ESET Internet Security

Vodič za korisnike

Kliknite ovdje za prikazivanje verzije mrežne pomoći dokumenta

Digital Security
Progress. Protected.

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

ESET Internet Security 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 pisanom obliku.

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.

1 ESET Internet Security 1
1.1 Novosti 2
1.2 Koji program imam? 2
1.3 Sistemski preduvjeti 3
1.3 Vaša verzija sustava Windows 7 je zastarjela 4
1.3 Microsoft više ne podržava Windows 7 4
1.3 Windows Vista više nije podržan 5
1.4 Prevencija 6
1.5 Stranice pomoći 7
2 Instalacija 8
2.1 Internetski instalacijski program 8
2.2 Izvanmrežna instalacija 10
2.3 Aktivacija proizvoda 11
2.3 Unos Licenčnog ključa prilikom aktivacije 12
2.3 Korištenje ESET HOME računa 12
2.3 Aktivacija probne licence 13
2.3 Besplatan ESET-ov licenčni ključ 14
2.3 Aktivacija nije uspjela – česti slučajevi 15
2.3 Aktivacija nije uspjela jer je licenca prekomjerno iskorištena 15
2.3 Nadogradnja licence 16
2.3 Nadogradnja programa 17
2.3 Prebacivanje licence na stariju verziju 17
2.3 Prebacivanje programa na stariju verziju 18
2.4 Alat za otklanjanje poteškoća s instalacijom 19
2.5 Prvo skeniranje nakon instalacije 19
2.6 Nadogradnja na noviju verziju 20
2.6 Automatska nadogradnja programa koji radi prema starom standardu 21
2.7 Preporučivanje ESET-ova programa prijatelju 21
2.7 Instalirat će se ESET Internet Security 22
2.7 Promijeni u drugu vrstu programa 22
2.7 Registracija 22
2.7 Napredak aktivacije 22
2.7 Aktivacija je uspješna 22
3 Vodič za početnike 23
3.1 Povežite se s ESET HOME računom 23
3.1 Prijava u ESET HOME 24
3.1 Prijava nije uspjela – obične pogreške 25
3.1 Dodavanje uređaja u ESET HOME 26
3.2 Glavni programski prozor 26
3.3 Nadogradnje 29
3.4 Podešavanje dodatnih ESET sigurnosnih alata 30
3.5 Konfiguriranje mrežne zaštite 30
3.6 Aktiviraj Anti-Theft 31
3.7 Alati roditeljske kontrole 32
4 Rad s programom ESET Internet Security 32
4.1 Zaštita računala 34
4.1 Modul detekcije 36
4.1 Napredne opcije modula detekcije 40
4.1 Otkrivena je infiltracija 40
4.1 rezidentna zaštita 43

4.1 Razine čišćenja 44
4.1 Kada treba izmijeniti konfiguraciju rezidentne zaštite 45
4.1 Provjera rezidentne zaštite 45
4.1 Što ako rezidentna zaštita ne funkcionira 45
4.1 Izuzeti procesi 46
4.1 Dodavanje ili uređivanje izuzetih procesa 47
4.1 Zaštita na bazi clouda 47
4.1 Filtar izuzetaka za zaštitu na bazi clouda 50
4.1 Skeniranje računala 50
4.1 Pokretač prilagođenog skeniranja 53
4.1 Napredak skeniranja 54
4.1 Dnevnik skeniranja računala 56
4.1 Skeniranja za zlonamjerne softvere 58
4.1 Skeniranje u stanju mirovanja 58
4.1 Profili skeniranja 59
4.1 Ciljevi skeniranja 59
4.1 Kontrola uređaja 60
4.1 Uređivač pravila kontrole uređaja 61
4.1 Otkriveni uređaji 62
4.1 Grupe uređaja 62
4.1 Dodavanje pravila kontrole uređaja 63
4.1 Zaštita web-kamere 66
4.1 Uređivač pravila zaštite web-kamere 66
4.1 Sustav za sprečavanje upada (HIPS) 67
4.1 HIPS interaktivni prozor 69
4.1 Otkriveno je moguće ponašanje ransomwarea 70
4.1 HIPS upravljanje pravilima 71
4.1 Postavke HIPS pravila 72
4.1 Dodavanje puta aplikacije/registra za HIPS 75
4.1 HIPS napredno podešavanje 75
4.1 Upravljački programi koji se uvijek smiju učitati 75
4.1 Način rada za igranje 75
4.1 Skeniranje pri pokretanju 76
4.1 Automatska provjera pokretačke datoteke 76
4.1 Zaštita dokumenata 77
4.1 Izuzeci 77
4.1 Izuzeci radi poboljšanja performansi 78
4.1 Dodavanje ili uređivanje izuzetka radi poboljšanja performansi 79
4.1 Format izuzetaka puta 81
4.1 Izuzeci detekcija poznatih prijetnji 82
4.1 Dodavanje ili uređivanje izuzetih detekcija poznatih prijetnji 83
4.1 Čarobnjak za stvaranje izuzetih detekcija poznatih prijetnji 84
4.1 Izuzeci iz HIPS-a 85
4.1 ThreatSense parameteri 85
4.1 Datotečne ekstenzije izuzete od skeniranja 89
4.1 Dodatni ThreatSense parametri 89
4.2 Internetska zaštita 90
4.2 Filtriranje protokola 91
4.2 Izuzete aplikacije 92
4.2 Izuzete IP adrese 92
4.2 Dodaj IPv4 adresu 93

4.2 Dodaj IPv6 adresu 93
4.2 SSL/TLS 94
4.2 Certifikati 95
4.2 Šifrirani mrežni promet 96
4.2 Popis poznatih certifikata 96
4.2 Popis filtriranih SSL/TLS aplikacija 97
4.2 zaštita klijenta e-pošte 97
4.2 Integracija s klijentima e-pošte 98
4.2 Alatna traka za Microsoft Outlook 99
4.2 Alatna traka za Outlook Express i Windows Mail 99
4.2 Dijaloški okvir s potvrdom 100
4.2 Ponovno skeniranje poruka 100
4.2 Protokoli e-pošte 100
4.2 POP3/POP3S filtar 102
4.2 Oznake e-pošte 102
4.2 Antispam zaštita 103
4.2 Rezultat obrade adresa 104
4.2 Antispam adresari 104
4.2 Adresari 105
4.2 Dodavanje/uređivanje adrese 107
4.2 zaštita web pristupa 107
4.2 Napredno podešavanje zaštite web pristupa 110
4.2 Web protokoli 110
4.2 Upravljanje URL adresama 111
4.2 Popis URL adresa 112
4.2 Stvaranje novog popisa URL adresa 113
4.2 Kako dodati URL masku 114
4.2 Anti-phishing zaštita 114
4.3 Mrežna zaštita 116
4.3 Napredno podešavanje Mrežne zaštite 117
4.3 Poznate mreže 119
4.3 Uređivač poznatih mreža 119
4.3 Autorizacija mreže – konfiguracija servera 122
4.3 Konfiguriranje zona 123
4.3 Firewall zone 123
4.3 Firewall 124
4.3 Firewall profili 126
4.3 Dijaloški prozor – uređivanje Firewall profila 126
4.3 Profili dodijeljeni mrežnim adapterima 126
4.3 Konfiguriranje i korištenje pravila 127
4.3 Popis pravila firewalla 127
4.3 Dodavanje ili uređivanje pravila firewalla 129
4.3 Pravilo firewalla – lokalno 130
4.3 Pravilo firewalla – udaljeno 131
4.3 Otkrivanje preinake aplikacije 132
4.3 Popis aplikacija izuzetih od otkrivanja prijetnji 133
4.3 Postavke načina rada za učenje 133
4.3 Zaštita od mrežnog napada (IDS) 134
4.3 Zaštita od napada grubom silom 134
4.3 Pravila 135
4.3 Pravila IDS-a 137

4.3 Blokirana je potencijalna prijetnja 140
4.3 Otklanjanje poteškoća mrežne zaštite 140
4.3 Dozvoljeni servisi i napredne opcije 140
4.3 Povezane mreže 143
4.3 Mrežni adapteri 144
4.3 Popis privremeno blokiranih IP adresa 144
4.3 Dnevnik mrežne zaštite 145
4.3 Uspostava veze – otkrivanje 146
4.3 Rješavanje problema s ESET firewallom 147
4.3 Čarobnjak za otklanjanje poteškoća 147
4.3 Zapisivanje i stvaranje pravila ili izuzetaka iz dnevnika 147
4.3 Stvori pravilo iz dnevnika 148
4.3 Stvaranje izuzetaka iz obavijesti osobnog firewalla 148
4.3 Napredno vođenje dnevnika Mrežne zaštite 148
4.3 Rješavanje problema s filtriranjem protokola 149
4.3 Otkrivena je nova mreža 150
4.3 Promjena aplikacije 150
4.3 Dolazna pouzdana komunikacija 151
4.3 Odlazna pouzdana komunikacija 152
4.3 Dolazna komunikacija 154
4.3 Odlazna komunikacija 155
4.3 Podešavanje pregleda veza 156
4.4 Sigurnosni alati 156
4.4 Zaštita bankarstva i plaćanja 157
4.4 Napredno podešavanje zaštite bankarstva i plaćanja 158
4.4 Zaštićene web stranice 159
4.4 Obavijest u pregledniku 159
4.4 Roditeljska kontrola 160
4.4 Iznimke web stranica 162
4.4 Korisnički računi 164
4.4 Kategorije 164
4.4 Rad s korisničkim računima 165
4.4 Kopiranje iznimke od korisnika 167
4.4 Kopiranje kategorija s računa 167
4.4 Aktiviraj roditeljsku kontrolu 167
4.4 Anti-Theft 167
4.4 Prijavite se na svoj račun ESET HOME. 169
4.4 Postavi naziv uređaja 170
4.4 Anti-Theft aktiviran/deaktiviran 171
4.4 Dodavanje novog uređaja nije uspjelo 171
4.5 Aktualizacija programa 171
4.5 Podešavanje aktualizacije 174
4.5 Vraćanje aktualizacije 176
4.5 Vremenski interval povrata 178
4.5 Nadogradnje programa 178
4.5 Opcije veze 178
4.5 Stvaranje aktualizacijskih zadataka 179
4.5 Dijaloški prozor – potrebno je restartati računalo 179
4.6 Alati 180
4.6 Mrežna provjera 181
4.6 Mrežni uređaj u Mrežnoj provjeri 183

4.6 Obavijesti | Mrežna provjera 186
4.6 Alati u programu ESET Internet Security 186
4.6 Dnevnici 188
4.6 Filtriranje dnevnika 190
4.6 Konfiguracija zapisivanja 191
4.6 Procesi koji se izvršavaju 192
4.6 Sigurnosno izvješće 194
4.6 Mrežne veze 196
4.6 Mrežna aktivnost 197
4.6 ESET SysInspector 198
4.6 Planer 199
4.6 Opcije planiranog skeniranja 202
4.6 Pregled zakazanog zadatka 203
4.6 Pojedinosti zadatka 203
4.6 Vrijeme pokretanja zadatka 203
4.6 Vrijeme pokretanja zadatka – jednom 203
4.6 Vrijeme pokretanja zadatka – svakodnevno 204
4.6 Vrijeme pokretanja zadatka – tjedno 204
4.6 Vrijeme pokretanja zadatka – pokretanje prilikom događaja 204
4.6 Preskočeni zadatak 204
4.6 Detalji o zadatku – nadogradnja 205
4.6 Detalji o zadatku – pokretanje aplikacije 205
4.6 Čistač sustava 206
4.6 ESET SysRescue Live 207
4.6 Karantena 207
4.6 Proxy server 210
4.6 Odabir uzorka za analizu 211
4.6 Odabir uzorka za analizu – Sumnjiva datoteka 212
4.6 Odabir uzorka za analizu – Sumnjiva web stranica 212
4.6 Odabir uzorka za analizu – Neispravno identificirana datoteka 213
4.6 Odabir uzorka za analizu – Neispravno identificirana web stranica 213
4.6 Odabir uzorka za analizu – Ostalo 213
4.6 Nadogradnja sustava Microsoft Windows® 214
4.6 Dijaloški prozor – nadogradnja sustava 214
4.6 Aktualiziranje podataka 214
4.7 Korisničko sučelje 214
4.7 Elementi korisničkog sučelja 215
4.7 Podešavanje pristupa 216
4.7 Lozinka za napredno podešavanje 216
4.7 Ikona trake sustava 217
4.7 Podrška za čitač zaslona 218
4.7 Pomoć i podrška 218
4.7 O programu ESET Internet Security 219
4.7 ESET vijesti 220
4.7 Slanje podataka o sistemskoj konfiguraciji 220
4.7 Tehnička podrška 221
4.8 Obavijesti 221
4.8 Dijaloški prozor – statusi aplikacije 222
4.8 Obavijesti na radnoj površini 222
4.8 Popis obavijesti na radnoj površini 224
4.8 Interaktivna upozorenja 225

4.8 Poruke za potvrdu 227
4.8 Izmjenjivi mediji 228
4.8 Proslјeđivanje 229
4.9 Postavke privatnosti 231
4.10 Profili 232
4.11 Tipkovnički prečaci 233
4.12 Dijagnostika 234
4.12 Tehnička podrška 236
4.12 Uvoz i izvoz postavki 236
4.12 Želite li vratiti sve postavke u ovom odjeljku 237
4.12 Vraćanje na standardne postavke 237
4.12 Pogreška prilikom spremanja konfiguracije 237
4.13 Skener naredbenog retka 237
4.14 ESET CMD 240
4.15 Otkrivanje stanja mirovanja 241
5 Najčešća pitanja 242
5.1 Kako nadograditi program ESET Internet Security 243
5.2 Uklanjanje virusa s računala 243
5.3 Dopuštanje komunikacije za određene aplikacije 243
5.4 Kako aktivirati roditeljsku kontrolu za neki račun 244
5.5 Stvaranje novog zadatka u Planeru 245
5.6 Zakazivanje tjednog skeniranja računala 246
5.7 Kako riješiti pogrešku 247
5.8 Kako otključati Napredno podešavanje 249
5.9 Kako riješiti deaktivaciju programa s ESET HOME portala 250
5.9 Program deaktiviran, uređaj odspojen 250
5.9 Program nije aktiviran 250
6 Program za poboljšanje iskustva korisnika 251
7 Licenčni ugovor za krajnjeg korisnika 252
8 Pravila privatnosti 263

ESET Internet Security

ESET Internet Security predstavlja novi pristup potpuno integriranoj zaštiti računala. Najnovija verzija sustava za skeniranje ESET LiveGrid®, u kombinaciji s našim prilagođenim modulima firewalla i antispama, brzo i precizno štiti vaše računalo. Rezultat je pametan sustav koji neprekidno vodi računa o napadima i zlonamjernom softveru koji bi mogao ugroziti vaše računalo.

ESET Internet Security potpuno je sigurnosno rješenje koje kombinira maksimalnu zaštitu s minimalnim utjecajem na rad sustava. Naše napredne tehnologije služe se umjetnom inteligencijom kako bi spriječile infiltraciju virusima, spywareom, trojanskim softverom, crvima, adwareom, rootkitima i drugim prijetnjama, pri čemu nema negativnog utjecaja na rad vašeg sustava i računala.

Značajke i prednosti

Redizajnirano korisničko sučelje	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 Internet Security i pruža sadržaj podrške koji se dinamički nadograđuje.
Antivirus i antispyware	Proaktivno otkriva i čisti veći broj poznatih i nepoznatih virusa, crva, trojanaca i rootkita. 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 Anti-Phishing 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).
Redovite nadogradnje	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.
ESET LiveGrid® (reputacija utemeljena na Cloud tehnologiji)	Reputaciju procesa koji se izvršavaju i datoteka možete provjeriti izravno iz programa ESET Internet Security.
Kontrola uređaja	Automatski skenira sve USB flash pogone, memorijske kartice i CD-ove/DVD-ove. Blokira izmjenjive medije ovisno o vrsti medija, proizvođaču, veličini i ostalim svojstvima.
Funkcija HIPS	Možete detaljnije prilagoditi ponašanje sustava, odrediti pravila za registar sustava, aktivne procese i programe te detaljno konfigurirati svoj sigurnosni položaj.
Način rada za igranje	Odgađa sve skočne prozore, nadogradnje ili druge radnje koje intenzivno koriste sustav te tako čuva njegove resurse za igranje i ostale aktivnosti koje se odvijaju na cijelom zaslonu.

Funkcije u programu ESET Internet Security

Zaštita bankarstva i plaćanja	Zaštita bankarstva i plaćanja pruža zaštićeni preglednik koji se upotrebljava prilikom pristupa internetskom bankarstvu ili platformama za plaćanje na internetu da bi se osiguralo da se sve internetske transakcije izvršavaju u pouzdanom i sigurnom okruženju.
Podrška za mrežne potpise	Mrežni potpisi omogućuju brzo otkrivanje i blokiranje zlonamjernog prometa u smjeru korisničkih uređaja ili iz njihova smjera, na primjer botova i paketa za zloupotrebu. Ta se značajka može smatrati poboljšanjem Zaštite od botneta.
Inteligentni firewall	Sprečava neovlaštene korisnike da pristupe računalu i iskoriste vaše osobne podatke.

ESET Antispam	Spam čini do 50% ukupne komunikacije e-poštom. Antispam zaštita sprječava taj problem.
Anti-Theft	Anti-Theft povećava sigurnost na korisničkoj razini u slučaju gubitka ili krađe računala. Nakon što korisnici instaliraju ESET Internet Security i Anti-Theft, njihov će uređaj biti naveden u web sučelju. Web sučelje omogućuje korisnicima konfiguriranje programa Anti-Theft i administriranje anti-theft značajki na uređaju.
Roditeljska kontrola	Štiti vašu obitelj od potencijalno uvredljivih web sadržaja blokirajući razne kategorije web stranica.

Da bi značajke programa ESET Internet Security funkcionirale, licenca mora biti aktivna. Preporučuje se da licencu za ESET Internet Security obnovite nekoliko tjedana prije isteka.

Novosti

Što je novo u ESET Internet Security 15

Poboljšana Mrežna provjera (prijašnja Kućna mreža)

Pomaže u zaštiti mreže i uređaja interneta stvari te prikazuje uređaje povezane na router. Saznajte kako provjeriti mreže koje upotrebljavate i koji su uređaji povezani.

ESET HOME (prijašnji myESET)

Osigurava veću vidljivost i kontrolu nad vašom sigurnosti. Instalirajte zaštitu za nove uređaje, dodajte i dijelite licence i primajte važne obavijesti pomoću mobilne aplikacije i web-portala. Za više informacija proučite priručnik online pomoći za ESET HOME.

Poboljšani sistem za sprječavanje upada (HIPS)

Skenira memorijska područja koja mogu mijenjati sofisticirane tehnike ubrizgavanja zlonamjernih programa. Poboljšanja proširuju njegovu tehnološku sposobnost otkrivanja najsofisticiranijih upada zlonamjernih programa.

Slike i dodatne informacije o novim funkcijama programa ESET Internet Security potražite u odjeljku Što je novo u najnovijoj verziji ESET-ovih programa za kućne korisnike.

> Da biste deaktivirali **Obavijesti o novostima**, kliknite **Napredno podešavanje** > **Obavijesti** > **Obavijesti na radnoj površini**. Kliknite **Uredi** pored **Obavijesti na radnoj površini** i poništite odabir potvrdnog okvira **Prikaži obavijesti o novostima**. Za više informacija o obavijestima pogledajte odjeljak Obavijesti.

Koji program imam?

ESET nudi više slojeva sigurnosti s novim programima od snažnih i brzih antivirusnih rješenja do cjelovitih sigurnosnih rješenja s minimalnom razinom utjecaja na rad sustava:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Kako biste utvrdili koji vam je program instaliran, otvorite glavni prozor programa i vidjet ćete naziv programa na vrhu prozora (pročitajte članak u ESET-ovoj bazi znanja).

U tablici u nastavku navode se značajke dostupne u svakom pojedinom programu.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Modul detekcije	✔	✔	✔
Napredno strojno učenje	✔	✔	✔
Sprječavanje ranjivosti	✔	✔	✔
Zaštita od napada na temelju skripti	✔	✔	✔
Anti-Phishing	✔	✔	✔
zaštita web pristupa	✔	✔	✔
HIPS (uključujući Zaštitu od ransomwarea)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Mrežna provjera		✔	✔
Zaštita web-kamere		✔	✔
Zaštita od mrežnog napada		✔	✔
Zaštita od botneta		✔	✔
Zaštita bankarstva i plaćanja		✔	✔
Roditeljska kontrola		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Neki od prethodno navedenih programa možda nisu dostupni za vaš jezik/regiju.

Sistemski preduvjeti

Vaš sustav mora ispunjavati sljedeće zahtjeve hardvera i softvera kako bi program ESET Internet Security optimalno radio:

Podržani procesori

Intel ili AMD procesor, 32-bitni (x86) sa skupom uputa SSE2 ili 64-bitni (x64), 1 GHz ili više
Procesor ARM64, 1 GHz ili više

Podržani operacijski sustavi*

Microsoft® Windows® 11

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1 s najnovijim nadogradnjama za sustav Windows
Microsoft® Windows® Home Server 2011 64-bit

Pobrinite se da je vaš operacijski sustav nadograđen.

Anti-Theft ne podržava Microsoft Windows Home Server.

Ostalo

Potrebna je internetska veza da bi aktivacija i nadogradnja programa ESET Internet Security pravilno funkcionirale.

Dva antivirusna programa koja su istovremeno pokrenuta na jednom uređaju uzrokuju neizbježne sukobe upotrebe resursa sustava, kao što je usporavanje sustava zbog kojeg on postaje neupotrebljiv.

* ESET od veljače 2021. ne pruža zaštitu za operacijske sustave koji nisu podržani.

Vaša verzija sustava Windows 7 je zastarjela

Problem

Upotrebljavate zastarjelu verziju operacijskog sustava. Da biste ostali zaštićeni, pobrinite se da je vaš operacijski sustav nadograđen.

Rješenje

Instalirali ste ESET Internet Security koji se pokreće u sustavu {GET_OSNAME} {GET_BITNESS}.

Provjerite jeste li instalirali servisni paket 1 (SP1) za Windows 7 s najnovijim nadogradnjama za Windows (barem KB4474419 i KB4490628).

Ako Windows 7 nije konfiguriran za automatsku nadogradnju, kliknite **Izbornik Start** > **Upravljačka ploča** > **Sustav i sigurnost** > **Windows Update** > **Provjera dostupnosti nadogradnji**, a zatim kliknite **Instaliraj nadogradnje**.

Također pogledajte odjeljak Microsoft više ne podržava Windows 7.

Microsoft više ne podržava Windows 7

Problem

Microsoftova podrška za Windows 7 završila je 14. siječnja 2020. Što to znači?

Ako nastavite upotrebljavati Windows 7 nakon završetka podrške, vaše računalo i dalje će funkcionirati, ali bi moglo biti izloženije sigurnosnim rizicima i virusima. Računalo više neće primati nadogradnje za Windows

(uključujući sigurnosne nadogradnje).

Rješenje

Nadogradnja sa sustava Windows 7 na Windows 10? Nadogradite ESET-ov program

Postupak nadogradnje je relativno jednostavan, a u mnogim slučajevima to možete učiniti bez gubitka datoteka. Prije nadogradnje na Windows 10:

1. Provjerite/nadogradite ESET-ov program
2. Sigurnosno kopiranje važnih podataka
3. Pročitajte česta pitanja u vezi s nadogradnjom sustava na Windows 10 tvrtke Microsoft i nadogradite svoj operacijski sustav Windows

Kupnja novog računala ili uređaja? Prenesite ESET-ov program

Ako ste kupili novo računalo ili uređaj ili to planirate učiniti, saznajte kako prenijeti postojeći ESET-ov program na novi uređaj.

Pogledajte i odjeljak Podrška za Windows 7 je završila.

Windows Vista više nije podržan

Problem

Zbog tehničkih ograničenja sustava Windows Vista, ESET Internet Security neće moći pružati zaštitu nakon **veljače 2021**. ESET-ov program **neće više funkcionirati**. To može uzrokovati ranjivost vašeg sustava na infiltracije.

Microsoftova podrška za sustav Windows Vista završila je 11. travnja 2017. Što to znači?

Ako nastavite upotrebljavati Windows Vista nakon završetka podrške, vaše računalo i dalje će funkcionirati, ali bi moglo biti izloženije sigurnosnim rizicima i virusima. Računalo više neće primati nadogradnje za Windows (uključujući sigurnosne nadogradnje).

Rješenje

Nadograđujete sustav Windows Vista na Windows 10? Nabavite novo računalo ili uređaj i prenesite ESET-ov program.

Prije nadogradnje na Windows 10:

1. Sigurnosno kopiranje važnih podataka
2. Pročitajte česta pitanja u vezi s nadogradnjom sustava na Windows 10 tvrtke Microsoft i nadogradite svoj operacijski sustav Windows
3. Instalirajte ili prenesite postojeći ESET-ov program na novi uređaj.

Pogledajte i odjeljak Podrška za Windows Vista je završila.

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 istraživanje tvrtke ESET svakodnevno analiziraju te prijetnje te pripremaju i izdaju nadogradnje 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 poglavlju 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 objavljuju sigurnosne aktualizacije za uklanjanje potencijalnih prijetnji. Važno je da takve sigurnosne nadogradnje preuzmete odmah nakon objavljivanja. Microsoft Windows i web preglednici poput sustava Internet Explorer primjeri su programa za koje se redovno objavljuju sigurnosne nadogradnje.

Sigurnosno kopiranje važnih podataka

Autore zlonamjernog softvera obično nije briga za potrebe korisnike, 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 pojednostavniti 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 mjesečno 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

Dobro došli u korisnički vodič za ESET Internet Security. Ovdje navedene informacije upoznat će vas s proizvodom i učiniti vaš rad na računalu sigurnijim.

Početak korištenja

Preporučujemo vam da se prije upotrebe programa ESET Internet Security upoznate s raznim vrstama otkrivenih prijetnji i udaljenih napada na koje biste mogli naići prilikom upotrebe računala.

Sastavili smo i popis novih značajki uvedenih u program ESET Internet Security i vodič za konfiguriranje osnovnih postavki.

Korištenje stranica pomoći programa ESET Internet Security

Teme pomoći podijeljene su u nekoliko poglavlja i potpoglavlja. Pritisnite **F1** za prikaz informacija o prozoru u kojem se trenutačno nalazite.

Program omogućuje da tražite neku temu pomoći prema ključnim riječima ili tražite sadržaj upisivanjem riječi ili izraza. Razlika između te dvije metode je u tome da se ključna riječ može logički povezati sa stranicama pomoći koje ne sadrže samu 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 samom tekstu.

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

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
Podebljan tekst	Nazivi stavki sučelja kao što su okviri i gumbi opcija.
Kosa slova	Rezervirana mjesta za informacije koje pružate. Na primjer, naziv datoteke ili put znači da morate upisati stvarni put ili naziv datoteke.
`Courier New`	Uzorci koda ili naredbe.

Konvencija	Značenje
Hiperveza	Omogućuje brz i jednostavan pristup temama na koje se unakrsno referira ili vanjskoj web-lokaciji. Hiperveze su plave boje i mogu biti podcrtane.
%ProgramFiles%	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.

Instalacija

Program ESET Internet Security na računalo možete instalirati na nekoliko načina. Načini instalacije su različiti i ovise o zemlji i načinu distribucije:

- Live Installer – preuzima se s ESET-ove web stranice ili CD-a/DVD-a. Instalacijski paket je univerzalan za sve jezike (odaberite odgovarajući jezik). Live Installer je mala datoteka, a dodatne datoteke potrebne za instalaciju programa ESET Internet Security automatski se preuzimaju.

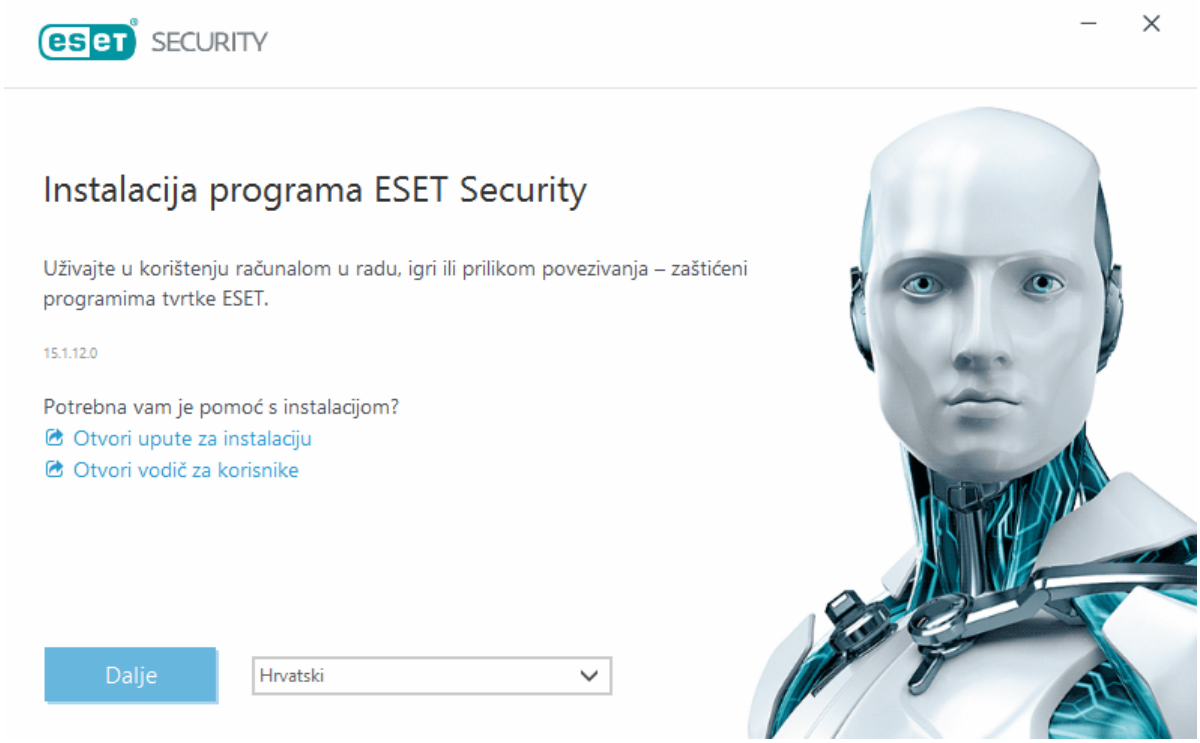
- Izvanmrežna instalacija – upotrebljava .exe datoteku veću od datoteke za Live Installer i ne zahtijeva internetsku vezu ili dodatne datoteke za dovršetak instalacije.

Prije instalacije programa ESET Internet Security provjerite da na računalu nije 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. Popis alata za deinstalaciju za uobičajen antivirusni softver potražite u našem članku ESET baze znanja (dostupan na engleskom i nekoliko drugih jezika).

Internetski instalacijski program

Nakon što preuzmete instalacijski paket Live Installer, dvokliknite instalacijsku datoteku i slijedite detaljne upute iz čarobnjaka za instalaciju.

Za ovu vrstu instalacije morate biti povezani na internet.



1. Odaberite odgovarajući jezik u padajućem izborniku i kliknite **Dalje**.

Ako instalirate noviju verziju u odnosu na prethodnu verziju s postavkama zaštićenima lozinkom, upišite lozinku. Lozinku za postavke možete konfigurirati u kartici Podešavanje pristupa.

2. Odaberite svoje preference za sljedeće funkcije, pročitajte Licenčni ugovor za krajnjeg korisnika i Pravila privatnosti i kliknite **Nastavi** ili kliknite **Dopusti sve i nastavi** kako biste aktivirali sve funkcije:

- Sustav za povratne informacije ESET LiveGrid®
- Potencijalno nepoželjne aplikacije
- Program za poboljšanje iskustva korisnika

Ako kliknete **Nastavi** ili **Prihvati i nastavi**, prihvaćate Licenčni ugovor za krajnjeg korisnika i potvrđujete da ste suglasni s Pravilima privatnosti.

3. Da biste aktivirali zaštitu uređaja, upravljali njome te je pregledavali s pomoću programa ESET HOME, povežite svoj uređaj s ESET HOME računom. Kliknite **Preskoči prijavu** da biste nastavili bez povezivanja s ESET HOME računom. Uređaj kasnije možete povezati s ESET HOME računom.

4. Ako nastavite bez povezivanja s ESET HOME računom, odaberite opciju aktivacije. Ako instalirate noviju verziju preko prethodne, licenčni ključ se automatski unosi.

5. Čarobnjak za instalaciju određuje koji će se ESET-ov program instalirati na temelju vaše licence. Uvijek se unaprijed odabire verzija s najviše sigurnosnih funkcija. Kliknite **Promijeni program** ako želite instalirati drugu verziju ESET-ova programa. Kliknite **Nastavi** da biste pokrenuli postupak instalacije. To bi moglo potrajati nekoliko trenutaka.

Ako postoje ostaci (datoteke ili mape) iz ESET-ovih programa deinstaliranih u prošlosti, od vas će se zatražiti da dopustite njihovo uklanjanje. Kliknite **Instaliraj** za nastavak.

6. Kliknite **Gotovo** za izlazak iz čarobnjaka za instalaciju.

Alat za otklanjanje poteškoća s instalacijom.

Nakon što se program instalira i aktivira, počinje preuzimanje modula. Zaštita se pokreće i neke funkcije možda neće biti potpuno funkcionalne ako preuzimanje nije dovršeno.

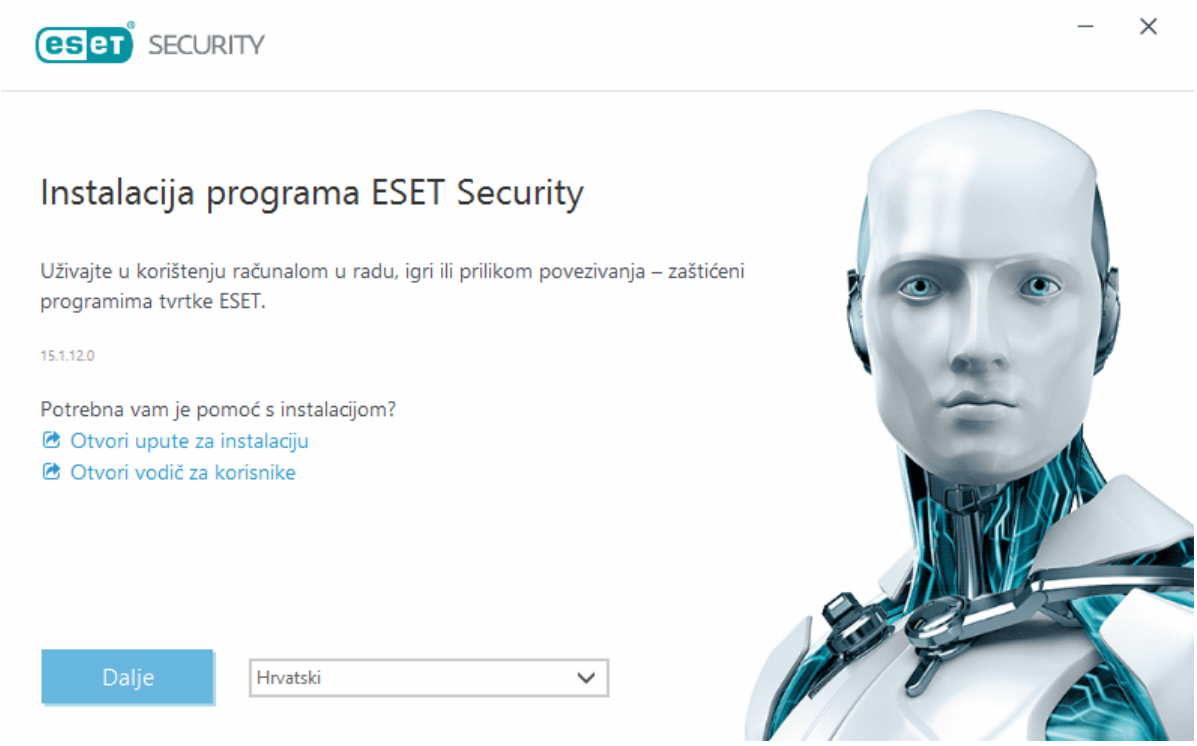
Izvanmrežna instalacija

Preuzmite i instalirajte ESET-ov Windows program za kućnu upotrebu pomoću izvanmrežnog instalacijskog programa (.exe) u nastavku. Odaberite koju verziju ESET HOME programa želite preuzeti (32-bitni, 64-bitni ili ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Preuzimanje 64-bitne verzije Preuzimanje 32-bitne verzije ARM preuzimanje	Preuzimanje 64-bitne verzije Preuzimanje 32-bitne verzije ARM preuzimanje	Preuzimanje 64-bitne verzije Preuzimanje 32-bitne verzije ARM preuzimanje

Ako imate aktivnu internetsku vezu, instalirajte ESET-ov program pomoću datoteke Live Installer.

Kada pokrenete izvanmrežni instalacijski program (.exe), čarobnjak za instalaciju provest će vas kroz proces podešavanja.



1. Odaberite odgovarajući jezik u padajućem izborniku i kliknite **Dalje**.

Ako instalirate noviju verziju u odnosu na prethodnu verziju s postavkama zaštićenima lozinkom, upišite lozinku. Lozinku za postavke možete konfigurirati u kartici Podešavanje pristupa.

2. Odaberite svoje preference za sljedeće funkcije, pročitajte Licenčni ugovor za krajnjeg korisnika i Pravila privatnosti i kliknite **Nastavi** ili kliknite **Dopusti sve i nastavi** kako biste aktivirali sve funkcije:

- Sustav za povratne informacije ESET LiveGrid®
- Potencijalno nepoželjne aplikacije
- Program za poboljšanje iskustva korisnika

Ako kliknete **Nastavi** ili **Prihvati i nastavi**, prihvaćate Licenčni ugovor za krajnjeg korisnika i potvrđujete da ste suglasni s Pravilima privatnosti.

3. Kliknite **Preskoči prijavu**. Kada uspostavite internetsku vezu, možete povezati uređaj s ESET HOME računom.

4. Kliknite **Preskoči aktivaciju**. ESET Internet Security se mora aktivirati nakon instalacije kako bi bio u potpunosti funkcionalan. Aktivacija programa zahtijeva aktivnu internetsku vezu.

5. Čarobnjak za instalaciju pokazuje koji će se ESET-ov program instalirati na temelju preuzetog izvanmrežnog instalacijskog programa. Kliknite **Nastavi** da biste pokrenuli postupak instalacije. To bi moglo potrajati nekoliko trenutaka.

Ako postoje ostaci (datoteke ili mape) iz ESET-ovih programa deinstaliranih u prošlosti, od vas će se zatražiti da dopustite njihovo uklanjanje. Kliknite **Instaliraj** za nastavak.

6. Kliknite **Gotovo** za izlazak iz čarobnjaka za instalaciju.

Alat za otklanjanje poteškoća s instalacijom.

Aktivacija proizvoda

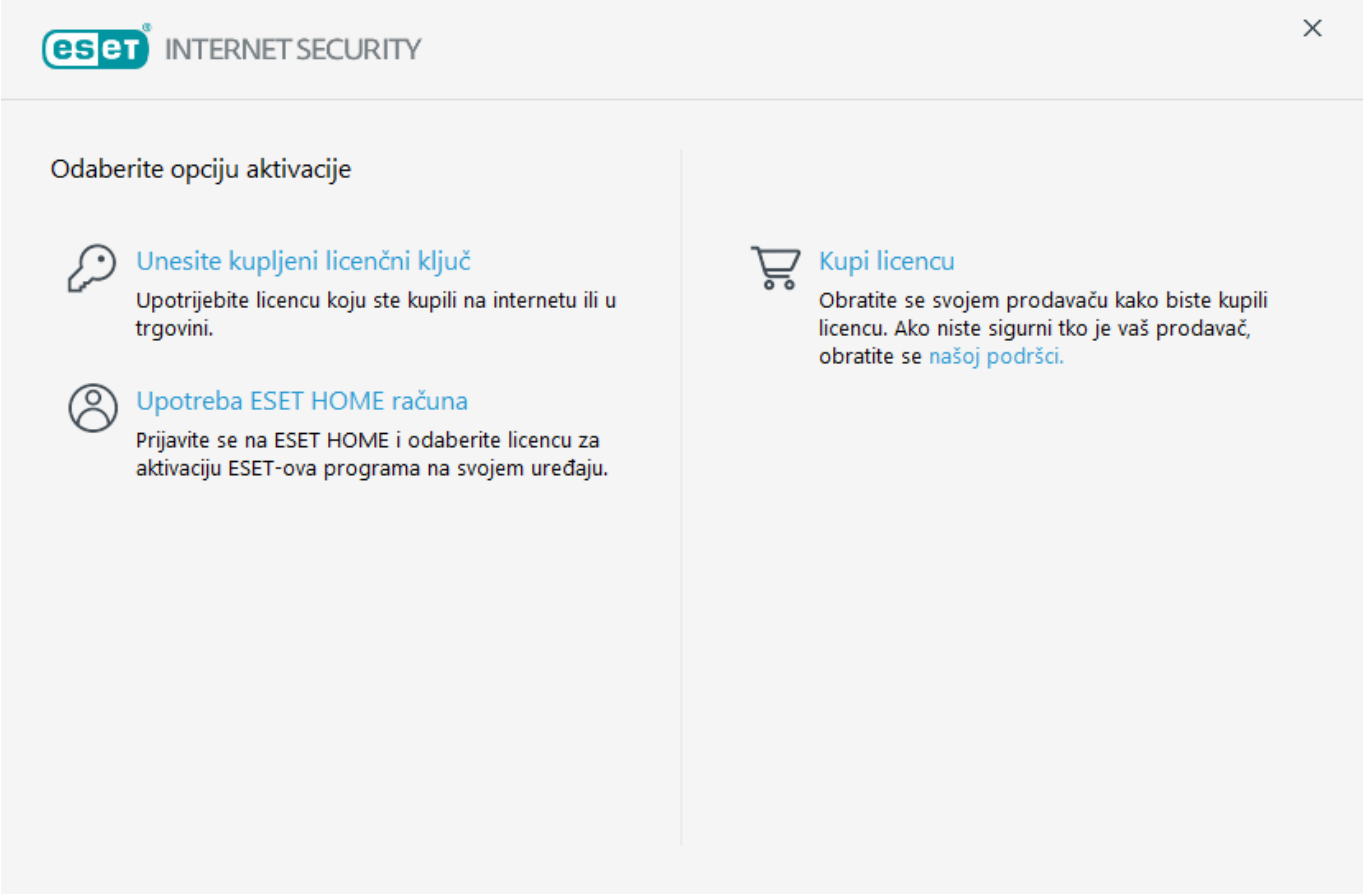
Svoj program možete aktivirati na nekoliko načina. Dostupnost određenog scenarija aktivacije u prozoru aktivacije ovisi o zemlji i načinu distribucije instalacijske datoteke (CD/DVD, ESET web stranice, itd.):

- Ako ste kupili maloprodajnu verziju proizvoda u kutiji ili primili e-poruku s podacima o licenci, aktivirajte program tako da kliknete na **Upotrijebi kupljeni licenčni ključ**. Licenčni ključ obično se nalazi u samom paketu programa ili na njegovoj poleđini. Da bi aktivacija uspjela, licenčni ključ mora biti točno unesen. Licenčni ključ – jedinstven niz u formatu XXXX-XXXX-XXXX-XXXX-XXXX ili XXXX-XXXXXXXX koji se upotrebljava za identifikaciju vlasnika licence i aktivaciju licence.
- Nakon odabira opcije Korištenje ESET HOME računa od vas će se tražiti da se prijavite u svoj ESET HOME račun.
- Ako želite isprobati program ESET Internet Security prije kupnje, odaberite Besplatna probna licenca. Unesite svoju adresu e-pošte da biste aktivirali program ESET Internet Security na ograničen vremenski rok. Vaša probna licenca bit će vam poslana e-poštom. Probne licence mogu se aktivirati samo jednom po korisniku.
- Ako nemate licencu, a željeli biste je kupiti, kliknite mogućnost **Kupi licencu**. To će vas preusmjeriti na web stranice vašeg lokalnog distributera tvrtke ESET. Pune licence za ESET-ov Windows program za kućnu upotrebu nisu besplatne.

Licencu programa možete promijeniti u svakom trenutku. Samo kliknite **Pomoć i podrška** > **Promijeni licencu** u glavnom prozoru programa. Prikazat će se javni ID licence koji se upotrebljava za identifikaciju vaše licence kod korisničke podrške tvrtke ESET.

Ako imate korisničko ime i lozinku za aktivaciju starijih ESET programa i ne znate kako aktivirati program ESET Internet Security, pretvorite svoje naslijeđene korisničke podatke u licenčni ključ.

Aktivacija programa nije uspjela?



Unos Licenčnog ključa prilikom aktivacije

Automatske nadogradnje važne su za vašu sigurnost. ESET Internet Security primit će nadogradnje koje su aktivirane.

Prilikom unosa **Licenčnog ključa** važno je upisati ga točno onako kako piše:

- Licenčni 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 licenčni ključ kopirate i zalijepite iz e-pošte koju ste dobili prilikom registracije.

