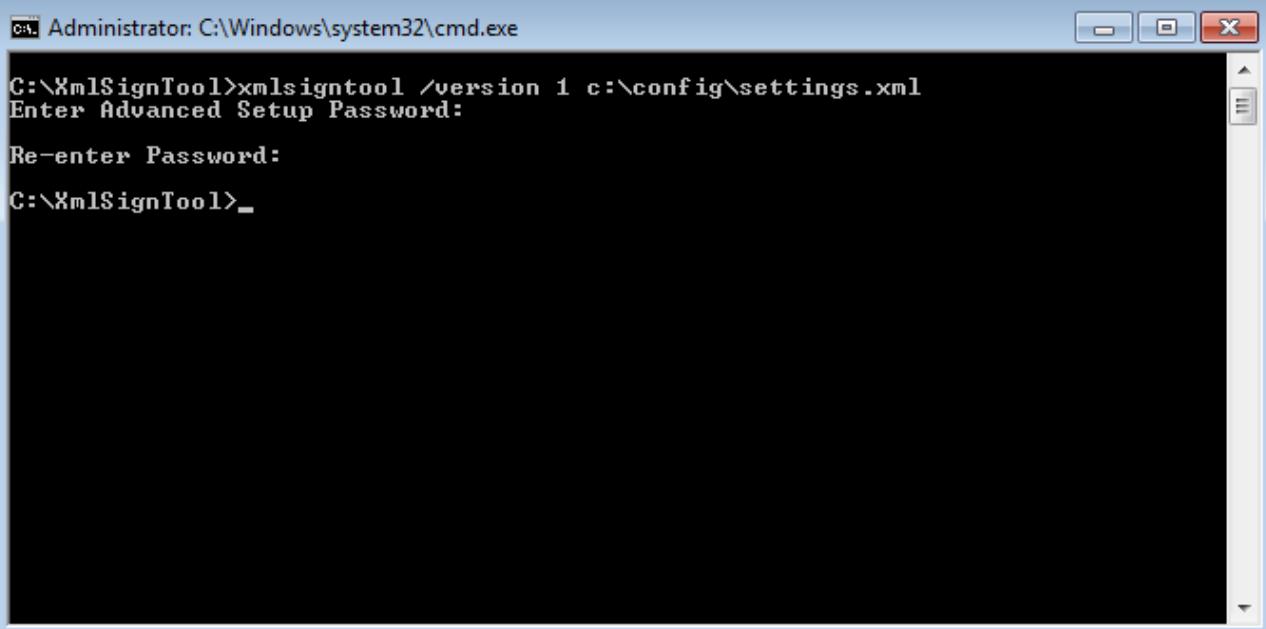


Vrijednost parametra /version ovisi o vašoj verziji programa ESET Endpoint Antivirus. Upotrebljavajte vrijednost /version 2 za verziju 7 i novije verzije.

5. Dvaput unesite lozinku za [napredno podešavanje](#) kada vas XmlSignTool to zatraži. Vaša konfiguracijska datoteka .xml/sada je potpisana i možete je upotrijebiti za uvoz druge instance programa ESET Endpoint Antivirus programom ESET CMD upotreboom metode autorizacije lozinkom.

Potpisite izvezenu naredbu konfiguracijske datoteke:

```
xmlsigntool /version 2 c:\config\settings.xml
```



```
C:\XmlSignTool>xmlsigntool /version 1 c:\config\settings.xml
Enter Advanced Setup Password:
Re-enter Password:
C:\XmlSignTool>_
```

Ako se vaša lozinka za [podešavanje pristupa](#) promijeni i želite uvesti konfiguraciju koja je ranije potpisana starijom lozinkom, morate ponovno potpisati konfiguracijsku datoteku .xml svojom trenutačnom lozinkom. To vam omogućuje upotrebu starije konfiguracijske datoteke bez potrebe da je izvozite na drugi uređaj s programom ESET Endpoint Antivirus prije uvoza.

**⚠️** Ne preporučuje se aktiviranje programa ESET CMD bez autorizacije jer će se time omogućiti uvoz svih nepotpisanih konfiguracija. Postavite lozinku pod **Napredno podešavanje > Korisničko sučelje > Podešavanje pristupa** da biste spriječili korisnike da provode neovlaštene izmjene.

## Popis JSON naredbi

Pojedinačne sigurnosne funkcije mogu se aktivirati i privremeno deaktivirati pomoću naredbe za pokretanje ESET PROTECT zadatka klijenta. Naredbe neće nadjačati postavke pravila i sve pauzirane postavke vratit će se u izvorno stanje nakon izvršenja naredbe ili ponovnog pokretanja uređaja. Da biste iskoristili ovu funkciju, naredbeni redak koji će se izvršiti navedite u polju istog naziva.

Pregledajte popis naredbi za svaku sigurnosnu funkciju u nastavku:

Sigurnosna funkcija	Naredba za privremenu pauzu	Naredba za aktivaciju
rezidentna zaštita	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Zaštita dokumenata	ecmd /setfeature document pause	ecmd /setfeature document enable
Kontrola uređaja	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Način rada za prezentacije	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable

Sigurnosna funkcija	Naredba za privremenu pauzu	Naredba za aktivaciju
Tehnologija Anti-Stealth	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Osobni firewall	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Zaštita od mrežnog napada (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Zaštita od botneta	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Kontrola weba	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
zaštita web pristupa	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
zaštita klijenta e-pošte	ecmd /setfeature email pause	ecmd /setfeature email enable
Antispam zaštita	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Anti-phishing zaštita	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

## Otkrivanje stanja mirovanja

Postavke otkrivanja stanja mirovanja mogu se konfigurirati u **Naprednom podešavanju** pod stavkom **Modul detekcije > Skeniranje zlonamjernih programa > Skeniranje u stanju mirovanja > Otkrivanje stanja mirovanja**. Ove postavke određuju pokretač za [Skeniranje u stanju mirovanja](#) kada:

- radi čuvar zaslona,
- je računalo zaključano,
- se korisnik odjavio.

Pomoću gornjih potvrđnih okvira za svako stanje aktivirajte ili deaktivirajte različite pokretače otkrivanja stanja mirovanja.

## Uvoz i izvoz postavki

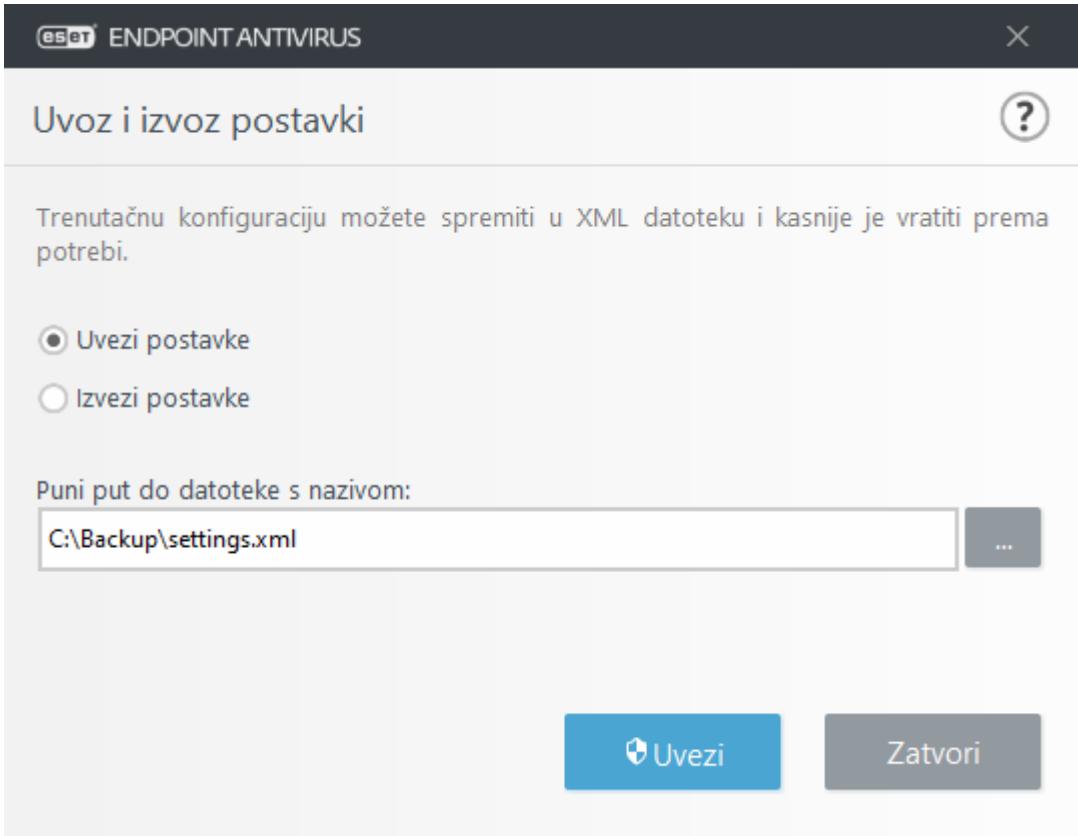
Možete uvesti ili izvesti svoju prilagođenu ESET Endpoint Antivirus .xml konfiguracijsku datoteku na izborniku **Podešavanje**.

Uvoz i izvoz konfiguracijskih datoteka korisni su ako trebate izraditi sigurnosnu kopiju trenutne konfiguracije programa ESET Endpoint Antivirus da biste je mogli koristiti kasnije. Mogućnost izvoza postavki praktična je i za korisnike koji žele koristiti svoju preferiranu konfiguraciju na više sustava – oni mogu jednostavno uvesti .xml datoteku za prijenos tih postavki.

Uvoz konfiguracije je vrlo jednostavan. U glavnom programskom prozoru kliknite **Podešavanje > Uvoz ili izvoz postavki**, a zatim odaberite opciju **Uvezi postavke**. Unesite naziv datoteke konfiguracijske datoteke ili kliknite gumb ... da biste pronašli konfiguracijsku datoteku koju želite uvesti.

Koraci za izvoz konfiguracije vrlo su slični. U glavnom programskom prozoru kliknite **Podešavanje > Uvoz ili izvoz postavki**. Odaberite mogućnost **Izvezi postavke** i unesite naziv datoteke konfiguracijske datoteke (npr. *izvoz.xml*). Koristite preglednik da biste odabrali mjesto na računalu gdje želite spremiti konfiguracijsku datoteku.

**i** Tijekom izvoza postavki može se pojaviti pogreška ako nemate dostatna prava za pisanje izvezene datoteke u navedeni direktorij.



## Vrati sve postavke na standardne

Kliknite **Standardno** u prozoru Napredno podešavanje (F5) kako biste vratili sve postavke programa za sve module. Ponovo će se postaviti na status koji bi imale nakon nove instalacije.

Također pogledajte [Uvoz i izvoz postavki](#).

## Želite li vratiti sve postavke u ovom odjeljku

Kliknite zakriviljenu strelicu da biste vratili sve postavke u trenutačnom odjeljku za standardne postavke koje određuje ESET.

Imajte na umu, sve promjene koje ste učinili izgubit će se nakon što kliknete **Vrati na standardne postavke**.

**Vrati sadržaj tablica** – Kad je aktivirano, sva pravila, zadaci ili profili dodani u tablice, bilo ručno ili automatski, bit će izgubljeni.

Također pogledajte [Uvoz i izvoz postavki](#).

## Pogreška prilikom spremanja konfiguracije

Ta poruka o pogrešci znači da postavke nisu ispravno spremljene jer je došlo do pogreške.

To obično znači da korisnik koji je pokušao promijeniti parametre programa:

- nema dovoljna prava pristupa ili nema ovlasti operacijskog sustava koje su potrebne za promjenu datoteka

konfiguracije i registra sustava.

> Za izvođenje željenih izmjena mora se prijaviti administrator sustava.

- nedavno je aktivirao način rada za učenje u HIPS-u ili firewallu i pokušao izvršiti promjene u naprednom podešavanju.

- Da biste spremili konfiguraciju i izbjegli konflikt konfiguracije, zatvorite Napredno podešavanje bez spremanja i pokušajte ponovno izvršiti željene promjene.

Drugi je najčešći slučaj taj da program više ne radi ispravno, oštećen je i potrebno ga je reinstalirati.

## Daljinsko praćenje i upravljanje

Daljinsko praćenje i upravljanje (RMM) proces je nadgledanja i kontrole softverskih sustava koji upotrebljava lokalno instaliranog agenta kojemu može pristupiti davatelj usluga upravljanja.

### ERMM – ESET-ov dodatak za RMM

- Standardna instalacija programa ESET Endpoint Antivirus sadrži datoteku `ermm.exe` koja se nalazi u Endpoint aplikaciji u sljedećoj mapi:

*C:\Program Files\ESET\ESET Security\ermm.exe*

- `ermm.exe` je naredbeni redak za uslužni program kojemu je cilj olakšati upravljanje sigurnosnim programima i komunikaciju s bilo kojim RMM dodatkom.
- `ermm.exe` razmjenjuje podatke s RMM dodatkom, koji komunicira s RMM agentom povezanim na RMM server. Alat ESET RMM deaktiviran je prema standardnim postavkama.