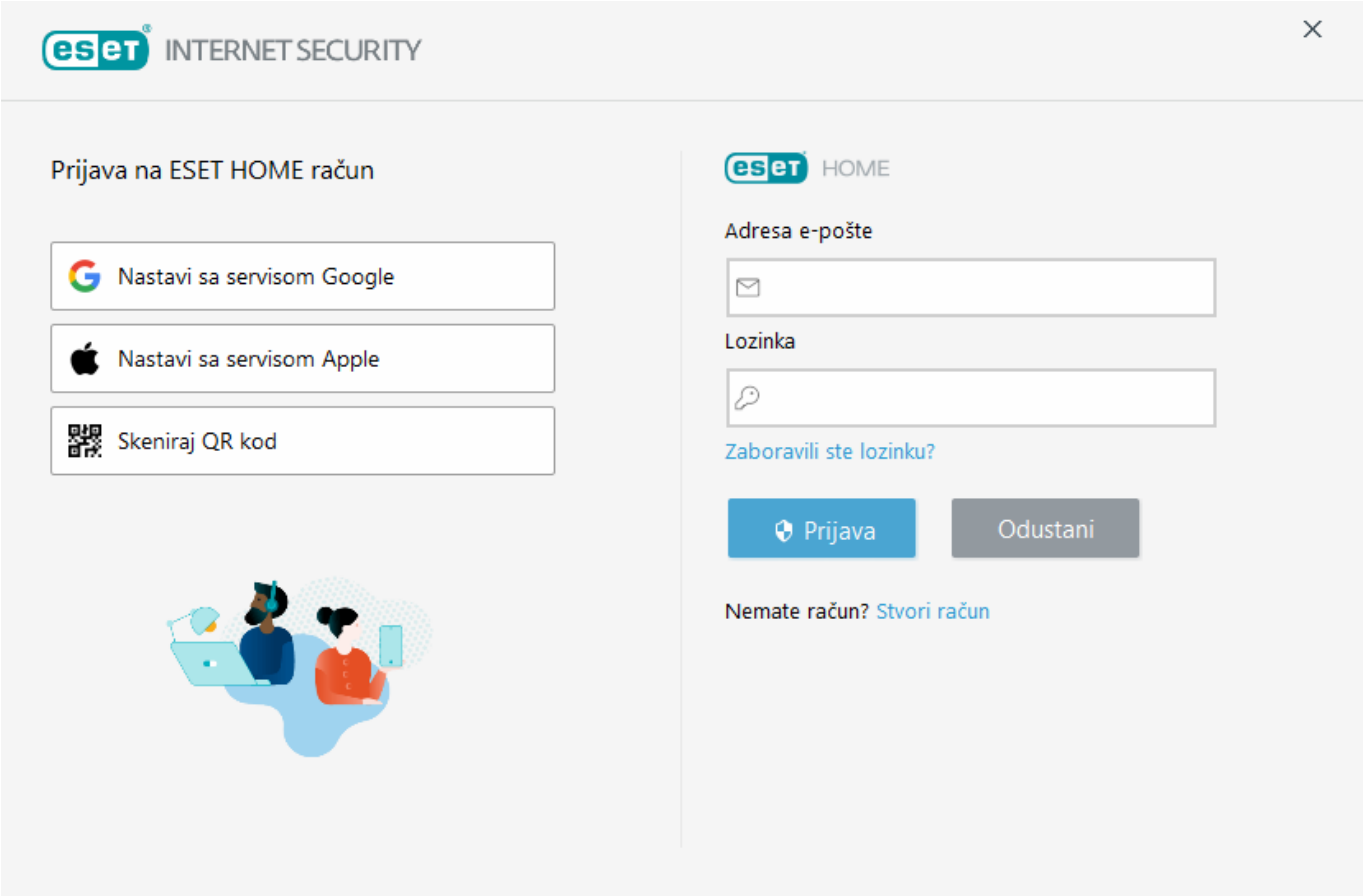
Ako nakon instalacije niste unijeli licenčni ključ, program se neće aktivirati. Aktivirati program ESET Internet Security možete uglavnom prozoru programa > **Pomoć i podrška** > **Aktiviraj licencu**.

Pune licence za ESET-ov Windows program za kućnu upotrebu nisu besplatne.

Korištenje ESET HOME računa

Povežite svoj uređaj s ESET HOME računom da biste pregledali sve aktivirane ESET-ove licence i uređaje te upravljali njima. Možete obnoviti, nadograditi ili produljiti licencu i pregledati važne pojedinosti o licenci. Na

portalu za upravljanje ili u mobilnoj aplikaciji ESET HOME možete uređivati postavke za Anti-Theft, dodavati različite licence, preuzimati programe na svoje uređaje, provjeravati sigurnosni status programa ili dijeliti licence putem e-pošte. Dodatne informacije potražite na stranicama mrežne pomoći za ESET HOME.



Nakon odabira opcije **Korištenje ESET HOME računa** kao metode aktivacije ili prilikom povezivanja s ESET HOME računom tijekom instalacije učinite sljedeće:

1. Prijavite se na svoj račun ESET HOME.

> Ako nemate ESET HOME račun, kliknite **Stvori račun** da biste se registrirali ili proučite upute u online pomoći za ESET HOME.
> Ako ste zaboravili lozinku, kliknite **Zaboravio/la sam lozinku** i slijedite korake na zaslonu ili proučite upute u online pomoći za ESET HOME.

2. Postavite **Naziv uređaja** za svoj uređaj koji će se upotrebljavati za sve ESET HOME servise i kliknite **Dalje**.

3. Odaberite licencu za aktivaciju ili dodajte novu licencu. Kliknite **Dalje** da biste aktivirali ESET Internet Security.

Aktivacija probne licence

Da biste aktivirali probnu verziju programa ESET Internet Security, unesite valjanu adresu e-pošte u polja **Adresa e-pošte** i **Potvrdi adresu e-pošte**. Nakon aktivacije, ESET-ova licenca će se generirati i poslati na vašu adresu e-pošte. Ova adresa e-pošte će se također upotrebljavati za obavijesti o isteku programa i za ostalu komunikaciju s tvrtkom ESET. Probna verzija se može aktivirati samo jednom.

S padajućeg izbornika **Zemlja** odaberite svoju zemlju da biste registrirali program ESET Internet Security kod

svojeg lokalnog distributera koji će vam osigurati tehničku podršku.

Besplatan ESET-ov licenčni ključ

Puna licenca za ESET Internet Security nije besplatna.

ESET-ov licenčni ključ je jedinstven niz slova i brojeva koji su odvojeni crticom, a tvrtka ESET ga pruža da bi se omogućila zakonita upotreba programa ESET Internet Security u skladu s Licenčnim ugovorom za krajnjeg korisnika. Svaki krajnji korisnik ima pravo upotrebljavati licenčni ključ samo u mjeri u kojoj ima pravo upotrebljavati program ESET Internet Security na temelju broja licenci koje je dodijelila tvrtka ESET. Licenčni ključ se smatra povjerljivim i ne može se dijeliti; međutim, možete podijeliti računala s licencom s pomoću ESET HOME.

Na internetu postoje izvori koji vam mogu pružiti „besplatne" ESET-ove licenčne ključeve, no zapamtite:

- Ako kliknete oglas "Besplatna licenca tvrtke ESET", može se ugroziti vaše računalo ili uređaj i to može dovesti do zaraze zlonamjernim programima. Zlonamjerni programi mogu biti skriveni u neslužbenom web sadržaju (npr. u videozapisima), na web stranicama koje prikazuju oglase da bi zaradile novac na temelju vaših posjeta itd. Obično se radi o zamkama.

- ESET može deaktivirati piratizirane licence te to i čini.

- Posjedovanje piratskog licenčnog ključa nije u skladu s Licenčnim ugovorom za krajnjeg korisnika koji morate prihvatiti da biste instalirali program ESET Internet Security.

- Kupujte licence tvrtke ESET samo putem službenih kanala, kao što je www.eset.com, distributera ili prodavača tvrtke ESET (nemojte kupovati licence s neslužbenih web-stranica treće strane kao što je eBay ili zajedničke licence od treće strane).

- Preuzimanje ESET Internet Security je besplatno, no za aktivaciju tijekom instalacije potreban je važeći ESET-ov licenčni ključ (možete ga preuzeti i instalirati, no bez aktivacije neće funkcionirati).

- Nemojte dijeliti svoju licencu na internetu ili društvenim mrežama (može se proširiti).

Upute za identifikaciju i prijavu piratizirane licence tvrtke ESET potražite u članku naše baze znanja.

Ako niste sigurni u kupnju ESET-ova sigurnosnog programa, možete upotrebljavati probnu verziju dok odlučujete:

1. Aktivirajte ESET Internet Security upotrebom besplatne probne licence

2. Sudjelujte u ESET-ovu BETA programu

3. Instalirajte ESET Mobile Security ako upotrebljavate mobilni uređaj sa sustavom Android, radi se o freemium verziji.

Da biste dobili popust / produljili licencu:

- preporučite ESET Internet Security prijatelju

- obnovite ESET (ako ste prije imali aktivnu licencu) ili aktivirajte na dulje razdoblje

Aktivacija nije uspjela – česti slučajevi

Ako aktivacija programa ESET Internet Security nije uspješna, to se najčešće događa zbog sljedećeg:

- Licenčni ključ je već u upotrebi
- Licenčni ključ nije valjan. Pogreška obrasca za aktivaciju proizvoda
- Dodatne informacije potrebne za aktivaciju nedostaju ili nisu valjane.
- 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 i ponovno pokušajte aktivirati program. Ako upotrebljavate ESET HOME račun za aktivaciju, pogledajte odjeljak ESET HOME Upravljanje licencama – pomoć na mreži.

Ako i dalje ne možete aktivirati program, ESET-ov alat za otklanjanje poteškoća pri aktivaciji vodi vas kroz česta pitanja, pogreške i probleme koji se odnose na aktivaciju i licenciranje (dostupno na engleskom jeziku i nekoliko ostalih jezika).

Aktivacija nije uspjela jer je licenca prekomjerno iskorištena

Problem

- Vaša licenca je možda prekomjerno iskorištena ili se zloupotrebljava
- Aktivacija nije uspjela jer je licenca prekomjerno iskorištena

Rješenje

Ovu licencu upotrebljava više uređaja od dopuštenog. Možda ste žrtva piratstva ili krivotvorenja softvera. Ova se licenca ne može upotrijebiti za aktivaciju drugih ESET-ovih programa. Ovaj problem možete izravno riješiti ako vam je dozvoljeno upravljati ovom licencom na vašem ESET HOME računu ili ako ste kupili licencu iz legitimnog izvora. Ako nemate račun, izradite ga.

Ako ste vlasnik licence i od vas se nije tražilo da unesete svoju adresu e-pošte:

1. Da biste upravljali ESET-ovom licencom, otvorite web preglednik i idite na https://home.eset.com. Pristupite opciji ESET License Manager i uklonite ili deaktivirajte računala. Više informacija potražite u odjeljku Što učiniti u slučaju prekomjerno iskorištene licence.

2. Upute za identifikaciju i prijavu piratizirane licence tvrtke ESET potražite u našem članku Identifikacija i prijava piratizirane licence tvrtke ESET.

3. Ako niste sigurni, kliknite **Natrag** i pošaljite poruku e-pošte ESET-ovoj tehničkoj podršci.

Ako niste vlasnik licence, obratite se vlasniku ove licence i obavijestite ga da ne možete aktivirati ESET-ov program zbog prekomjerne iskorištenosti licence. Vlasnik može riješiti problem na ESET HOME portalu.

Ako se od vas zatraži da potvrdite adresu e-pošte (samo u nekim slučajevima), unesite adresu e-pošte koju ste upotrijebili prilikom kupnje ili aktivacije programa ESET Internet Security.

Nadogradnja licence

Ovaj prozor s obavijestima se prikazuje kada se licenca koja se upotrijebila za aktivaciju ESET-ovog programa promijenila. Vaša promijenjena licenca omogućuje vam da aktivirate program s više sigurnosnih funkcija. Ako nije došlo do promjene, u programu ESET Internet Security će se jednom prikazati upozorenje koje se naziva **Promjena u program s više funkcija**.

Da (preporučeno) – automatski će se instalirati program s više sigurnosnih funkcija.

Ne, hvala – nikakve promjene neće biti izvršene, a obavijest će trajno nestati.

Da biste kasnije promijenili program, pročitajte naš članak u ESET-ovoj bazi znanja. Za više informacija o ESET-ovim licencama pogledajte Najčešća pitanja o licenciranju.

U tablici u nastavku navode se značajke dostupne u svakom pojedinom programu.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Modul detekcije	✔	✔	✔
Napredno strojno učenje	✔	✔	✔
Sprječavanje ranjivosti	✔	✔	✔
Zaštita od napada na temelju skripti	✔	✔	✔
Anti-Phishing	✔	✔	✔
zaštita web pristupa	✔	✔	✔
HIPS (uključujući Zaštitu od ransomwarea)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Mrežna provjera		✔	✔
Zaštita web-kamere		✔	✔
Zaštita od mrežnog napada		✔	✔
Zaštita od botneta		✔	✔
Zaštita bankarstva i plaćanja		✔	✔
Roditeljska kontrola		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Nadogradnja programa

Preuzeli ste standardni instalacijski program i odlučili promijeniti program aktivacijom ili želite zamijeniti instalirani program za program s više sigurnosnih funkcija.

Promijenite program tijekom instalacije.

U tablici u nastavku navode se značajke dostupne u svakom pojedinom programu.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Modul detekcije	✔	✔	✔
Napredno strojno učenje	✔	✔	✔
Sprječavanje ranjivosti	✔	✔	✔
Zaštita od napada na temelju skripti	✔	✔	✔
Anti-Phishing	✔	✔	✔
zaštita web pristupa	✔	✔	✔
HIPS (uključujući Zaštitu od ransomwarea)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Mrežna provjera		✔	✔
Zaštita web-kamere		✔	✔
Zaštita od mrežnog napada		✔	✔
Zaštita od botneta		✔	✔
Zaštita bankarstva i plaćanja		✔	✔
Roditeljska kontrola		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Prebacivanje licence na stariju verziju

Ovaj dijaloški prozor se prikazuje kada se licenca koja se upotrijebila za aktivaciju ESET-ovog programa promijenila. Vaša promijenjena licenca može se upotrebljavati samo s drugim ESET-ovim programom s manje sigurnosnih funkcija. Program je automatski promijenjen da bi se spriječio gubitak zaštite.

Za više informacija o ESET-ovim licencama pogledajte Najčešća pitanja o licenciranju.

U tablici u nastavku navode se značajke dostupne u svakom pojedinom programu.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Modul detekcije	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Napredno strojno učenje	✔	✔	✔
Sprječavanje ranjivosti	✔	✔	✔
Zaštita od napada na temelju skripti	✔	✔	✔
Anti-Phishing	✔	✔	✔
zaštita web pristupa	✔	✔	✔
HIPS (uključujući Zaštitu od ransomwarea)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Mrežna provjera		✔	✔
Zaštita web-kamere		✔	✔
Zaštita od mrežnog napada		✔	✔
Zaštita od botneta		✔	✔
Zaštita bankarstva i plaćanja		✔	✔
Roditeljska kontrola		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Prebacivanje programa na stariju verziju

Trenutačno instalirani program ima više sigurnosnih funkcija od onog koji namjeravate aktivirati. Izgubit ćete zaštitu u slučaju krađe i pristup povezanim podacima spremljenima u programu ESET HOME.

U tablici u nastavku navode se značajke dostupne u svakom pojedinom programu.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Modul detekcije	✔	✔	✔
Napredno strojno učenje	✔	✔	✔
Sprječavanje ranjivosti	✔	✔	✔
Zaštita od napada na temelju skripti	✔	✔	✔
Anti-Phishing	✔	✔	✔
zaštita web pristupa	✔	✔	✔
HIPS (uključujući Zaštitu od ransomwarea)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Mrežna provjera		✔	✔
Zaštita web-kamere		✔	✔
Zaštita od mrežnog napada		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Zaštita od botneta		✔	✔
Zaštita bankarstva i plaćanja		✔	✔
Roditeljska kontrola		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Alat za otklanjanje poteškoća s instalacijom

Ako se tijekom instalacije pojave problemi, čarobnjak za instalaciju nudi alat za otklanjanje poteškoća koji rješava problem, ako je moguće.

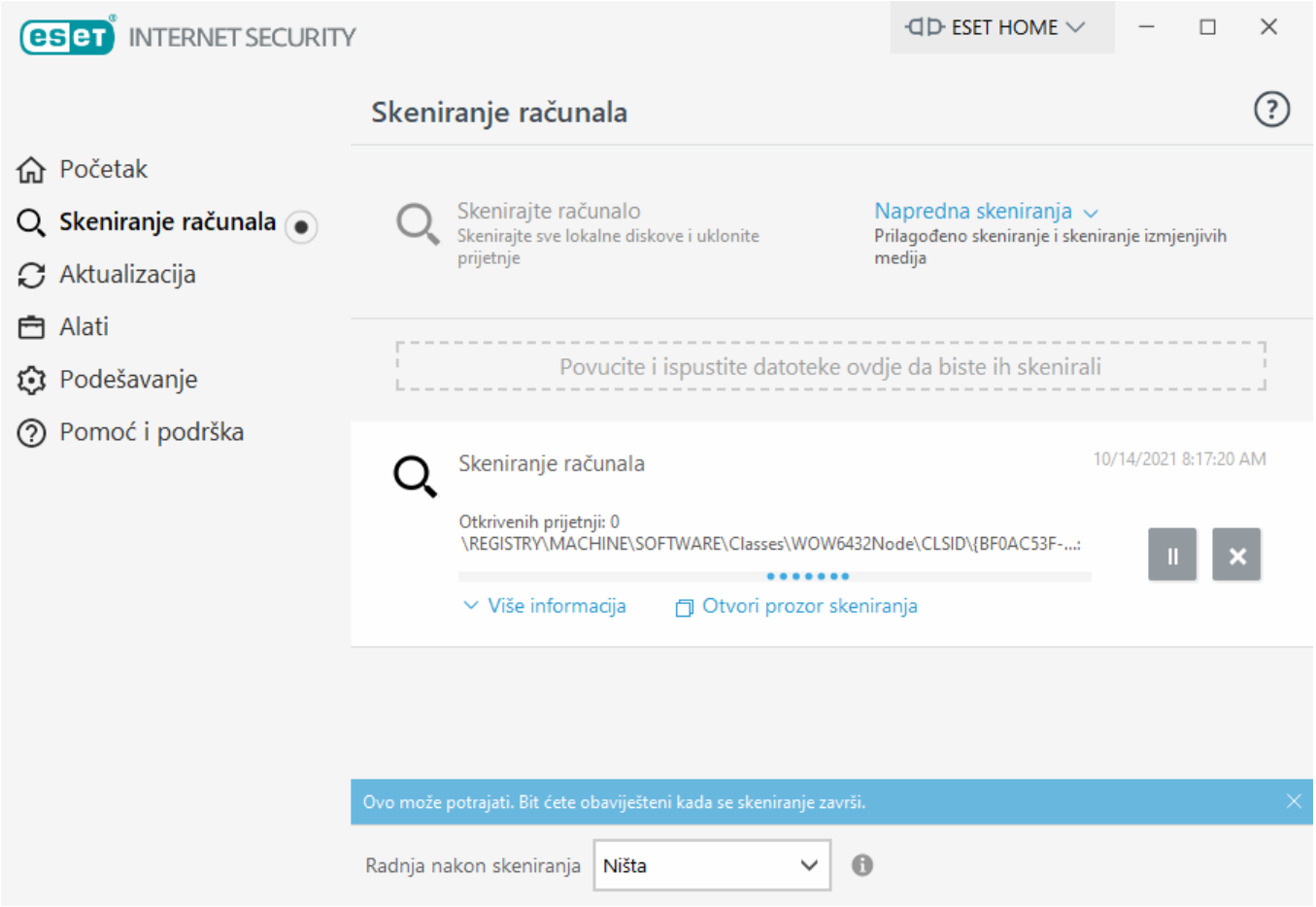
Kliknite **Pokreni alat za otklanjanje poteškoća** da biste pokrenuli alat za otklanjanje poteškoća. Kada alat za otklanjanje poteškoća završi, slijedite preporučeno rješenje.

Ako se problem nastavi pojavljivati, pogledajte popis uobičajenih pogrešaka u instalaciji i rješenja.

Prvo skeniranje nakon instalacije

Nakon što instalirate program ESET Internet Security, skeniranje računala pokrenut će se automatski nakon prve uspješne nadogradnje kako bi se provjerila prisutnost zlonamjernog koda.

Skeniranje računala možete pokrenuti i ručno iz glavnog prozora programa klikom stavke **Skeniranje računala** > **Skenirajte svoje računalo**. Više informacija o skeniranjima računala potražite u odjeljku Skeniranje računala.



Nadogradnja na noviju verziju

Nove verzije programa ESET Internet Security 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 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 omogućili opciju **Nadogradnje funkcija aplikacije** u odjeljku **Napredno podešavanje** (F5) > **Nadogradnja** > **Profili** > **Nadogradnje**.

2. Ručno, u glavnom prozoru programa, klikom na **Potraži nadogradnje** u odjeljku **Aktualizacija**.

3. Ručno preuzimanjem i instaliranjem nove verzije preko prethodne.

Za dodatne informacije i ilustrirane upute pogledajte:

- Nadogradnja ESET-ovih programa – potražite najnovije module programa
- Koje su različite vrste nadogradnji i izdanja programa tvrtke ESET?

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 prihvatili 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® i Program za poboljšanje iskustva korisnika 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.

Preporučivanje ESET-ova programa prijatelju

Ova verzija programa ESET Internet Security sada nudi nagrade za preporuku, tako da možete podijeliti iskustvo upotrebe ESET-ova programa s obitelji i prijateljima. Preporuke možete dijeliti i iz programa aktiviranog s pomoću probne licence. Ako ste korisnik koji rabi probnu licencu, za svaku uspješno poslanu preporuku koja dovede do aktivacije programa vi i vaš prijatelj primit ćete dodatno razdoblje upotrebe probne licence.

Preporuke možete slati s pomoću instaliranog programa ESET Internet Security. Program koji možete preporučiti ovisi o programu iz kojeg šaljete preporuku. Pogledajte tablicu u nastavku.

Vaš instalirani program	Program koji možete preporučiti
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Preporučivanje programa

Da biste poslali pozivni link, kliknite **Preporučite nas prijatelju** u glavnom izborniku programa ESET Internet Security. Kliknite **Podijeli pozivni link**. Program će generirati pozivni link koji će se prikazati u novom prozoru. Kopirajte link i pošaljite ga obitelji i prijateljima. Pozivni link možete podijeliti izravno iz ESET-ova programa uz pomoć opcija **Podijelite na Facebooku**, **Preporučite nas svojim kontaktima u Gmailu** i **Podijelite na Twitteru**.

Kada prijatelj klikne na link za preporuku koji ste mu poslali, bit će preusmjeren na web stranicu na kojoj može preuzeti program i upotrebljavati ga uz jedan dodatan mjesec BESPLATNE zaštite. Kao korisnik koji rabi probnu licencu, primit ćete obavijest za svaki link za preporuku koji se uspješno aktivira, a vaša će se licenca automatski produljiti za jedan dodatan mjesec BESPLATNE zaštite. Na taj način možete produljiti svoju BESPLATNU zaštitu za do 5 mjeseci. Broj uspješno aktiviranih linkova za preporuku možete provjeriti u prozoru **Preporučite nas prijatelju** u ESET-ovu programu.

Funkcija preporuke možda neće biti dostupna za vaš jezik/regiju.

Instalirat će se ESET Internet Security

Ovaj dijaloški prozor može se prikazati:

- Tijekom postupka instalacije – kliknite **Nastavi** da biste instalirali program ESET Internet Security.
- Prilikom promjene licence u programu ESET Internet Security – kliknite **Aktiviraj** da biste promijenili licencu i aktivirali program ESET Internet Security.

Opcija **Promijeni program** omogućuje vam da se prebacujete između ESET-ovih Windows programa za kućnu upotrebu u skladu s ESET-ovom licencom. Pogledajte odjeljak Koji program imam? za više informacija.

Promijeni u drugu vrstu programa

Prema ESET-ovoj licenci, možete se prebacivati između različitih ESET-ovih Windows programa za kućnu upotrebu. Pogledajte odjeljak Koji program imam? za više informacija.

Registracija

Registrirajte svoju licencu ispunjavanjem polja koja se nalaze u obrascu za registraciju i kliknite Aktiviraj. Polja označena u zagradi kao potrebna, su obavezna. Polja u zagradi označena kao potrebna obavezna su. Ovi će se podaci koristiti samo za pitanja povezana s licencom tvrtke ESET.

Napredak aktivacije

Pričekajte nekoliko sekundi da postupak aktivacije završi (potrebno vrijeme može se razlikovati ovisno o brzini internetske veze ili računalu).

Aktivacija je uspješna

Proces aktivacije je završen. Slijedite čarobnjak za korištenje nakon instalacije kako biste dovršili postavljanje programa ESET Internet Security.

Nadogradnja modula započet će za nekoliko sekundi. Redovite nadogradnje programa ESET Internet Security odmah će započeti.

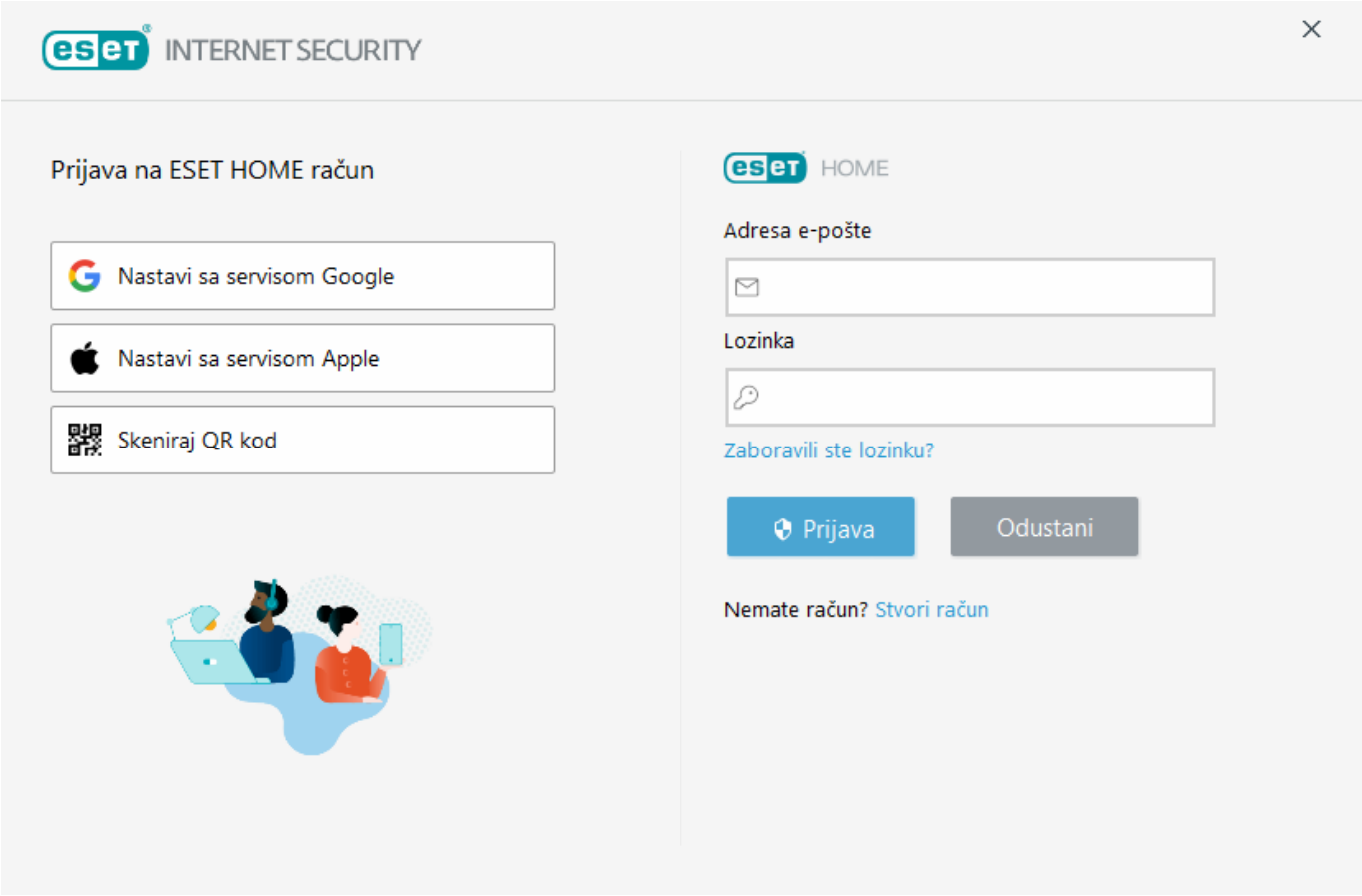
Prvo skeniranje počinje automatski unutar 20 minuta nakon nadogradnje modula.

Vodič za početnike

U ovom poglavlju pronaći ćete uvod u program ESET Internet Security i njegove osnovne postavke.

Povežite se s ESET HOME računom

Povežite svoj uređaj s ESET HOME računom da biste pregledali sve aktivirane ESET-ove licence i uređaje te upravljali njima. Možete obnoviti, nadograditi ili produljiti licencu i pregledati važne pojedinosti o licenci. Na portalu za upravljanje ili u mobilnoj aplikaciji ESET HOME možete uređivati postavke za Anti-Theft, dodavati različite licence, preuzimati programe na svoje uređaje, provjeravati sigurnosni status programa ili dijeliti licence putem e-pošte. Dodatne informacije potražite na stranicama mrežne pomoći za ESET HOME.



Povežite svoj uređaj s programom ESET HOME:

Ako se povezujete s ESET HOME računom tijekom instalacije ili pri odabiru opcije **Upotrijebi ESET HOME račun** kao načina aktivacije, slijedite upute u temi Upotrijebi ESET HOME račun.
Ako ste već instalirali i aktivirali ESET Internet Security putem licence dodane vašem ESET HOME računu, uređaj možete povezati s programom ESET HOME putem portala ESET HOME. Slijedite upute u priručniku online pomoći za ESET HOME i dopustite povezivanje u programu ESET Internet Security.

1. U glavnom prozoru programa kliknite **ESET HOME** > **Poveži se s ESET HOME** računom ili kliknite **Poveži se s ESET HOME** računom u obavijesti **Povežite ovaj uređaj s ESET HOME računom**.

2. Prijavite se na svoj račun ESET HOME.

Ako nemate ESET HOME račun, kliknite **Stvori račun** da biste se registrirali ili proučite upute u online pomoći za ESET HOME.
Ako ste zaboravili lozinku, kliknite **Zaboravio/la sam lozinku** i slijedite korake na zaslonu ili proučite upute u online pomoći za ESET HOME.

3. Postavite **Naziv uređaja** i kliknite **Dalje**.

4. Nakon uspješnog povezivanja prikazuje se prozor s detaljima. Kliknite **Gotovo**.

Prijava u ESET HOME

Postoji nekoliko načina prijave na vaš ESET HOME račun:

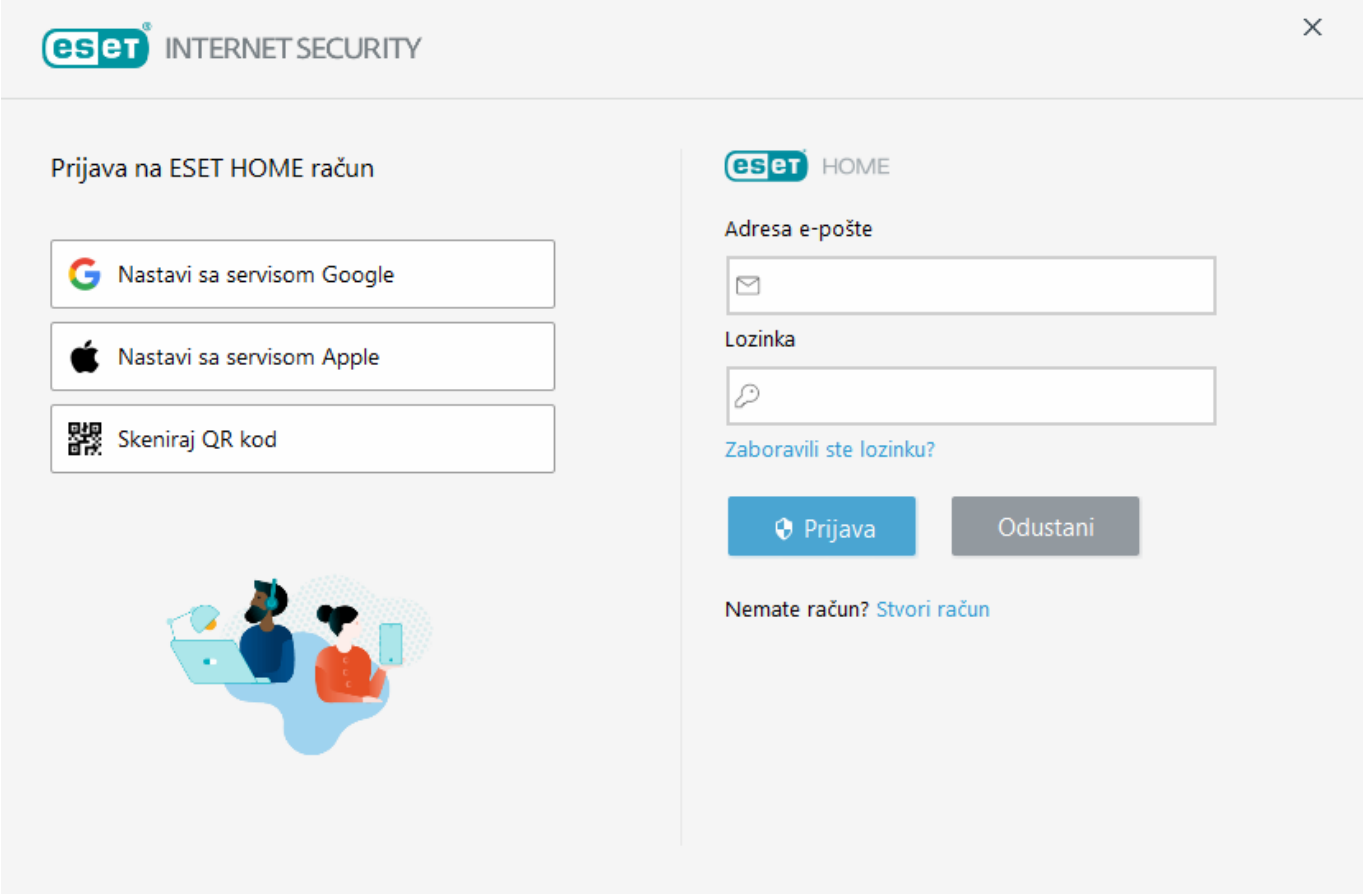
- **Upotrijebite svoj adresu e-pošte i lozinku za ESET HOME** – upišite **adresu e-pošte** i **lozinku** koju ste upotrijebili za stvaranje svojeg ESET HOME računa i kliknite **Prijava**.

- **Upotrijebite svoj račun sa servisa Google / AppleID** – kliknite **Nastavi sa servisom Google** ili **Nastavi sa servisom Apple** i prijavite se u odgovarajući račun. Nakon uspješne prijave bit ćete preusmjereni na stranicu za potvrdu ESET HOME. Za nastavak se prebacite natrag na prozor ESET-ova programa. Za više informacija o prijavi putem računa servisa Google / AppleID pogledajte upute u online pomoći za ESET HOME.

- **Skenirajte QR kôd** – kliknite **Skeniraj QR kôd** za prikaz QR kôda. Otvorite mobilnu aplikaciju ESET HOME i skenirajte QR kôd ili usmjerite kameru uređaja na QR kôd. Dodatne informacije potražite u online pomoći za ESET HOME.

Ako nemate ESET HOME račun, kliknite **Stvori račun** da biste se registrirali ili proučite upute u online pomoći za ESET HOME.
Ako ste zaboravili lozinku, kliknite **Zaboravio/la sam lozinku** i slijedite korake na zaslonu ili proučite upute u online pomoći za ESET HOME.

Prijava nije uspjela – česte pogreške.



Prijava nije uspjela – česte pogreške

Nismo mogli pronaći račun koji odgovara unesenoj adresi e-pošte

Adresa e-pošte koju ste unijeli ne odgovara nijednom ESET HOME računu. Kliknite **Natrag** i upišite ispravnu adresu e-pošte i lozinku.

Da biste se prijavili, morate stvoriti ESET HOME račun. Ako nemate ESET HOME račun, kliknite **Natrag** > **Stvori račun** ili pogledajte Stvaranje novog ESET HOME računa.

Korisničko ime i lozinka se ne podudaraju

Unesena lozinka ne odgovara unesenoj adresi e-pošte. Kliknite **Natrag**, upišite ispravnu lozinku i provjerite je li unesena adresa e-pošte točna. Ako se još uvijek ne možete prijaviti, kliknite **Natrag** > **Zaboravio/la sam lozinku** da biste ponovno postavili lozinku i slijedite korake na zaslonu ili pogledajte Zaboravio/la sam lozinku za ESET HOME.

Odabrana opcija prijave ne odgovara vašem računu

Vaš je račun povezan s vašim računom na društvenim mrežama. Da biste se prijavili na ESET HOME, kliknite **Nastavi sa servisom Google** ili **Nastavi sa servisom Apple** i prijavite se u odgovarajući račun. Nakon uspješne prijave bit ćete preusmjereni na stranicu za potvrdu ESET HOME. Svoj račun na društvenim mrežama možete odspojiti od ESET HOME računa na ESET HOME portalu.

Neispravna lozinka

Ova se pogreška može pojaviti ako je vaš ESET Internet Security već povezan s ESET HOME računom i ako unosite promjene koje zahtijevaju prijavu (na primjer, deaktiviranje opcije anti-theft), a lozinka koju ste unijeli ne odgovara vašem računu. Kliknite **Natrag** i upišite ispravnu lozinku. Ako se još uvijek ne možete prijaviti, kliknite **Natrag** > **Zaboravio/la sam lozinku** da biste ponovno postavili lozinku i slijedite korake na zaslonu ili pogledajte Zaboravio/la sam lozinku za ESET HOME.

Dodavanje uređaja u ESET HOME

Ako ste već instalirali i aktivirali ESET Internet Security putem licence dodane na vaš ESET HOME račun, možete povezati uređaj s programom ESET HOME putem portala ESET HOME:

1. Pošalji zahtjev za povezivanje na uređaj.

2. ESET Internet Security prikazuje dijaloški prozor **Povezivanje ovog uređaja s ESET HOME računom** s nazivom ESET HOME računa. Kliknite **Dopusti** za povezivanje uređaja s navedenim ESET HOME računom.

Ako nema interakcije, zahtjev za povezivanje će se automatski otkazati nakon otprilike 30 minuta.

Glavni programski prozor

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

Ilustrirane upute
Pogledajte naše ilustrirane upute dostupne na engleskom i na još nekoliko jezika za otvaranje glavnog programskog prozora ESET-ovih programa za Windows.

ESET HOME – povežite uređaj s programom ESET HOME. Upotrijebite ESET HOME ako želite pregledati postavke za Anti-Theft i aktivirane ESET-ove licence i uređaje te upravljati njima.

Slijedi opis mogućnosti na glavnom izborniku:

Početni zaslon – Pruža informacije o statusu zaštite programa ESET Internet Security.

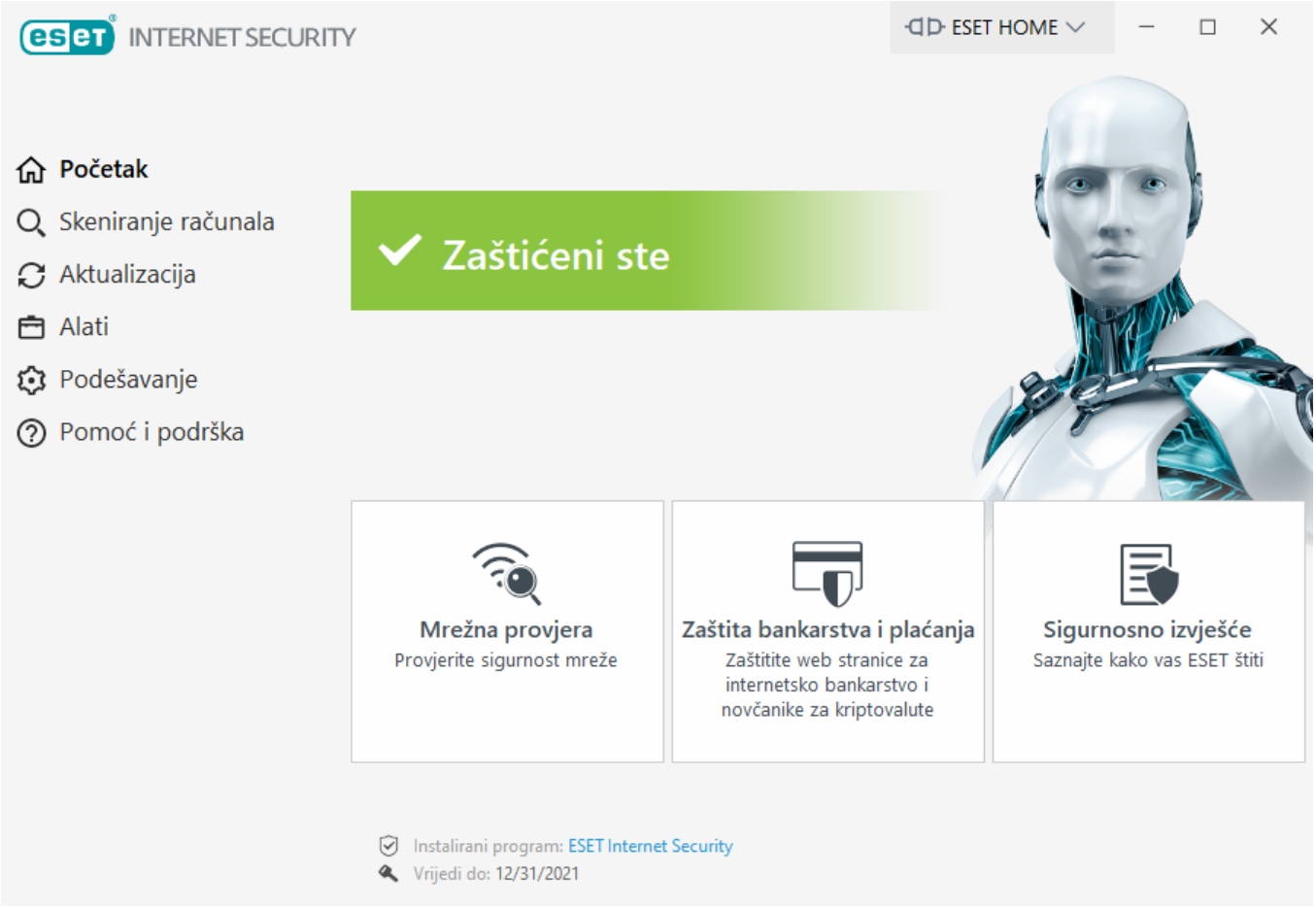
Skeniranje računala – Konfigurirajte i pokrenite skeniranje računala ili stvorite prilagođeno skeniranje.

Aktualizacija – Prikazuje informacije o nadogradnji modula za otkrivanje virusa.

Alati – omogućuje pristup programima Mrežna provjera, Zaštita bankarstva i plaćanja, Anti-Theft i ostalim modulima koji pomažu pojednostaviti administraciju programa i nude dodatne opcije za napredne korisnike. Za više informacija pogledajte odjeljak Alati u programu ESET Internet Security.

Podešavanje – Odaberite ovu opciju za prilagodbu sigurnosne razine za računalo, internet, mežnu zaštitu i sigurnosne alate.

Pomoć i podrška – Omogućuje pristup datotekama pomoći, ESET-ovoj bazi znanja i web stranici tvrtke ESET te vezama za slanje zahtjeva za podršku korisničke službe.

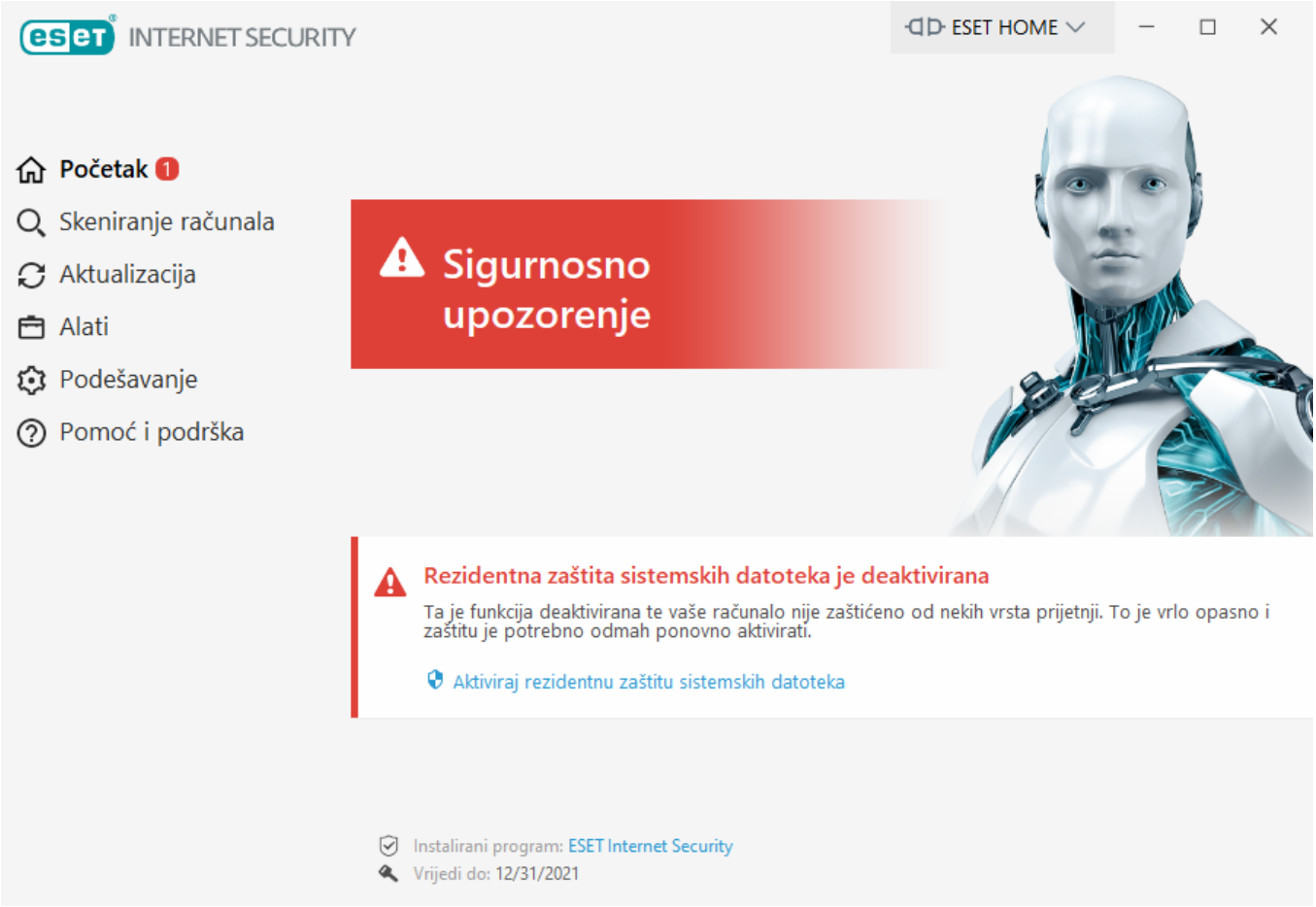


Početni **zaslon** sadrži važne informacije o trenutačnoj razini zaštite računala. Prozor sa statusom prikazuje najčešće korištene funkcije u programu ESET Internet Security. Ovdje možete pronaći i informacije o instaliranom programu i datumu isteka licence. Kliknite **ESET Internet Security** ako želite instalirati drugu verziju ESET-ova programa. Za više informacija o funkcijama određenog programa kliknite ovdje.

Zelena ikona i zeleni status **Zaštićeni ste** označavaju da je osigurana maksimalna zaštita.

Što učiniti ako program ne radi ispravno?

Ako aktivirani modul za zaštitu ispravno radi, ikona statusa zaštite bit će zelena. Crveni uskličnik ili narančasta obavijest znače da nije osigurana maksimalna zaštita. Dodatne informacije o statusu zaštite svakog modula kao i predložena rješenja za vraćanje potpune zaštite prikazat će se u izborniku **Početak**. Za promjenu statusa pojedinačnih modula kliknite **Podešavanje** i odaberite željeni modul.



Crvena ikona i crveni status **sigurnosnog upozorenja** ukazuju na kritične probleme. Nekoliko je mogućih razloga za prikaz tog statusa, na primjer:

- **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.
- **Modul detekcije je zastario** – ova pogreška pojavit će se nakon nekoliko neuspješnih pokušaja aktualizacije modula detekcije. Preporučujemo da provjerite aktualizacijske postavke. Najčešći je uzrok ove pogreške neispravan unos podataka za autentikaciju ili neispravna konfiguracija postavki povezivanja.
- **Deaktivirana je rezidentna zaštita** – korisnik je deaktivirao rezidentnu zaštitu. Vaše računalo nije zaštićeno od prijetnji. Kliknite **Aktiviraj rezidentnu zaštitu sistemskih datoteka** da biste ponovno aktivirali tu funkciju.
- **Deaktivirane su antivirusna i antispyware zaštita** – antivirusnu i antispyware zaštitu možete ponovno aktivirati tako da kliknete **Aktiviraj antivirusnu i antispyware zaštitu**.
- **ESET osobni firewall je deaktiviran** – Taj problem naznačava i obavijest o sigurnosti uz stavku **Mreža** na radnoj površini. Mrežnu zaštitu možete ponovno aktivirati tako da kliknete **Aktiviraj firewall**.

Narančasta ikona označava da je zaštita računala ograničena. Primjerice, možda postoji problem s nadogradnjom programa ili se bliži datum isteka licence.
Nekoliko je mogućih razloga za prikaz tog statusa, na primjer:

- **Upozorenje o Anti-Theft optimizaciji** – Ovaj uređaj nije optimiziran za Anti-Theft. Primjerice, na vašem računalu možda nije stvoren fantomski račun (sigurnosna značajka koja se automatski uključuje

ako označite da je uređaj izgubljen). Fantomski račun možete stvoriti pomoću značajke Optimizacija u Anti-Theft web sučelju.

- **Aktivan je Način rada za igranje** – aktivacija Načina rada za igranje predstavlja mogući sigurnosni rizik. Aktiviranjem te značajke deaktiviraju se svi skočni prozori i prekidaju se svi planirani zadaci.
- **Vaša licenca će uskoro isteći** – To je naznačeno ikonom statusa zaštite s uskličnikom pored sistemskog sata. Nakon isteka licence program se neće moći nadograditi i ikona statusa zaštite postat će crvena.

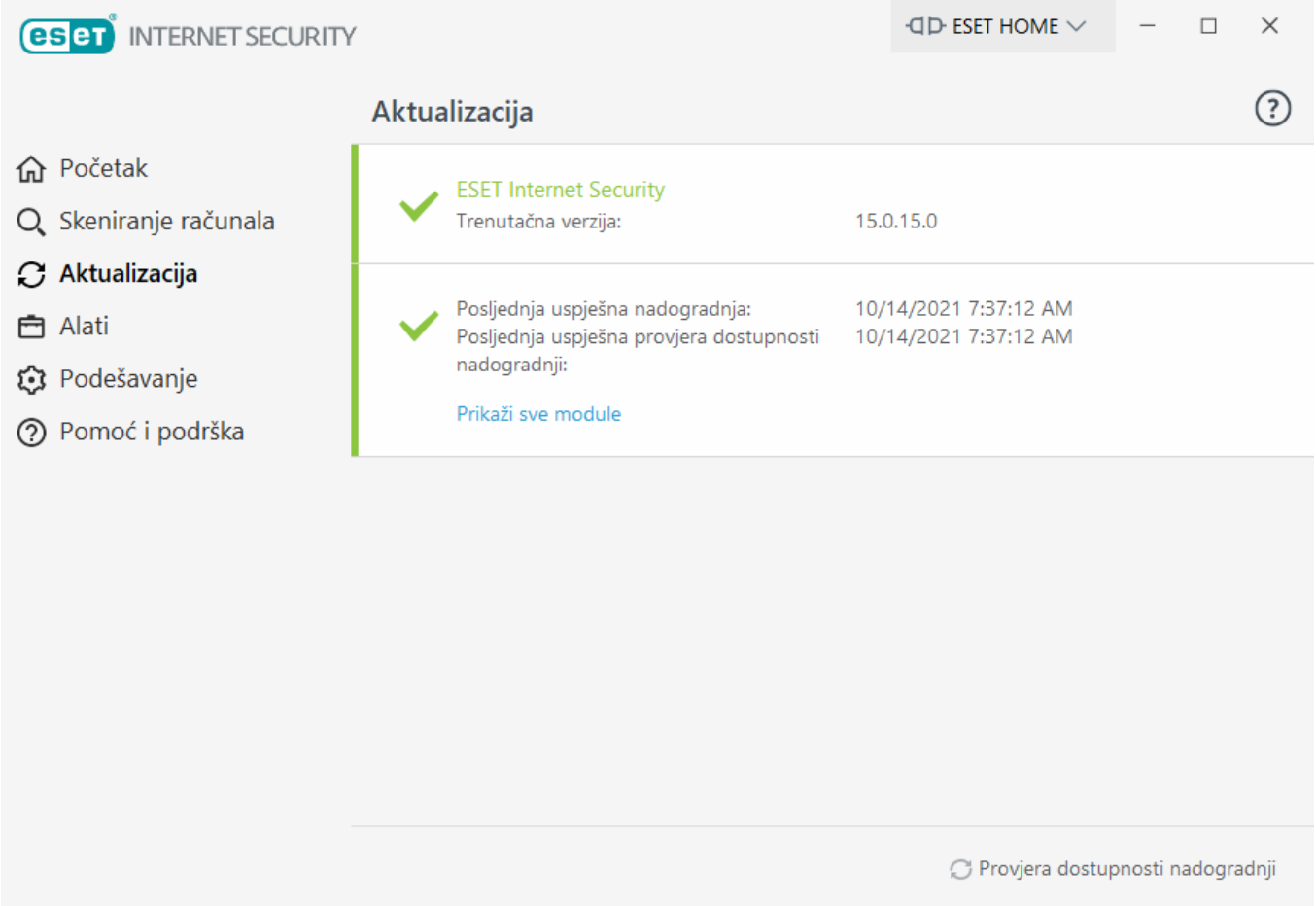
Ako problem ne možete riješiti s pomoću predloženih rješenja, kliknite stavku **Pomoć i podrška** da biste pristupili datotekama pomoći ili pretražili ESET-ovu bazu znanja. Ako vam je i nakon toga potrebna pomoć, možete poslati zahtjev za podršku. ESET-ova tehnička podrška brzo će odgovoriti na vaša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

Nadogradnje

Redovita nadogradnja programa ESET Internet Security najbolji je način osiguravanja maksimalne razine sigurnosti na računalu. Modul nadogradnje osigurava da su moduli programa i komponente sustava uvijek aktualni.

Klikom gumba **Aktualizacija** u glavnom prozoru programa možete provjeriti status trenutačne nadogradnje, datum i vrijeme zadnje uspješne nadogradnje te je li nadogradnja potrebna.

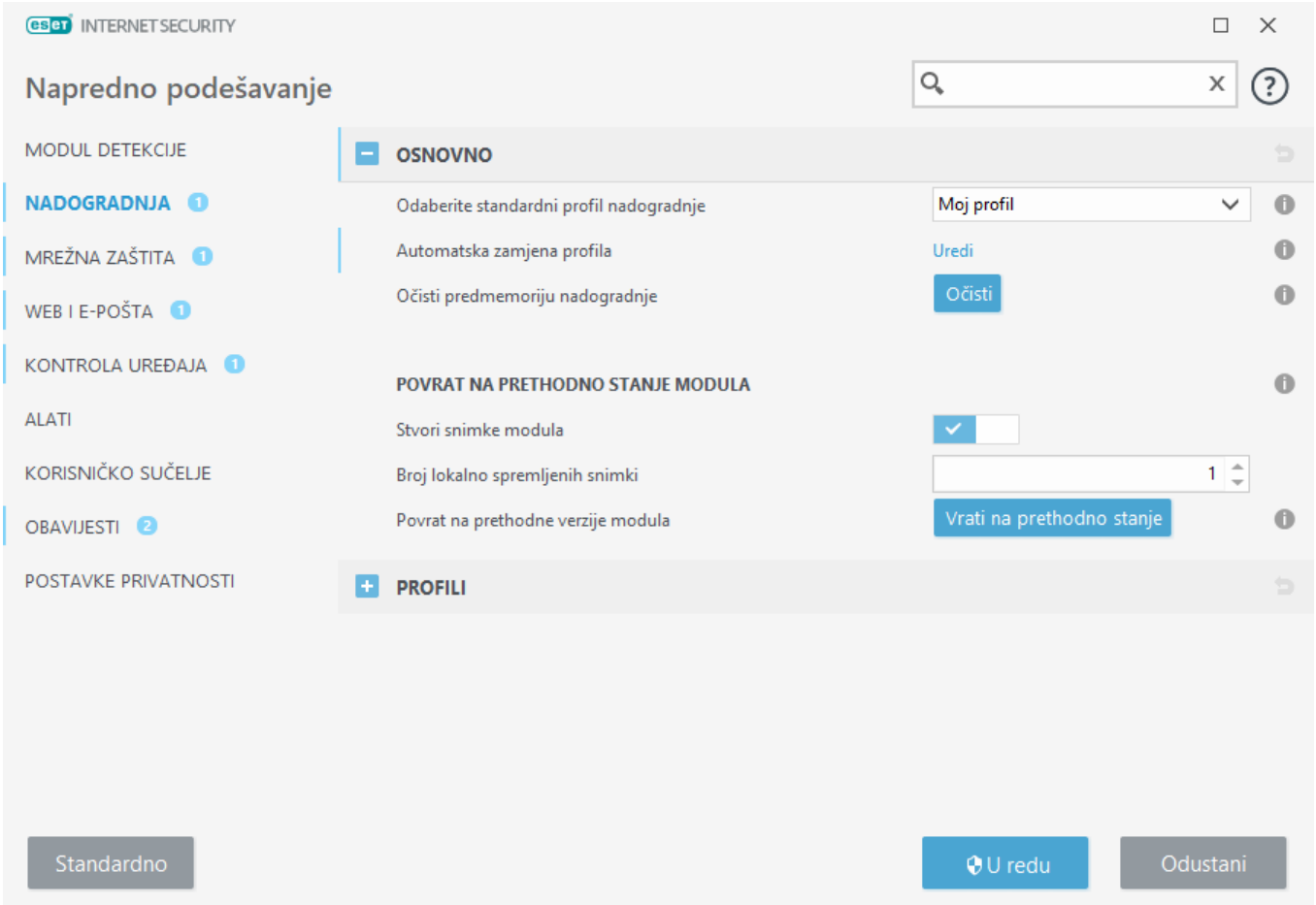
Osim automatskih nadogradnji, možete kliknuti opciju **Potraži nadogradnje** da biste pokrenuli ručnu nadogradnju.



Prozor naprednog podešavanja (kliknite **Podešavanje** u glavnom izborniku, a zatim kliknite **Napredno podešavanje** ili pritisnite **F5** na tipkovnici) sadrži dodatne opcije nadogradnje. Da biste konfigurirali napredne

mogućnosti nadogradnje kao što su način nadogradnje, pristup proxy serveru i LAN veze, kliknite **Nadogradnja** na stablu naprednog podešavanja.

Ako imate problema s nadogradnjom, kliknite **Očisti** da biste izbrisali privremenu memoriju nadogradnje. Ako i dalje ne možete nadograditi module programa, pogledajte odjeljak Otklanjanje poteškoća za poruku "Nadogradnja modula nije uspjela".



Podešavanje dodatnih ESET sigurnosnih alata

Prije nego što počnete upotrebljavati program ESET Internet Security, postavite dodatne sigurnosne alate kako biste maksimalno povećali svoju zaštitu:

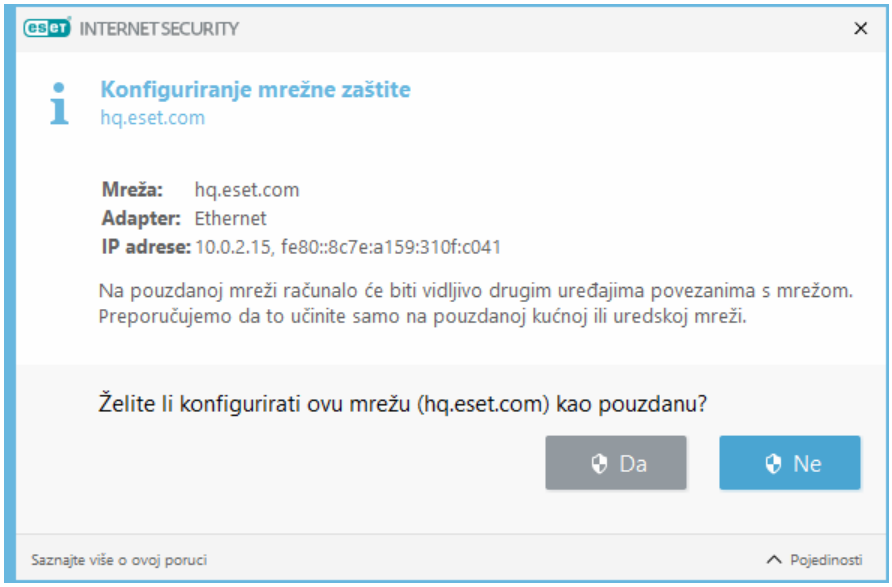
- Roditeljska kontrola
- Anti-Theft

Za više informacija o postavljanju sigurnosnih alata u programu ESET Internet Security pročitajte sljedeći članak u ESET-ovoj bazi znanja.

Konfiguriranje mrežne zaštite

Da biste zaštitili računalo u mrežnom okruženju, morate konfigurirati povezane mreže. Konfiguriranjem mrežne zaštite i dopuštanjem dijeljenja možete dopustiti drugim korisnicima pristup svom računalu. Kliknite **Podešavanje** > **Mrežna zaštita** > **Povezane mreže** i kliknite vezu ispod povezane mreže. Prikazat će se skočni prozor s opcijama za konfiguriranje odabrane mreže kao pouzdane.

Kad se otkrije mreža, ESET Internet Security standardno upotrebljava postavke Windowsa. Da bi se prikazao prozor kad se otkrije nova mreža, promijenite vrstu zaštite novih mreža u "Pitaj korisnika" u odjeljku Poznate mreže. Do konfiguracije mrežne zaštite dolazi prilikom svakog povezivanja računala s novom mrežom. Zato najčešće nije potrebno definirati pouzdane zone.



Postoje dva načina mrežne zaštite koja možete odabrati u prozoru za konfiguriranje mrežne zaštite:

- **Da** – za pouzdanu mrežu (kućnu ili uredsku mrežu). Vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi su drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži. Preporučujemo upotrebu ove postavke prilikom pristupa sigurnoj lokalnoj mreži.

- **Ne** – za nepouzdanu mrežu (javnu mrežu). Datoteke i mape u vašem sustavu ne dijele se s drugim korisnicima na mreži niti su im vidljive i deaktivirano je dijeljenje resursa sustava. Preporučujemo upotrebu ove postavke prilikom pristupa bežičnim mrežama.

Neispravna konfiguracija mreže može predstavljati sigurnosni rizik za računalo.

Po standardnim je postavkama radnim stanicama iz pouzdane mreže omogućen pristup zajedničkim datotekama i pisačima, dolazna je RPC komunikacija aktivirana, a moguće je i zajedničko korištenje udaljene radne površine.

Više informacija o toj značajci pročitajte u ovom članku ESET-ove baze znanja:

- Promjena postavke firewalla za mrežnu vezu u ESET-ovim Windows programima za kućne korisnike

Aktiviraj Anti-Theft

Za osobne uređaje stalno postoji rizik od gubljenja ili krađe tijekom puta od kuće na posao ili na drugim javnim mjestima. Anti-Theft je funkcija koja povećava sigurnost na korisničkoj razini u slučaju gubitka ili krađe uređaja. Anti-Theft omogućuje nadziranje upotrebe uređaja i praćenje nestalog uređaja pomoću lokalizacije pomoću IP adrese u ESET HOME računu, čime vam pomaže da vratite uređaj i zaštitite osobne podatke.

Upotreba modernih tehnologija kao što su traženje geografske lokacije IP adrese, snimanje slike web-kamerom, zaštita korisničkog računa i nadzor uređaja Anti-Theft mogu pomoći vama i organima za provedbu zakona pri lociranju izgubljenog ili ukradenog računala ili uređaja. U ESET HOME računu možete vidjeti koje se aktivnosti

odvijaju na vašem računalu ili uređaju.

Dodatne informacije o programu Anti-Theft u ESET HOME računu potražite u pomoći na mreži za ESET HOME.

Da biste aktivirali Anti-Theft i zaštitili uređaj u slučaju gubitka ili krađe, odaberite jednu od sljedećih opcija:

- Nakon instalacije programa kliknite **Aktiviraj Anti-Theft** da biste aktivirali Anti-Theft.
- Ako vidite poruku "Anti-Theft je dostupan" u glavnom prozoru programa > **Početni** zaslon, kliknite **Aktiviraj Anti-Theft**.
- U glavnom prozoru programa kliknite **Alati** > **Anti-Theft**.
- U glavnom prozoru programa kliknite **Podešavanje** > **Sigurnosni alati**. Kliknite ikonu trake klizača **Anti-Theft** i slijedite upute na zaslonu.

Ako vaš uređaj nije povezan s ESET HOME računom, morate:
1. Prijaviti se na ESET HOME račun kad aktivirate Anti-Theft.
2. Postavi naziv uređaja

Anti-Theft ne podržava Microsoft Windows Home Server.

Nakon što aktivirate Anti-Theft možete optimizirati sigurnost svojeg uređaja na glavnom prozoru programa > **Alati** > **Anti-Theft**.

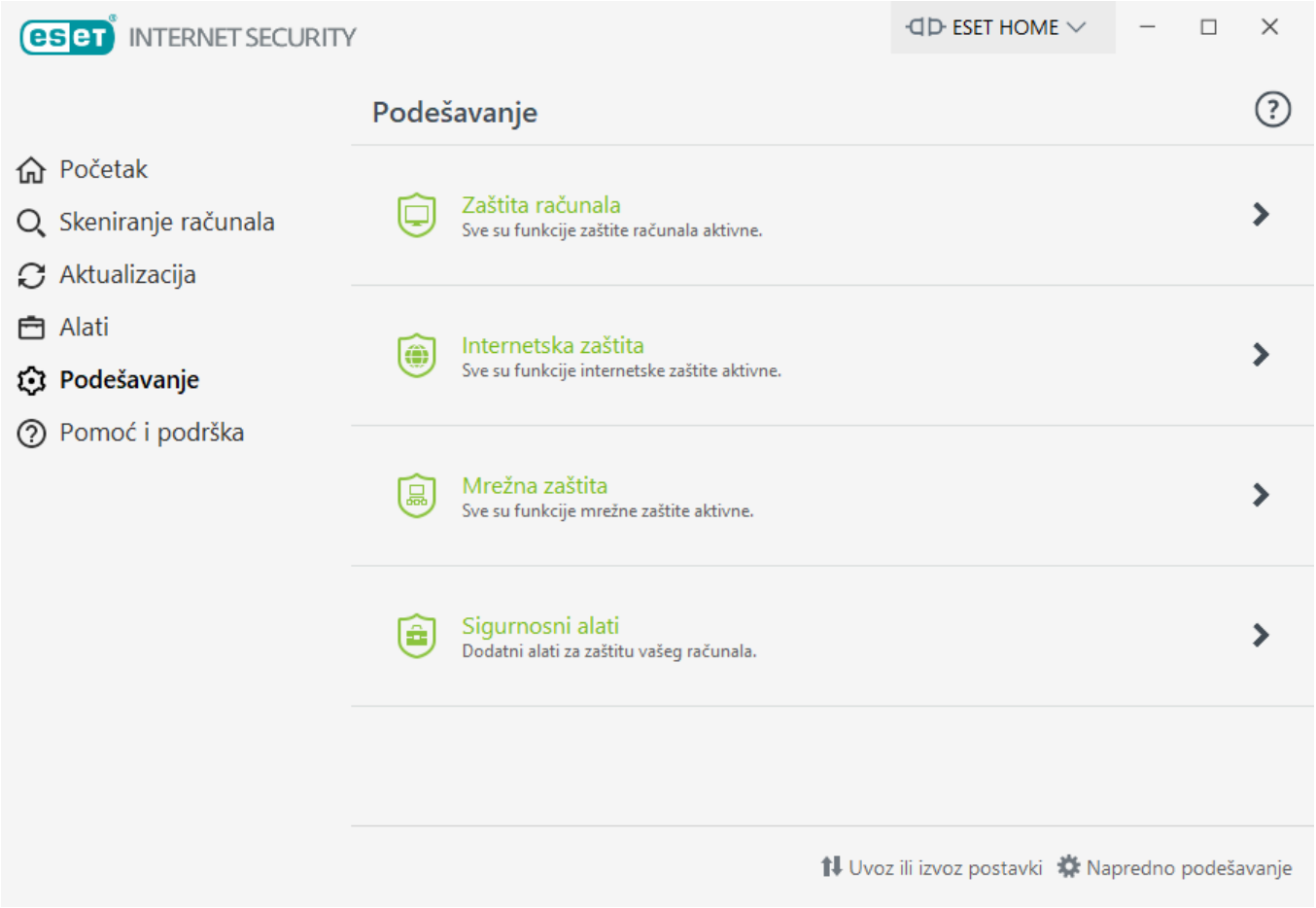
Alati roditeljske kontrole

Ako ste već aktivirali roditeljsku kontrolu u programu ESET Internet Security, morate konfigurirati i roditeljsku kontrolu za sve korisničke račune.

Kada je roditeljska kontrola aktivna, a korisnički računi nisu konfigurirani, na **početnom** zaslonu se prikazuje "Roditeljska kontrola nije postavljena". Kliknite **Postavi pravila** i potražite više informacija u odjeljku Roditeljska kontrola.

Rad s programom ESET Internet Security

Mogućnosti podešavanja programa ESET Internet Security omogućuju vam prilagođavanje razine zaštite računala i mreže.



Izbornik **Podešavanje** podijeljen je na sljedeće odjeljke:

Zaštita računala

Internetska zaštita

Mrežna zaštita

Sigurnosni alati

Kliknite komponentu da biste prilagodili napredne postavke za odgovarajući modul za zaštitu.

Odjeljak **Zaštita računala** 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** – Taj modul omogućuje skeniranje, blokiranje ili prilagođavanje dodatnih filtara/ovlaštenja i odabir načina na koji korisnik pristupa i upotrebljava određeni uređaj (CD/DVD/USB...).
- **Sistem za sprječavanje upada** – sustav HIPS prati događaje u operacijskom sustavu i reagira na njih sukladno prilagođenom setu pravila.
- **Način rada za igranje** – Aktivira ili deaktivira Način rada za igranje. Nakon aktivacije Načina rada za igranje

primit ćete poruku upozorenja (mogući sigurnosni rizik) i glavni će prozor postati narančast.

- **Zaštita web kamere** – upravlja procesima i aplikacijama koje pristupaju kameri povezanoj s računalom.

Podešavanje **Internetske zaštite** omogućuje aktiviranje ili deaktiviranje sljedećih komponenti:

- **Zaštita web pristupa** – Ako se aktivira ova postavka, sav promet putem HTTP-a ili HTTPS-a skenira se da bi se otkrili zlonamjerni programi.
- **Zaštita klijenta e-pošte** – Nadzire komunikaciju koja se prima putem protokola POP3(S) i IMAP(S).
- **Antispam zaštita** – Skenira neželjenu e-poštu, tj. spam poruke.
- **Anti-phishing zaštita** – Filtrira web stranice za koje se sumnja da distribuiraju sadržaj namijenjen navođenju korisnika na odavanje povjerljivih informacija.

Odjeljak **Mrežna zaštita** omogućuje aktivaciju ili deaktivaciju značajki Firewall, Zaštita od mrežnog napada (IDS) i Zaštita od botneta.

Podešavanje **Sigurnosnih alata** omogućuje vam prilagođavanje sljedećih modula:

- **Zaštita bankarstva i plaćanja** – pruža dodatan sloj zaštite preglednika koji je osmišljen za zaštitu financijskih podataka tijekom online transakcija. Aktivirajte opciju **Zaštiti sve preglednike** da biste pokrenuli sve podržane web preglednike u sigurnom načinu rada. Više informacija potražite u odjeljku Zaštita bankarstva i plaćanja.
- **Roditeljska kontrola** – modul roditeljske kontrole štiti vašu djecu tako što blokira neprimjeren ili štetan sadržaj na internetu.
- **Anti-Theft** – aktivirajte Anti-Theft da biste zaštitili računala u slučaju gubitka ili krađe.

Roditeljska kontrola omogućuje blokiranje web stranica s potencijalno uvredljivim sadržajima. Osim toga, roditelji mogu zabraniti pristup do 40 unaprijed definiranih kategorija web stranica i više od 140 podkategorija.

Da biste ponovno aktivirali deaktiviranu sigurnosnu komponentu, kliknite klizač  tako da se na njemu prikaže zelena kvačica .

> Kod deaktiviranja zaštite ovom metodom svi deaktivirani zaštitni moduli aktivirat će se nakon restarta računala.

Dodatne mogućnosti dostupne su u dnu prozora podešavanja. Pomoću veze **Napredno postavljanje** postavite detaljnije parametre za svaki modul. Koristite značajku **Uvoz ili izvoz postavki** da biste učitali parametre podešavanja pomoću konfiguracijske datoteke .xml ili spremili trenutačne parametre podešavanja u konfiguracijsku datoteku.

Zaštita računala

Kliknite **Zaštita računala** u prozoru **Podešavanje** za prikaz svih modula za zaštitu:

- rezidentna zaštita

- Kontrola uređaja
- Sustav za sprečavanje upada (HIPS)
- Način rada za igranje
- Zaštita web-kamere

Da biste pauzirali ili deaktivirali pojedinačne module za zaštitu, kliknite ikonu trake klizača .

Isključivanjem modula za zaštitu može se smanjiti razina zaštite vašeg računala.

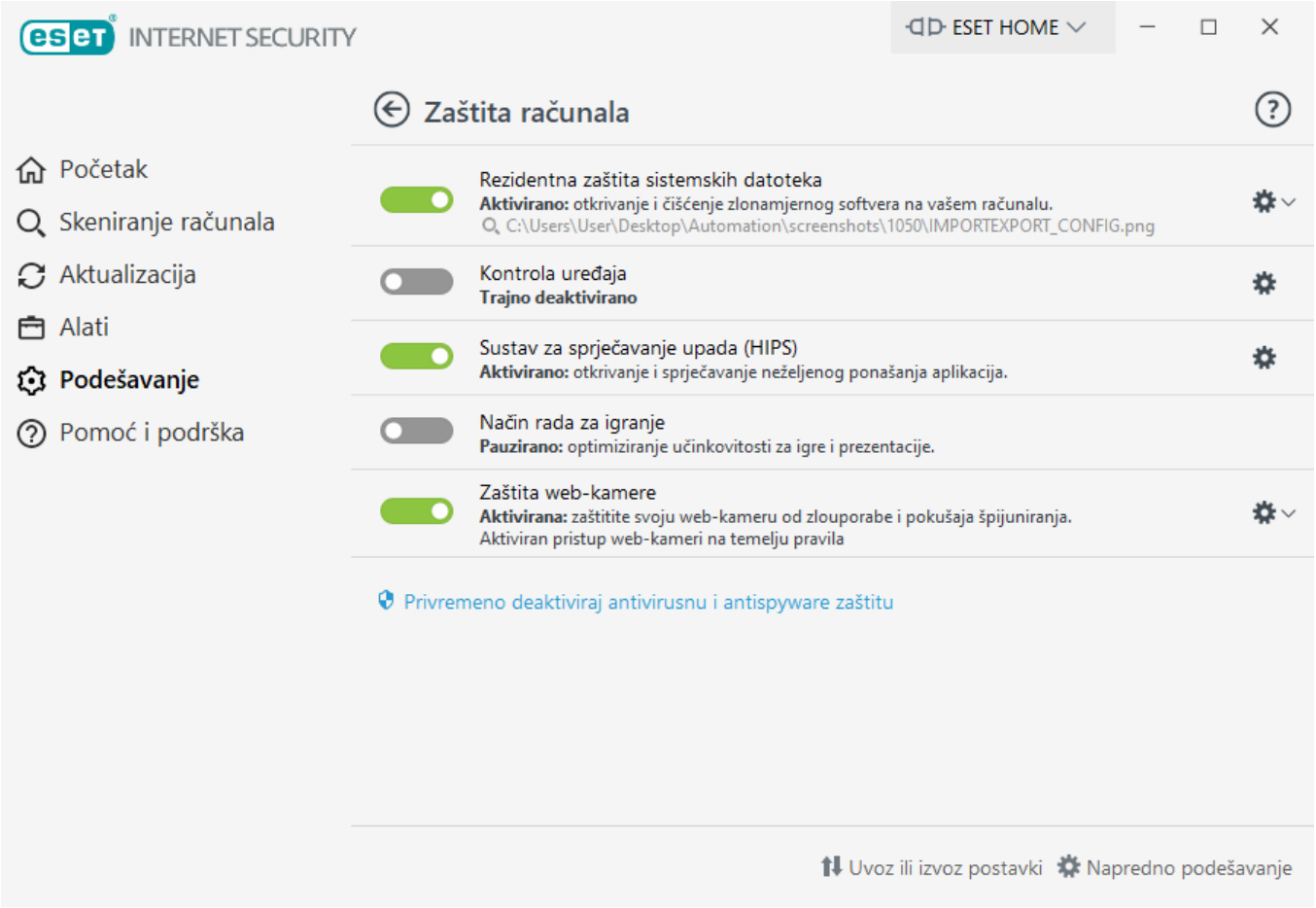
Kliknite ikonu zupčanika uz zaštitni modul da biste pristupili naprednim postavkama za taj modul.

Za **rezidentnu zaštitu sistemskih datoteka** kliknite ikonu zupčanika i odaberite jednu od sljedećih opcija:

- **Konfiguriranje** – otvara napredno podešavanje Rezidentne zaštite sistemskih datoteka.
- **Uređivanje izuzetaka** – otvara prozor za podešavanje izuzetaka tako da možete izuzeti datoteke i mape od skeniranja.

Za **zaštitu web kamere** kliknite ikonu zupčanika i odaberite jednu od sljedećih opcija:

- **Konfiguriranje** – otvara napredno podešavanje Zaštite web kamere.
- **Blokiraj sve pokušaje pristupa do ponovnog pokretanja** – blokira sav pristup web kameri do ponovnog pokretanja računala.
- **Trajno blokiraj sve pokušaje pristupa** – blokira sav pristup web kameri dok se ova postavka ne deaktivira.
- **Prestani blokirati sve pokušaje pristupa** – deaktivira mogućnost blokiranja pristupa web kameri. Ova opcija je dostupna samo ako je pristup web kameri blokiran.



Privremeno deaktiviraj antivirusnu i antispyware zaštitu – deaktivira sve module antivirusne i antispyware zaštite. Kada deaktivirate zaštitu, otvorit će se prozor u kojemu pomoću padajućeg izbornika **Vremenski interval** možete odrediti koliko će dugo zaštita biti deaktivirana. Upotrijebite samo ako ste iskusni korisnik ili ako ste dobili upute od ESET-ove tehničke podrške.

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**.

Promjene postavki modula detekcije treba izvršiti samo iskusni korisnik. Neispravna konfiguracija postavki može dovesti do smanjene razine zaštite.

U ovom odjeljku:

- Kategorije rezidentne zaštite i zaštite na temelju strojnog učenja
- Skeniranja za zlonamjerne softvere
- Podešavanje izvješćivanja
- Podešavanje zaštite

Kategorije rezidentne zaštite i zaštite na temelju strojnog učenja

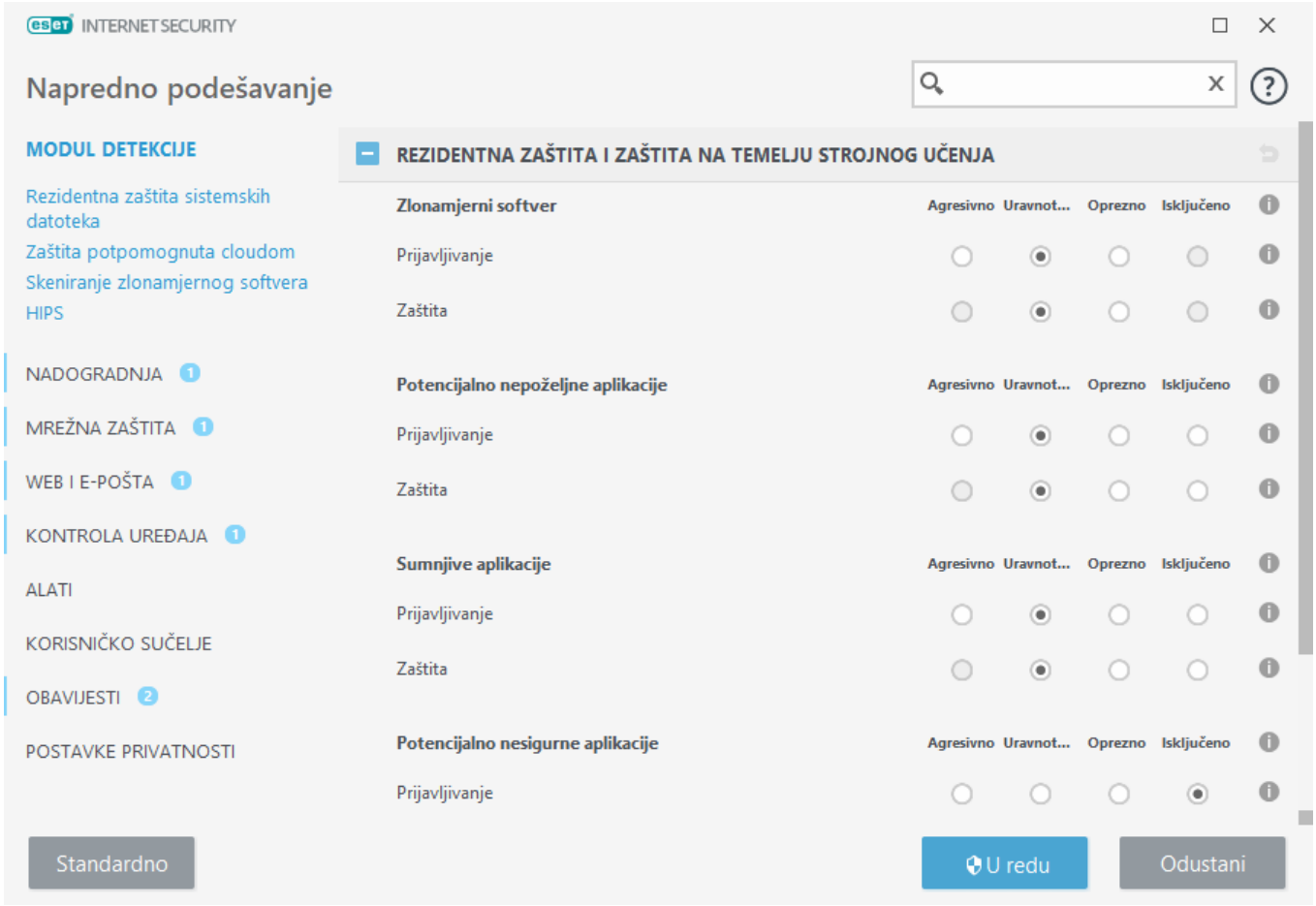
Rezidentna zaštita i zaštita na temelju strojnog učenja za sve module za zaštitu (na primjer, rezidentna zaštita sistemskih datoteka, zaštita web pristupa...) omogućuje vam konfiguriranje razina izvještavanja i zaštite sljedećih kategorija:

- **Zlonamjerni programi** – Računalni virus primjerak je zlonamjernog koda koji se dodaje ispred ili uz postojeće datoteke na 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 nepoželjne 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.

- **Sumnjive aplikacije** obuhvaćaju programe komprimirane pomoću arhivatora ili protektora. Autori zlonamjernih programa često iskorištavaju te vrste programa kako bi spriječili otkrivanje.

- **Potencijalno nesigurne aplikacije** – Naziv je koji se odnosi na legitiman komercijalni softver koji bi se mogao zloupotrijebiti. Primjeri potencijalno nesigurnih aplikacija (PUA) obuhvaćaju alate za daljinski pristup, aplikacije za probijanje lozinki i keyloggere (programe koji bilježe svaki korisnikov pritisak tipke). Više o tim vrstama aplikacija pročitajte u rječniku.



> **Poboljšana zaštita**
> 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**. Za više informacija pogledajte skeniranje zlonamjernih programa.

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 Internet Security.

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
Agresivno	Prijavljivanje KATEGORIJE konfigurirano je na najveću osjetljivost. Prijavljuje se više otkrivenih prijetnji. Postavka **Agresivno** može pogrešno prepoznati objekte kao KATEGORIJU.
Uravnoteženo	Prijavljivanje KATEGORIJE konfigurirano je kao uravnoteženo. Ova postavka je optimizirana kako bi se uravnotežili rezultati i stopa otkrivanja prijetnji i broj pogrešno prijavljenih objekata.
Oprezno	Prijavljivanje KATEGORIJE konfigurirano 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.
Isključeno	Prijavljivanje 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 Internet Security

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 Internet Security 13.1 i novijima.
** Nije preporučeno

Određivanje verzije programa, modula programa i datuma podverzije

1. Kliknite **Pomoć i podrška** > **O programu ESET Internet Security**.
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 Internet Security (13.0 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 Internet Security 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
Agresivno	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.
Uravnoteženo	Blokiraju se prijavljene otkrivene prijetnje uravnotežene razine (ili prijetnje niže razine) i pokreće se automatsko ispravljanje (npr. čišćenje).
Oprezno	Blokiraju se prijavljene otkrivene prijetnje na opreznoj razini rada i pokreće se automatsko ispravljanje prijetnji (npr. čišćenje).
Isključeno	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 za ESET Internet Security 13.0 i starije verzije

Pri nadogradnji s verzije 13.0 i starijih na verziju 13.1 i novije, novo stanje praga bit će sljedeće:

Prebacivanje kategorije prije nadogradnje	✓	✗
Novi prag za KATEGORIJE nakon nadogradnje	Uravnoteženo	Isključeno

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.).

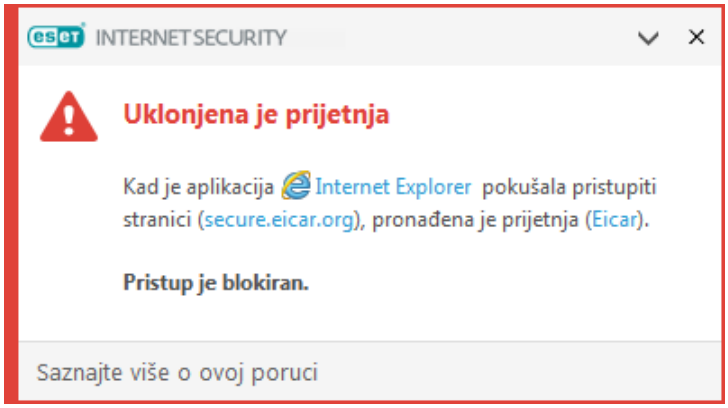
Standardno ponašanje

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

- rezidentna 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 Dnevnici. Dodatne informacije o razinama čišćenja i ponašanju potražite u odjeljku Razina čišćenja.



Skeniranje računala radi otkrivanja zaraženih datoteka

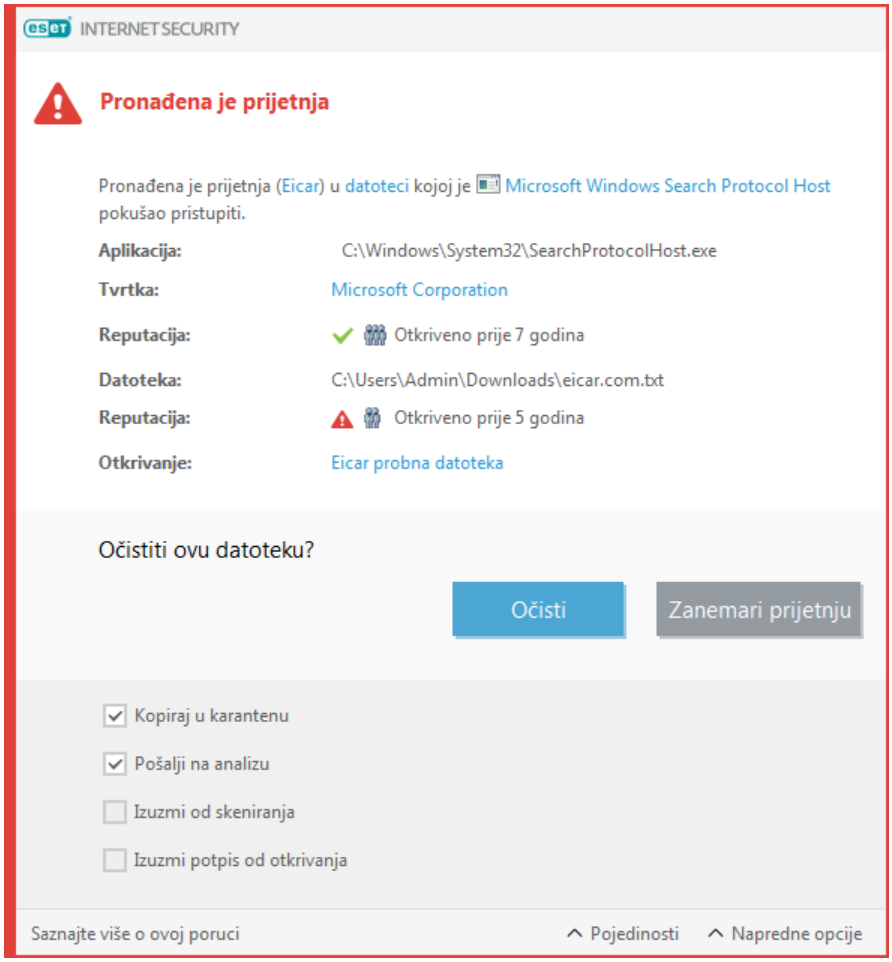
Ako računalo pokazuje znakove zaraze zlonamjernim softverom (npr. sporije radi, često se "zamrzava" itd.), preporučujemo sljedeće:

1. Otvorite program ESET Internet Security i kliknite **Skeniranje računala**.
2. Kliknite **Skenirajte svoje računalo** (dodatne informacije potražite u odjeljku Skeniranje računala).
3. 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.

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.



Primijenite 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 Internet Security klikom na **Alati** > **Više alata** > **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

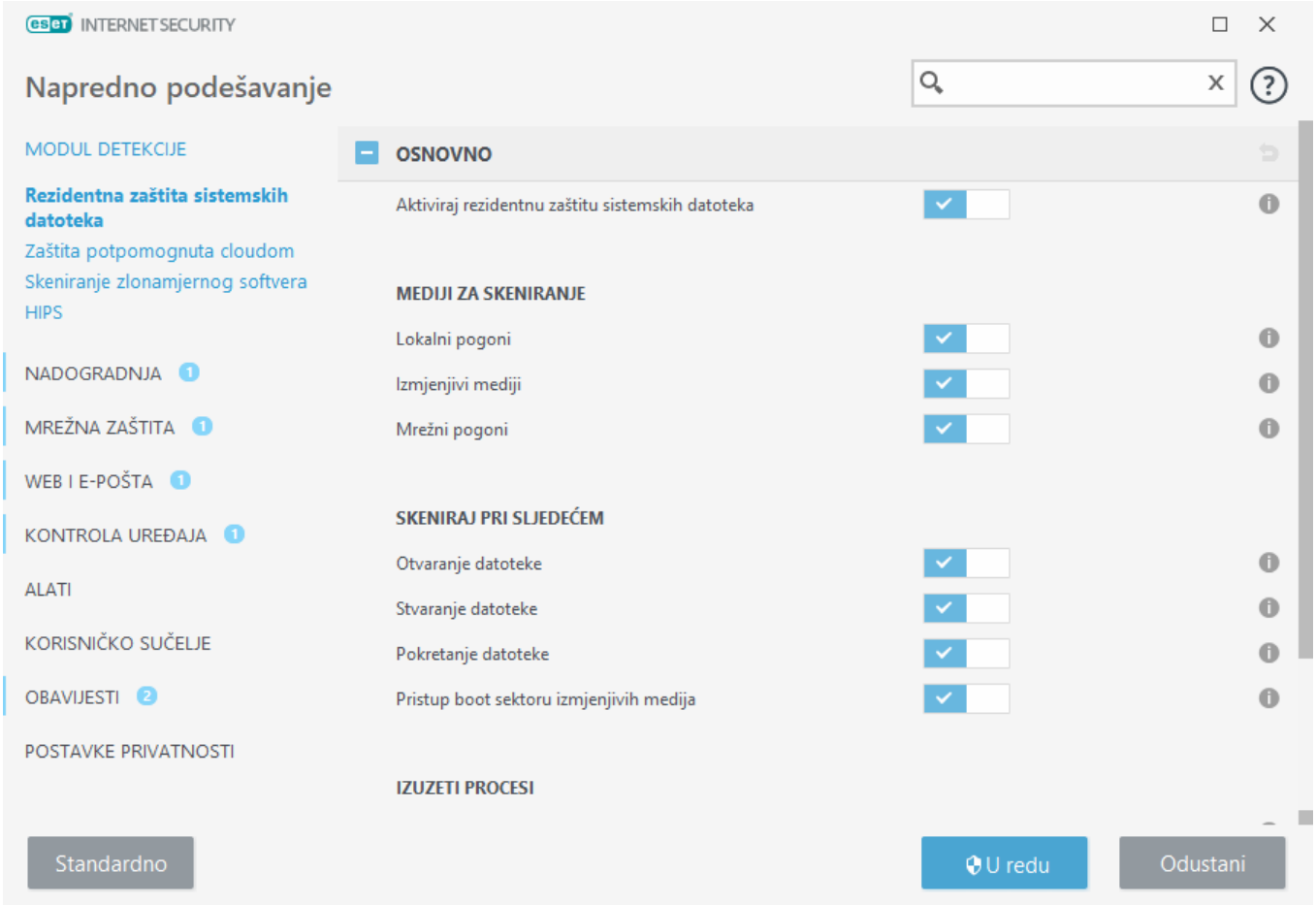
Ako neke zaražene datoteke nisu očišćene tijekom skeniranja (ili je Razina čišćenja postavljena na **Bez čišćenja**), prikazuje se prozor upozorenja s upitom o odabiru radnji za te datoteke. Odaberite akcije za datoteke (akcije se postavljaju posebno za svaku datoteku na popisu), a zatim kliknite **Završetak**.

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.

rezidentna zaštita

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



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 datoteka** – 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.

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 odmah ponovno skeniraju nakon svake nadogradnje 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 parametar** > **Ostalo** i odaberite ili poništite odabir mogućnosti **Aktiviraj Smart optimizaciju**.