### Dodatni resursi

- [ERMM naredbeni redak](#)
- [Popis ERMM JSON naredbi](#)
- [Kako aktivirati daljinsko praćenje i upravljanje ESET Endpoint Antivirus](#)

### Dodaci ESET Direct Endpoint Management za RMM rješenja trećih strana

RMM server pokrenut je kao usluga na serveru treće strane. Više informacija potražite u sljedećim online korisničkim vodičima za ESET Direct Endpoint Management:

- Dodatak [ESET Direct Endpoint Management za ConnectWise Automate](#)
- Dodatak [ESET Direct Endpoint Management za Datto RMM](#)
- [ESET Direct Endpoint Management za Solarwinds N-Central](#)
- [ESET Direct Endpoint Management za NinjaRMM](#)

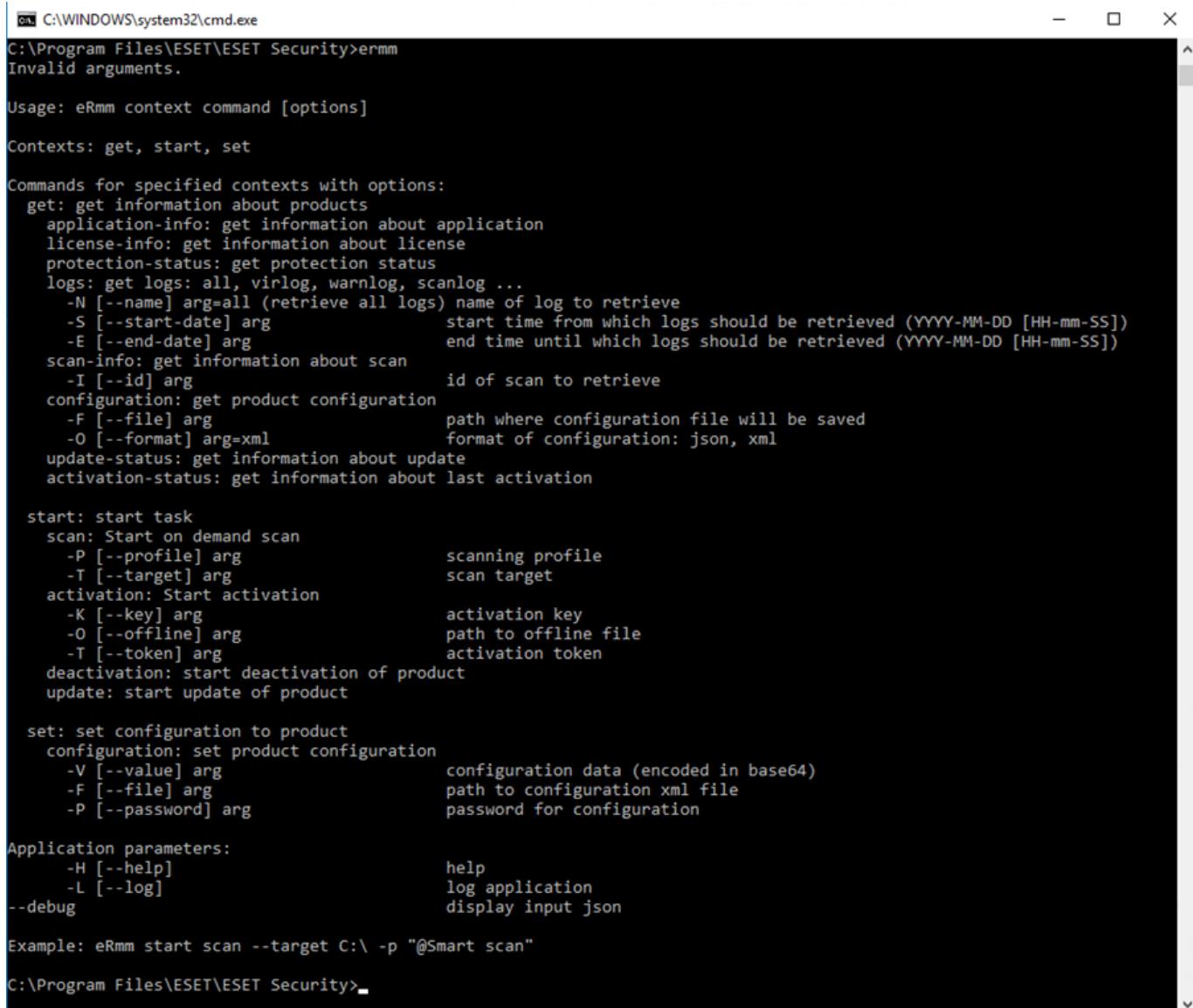
# ERMM naredbeni redak

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\ESET\ESET Security>ermm
Invalid arguments.

Usage: eRmm context command [options]

Contexts: get, start, set

Commands for specified contexts with options:
get: get information about products
    application-info: get information about application
    license-info: get information about license
    protection-status: get protection status
    logs: get logs: all, virlog, warnlog, scanlog ...
        -N [--name] arg=all (retrieve all logs) name of log to retrieve
        -S [--start-date] arg                         start time from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
        -E [--end-date] arg                           end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
    scan-info: get information about scan
        -I [--id] arg                                id of scan to retrieve
configuration: get product configuration
    -F [--file] arg                               path where configuration file will be saved
    -O [--format] arg                            format of configuration: json, xml
update-status: get information about update
activation-status: get information about last activation

start: start task
    scan: Start on demand scan
        -P [--profile] arg                      scanning profile
        -T [--target] arg                        scan target
    activation: Start activation
        -K [--key] arg                          activation key
        -O [--offline] arg                     path to offline file
        -T [--token] arg                       activation token
    deactivation: start deactivation of product
    update: start update of product

set: set configuration to product
    configuration: set product configuration
        -V [--value] arg                      configuration data (encoded in base64)
        -F [--file] arg                        path to configuration xml file
        -P [--password] arg                   password for configuration

Application parameters:
    -H [--help]                                help
    -L [--log]                                  log application
--debug                                     display input json

Example: eRmm start scan --target C:\ -p "@Smart scan"
C:\Program Files\ESET\ESET Security>
```

ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		<b>Get information about products</b>
	<a href="#">aplikacija-informacije</a>	Get information about product
	<a href="#">licenca-informacije</a>	Get information about license
	<a href="#">zaštita-status</a>	Get protection status
	<a href="#">dnevnići</a>	Get logs
	<a href="#">skeniranje-informacije</a>	Get information about running scan
	<a href="#">konfiguracija</a>	Get product configuration
	<a href="#">nadogradnja-status</a>	Get information about update
	<a href="#">aktivacija-status</a>	Get information about last activation
start		<b>Start task</b>
	<a href="#">skeniraj</a>	Start on demand scan
	<a href="#">aktivacija</a>	Start activation of product
	<a href="#">deaktivacija</a>	Start deactivation of product
	<a href="#">nadogradnja</a>	Start update of product
set		<b>Set options for product</b>
	<a href="#">konfiguracija</a>	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

## Popis ERMM JSON naredbi

- [nabavi zaštitu-status](#)
- [nabavi aplikaciju-informacije](#)
- [nabavi licencu-informacije](#)
- [nabavi dnevnike](#)
- [nabavi aktivaciju-status](#)

- [nabavi skeniranje-informacije](#)
- [nabavi konfiguraciju](#)
- [preuzmi nadogradnju-status](#)
- [pokreni skeniranje](#)
- [pokreni aktivaciju](#)
- [pokreni deaktivaciju](#)
- [pokreni nadogradnju](#)
- [postavi konfiguraciju](#)

## get protection-status

**Get the list of application statuses and the global application status**

### Command line

```
ermm.exe get protection-status
```

### Parameters

**None**

### Example

<b>call</b>
{ "command": "get_protection_status", "id": 1, "version": "1" }

<b>result</b>
{ "id": 1, "result": { "statuses": [ { "id": "EkrnNotActivated", "status": 2, "priority": 768, "description": "Product not activated" }], "status": 2, "description": "Security alert" }, "error": null }

# get application-info

Get information about the installed application

## Command line

```
ermm.exe get application-info
```

## Parameters

None

## Example

```
call
{
  "command": "get_application_info",
  "id": 1,
  "version": "1"
}
```

```
result
```

```
{  
  "id":1,  
  "result":{  
    "description":"ESET Endpoint Antivirus",  
    "version":"6.6.2018.0",  
    "product":"eea",  
    "lang_id":1033,  
    "modules":[{  
      "id":"SCANNER32",  
      "description":"Detection engine",  
      "version":"15117",  
      "date":"2017-03-20"  
    }, {  
      "id":"PEGASUS32",  
      "description":"Rapid Response module",  
      "version":"0734",  
      "date":"2017-03-20"  
    }, {  
      "id":"LOADER32",  
      "description":"Update module",  
      "version":"1009",  
      "date":"2016-12-05"  
    }, {  
      "id":"PERSEUS32",  
      "description":"Antivirus and antispyware scanner module",  
      "version":"1513",  
      "date":"2017-03-06"  
    }, {  
      "id":"ADVHEUR32",  
      "description":"Advanced heuristics module",  
      "version":"1176",  
      "date":"2017-01-16"  
    }, {  
      "id":"ARCHIVER32",  
      "description":"Archive support module",  
      "version":"1261",  
      "date":"2017-02-22"  
    }, {  
      "id":"CLEANER32",  
      "description":"Cleaner module",  
      "version":"1132",  
      "date":"2017-03-15"  
    }, {  
      "id":"ANTISTEALTH32",  
      "description":"Anti-Stealth support module",  
      "version":"1106",  
      "date":"2016-10-17"  
    }, {  
      "id":"SYSTEMSTATUS32",  
      "description":"ESET SysInspector module",  
      "version":"1266",  
      "date":"2016-12-22"  
    }, {  
      "id":"TRANSLATOR32",  
      "description":"Translation support module",  
      "version":"1588B",  
      "date":"2017-03-01"  
    }, {  
      "id":"HIPS32",  
      "description":"HIPS support module",  
      "version":"1267",  
      "date":"2017-02-16"  
    }, {  
      "id":"PROTOSCAN32",  
      "description":"Internet protection module",  
      "version":"1300",  
      "date":"2017-03-03"  
    }, {  
      "id":"DBLITE32",  
      "description":"Database module",  
      "version":"1088",  
      "date":"2017-01-05"  
    }, {  
      "id":"CONFENG32",  
      "description":"Configuration module (33)",  
      "version":"1496B",  
      "date":"2017-03-17"  
    }, {  
      "id":"IRIS32",  
      "description":"LiveGrid communication module",  
      "version":"1022",  
      "date":"2016-04-01"  
    }, {  
      "id":"SAURON32",  
      "description":"Rootkit detection and cleaning module",  
      "version":"1006",  
      "date":"2016-07-15"  
    }, {  
      "id":"SSL32",  
      "description":"Cryptographic protocol support module",  
      "version":"1009",  
      "date":"2016-12-02"  
    }  
  },  
  "error":null  
}
```

# get license-info

Get information about the license of the product

## Command line

```
ermm.exe get license-info
```

## Parameters

None

## Example

<b>call</b>
{ "command": "get_license_info", "id": 1, "version": "1" }

<b>result</b>
{ "id": 1, "result": { "type": "NFR", "expiration_date": "2020-12-31", "expiration_state": "ok", "public_id": "3XX-7ED-7XF", "seat_id": "6f726793-ae95-4e04-8ac3-e6a20bc620bf", "seat_name": "M" }, "error": null }

# get logs

Get logs of the product

## Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

## Parameters

Name	Value
<b>name</b>	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
<b>start-date</b>	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
<b>end-date</b>	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

## Example

```
call
{
  "command": "get_logs",
  "id": 1,
  "version": "1",
  "params": {
    "name": "warnlog",
    "start_date": "2017-04-04 06-00-00",
    "end_date": "2017-04-04 12-00-00"
  }
}

result
{
  "id": 1,
  "result": {
    "warnlog": {
      "display_name": "Events",
      "logs": [
        {
          "Time": "2017-04-04 06-05-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15198 (20170404).",
          "UserData": ""
        },
        {
          "Time": "2017-04-04 11-12-59",
          "Severity": "Info",
          "PluginId": "ESET Kernel",
          "Code": "Malware database was successfully updated to version 15199 (20170404).",
          "UserData": ""
        }
      ]
    }
  },
  "error": null
}
```

## get activation-status

Get information about the last activation. Result of status can be {

```
success, error }
```

## Command line

```
ermm.exe get activation-status
```

## Parameters

### None

## Example

call	
{	
"command": "get_activation_status",	
"id": 1,	
"version": "1"	
}	

result	
{	
"id": 1,	
"result": {	
"status": "success"	
},	
"error": null	
}	

## get scan-info

Get information about running scan.

## Command line

```
ermm.exe get scan-info
```

## Parameters

### None

## Example

call	
{	
"command": "get_scan_info",	
"id": 1,	
"version": "1"	
}	