Razine čišćenja

Da biste pristupili postavkama razine čišćenja za željeni zaštitni modul, proširite **ThreatSense parametre** (na primjer, **Rezidentnu zaštitu sistemskih datoteka**), a zatim pronađite **Čišćenje > Razina čišćenja**.

ThreatSense parametri imaju sljedeće razine ispravljanja (tj. čišćenja).

Ispravljanje u programu ESET Internet Security

Razina čišćenja	Opis
Uvijek ispravi prijetnju	Pokušaj ispravljanja 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.
Ispravi otkrivenu prijetnju ako je sigurna, u suprotnom je zadrži	Pokušaj ispravljanja otkrivene prijetnje prilikom čišćenja objekata 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.
Ispravi otkrivenu prijetnju ako je sigurna, u suprotnom postavi pitanje	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.
Uvijek pitaj krajnjeg korisnika	Tijekom čišćenja objekata krajnjem korisniku se prikazuje interaktivno upozorenje i potrebno je odabrati radnju za ispravljanje (npr. uklanjanje ili zanemarivanje). Ta razina namijenjena je naprednijim korisnicima koji znaju koje korake treba poduzeti u slučaju prijetnje.

Kada treba izmijeniti konfiguraciju rezidentne zaštite

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

Nakon instalacije programa ESET Internet Security 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**).

Provjera rezidentne zaštite

Da biste provjerili funkcioniranje rezidentne zaštite i njezino otkrivanje virusa, upotrijebite probnu datoteku s adrese *www.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.

Što ako rezidentna zaštita ne funkcionira

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. Da biste riješili ovaj problem, stvorite SysInspector dnevnik i pošaljite ga ESET-ovoj tehničkoj podršci na analizu.

Izuzeti procesi

Funkcija Izuzeti procesi omogućuje vam da izuzmete procese aplikacija iz Rezidentne zaštite sistemskih datoteka. Za poboljšanje brzine sigurnosnog kopiranja, cjelovitosti 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. 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.

> Ne smije se pomiješati s drugim izuzecima kao što su Izuzete datotečne ekstenzije, Izuzeci iz HIPS-a, Izuzeci detekcija poznatih prijetnji ili Izuzeci radi poboljšanja performansi.

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*).

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 Internet Security 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.

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 Internet Security 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.

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 ESET LiveGrid® omogućuje nam da brzo reagiramo na potrebe svojih korisnika i da održimo ESET-ovu sposobnost reagiranja na najnovije prijetnje.

Dostupne su sljedeće opcije:

Aktiviraj sustav 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®.

Aktiviraj sustav za povratne informacije ESET LiveGrid®

Uz sustav reputacije ESET LiveGrid® sustav ESET LiveGrid® za povratne informacije prikupljat će informacije o vašem računalu koje se odnose na nove pronađene prijetnje. Te informacije mogu obuhvaćati sljedeće:

- Uzorak ili kopiju datoteke u kojoj se pojavila prijetnja
- Put do datoteke
- Naziv datoteke
- Datum i vrijeme
- Proces u kojem se prijetnja pojavila na računalu
- Informacije o operacijskom sustavu računala

Prema standardnim je postavkama sustav ESET Internet Security 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.

Pročitajte više o slanju relevantnih podataka u Pravilima privatnosti.

Ne morate aktivirati ESET LiveGrid®

Nećete izgubiti funkcionalnost softvera, no u nekim slučajevima ESET Internet Security može reagirati brže na nove prijetnje kada je aktiviran ESET LiveGrid®. Ako ste ranije koristili sustav ESET LiveGrid® i deaktivirali ste ga, možda još uvijek ima pakete podataka koje treba poslati. Ti će se paketi slati tvrtki ESET čak i nakon deaktivacije. Nakon slanja svih trenutačnih informacija, neće se stvarati novi paketi.

Pročitajte više o sustavu ESET LiveGrid® u rječniku.
Pogledajte naše ilustrirane upute dostupne na engleskom i na još nekoliko jezika za aktiviranje ili deaktiviranje sustava ESET LiveGrid® u programu ESET Internet Security.

Konfiguracija zaštite utemeljene na cloudu u naprednom podešavanju

Da biste pristupili postavkama za ESET LiveGrid®, otvorite **Napredno podešavanje** (F5) > **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 cloudu.

- **Aktiviraj sustav za povratne informacije ESET LiveGrid®** – Šalje laboratoriju tvrtke ESET za istraživanje relevantne podatke (opisane u odjeljku **Slanje uzoraka** u nastavku) uz izvješća o padu sustava i statistiku radi daljnje analize.

- **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.

Slanje uzoraka

Ručno slanje uzoraka – omogućuje vam ručno slanja uzoraka ESET-u iz kontekstnog izbornika, opcije Karantena ili opcije Alati.

Automatsko slanje otkrivenih uzoraka

Odaberite vrstu uzoraka koji će se slati ESET-u na analizu da bi se poboljšalo buduće otkrivanje prijetnji (standardna maksimalna veličina uzorka iznosi 64 MB). Dostupne su sljedeće opcije:

- **Svi otkriveni uzorci** – Svi objekti koje otkriva 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

Ti uzorci će se također poslati ESET-u ako ih ne otkrije modul detekcije. Na primjer, uzorci koji gotovo nisu otkriveni ili uzorci čije ponašanje jedan od modula zaštite sustava ESET Internet Security smatra sumnjivim ili nejasnim (standardna maksimalna veličina uzorka iznosi 64 MB).

- **Izvršne datoteke** – Uključuje izvršne datoteke poput .exe, .dll, .sys.

- **Arhive** – Uključuje arhivske vrste datoteka poput .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

- **Skripte** – Uključuje vrste datoteka skripti 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 cjelovitih 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** > **Modul detekcije** > **Zaštita na bazi clouda** > **Slanje uzoraka** i kliknite **Uredi** pored stavke **Izuzeci**. Dodajte izuzetak `.download.domain.com`.

Maksimalna veličina uzoraka (MB) – Definira maksimalnu veličinu uzoraka (1-64 MB).

Filtar izuzetaka za zaštitu na bazi clouda

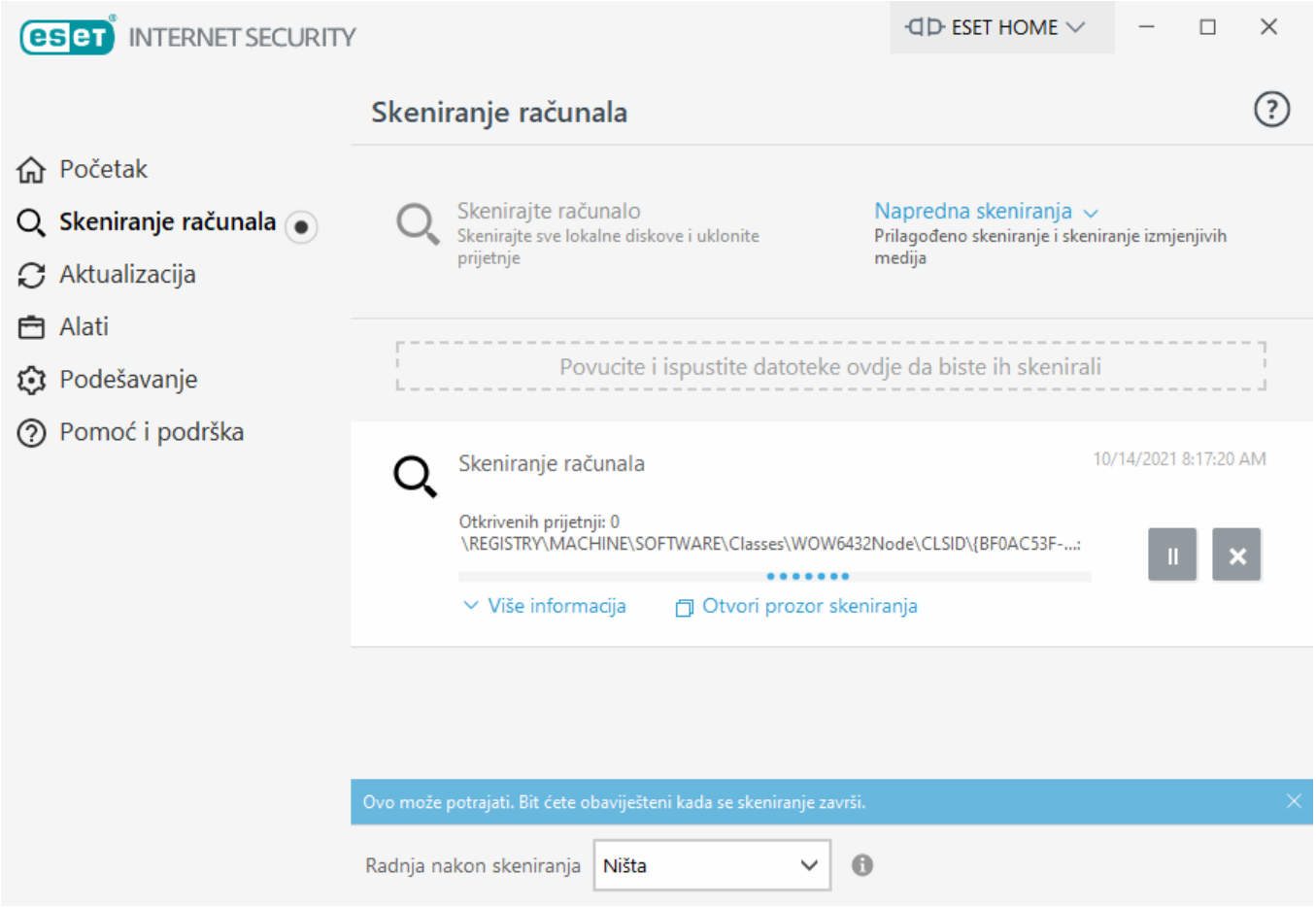
Filtar izuzetaka omogućuje vam izuzimanje određenih datoteka ili mapa od slanja. Datoteke s popisa nikada se neće slati u laboratorije tvrtke ESET na analizu, čak i ako sadrže sumnjiv kod. Česte se vrste datoteka (kao što je .doc itd.) izostavljaju prema standardnim postavkama.

Ova je značajka korisna za izuzimanje datoteka koje mogu sadržavati povjerljive informacije, kao što su dokumenti ili proračunske tablice.

Da biste isključili datoteke preuzete s web stranice download.domain.com, kliknite **Napredno podešavanje** > **Modul detekcije** > **Zaštita na bazi clouda** > **Slanje uzoraka** > **Izuzeci** i dodajte izuzetak *download.domain.com*.

Skeniranje računala

Skener na zahtjev važan je dio ovog antivirusnog rješenja. Koristi se za skeniranje datoteka i mapa na računalu. Sa stanovišta sigurnosti, važno je redovito provoditi skeniranja računala u sklopu rutinskih mjera zaštite, a ne samo u slučaju sumnje na zarazu. Preporučujemo da redovito izvršavate dubinska skeniranja sustava da biste otkrili viruse koje nije otkrila Rezidentna zaštita kod njihovog zapisivanja na disk. To se može dogoditi ako je u tom trenutku rezidentna zaštita bila deaktivirana, modul za otkrivanje virusa zastario ili ako datoteka nije bila otkrivena kao virus kada je spremljena na disk.



Dostupne su dvije vrste **Skeniranja računala**. **Skeniraj računalo** brzo skenira sustav, bez određivanja parametara skeniranja. **Prilagođeno skeniranje** (u sklopu naprednih skeniranja) omogućuje odabir prethodno definiranih profila skeniranja namijenjenih ciljanju određenih lokacija i biranje određenih objekata skeniranja.

Dodatne informacije o procesu skeniranja potražite u poglavlju Napredak skeniranja.

Prema standardnim postavkama, ESET Internet Security automatski pokušava očistiti ili ukloniti prijetnje pronađene tijekom skeniranja računala. U nekim slučajevima, ako nije moguće provesti nijednu radnju, primit ćete interaktivno upozorenje i morate odabrati radnju čišćenja (na primjer, brisanje ili ignoriranje). Za promjenu razine čišćenja i detaljnije informacije pogledajte odjeljak Čišćenje. Za pregled prethodnih skeniranja pogledajte odjeljak Dnevnici.

Skenirajte svoje računalo

Mogućnost „**Skenirajte računalo**" omogućuje brzo pokretanje skeniranja računala i čišćenje zaraženih datoteka bez potrebe za korisničkom intervencijom. Prednost mogućnosti "**Skenirajte svoje računalo**" jest to što je jednostavna za upotrebu i ne zahtijeva detaljnu konfiguraciju skeniranja. To 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.

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 se aplikacija prebacuje u prvi plan.

Sljedeće opcije skeniranja dostupne su pod **Napredna skeniranja**:

Prilagođeno skeniranje

Prilagođeno skeniranje omogućuje vam zadavanje parametara skeniranja kao što su objekti i metode. Prednost **Prilagođenog skeniranja** je u tome što parametre možete detaljno konfigurirati. Konfiguracije možete spremiti u korisnički definirane profile skeniranja koji mogu biti korisni ako se skeniranje opetovano provodi prema istim parametrima.

Skeniranje izmjenjivih medija

Slično opciji „**Skenirajte 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 kao i prije.

Padajući izbornik **Radnja nakon skeniranja** omogućava postavljanje automatskog pokretanja radnje nakon dovršetka skeniranja:

- **Bez radnje** – Kada skeniranje završi, neće se izvršiti nijedna radnja.
- **Isključi** – Kada skeniranje završi, računalo se isključuje.
- **Ponovno pokreni** – Zatvara sve otvorene programe i restarta računalo kada završi skeniranje.
- **Ponovno pokreni po potrebi** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Prisilno ponovno pokreni** – prisilno zatvara sve otvorene programa bez čekanja interakcije korisnika i ponovno pokreće računalo nakon što se skeniranje dovrši.
- **Prisilno ponovno pokrenite ako je potrebno** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **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.

> Radnje **Mirovanje** ili **Hibernacija** dostupne su na temelju postavki operacijskog sustava na vašem računalu za uštedu energije i stanje mirovanja ili na temelju mogućnosti stolnog/prijenosnog računala. Imajte na umu da računalo koje je u stanju mirovanja i dalje radi. I dalje pokreće osnovne funkcije i troši električnu energiju dok se napaja putem baterije. Da bi baterija dulje trajala, na primjer, kada se nalazite izvan ureda, preporučujemo da upotrijebite opciju Hibernacija.

Odabrana radnja će započeti nakon završetka svih trenutačno pokrenutih skeniranja. Kada odaberete opciju **Isključi** ili **Ponovno pokreni**, prikazat će se potvrdni dijaloški okvir za potvrdu s istekom vremena od 30 sekundi (kliknite **Odustani** da biste deaktivirali zatraženu radnju).

Preporučujemo da skenirate računalo barem jednom mjesečno. Skeniranje se može konfigurirati kao planirani zadatak u odjeljku **Alati** > **Više alata** > **Planer**. Kako zakazati tjedno skeniranje računala?

Pokretač prilagođenog skeniranja

Možete koristiti prilagođeno skeniranje da biste skenirali radnu memoriju, mrežu ili određene dijelove diska umjesto cijelog diska. Kliknite **Napredna skeniranja** > **Prilagođeno skeniranje** odaberite određene objekte iz (stablaste) strukture mape.

Iz padajućeg izbornika **Profil** možete odabrati profil koji ćete upotrebljavati za skeniranje određenih objekata. Standardni je profil **Smart skeniranje**. Postoje još tri unaprijed definirana profila skeniranja: **Dubinsko skeniranje**, **Skeniranje iz kontekstnog izbornika** i **Skeniranje računala**. Ovi profili skeniranja upotrebljavaju različite ThreatSense parametre. Dostupne opcije opisane su u izborniku **Napredno podešavanje** (F5) > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Skeniranje na zahtjev** > ThreatSense parametri.

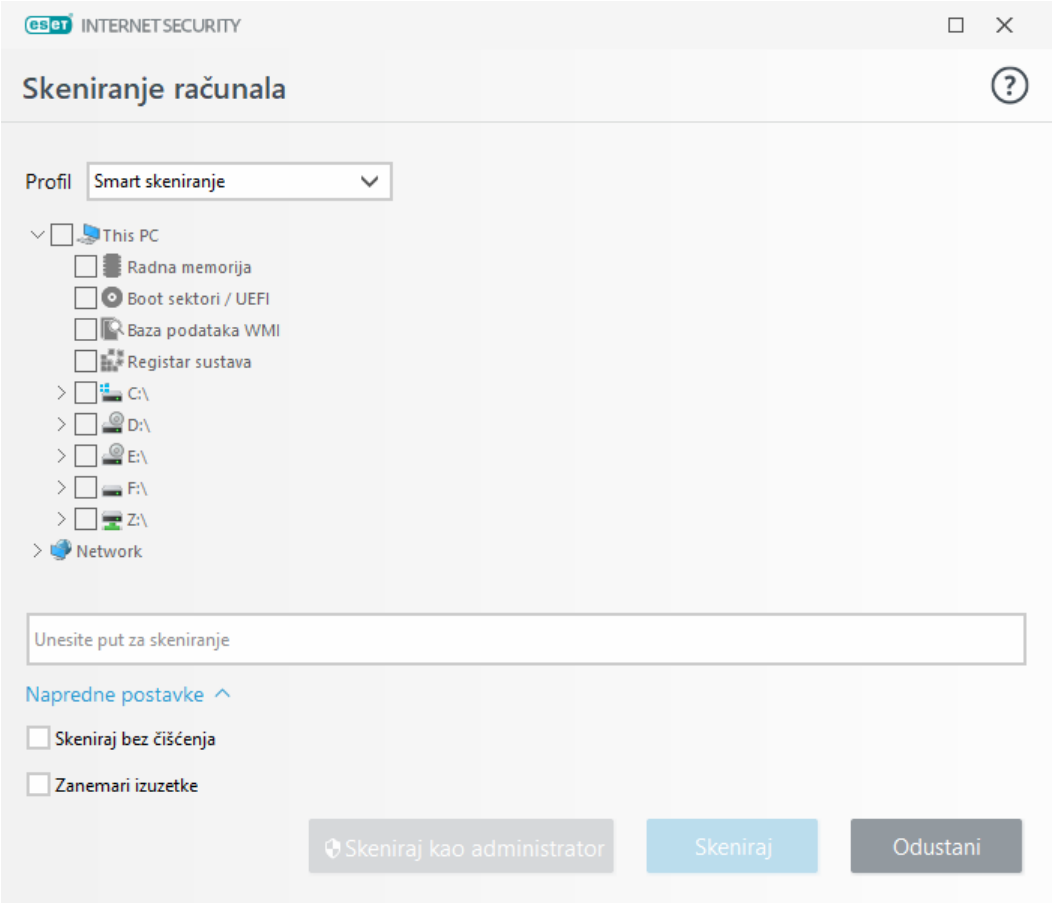
Struktura mape (stablo) također sadrži specifične ciljeve skeniranja.

- **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 cilja skeniranja (datoteke ili mape), upišite njegov put u tekstno polje ispod strukture stabla. Put je osjetljiv na velika i mala slova. Da biste cilj uključili u skeniranje, označite njegov potvrdni okvir u strukturi stabla.

Zakazivanje tjednog skeniranja računala

Da biste zakazali redoviti zadatak, pročitajte poglavlje Zakazivanje tjednog skeniranja računala.



Možete konfigurirati parametre čišćenja za skeniranje pod **Napredno podešavanje** (F5) > **Modul detekcije** > **Skeniranje na zahtjev** > **ThreatSense parametri** > **Čišćenje**. Da biste pokrenuli skeniranje bez čišćenja, odaberite mogućnost **Napredno podešavanje** > **Skeniranje bez čišćenja**. Povijest skeniranja sprema se u dnevnik skeniranja.

Kada je odabrana opcija **Zanemari izuzetke**, datoteke s prethodno izuzetim ekstenzijama skenirat će se bez iznimke.

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

Mogućnost **Skeniraj kao administrator** omogućuje vam skeniranje s administratorskog računa. Koristite se tom mogućnosti ako trenutačno prijavljeni korisnik nema dovoljno ovlasti za pristup datotekama koje želite skenirati. Taj gumb nije dostupan ako trenutačno prijavljeni korisnik ne može zakazivati operacije kontrole korisničkih računa kao administrator.

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.

Uobičajeno je da se neke datoteke, na primjer one koje su zaštićene lozinkom ili datoteke koje koristi isključivo sustav (najčešće *pagefile.sys* i određeni dnevnici), ne mogu skenirati. Više informacija možete pronaći u članku u bazi znanja.

Zakazivanje tjednog skeniranja računala

Da biste zakazali redoviti zadatak, pročitajte poglavlje Zakazivanje tjednog skeniranja računala.

Napredak skeniranja – Na traci napretka prikazuju se paralelno 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.

Pronađeno prijetnji – Prikazuje ukupan broj skeniranih datoteka, pronađenih prijetnji i prijetnji koje su izbrisane tijekom skeniranja.

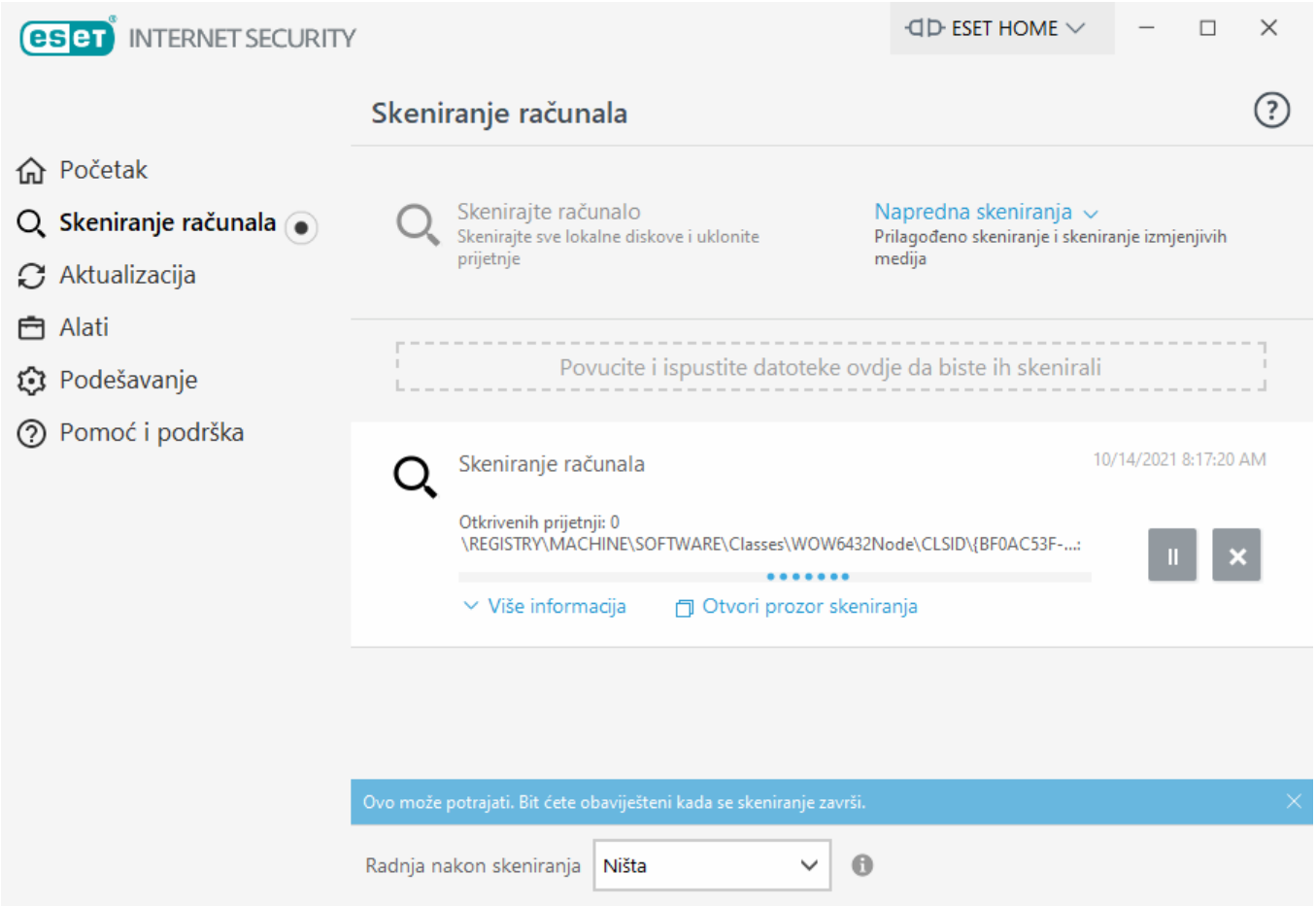
Pauza – Pauzira skeniranje.

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.

Kliknite povećalo ili strelicu da biste pregledali detalje skeniranja koje je u tijeku. Možete pokrenuti još jedno, paralelno skeniranje tako da kliknete **Skenirajte svoje računalo** ili **Napredna skeniranja** > **Prilagođeno skeniranje**.



Padajući izbornik **Radnja nakon skeniranja** omogućava postavljanje automatskog pokretanja radnje nakon dovršetka skeniranja:

- **Bez radnje** – Kada skeniranje završi, neće se izvršiti nijedna radnja.
- **Isključi** – Kada skeniranje završi, računalo se isključuje.
- **Ponovno pokreni** – Zatvara sve otvorene programe i restarta računalo kada završi skeniranje.
- **Ponovno pokreni po potrebi** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Prisilno ponovno pokreni** – prisilno zatvara sve otvorene programa bez čekanja interakcije korisnika i ponovno pokreće računalo nakon što se skeniranje dovrši.
- **Prisilno ponovno pokrenite ako je potrebno** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **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.

> Radnje **Mirovanje** ili **Hibernacija** dostupne su na temelju postavki operacijskog sustava na vašem računalu za uštedu energije i stanje mirovanja ili na temelju mogućnosti stolnog/prijenosnog računala. Imajte na umu da računalo koje je u stanju mirovanja i dalje radi. I dalje pokreće osnovne funkcije i troši električnu energiju dok se napaja putem baterije. Da bi baterija dulje trajala, na primjer, kada se nalazite izvan ureda, preporučujemo da upotrijebite opciju Hibernacija.

Odabrana radnja će započeti nakon završetka svih trenutačno pokrenutih skeniranja. Kada odaberete opciju **Isključi** ili **Ponovno pokreni**, prikazat će se potvrdni dijaloški okvir za potvrdu s istekom vremena od 30 sekundi (kliknite **Odustani** da biste deaktivirali zatraženu radnju).

Dnevnik skeniranja računala

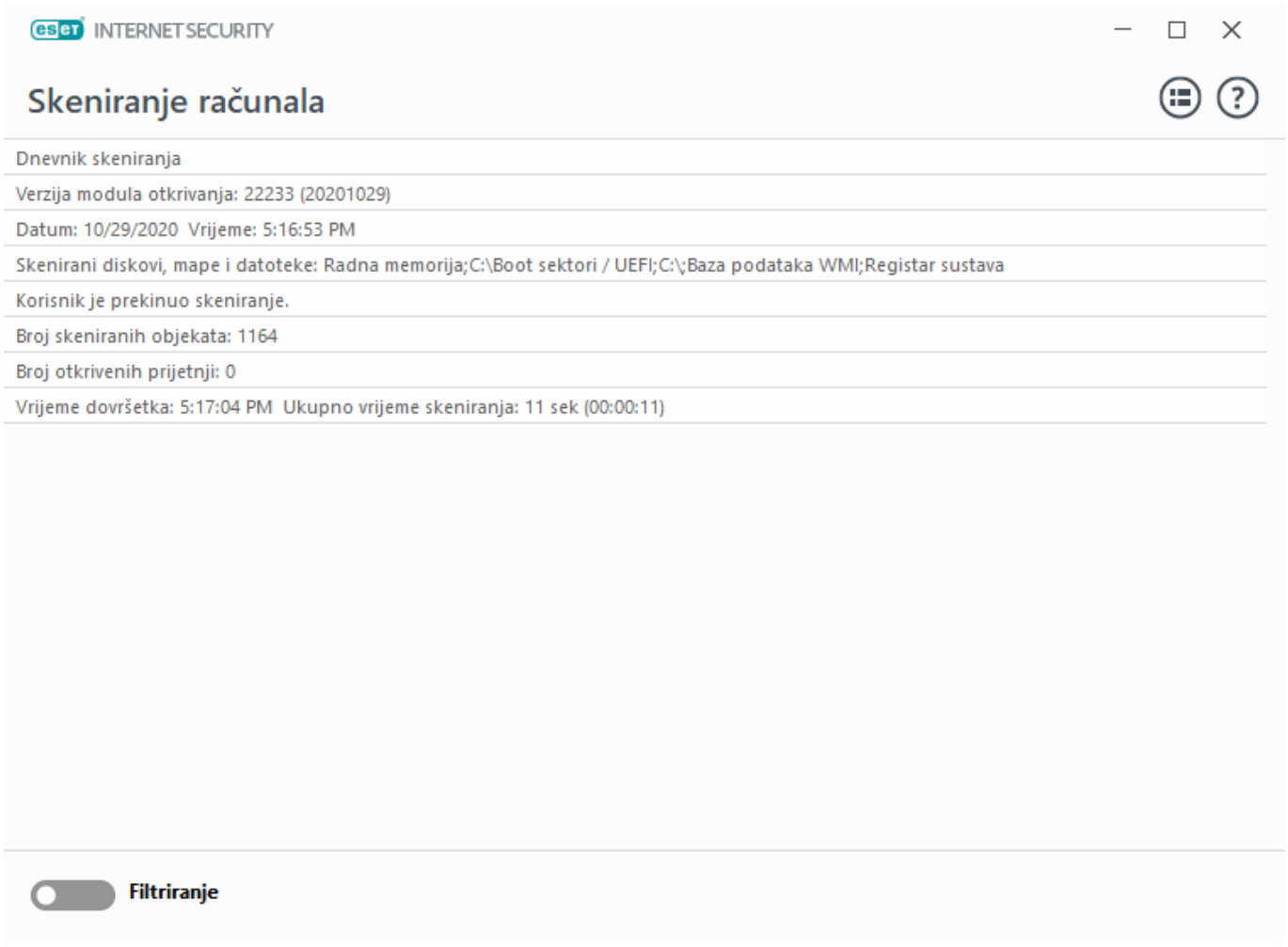
Po završetku skeniranja otvara se Dnevnik skeniranja računala sa svim relevantnim informacijama povezanima s određenim skeniranjem. Dnevnik skeniranja pruža vam informacije kao što su:

- Verzija modula za otkrivanje virusa
- Datum i vrijeme početka
- Popis skeniranih diskova, mapa i datoteka
- Naziv planiranog skeniranja (samoplanirano skeniranje)
- Status skeniranja
- Broj skeniranih objekata
- Broj otkrivenih prijetnji
- Vrijeme dovršetka

- Ukupno vrijeme skeniranja

Novi početak planiranog zadatka skeniranja računala se preskače ako se još uvijek izvodi isti planirani zadatak koji je prethodno pokrenut. Preskočeni zadatak planiranog skeniranja će stvoriti Dnevnik skeniranja računala s 0 skeniranih objekata i statusom **Skeniranje se nije pokrenulo jer je prethodno skeniranje još uvijek bilo u tijeku**.

Da biste pronašli prethodne dnevnike skeniranja, u glavnom programskom prozore odaberite **Alati** > **Više alata** > **Dnevnici**. U padajućem izborniku odaberite **Skeniranje računala** i dvaput kliknite željeni zapis.



Dodatne informacije o zapisima koje "nije moguće otvoriti", s "pogreškom prilikom otvaranja" i/ili s "oštećenom arhivom" potražite u članku ESET-ove baze znanja.

Kliknite ikonu trake klizača **Filtriranje** da biste otvorili prozor Filtriranje dnevnika u kojem možete suziti pretraživanje prema prilagođenim kriterijima. Za prikaz kontekstnog izbornika klikom desne tipke miša odaberite određenu stavku u dnevniku:

Akcija	Korištenje
Filtriraj iste zapise	Aktivira filtriranje dnevnika. Dnevnik će prikazati samo zapise iste vrste kao što je odabrani.
Filtar	Ova opcija otvara prozor Filtriranje dnevnika i omogućuje vam da definirate kriterije za određene stavke u dnevniku. Prečac: `Ctrl+Shift+F`
Aktiviraj filtar	Aktivira postavke filtra. Ako prvi put aktivirate filtar, morate definirati postavke, nakon čega se otvara prozor Filtriranje dnevnika.

Akcija	Korištenje
Deaktiviraj filtar	Isključuje filtar (isto kao i klik na prekidač u donjem dijelu).
Kopiraj	Kopira istaknute zapise u međuspremnik. Prečac: `Ctrl+C`
Kopiraj sve	Kopira sve zapise u prozoru.
Izvoz	Izvozi istaknute zapise u međuspremnik, u XML datoteku.
Izvezi sve	Ova opcija izvozi sve zapise u prozoru u XML datoteku.
Opis prijetnje	Otvara enciklopediju prijetnji tvrtke ESET koja sadrži detaljne informacije o opasnostima i simptomima istaknute infiltracije.

Skeniranja za zlonamjerne softvere

Odjeljak **Skeniranje zlonamjernih programa** dostupan je u odjeljku **Napredno podešavanje** (F5) > **Modul detekcije** > **Skeniranje zlonamjernih programa** i pruža opcije za odabir parametara skeniranja. Taj odjeljak sadrži sljedeće stavke:

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 Profili skeniranja.

Objekti skeniranja – ako samo želite skenirati određeni objekt, možete kliknuti **Uredi** pored stavke **Objekti skeniranja** i odabrati opciju iz padajućeg izbornika ili odabrati određene objekte iz strukture mapa (stablaste strukture). Pojedinosti potražite u odjeljku Ciljevi skeniranja.

ThreatSensepodešavanje parametara sustava – 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

Aktivirajte traku klizača uz stavku **Aktiviraj skeniranje u stanju mirovanja** da biste aktivirali ovu funkciju. Kad se računalo nalazi u stanju mirovanja, na svim lokalnim pogonima se provodi tiho skeniranje računala.

Prema standardnim postavkama skener za stanje mirovanja ne pokreće se kada se računalo (prijenosno računalo) napaja iz baterije. Ovu postavku možete zaobići aktiviranjem trake klizača uz stavku **Pokreni čak i ako se računalo napaja putem baterije** u naprednom podešavanju.

Aktivirajte traku klizača pored stavke **Aktiviraj vođenje dnevnika** u naprednom podešavanju da biste zapisali rezultate skeniranja računala u odjeljku Dnevnici (iz glavnog prozora programa kliknite **Alati** > **Više alata** > **Dnevnici** i zatim odaberite **Skeniranje računala** iz 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.

Profili skeniranja

U programu ESET Internet Security 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.

> Pretpostavimo 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 primijeniti **Uvijek ukloni prijetnju**. 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

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 cilja skeniranja (datoteke ili mape), upišite njegov put u tekstno polje ispod strukture stabla. Put je osjetljiv na velika i mala slova. Da biste cilj uključili u skeniranje, označite njegov potvrdni okvir u strukturi stabla.

Kontrola uređaja

ESET Internet Security 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 Spremište
- 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**.

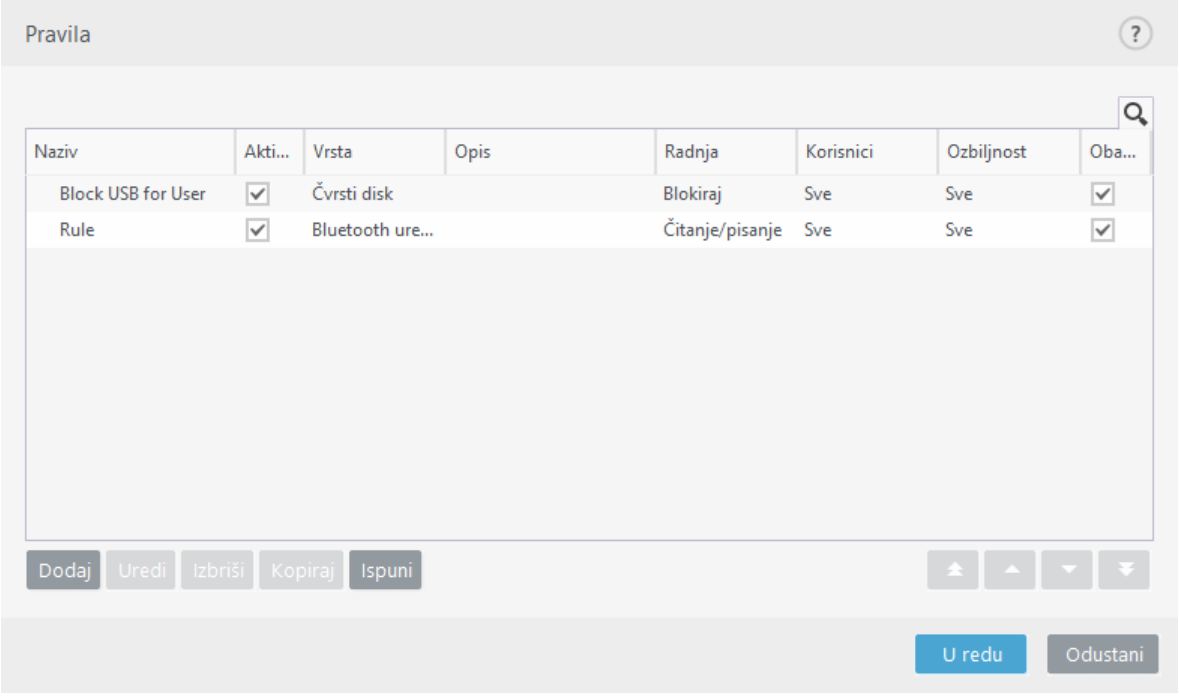
Aktivirajte traku klizača uz stavku **Aktiviraj kontrolu uređaja** da biste aktivirali funkciju kontrole uređaja u programu ESET Internet Security. Morat ćete ponovno pokrenuti računalo da bi ova promjena stupila na snagu. Nakon što se kontrola uređaja aktivira, **pravila** će postati aktivna, što će omogućiti otvaranje prozora Uređivač pravila.

> 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 radnjom **Čitaj/piši** ili **Samo čitaj**. Tako će svi uređaji koje kontrola uređaja ne prepoznaje biti blokirani prilikom povezivanja na vaše računalo.

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.



Moguće je dopustiti ili blokirati određene uređaje po korisniku ili korisničkoj grupi na temelju parametara dodatnih uređaja koje je moguće odrediti u konfiguraciji pravila. Popis pravila sadrži nekoliko opisa pravila poput naziva, vrste vanjskog uređaja, radnje koju treba provesti nakon povezivanja vanjskog uređaja s računalom i opširnosti vođenja dnevnika. Također pogledajte stavku Dodavanje pravila kontrole uređaja.

Kliknite **Dodaj** ili **Uredi** da biste upravljali pravilom. Kliknite **Kopiraj** da biste stvorili novo pravilo s unaprijed definiranim mogućnostima koje se koriste za drugo odabrano pravilo. XML nizovi koji se prikazuju kada se klikne pravilo mogu se kopirati u međuspremnik kako bi pomogli administratorima sustava da izvezu/uvezu te podatke i

koriste ih, na primjer u programu .

Pritiskom tipke **CTRL** i klikom možete odabrati više pravila i primijeniti radnje, kao što su brisanje ili pomicanje prema gore ili dolje na popisu, na sva odabrana pravila. Potvrdni okvir **Aktivirano** deaktivira ili aktivira pravilo; to može biti korisno ako ne želite trajno izbrisati pravilo u slučaju da ga ubuduće želite koristiti.

Kontrola se postiže pravilima koja su sortirana prema redoslijedu prioriteta, s pravilima višeg prioriteta na vrhu.

Unosi u dnevniku mogu se pregledati u glavnom prozoru programa ESET Internet Security, u odjeljku **Alati** > **Više alata** > Dnevnici.

Dnevnik kontrole uređaja bilježi sve slučajeve uključivanja kontrole uređaja.

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).

Odaberite uređaj s popisa otkrivenih uređaja i kliknite **U redu** kako biste dodali pravilo kontrole uređaja s unaprijed definiranim informacijama (sve postavke se mogu prilagoditi).

Uređaji u načinu rada male snage (stanje mirovanja) označeni su ikonom upozorenja . Da biste aktivirali gumb **U redu** i dodali pravilo za ovaj uređaj:

- Ponovno povežite uređaj
- Upotrebljavajte uređaj (na primjer, pokrenite aplikaciju Kamera u sustavu Windows da biste probudili web kameru)

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).

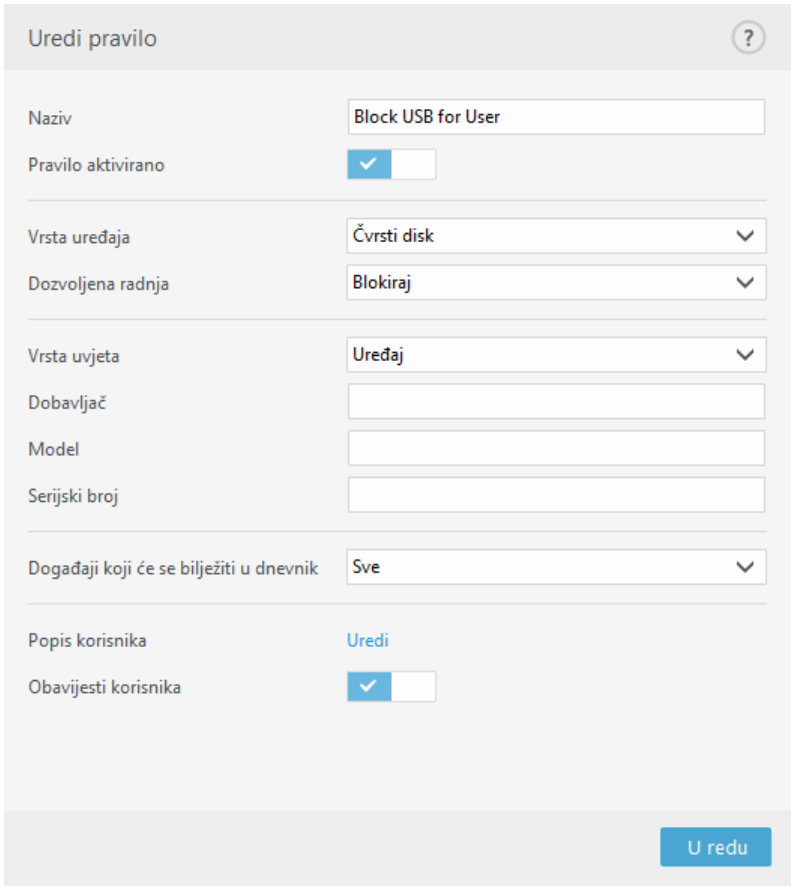
Kada završite s prilagodbom, kliknite **U redu**. Kliknite **Odustani** ako želite zatvoriti prozor **Grupe uređaja** bez spremanja promjena.

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 radnjom **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 radnje (npr. radnja **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.



Unesite opis pravila u polje **Naziv** radi bolje identifikacije. Kliknite traku klizača uz opciju **Pravilo aktivirano** da biste deaktivirali ili aktivirali to pravilo; to može biti korisno ako ne želite trajno izbrisati pravilo.

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 elektroničkim 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 radnjama, bez informacija o korisnicima, mogu se samo globalno blokirati.

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 radnje (npr. radnja **Samo za čitanje**

nije dostupna za Bluetooth, što znači da je Bluetooth uređaje moguće samo dopustiti, blokirati ili upozoriti).

Vrsta uvjeta

Odaberi **Grupa uređaja** ili **Uređaj**.

Pomoću 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.

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 (*, ?).

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

ESET Internet Security sprema sve važne događaje u dnevnik koji je moguće prikazati izravno iz glavnog izbornika. Kliknite **Alati** > **Više alata** > **Dnevnici**, a zatim odaberite **Kontrola uređaja** u padajućem izborniku **Dnevnik**.

- **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 uspješnoj nadogradnji, te svi prethodno navedeni zapisi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke s upozorenjima.
- **Ništa** – neće se stvoriti dnevnici.

Popis korisnika

Pravila je moguće ograničiti na određene korisnike ili grupe korisnika tako da ih dodate na popis korisnika klikom na **Uredi** pored opcije **Popis korisnika**.

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

Ograničenja popisa korisnika

Popis korisnika ne može se definirati za pravila s određenim vrstama uređaja:

- USB pisač
- Bluetooth uređaj
- Čitač pametnih kartica
- Uređaj za obradu slike
- Modem
- LPT/COM port

Obavijesti korisnika – ako se umetne uređaj blokiran postojećim pravilom, prikazat će se prozor obavijesti.

Zaštita web-kamere

Zaštita web kamere obavještava vas o procesima i aplikacijama koje pristupaju web kameri računala. Ako aplikacija pokuša pristupiti kameri, primit ćete obavijest u kojoj možete **dopustiti** ili **blokirati** pristup. Boja prozora upozorenja ovisi o reputaciji aplikacije.

Opcije podešavanja zaštite web kamere mogu se izmijeniti pod **Napredno podešavanje** (F5) > **Kontrola uređaja** > **Zaštita web kamere**.

Da biste aktivirali funkciju zaštite web kamere u sustavu ESET Internet Security, aktivirajte traku klizača pokraj opcije **Aktiviraj zaštitu web kamere**.

Kada se zaštita web kamere aktivira, stavka **Pravila** će postati aktivna, što će omogućiti otvaranje prozora Uređivač pravila.

Da biste isključili upozorenja za aplikacije s prisutnim pravilom koje su izmijenjene, ali još uvijek imaju valjan digitalni potpis (na primjer, nadogradnja aplikacije), aktivirajte traku klizača pokraj opcije **Deaktiviraj upozorenja o pristupu web-kameri za izmijenjene aplikacije**.

Uređivač pravila zaštite web-kamere

Ovaj prozor prikazuje postojeća pravila i omogućuje kontrolu aplikacija i procesa koji pristupaju web-kameri računala na temelju poduzete radnje.

Na raspolaganju su sljedeće akcije:

- **Dopusti pristup**
- **Blokiraj pristup**

- **Pitaj** (pita korisnika svaki put kada aplikacija pokuša pristupiti web kameri)

Poništite odabir potvrdnog okvira u stupcu **Obavijesti** da biste prestali primati obavijesti kada aplikacije pristupe web kameri.

Ilustrirane upute

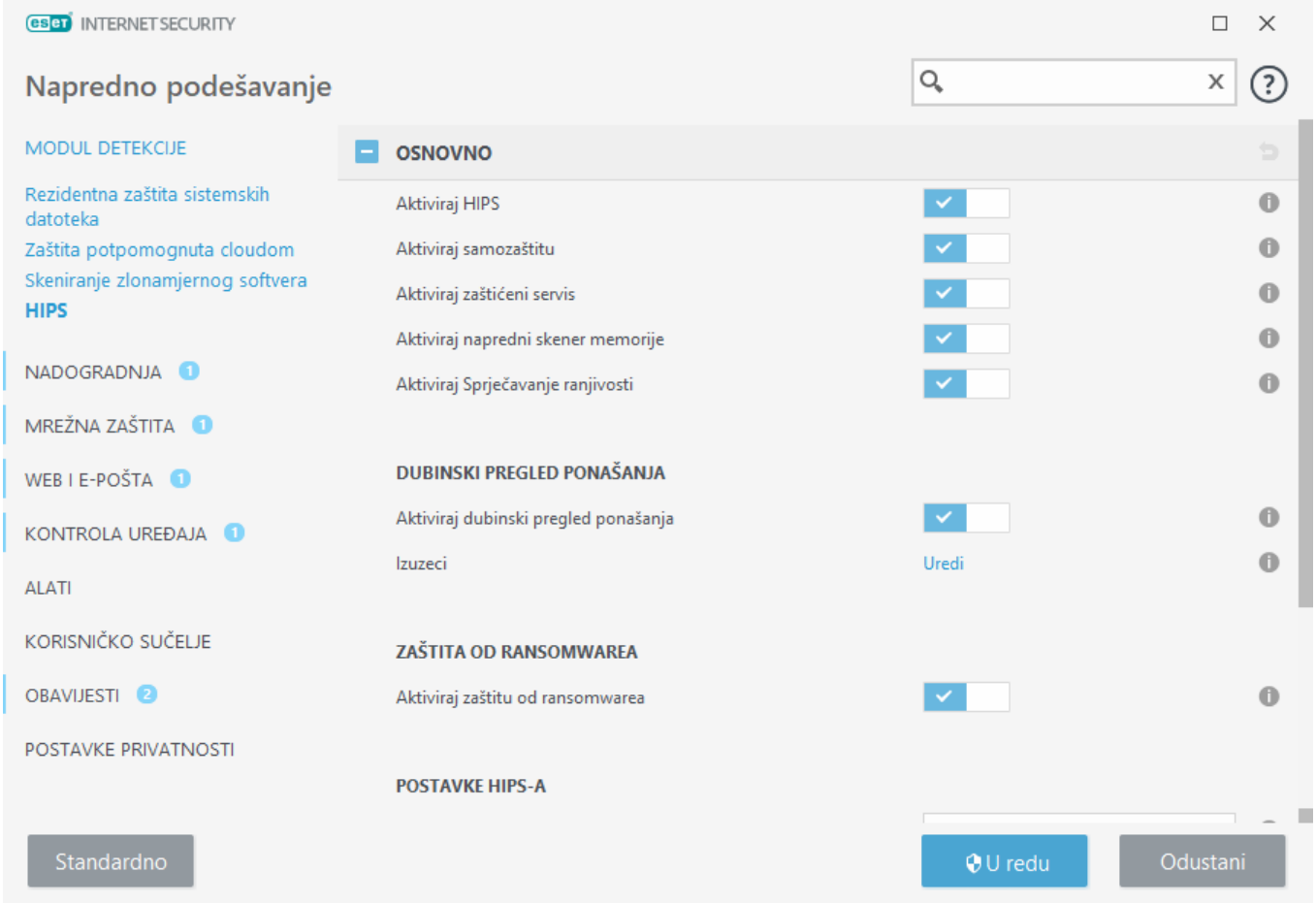
Stvaranje i uređivanje pravila web kamere u programu ESET Internet Security.

Sustav za sprečavanje upada (HIPS)

Samo bi iskusan korisnik trebao mijenjati HIPS postavke. Neispravno konfiguriranje HIPS postavki može uzrokovati nestabilnost sustava.

Sustav za sprječavanje 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.

Postavke za HIPS možete pronaći pod **Napredno podešavanje** (F5) > **Modul za otkrivanje** > **HIPS** > **Osnovno**. Stanje značajke HIPS (aktivirano/deaktivirano) prikazuje se u glavnom prozoru programa ESET Internet Security, u oknu **Podešavanje** > **Zaštita računala**.



Osnovno

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

Aktiviraj samozaštitu – ESET Internet Security 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.

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 noviji.

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. Prema standardnim postavkama napredni je skener memorije aktiviran. Više o toj vrsti zaštite pročitajte u rječniku.

Aktiviraj zaštitu od zloupotrebe – Osmišljena 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. 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 zloćudno.

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.

Postavke HIPS-a

Način filtriranja može se izvesti na jedan od sljedećih načina:

Način filtriranja	Opis
Automatski način rada	Operacije su aktivirane, uz iznimku onih koje su blokirane putem unaprijed definiranih pravila koja štite vaš sustav.
Pametni način rada	Korisnik će biti obaviješten samo o vrlo sumnjivim događajima.
Interaktivni način	Korisnik će dobiti upit da potvrdi operacije.
Način rada na temelju pravila	blokira sve operacije koje nisu definirane određenim pravilom koje ih dopušta.
Način rada za učenje	Operacije su aktivirane i pravilo se stvara nakon svake operacije. Pravila stvorena u ovom načinu rada mogu se prikazati u **Uređivaču HIPS pravila**, ali je njihov prioritet niži od prioriteta ručno stvorenih pravila ili pravila koja su stvorena u automatskom načinu rada. Ako s padajućeg izbornika **načina filtriranja** odaberete **način rada za učenje**, postavka **Način rada za učenje završava 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 odabrati 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 odabrati, 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.

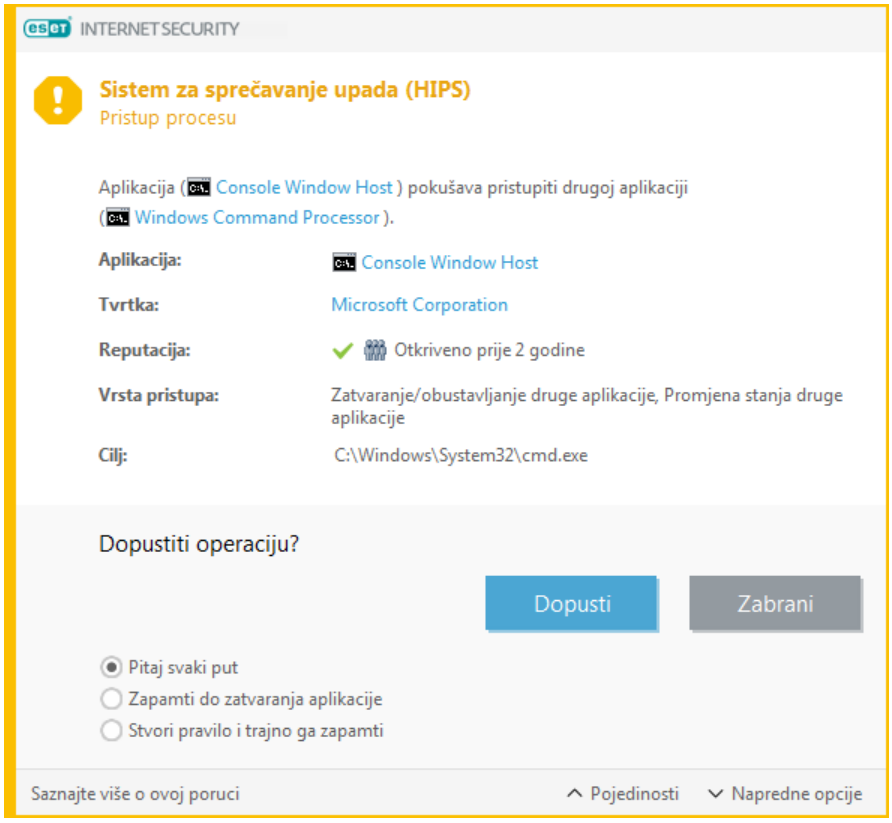
Opcija **Stvori pravilo i trajno ga zapamti** stvorit će novo HIPS pravilo koje se kasnije može mijenjati u odjeljku HIPS upravljanje pravilima (potrebne administratorske ovlasti).

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**:

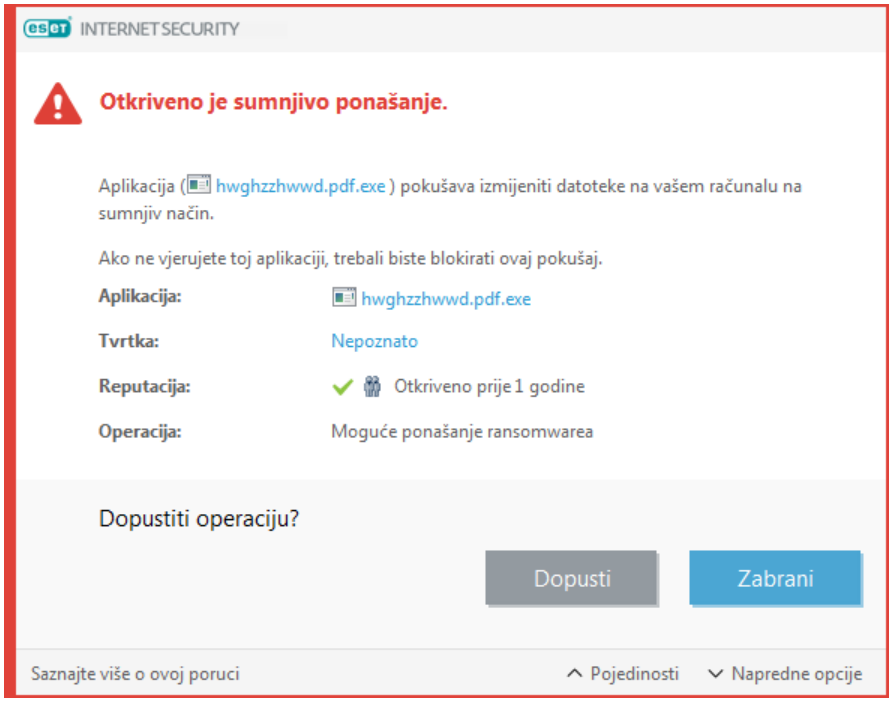
- **Stvori pravilo valjano samo za ovu aplikaciju** – Ako odznačite ovaj potvrdni okvir, pravilo će se stvoriti za sve izvorne aplikacije.
- **Samo za operaciju** – Odaberite operacije pravila za datoteku/aplikaciju/registar. Pogledajte opise svih HIPS operacija.
- **Samo za cilj** – Odaberite ciljeve pravila za datoteku/aplikaciju/registar.

> **Beskrajne HIPS obavijesti?**
> 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

Popis korisnički definiranih i automatski dodanih pravila iz sustava HIPS. Dodatne pojedinosti o stvaranju pravila i HIPS operacijama možete pronaći u poglavlju Postavke HIPS pravila. Također pogledajte Opći princip HIPS-a.

Stupci

Pravilo – Korisnički definiran ili automatski odabran naziv pravila.

Aktivirano – deaktivirajte traku klizača ako želite zadržati pravilo na popisu, ali ga ne želite primijeniti.

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 mali skočni prozor 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 (kao kod pravila firewalla gdje se pravila izvršavaju s vrha prema dnu).

- Sva pravila koja stvorite imaju isti prioritet
- Što je pravilo određenije, 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)

Uredite HIPS pravilo

Prvo 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 odabrati vrstu operacije na koje će se pravilo primijeniti. Pravilo će se koristiti samo za tu vrstu operacije i za odabrani cilj.

Aktivirano – deaktivirajte traku klizača ako želite zadržati pravilo na popisu, ali ne i primijeniti ga.

Razina ozbiljnosti za vođenje dnevnika – Ako aktivirate ovu opciju, informacije o ovom pravilu bit će zapisane u HIPS dnevnik.

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

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

Izvorne aplikacije – Pravilo će 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 će 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 će 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 će se koristiti samo ako se operacija odnosi na taj objekt. S padajućeg izbornika odaberite **Specifični unosi** i kliknite **Dodaj** za ručno upisivanje ili kliknite **Uređivač otvorenog registra** za odabir ključa iz Registra. Osim toga, možete odabrati stavku **Svi unosi** s padajućeg izbornika da biste dodali sve aplikacije.

> 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.

Opisi važnih operacija:

Operacije datoteke

- **Izbriši datoteku** – Aplikacija traži dopuštenje za brisanje ciljane datoteke.
- **Piši u datoteku** – Aplikacija traži dopuštenje za zapisivanje u ciljanu datoteku.
- **Izravan pristup disku** – Aplikacija pokušava očitati podatke s diska ili zapisivati na disk na nestandardan način koji zaobilazi uobičajene procedure sustava Windows. To može rezultirati izmjenom datoteka bez primjene odgovarajućih pravila. Tu operaciju može uzrokovati zlonamjerni softver koji pokušava izbjeći

otkrivanje, softver za sigurnosno kopiranje koji pokušava napraviti točnu kopiju diska ili upravitelj particije koji pokušava reorganizirati podatke na disku.

- **Instaliraj globalnu kuku** – Odnosi se na pozivanje funkcije SetWindowsHookEx iz biblioteke MSDN.

- **Učitaj upravljački program** – Instalacija i učitavanje upravljačkih programa u sustav.

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.

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

Operacije registra

- **Promijeni 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.

- **Izbriši iz registra** – Brisanje ključa registra ili njegove vrijednosti.

- **Promijeni naziv ključa registra** – Mijenja 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.

Prilikom unosa cilja možete koristiti zamjenske znakove uz određena ograničenja. Umjesto određenog ključa, u putovima registra može se koristiti simbol * (zvjezdica). Na primjer, *HKEY_USERS*\software* može značiti *HKEY_USER\.default\software*, no ne i *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
*HKEY_LOCAL_MACHINE\system\ControlSet** nije valjani put ključa registra. Put ključa registra koji sadrži * znači "ovaj put ili bilo koji put na bilo kojoj razini nakon tog simbola". To je jedini način korištenja zamjenskih znakova u ciljnim datotekama. Prvo će se procijeniti specifičan dio puta, a zatim put koji se nalazi iza zamjenskog znaka (*).

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 traku klizača pored **Obavijesti korisnika** da bi se prikazala obavijest svaki put kada se primijeni pravilo.

3. Odaberite barem jednu operaciju u odjeljku **Operacije koje utječu na sljedeće objekte** na koje će se primjenjivati pravilo.

4. Kliknite **Dalje**.

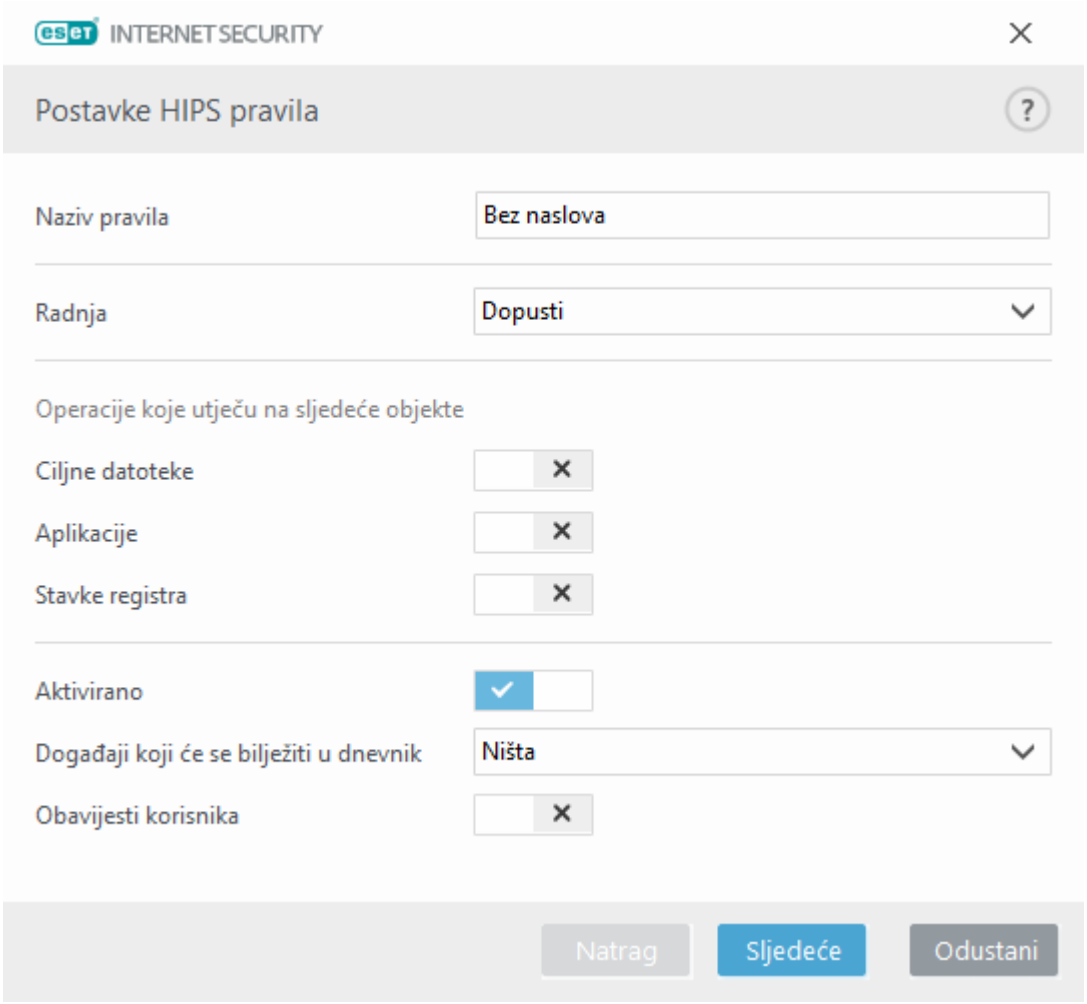
5. U prozoru **Izvorne aplikacije** na padajućem izborniku odaberite **Određene aplikacije** kako biste novo pravilo primijenili na sve aplikacije koje pokušavaju izvršiti bilo koju od odabranih operacija aplikacije na aplikacijama koje ste odredili.

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.



Dodavanje puta aplikacije/registra za HIPS

Put aplikacijske datoteke odaberite klikom na mogućnost **...**. Ako odaberete mapu, uključit će se sve aplikacije koje se nalaze na toj lokaciji.

Mogućnost **Pokreni Registry Editor** pokrenut će uređivač Windows registra (regedit). Prilikom dodavanja puta registra točnu lokaciju unesite u polje **Vrijednost**.

Primjeri puta datoteke ili registra:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

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 konfiguriranom filtarskom načinu, osim ako su izričito blokirani korisničkim pravilom.

Zabilježi sve blokirane operacije – sve blokirane operacije zapisat će se u HIPS dnevnik. Upotrijebite ovu funkciju samo prilikom otklanjanja poteškoća ili kada to zatraži ESET-ova tehnička podrška jer bi se time mogao generirati veliki dnevnik i usporiti rad vašeg računala.

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 filtarskom 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.

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 igranje

Način rada za igranje značajka je za igrače koji softver žele koristiti bez prekida, ne žele biti ometani skočnim prozorima te žele smanjiti korištenje CPU-a. Način rada za igranje može se koristiti i tijekom prezentacija koje se

ne smiju prekidati antivirusnim aktivnostima. Aktiviranjem te funkcije deaktiviraju se svi skočni prozori, a aktivnost planera u potpunosti se prekida. Zaštita sustava i dalje se izvodi u pozadini, no ne zahtijeva nikakvu aktivnost korisnika.

Način rada za igranje možete aktivirati ili deaktivirati u glavnom prozoru programa, u odjeljku **Podešavanje** > **Zaštita računala**, tako da kliknete  ili  uz opciju **Način rada za igranje**. Aktiviranje načina rada za igranje 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 opcija **Aktivan je način rada za igranje** biti označena narančastom bojom.

Aktivirajte **Automatski aktiviraj Način rada za igranje prilikom izvršavanja aplikacija u načinu rada cijelog zaslona** u odjeljku **Napredno podešavanje** (F5) > **Alati** > **Način rada za igranje** da bi se način rada za igranje pokrenuo svaki put kada pokrenete aplikaciju na cijelom zaslonu i da bi se prekinuo nakon što zatvorite aplikaciju.

Aktivirajte **Automatski deaktiviraj način rada za igranje nakon** da biste definirali nakon koliko će se vremena način rada za igranje automatski deaktivirati.

> Ako je firewall u Interaktivnom načinu i aktiviran je Način rada za igranje, možda ćete imati poteškoće pri povezivanju s internetom. To može biti problematično ako pokrenete igru koja se povezuje na internet. Obično će se od vas zatražiti da potvrdite takvu radnju (ako nije definirano nijedno komunikacijsko pravilo ili iznimka), no u Načinu rada za igranje intervencija korisnika je deaktivirana. Da biste omogućili komunikaciju, definirajte komunikacijsko pravilo za sve aplikacije koje bi mogle imati taj problem ili upotrijebite drugi filtarski način rada u firewallu. Imajte na umu da bi, aktivirate li Način rada za igranje i potom posjetite web stranicu ili aplikaciju koja može predstavljati sigurnosni rizik, one mogle biti blokirane bez ikakvog objašnjenja ili upozorenja jer je interakcija s korisnikom onemogućena.

Skeniranje pri pokretanju

Prema standardnim postavkama prilikom pokretanja sustava ili nadogradnje modula za otkrivanje pokreće se automatska provjera pokretačkih datoteka. To skeniranje ovisi o mogućnosti Konfiguracija i zadaci planera.

Mogućnosti skeniranja pri pokretanju spadaju pod zadatak planera **Provjera datoteke za pokretanje sustava**. Da biste izmijenili njegove postavke, idite na **Alati** > **Više alata** > **Planer** i kliknite na **Automatska provjera pokretačke datoteke** te zatim na **Uredi**. U zadnjem koraku prikazat će se prozor Automatska provjera pokretačkih datoteka (dodatne pojedinosti potražite u sljedećem poglavlju).

Detaljne upute o stvaranju i upravljanju zadacima planera potražite u odjeljku 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 mjesta 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 mjesta kojima je moguće pristupiti samo nakon prijave korisnika (obuhvaća datoteke koje su pokrenute samo za određenog korisnika, obično datoteke u direktoriju *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Popisi datoteka koje je potrebno skenirati fiksni su za svaku prethodno navedenu grupu. Ako odaberete manju dubinu skeniranja za datoteke koje se pokreću prilikom pokretanja sustava, datoteke koje se ne skeniraju skenirat će se nakon otvaranja ili pokretanja.

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** (F5) > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Zaštita dokumenata** i kliknite traku klizača uz **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 prijetnji 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.

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

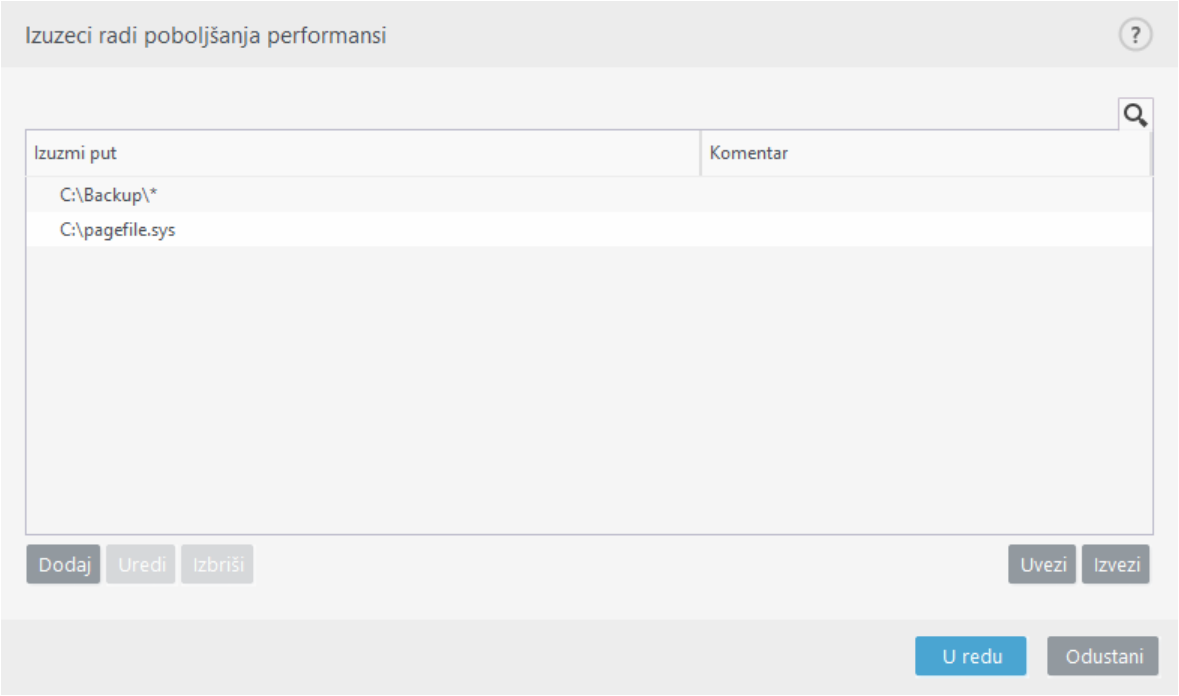
Izuzeci radi poboljšanja performansi omogućuju vam izuzimanje datoteka i mapa od skeniranja.

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**.

> Ne smije se pomiješati s drugim izuzecima kao što su Izuzeci detekcija poznatih prijetnji, Izuzete datotečne ekstenzije, Izuzeci iz HIPS-a ili Izuzeti procesi.

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



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

Kontrolni elementi

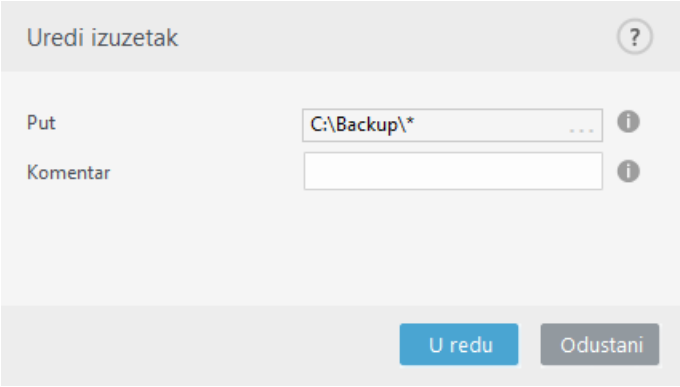
- **Dodaj** – Izuzima objekte od otkrivanja.
- **Uredi** – Omogućuje vam uređivanje odabranih unosa.
- **Ukloni** – uklanja odabrane unose (CTRL + klik za odabir više unosa).

Dodavanje ili uređivanje izuzetka radi poboljšanja performansi

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

Odaberite odgovarajući put ili unesite ručno

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.

Oblik izuzetaka

- 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.

Varijable sustava u izuzecima

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.

Zamjenski znakovi u sredini puta nisu podržani

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 (kao kod pravila firewalla gdje se pravila izvršavaju s vrha prema dnu).
- 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.

Oblik izuzetaka

- 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.

Varijable sustava u izuzecima

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%*

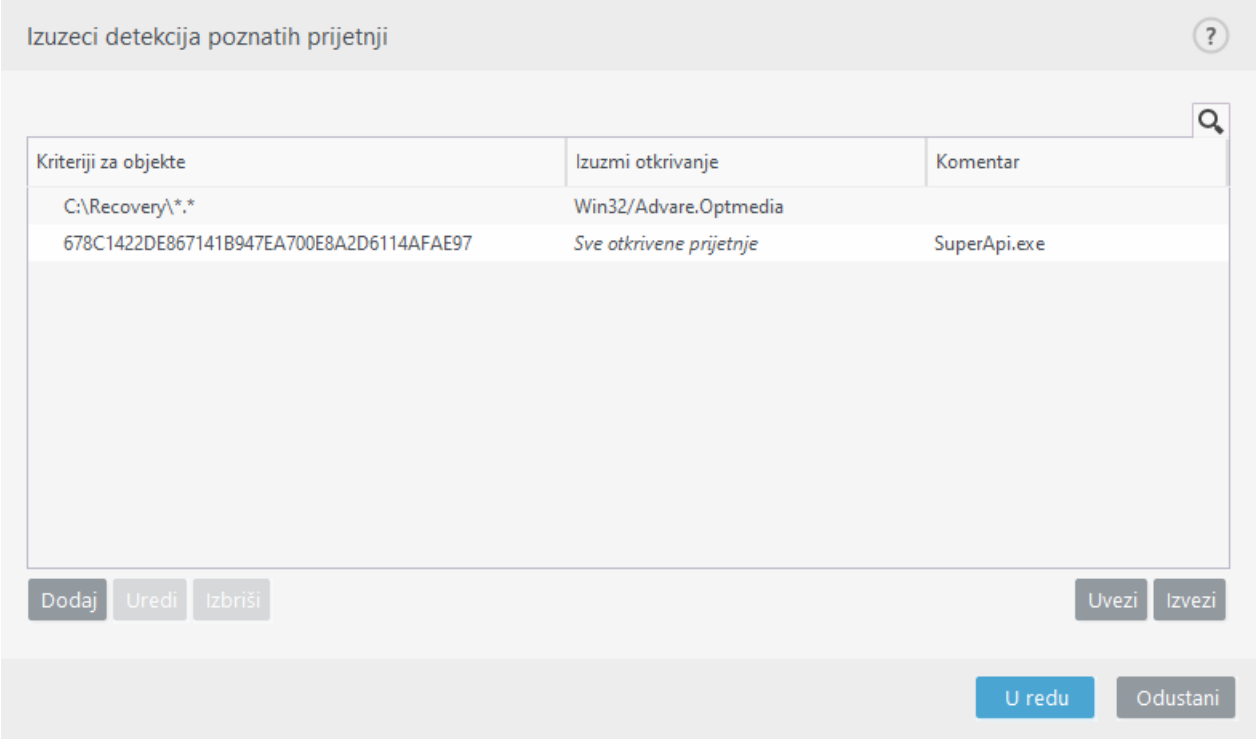
Varijable sustava specifične za korisnika (primjerice *%TEMP%* ili *%USERPROFILE%*) ili varijable okruženja (primjerice *%PATH%*) nisu podržane.

Izuzeci detekcija poznatih prijetnji

Izuzeci detekcija poznatih prijetnji omogućuju vam da izuzmete objekte iz prijetnji filtriranjem naziva prijetnje, puta objekta ili hasha.

Kako funkcioniraju izuzeci detekcija poznatih prijetnji

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.



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**.

Nemojte da vas zbune izuzeci radi poboljšanja performansi, izuzete datotečne ekstenzije, izuzeci iz HIPS-a ili izuzeti procesi.

Da biste izuzeli objekt (prema nazivu prijetnje ili hashu) iz modula detekcije, 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.

• Klikom na opciju **Alati** > **Više alata** > **Karantena**, a potom klikom desne tipke miša na datoteku u karanteni te odabirom stavke **Vrati i izuzmi od skeniranja** u kontekstnom izborniku.

Kriteriji za objekte koji su izuzete otkrivene prijetnje

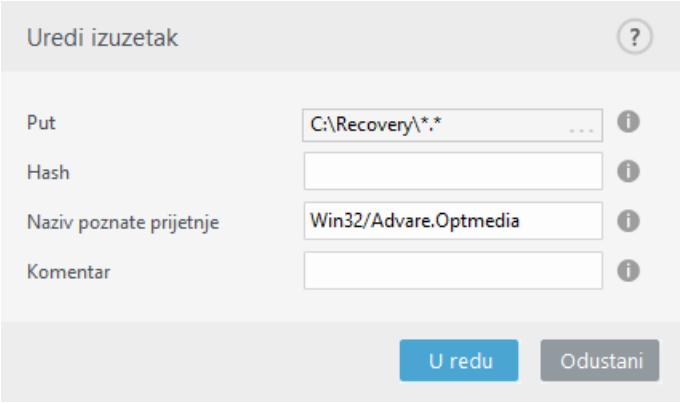
- **Put** – Ograničavanje izuzetih otkrivenih prijetnji na određeni put (ili više njih).
- **Naziv prijetnje** – ako je pored izuzete datoteke naziv prijetnje, to znači da datoteka nije izuzeta u potpunosti, već samo za tu prijetnju. Ako ta datoteka kasnije bude zaražena nekom drugom vrstom zlonamjernog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

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 Internet Security 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.

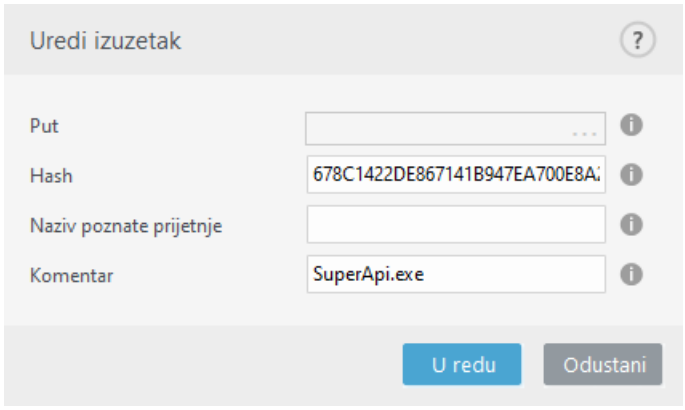
Također pogledajte Format izuzetaka puta.



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.



Izuzeci prema nazivu prijetnje

Da biste izuzeli određenu prijetnju prema nazivu, unesite valjani naziv otkrivene prijetnje:
Win32/Adware.Optmedia
Kada izuzimate otkrivenu prijetnju iz prozora upozorenja programa ESET Internet Security, 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 odabranih 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 Dnevnici (nije dostupno za detekciju zlonamjernih programa):

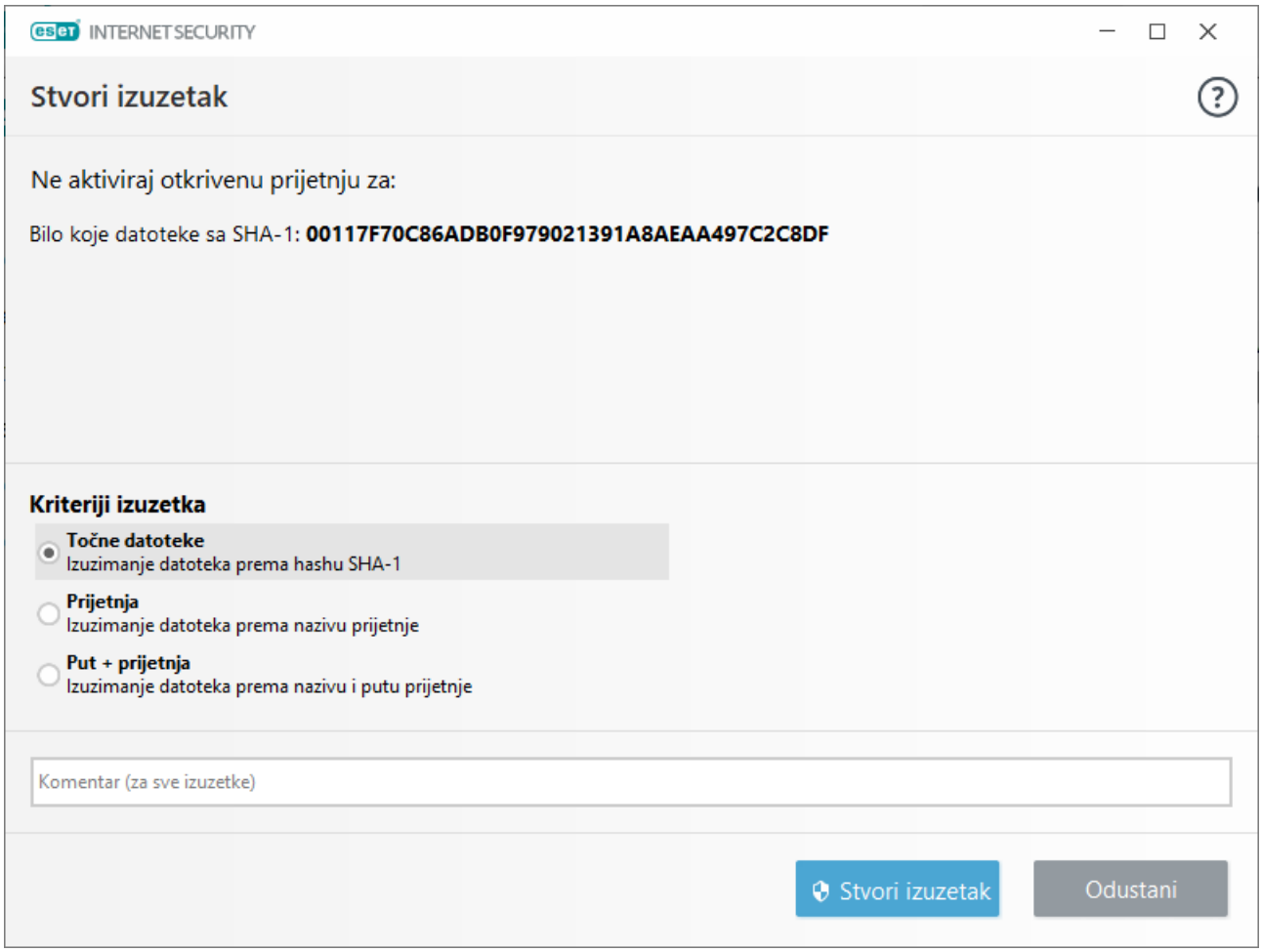
1. U glavnom prozoru programa kliknite **Alati** > **Više alata** > **Dnevnici**.
2. Kliknite desnom tipkom miša prijetnju u **Dnevniku prijetnji**.
3. Kliknite **Stvori izuzetak**.

Za izuzimanje jedne ili više prijetnji na temelju **Kriterija izuzetka** kliknite **Promijeni 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 iz HIPS-a

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

Da biste uredili izuzetke iz HIPS-a, idite na **Napredno podešavanje** (F5) > **Modul detekcije** > **HIPS** > **Osnovno** > **Izuzeci** > **Uredi**.

Ne smije se pomiješati s drugim izuzecima kao što su Izuzete datotečne ekstenzije, Izuzeci detekcija poznatih prijetnji, Izuzeci radi poboljšanja performansi ili Izuzeti procesi.

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

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 mogle 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

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. Dostupne su sljedeće opcije:

Heuristika – Heuristika je algoritam pomoću kojega se analizira (zlonamjerna) aktivnost programa. Glavna prednost ove tehnologije je sposobnost identifikacije zlonamjernog softvera koji nije postojao 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 viruse. 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 Internet Security prilikom čišćenja objekata. Postoje četiri razine čišćenja:

ThreatSense parametri imaju sljedeće razine ispravljanja (tj. čišćenja).

Ispravljanje u programu ESET Internet Security

Razina čišćenja	Opis
Uvijek ispravi prijetnju	Pokušaj ispravljanja 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.
Ispravi otkrivenu prijetnju ako je sigurna, u suprotnom je zadrži	Pokušaj ispravljanja otkrivene prijetnje prilikom čišćenja objekata 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.
Ispravi otkrivenu prijetnju ako je sigurna, u suprotnom postavi pitanje	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.
Uvijek pitaj krajnjeg korisnika	Tijekom čišćenja objekata krajnjem korisniku se prikazuje interaktivno upozorenje i potrebno je odabrati radnju za ispravljanje (npr. uklanjanje ili zanemarivanje). Ta razina namijenjena je naprednijim korisnicima koji znaju koje korake treba poduzeti u slučaju prijetnje.

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

Skeniraj alternativne protoke podataka (ADS) – Alternativni protoci podataka koje koristi datotečni sustav NTFS pridruživanja su datoteka i mapa nevidljiva običnim tehnikama skeniranja. Mnoge infiltracije pokušavaju izbjeći 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 ugniježđenih 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 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. Maksimalna vrijednost je **3 GB**.

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

Datotečne ekstenzije izuzete od skeniranja

Izuzete ekstenzije datoteka su dio ThreatSense parametara. Da biste konfigurirali izuzete ekstenzije datoteka, kliknite opciju **ThreatSense parametri** u prozoru Napredno podešavanje za svaki modul koji upotrebljava ThreatSense tehnologiju.

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 Nemojte da vas zbune izuzeti procesi, izuzeci iz HIPS-a ili izuzete datoteke/mape.

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

Da biste uredili ove postavke, idite na **Napredno podešavanje** (F5) > **Modul detekcije** > **Rezidentna zaštita sistemskih datoteka** > **Dodatni ThreatSense parametri**.

Dodatni ThreatSense parametri za novostvorene i izmijenjene datoteke

Vjerojatnost zaraze novostvorenih ili izmijenjenih datoteka usporedno je veća od zaraze postojećih datoteka. Zbog toga program provjerava ove datoteke s pomoću dodatnih parametara skeniranja. ESET Internet Security upotrebljava naprednu heuristiku koja može otkriti nove prijetnje prije objavljivanja nadogradnje modula detekcije u kombinaciji s metodama skeniranja na temelju potpisa.

Osim novostvorenih datoteka, skeniranje se također provodi na **samoraspakirajućim arhivama** (.sfx) i **runtime packer programima** (interno sažete izvršne datoteke). Prema standardnim postavkama, arhive se skeniraju do desetog stupnja gniježđenja te se provjeravaju bez obzira na njihovu stvarnu veličinu. Da biste izmijenili postavke skeniranja arhive, poništite odabir opcije **Standardne postavke skeniranja arhive**.

Dodatni ThreatSense parametri za pokrenute datoteke

Napredna heuristika pri pokretanju datoteka – Standardno, Napredna heuristika obično se koristi prilikom pokretanja datoteka. Preporučujemo da, dok je ta mogućnost aktivirana, budu aktivirane i mogućnosti Smart optimizacija i ESET LiveGrid® kako se ne bi narušile performanse sustava.

Napredna heuristika pri pokretanju datoteka s izmjenjivih medija – Napredna heuristika imitira kôd u virtualnom okruženju i procjenjuje njegovo ponašanje prije nego se dopusti izvršavanje koda s prijenosnog medija.

Internetska zaštita

Da biste konfigurirali zaštitu weba i e-pošte, u prozoru **Podešavanje** kliknite **Internetska zaštita**. S tog mjesta možete pristupiti detaljnijim postavkama programa.

Da biste pauzirali ili deaktivirali pojedinačne module za zaštitu, kliknite ikonu trake klizača .

Isključivanjem modula za zaštitu može se smanjiti razina zaštite vašeg računala.



Kliknite ikonu zupčanika da biste otvorili web/e-poštu/anti-phishing/antispam zaštite ili zaštite e-pošte u odjeljku Naprednog podešavanja.

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 Internet Security omogućuje nadzor sve komunikacije iz klijenta e-pošte.

Antispam zaštita filtrira neželjene poruke e-pošte.

Za **antispam zaštita** kliknite ikonu zupčanika i odaberite jednu od sljedećih opcija:

- **Konfiguriranje** – Otvara napredne postavke za antispam zaštitu klijenta e-pošte.
- **Korisnički adresar** (ako je aktiviran) – otvaradijaloški okvir u koji možete dodavati adrese, koji možete uređivati ili ukloniti da biste definirali pravila protiv spama. Pravila na ovom popisu primijenit će se na trenutačnog korisnika.
- **Globalni adresar** (ako je aktiviran) – otvaradijaloški okvir u koji možete dodavati adrese, koji možete uređivati ili ukloniti da biste definirali pravila protiv spama. Pravila na ovom popisu će se primijeniti na sve korisnike.

Anti-Phishing zaštita omogućuje blokiranje web stranica koje distribuiraju phishing sadržaj. Preporučujemo da obavezno ostavite Anti-Phishing aktiviran.

Filtriranje protokola

Antivirusnu zaštitu za aplikacijske protokole daje modul za skeniranje ThreatSense u koji su integrirane sve napredne tehnike skeniranja zlonamjernih programa. Filtriranje protokola funkcionira automatski, neovisno o web pregledniku ili klijentu e-pošte koji se koriste. Za uređivanje šifriranih (SSL/TLS) 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 Internet Security (zaštita web pristupa, zaštita protokola za e-poštu, anti-phishing zaštita, roditeljska kontrola) 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.

Dodaje (na primjer *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podmreža – Podmreža (grupa računala) definira se putem IP adrese i maske (na primjer: *2002:c0a8:6301:1::1/64*).

Primjer izuzetih IP adresa

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.

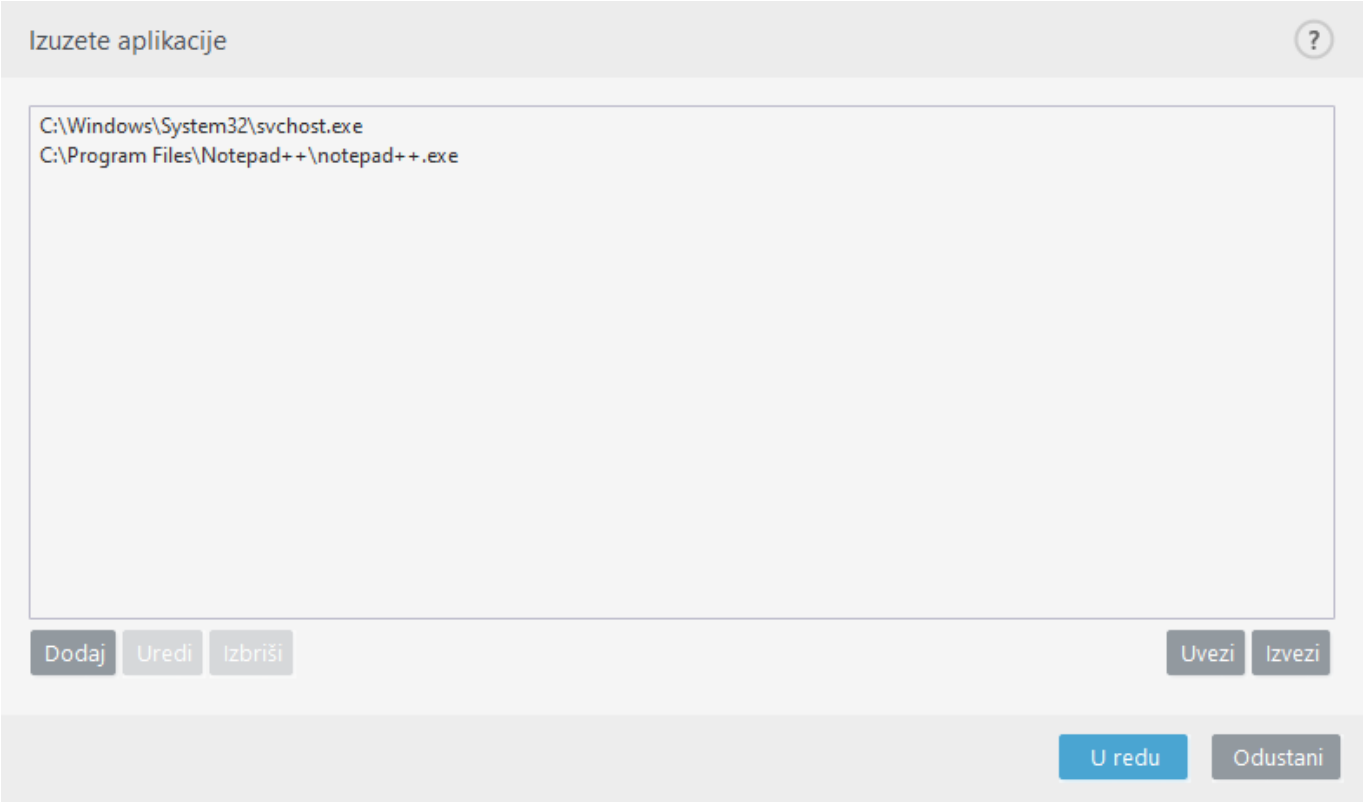
IPv6 adresa i maska:

- *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:c0a8:6301:0001:0000:0000:0000:0000 do 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

Izuzete aplikacije

Da biste komunikaciju određenih aplikacija koje su svjesne mreže isključili iz filtriranja sadržaja, odaberite ih na popisu. HTTP/POP3/IMAP komunikacija odabranih aplikacija neće se provjeravati da bi se pronašle prijetnje. Preporučujemo da tu mogućnost koristite samo za aplikacije koje ne rade ispravno ako se njihova komunikacija provjerava.