```

result
{
  "id":1,
  "result": {
    "scan-info": {
      "scans": [
        {
          "scan_id":65536,
          "timestamp":272,
          "state": "finished",
          "pause_scheduled_allowed":false,
          "pause_time_remain":0,
          "start_time": "2017-06-20T12:20:33Z",
          "elapsed_tickcount":328,
          "exit_code":0,
          "progress_filename": "Operating memory",
          "progress_arch_filename": "",
          "total_object_count":268,
          "infected_object_count":0,
          "cleaned_object_count":0,
          "log_timestamp":268,
          "log_count":0,
          "log_path": "C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
          "username": "test-PC\\test",
          "process_id":3616,
          "thread_id":3992,
          "task_type":2
        }
      ],
      "pause_scheduled_active":false
    }
  },
  "error":null
}

```

## get configuration

**Get the product configuration. Result of status may be { success, error }**

### Command line

```
ermmm.exe get configuration --file C:\\tmp\\conf.xml --format xml
```

### Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

### Example

call
------

```
{  
  "command": "get_configuration",  
  "id": 1,  
  "version": "1",  
  "params": {  
    "format": "xml",  
    "file": "C:\\tmp\\conf.xml"  
  }  
}
```

#### result

```
{  
  "id": 1,  
  "result": {  
    "configuration": "PD94bWwgdmVyc2lvbj0iMS4w=="  
  },  
  "error": null  
}
```

## get update-status

**Get information about the update. Result of status may be { success, error }**

### Command line

```
ermm.exe get update-status
```

### Parameters

#### None

### Example

#### call

```
{  
  "command": "get_update_status",  
  "id": 1,  
  "version": "1"  
}
```

#### result

```
{  
  "id": 1,  
  "result": {  
    "last_update_time": "2017-06-20 13-21-37",  
    "last_update_result": "error",  
    "last_successful_update_time": "2017-06-20 11-21-45"  
  },  
  "error": null  
}
```

# start scan

## Start scan with the product

### Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

### Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

### Example

```
call
{
  "command": "start_scan",
  "id": 1,
  "version": "1",
  "params": {
    "profile": "Smart scan",
    "target": "c:\\\"
  }
}
```

```
result
{
  "id": 1,
  "result": {
    "task_id": 458752
  },
  "error": null
}
```

# start activation

## Start activation of product

### Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

### Parameters

Name	Value

key	Activation key
offline	Path to offline file

## Example

<b>call</b>	
{ "command": "start_activation" "id": 1, "version": "1", "params": { "key": "XXXX-XXXX-XXXX-XXXX-XXXX" } }	

<b>result</b>	
{ "id": 1, "result": {} , "error": null }	

## start deactivation

Start deactivation of the product

### Command line

ermm.exe start deactivation

### Parameters

### None

## Example

<b>call</b>	
{ "command": "start_deactivation", "id": 1, "version": "1" }	

<b>result</b>	
{ "id": 1, "result": {} , "error": null }	

## start update

**Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned**

### Command line

```
ermm.exe start update
```

### Parameters

**None**

### Example

call	<pre>{   "command": "start_update",   "id": 1,   "version": "1" }</pre>
result	<pre>{   "id": 1,   "result": {   },   "error": {     "id": 4,     "text": "Task already running."   } }</pre>

## set configuration

Set configuration to the product. Result of status may be { success, error }

### Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

### Parameters

Name	Value
file	the path where the configuration file will be saved

password	password for configuration
value	configuration data from the argument (encoded in base64)

## Example

<b>call</b>	<pre>{ "command": "set_configuration", "id": 1, "version": "1", "params": { "format": "xml", "file": "C:\\tmp\\conf.xml", "password": "pass" } }</pre>
<b>result</b>	<pre>{ "id": 1, "result": {}, "error": null }</pre>

## Najčešća pitanja

Ovo poglavlje bavi se najčešćim pitanjima i problemima s kojima se možete susresti. Kliknite naslov teme da biste saznali rješenje problema:

- [Aktualizacija programa ESET Endpoint Antivirus](#)
- [Aktivacija programa ESET Endpoint Antivirus](#)
- [Korištenje trenutačnih podataka za aktivaciju novog proizvoda.](#)
- [Uklanjanje virusa s računala](#)
- [Stvaranje novog zadatka u Planeru](#)
- [Zakazivanje tjednog skeniranja računala](#)
- [Povezivanje proizvoda s programom ESET Security Management Center](#)
  - [Korištenje načina nadjačavanja](#)
  - [Primjena preporučenog pravila za program ESET Endpoint Antivirus](#)
- [Konfiguriranje mirrora](#)
- [Kako nadograditi na Windows 10 s proizvodom ESET Endpoint Antivirus](#)
- [Kako aktivirati daljinsko praćenje i upravljanje](#)
- [Kako blokirati preuzimanje specifičnih vrsti datoteka s interneta](#)

- [Kako minimizirati korisničko sučelje programa ESET Endpoint Antivirus](#)

Ako vaš problem nije naveden na gornjim stranicama pomoći, pokušajte tražiti ključnu riječ ili pojam koji opisuje vaš problem te pretražite stranice pomoći za program ESET Endpoint Antivirus.

Ako ne pronađete rješenje za svoj problem/odgovor na pitanje na stranicama pomoći, posjetite [ESET-ovu bazu znanja](#) u kojoj su dostupni odgovori na najčešća pitanja i rješenja za najčešće probleme.

- [Najbolje prakse za zaštitu od zlonamjernog programa poznatog kao filecoder \(ransomware\)](#)
- [Najčešća pitanja za ESET Endpoint Security i ESET Endpoint Antivirus](#)
- [Koje adrese i portovi moraju biti otvoreni u firewallu treće strane da bi proizvod tvrtke ESET bio u potpunosti funkcionalan?](#)

Ako želite, svoje pitanje ili problem možete uputiti našoj korisničkoj službi. Veza na web obrazac za kontakt nalazi se u oknu **Pomoć i podrška** u glavnom programskom prozoru.

## Aktualizacija programa ESET Endpoint Antivirus

Program ESET Endpoint Antivirus može se nadograditi ručno ili automatski. Da biste pokrenuli nadogradnju, kliknite **Nadogradi** u glavnom prozoru programa i zatim kliknite **Potraži nadogradnje**.

Standardnom se instalacijom stvara automatski zadatak nadogradnje koji se izvršava svakog sata. Ako želite promjeniti interval, idite na stavku **Alati > Planer** (pogledajte [dodatne informacije o planeru](#)).

## Aktivacija programa ESET Endpoint Antivirus

Po završetku instalacije od vas će se zatražiti da aktivirate proizvod.

Program možete aktivirati na nekoliko načina. Dostupnost određenog scenarija aktivacije u prozoru aktivacije ovisi o zemlji i načinu distribucije instalacijske datoteke (ESET-ova stranica, vrsta instalacijskog programa .msi ili .exe itd.).

Da biste aktivirali svoj primjerak programa ESET Endpoint Antivirus izravno iz programa, otvorite glavni prozor programa ESET Endpoint Antivirus i u glavnom izborniku kliknite **Pomoć i podrška > Aktiviraj program** ili **Status zaštite > Aktiviraj program**.

Možete koristiti bilo koji od sljedećih način za aktivaciju ESET Endpoint Antivirus:

- **Unesite kupljeni licenčni ključ** – Jedinstveni niz formata XXXX-XXXX-XXXX-XXXX-XXXX koji se koristi za identifikaciju vlasnika licence i za aktivaciju licence.
- **ESET Business Account** – Račun stvoren na portalu [ESET Business Account](#) s korisničkim podacima (adresa e-pošte + lozinka). Ovaj način omogućuje vam upravljanje većim brojem licenci s jedne lokacije.
- **Izvanmrežna licenca** – Automatski stvorena datoteka koja će se prenijeti u ESET-ov program kako bi pružila informacije o licenci. Ako licenca omogućuje preuzimanje datoteke izvanmrežne licence (.lf), ta datoteka može se upotrijebiti za izvanmrežnu aktivaciju. Broj izvanmrežnih licenci bit će oduzet od ukupnog broja dostupnih licenci. Dodatne informacije o stvaranju izvanmrežne datoteke potražite u [online korisničkom priručniku za ESET Business Account](#).

Kliknite mogućnost **Aktiviraj kasnije** ako je vaše računalo član upravljane mreže i ako će vaš administrator obaviti daljinsku aktivaciju putem sučelja ESET Security Management Center. Tu mogućnost možete upotrijebiti i ako klijenta želite aktivirati kasnije.

Ako imate korisničko ime i lozinku za aktivaciju starijih ESET programa i ne znate kako aktivirati program ESET Endpoint Antivirus, [pretvorite svoje naslijedene korisničke podatke u licenčni ključ](#).

#### [Aktivacija programa nije uspjela?](#)

Licencu programa možete promijeniti u svakom trenutku. Samo kliknite **Pomoć i podrška > Promjeni licencu** u glavnom programskom prozoru. Prikazat će se javni ID licence koji se upotrebljava za identifikaciju vaše licence kod korisničke podrške tvrtke ESET. Korisničko ime pod kojim je vaše računalo registrirano pohranjeno je u odjelu **O programu**, koji možete prikazati desnim klikom na ikonu trake sustava .

 ESET Security Management Center 7.2 ili ESET PROTECT 8.0 može neprimjetno aktivirati klijentska računala koristeći se licencama koje je omogućio administrator. Upute za to potražite u odjelu [Mrežna pomoć za ESET PROTECT](#).

## Unos Lisenčnog ključa prilikom aktivacije

Automatske nadogradnje važne su za vašu sigurnost. ESET Endpoint Antivirus primit će nadogradnje koje su aktivirane **licenčnim ključem**.

Ako nakon instalacije niste unijeli licenčni ključ, program se neće aktivirati. Možete promijeniti licencu u glavnom prozoru programa. Da biste to učinili, kliknite **Pomoć i podrška > Aktiviraj licencu** i unesite podatke licence koje ste primili sa sigurnosnim programom tvrtke ESET u prozor Aktivacije programa.

Prilikom unosa **Lisenčnog ključa** važno je upisati ga točno onako kako piše:

- Lisenčni ključ jedinstveni je niz u formatu XXXX-XXXX-XXXX-XXXX-XXXX koji se koristi za identifikaciju vlasnika licence i aktivaciju licence.

Radi točnosti, preporučujemo da lisenčni ključ kopirate i zaliđepite iz e-pošte koju ste dobili prilikom registracije.

## Prijava u ESET Business Account korisnički račun

Račun sigurnosnog administratora je račun stvoren na portalu ESET Business Account s vašom **adresom e-pošte** i **lozinkom** koji može vidjeti sve računalne autorizacije. Račun sigurnosnog administratora omogućuje vam upravljanje većim brojem licenci. Ako nemate račun sigurnosnog administratora, kliknite **Stvorи račun** i bit ćete preusmjereni na portal ESET Business Account gdje se možete registrirati sa svojim korisničkim podacima.

Ako ste zaboravili svoju lozinku, kliknite **Zaboravio/la sam lozinku** i bit ćete preusmjereni na portal ESET Business Account. Unesite adresu e-pošte i kliknite **Prijava** da biste potvrdili. Nakon toga poslat ćemo vam poruku s uputama za ponovno postavljanje lozinke.

# Upotreba podataka o staroj licenci za aktivaciju novijeg ESET-ova sigurnosnog programa

Ako već imate korisničko ime i lozinku i želite ključ licence, posjetite [ESET Business Account portal tvrtke ESET za administriranje licenci](#) gdje svoje podatke možete pretvoriti u novi ključ licence.

## Uklanjanje virusa s računala

Ako računalo pokazuje simptome zaraze zlonamjernim softverom, npr. sporije radi ili se često "zamrzava", preporučujemo sljedeće:

1. U glavnom prozoru programa kliknite **Skeniranje računala**.
2. Kliknite **Smart skeniranje** da biste pokrenuli skeniranje sustava.
3. Nakon završetka skeniranja u dnevniku pogledajte koliko je skeniranih, zaraženih i očišćenih datoteka.
4. Ako želite skenirati samo određeni dio diska, odaberite **Prilagođeno skeniranje** te zatim ciljeve u kojima će se tražiti virusi.

Dodatne informacije možete pronaći u ovom redovito ažuriranom [članku ESET-ove baze znanja](#).

## Stvaranje novog zadatka u Planeru

Da biste stvorili novi zadatak u odjeljku **Alati > Planer**, kliknite **Dodaj zadatak** ili kliknite desnom tipkom miša i odaberite **Dodaj** na kontekstnom izborniku. Na raspolaganju je sedam vrsta planiranih zadataka:

- **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
- **Održavanje dnevnika** – Dnevniči sadrže i zaostatke već izbrisanih zapisa. Taj zadatak redovito optimizira zapise u dnevnicima radi učinkovitijeg rada.
- **Provjera datoteke za pokretanje sustava** – Provjerava datoteke kojima je dopušteno pokretanje prilikom pokretanja sustava ili prijave.
- **Stvori snimku statusa računala** – Stvara snimku računala pomoću programa ESET SysInspector – prikuplja detaljne informacije o komponentama sustava (primjerice upravljačkim programima, aplikacijama) i procjenjuje razinu rizika za svaku komponentu.
- **Skeniranje računala na zahtjev** – Izvodi skeniranje datoteka i mapa na računalu.
- **Aktualizacija** – Planira zadatak aktualizacije aktualizacijom modula.

Budući da je **Aktualizacija** jedan od najčešće korištenih planiranih zadataka, u nastavku slijedi objašnjenje kako dodati novi zadatak aktualizacije:

S padajućeg izbornika **Planirani zadatak** odaberite **Aktualizacija**. Unesite naziv zadatka u polje **Naziv zadatka** i kliknite **Dalje**. Odaberite učestalost zadatka. Na raspolaganju su sljedeće mogućnosti: **Jednom**, **Opetovano**,

**Svakodnevno, Tjedno i Pri događaju.** Odaberite mogućnost Nemoj izvršavati zadatak ako računalo koristi bateriju da biste minimizirali korištenje sistemskih resursa dok prijenosno računalo koristi bateriju. Zadatak će se izvršiti na datum i vrijeme zadani u poljima **Izvršavanje zadatka**. Zatim definirajte akciju koju treba poduzeti ako se zadatak ne može izvršiti ili dovršiti u zakazano vrijeme. Na raspolaganju su sljedeće mogućnosti:

- U sljedećem zakazanom terminu
- Što prije
- Odmah, ako vrijeme proteklo od zadnjeg izvršavanja premašuje određenu vrijednost (interval se može definirati putem okvira za listanje Vrijeme od zadnjeg izvršavanja).

U sljedećem koraku prikazuje se prozor sažetaka informacija o trenutno planiranom zadatku. Kliknite **Završetak** kada završite s unošenjem promjena.

Pojavit će se dijaloški okvir gdje korisnik može izabrati profile koji će se koristiti za planirani zadatak. Tu možete postaviti primarni i alternativni profil. Alternativni profil koristi se u slučaju da zadatak nije moguće dovršiti pomoću primarnog profila. Potvrdite klikom na **Završetak**, čime se novi planirani zadatak dodaje na popis trenutno planiranih zadataka.

## Zakazivanje tjednog skeniranja računala

Da biste zakazali redoviti zadatak, otvorite glavni prozor programa i kliknite **Alati > Planer**. U nastavku se nalaze kratke upute o zakazivanju zadatka koji će skenirati lokalne pogone svakog tjedna. Dodatne upute potražite u našem [članku iz baze znanja](#).

Da biste zakazali zadatak skeniranja:

1. Na glavnom zaslonu Planera kliknite **Dodaj**.
2. S padajućeg izbornika odaberite **Skeniranje računala na zahtjev**.
3. Upišite naziv zadatka pa odaberite mogućnost **Tjedno za učestalost zadatka**.
4. Odaberite vrijeme i dan za izvršenje zadatka.
5. Odaberite **Izvrši zadatak čim to bude moguće** za kasnije izvršenje zadatka u slučaju da se zakazani zadatak iz nekog razloga ne izvrši (primjerice, računalo je bilo isključeno).
6. Pregledajte sažetak planiranog zadatka pa kliknite **Završetak**.
7. S padajućeg izbornika **Ciljevi** odaberite **Lokalni pogoni**.
8. Kliknite **Završetak** da biste primijenili zadatak.

## Povezivanje programa ESET Endpoint Antivirus s alatom

# ESET PROTECT

Ako je na računalu instaliran program ESET Endpoint Antivirus i želite se povezati putem programa ESET PROTECT, provjerite je li i na klijentskoj radnoj stanici instaliran ESET Management Agent. To je ključan dio svakog klijentskog rješenja koje komunicira s ESMC serverom.