Aplikacije i servisi koji se izvršavaju bit će ovdje dostupni automatski. Kliknite **Dodaj** da biste ručno odabrali aplikaciju koja nije prikazana na popisu za filtriranje protokola.



Izuzete IP adrese

Unosi na 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.

Kliknite **Dodaj** za isključivanje IP adrese/raspona adresa/podmreže udaljene točke koja nije na popisu za filtriranje protokola.

Kliknite **Izbriši** za uklanjanje odabranih unosa s popisa.



Dodaj IPv4 adresu

Ova vam mogućnost dopušta dodavanje IP adrese, raspona adresa ili podmreže udaljene točke na koju se primjenjuje pravilo. Verzija internetskog protokola 4 starija je verzija, ali još uvijek se najčešće koristi.

Zasebna adresa – Time se dodaje IP adresa pojedinačnog računala na koje treba primijeniti pravilo (na primjer *192.168.0.10*).

Raspon adresa – Unesite početnu i završnu IP adresu da biste odredili IP raspon (nekoliko računala) na koja se pravilo treba primijeniti(na primjer od *192.168.0.1* do *192.168.0.99*).

Podmreža – 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.

Dodaj IPv6 adresu

Ovo vam omogućuje dodavanje IPv6 adrese ili podmreže udaljene točke na koju se primjenjuje pravilo. To je najnovija verzija internetskog protokola koja će zamijeniti stariju verziju 4.

Zasebna adresa – Time se dodaje IP adresa pojedinačnog računala na koje treba primijeniti pravilo (na primjer *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podmreža – Podmreža (grupa računala) definira se putem IP adrese i maske (na primjer: *2002:c0a8:6301:1::1/64*).

SSL/TLS

ESET Internet Security 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.

Omogući filtriranje SSL/TLS protokola – 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
Automatski način rada	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.
Interaktivni način	Ako unesete novu web stranicu s SSL zaštitom (s nepoznatim certifikatom), prikazat će se prozor za odabir radnje. Taj način rada omogućuje vam stvaranje popisa SSL certifikata / aplikacija koji će se izuzeti od skeniranja.
Način rada prema zadanim pravilima	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 Internet Security za određene aplikacije.

Popis poznatih certifikata – Omogućuje vam prilagodbu ponašanja programa ESET Internet Security 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.

Verifikacijski (root) certifikat

Dodaj root certifikat u poznate preglednike – Da bi SSL komunikacija ispravno radila u vašim preglednicima / klijentima e-pošte, važno je da dodate root certifikat za ESET na popis poznatih root certifikata (izdavača). Kada se aktivira, ESET Internet Security će automatski dodati certifikat ESET SSL Filter CA poznatim preglednicima (npr. Opera). Taj certifikat se automatski dodaje preglednicima koji upotrebljavaju spremište sistemskih certifikata. Primjerice, Firefox se automatski konfigurira tako da smatra root ovlaštenja u spremištu sistemskih certifikata pouzdanima.

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 ne može se provjeriti s pomoću pouzdanog izvora root certifikata (TRCA). To znači da je certifikat netko potpisao (npr. administrator web servera ili manje tvrtke) te postavljanje tog certifikata kao pouzdanog ne predstavlja uvijek rizik. Većina velikih tvrtki (npr. 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 potpisan ili oštećen. U tom slučaju ESET preporučuje da napustite **blok komunikaciju koja upotrebljava** odabrani certifikat. Ako je odabrana opcija **Pitaj o valjanosti certifikata** , od korisnika će se zatražiti da odabere radnju koja će se provesti prilikom uspostavljanja šifrirane komunikacije.

> **Ogledni primjeri**
>
> Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
> - Obavijesti o certifikatima u ESET-ovim Windows programima za kućnu upotrebu
> - „Šifrirani mrežni promet: certifikat nije vjerodostojan" prikazuje se prilikom posjećivanja web stranica

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 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.

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 opcija **Pitaj o valjanosti certifikata** (standardna postavka), od korisnika će se zatražiti da odabere radnju koja će se provesti 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 samopotpisan. U tom slučaju preporučujemo da blokirate komunikaciju koja koristi taj certifikat.

Šifrirani mrežni promet

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

Prvo, ako web stranica upotrebljava certifikat koji se ne može potvrditi ili neispravan certifikat, a ESET Internet Security 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 Internet Security mora **ignorirati** taj promet da bi aplikacija nastavila raditi.

> **Ogledni primjeri**
> Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
> - Obavijesti o certifikatima u ESET-ovim Windows programima za kućnu upotrebu
> - „Šifrirani mrežni promet: certifikat nije vjerodostojan" prikazuje se prilikom posjećivanja web stranica

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 Internet Security za određene SSL certifikate i pamćenje odabrane akcije ako je odabrana mogućnost **Interaktivni način rada** u odjeljku **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 spremljenim 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 – Dodajte novi certifikat i prilagodite njegove postavke za opcije pristupa i skeniranja.

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.

Popis filtriranih SSL/TLS aplikacija

Popis filtriranih SSL/TLS aplikacija se može upotrebljavati za podešavanje ponašanja programa ESET Internet Security za određene aplikacije i za pamćenje radnji koje su odabrane kada je **Način filtriranja SSL/TLS protokola** postavljen na **Interaktivni način**. 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 – Odaberite izvršnu datoteku iz stabla direktorija, kliknite opciju **...** ili unesite put ručno.

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 aplikaciju koju želite konfigurirati i kliknite **Uredi**.

Izbriši – Odaberite aplikaciju koju želite izbrisati i kliknite **Izbriši**.

Uvezi/izvezi – Uvezite aplikacije iz datoteke ili spremite trenutačni popis aplikacija u datoteku.

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

zaštita klijenta e-pošte

Pogledajte stavku Integracija programa ESET Internet Security s klijentom e-pošte da biste konfigurirali integraciju.

Postavke klijenta e-pošte nalaze se u odjeljku **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita klijenta e-pošte** > **Klijenti e-pošte**.

Klijenti e-pošte

Aktiviraj zaštitu e-pošte klijentskim dodacima – Kada je deaktivirana, isključena je zaštita klijentskim podacima za e-poštu.

E-pošta za skeniranje

Odaberite e-poruke za skeniranje:

- **Primljene poruke e-pošte**
- **Poslane poruke e-pošte**
- **Pročitane poruke e-pošte**
- **Izmijenjene e-poruke**

> Preporučujemo da aktivirate opciju **Aktiviraj zaštitu e-pošte klijentskim dodacima**. Čak i ako integracija nije aktivirana ili funkcionalna, značajka Filtriranje protokola (IMAP/IMAPS i POP3/POP3S) svejedno štiti komunikaciju e-poštom.

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.

Integracija s klijentima e-pošte

Integracija programa ESET Internet Security 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 Internet Security. Nakon integracije u klijent e-pošte alatna traka programa ESET Internet Security 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** > **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 funkcionira 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.

Deaktivirajte opcije **Optimizacija postupanja s privitcima** i **Napredna obrada klijenta e-pošte** ako dođe do usporavanja sustava prilikom dohvaćanja e-pošte.

Alatna traka za Microsoft Outlook

Zaštita programa Microsoft Outlook radi kao dodatni modul. Nakon instalacije programa ESET Internet Security ova alatna traka na kojoj se nalazi mogućnosti antivirusne/antispam zaštite dodaje se programu Microsoft Outlook:

Spam poruke – Označuje odabrane poruke kao spam poruke. Nakon označivanja središnjem serveru s pohranom potpisa spam poruka šalje se "otisak" poruke. Ako server primi slične "otiske" od nekoliko korisnika, poruka će ubuduće biti klasificirana kao spam.

Nisu spam poruke – Označuje da odabrane poruke nisu spam poruke.

Spam adresa (popis spam adresa) – Dodaje novu adresu pošiljatelja na popis spam adresa. Sve poruke primljene s neke od adresa na popisu automatski se klasificiraju kao spam.

Čuvajte se zavaravanja – Krivotvorenja pošiljateljeve adrese na poruku e-pošte kako bi se zavaralo primatelje e-pošte da pročitaju i odgovore.

Pouzdana adresa (popis pouzdanih stavki) – Dodaje novu adresu pošiljatelja na popis pouzdanih stavki. Poruke primljene s adresa na popisu pouzdanih adresa nikad se neće automatski klasificirati kao spam.

ESET Internet Security – dvokliknite ikonu da biste otvorili glavni prozor programa ESET Internet Security.

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.

Podešavanje antispama – Prikazuje opcije podešavanja antispam zaštite.

Adresari – Otvara prozor antispam zaštite u kojem možete pristupiti popisu izuzetih, pouzdanih i spam adresa.

Alatna traka za Outlook Express i Windows Mail

Zaštita programa Outlook Express i Windows Mail radi kao dodatni modul. Nakon instalacije programa ESET Internet Security ova alatna traka na kojoj se nalazi mogućnosti antivirusne/antispam zaštite dodaje se programu Outlook Express ili Windows Mail:

Spam poruke – Označuje odabrane poruke kao spam poruke. Nakon označivanja središnjem serveru s pohranom potpisa spam poruka šalje se "otisak" poruke. Ako server primi slične "otiske" od nekoliko korisnika, poruka će ubuduće biti klasificirana kao spam.

Nisu spam poruke – Označuje da odabrane poruke nisu spam poruke.

Spam adresa – Dodaje novu adresu pošiljatelja na popis spam adresa. Sve poruke primljene s neke od adresa na popisu automatski se klasificiraju kao spam.

Čuvajte se zavaravanja – Krivotvorenja pošiljateljeve adrese na poruku e-pošte kako bi se zavaralo primatelje e-pošte da pročitaju i odgovore.

Pouzdana adresa – Dodaje novu adresu pošiljatelja na popis pouzdanih stavki. Poruke primljene s adresa na popisu pouzdanih adresa nikad se neće automatski klasificirati kao spam.

ESET Internet Security – dvokliknite ikonu da biste otvorili glavni prozor programa ESET Internet Security.

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.

Podešavanje antispama – Prikazuje opcije podešavanja antispam zaštite.

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 pomiču se s dna na desnu stranu ikona.

Velike ikone – Prikazuje velike ikone za mogućnosti izbornika.

Dijaloški okvir s potvrdom

Ta obavijest služi kao potvrda da korisnik zaista želi izvršiti odabranu radnju te se eliminiraju moguće pogreške.

S druge strane, dijaloški okvir nudi i mogućnost deaktiviranja potvrda.

Ponovno skeniranje poruka

Antivirusna alatna traka sustava ESET Internet Security 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.

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 odgovoreno ili je izbrisana.

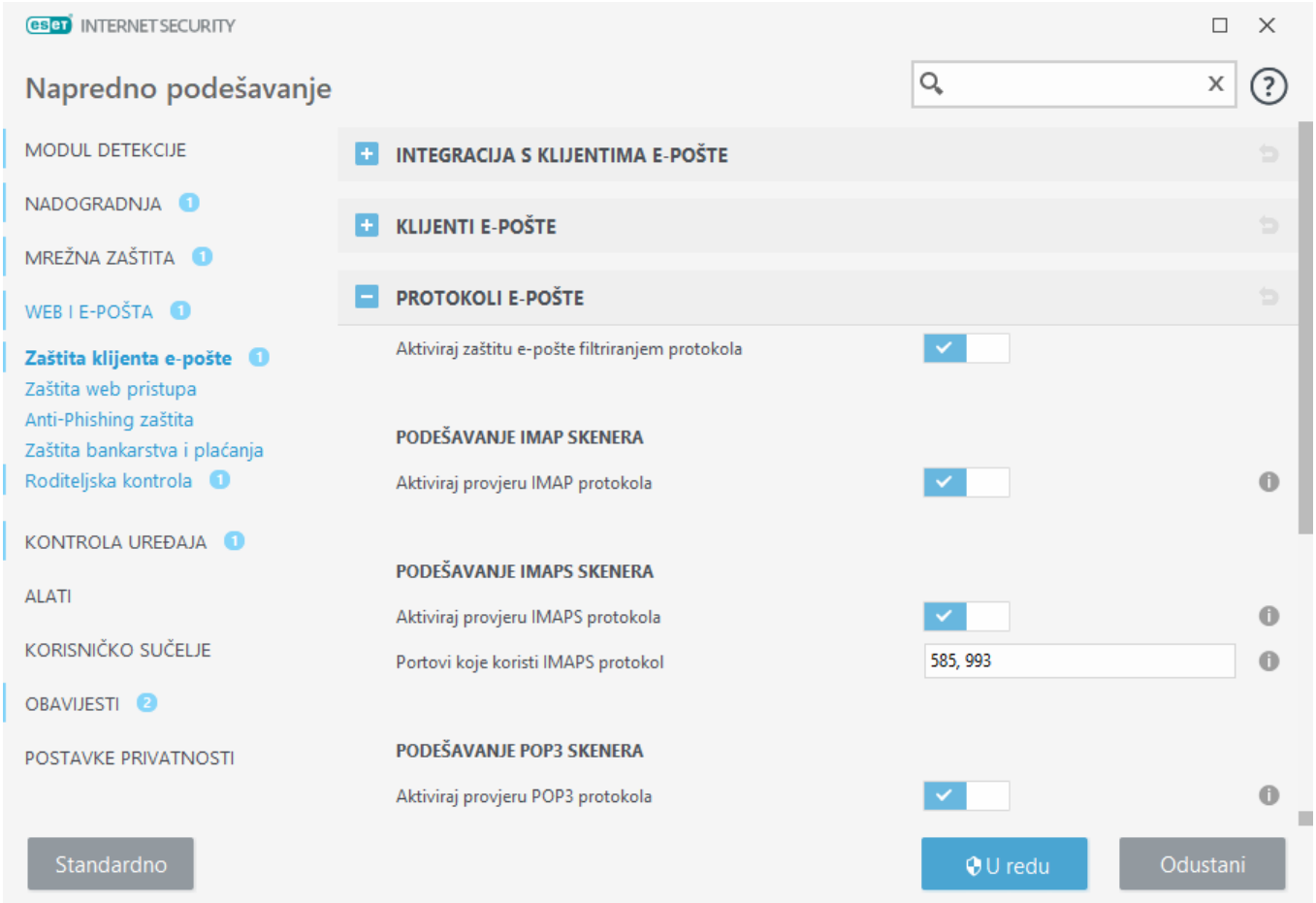
Modul zaštite koji omogućuje tu kontrolu automatski se pokreće prilikom pokretanja sustava i ostaje aktivan u memoriji.

ESET Internet Security 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 IMAP 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 konfigurirali provjeru protokola IMAP/IMAPS i POP3/POP3S, idite na **Napredno podešavanje** > **Web i e-pošta** > **Zaštita klijenta e-pošte** > **Protokoli e-pošte**.

ESET Internet Security podržava i skeniranje protokola IMAPS (585, 993) i POP3S (995) koji koriste šifrirani kanal za prijenos informacija između servera i klijenata. ESET Internet Security provjerava komunikaciju koja koristi protokole SSL (Secure Socket Layer) i TLS (Transport Layer Security). Program skenira samo promet e-pošte na portovima definiranima 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 skenirat će se prema standardnim postavkama. Za prikaz podešavanja skenera otvorite Napredno podešavanje > **Web i e-pošta** > **SSL/TLS**.



POP3/POP3S filtar

Protokol POP3 najraširenij je protokol koji se koristi za primanje komunikacije e-poštom u aplikaciji klijenta e-pošte. ESET Internet Security pruža zaštitu tog protokola bez obzira na to koji klijent e-pošte koristite.

Modul zaštite koji omogućuje tu kontrolu automatski se pokreće prilikom pokretanja sustava i ostaje aktivan u memoriji. Provjerite je li modul aktiviran da bi ispravno funkcionirao – protokol POP3 provjerava se automatski, bez potrebe za ponovnom konfiguracijom klijenta e-pošte. Prema standardnim postavkama skenira se sva komunikacija na portu 110, ali se prema potrebi mogu dodati i drugi komunikacijski portovi. Višestruke brojeve portova potrebno je razgraničiti zarezima.

Šifrirana komunikacija skenirat će se prema standardnim postavkama. Za prikaz podešavanja skenera otvorite Napredno podešavanje > **Web i e-pošta** > **SSL/TLS**.

U tom odjeljku možete konfigurirati provjeru protokola POP3 i POP3S.

Aktiviraj provjeru POP3 protokola – Ako je ta opcija aktivirana, sav promet kroz POP3 protokol nadzire se radi prepoznavanja zlonamjernog softvera.

Portovi koje upotrebljava protokol POP3 – Popis portova koje upotrebljava protokol POP3 (110 prema standardnim postavkama).

ESET Internet Security podržava i provjeru POP3S protokola. Ta vrsta komunikacije koristi šifrirani kanal za prijenos informacija između servera i klijenta. ESET Internet Security provjerava komunikaciju pomoću metoda šifriranja SSL (Secure Socket Layer) i TLS (Transport Layer Security).

Nemoj upotrebljavati POP3S provjeru – Šifrirana se komunikacija neće provjeravati.

Koristi provjeru POP3S protokola za odabrane portove – Označite ovu opciju da biste aktivirali provjeru protokola POP3S samo za portove zadane u odjeljku **Portovi koje koristi POP3S protokol**.

Portovi koje koristi POP3S protokol – Popis POP3S portova za provjeru (995 prema standardnim postavkama).

Oznake e-pošte

Mogućnosti za tu funkciju dostupne su pod stavkom **Napredno podešavanje** > **Web i e-pošta** > **Zaštita klijenta e-pošte Upozorenja i obavijesti**.

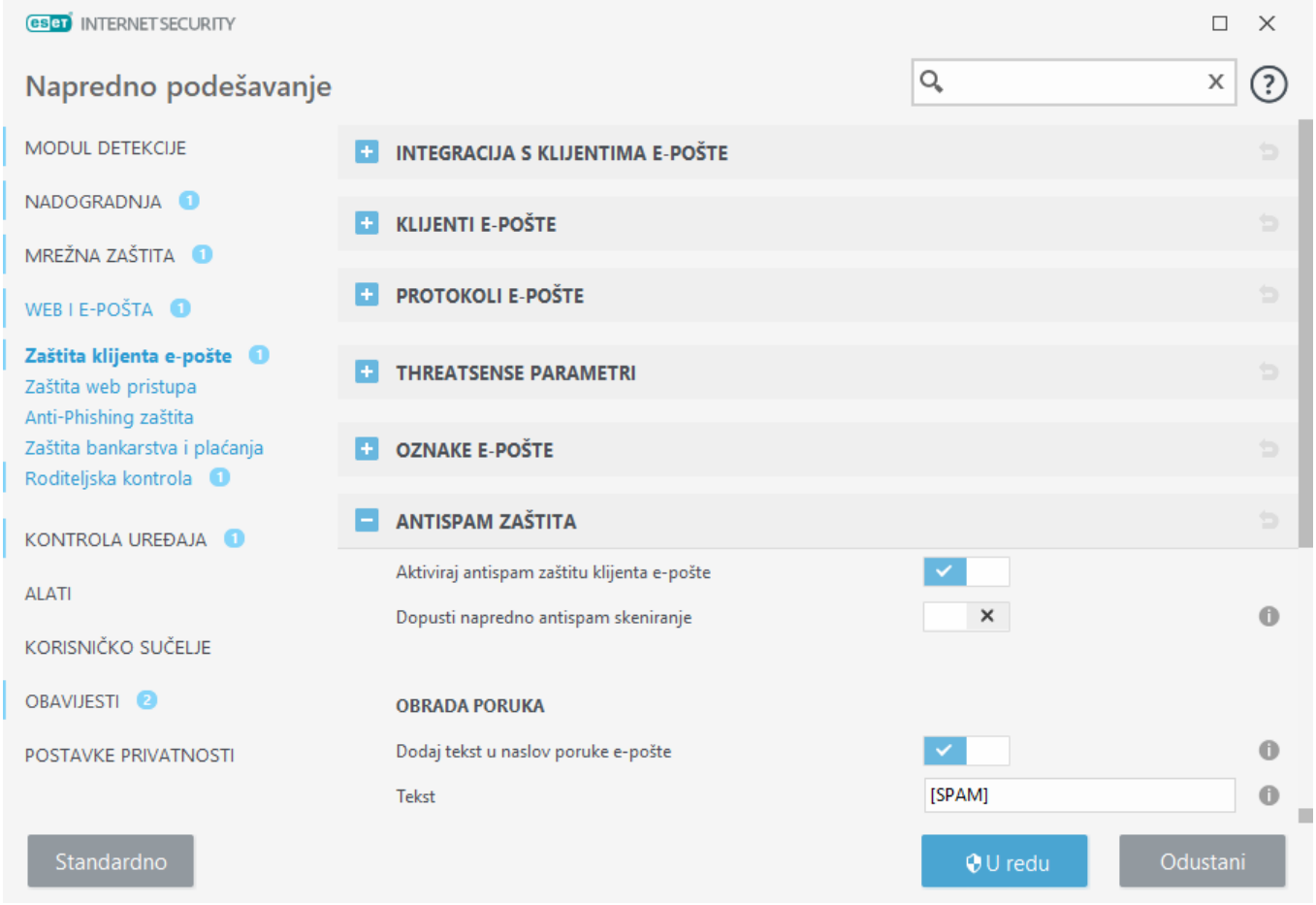
Nakon provjere, poruci e-pošte može se dodati obavijest s rezultatima skeniranja. Možete odabrati opciju **Dodaj oznake primljenim i pročitanim porukama e-pošte** ili **Dodaj oznake poslanim porukama e-pošte**. Imajte na umu da se u rijetkim slučajevima oznake mogu izostaviti u problematičnim HTML porukama 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 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.

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 zamijenit će predmet poruke "Hello" u sljedeći format: "[prijetnja %DETECTIONNAME%] Hello". Varijabla %DETECTIONNAME% predstavlja otkrivenu prijetnju.

Antispam zaštita

Neželjena e-pošta ili spam jedan je od najvećih problema elektroničke komunikacije. Spam čini do 30% ukupne komunikacije e-poštom. Antispam zaštita sprječava taj problem. Kombiniranjem nekoliko učinkovitih sigurnosnih načela antispam modul omogućuje vrhunsko filtriranje i održava vašu mapu ulazne pošte čistom. Kako biste konfigurirali antispam zaštitu, otvorite **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita klijenta e-pošte** > **Antispam zaštita**.



Za detekciju spama jedno od važnih načela je prepoznavanje neželjenih e-poruka na temelju unaprijed definiranih pouzdanih adresa (dopuštenih) i spam adresa (blokiranih).

Primarna metoda detekcije spam poruka je skeniranje svojstava poruke e-pošte. Primljene se poruke skeniraju prema osnovnim kriterijima za antispam (definicijama poruka, statističkom heuristikom, prepoznavanjem algoritama i drugim jedinstvenim metodama), a dobivena indeksna vrijednost određuje radi li se o spam porukama.

Aktiviraj antispam zaštitu klijenta e-pošte – Kada je aktivirana, antispam zaštita automatski će se aktivirati pri pokretanju sustava.

Dopusti napredno antispam skeniranje – Povremeno će se preuzimati dodatni antispam podaci, čime se poboljšavaju mogućnosti antispama i ostvaruju bolji rezultati.

Antispam zaštita u programu ESET Internet Security omogućuje vam postavljanje različitih parametara za poruke.

Obrada poruka

Dodaj tekst u naslov poruke e-pošte – Omogućuje dodavanje niza prilagođenog prefiksa u redak naslova poruke koje su klasificirane kao spam. Standardna je postavka "[SPAM]".

Premjesti poruke u mapu sa spam porukama – Kada je ta mogućnost aktivirana, spam poruke premještaju se u standardnu mapu za bezvrijednu poštu, a poruke koje su ponovno klasificirane kao poruke koje nisu spam premještaju se u ulaznu poštu. Ako desnom tipkom miša kliknete poruku e-pošte i odaberete ESET Internet Security u kontekstnom izborniku, bit će vam dostupne sljedeće mogućnosti za odabir.

Upotrijebi mapu – navedite prilagođenu mapu u koju želite premjestiti zaražene e-poruke nakon što se otkriju.

Označi spam poruke kao pročitane – Aktivirajte ovu opciju da biste spam poruku automatski označili kao pročitanu. To vam pomaže da obratite pozornost na "čiste" poruke.

Označi ponovno klasificirane poruke kao nepročitane – Time će se poruke, izvorno klasificirane kao spam, ali kasnije označene kao „čiste”, prikazati kao nepročitane.

Zapisivanje u dnevnik rezultata spam poruka – Antispam modul programa ESET Internet Security svakoj skeniranoj poruci dodjeljuje spam rezultat. Poruka će se zabilježiti u antispam dnevnik (glavni programski prozor > **Alati** > **Više alata** > **Dnevnici** > **Antispam zaštita**).

- **Ništa** – Rezultat antispam skeniranja neće se zapisati u dnevnik.
- **Ponovno klasificirano i označeno kao spam** – Odaberite ovu opciju ako želite zabilježiti spam rezultat za poruke označene kao SPAM.
- **Sve** – U dnevnik će se zapisati sve poruke sa spam rezultatom.

Klikom na poruku u mapi s bezvrijednom poštom i odabirom mogućnosti **Ponovno klasificiraj odabrane poruke kao NE spam** poruku možete premjestiti u ulaznu poštu. Klikom na poruku koju smatrate spam porukom u ulaznoj pošti i odabirom mogućnosti **Ponovno klasificiraj odabrane poruke kao spam** poruku možete premjestiti u mapu s bezvrijednom poštom. Možete odabrati više poruka i provesti radnju za sve njih istovremeno.

ESET Internet Security podržava antispam zaštitu za programe Microsoft Outlook, Outlook Express, Windows Mail i Windows Live Mail.

Rezultat obrade adresa

Prilikom dodavanja novih adresa ili promjene radnje poduzete za adresu e-pošte program ESET Internet Security prikazuje poruke obavijesti. Sadržaj poruka obavijesti ovisi o akciji koju pokušavate izvršiti.

Potvrdite okvir **Više ne pitaj** da bi se akcija sljedeći put izvršila automatski bez prikazivanja poruke.

Antispam adresari

Antispam značajka u programu ESET Internet Security omogućuje vam konfiguraciju različitih parametara za popise adresa.

Aktiviraj korisnički adresar – aktivirajte ovu opciju kako biste aktivirali korisnički adresar.

Korisnički adresar – popis adresa e-pošte na koje možete dodavati, uređivati ili uklanjati adrese da biste definirali pravila protiv spama. Pravila na ovom popisu primijenit će se na trenutačnog korisnika.

Aktiviraj globalni adresar – aktivirajte ovu opciju da biste aktivirali globalni adresar koji zajednički upotrebljavaju svi korisnici na ovom uređaju.

Globalni adresar – popis adresa e-pošte na koje možete dodavati, uređivati ili uklanjati adrese da biste definirali pravila protiv spama. Pravila na ovom popisu će se primijeniti na sve korisnike.

Automatski dopusti i dodaj u korisnički adresar

Postupaj s adresama iz adresara kao s pouzdanim adresama – S adresama s popisa kontakata postupat će se kao s pouzdanim adresama bez dodavanja u korisnički adresar.

Dodaj adrese primatelja iz odlaznih poruka – služi za dodavanje adresa primatelja iz poslanih poruka u korisnički adresar kao dopuštene.

Dodaj adrese iz poruka ponovno klasificiranih kao NIJE spam – služi za dodavanje adresa pošiljatelja poruka koje su klasificirane kao NIJE spam u korisnički adresar kao dopuštene.

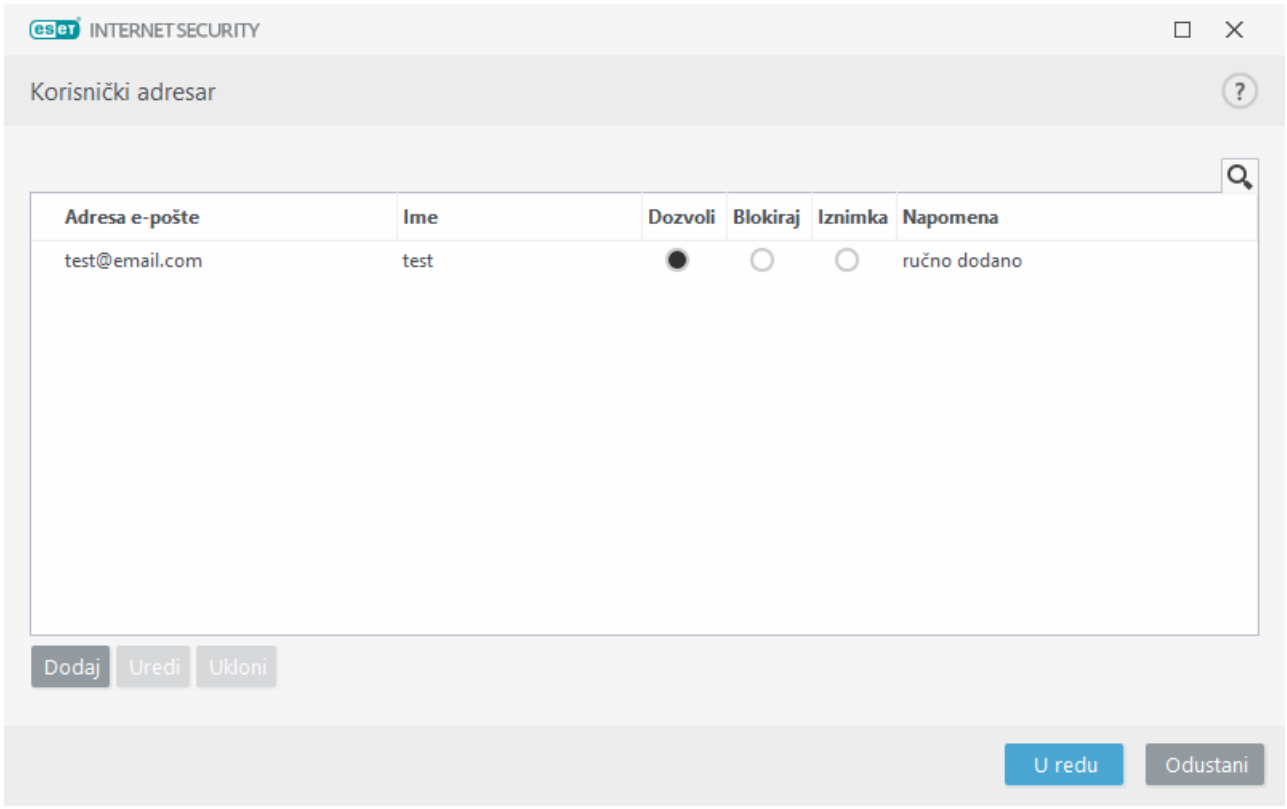
Automatski dodaj u korisnički adresar kao iznimku

Dodaj adrese s vlastitih računa – dodajte adrese iz postojećih računa klijenta e-pošte u korisnički adresar kao iznimke.

Adresari

Da biste se zaštitili od neželjenih e-poruka, program ESET Internet Security vam omogućuje da klasificirate adrese e-pošte u adresare.

Da biste uredili adresare, otvorite **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita klijenta e-pošte** > **Antispam adresari** i kliknite **Uredi** pored stavke **Korisnički adresar** ili **Globalni adresar**.



Stupci

Adresa e-pošte – adresa na koju će se pravilo primjenjivati.

Naziv – prilagođeni naziv pravila.

Dopusti/blokiraj/iznimka – izborni gumbi koji se upotrebljavaju za određivanje radnje koju treba poduzeti za adresu e-pošte (kliknite izborni gumb u željenom stupcu da biste brzo promijenili radnju):

- **Dopusti** – adrese koje se smatraju sigurnima i od kojih želite primati poruke.
- **Blokiraj** – adrese koje se smatraju nesigurnima/spamom i od kojih ne želite primati poruke.
- **Iznimka** – adrese koje se uvijek provjeravaju radi spama i koje se mogu lažirati i upotrebljavati za slanje spama.

Napomena – informacije o tome kako je pravilo stvoreno i odnosi li se na cijelu domenu / domene niže razine.

Upravljanje adresama

- **Dodaj** – kliknite da biste dodali pravilo za novu adresu.
- **Uredi** – odaberite i kliknite da biste uredili postojeće pravilo.
- **Ukloni** – odaberite i kliknite ako želite ukloniti pravilo iz adresara.

Dodavanje/uređivanje adrese

Ovaj prozor omogućuje dodavanje ili uređivanje adrese na popisu antispam adresa i konfiguriranje poduzete radnje:

Adresa e-pošte – adresa na koju će se pravilo primjenjivati.

Naziv – prilagođeni naziv pravila.

Radnja – radnja koju treba poduzeti ako adresa e-pošte kontakta odgovara adresi navedenoj u polju **Adresa e-pošte**:

- **Dopusti** – adrese koje se smatraju sigurnima i od kojih želite primati poruke.
- **Blokiraj** – adrese koje se smatraju nesigurnima/spamom i od kojih ne želite primati poruke.
- **Iznimka** – adrese koje se uvijek provjeravaju radi spama i koje se mogu lažirati i upotrebljavati za slanje spama.

Cijela domena – odaberite ovu opciju ako želite da se pravilo primijeni na cijelu domenu kontakta (ne samo na adresu navedenu u polju **Adresa e-pošte** nego na sve adrese e-pošte u domeni *address.info*).

Domene niže razine – odaberite ovu opciju ako želite da se pravilo primijeni na domene niže razine kontakta (*address.info* predstavlja domenu, dok *my.address.info* predstavlja poddomenu).

zaštita web pristupa

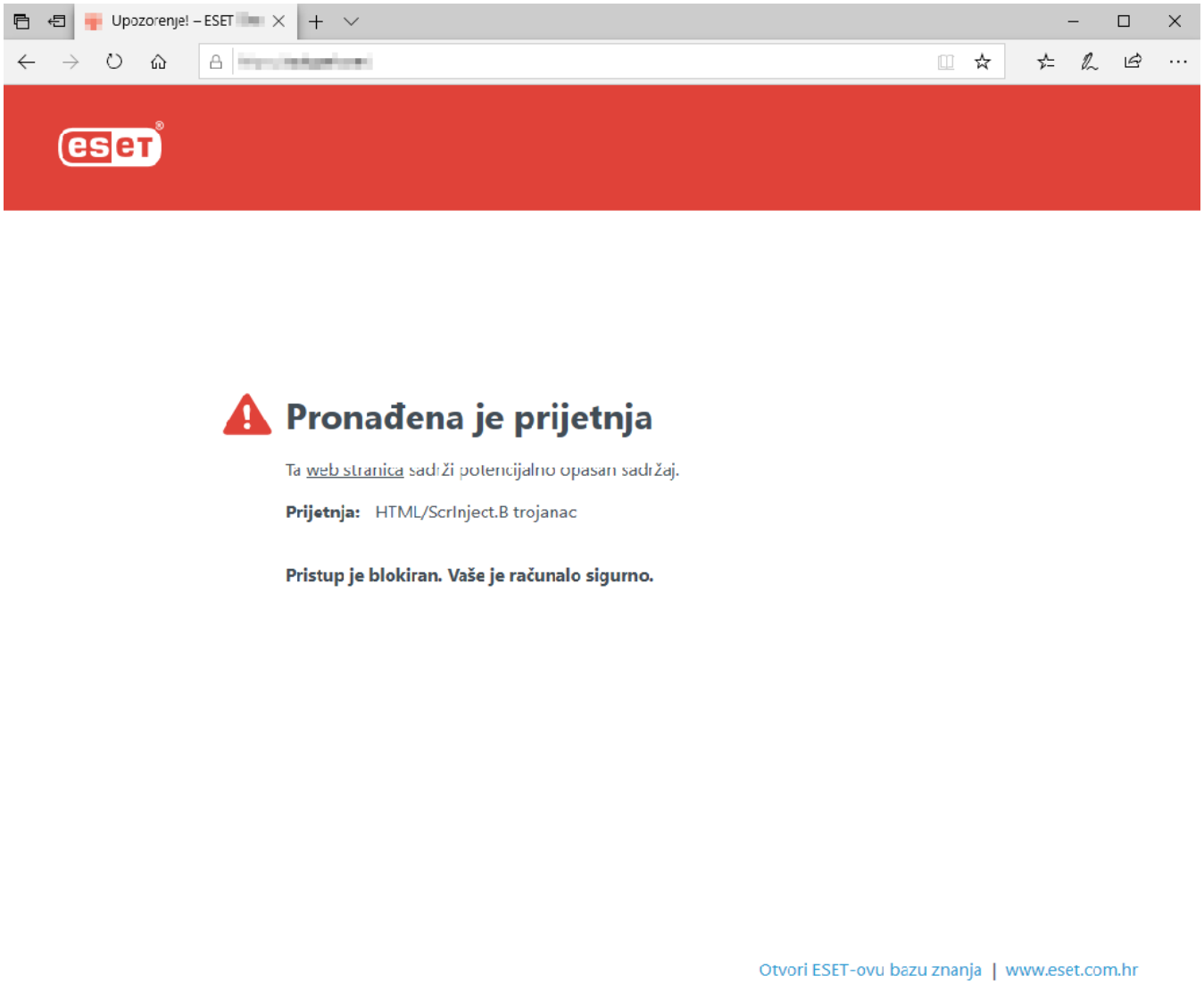
Povezivost s internetom standardna je značajka osobnih računala. Nažalost, postala je i glavni medij za prijenos zlonamjernog koda. Zaštita web pristupa vrši se nadgledanjem komunikacije između internetskih preglednika i udaljenih servera te je u skladu s pravilima o HTTP-u (Hypertext Transfer Protocol, 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 aktivirate opciju Zaštita web pristupa. Toj se opciji može pristupiti u glavnom prozoru programa > **Podešavanje** > **Internetska zaštita** > **Zaštita web pristupa**.



Zaštita web pristupa prikazat će sljedeću poruku u vašem pregledniku kad je web stranica blokirana:



Ilustrirane upute

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

- Izuzimanje sigurne web stranice od blokiranja funkcijom Zaštita web pristupa
- Blokiranje web stranice s pomoću programa ESET Internet Security

---

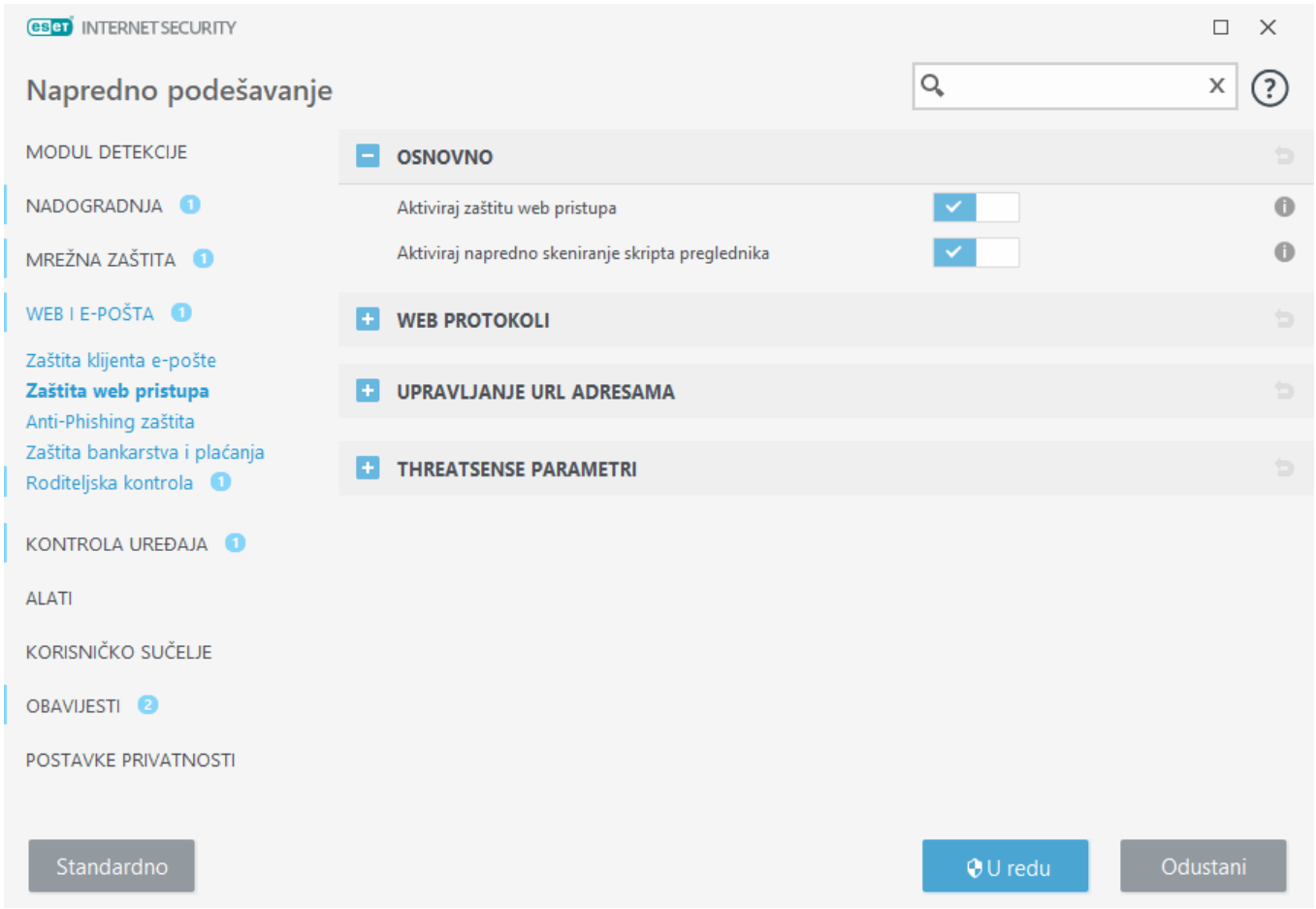
Sljedeće su mogućnosti dostupne pod **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita web pristupa**:

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 parameteri – 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 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. Ta opcija dostupna je samo kada je aktivirano filtriranje protokola SSL/TLS.

Aktiviraj napredno skeniranje skripta preglednika – Nakon aktivacije modul detekcije pregledat će sve programe JavaScript koje pokrenu internetski preglednici.

Preporučujemo da obavezno ostavite aktiviranu mogućnost Zaštita web pristupa.

Web protokoli

ESET Internet Security 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 Internet Security podržava provjeru HTTPS protokola. HTTPS komunikacija koristi šifrirani kanal za prijenos informacija između servera i klijenta. ESET Internet Security 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 skenirat će se prema standardnim postavkama. Za prikaz podešavanja skenera otvorite Napredno podešavanje > **Web i e-pošta** > **SSL/TLS**.

Upravljanje URL adresama

U odjeljku za upravljanje URL adresama omogućeno je navođenje HTTP adresa koje želite blokirati, omogućiti ili izuzeti od skeniranja.

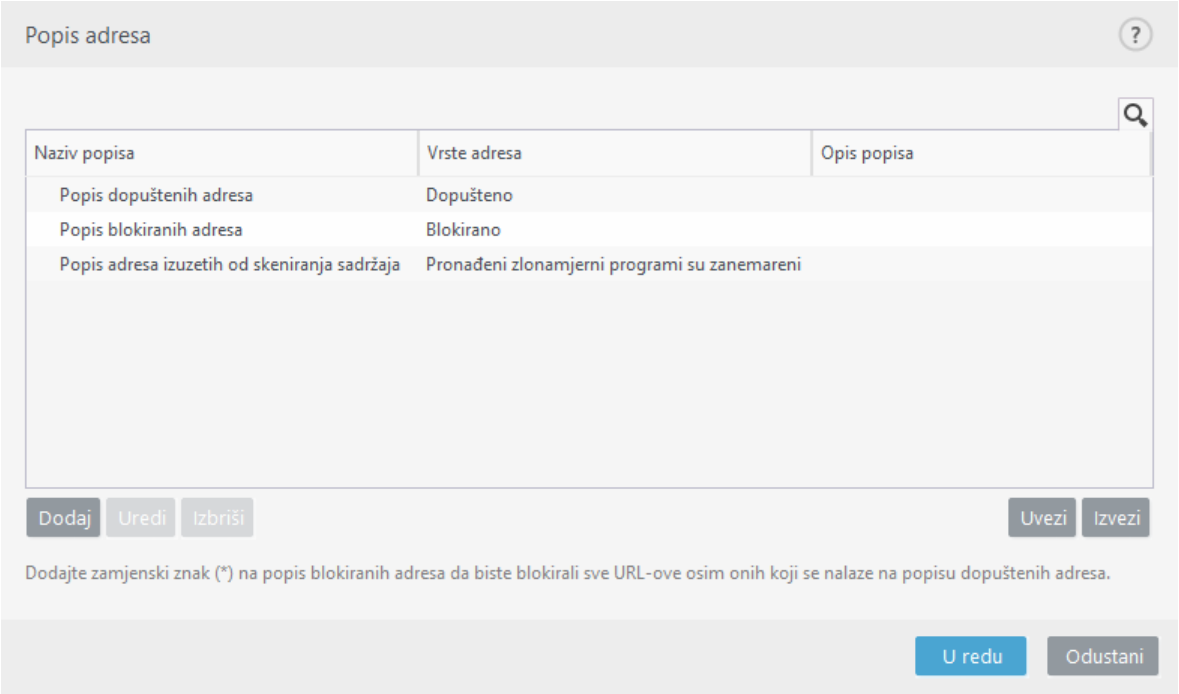
Opcija Aktiviraj filtriranje SSL/TLS protokola mora biti označena ako želite filtrirati HTTPS adrese uz HTTP web stranice. U suprotnom će se dodati samo domene posjećenih HTTPS stranica, ali ne i puna URL adresa.

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**.

> **Pouzdane domene**
> 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.



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.