- [Instalirajte ESET Management Agent na klijentske radne stanice](#)

Pogledajte i:

- [Dokumentacija za daljinski upravljanje krajnje točke](#)
- [Korištenje načina nadjačavanja](#)
- [Primjena preporučenog pravila za program ESET Endpoint Antivirus](#)

## Korištenje načina nadjačavanja

Korisnici koji na uređaju imaju ESET-ove Endpoint programe (verzija 6.5 i novije) za Windows mogu se koristiti funkcijom nadjačavanja. Način nadjačavanja omogućuje korisnicima na razini klijentskog računala da promijene postavke instaliranog ESET-ovog programa, čak i ako se na te postavke primjenjuje pravilo. Način nadjačavanja može se aktivirati za određene AD korisnike ili može biti zaštićen lozinkom. Funkcija ne može biti aktivirana dulje od četiri uzastopna sata.

- Nakon aktivacije načina nadjačavanja, ne možete ga zaustaviti iz ESMC web konzole. Način nadjačavanja deaktivirat će se automatski nakon isteka razdoblja nadjačavanja. Moguće ga je isključiti i na klijentskom računalu.
- ⚠ • Korisnik koji upotrebljava način nadjačavanja također mora imati administratorska prava za Windows. U suprotnome korisnik ne može spremiti promjene u postavkama programa ESET Endpoint Antivirus.
- Grupna autentikacija aktivne mape podržana je za verziju 7.0.2100.4 programa ESET Endpoint Antivirus ili noviju verziju.

Da biste postavili **način nadjačavanja**:

1. Idite na **Pravila > Novo pravilo.**
2. U odjeljku **Osnovno** upišite **naziv** i **opis** pravila.
3. U odjeljku **Postavke** odaberite **ESET Endpoint za Windows**.
4. Kliknite na opciju **Način nadjačavanja** i konfigurirajte pravila za način nadjačavanja.
5. U odjeljku **Dodijeli** odaberite računalo ili skupinu računala na koja će se pravilo primjenjivati.
6. Pregledajte postavke u odjeljku **Sažetak** i kliknite **Završi** da biste primijenili pravilo.

The screenshot shows the ESET Security Management Center interface for creating a new policy. The 'Basic' tab is selected on the left. In the main area, under 'ESET Endpoint for Windows', there are several configuration sections. One section, 'OVERRIDE MODE SETTINGS', is expanded and contains three sub-sections: 'TEMPORARY CONFIGURATION OVERRIDE', 'OVERWRITE CREDENTIALS', and 'OVERRIDE MODE'. Under 'TEMPORARY CONFIGURATION OVERRIDE', there are three radio buttons: 'Allow override by local admin' (selected), 'Maximum override time' (set to 4 hours), and 'Scan computer after override'. Under 'OVERWRITE CREDENTIALS', there are two radio buttons: 'Authentication type' (set to 'Active directory user') and 'Active directory user'. At the bottom of the configuration area are 'CONTINUE', 'FINISH', and 'CANCEL' buttons.

Ako *John* ima problem jer mu sigurnosne postavke blokiraju neku važnu funkciju ili pristup webu na njegovom uređaju, administrator može omogućiti korisniku *John* da nadjača postojeće sigurnosno pravilo i ručno podesi postavke na svom uređaju. ESMC nakon toga može zatražiti te nove postavke da bi administrator mogao iz njih stvoriti novo pravilo.

Da biste to učinili, slijedite ove korake:

- 1.Idite na **Pravila > Novo pravilo**.
- 2.Ispunite polja **Naziv** i **Opis**. U odjeljku **Postavke** odaberite **ESET Endpoint za Windows**.
- 3.Kliknite **Način nadjačavanja**, aktivirajte ga na sat vremena i odaberite stavku *John* kao AD korisnika.
- 4.Dodijelite pravilo *Johnovom računalu* i kliknite **Završi** da biste spremili pravilo.
- 5.*John* mora aktivirati **način nadjačavanja** u ESET-ovom sigurnosnom programu i ručno promjeniti postavke na svom uređaju.
- 6.Na ESMC web-konzoli idite do opcije **Računala**, odaberite *Johnovo računalo* i kliknite **Prikaži detalje**.
- 7.U odjeljku **Konfiguracija** kliknite **Zatraži konfiguraciju** da biste zakazali zadatak klijenta i odmah dobili konfiguraciju od klijenta.
- 8.Ubrzo će se pojaviti nova konfiguracija. Kliknite na program čije postavke želite spremiti i potom kliknite **Otvori konfiguraciju**.
- 9.Možete pregledati postavke, a zatim kliknite **Pretvori u pravilo**.
- 10.Ispunite polja **Naziv** i **Opis**.
- 11.U odjeljku **Postavke** prema potrebi možete promjeniti postavke.
- 12.U odjeljku **Dodijeli** možete dodijeliti to pravilo *Johnovom računalu* (ili drugima).
- 13.Kliknite **Završi** da biste spremili postavke.
- 14.Nemojte zaboraviti ukloniti pravilo nadjačavanja kada više ne bude potrebno.

## Primjena preporučenog pravila za program ESET Endpoint Antivirus

Nakon što povežete programe ESET Endpoint Antivirus i ESET Security Management Center, najbolja je praksa primijeniti preporučeno ili prilagođeno [pravilo](#).

Postoji nekoliko ugrađenih pravila za program ESET Endpoint Antivirus:

Pravilo	Opis
Antivirus – Uravnoteženo	Preporučena sigurnosna konfiguracija za većinu postavki.
Antivirus – maksimalna sigurnost	Iskorištava prednosti strojnog učenja, dubinskog pregleda ponašanja i filtriranja SSL protokola. Utječe na otkrivanje potencijalno nesigurnih, neželjenih i sumnjivih aplikacija.
Sustav reputacije i povratnih informacija na temelju cloud tehnologije	Aktivira sustav reputacije i povratnih informacija na temelju cloud tehnologije <a href="#">ESET LiveGrid®</a> za poboljšanje otkrivanja najnovijih prijetnji te kao pomoć u dijeljenju zločudnih ili nepoznatih potencijalnih prijetnji za daljnju analizu.
Kontrola uređaja – Maksimalna sigurnost	Svi su uređaji blokirani. Za povezivanje bilo kojeg uređaja potrebno je dopuštenje administratora.
Kontrola uređaja – Samo za čitanje	Svi se uređaji mogu samo čitati. Zapisivanje nije dopušteno.
Firewall – Blokiraj sav promet osim veze s ESMC-om i EEI-om	Blokira sav promet osim veze s programom ESET Security Management Center i <a href="#">serverom programa ESET Enterprise Inspector</a> (samo ESET Endpoint Security).
Vođenje dnevnika – Potpuno dijagnostičko zapisivanje	Ovaj predložak osigurava da će svi dnevnički biti dostupni administratoru kada mu budu potrebni. Zapisivati će sve uz minimalnu opširnost zapisivanja, uključujući HIPS i <a href="#">ThreatSense parametre</a> te firewall. Dnevnički se automatski brišu nakon 90 dana.
Vođenje dnevnika – Zapiši samo važne događaje	Ovo pravilo osigurava da će se zapisati upozorenja, pogreške i kritični događaji. Dnevnički se automatski brišu nakon 90 dana.
Vidljivost – Uravnoteženo	Standardna postavka za vidljivost. Aktivirani su statusi i obavijesti.
Vidljivost – Nevidljivi način	Deaktivirane su obavijesti, upozorenja, <a href="#">GUI</a> i integracija u kontekstni izbornik. Datoteka egui.exe neće se pokrenuti. Prikladno za upravljanje isključivo s <a href="#">ESET PROTECT Cloud</a> -e.
Vidljivost – Smanjena interakcija s korisnikom	Deaktivirani su statusi i obavijesti, GUI se prikazuje.

Slijedite korake u nastavku da biste postavili pravilo s nazivom **Antivirus – maksimalna sigurnost**, koje provodi više od 50 preporučenih postavki za program ESET Endpoint Antivirus instaliran na vašim radnim stanicama:

**i** Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:

- [Upotrijebite ESMC za primjenu preporučenog ili unaprijed definiranog pravila za program ESET Endpoint Antivirus](#)

1. Otvorite ESMC web konzolu.
2. Idite na **Pravila** i proširite stavku **Ugrađena pravila > ESET Endpoint za Windows**.
3. Kliknite **Antivirus – maksimalna sigurnost – preporučeno**.
4. Na kartici **Dodijeljeno** kliknite **Dodijeli klijente** ili **Dodijeli grupe** i odaberite odgovarajuća računala za koje želite primijeniti ovo pravilo.

Da biste vidjeli koje su postavke primjenjene za ovo pravilo, kliknite karticu **Postavke** i proširite stablo odjeljka Napredno podešavanje.

- Plava točka označava izmijenjenu postavku za ovo pravilo
- Broj u plavom okviru označava broj postavki koje je ovo pravilo promijenilo
- [Možete pročitati više o ESMC pravilima](#)

# Konfiguriranje mirrora

ESET Endpoint Antivirus može se konfigurirati da sprema kopije datoteka aktualizacije modula za otkrivanje virusa na druge radne stanice koje rade sa sustavom ESET Endpoint Security ili ESET Endpoint Antivirus.

## Konfiguriranje programa ESET Endpoint Antivirus kao mirror servera za aktualizacije putem internog HTTP servera

1. Pritisnite **F5** da biste pristupili Naprednom podešavanju i proširite stavku **Nadogradnja > Profili > Mirror za nadogradnju**.
2. Proširite **Nadogradnje** i provjerite je li aktivirana opcija **Odaberite automatski** pod stavkom **Nadogradnje modula**.
3. Proširite **Mirror za nadogradnju** i aktivirajte stavke **Stvori mirror za nadogradnju** i **Aktiviraj HTTP server**.

Više informacija potražite u odjeljku [Mirror za nadogradnju](#).

## Konfiguriranje mirror poslužitelja za aktualizacije putem zajedničke mrežne mape

1. Stvorite zajedničku mapu na lokalnom ili mrežnom uređaju. Mapa mora biti dostupna za čitanje svim korisnicima koji upotrebljavaju sigurnosna rješenja tvrtke ESET i slobodna za pisanje s lokalnog SISTEMSKOG računa.
2. Aktivirajte **Stvori mirror za nadogradnju** pod stavkom **Napredno podešavanje > Nadogradnja > Profili > Mirror za nadogradnju**.
3. Odaberite odgovarajuću **mapu za pohranu** tako da kliknete **Očisti** i zatim **Uredi**. Potražite i odaberite stvorenu zajedničku mapu.

**i** Ako ne želite pružati nadogradnje modula putem internog HTTP servera, deaktivirajte opciju **Stvori mirror za nadogradnju**.

## Kako nadograditi na Windows 10 s proizvodom ESET Endpoint Antivirus

**!** Toplo preporučujemo da nadogradite svoj ESET-ov program na posljednju verziju, a zatim preuzmete najnovije aktualizacije modula prije nadogradnje na Windows 10. To će osigurati maksimalnu zaštitu i sačuvati vaše programske postavke i licenčne informacije tijekom nadogradnje na Windows 10.

### Verzija 7.x:

Kliknite odgovarajuću vezu u nastavku za preuzimanje i instalaciju najnovije verzije kako biste se pripremili za nadogradnju na Windows 10:

[Preuzmi ESET Endpoint Security 7 32-bitni](#) [Preuzmi ESET Endpoint Antivirus 7 32-bitni](#)

[Preuzmi ESET Endpoint Security 7 64-bitni](#) [Preuzmi ESET Endpoint Antivirus 7 64-bitni](#)

## Verzija 5.x:

**!** ESET Endpoint programi verzije 5 više [nisu podržani](#). To znači da podverzije više nisu javno dostupne za preuzimanje. Preporučujemo nadogradnju na [najnoviju verziju ESET Endpoint programa](#).

## Verzije na drugim jezicima:

Ako tražite verziju ESET-ova endpoint proizvoda na nekom drugom jeziku, [posjetite našu stranicu za preuzimanje](#).

**i** [Dodatne informacije o kompatibilnosti ESET-ovih poslovnih programa sa sustavom Windows 10.](#)

## Kako aktivirati daljinsko praćenje i upravljanje

Daljinsko praćenje i upravljanje (RMM) proces je nadgledanja i kontrole softverskih sustava (poput onih na radnoj površini, serverima i mobilnim uređajima) koji upotrebljava lokalno instaliran agent kojemu može pristupiti davatelj usluga upravljanja. RMM može upravljati programom ESET Endpoint Antivirus od verzije 6.6.2028.0.

Napredno podešavanje

MODUL DETEKCIJE ②

NADOGRADNJA ②

MREŽNA ZAŠTITA

WEB I E-POŠTA ③

KONTROLA UREĐAJA ②

**ALATI** ③

Dnevnički

Proxy server ①

Obavijesti ⑪

Način rada za prezentacije

Dijagnostika ①

KORISNIČKO SUČELJE ①

+ VREMENSKO RAZDOBLJE

+ MICROSOFT WINDOWS® UPDATE

+ ESET CMD

- ESET RMM

Aktiviraj RMM

Način rada

Autorizacijska metoda

Put aplikacije

+ LICENCA

Standardno

U redu

Odustani

ESET RMM standardno je deaktiviran. Da biste aktivirali ESET RMM, pritisnite **F5** za pristup Naprednom podešavanju, kliknite **Alati**, proširite **ESET RMM** i uključite oznaku pored **Aktiviraj RMM**.

**Radni način** – odaberite **Samo sigurne operacije** ako želite aktivirati sučelje RMM za sigurne operacije i operacije

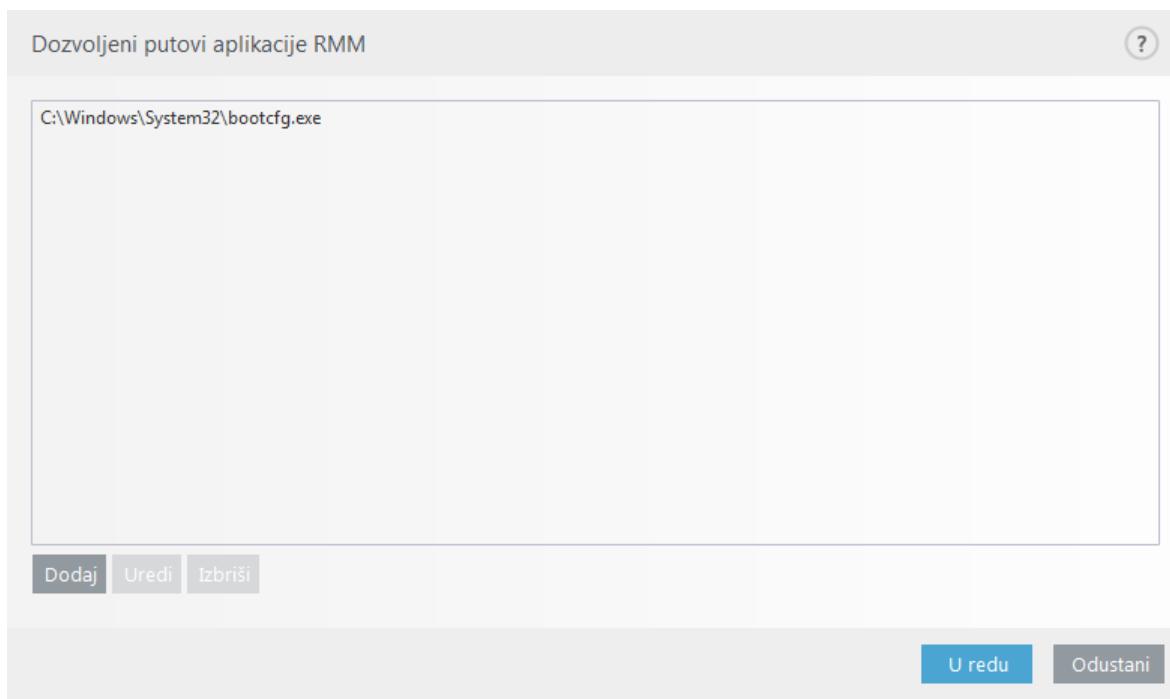
samo za čitanje. Odaberite **Sve operacije** ako želite aktivirati sučelje RMM za sve operacije.

Operacija	Način samo sigurnih operacija	Način svih operacija
Nabavi aplikaciju-informacije	✓	✓
Nabavi konfiguraciju	✓	✓
Nabavi podatke o licenci	✓	✓
Nabavi dnevнике	✓	✓
Nabavi status zaštite	✓	✓
Nabavi status nadogradnje	✓	✓
Postavi konfiguraciju		✓
Pokreni aktivaciju		✓
Pokreni skeniranje	✓	✓
Pokreni nadogradnju	✓	✓

**Način autorizacije** – Postavite način autorizacije RMM-a. Za upotrebu autorizacije odaberite **Put aplikacije** iz padajućeg izbornika, u suprotnome odaberite **Ništa**.

**!** RMM uvijek treba upotrebljavati autorizaciju kako zlonamjerni softver ne bi mogao deaktivirati ili zaobići zaštitu programom ESET Endpoint.

**Putovi aplikacije** – određena aplikacija koja smije pokrenuti RMM. Ako ste odabrali **Put aplikacije** kao način autorizacije, kliknite **Uredi** da biste otvorili konfiguracijski prozor **Dopušteni putovi aplikacije RMM**.



**Dodaj** – Stvorite novi dopušteni put aplikacije RMM. Unesite put ili kliknite gumb ... za odabir izvršne datoteke.

**Uredi** – Preinačite postojeći dopušteni put. Koristite **Uredi** ako se lokacija izvršne datoteke promijenila u drugu mapu.

**Izbriši** – Izbrišite postojeći dopušteni put.

Standardna instalacija programa ESET Endpoint Antivirus sadrži datoteku ermm.exe koja se nalazi u direktoriju Endpoint aplikacije (standardni put C:\Program Files\ESET\ESET Security). ermm.exe razmjenjuje podatke s dodatkom RMM, koji komunicira s RMM agentom, povezanim s RMM serverom.

- ermm.exe – naredbeni redak za uslužni program koji je razvio ESET, a koji omogućuje upravljanje Endpoint programima i komunikaciju s bilo kojim RMM dodatkom.
- RMM dodatak jest aplikacija treće strane koja je pokrenuta lokalno na sustavu Endpoint Windows. Dodatak je dizajniran kako bi komunicirao s određenim RMM agentom (npr. samo Kaseya) i s ermm.exe.
- RMM agent aplikacija je treće strane (npr. od Kaseye) koja je pokrenuta lokalno na sustavu Endpoint Windows. Agent komunicira s RMM dodatkom i RMM serverom.

## Kako blokirati preuzimanje specifičnih vrsti datoteka s interneta

Ako ne želite dopustiti preuzimanje određenih vrsta datoteka (npr. exe, pdf ili zip) s interneta, upotrijebite [Upravljanje URL adresama](#) s kombinacijom zamjenskih znakova. Pritisnite tipku F5 da biste pristupili odjeljku **Napredno podešavanje**. Kliknite "Web i e-pošta" > "Zaštita web pristupa" i proširite odjeljak **Upravljanje URL adresama**. Kliknite "Uredi" pored stavke "Popis adresa".

U prozoru **popisa adresa** odaberite "Popis blokiranih adresa" i kliknite "Uredi" ili "Dodaj" za stvaranje novog popisa. Otvorit će se novi prozor. Ako stvarate novi popis, odaberite "Blokirano" u padajućem izborniku "Vrsta popisa adresa" i navedite naziv popisa. Ako želite primiti obavijest prilikom pristupa nekoj vrsti datoteke s trenutačnog popisa, omogućite traku klizača "Obavijesti" prilikom primjene. Odaberite "Opširnost vođenja dnevnika" u padajućem izborniku. Remote Administrator može prikupljati zapise s **upozorenjem o opsegu**.

Uredi popis

Vrsta popisa adresa

Blokirano

Naziv popisa

Popis blokiranih adresa

Opis popisa

Aktivan popis

Obavijesti prilikom primjene

X

Minimalna opširnost zapisivanja

Informacije

Popis adresa

\*?.exe  
\*.\*.zip  
\*.\*.exe

Dodaj Uredi Izbriši Uvezi

U redu Odustani

Kliknite "Dodaj" da biste unijeli masku koja određuje vrste datoteka čije preuzimanje želite blokirati. Unesite potpunu URL adresu ako želite blokirati preuzimanje određene datoteke s određene web stranice, primjerice <http://example.com/file.exe>. Možete upotrijebiti zamjenske znakove da biste obuhvatili grupu datoteka. Upitnik (?) predstavlja jedan varijabilni znak, a zvjezdica (\*) varijabilni znakovni niz od nula ili više znakova. Primjerice, maska \*/\*.zip blokira preuzimanje svih komprimiranih datoteka.

Imajte na umu da pomoću ove metode možete blokirati preuzimanje određenih vrsta datoteka ako je ekstenzija datoteke dio URL-a datoteke. Ako web stranica upotrebljava URL-ove za preuzimanje datoteka, primjerice [www.example.com/download.php?fileid=42](http://www.example.com/download.php?fileid=42), preuzet će se bilo koja datoteka koja se nalazi na ovom linku, čak i ako ste blokirali njezinu ekstenziju.

## Kako minimizirati korisničko sučelje programa ESET Endpoint Antivirus

Prilikom daljinskog upravljanja možete primijeniti unaprijed definirano pravilo "[Vidljivost](#)".

Ako to nije moguće, izvršite korake ručno.

- Pritisnite **F5** da biste pristupili Naprednom podešavanju i proširite **Korisničko sučelje > Elementi korisničkog sučelja**.

2. Postavite opciju **Način rada za pokretanje** na željenu vrijednost. [Više informacija o načinima rada za pokretanje.](#)
3. Deaktivirajte opcije **Prikaži uvodni prozor pri pokretanju programa** i **Koristi zvučni signal**.
4. Konfigurirajte [Obavijesti](#).
5. Konfigurirajte dio [Statusi aplikacije](#).
6. Konfigurirajte dio [Poruke za potvrdu](#).
7. Konfigurirajte dio [Upozorenja i okviri s porukama](#).

## Licenčni ugovor za krajnjeg korisnika

**VAŽNO:** Prije preuzimanja, instaliranja, kopiranja ili korištenja pažljivo pročitajte uvjete i odredbe koje se primjenjuju na korištenje programa. **PREUZIMANJEM, INSTALIRANJEM, KOPIRANJEM ILI UPORABOM SOFTVERA PRIHVAĆATE OVE UVJETE I ODREDBE I POTVRĐUJETE [PRAVILA PRIVATNOSTI](#).**

### Licenčni ugovor za krajnjeg korisnika

Prema uvjetima ovog Licenčnog ugovora za krajnjeg korisnika (dalje u tekstu: „Ugovor”) sklopljenog između društva ESET, spol. s r. o., sa sjedištem na adresi Einsteinova 24, 851 01 Bratislava, Slovak Republic, registriranog u trgovackom registru Okružnog suda u Bratislavi I, odjeljak Sro, unos br. 3586/B, registracijski broj: 31333532 (dalje u tekstu: „ESET” ili „Dobavljač”) i Vas, fizičke ili pravne osobe (dalje u tekstu: „Vi, Vas, Vama” ili „Krajnji korisnik”), imate pravo upotrebljavati Softver definiran u članku 1. ovog Ugovora. Softver definiran u članku 1. ovog Ugovora može se pohraniti na nosaču podataka, poslati elektroničkom poštom, preuzeti s interneta, preuzeti s Dobavljačevih servera ili nabaviti iz nekih drugih izvora u skladu s uvjetima i odredbama navedenima u dalnjem tekstu.

ODO JE UGOVOR O PRAVIMA KRAJNJEG KORISNIKA, A NE UGOVOR O PRODAJI. Dobavljač ostaje vlasnikom kopije Softvera i fizičkog medija za pohranu koji se nalazi u prodajnom pakiranju te svih drugih kopija koje Krajnji korisnik ima pravo izraditi prema odredbama ovog Ugovora.

Klikom na gumb „Prihvaćam” ili „Prihvaćam...” tijekom instaliranja, preuzimanja, kopiranja ili upotrebe Softvera Vi izražavate suglasnost s uvjetima i odredbama ovog Ugovora. Ako se ne slažete s nekim od uvjeta ili nekom od odredbi Ugovora, odmah kliknite na opciju za odustajanje, odustanite od instalacije ili preuzimanja odnosno uništite ili vratite Softver, instalacijski medij, popratnu dokumentaciju i račun Dobavljaču ili na lokaciju na kojoj ste nabavili Softver.

SUGLASNI STE DA VAŠE KORIŠTENJE SOFTVERA ZNAČI DA STE PROČITALI OVAJ UGOVOR, DA GA RAZUMIJETE TE DA STE SUGLASNI UVJETE I ODREDBE KOJE SADRŽI SMATRATI OBVEZUJUĆIMA.

**1. Softver.** Prema načinu na koji se upotrebljava u Ugovoru pojам „Softver” znači sljedeće: (i) računalni program koji se isporučuje s ovim Ugovorom i svi njegovi dijelovi; (ii) cijelokupan sadržaj diskova, CD-ROM-ova, DVD-ova, poruka e-pošte i svih privitaka ili ostalih medija uz koje je priložen ovaj Ugovor, uključujući oblik objektnog koda Softvera isporučenog na nosaču podataka, putem elektroničke pošte ili preuzimanjem putem interneta; (iii) svi povezani pisani materijali s objašnjenjima i sva moguća dokumentacija povezana sa Softverom, iznad svega, svi opisi Softvera, njegove specifikacije, svi opisi svojstava ili rada Softvera, svi opisi radnog okruženja u kojemu se Softver upotrebljava, upute za upotrebu ili instalaciju Softvera ili bilo kakav opis načina upotrebe Softvera (u dalnjem tekstu: „Dokumentacija”); (iv) kopije Softvera, eventualne popravke pogrešaka u Softveru, dodatke i proširenja Softvera, izmijenjene verzije Softvera, moguće nadogradnje komponenti Softvera za koje Vam

Dobavljač daje licencu u skladu s člankom 3. ovog Ugovora. Softver se isporučuje isključivo u obliku izvršnog objektnog koda.

**2. Instalacija, Računalo i Licenčni ključ.** Softver isporučen na nosaču podataka, poslan elektroničkom poštom, preuzet s interneta, preuzet s Dobavljačevih servera ili nabavljen iz nekih drugih izvora potrebno je instalirati. Softver se mora instalirati na ispravno konfiguirirano Računalo koje zadovoljava preduvjete navedene u Dokumentaciji. Način instalacije opisan je u Dokumentaciji. Na Računalu na kojem instalirate Softver ne smiju biti instalirani nikakvi računalni programi ni hardver koji bi mogli negativno utjecati na Softver. Računalo znači hardver, uključujući bez ograničenja osobna računala, prijenosna računala, radne stанице, dlanovnike, pametne telefone, ručne elektroničke uređaje ili druge elektroničke uređaje za koje je osmišljen Softver i na kojima će se instalirati i/ili upotrebljavati. Licenčni ključ znači jedinstveni niz simbola, slova, brojeva ili posebnih znakova pružen Krajnjem korisniku kako bi se dopustila zakonita upotreba Softvera, njegovih verzija ili produžetak trajanja Licence u skladu s ovim Ugovorom.

**3. Licenca.** Pod uvjetom da ste suglasni s uvjetima ovog Ugovora i poštujete sve ugovorne uvjete i odredbe, Dobavljač Vam dodjeljuje sljedeća prava (dalje u tekstu: „Licenca”):

- a) **Instalacija i korištenje.** Dobavljač Vam daje neisključivo i neprenosivo pravo da instalirate Softver na tvrdi disk računala ili na neki drugi medij za trajnu pohranu podataka, da instalirate i pohranite Softver u memoriju računalnog sustava te da primjenjujete, pohranjujete i prikazujete Softver.
- b) **Odredba o broju licenci.** Pravo na korištenje Softvera povezano je s brojem Krajnjih korisnika. Smatrat će se da jedan Krajnji korisnik označava: (i) instalaciju Softvera na jednom računalnom sustavu ili (ii) ako je opseg licence povezan s brojem poštanskih pretinaca, jedan Krajnji korisnik označava računalnog korisnika koji primi elektroničku poštu putem agenta korisnika pošte (Mail User Agent, dalje u tekstu: „MUA“). Ako MUA prihvati elektroničku poštu i zatim je automatski distribuira većem broju korisnika, broj Krajnjih korisnika određuje se prema stvarnom broju korisnika kojima se distribuira ta elektronička pošta. Ako server za poštu vrši funkciju poštanskog pristupnika, broj Krajnjih korisnika bit će jednak broju korisnika servera za poštu za koje pristupnik obavlja tu funkciju. Ako se neodređen broj adresa elektroničke pošte usmjerava prema jednom korisniku i prihvaca ih jedan korisnik (primjerice putem zamjenskih naziva, alias), a klijent ne distribuira poruke automatski većem broju korisnika, potrebna je Licenca za samo jedno računalo. Jedna se Licenca istodobno smije koristiti samo na jednom računalu. Krajnji korisnik ima pravo unijeti Licenčni ključ Softvera samo u mjeri u kojoj ima pravo upotrebljavati Softver u skladu s ograničenjima koja proizlaze iz broja Licenci koje je dodijelio Dobavljač. Licenčni ključ smatra se povjerljivim te ga ne smijete dijeliti s trećim stranama ili dopustiti trećim stranama upotrebu Licenčnog ključa, osim ako to nije dopušteno Ugovorom ili ako to dopušta Dobavljač. Ako je Licenčni ključ ugrožen, odmah o tome obavijestite Dobavljača.
- c) **Business Edition.** Za korištenje Softvera na serverima za poštu, relejima za poštu, pristupnicima za poštu i internetskim pristupnicima potrebno je nabaviti Business Edition verziju Softvera.
- d) **Trajanje Licence.** Vaše pravo korištenja Softvera vremenski je ograničeno.
- e) **OEM Softver.** Korištenje OEM Softvera ograničeno je na računalo s kojim ste ga pribavili. Ne smije se prenositi na drugo računalo.
- f) **NFR, TRIAL softver.** Softver koji je klasificiran kao verzija koja nije za daljnju prodaju (Not-for-resale, dalje u tekstu: NFR) ili probna verzija (TRIAL) ne smije se drugima dodjeljivati uz naknadu i smije se koristiti samo u svrhu demonstracije ili testiranja značajki Softvera.
- g) **Prekid valjanosti Licence.** Valjanost Licence prekida se automatski na kraju razdoblja za koje je dodijeljena. Ako se Vi ne pridržavate bilo koje odredbe ovog Ugovora, Dobavljač ima pravo povući se iz Ugovora bez utjecaja na bilo koje pravo ili pravni lik dostupan Dobavljaču u takvom slučaju. U slučaju ponistiavanja Licence morate bez

odgode izbrisati, uništiti ili o vlastitom trošku vratiti Softver i sve sigurnosne kopije tvrtki ESET ili na prodajno mjesto na kojemu ste nabavili Softver. Nakon prekida Licence, Dobavljač također ima pravo poništiti pravo Krajnjeg korisnika na upotrebu funkcija Softvera koje zahtijevaju povezivanje na servere Dobavljača ili trećih strana.