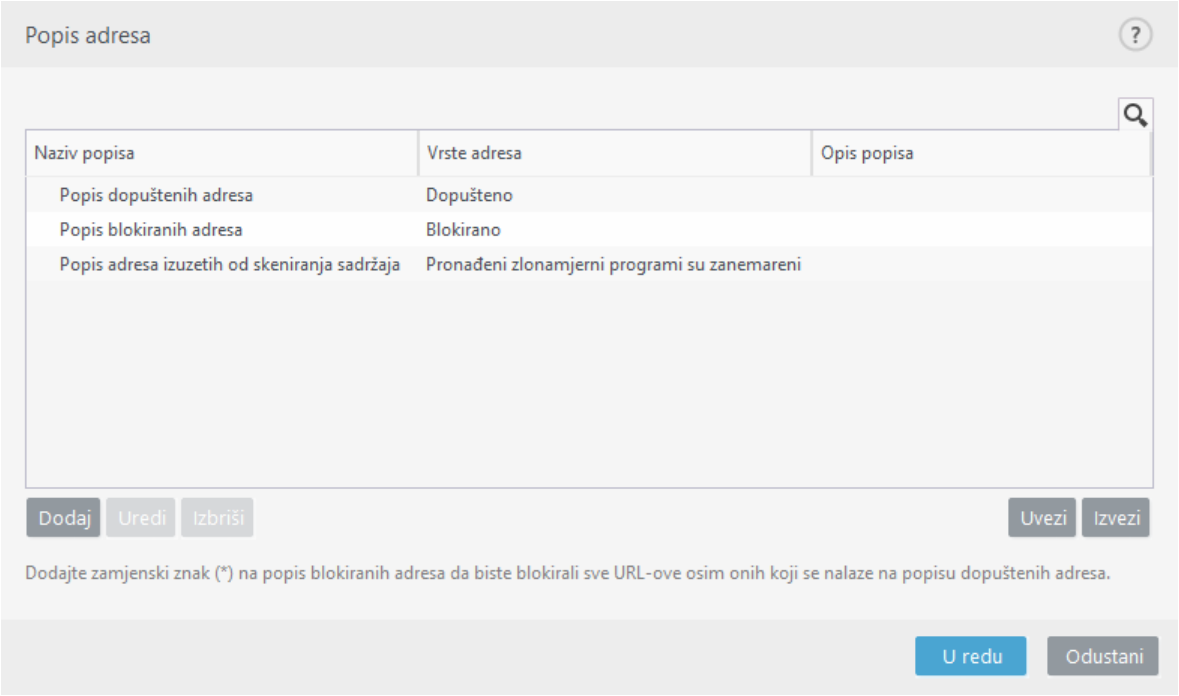
Popis URL adresa

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.



Ilustrirane upute

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

- Izuzimanje sigurne web stranice od blokiranja funkcijom Zaštita web pristupa
- Blokiranje web stranice ESET-ovim Windows programima za kućne korisnike

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 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.
- **Popis dopuštenih adresa** – Ako je aktivirana opcija 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 podudaraju s popisom blokiranih adresa.

Naziv popisa – Navedite naziv popisa. Prilikom uređivanja jednog od triju unaprijed definiranih popisa to je polje zasivljeno.

Opis popisa – Unesite kratak opis popisa (nije obavezno). Prilikom uređivanja jednog od triju unaprijed definiranih popisa to je polje zasivljeno.

Da bite aktivirali popis, odaberite **Aktivan popis** pored njega. Ako želite primiti obavijesti prilikom korištenja tog popisa za procjenu HTTP stranice koju posjećujete, odaberite **Obavijesti prilikom primjene**. Obavijest se, primjerice, šalje ako je web stranica blokirana ili dopuštena jer se nalazi na popisu blokiranih ili dopuštenih adresa. Obavijest sadrži naziv popisa na kojem se nalazi dotična web stranica.

Kontrolni elementi

Dodaj – Služi za dodavanje URL adrese na popis (moguć je unos više vrijednosti sa separatorom).

Uredi – Uređuje postojeće adrese na popisu. Ta je opcija dostupna samo za adrese stvorene putem opcije **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 Internet Security 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 nepoznati 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 zaobilaženje 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 usklađivanje čitave domene zajedno sa svim poddomenama pomoću 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

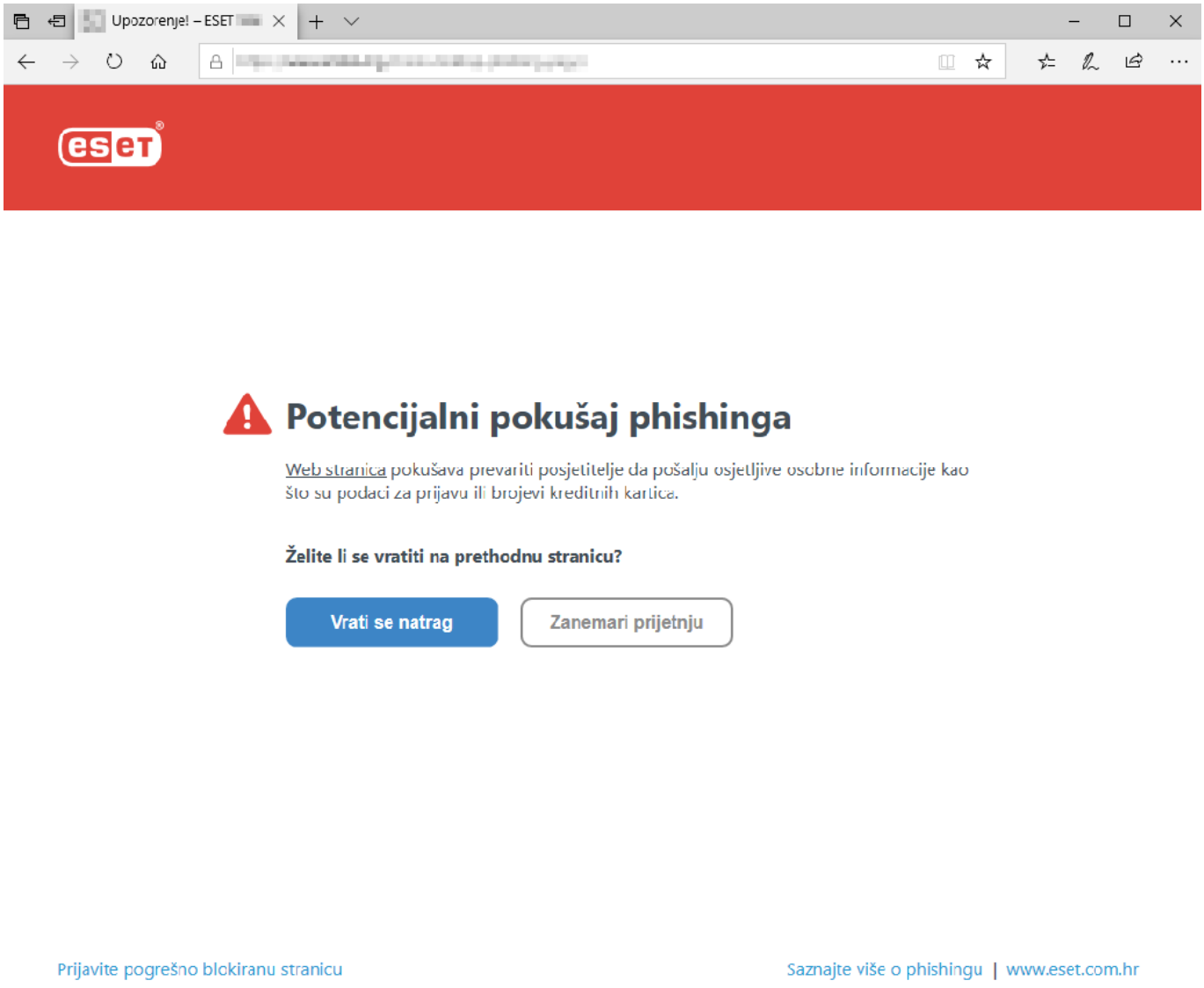
Pojam phishing odnosi se na protuzakonitu aktivnost koja se koristi tehnikom društvenog inženjeringa (manipuliranje korisnicima radi stjecanja povjerljivih informacija). Phishing upotrebljavaju za pristup osjetljivim podacima, kao što su brojevi bankovnih računa, PIN-ovi i drugo. Više o toj aktivnosti pročitajte u rječniku. ESET Internet Security 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 Internet Security. 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 Internet Security.

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 toj web stranici, kliknite **Zanemari prijetnju** (ne preporučuje se).



Potencijalne web stranice za phishing koje su stavljene na popis pouzdanih adresa prema standardnim postavkama nestat će nakon nekoliko sati. Da biste trajno dopustili web stranicu, upotrijebite alat Upravljanje URL adresama. U odjeljku **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita web pristupa** > **Upravljanje URL adresama** > **Popis adresa** > **Uredi** dodajte web stranicu koju želite urediti na popis.

Prijava stranice za phishing

Veza **Prijavi** omogućuje vam da prijavite phishing/zlonamjernu web stranicu tvrtki ESET radi analize.

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 pogrešno blokiranu stranicu.

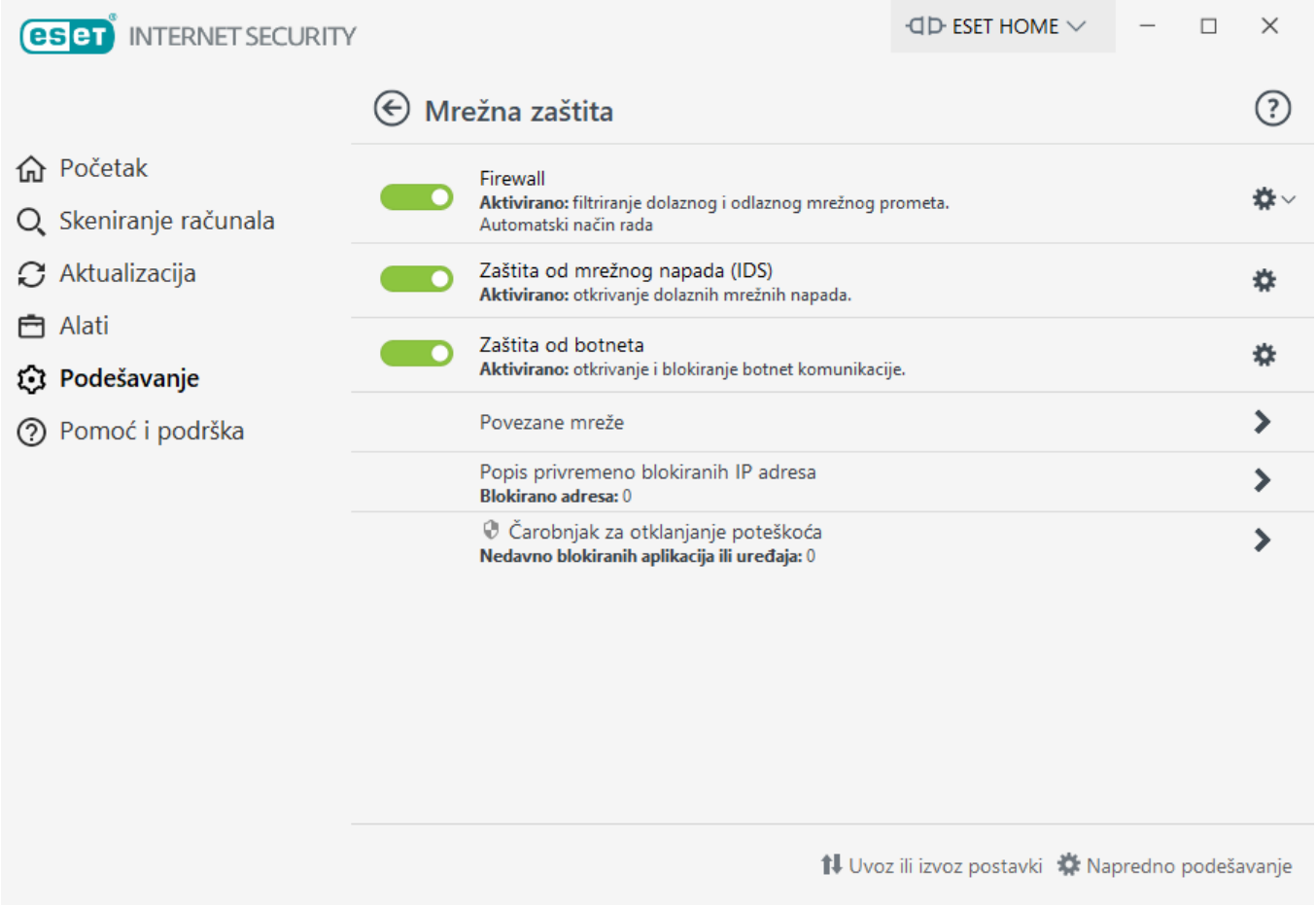
Web stranicu možete poslati i e-poštom. Pošaljite poruku e-pošte na adresu samples@eset.com. Napominjemo da predmet poruke mora sadržavati opis, a sama poruka što više informacija o web stranici (primjerice, informacije o web stranici preko koje ste došli do nje, kako ste čuli za tu web stranicu itd.).

Mrežna zaštita

Konfiguracija mrežne zaštite može se pronaći u oknu **Podešavanje** pod stavkom **Mrežna zaštita**.

Da biste pauzirali ili deaktivirali pojedinačne module za zaštitu, kliknite ikonu trake klizača .

Isključivanjem modula za zaštitu može se smanjiti razina zaštite vašeg računala.



Firewall – ovdje možete podesiti način filtriranja za ESET firewall. Za pristup detaljnijim postavkama kliknite zupčanik > **Konfiguriranje** pored opcije **Firewall** ili pritisnite **F5** da biste pristupili izborniku Napredno podešavanje.

Konfiguriranje – Otvara prozor firewalla u Naprednom podešavanju u kojem možete definirati kako će firewall upravljati mrežnom komunikacijom.

Pauziraj firewall (dopusti sav promet) – ova je opcija suprotna onoj blokiranja svega mrežnog prometa. Ako

se odabere, sve se opcije filtriranja firewalla isključuju te se dopuštaju sve ulazne i izlazne veze. Kliknite **Aktiviraj firewall** da biste ponovno aktivirali firewall dok je filtriranje mrežnog prometa u ovom načinu.

Blokiraj sav promet – Firewall će blokirati svu ulaznu i izlaznu komunikaciju. Tu mogućnost koristite samo ako sumnjate na kritične sigurnosne rizike zbog kojih je potrebno prekinuti vezu sustava i mreže. Dok je Filtriranje mrežnog prometa u načinu rada **Blokiraj sav promet**, kliknite **Prestani blokirati sav promet** da biste firewall vratili u normalan način rada.

Automatski način rada – (kada je aktiviran drugi način filtriranja) – Kliknite za promjenu načina filtriranja na automatski način filtriranja (s pravilima koje definira korisnik).

Interaktivni način rada – (kada je aktiviran drugi način filtriranja) – Kliknite za promjenu načina filtriranja na interaktivan način filtriranja.

Zaštita od mrežnog napada (IDS) – Analizira sadržaj mrežnog prometa i štiti od mrežnih napada. Blokira se sav promet koji se smatra štetnim. ESET Internet Security obavijestit će vas kada se povežete s nezaštićenom bežičnom mrežom ili s mrežom sa slabom zaštitom.

Zaštita od botneta – Brzo i precizno uočava zlonamjerni softver u sustavu.

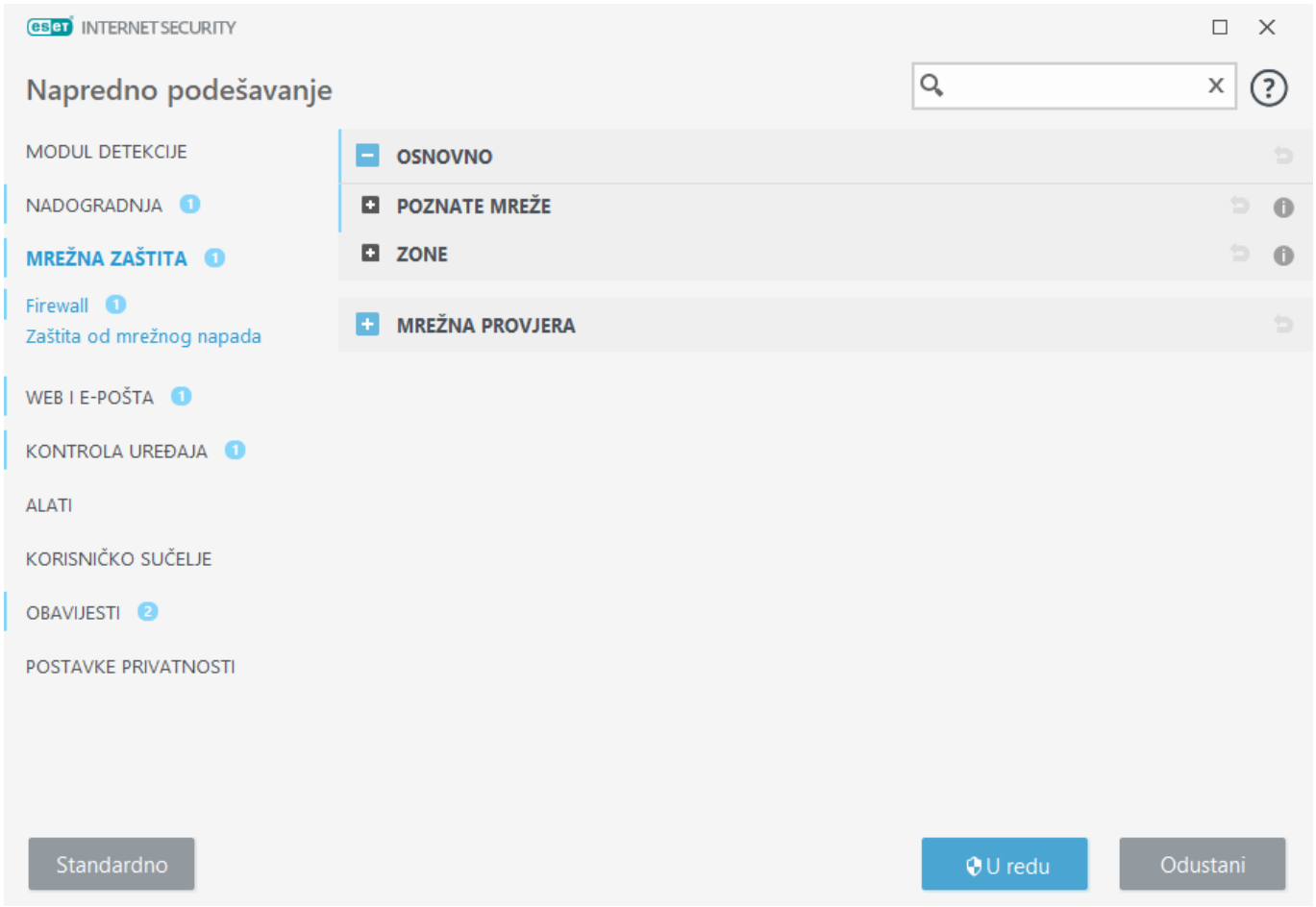
Povezane mreže – Prikazuje mreže na koje su povezani mrežni prilagodnici. Nakon što kliknete vezu ispod naziva mreže, skočni prozor će vam omogućiti konfiguriranje mreže kao pouzdane.

Popis privremeno blokiranih IP adresa – Prikazuje popis IP adresa koje su prepoznate kao izvori napada te su dodane na popis blokiranih adresa radi sprečavanja povezivanja na određeno razdoblje. Za više informacija kliknite ovu mogućnost, a zatim 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.

Napredno podešavanje Mrežne zaštite

U glavnom prozoru programa kliknite **Podešavanje** > **Napredno podešavanje** (F5) > **Mrežna zaštita**.



Osnovno

Poznate mreže

Više informacija potražite u odjeljku Poznate mreže.

Zone

Zona predstavlja skup mrežnih adresa koje čine jednu logičku grupu. Za više informacija pogledajte Konfiguriranje zona.

Mrežna provjera

Aktiviraj mrežnu provjeru

Mrežna provjera pomaže u prepoznavanju ranjivosti u kućnoj mreži, kao što su otvoreni portovi ili slaba lozinka routera. Također pruža popis povezanih uređaja kategoriziranih prema vrsti uređaja.

Obavijesti o novootkrivenim mrežnim uređajima

Obavještava vas kad se otkrije novi uređaj na mreži.

Poznate mreže

Prilikom upotrebe računala koje se često povezuje na nepouzdane mreže ili mreže izvan vaše uobičajene pouzdane (kućne ili uredske) mreže preporučuje se provjera vjerodostojnosti novih mreža s kojima se povezujete. Kada su mreže definirane, ESET Internet Security može prepoznati pouzdane (kućne ili uredske) mreže s pomoću mrežnih parametara konfiguriranih u odjeljku **Identifikacija mreže**. Računala često pristupaju mrežama s IP adresama koje su slične onima pouzdanih mreža. U takvim slučajevima ESET Internet Security može nepoznatu mrežu smatrati pouzdanom (kućnom ili uredskom mrežom). Preporučuje se korištenje **autorizacije mreže** kako bi se izbjegla takva situacija. Kako biste pristupili postavkama poznatih mreža, idite na **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Osnovno** > **Poznate mreže**.

Kada je mrežni adapter povezan s mrežom ili su ponovno konfigurirane njegove mrežne postavke, ESET Internet Security će na popisu poznatih mreža pretražiti zapis koji odgovara novoj mreži. Ako se **Identifikacija mreže** i **Autorizacija mreže** (dodatno) podudaraju, mreža će se označiti kao povezana u ovom sučelju. Kad se ne otkrije nijedna poznata mreža, konfiguracijom mrežne identifikacije stvorit će se nova mrežna veza kako bi se mreža identificirala sljedeći put kad se povežete s njom. Prema standardnim postavkama nova mrežna veza koristi se vrstom zaštite koja je definirana u postavkama Windowsa. Putem dijaloškog prozora **Otkrivena je nova mrežna veza** od vas će se zatražiti da odaberete vrstu zaštite, odnosno opciju **pouzdana mreža**, **nepouzdana mreža** ili **Upotrijebi postavku sustava Windows**. Ako je mrežni adapter povezan s poznatom mrežom, a ta je mreža označena kao **pouzdana mreža**, lokalne podmreže adaptera bit će dodane u pouzdanu zonu.

Vrsta zaštite novih mreža – Odaberite koja se od sljedećih opcija: **Upotrijebi postavke za Windows**, **Pitaj korisnika** ili **Označi kao nepouzdano** se upotrebljava kao standardna postavka za nove mreže.

Odjeljak Poznate mreže omogućuje vam da konfigurirate naziv mreže, identifikaciju mreže, vrstu zaštite itd. Za pristup podešavanju poznatih mreža kliknite **Uredi**.

> Kada odaberete **Upotrijebi postavku sustava Windows**, neće se pojaviti dijaloški prozor, a mreža s kojom ste povezani automatski će se označiti prema postavkama sustava Windows. To će omogućiti pristup određenim funkcijama (npr. dijeljenje datoteka i udaljeni pristup radnoj površini) s novih mreža.

Uređivač poznatih mreža

Poznate mreže mogu se ručno konfigurirati u **Naprednom podešavanju** > **Mrežna zaštita** > **Napredno** > **Poznate mreže** tako da kliknete **Uredi**.

Stupci

Naziv – naziv poznate mreže.

Vrsta zaštite – prikazuje je li mreža postavljena kao **pouzdana**, **nepouzdana** ili **Upotrijebi postavke sustava Windows**.

Profil firewalla – Odaberite profil iz padajućeg izbornika **Prikaz pravila koja se upotrebljavaju u profilu** za prikaz filtra pravila profila.

Profil za nadogradnju – Omogućuje vam primjenu stvorenog profila za nadogradnju kada ste povezani s ovom mrežom.

Kontrolni elementi

Dodaj – Stvara novu poznatu mrežu.

Uredi – Kliknite da biste uredili postojeću poznatu mrežu.

Ukloni – odaberite mrežu i kliknite **Ukloni** da biste je uklonili s popisa poznatih mreža.

Vrh/Gore/Dolje/Dno – Omogućuje vam da podesite razinu prioriteta poznatih mreža (mreže se procjenjuju od vrha prema dnu).

Postavke konfiguracije mreže raspoređene su na sljedeće kartice:

Mreža

Ovdje možete definirati **naziv mreže** i odabrati **vrstu zaštite** (pouzdana, nepouzdana ili postavka "Upotrijebi postavku sustava Windows") za mrežu. U padajućem izborniku **profil Firewalla** odaberite profil za mrežu. Ako je na mreži odabrana vrsta zaštite **pouzdana**, sve izravno povezane podmreže smatraju se pouzdanima. Na primjer, ako je mrežni adapter spojen na ovu mrežu s IP adresom 192.168.1.5 i maska podmreže 255.255.255.0, u pouzdanu zonu adaptera dodaje se podmreža 192.168.1.0/24. Ako adapter ima više adresa/podmreža, sve se smatraju pouzdanima, neovisno o konfiguraciji **Identifikacija mreže** poznate mreže.

Također, adrese dodane pod **Dodatne pouzdane adrese** uvijek su dodane u pouzdanu zonu adaptera povezanih na mrežu (neovisno o vrsti zaštite mreže).

Upozori o slabom WiFi šifriranju – ESET Internet Security će vas obavijestiti kada se povežete s nezaštićenom bežičnom mrežom ili s mrežom sa slabom zaštitom.

Firewall profil – odaberite firewall profil koji se upotrebljava prilikom povezivanja s ovom mrežom.

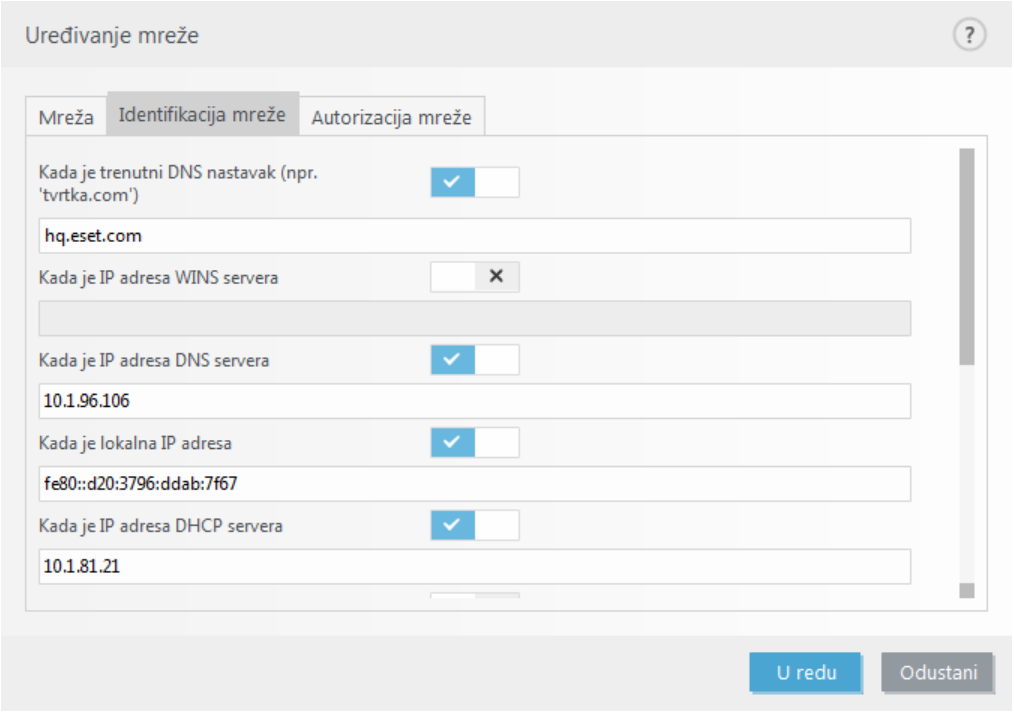
Nadogradnja profila – odaberite nadogradnju profila koji se upotrebljava prilikom povezivanja s ovom mrežom.

Sljedeći uvjeti moraju biti ispunjeni kako bi se mreža mogla označiti kao povezana u popisu povezanih mreža:

- **Identifikacija mreže** – Svi ispunjeni parametri moraju se podudarati s parametrima aktivne veze.
- **Autentikacija mreže** – Ako je odabran server za autentikaciju, potrebno je ostvariti uspješnu autentikaciju s pomoću ESET-ovog servera za autentikaciju.

Identifikacija mreže

Identifikacija mreže izvršava se na temelju parametara adaptera lokalne mreže. Svi odabrani parametri uspoređuju se s trenutnim parametrima aktivnih mrežnih veza. Dopuštene su IPv4 i IPv6 adrese.



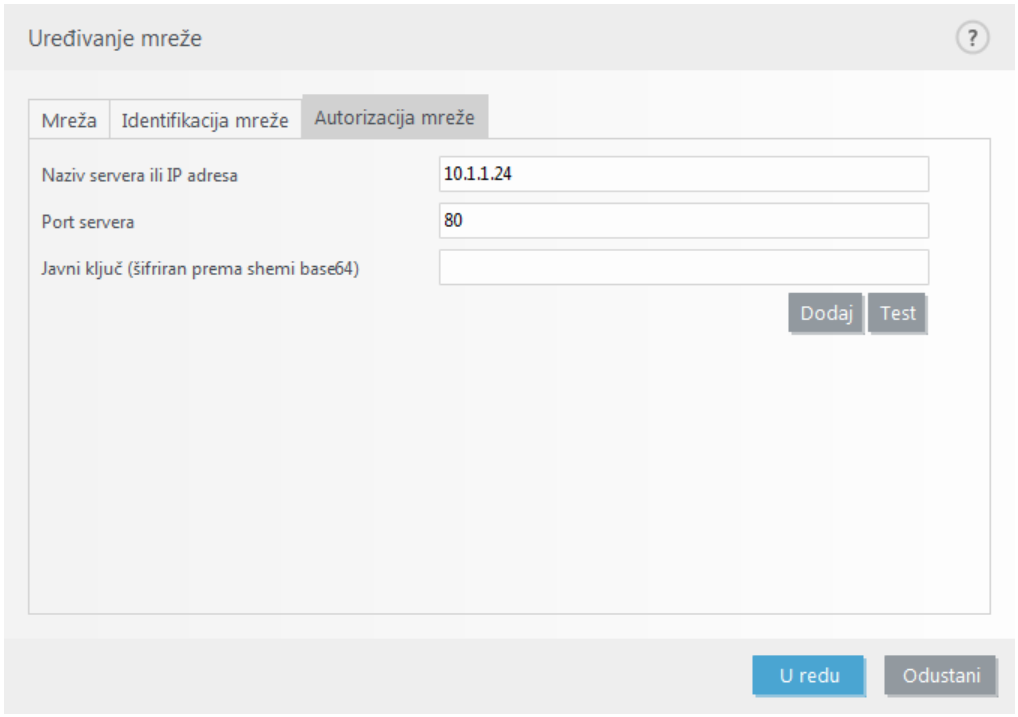
Autorizacija mreže

Autorizacija mreže traži određeni server u mreži i koristi asimetrično šifriranje (RSA) da bi ga autorizirala. Naziv mreže koja se autorizira mora se podudarati s nazivom zone postavljenim u postavkama servera za autorizaciju. Naziv je osjetljiv na velika i mala slova. Odredite naziv servera, port koji osluškuje server i javni ključ koji odgovara privatnom ključu servera (pogledajte odjeljak Autentikacija mreže – konfiguracija servera). Naziv servera može se unijeti u obliku IP adrese, DNS-a ili NetBios naziva te ga može slijediti put koji opisuje lokaciju ključa na serveru (npr., naziv_servera_/direktorij1/direktorij2/autorizacija). Možete odrediti alternativne servere za korištenje dodavanjem njihovih puteva, odvojenih točka-zarezom.

Preuzmite ESET-ov autorizacijski server.

Javni se ključ može uvesti uporabom bilo kojeg od sljedećih tipova datoteka:

- Šifrirani javni ključ PEM (.pem), ovaj se ključ može generirati s pomoću ESET-ovog servera za autentikaciju (pogledajte Autentikacija mreže – konfiguracija servera).
- Šifrirani javni ključ
- Certifikat javnog ključa (.crt)



Kliknite **Test** za testiranje postavki. Ako se autorizacija uspješno izvrši, prikazat će se obavijest Autorizacija servera uspješno je dovršena. Ako autorizacija nije ispravno konfigurirana, prikazat će se jedna od sljedećih poruka o pogreškama:

Autorizacija servera nije uspjela. Digitalni potpis nije ispravan ili se ne podudara.
Potpis servera ne odgovara unesenom javnom ključu.

Autorizacija servera nije uspjela. Naziv mreže ne odgovara.
Naziv konfigurirane mreže ne odgovara nazivu zone autorizacijskog servera. Pregledajte oba naziva i provjerite jesu li identični.

Autorizacija servera nije uspjela. Odgovor sa servera nije ispravan ili ga nema.
Ako server nije uključen ili je nedostupan, ne može se primiti odgovor. Odgovor može biti neispravan ako drugi HTTP server radi na navedenoj adresi.

Unesen je nevaljan javni ključ.
Provjerite je li uneseni javni ključ ispravan.

Autentikacija mreže – konfiguracija servera

Postupak autorizacije može provesti bilo koje računalo/server povezan s mrežom koju je potrebno autorizirati. Aplikacija ESET-ov autorizacijski server mora biti instalirana na računalo/server dostupan za autorizaciju kad god se klijent pokuša povezati s mrežom. Instalacijska datoteka aplikacije ESET-ov autorizacijski server dostupna je za preuzimanje na web stranici tvrtke ESET.

Nakon instalacije aplikacije ESET-ova servera za autorizaciju, pojavit će se dijaloški okvir (aplikaciji možete pristupiti klikom na **Start** > **Programi** > **ESET** > **ESET server za autorizaciju**).

Da biste konfigurirali autorizacijski server, unesite naziv zone za autorizaciju, port koji server osluškuje (standardna vrijednost je 80) i mjesto gdje će se pohraniti par javnog i privatnog ključa. Zatim generirajte javni i privatni ključ koji će biti korišteni tijekom postupka autorizacije. Privatni će ključ ostati postavljen na serveru dok javni ključ treba biti uvezen od strane klijenta u odjeljku Autorizacija zone kod postavljanja zone u podešavanju firewalla.

Dodatne informacije pročitajte u ovom članku ESET-ove baze znanja.

Konfiguriranje zona

Zona predstavlja skup mrežnih adresa koje čine jednu logičku grupu IP adresa i korisna je za ponovnu upotrebu istog skupa adresa za više različitih pravila. Svim adresama u određenoj grupi se dodjeljuju slična pravila koja se centralno definiraju za cijelu grupu. Primjer takve grupe je **Pouzdana zona**. Pouzdana zona predstavlja grupu mrežnih adresa koje Firewall ni na koji način ne blokira.

Da biste dodali pouzdanu zonu:

1. Otvorite **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Osnovno** > **Zone**.
2. Kliknite **Uredi** pokraj **Zone**.
3. Kliknite **Dodaj**, upišite **naziv** i **opis** zone te udaljenu IP adresu u odjeljak **Adresa udaljenog računala (IPv4/IPv6, raspon, maska)**.
4. Kliknite **U redu**.

Dodatne informacije potražite u odjeljku Zone firewalla.

Firewall zone

Dodatne informacije o zonama potražite u odjeljku Konfiguriranje zona.

Stupci

Naziv – Naziv grupe udaljenih računala.

IP adrese – Udaljene IP adrese koje pripadaju zoni.

Kontrolni elementi

Kada **dodajete** ili **uređujete** zonu, dostupna su sljedeća polja:

Naziv – Naziv grupe udaljenih računala.

Opis – Općeniti opis grupe.

Adresa udaljenog računala (IPv4/IPv6, raspon, maska) – Omogućuje vam dodavanje udaljene adrese, raspona adresa ili podmreže.

Izbriši – Uklanja zonu s popisa.

Imajte na umu da se unaprijed definirane zone ne mogu ukloniti.

Firewall

Firewall upravlja svim dolaznim i odlaznim mrežnim prometom u sustavu. To se postiže dopuštanjem ili zabranom pojedinačnih mrežnih veza na temelju navedenih pravila filtriranja. Nudi zaštitu od napada s udaljenih računala i može blokirati potencijalno prijeteće servise.

Osnovno

Aktiviraj firewall

Preporučujemo da tu funkciju ostavite aktiviranu kako biste osigurali zaštitu sustava. Kad je firewall aktiviran, mrežni promet skenira se u oba smjera.

Procijeni i pravila Windows Firewalla

U automatskom načinu rada dopusti dolazni promet koji dopuštaju pravila Windows Firewalla, osim ako nije eksplicitno blokiran ESET-ovim pravilima.

Način filtriranja

Ponašanje firewalla mijenja se ovisno o filtarskom načinu rada. Filtarski načini rada utječu i na razinu potrebne korisničke interakcije.

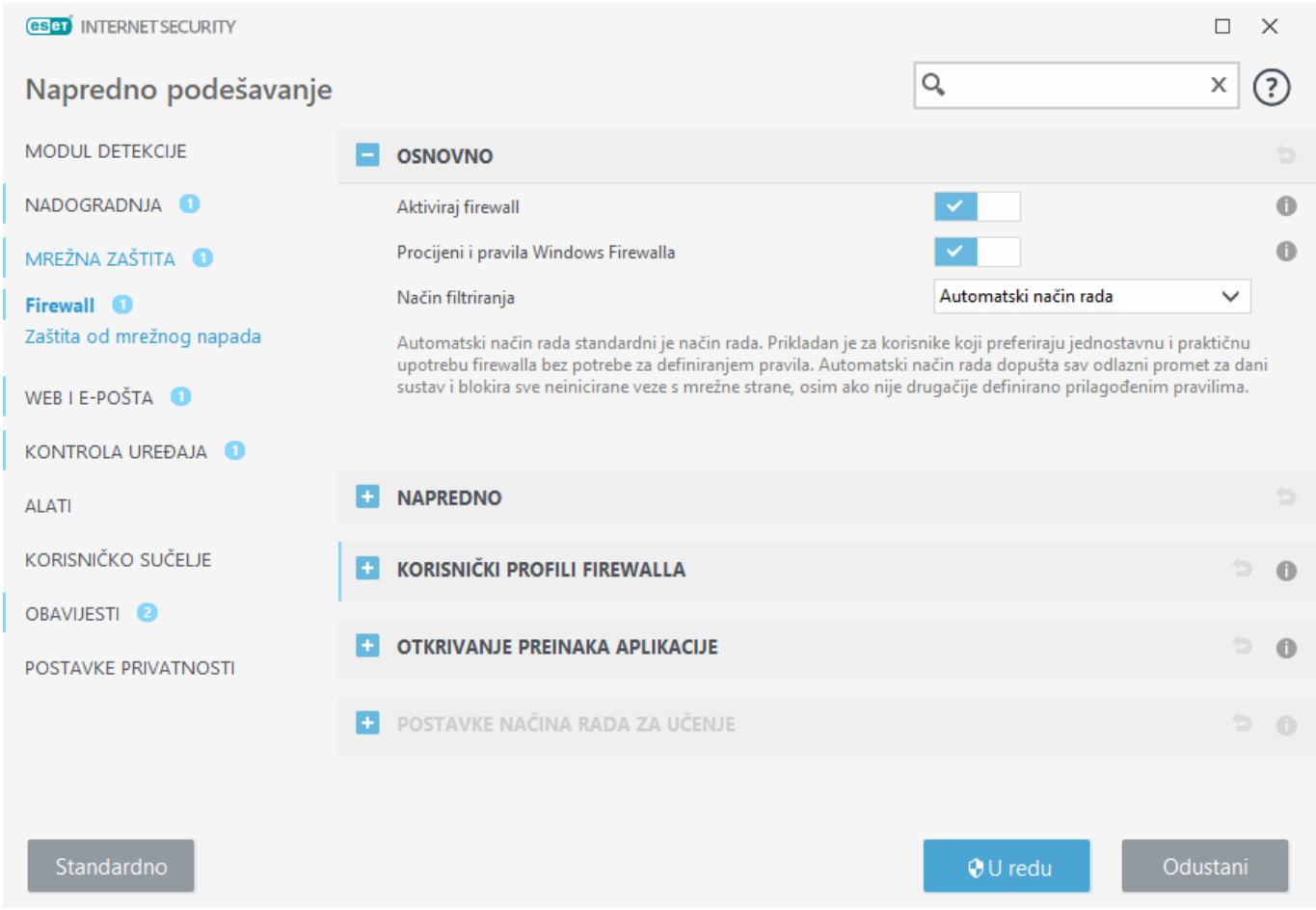
Za firewall programa ESET Internet Security dostupni su sljedeći filtarski načini rada:

Način filtriranja	Opis
Automatski način rada	Standardni način rada. Ovaj način rada prikladan je za korisnike koji daju prednost jednostavnoj i praktičnoj upotrebi firewalla, bez definiranja pravila. U **automatskom je načinu rada** moguće stvoriti korisnički definirana, prilagođena pravila, ali nije nužno. Automatski način rada dopušta sav odlazni promet za dani sustav i blokira većinu dolaznog prometa osim dijela prometa iz pouzdane zone (kao što je navedeno u odjeljku IDS i napredne mogućnosti / Dopušteni servisi) te odgovora na nedavnu odlaznu komunikaciju.
Interaktivni način	Omogućuje vam izradu prilagođene konfiguracije za vaš firewall. Kada se otkrije komunikacija na koju se ne primjenjuje nijedno od postojećih pravila, prikazat će se dijaloški prozor koji izvješćuje o nepoznatoj vezi. U tom dijaloškom prozoru postoji opcija dopuštanja ili zabrane komunikacije, a odluku o dopuštanju ili zabrani moguće je spremiti kao novo pravilo za firewall. Ako odlučite stvoriti novo pravilo, sve buduće veze te vrste bit će, ovisno o pravilu, dopuštene ili zapriječene.
Način rada na temelju pravila	Blokira sve veze koje nisu definirane posebnim pravilom koje ih dopušta. Taj način rada naprednim korisnicima omogućuje definiranje pravila koja dopuštaju samo željene i sigurne veze. Firewall će blokirati sve ostale nedefinirane veze.
Način rada za učenje	Automatski stvara i sprema pravila. Reakcija korisnika nije potrebna jer ESET Internet Security sprema pravila prema unaprijed definiranim parametrima. Da bi se izbjegli sigurnosni rizici, način rada za učenje trebalo bi koristiti samo dok još nisu stvorena sva pravila za potrebnu komunikaciju.

Napredno

Pravila

Podešavanje pravila omogućuje vam pregled svih pravila koja se primjenjuju na promet koji generiraju pojedinačne aplikacije unutar pouzdanih zona i interneta.



Pravilo IDS-a možete stvoriti kada vam računalo napadne botnet. Pravilo se može promijeniti u opcijama **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Zaštita od mrežnog napada** > **Pravila IDS-a** klikom na **Uredi**.

Dopušteni servisi

Konfigurirajte pristup uobičajenim mrežnim servisima koji su pokrenuti na računalu. Više informacija potražite u odjeljku Dopušteni servisi.

Firewall profili

Profili firewalla se mogu koristiti za prilagodbu ponašanja ESET Internet Security firewalla određivanjem različitih kompleta pravila u različitim situacijama.

Otkrivanje preinake aplikacije

Funkcija otkrivanja preinaka aplikacije prikazuje obavijesti ako preinačene aplikacije za koje postoji pravilo firewalla pokušaju uspostaviti veze.

Firewall profili

Profili se mogu koristiti za reguliranje funkcioniranja firewalla programa ESET Internet Security. Kada stvarate ili uređujete pravila firewalla, možete ih dodijeliti određenom profilu ili ih primijeniti na sve profile. Kada je profil aktivan na mrežnom sučelju, primjenjuju se samo globalna pravila (pravila za koja profil nije naveden) i pravila dodijeljena tom profilu. Možete stvoriti više profila s različitim pravilima dodijeljenim mrežnim adapterima ili mrežama kako biste lakše mijenjali ponašanje firewalla.

Kliknite **Uredi** pored mogućnosti Popis profila da biste otvorili prozor **Firewall profili** u kojem možete uređivati profile.

Mrežni adapter može se postaviti da koristi profil konfiguriran za određenu mrežu kada je povezan s tom mrežom. Možete također dodijeliti specifični profil za uporabu na određenoj mreži u **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Poznate mreže** > **Uredi**. Odaberite mrežu s popisa **Poznatih mreža** i kliknite **Uredi** da biste dodijelili firewall profil specifičnoj mreži iz padajućeg izbornika **Profil firewalla**.

Ako ta mreža nema dodijeljeni profil, tada se koristi standardni profil adaptera. Ako je adapter postavljen da ne koristi mrežni profil, standardni profil koristit će se neovisno o tome s kojom mrežom je povezan. Ako na mreži ili u konfiguraciji adaptera nema dostupnog profila, koristi se globalni standardni profil. Kako biste dodijelili profil mrežnom adapteru, odaberite mrežni adapter, kliknite **Uredi** uz **Profili dodijeljeni mrežnim adapterima**, uredite odabrane mrežne adaptere i odaberite profil iz padajućeg izbornika **Standardni profil firewalla**.

Kada se firewall prebaci na drugi profil, u donjem desnom kutu zaslona uz sistemski sat prikazat će se obavijest.

Dijaloški prozor – uređivanje Firewall profila

Ovdje možete odabrati mogućnosti **Dodaj**, **Uredi** ili **Ukloni** za profile. Imajte na umu da za korištenje mogućnosti **Uredi** ili **Ukloni** za profil, dotični profil mora biti odabran na popisu u prozoru **Profili firewalla**.

Dodatne informacije potražite u pomoći na temu Profili firewalla.

Profili dodijeljeni mrežnim adapterima

Promjenom profila možete brzo promijeniti ponašanje firewalla. Prilagođena pravila mogu se postaviti i primijeniti za određene profile. Unosi mrežnih adaptera za sve adaptere prisutne na računalu automatski se dodaju na popis **Mrežni adapteri**.

Stupci

Naziv – Naziv mrežnog adaptera.

Standardni profil firewalla – Zadani se profil upotrebljava kada mreža s kojom ste povezani nema konfigurirani profil ili ako je vaš mrežni adapter postavljen da ne upotrebljava mrežni profil.

Preferiraj profil mreže – Kada je aktivirano **Preferiraj firewall profil povezane mreže**, mrežni adapter koristit će firewall profil dodijeljen povezanoj mreži kad god je to moguće.

Kontrolni elementi

Dodaj – Dodaje novi mrežni adapter.

Uredi – Omogućuje vam uređivanje postojećeg mrežnog adaptera.

Ukloni – Odaberite mrežni adapter i kliknite **Ukloni** ako želite ukloniti mrežni adapter s popisa.

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

Konfiguriranje i korištenje pravila

Pravila predstavljaju skup uvjeta koji se koriste za smisleno testiranje svih mrežnih veza i sve radnje dodijeljene tim uvjetima. Korištenjem pravila firewalla možete definirati radnju koja će se poduzeti nakon uspostave različitih vrsta mrežnih veza. Da biste pristupili podešavanju filtriranja pravila, idite na **Napredno podešavanje** (F5) > **Firewall** > **Osnovno**. Neka od unaprijed definiranih pravila potvrdit će okvire iz odjeljka **dopušteni servisi** (IDS i napredne mogućnosti) i ne može ih se izravno isključiti, no možete koristiti te povezane potvrdne okvire kako biste to učinili.

Za razliku od prethodne verzije programa ESET Internet Security, pravila se procjenjuju s vrha prema dnu. Akcija prvog pravila koje se podudara primjenjuje se za svaku mrežnu vezu koja se pregledava. Ovo je važna promjena u ponašanju u odnosu na prethodnu verziju u kojoj je prioritet pravila bio automatski, a specifičnija pravila imala su veći prioritet nego općenita pravila.