**4. Funkcije koje zahtijevaju prikupljanje podataka i internetsku vezu.** Za pravilno funkcioniranje Softvera potrebna je veza s internetom i povezivanje sa serverima Dobavljača ili trećih strana u redovitim intervalima te primjenjivo prikupljanje podataka u skladu s Pravilima privatnosti. Veza s internetom i primjenjivo prikupljanje podataka neophodni su za sljedeće funkcije Softvera:

- a) **Aktualizacija Softvera.** Dobavljač ima pravo povremeno izdavati aktualizacije Softvera („Aktualizacije“), ali nije obvezan nuditi Aktualizacije. Ta je funkcija omogućena u standardnim postavkama Softvera te se Aktualizacije instaliraju automatski, osim ako Krajnji korisnik onemogući automatsko instaliranje Aktualizacija. U svrhu pružanja Nadogradnji potrebno je provjeriti autentičnost Licence, uključujući podatke o Računalu i/ili platformi na kojoj je instaliran Softver u skladu s Pravilima privatnosti.
- b) **Prosljeđivanje infiltracija i informacija Dobavljaču.** Softver sadrži funkcije koje prikupljaju uzorce računalnih virusa i ostalih zlonamjernih računalnih programa i sumnjive, problematične, potencijalno neželjene ili potencijalno nesigurne objekte kao što su datoteke, URL adrese, IP paketi i ethernet okviri (dalje u tekstu „infiltracije“), a zatim ih šalju Dobavljaču, uključujući, ali ne isključivo, informacije o instalacijskom postupku, računalu i/ili platformi na kojoj je Softver instaliran, informacije o operacijama i funkcionalnosti Softvera te informacije o uređajima na lokalnoj mreži kao što su vrsta, dobavljač, model i/ili naziv uređaja (dalje u tekstu „informacije“). Informacije i infiltracije mogu sadržavati podatke (uključujući nasumično ili slučajno prikupljene osobne podatke) o krajnjem korisniku ili drugim korisnicima računala na kojem je softver instaliran i datoteke koje su pod utjecajem infiltracija s povezanim metapodacima.

Informacije i Infiltracije mogu se prikupljati sljedećim funkcijama Softvera:

- i. Funkcija LiveGrid Reputation System uključuje prikupljanje i slanje jednostranih ključeva vezanih uz Infiltracije Dobavljaču. Ta funkcija je prema standardnim postavkama Softvera aktivirana.
- ii. Funkcija LiveGrid Feedback System uključuje prikupljanje i slanje Infiltracija s povezanim metapodacima i Informacijama Dobavljaču. Tu funkciju može aktivirati Krajnji korisnik tijekom postupka instalacije Softvera.

Dobavljač primljene Informacije i Infiltracije upotrebljava samo za analizu i istraživanje Infiltracija i poboljšanje Softvera i provjere autentičnosti Licence te poduzima odgovarajuće mjere kako bi osigurao da primljene Infiltracije i Informacije ostanu sigurne. Aktivacijom ove funkcije Softvera Dobavljač može prikupljati i obrađivati Infiltracije i Informacije kao što je navedeno u Pravilima privatnosti i u skladu s važećim zakonskim propisima. Ove funkcije možete deaktivirati u bilo kojem trenutku.

Za potrebe ovog Ugovora potrebno je prikupljati, obrađivati i pohranjivati podatke pomoću kojih Vas Dobavljač može identificirati u skladu s Pravilima privatnosti. Ovime se slažete da Dobavljač može vlastitim sredstvima provjeravati upotrebljavate li Softver u skladu s odredbama ovog Ugovora. Ovime se slažete s tim da je za potrebe ovog Ugovora potrebno prenositi podatke tijekom komunikacije između Softvera i Dobavljačevih računalnih sustava ili računalnih sustava poslovnih partnera u sklopu Dobavljačeve distribucijske mreže i mreže podrške kako bi se osigurala funkcionalnost Softvera i autorizacija za upotrebu Softvera te za zaštitu Dobavljačevih prava.

Nakon prihvatanja ovog Ugovora Dobavljač ili bilo koji poslovni partner u sklopu Dobavljačeve distribucijske mreže ili mreže podrške ima pravo na prijenos, obradu i pohranu osnovnih podataka koji Vas identificiraju u svrhu fakturiranja, izvršavanja ovog Ugovora i slanja obavijesti na vaše Računalo. Ovime pristajete na primanje obavijesti i poruka uključujući bez ograničenja marketinške informacije.

**Pojedinosti o privatnosti, zaštiti osobnih podataka i svojim pravima kao sudionik možete potražiti u Pravilima**

**privatnosti koje su dostupne na web-stranici Dobavljača i kojima se može izravno pristupiti tijekom postupka instalacije. Također im možete pristupiti putem odjeljka pomoći u Softveru.**

**5. Ostvarivanje prava Krajnjeg korisnika.** Prava Krajnjeg korisnika morate ostvarivati osobno ili putem svojih zaposlenika. Pravo na upotrebu Softvera imate isključivo u svrhu zaštite poslovanja i Računala ili računalnih sustava za koje ste nabavili Licencu.

**6. Ograničenja prava.** Softver ne smijete kopirati, distribuirati, izvlačiti komponente iz njega ni stvarati izvedene radove koji se temelje na Softveru. Pri korištenju Softvera dužni ste poštovati sljedeća ograničenja:

a) Smijete stvoriti jednu arhivsku sigurnosnu kopiju Softvera na mediju za trajnu pohranu podataka pod uvjetom da tu arhivsku sigurnosnu kopiju ne instalirate i ne koristite na bilo kojem drugom računalu. Bilo kakve druge kopije Softvera predstavljat će povredu ovog Ugovora.

b) Ne smijete koristiti, mijenjati, prevoditi, reproducirati ni prenosići prava na korištenje Softvera ili kopija Softvera ni na koji način koji nije izričito dopušten ovim Ugovorom.

c) Softver ne smijete prodavati, podlicencirati, davati u zakup ili najam niti ga posuđivati, odnosno koristiti za pružanje komercijalnih usluga.

d) Softver ne smijete dekompilirati, na njemu vršiti obrnuti inženjering ni obrnuto kompiliranje niti na drugi način pokušati otkriti izvorni kod Softvera, osim u mjeri u kojoj je ovo ograničenje izrijekom zakonski zabranjeno.

e) Suglasni ste Softver koristiti na način sukladan svim nadležnim zakonima u jurisdikciji u kojoj koristite Softver, uključujući, ali ne ograničavajući se na primjenjiva ograničenja koja se odnose na zaštitu autorskih prava i drugih prava na zaštitu intelektualnog vlasništva.

f) Suglasni ste da ćete Softver i njegove funkcije koristiti na način koji ne ograničava mogućnost drugih Krajnjih korisnika da pristupaju tim uslugama. Dobavljač zadržava pravo ograničavanja isporučenih usluga pojedinačnim Krajnjim korisnicima, a kako bi omogućio korištenje usluga što većem mogućem broju Krajnjih korisnika.

Ograničavanje usluga također znači mogućnost potpunog ukidanja mogućnosti korištenja bilo koje funkcije softvera i brisanje podataka i informacija na proxy serverima Dobavljača ili serverima trećih strana koji se odnose na određenu funkciju Softvera.

g) Pristajete da se nećete baviti nikakvim aktivnostima koje uključuju upotrebu Licenčnog ključa protivno uvjetima ovog Ugovora ili za koje se Licenčni ključ ustupa bilo kojoj osobi koja nema pravo upotrebljavati Softver, kao što je prijenos iskorištenih ili neiskorištenih Licenčnih ključeva u bilo kojem obliku, neautorizirana reprodukcija ili distribucija duplicitarnih ili generiranih Licenčnih ključeva ili upotreba Softvera koja proizlazi iz upotrebe Licenčnog ključa koji je nabavljen iz izvora koji nije Dobavljač.

**7. Autorska prava.** Softver i sva prava, uključujući bez ograničenja pravo vlasništva i pripadajuća prava intelektualnog vlasništva, vlasništvo su tvrtke ESET i/ili njezinih davatelja licence. Ti su entiteti zaštićeni odredbama međunarodnih sporazuma i svim ostalim nadležnim zakonima zemlje u kojoj se Softver koristi. Struktura, organizacija i kôd Softvera vrijedne su poslovne tajne i povjerljive informacije tvrtke ESET i/ili njezinih davatelja licence. Ne smijete kopirati Softver, osim u slučaju opisanom u članku 6 (a). Bilo kakve kopije koje prema ovom Ugovoru smijete stvarati moraju sadržavati iste obavijesti o zaštiti autorskih prava i vlasništvu koje se pojavljuju na Softveru. Ako dekompilirate Softver, na njemu vršite obrnuti inženjering ili na drugi način pokušate otkriti izvorni kôd Softvera, kršeći time odredbe ovog Ugovora, ovime se slažete da se sve tako dobivene informacije automatski i neopozivo smatraju prenesenima Dobavljaču i postaju u potpunosti njegovo vlasništvo od trenutka nastanka tih informacija, bez utjecaja na prava Dobavljača u odnosu na kršenje ovog Ugovora.

**8. Pridržavanje prava.** Dobavljač ovime pridržava sva prava na Softver, s izuzetkom prava izrijekom dodijeljenih Vama kao Krajnjem korisniku Softvera prema odredbama ovog Ugovora.

**9. Višejezične verzije, Softver na dva nosača podataka, veći broj kopija.** U slučaju da Softver podržava više platformi ili jezika, odnosno ako dobijete više kopija Softvera, Softver smijete koristiti samo na onom broju računalnih sustava za koji imate Licence te smijete koristiti samo verzije za koje imate Licencu. Verzije ili kopije Softvera koje ne koristite ne smijete prodati, dati u najam ili zakup, podlicencirati, posuđivati ni prenijeti na treće strane.

**10. Početak i prekid Ugovora.** Ovaj Ugovor stupa na snagu s datumom Vašeg prihvaćanja ovog Ugovora. Ovaj Ugovor možete u bilo kojem trenutku prekinuti tako da trajno deinstalirate, uništite ili o vlastitom trošku vratite Softver, sve sigurnosne kopije i sve povezane materijale koje ste dobili od Dobavljača ili njegovih poslovnih partnera. Bez obzira na način prekida ovog Ugovora, odredbe članaka 7., 8., 11., 13., 19. i 21. primjenjuju se bez vremenskog ograničenja.

**11. IZJAVE KRAJNJE KORISNIKA.** KAO KRAJNJI KORISNIK PRIHVACATE ČINJENICU DA SE SOFTVER ISPORUČUJE „U ZATEČENOM STANJU“, BEZ IKAVOG JAMSTVA, IZRIČITOG ILI IMPLICIRANOG, TE U MAKSIMALNOJ MJERI DOPUŠTENOJ NADLEŽNIM ZAKONOM. DOBAVLJAČ, NJEGOVI DAVATELJI LICENCE NI POVEZANA DRUŠTVA, KAO NI NOSITELJI AUTORSKIH PRAVA, NE DAJU NIKAKVE IZJAVE NI JAMSTVA, IZRIČITA ILI IMPLICIRANA, UKLJUČUJUĆI BEZ OGRANIČENJA JAMSTVO UTRŽIVOSTI ILI PRIKLADNOSTI ZA ODREĐENU NAMJENU, JAMSTVO DA SOFTVER NE POVRJEĐUJE PATENTE, AUTORSKA PRAVA, TRŽIŠNE ZNAKOVE ILI NEKA DRUGA PRAVA TREĆIH STRANA. DOBAVLJAČ NI BILO KOJA DRUGA STRANA NE DAJE NIKAKVA JAMSTVA DA ĆE FUNKCIJE KOJE SOFTVER SADRŽI BITI U SKLADU S VAŠIM POTREBAMA NI DA ĆE SOFTVER FUNKCIONIRATI BEZ POTEŠKOĆA I POGREŠAKA. VI PREUZIMATE POTPUNU ODGOVORNOST I RIZIK KOJI PROIZLAZE IZ ODABIRA SOFTVERA RADI POSTIZANJA REZULTATA KOJE ŽELITE, KAO I ZA INSTALIRANJE I KORIŠTENJE SOFTVERA TE TAKO DOBIVENE REZULTATE.

**12. Odsutnost ostalih obveza.** Ovaj Ugovor ne stvara nikakve obveze Dobavljača i njegovih davatelja licence osim onih izrijekom navedenih u ovom Ugovoru.

**13. OGRANIČENJE ODGOVORNOSTI.** U NAJVEĆOJ MJERI DOPUŠTENOJ NADLEŽNIM ZAKONIMA, NI DOBAVLJAČ, NI NJEGOVI ZAPOSLENICI NI DAVATELJI LICENCE NEĆE SNOSITI ODGOVORNOST NI ZA KAKAV GUBITAK PRIHODA, DOBITI ILI PRODAJE, GUBITAK PODATAKA NI ZA TROŠKOVE NASTALE NABAVOM ZAMJENSKIH PROIZVODA ILI USLUGA, ZA OŠTEĆENJE IMOVINE, OSOBNE ŠTETE, PREKID POSLOVANJA, GUBITAK POSLOVNIH PODATAKA, KAO NI ZA BILO KAKVE POSEBNE, IZRAVNE, NEIZRAVNE, SLUČAJNE, GOSPODARSKE, KOMPENZACIJSKE, KAZNENE ILI POSLJEDIČNE ŠTETE, ODNOSNO ŠTETE NASTALE NA BILO KOJI NAČIN, NASTALE NA TEMELJU UGOVORA, NAMJERNOG DJELOVANJA, NEPAŽNJOM ILI NEKOM DRUGOM ČINJENICOM NA KOJOJ SE TEMELJI ODGOVORNOST, NASTALE KORIŠTENJEM ILI NEMOGUĆNOŠĆU KORIŠTENJA SOFTVERA, ČAK I U SLUČAJU DA SU DOBAVLJAČ ILI NJEGOVI DAVATELJI LICENCE UPOZORENI NA MOGUĆNOST TAKVE ŠTETE. BUDUĆI DA ODREĐENE DRŽAVE I JURISDIKCIJE NE DOPUŠTAJU IZUZEĆE OD ODGOVORNOSTI, ALI MOGU DOPUSTITI NJENO OGRANIČENJE, U TAKVIM SLUČAJEVIMA ODGOVORNOST DOBAVLJAČA, NJEGOVIH ZAPOSLENIKA ILI DAVATELJA LICENCE BIT ĆE OGRANIČENA NA IZNOS KOJI STE PLATILI ZA LICENCU.

14. Nijedna odredba ovog Ugovora nema utjecaja na zakonska prava bilo koje strane koja je u svojstvu potrošača u slučaju da je protivna tim pravima.

**15. Tehnička podrška.** ESET i treće strane koje ESET angažira pružat će tehničku podršku prema vlastitom nahođenju, bez ikakvih jamstava ili izjava. Krajnji korisnik dužan je prije primanja tehničke podrške izraditi sigurnosnu kopiju svih postojećih podataka, softvera i programa. ESET i/ili treće strane koje je angažirao ESET ne mogu prihvatiti odgovornost za štete ili gubitke podataka, vlasništva, softvera ili hardvera ni gubitak dobiti do kojeg može doći uslijed pružanja tehničke podrške. ESET i/ili treće strane koje je angažirao ESET pridržavaju pravo na odluku da tehnička podrška ne obuhvaća rješavanje određenog problema. ESET pridržava pravo na odbijanje, privremeni prekid ili trajni prekid davanja tehničke podrške po vlastitom nahođenju. Podaci o Licenci, Informacije i drugi podaci u skladu s Pravilima privatnosti mogu biti potrebni za pružanje tehničke podrške.

**16. Prijenos Licence.** Softver se smije prenositi s jednog računalnog sustava na drugi, osim ako je to u suprotnosti

s odredbama ovog Ugovora. Ako to nije u suprotnosti s odredbama Ugovora, Krajnji korisnik ima pravo trajno prenijeti Licencu i sva prava koja proizlaze iz ovog Ugovora drugom Krajnjem korisniku isključivo uz odobrenje Dobavljača te pod uvjetom (i) da izvorni Krajnji korisnik ne zadrži nijednu kopiju Softvera, (ii) da je prijenos prava izravan, tj. od izvornog Krajnjeg korisnika novom Krajnjem korisniku, (iii) da novi Krajnji korisnik preuzme sva prava i obveze koje je, prema odredbama ovog Ugovora, imao izvorni Krajnji korisnik; (iv) da izvorni Krajnji korisnik novom Krajnjem korisniku dostupnim učini dokumentaciju koja omogućuje provjeru izvornosti Softvera kako je to navedeno u članku 17.

**17. Provjera izvornosti Softvera.** Krajnji korisnik može dokazati svoje pravo na upotrebu Softvera na sljedeće načine: (i) pomoću certifikata o licenci koji je izdao Dobavljač ili treća strana koju je Dobavljač angažirao, (ii) pomoću pisanog licenčnog ugovora, ako je takav ugovor sklopljen, (iii) slanjem poruke e-pošte koju je poslao Dobavljač i koja sadrži pojedinosti o licenciranju (korisničko ime i lozinku). Podaci o Licenci i podaci za identifikaciju Krajnjeg korisnika u skladu s Pravilima privatnosti mogu biti potrebni za provjeru izvornosti Softvera.

**18. Licenciranje za javna tijela i vlasti SAD-a.** Softver se javnim tijelima, uključujući vlasti SAD-a, daje na korištenje uz prava i ograničenja opisana u ovom Ugovoru.

**19. Usklađenost s kontrolom trgovine.**

a) Slažete se da nećete izravno ili neizravno izvoziti, ponovno izvoziti, prenositi ili drugim metodama staviti Softver na raspolaganje bilo kojoj osobi ili ga upotrebljavati na bilo koji način ili sudjelovati u bilo kojoj radnji kojom bi ESET ili njegovi holdinzi, podružnice i podružnice bilo kojeg njegova holdinga, kao i subjekti koje holdinzi kontroliraju (dalje u tekstu: „Povezana društva”), kršili zakone o kontroli trgovine ili trpjeli negativne posljedice na temelju njih, što uključuje

i. bilo koje zakone kojima se kontroliraju, ograničavaju ili nameću uvjeti licenciranja za izvoz, ponovni izvoz ili prijenos robe, softvera, tehnologije ili usluga, koje izdaju ili donose bilo koje državne uprave, državna ili regulatorna tijela Sjedinjenih Američkih Država, Singapura, Ujedinjenog Kraljevstva, Europske Unije ili bilo koje njezine države članice ili bilo koje države u kojoj se provode obveze iz Ugovora ili u kojoj su tvrtka ESET ili bilo koja njegova Povezana društva osnovani ili posluju (dalje u tekstu: „Zakoni kontrole izvoza“) te

ii. bilo koje ekonomске, financijske, trgovačke ili druge sankcije, ograničenja, embarga, zabrane uvoza ili izvoza, zabrane prijenosa sredstava ili imovine ili zabrane pružanja usluga ili ekvivalentne mjere koje propisuju bilo koja državna uprava, državna ili regulatorna tijela Sjedinjenih Američkih Država, Singapura, Ujedinjenog Kraljevstva, Europske Unije ili bilo koje njezine države članice ili bilo koje države u kojoj se provode obveze iz Ugovora ili u kojoj su tvrtka ESET ili bilo koja Povezana društva osnovana ili posluju (dalje u tekstu: „Zakoni o sankcijama“).

b) ESET ima pravo privremeno ili trajno obustaviti svoje obveze iz ovih Uvjeta s trenutnim učinkom u slučaju da:

i. ESET utvrdi da je korisnik, prema mišljenju tvrtke, prekršio ili bi mogao prekršiti odredbe članka 19. (a) ovog Ugovora ili

ii. krajnji korisnik i/ili Softver budu podložni zakonima o kontroli trgovine i ESET na temelju toga utvrdi da bi, prema njegovu mišljenju, nastavkom provedbe korisnikovih obveza iz ovog Ugovora tvrtka ESET ili njezina Povezana društva mogla kršiti zakone o kontroli trgovine ili trpjeli negativne posljedice na temelju njih.

c) Nijedna odredba ovog Ugovora nije predviđena da se tumači i nijedna se odredba ne smije tumačiti tako da navodi ili zahtijeva od druge strane da djeluje ili da se suzdržava od djelovanja (ili da pristane djelovati ili suzdržati se od djelovanja) na bilo koji način koji je nedosljedan, kažnjiv ili zabranjen prema bilo kojim važećim zakonima o kontroli trgovine.

**20. Obavijesti.** Sve obavijesti, Softver koji se vraća i Dokumentacija šalju se na adresu: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

**21. Nadležni zakon.** Na ovaj Ugovor i njegovo tumačenje primjenjivat će se zakoni Republike Slovačke. Krajnji korisnik i Dobavljač suglasni su da se neće primjenjivati principi sukoba zakonskih nadležnosti ni Konvencija Ujedinjenih naroda o ugovorima o međunarodnoj prodaji robe. Izričito se slažete da će za sve sporove i sva potraživanja koja proizlaze iz ovog Ugovora, a odnose se na Dobavljača te sve sporove i sva potraživanja koja se odnose na korištenje Softvera nadležan biti Okružni sud u Bratislavi I te se izričito slažete s pravom navedenog suda da provodi svoju nadležnost.

**22. Opće odredbe.** Ako se bilo koja odredba ovog Ugovora pokaže nevaljanom ili neprovedivom, to neće utjecati na valjanost ostalih odredbi Ugovora, koje ostaju valjane i provedive sukladno uvjetima iz Ugovora. U slučaju odstupanja između različitih jezičnih verzija ovog Ugovora, mjerodavna je verzija na engleskom jeziku. Izmjene ovog Ugovora mogu se vršiti samo u pisanom obliku, potpisane od strane ovlaštenog predstavnika Dobavljača ili osobe izrijekom ovlaštene za djelovanje u tom svojstvu odredbama o pravnom zastupanju.

Ovo je cjelokupan Ugovor između Vas i Dobavljača koji se odnosi na Softver i kao takav potpuno nadomješta sve prijašnje tvrdnje, pregovore, obveze, izvješća ili oglase u vezi sa Softverom.

EULA ID: BUS-STANDARD-20-01

## Pravila privatnosti

ESET, spol. s.r. o, s registriranim uredom na adresi Einsteinova 24, 851 01 Bratislava, Republika Slovačka, tvrtka registrirana u trgovačkom registru Okružnog suda u Bratislavi I, odjeljak Sro, unos br. 3586/B, broj poslovne registracije: 31333532, kao voditelj obrade podataka („ESET” ili „Mi”) želi biti transparentna u vezi s obradom osobnih podataka i privatnosti svojih korisnika. Radi postizanja tog cilja objavljujemo ova Pravila privatnosti isključivo u svrhu informiranja svojih korisnika („Krajnji korisnik” ili „Vi”) o sljedećim temama:

- obradi osobnih podataka,
- povjerljivosti podataka,
- pravima ispitnika.

## Obrada osobnih podataka

Usluge koje pruža ESET implementirane u naš program pružaju se pod uvjetima Licenčnog ugovora za krajnjeg korisnika („EULA”), ali neki od njih mogu zahtijevati posebnu pažnju. Želimo vam pružiti više detalja o prikupljanju podataka u vezi s uslugama koje vam pružamo. Pružamo različite usluge opisane u EULA-i i dokumentaciji programa, kao što su usluge nadogradnje, sustava ESET LiveGrid®, zaštite od zloupotrebe podataka, podrške itd. Kako bi usluge funkcionirale, moramo prikupljati sljedeće podatke:

- Statistike o nadogradnji i druge statistike koje obuhvaćaju informacije o procesu instalacije i vašem računalu, uključujući platformu na kojoj je instaliran naš program i informacije o operacijama i funkcijama naših programa kao što su operacijski sustav, informacije o hardveru, instalacijski ID-ovi, ID-ovi licenci, IP adresa, MAC adresa i postavke konfiguracije programa.
- Jednostrani hashevi povezani s infiltracijama kao dio sustava reputacije ESET LiveGrid® koji poboljšava učinkovitost naših rješenja protiv zlonamjernih programa usporedbom skeniranih datoteka i baze podataka pouzdanih i nepoželjnih stavki u cloudu.
- Sumnjivi uzorci i metapodaci iz divljine kao dio sustava za povratne informacije ESET LiveGrid® koji omogućuje tvrtki ESET da odmah reagira na potrebe naših krajnjih korisnika i da održi našu sposobnost reagiranja na najnovije prijetnje. Ovisimo o tome da nam šaljete

Oinfiltracije kao što su potencijalni uzorci virusa i drugih zlonamjernih programa i sumnjive, problematične, potencijalno neželjene ili potencijalno nesigurne objekte kao što su izvršne datoteke, poruke e-pošte koje ste prijavili kao spam ili koje je kao takve označio naš program;

Oinformacije o uređajima u lokalnoj mreži kao što su vrsta, dobavljač, model i/ili naziv uređaja;

Oinformacije o upotrebi interneta kao što su IP adresa i geografske informacije, IP paketi, URL-ovi i ethernet okviri;

Odatoteke sa stanjem nakon pada sustava i informacije u njima.

Ne želimo prikupljati vaše podatke izvan tog opsega, ali ponekad je to nemoguće spriječiti. Slučajno prikupljeni podaci mogu biti uključeni u samim zlonamjernim programima (prikupljeni bez vašeg znanja ili odobrenja) ili kao dio naziva datoteka ili URL-ova i nije nam namjera da oni budu dio naših sustava niti da ih obrađujemo u svrhu opisanu u ovim Pravilima privatnosti.

- Informacije o licenciranju, kao što su ID licence i osobni podaci poput imena, prezimena, adrese i adrese e-pošte, potrebni su za potrebe fakturiranja, provjeru izvornosti licence i pružanje naših usluga.
- Za pružanje usluge podrške mogu biti potrebni kontaktni podaci i podaci koji se nalaze u vašim zahtjevima za podršku. Ovisno o kanalu koji odaberete za kontakt s nama, možemo prikupiti Vašu adresu e-pošte, telefonski broj, licenčne informacije, podatke o programu i opis Vašeg slučaja za podršku. Možemo od vas zatražiti i druge podatke radi olakšavanja pružanja usluge podrške.

## Povjerljivost podataka

ESET je tvrtka koja djeluje diljem svijeta putem povezanih subjekata ili partnera kao dio naše mreže za distribuciju, usluge i podršku. Informacije koje ESET obrađuje mogu se prenijeti povezanim subjektima ili partnerima ili preuzeti od njih radi provedbe Licenčnog ugovora za krajnjeg korisnika, uključujući npr. pružanje usluga ili podrške ili naplatu. Ovisno o Vašoj lokaciji i usluzi koju odaberete, može biti potrebno da prenesemo Vaše podatke u zemlju u kojoj ne postoji odluka Europske komisije o odgovarajućoj zaštiti. Čak i u tom slučaju svaki prijenos informacija podložan je zakonodavstvu o zaštiti podataka i izvršava se samo ako je to potrebno. Standardne ugovorne klauzule, obvezujuća korporativna pravila ili druga odgovarajuća zaštita moraju se utvrditi bez iznimke.

Dajemo sve od sebe kako bismo spriječili pohranjivanje podataka dulje nego što je potrebno tijekom pružanja usluga prema Licenčnom ugovoru za krajnjeg korisnika. Vrijeme zadržavanja može biti duže od valjanosti vaše licence kako bismo vam pružili dovoljno vremena za jednostavnu i pravovremenu obnovu licence. Minimizirane i pseudonimizirane statistike i drugi podaci iz sustava ESET LiveGrid® mogu se dalje obrađivati u statističke svrhe.

ESET provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao odgovarajuću razinu sigurnosti za potencijalne opasnosti. Činimo sve što možemo kako bismo zajamčili kontinuiranu povjerljivost, cjelovitost, dostupnost i otpornost sustava i usluga obrade. Međutim, u slučaju povrede osobnih podataka koja uzrokuje opasnosti za Vaša prava i slobode, spremni smo obavijestiti nadzorno tijelo, kao i osobe čiji se podaci obrađuju. Kao ispitanik imate pravo podnijeti prigovor nadzornom tijelu.

## Pravima ispitanika.

Tvrtka ESET podložna je zakonskim odredbama Slovačke Republike i obvezuje nas zakonodavstvo o zaštiti podataka kao dio Europske unije. Podložno uvjetima utvrđenima primjenjivim zakonima za zaštitu podataka, kao ispitanik imate sljedeća prava:

- pravo zatražiti od tvrtke ESET pristup svojim osobnim podacima,
- pravo na ispravak svojih osobnih podataka ako su netočni (također imate pravo na dopunu nepotpunih

osobnih podataka),

- pravo zatražiti brisanje svojih osobnih podataka,
- pravo zatražiti ograničenje obrade svojih osobnih podataka,
- pravo uložiti prigovor na obradu,
- pravo podnijeti pritužbu i
- pravo na prenosivost podataka.

Smatramo da su svi podaci koje obrađujemo vrijedni i neophodni za svrhu našeg legitimnog interesa, a to je pružanja usluga i programa korisnicima.

Ako želite ostvariti svoje pravo kao ispitanik ili ako imate pitanja, pošaljite nam poruku na:

ESET, spol. s r.o.  
Data Protection Officer  
Einsteinova 24  
85101 Bratislava  
Slovak Republic  
[dpo@eset.sk](mailto:dpo@eset.sk)