Veze se mogu podijeliti na dolazne i odlazne. Dolazne veze inicira udaljeno računalo koje pokušava uspostaviti vezu s lokalnim sustavom. Odlazne veze funkcioniraju obrnuto – lokalni sustav uspostavlja vezu s udaljenim računalom.

Ako se otkrije nova nepoznata komunikacija, potrebno je dobro razmisliti želite li je dopustiti ili zabraniti. Neželjene, nesigurne ili nepoznate veze predstavljaju sigurnosni rizik za sustav. Ako se uspostavlja takva veza, preporučuje vam se da posvetite osobitu pozornost udaljenoj strani i aplikaciji koja se pokušava povezati s računalom. Mnoge infiltracije pokušavaju dohvatiti i preuzeti vaše osobne podatke ili infiltrirati druge zlonamjerne aplikacije na radne stanice u koje su provalile. Firewall korisniku omogućuje otkrivanje i prekid takvih veza.

Popis pravila firewalla

Popis pravila firewalla možete pronaći u izborniku **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Firewall** > **Napredno** tako da kliknete gumb **Uredi** pokraj stavke **Pravila**.

Stupci

Naziv – Naziv pravila.

Aktivirano – Prikazuje je li pravilo aktivirano ili deaktivirano; odgovarajući potvrdni okvir mora biti označen da bi se pravilo aktiviralo.

Protokol – Internet Protokol za koji vrijedi dotično pravilo.

Profil – Prikazuje profil firewalla za koji vrijedi dotično pravilo.

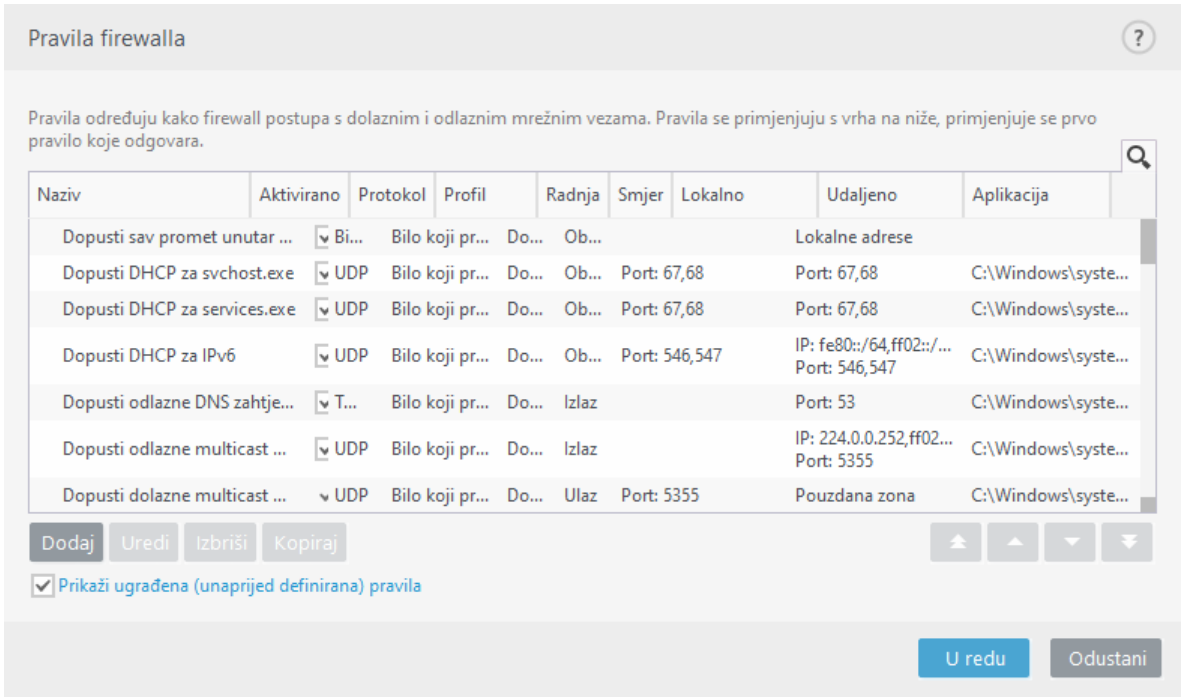
Radnja – prikazuje status komunikacije (blokiraj/dopusti/pitaj).

Smjer – Smjer komunikacije (dolazna/odlazna/oboje).

Lokalno – udaljena IPv4 ili IPv6 adresa/raspon/podmreža i port lokalnog računala.

Udaljeno – udaljena IPv4 ili IPv6 adresa/raspon/podmreža i port udaljenog računala.

Aplikacija – Aplikacija na koju se primjenjuje pravilo.



Kontrolni elementi

Dodaj – Stvara novo pravilo.

Uredi – Uređuje postojeće pravilo.

Obriši – Uklanja postojeće pravilo.

Kopiraj – Stvara kopiju odabranog pravila.

Prikaži ugrađena (prethodno definirana) pravila – Pravila koja je prethodno definirao ESET Internet Security, a koja dopuštaju ili zabranjuju određenu komunikaciju. Ova pravila možete deaktivirati, ali brisanje unaprijed definiranog pravila nije moguće.

Vrh/Gore/Dolje/Dno – Omogućuje prilagodbu razine prioriteta pravila (pravila se izvršavaju s vrha prema dnu).

Kliknite ikonu za pretraživanje u gornjem desnom kutu za pretraživanje pravila prema nazivu, protokolu ili portu.

Dodavanje ili uređivanje pravila firewalla

Izmjena je potrebna svaki put kada se promijeni neki od nadziranih parametara. Ako se izvrše izmjene zbog kojih pravilo ne može zadovoljiti uvjete i određena akcija ne može biti primijenjena, dotična će veza možda biti odbijena. To može uzrokovati probleme u radu aplikacije na koju se pravilo odnosi. Primjer je promjena mrežne adrese ili broja porta na udaljenoj strani.

> **Ilustrirane upute**
>
> Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
> - Otvorite ili zatvorite (dopustite ili zabranite) određeni port na ESET firewallu
> - Stvorite pravilo firewalla u dnevnicima u programu ESET Internet Security

U gornjem dijelu prozora nalaze se tri kartice:

- **Opće** – navodi naziv pravila, smjer veze, radnju (**Dopusti**, **Zabrani**, **Pitaj**), protokol i profil na koji će se pravilo primjenjivati.

- **Lokalno** – Prikazuje informacije o lokalnoj strani veze, uključujući broj lokalnog porta ili raspona portova te naziv komunikacijske aplikacije. Ovdje možete dodati i unaprijed definirane ili stvorene zone s rasponom IP adresa klikom na mogućnost **Dodaj**.

- **Udaljeno** – Na toj kartici nalaze se informacije o udaljenom portu (rasponu portova). Možete definirati popis udaljenih IP adresa ili zona za dotično pravilo. Ovdje možete dodati i unaprijed definirane ili stvorene zone s rasponom IP adresa klikom na mogućnost **Dodaj**.

Prilikom stvaranja novog pravila morate unijeti naziv pravila u polje **Naziv**. Odaberite smjer u kojem će se pravilo primjenjivati s padajućeg izbornika **Smjer** i akciju s padajućeg izbornika **Akcija** koja će se izvršiti kada komunikacija zadovolji pravilo.

Protokol predstavlja protokol prijenosa koji se koristi za pravilo. S padajućeg izbornika odaberite protokol koji će se koristiti za dotično pravilo.

ICMP vrsta/kôd predstavlja ICMP poruku označenu brojem (na primjer, 0 označava "Odgovor odjeka").

Prema standardnim su postavkama sva pravila aktivirana za **Svaki profil**. Možete odabrati i prilagođeni profil firewalla na padajućem izborniku **Profil**.

Ako aktivirate **Minimalna opširnost zapisivanja**, aktivnost povezana s pravilom zabilježit će se u dnevnik. Mogućnost **Obavijesti korisnika** prikazuje obavijest kada se primijeni pravilo.

Stvaramo novo pravilo da bismo dopustili aplikaciji web preglednika Firefox pristup za Internet / web stranice lokalne mreže. U ovom slučaju potrebno je konfigurirati sljedeće stavke:
1.Na kartici **Općenito** aktivirajte odlaznu komunikaciju putem TCP i UDP protokola.
2.Kliknite karticu **Lokalno**.
3.Odaberite put datoteke web preglednika koji upotrebljavate tako da kliknete **...** (primjerice, *C:\Program Files\Firefox\Firefox.exe*). NEMOJTE upisati naziv aplikacije.
4.Ako želite dopustiti samo standardne aktivnosti pregledavanja interneta, na kartici **Udaljeno** aktivirajte brojeve porta 80 i 443.

Napominjemo da su izmjene unaprijed definiranih pravila ograničene.

Pravilo firewalla – lokalno

Navedite naziv lokalne aplikacije i lokalnih portova na koje će se pravilo primjenjivati.

Port – brojevi lokalnih portova. Ako se ne navede nijedan broj, pravilo će se primijeniti na sve portove. Dodajte jedan komunikacijski port ili niz komunikacijskih portova.

IP – Omogućuje vam dodavanje udaljene adrese/adresa, raspona adresa ili podmreže na koje će se pravilo primijeniti. Ako ne navedete vrijednost, pravilo će se primjenjivati na sve portove.

Zone – Popis dodanih zona.

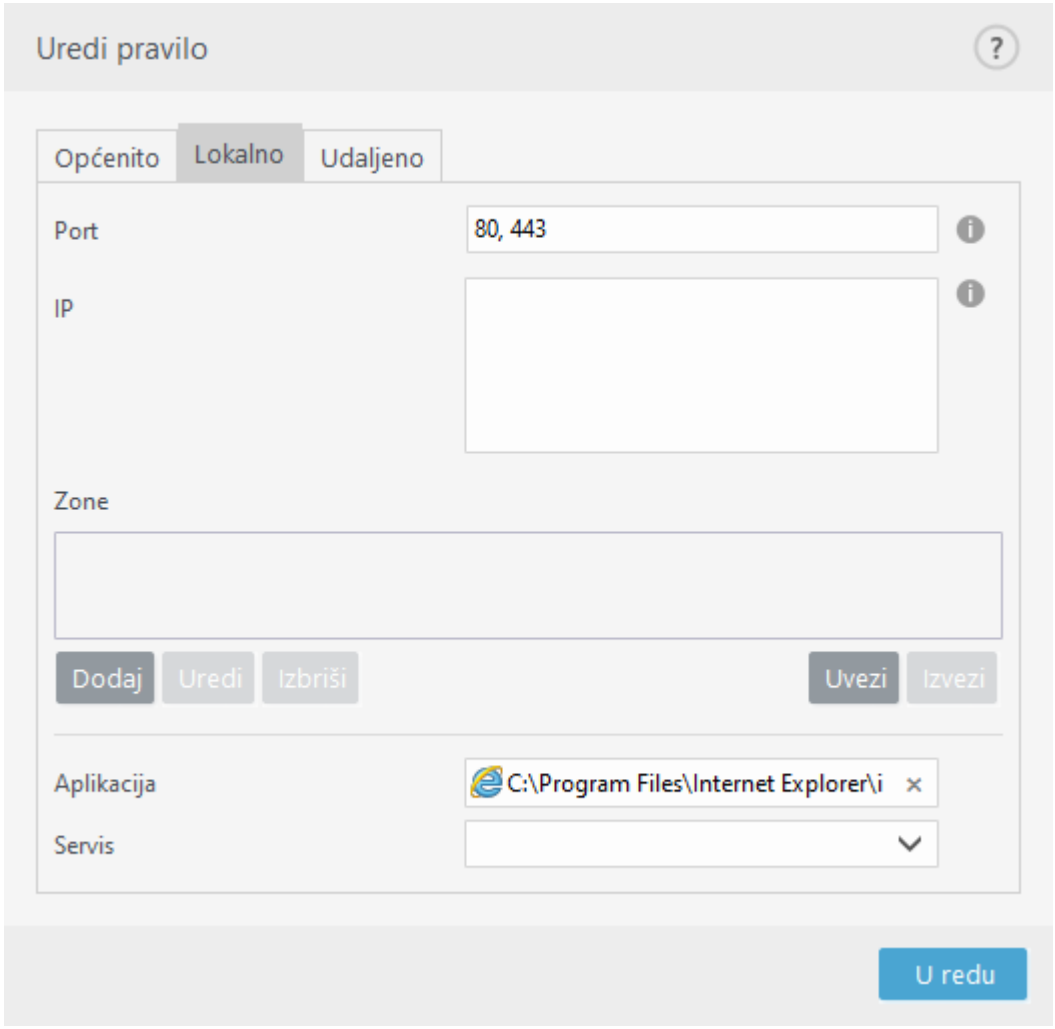
Dodaj – Dodavanje stvorene zone s padajućeg izbornika. Da biste stvorili zonu, koristite karticu Podešavanje zona.

Ukloni – Uklanja zone s popisa.

Aplikacija – Naziv aplikacije na koju se pravilo odnosi. Dodajte lokaciju aplikacije na koju će se pravilo primijeniti.

Servis – Padajući izbornik prikazuje servise sustava.

> Bilo bi dobro da na padajućem izborniku za komunikaciju stvorite pravilo za mirror koji omogućuje nadogradnje preko porta 2221 pomoću značajke EHttpSrv servis .



Pravilo firewalla – udaljeno

Port – Brojevi udaljenih portova. Ako se ne navede nijedan broj, pravilo će se primijeniti na sve portove. Dodajte jedan komunikacijski port ili niz komunikacijskih portova.

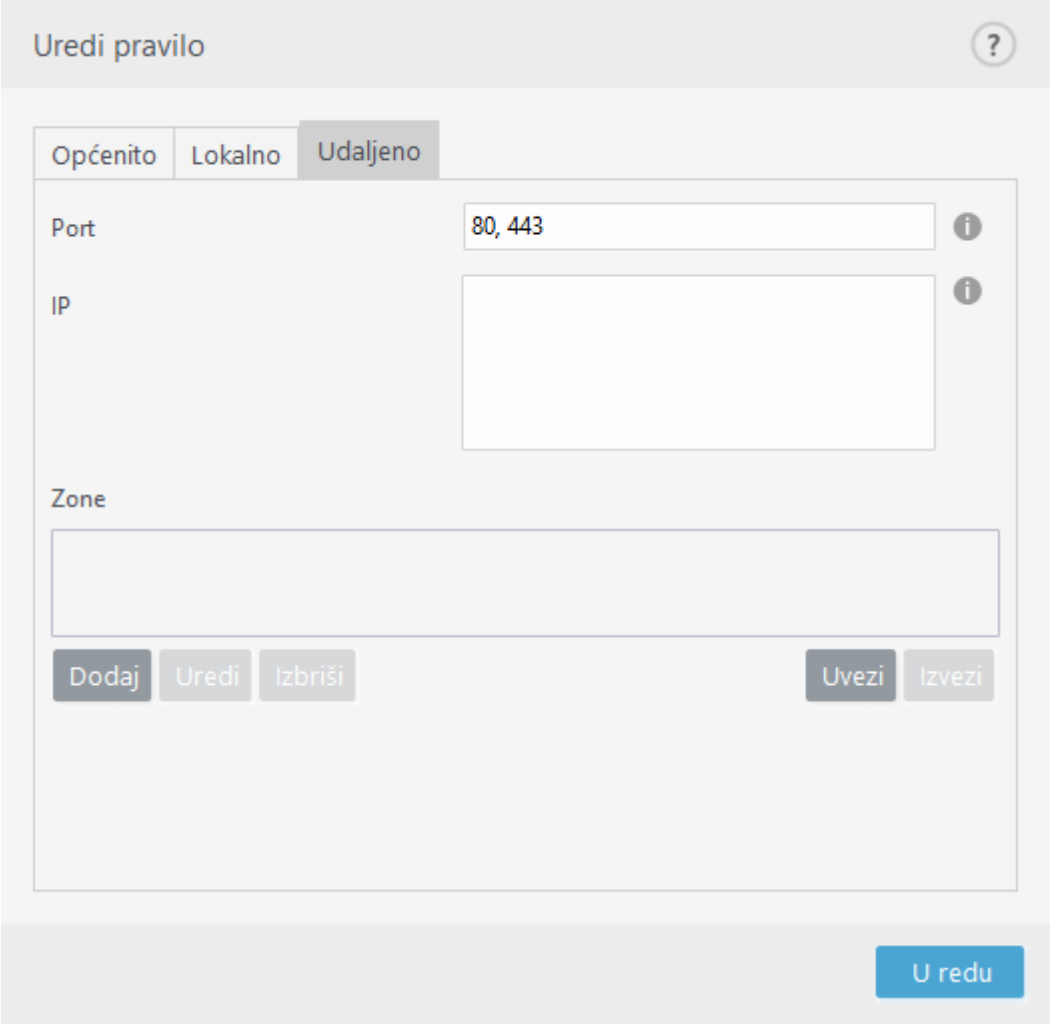
IP – Omogućuje vam dodavanje udaljene adrese, raspona adresa ili podmreže. Adresa, raspon adresa/podmreža ili udaljena zona na koju se primjenjuje pravilo. Ako se ne navede nijedna vrijednost, pravilo će se primjenjivati na svu komunikaciju.

Zone – Popis dodanih zona.

Dodaj – Dodavanje zone odabrane iz padajućeg izbornika. Da biste stvorili zonu, koristite karticu Podešavanje

zona.

Ukloni – Uklanja zone s popisa.



Otkrivanje preinake aplikacije

Funkcija otkrivanja preinaka aplikacije prikazuje obavijesti ako preinačene aplikacije za koje postoji pravilo firewalla pokušaju uspostaviti veze. Preinačavanje aplikacija je mehanizam privremene ili trajne zamjene izvorne aplikacije drugom aplikacijom s drugom izvršnom datotekom (štiti od zloporabe pravila firewalla).

Imajte na umu da ova značajka ne može otkriti preinake na svim aplikacijama općenito. Cilj je izbjegavanje zlouporabe pravila firewalla te se provjeravaju samo aplikacije za koje postoje specifična pravila firewalla.

Aktiviraj otkrivanje preinaka aplikacija – Ako je odabran taj okvir, program će pratiti promjene aplikacija (aktualizacije, zaraze i druge preinake). Kada preinačena aplikacija pokuša uspostaviti vezu, dobit ćete obavijest od firewalla.

Dopusti preinaku potpisanih (pouzdanih) aplikacija – Ako aplikacija ima isti važeći digitalni potpis prije i poslije preinaka, nemoj slati obavijest.

Popis aplikacija izuzetih od otkrivanja prijetnji – u ovom prozoru možete dodati ili ukloniti zasebne aplikacije za koje se dopuštaju preinake bez obavijesti.

Popis aplikacija izuzetih od otkrivanja prijetnji

Firewall programa ESET Internet Security otkriva promjene aplikacija za koje postoje pravila (pogledajte Otkrivanje preinaka aplikacije).

U određenim slučajevima možda nećete htjeti upotrebljavati ovu funkcionalnost za neke aplikacije ako ih želite izuzeti iz provjere firewalla.

Dodaj – Otvara prozor u kojem možete dodati aplikacije na popis aplikacija izuzetih od otkrivanja preinaka. Postoji popis pokrenutih aplikacija s otvorenom mrežnom komunikacijom za koji postoji pravilo firewalla s kojeg možete birati ili možete dodati određenu aplikaciju.

Uredi – Otvara prozor u kojem možete promijeniti lokaciju aplikacije koja je na popisu aplikacija izuzetih od otkrivanja preinaka. Postoji popis pokrenutih aplikacija s otvorenom mrežnom komunikacijom za koji postoji pravilo firewalla s kojeg možete birati ili možete promijeniti lokaciju ručno.

Ukloni – Uklanja unose s popisa aplikacija koje su izuzete od otkrivanja preinaka.

Postavke načina rada za učenje

Značajka načina rada za učenje automatski stvara i sprema pravilo za svaku komunikaciju koja se uspostavi u sustavu. Reakcija korisnika nije potrebna jer ESET Internet Security sprema pravila prema unaprijed definiranim parametrima.

Taj način rada nije siguran te se preporuča samo za početnu konfiguraciju firewalla.

Odaberite **Način učenja** iz padajućeg izbornika pod **Napredno podešavanje** (F5) > **Firewall** > **Osnovno** > **Način filtriranja** za aktivaciju **Opcija načina učenja**. Taj odjeljak sadrži sljedeće stavke:

> ⚠ U načinu rada za učenje firewall ne filtrira komunikaciju. Dopuštena je sva izlazna i ulazna komunikacija. U tom načinu rada firewall ne štiti računalo u potpunosti.

Način rada postavljen nakon isteka načina rada za učenje – Definirajte na koji će se način filtriranja ESET Internet Security Firewall vratiti nakon isteka razdoblja načina rada za učenje. Pročitajte više o načinima filtriranja. Nakon isteka opcija **Pitaj korisnika** zahtijeva administratorske ovlasti da bi izvršila promjenu načina filtriranja firewalla.

Vrsta komunikacije – Odaberite pojedinačne principe stvaranja pravila za svaku vrstu komunikacije. Postoje četiri vrste komunikacije:

Ulazni promet iz pouzdane zone – Primjer dolazne veze unutar pouzdane zone bilo bi udaljeno računalo koje se nalazi unutar pouzdane zone, a pokušava uspostaviti komunikaciju s lokalnom aplikacijom koja je pokrenuta na vašem računalu.

Izlazni promet u pouzdanu zonu – Lokalna aplikacija pokušava uspostaviti vezu s nekim drugim računalom u lokalnoj mreži ili u mrežama u pouzdanoj zoni.

Ulazni internetski promet – Udaljeno računalo pokušava komunicirati s aplikacijom na vašem računalu.

Izlazni internetski promet – Lokalna aplikacija pokušava uspostaviti vezu s drugim računalom.

Svaki odjeljak omogućuje definiranje parametara koji će se dodati novostvorenim pravilima:

Dodaj lokalni port – Sadrži broj lokalnog porta mrežne komunikacije. Za potrebe odlazne komunikacije obično se generiraju nasumični brojevi. Zbog toga preporučujemo da tu mogućnost aktivirate samo za ulaznu komunikaciju.

Dodaj aplikaciju – Sadrži naziv lokalne aplikacije. Ta je mogućnost pogodna za buduća pravila na razini aplikacije (pravila koja definiraju komunikaciju za cijelu aplikaciju). Možete, primjerice, aktivirati komunikaciju samo za web preglednik ili klijent e-pošte.

Dodaj udaljeni port – Sadrži broj udaljenog porta mrežne komunikacije. Možete, primjerice, dopustiti ili uskratiti određenu uslugu povezanu sa standardnim brojem porta (HTTP – 80, POP3 – 110 itd.)

Dodaj udaljenu IP adresu / pouzdanu zonu – Udaljena IP adresa ili zona može se koristiti kao parametar za nova pravila koja definiraju sve mrežne veze između lokalnog sustava i udaljene adrese/zone. Ta je mogućnost pogodna ako želite definirati akcije za određeno računalo ili grupu umreženih računala.

Maksimalan broj različitih pravila za aplikaciju – Ako aplikacija komunicira putem različitih portova, s različitim IP adresama itd., firewall u načinu rada za učenje stvorit će odgovarajući broj pravila za tu aplikaciju. To omogućuje da ograničite broj pravila koja se mogu stvoriti za jednu aplikaciju.

Zaštita od mrežnog napada (IDS)

Zaštita od mrežnog napada (IDS) poboljšava otkrivanje zlouporaba poznatih ranjivosti. Više o zaštiti od mrežnog napada pročitajte u Rječniku.

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 zlоćudnim 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.

> **Ilustrirane upute**
> Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
> - Izuzimanje IP adrese iz IDS-a u programu ESET Internet Security

Svi važni događaji otkriveni uz pomoć mrežne zaštite spremaju se u datoteku dnevnika. Dodatne informacije potražite u dnevniku mrežne zaštite.

Zaštita od napada grubom silom

Zaštita od napada grubom silom blokira napade pogađanjem lozinke za RDP i SMB servise. Napad grubom silom je metoda otkrivanja ciljane lozinke koja obuhvaća sustavno isprobavanje svih kombinacija slova, brojeva i simbola. Da biste konfigurirali zaštitu od napada grubom silom, u glavnom prozoru programa kliknite **Podešavanje** > **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Zaštita od mrežnog napada** > **Zaštita od napada grubom silom**.

Aktiviraj zaštitu od napada grubom silom – ESET Internet Security provjerava sadržaj mrežnog prometa i blokira

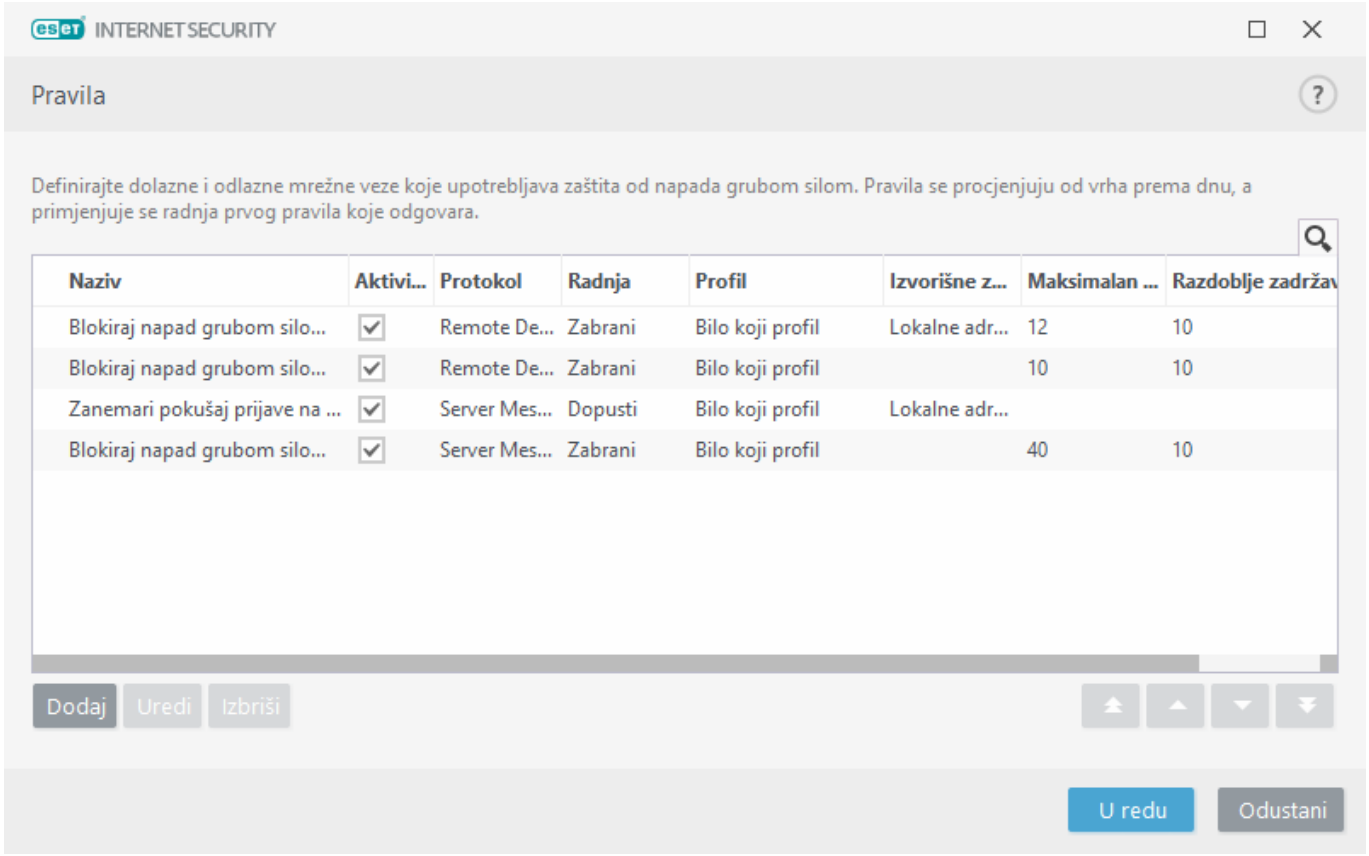
pokušaje napada pogađanjem lozinki.

Pravila – omogućuju vam da stvarate, uređujete i pregledavate pravila za dolazne i odlazne mrežne veze. Više informacija potražite u poglavlju Pravila.

Pravila

Pravila zaštite od napada grubom silom omogućuju vam da stvorite, uredite i prikažete pravila za dolazne i odlazne mrežne veze. Unaprijed definirana pravila ne mogu se uređivati niti brisati.

Upravljanje pravilima zaštite od napada grubom silom



Dodaj – Stvara novo pravilo.

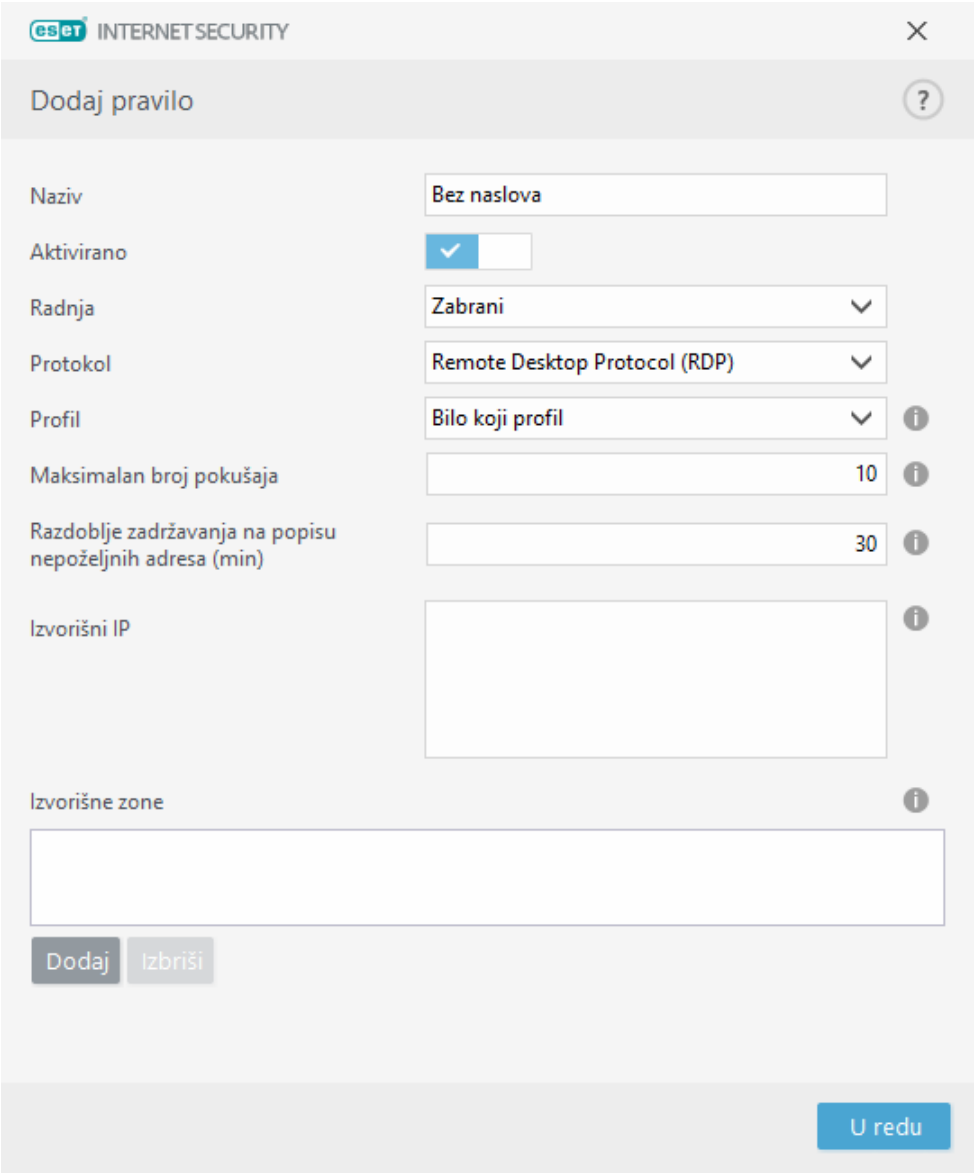
Uredi – Uređuje postojeće pravilo.

Izbriši – uklonite postojeće pravilo s popisa pravila.

Vrh/gore/dolje/dno – prilagodite razinu prioriteta pravila.

Da bi se osigurala najveća zaštita, primjenjuje se pravilo za blokiranje s najnižom vrijednošću za **Maksimalni broj pokušaja**, čak i ako je pravilo postavljeno niže na popisu pravila kada se višestruka pravila za blokiranje podudaraju s uvjetima za otkrivanje prijetnji.

Uređivač pravila



Naziv – naziv pravila.

Aktivirano – deaktivirajte traku klizača ako želite zadržati pravilo na popisu, ali ne i primijeniti ga.

Radnja – odaberite želite li **odbiti** ili **dopustiti** vezu ako su postavke pravila ispunjene.

Protokol – komunikacijski protokol koji će ovo pravilo pregledati.

Profil – prilagođena pravila mogu se postaviti i primijeniti za određene profile.

Maksimalan broj pokušaja – Maksimalan broj dopuštenih pokušaja ponavljanja napada dok se IP adresa ne blokira i doda na popis nepoželjnih adresa.

Razdoblje zadržavanja na popisu nepoželjnih adresa (u minutama) – postavlja vrijeme nakon kojeg se adresa uklanja s popisa nepoželjnih adresa. Standardno vremensko razdoblje za brojanje pokušaja je 30 minuta.

Izvorišni IP – popis IP adresa / raspona / podmreža. Adrese moraju biti odvojene zarezom.

Izvorišne zone – omogućuje da se dodaju unaprijed definirane ili stvorene zone s nizom IP adresa kad kliknete **Dodaj**.

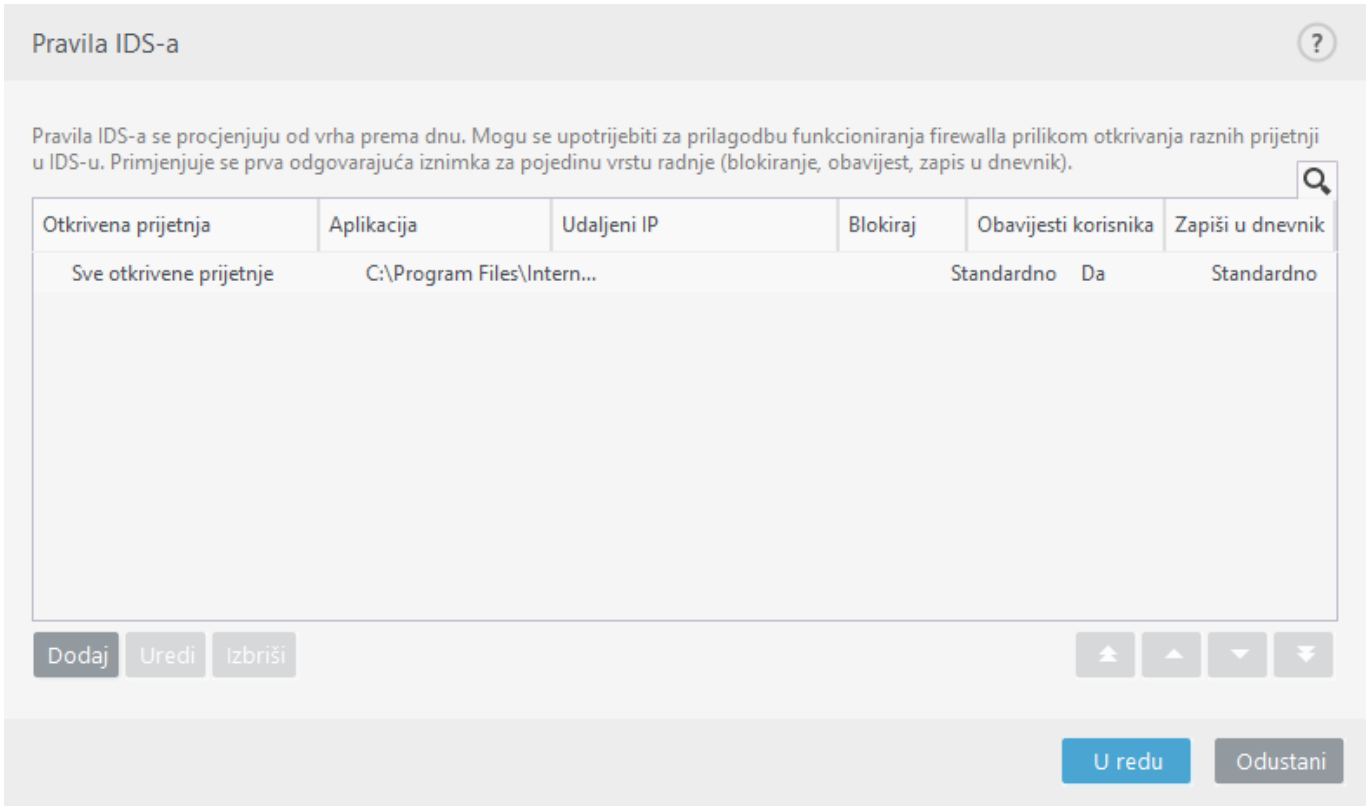
IDS pravila

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.

> **Ilustrirane upute**
> Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
> - Izuzimanje IP adrese iz IDS-a u programu ESET Internet Security

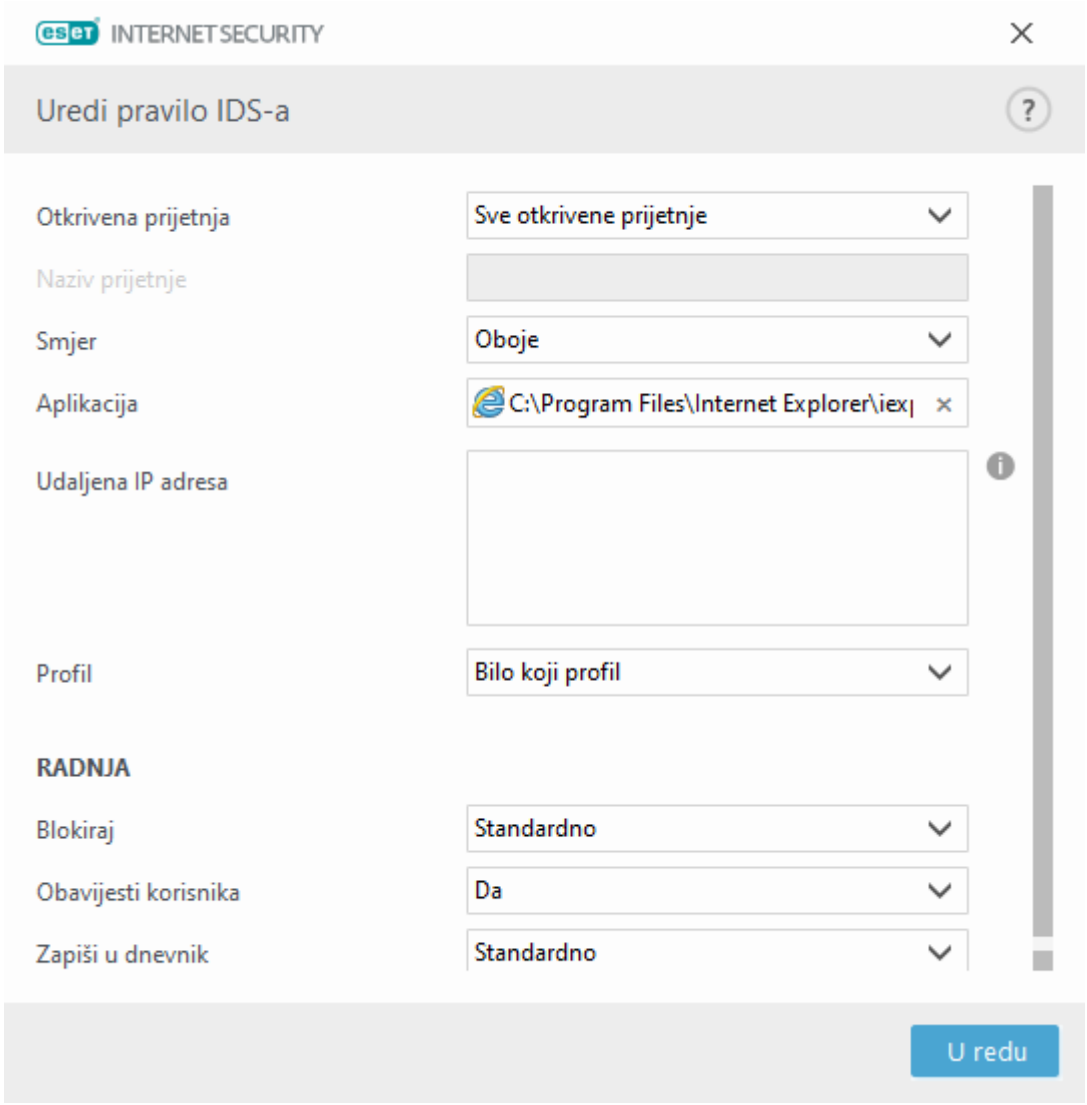
Stupci

- **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 proces sustava ima svoje standardno ponašanje i dodijeljenu radnju (blokiraj ili dopusti). Da biste nadjačali standardno ponašanje programa ESET Internet Security, putem padajućeg izbornika možete odabrati želite li ga blokirati ili dopustiti.
- **Obavijesti korisnika** – odaberite želite li da se prikazuju Obavijesti na radnoj površini na vašem računalu. Odaberite jednu od opcija **Standardno**/**Da**/**Ne**.
- **Dnevnik** – zapisivanje događaja u dnevnike programa ESET Internet Security. Odaberite jednu od opcija **Standardno**/**Da**/**Ne**.



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 pravilo s popisa pravila IDS-a.
- **Vrh/Gore/Dolje/Dno** – Omogućuje prilagodbu razine prioriteta pravila (pravila se procjenjuju s vrha prema dnu).



Ako želite prikazati obavijest i prikupiti dnevnik svaki put kada se događaj pojavi:
1.Kliknite **Dodaj** da biste dodali novo pravilo IDS-a.
2.Odaberite određenu prijetnju iz padajućeg izbornika **Prijetnja**.
3.Odaberite put aplikacije tako da kliknete **...** za aplikaciju na koju želite primijeniti ovu obavijest.
4.Ostavite postavku **Standardno** u padajućem izborniku **Blokiraj**. Time će se preuzeti standardna radnja koju primjenjuje ESET Internet Security.
5.Postavite padajuće izbornike **Obavijesti** i **Dnevnik** na **Da**.
6.Kliknite **U redu** da biste spremili ovu obavijest.

Ako ne želite prikazivati učestale obavijesti koje ne smatrate prijetnjom, a dio su određene vrste **Prijetnja**:
1.Kliknite **Dodaj** da biste dodali novo pravilo IDS-a.
2.Odaberite određenu prijetnju iz padajućeg izbornika **Prijetnja**, na primjer **SMB sesija bez sigurnosnih ekstenzija napad skeniranjem TCP porta**.
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 iskorištavajući sigurnosnu rupu ili čak ako se otkrije pokušaj skeniranja portova u vašem sustavu.

Prijetnja – Naziv prijetnje.

Udaljena adresa – Udaljena IP adresa.

Dopusti – stvara pravilo za uslugu otkrivanja upada (IDS) s tim da je za svaku vrstu radnje unaprijed definirano nepoduzimanje radnje (blokiranje, obavještavanje, zapisivanje).

Nastavi blokirati – Blokira otkrivenu prijetnju. Za stvaranje IDS iznimke za ovu prijetnju odaberite potvrdni okvir **Nemoj me ponovno obavijestiti** i pravilo će se dodati bez obavijesti i vođenja dnevnika.

> 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.
> Da biste riješili **duplikate IP adresa na mreži**, pogledajte članak iz ESET-ove baza znanja.

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**, komunkacija 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. Uz to, pravila koja je stvorio čarobnjak možete vidjeti u odjeljku **Napredno podešavanje** > **Mrežna zaštita** > **Firewall** > **Napredno** > **Pravila**.

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

Dozvoljeni servisi i napredne opcije

Napredne opcije u odjeljcima Firewall i Zaštita od mrežnih napada omogućuju vam da konfigurirate pristup nekim servisima pokrenutima na računalu iz pouzdane zone.

Možete omogućiti ili onemogućiti otkrivanje nekoliko vrsta napada i izrabljivača koji bi mogli naštetiti računalu.

> 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 pojedinih opcija u ovom prozoru može se razlikovati, ovisno o vrsti programa tvrtke ESET, modula firewalla i verziji vašeg operacijskog sustava.

Dopušteni servisi

Postavke iz ove grupe namijenjene su za lakše konfiguriranje pristupa servisima tog računala iz pouzdane zone. Mnogi od njih aktiviraju/deaktiviraju unaprijed definirana pravila firewalla. Dopuštene servise možete uređivati u odjeljku **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Firewall** > **Napredno** > **Dopušteni servisi**.

- **Dopusti zajedničko korištenje datoteka i pisača u pouzdanoj zoni** – Dopušta udaljenim računalima u pouzdanoj zoni pristup zajedničkim datotekama i pisačima.

- **Dopusti UPNP za sistemske servise u pouzdanoj zoni** – Dopušta dolazne i odlazne zahtjeve UPnP protokola za sistemske servise. UPnP (Universal Plug and Play, poznat i kao Microsoft Network Discovery) koristi se u sustavu Windows Vista i novijim operacijskim sustavima.

- **Dopusti dolaznu RPC komunikaciju u pouzdanoj zoni** – Aktivira se TCP povezivanje iz pouzdane zone čime se dopušta pristup servisima MS RPC Portmapper i RPC/DCOM.

- **Dopusti udaljeni pristup radnoj površini u pouzdanoj zoni** – Aktivira se povezivanje putem protokola Microsoft Remote Desktop Protocol (RDP) te se dopušta računalima u pouzdanoj zoni da pristupaju vašem računalu pomoću programa koji koristi RDP (kao što je Remote Desktop Connection).

- **Aktiviraj prijavu na višeodredišne grupe putem IGMP**-a – Dopušta se dolazni/odlazni IGMP i dolazni UDP višeodredišni streaming, primjerice videostreaming koji su generirali programi koji upotrebljavaju protokol IGMP (Internet Group Management Protocol).

- **Dopusti komunikaciju za premošćene veze** – odaberite ovu opciju da biste izbjegli prekid premošćenih veza. Premošćeno umrežavanje povezuje virtualno računalo s mrežom putem adaptera za Ethernet serverskog računala. Ako upotrebljavate premošćeno umrežavanje, virtualno računalo može pristupiti drugim uređajima na mreži i obrnuto, kao da se radi o fizičkom računalu na mreži.

- **Dopusti automatsko otkrivanje web servisa (WSD) za sistemske servise u pouzdanoj zoni** – Propušta kroz firewall dolazne zahtjeve Web Services Discovery iz pouzdanih zona. WSD je protokol koji se koristi za pronalaženje servisa na lokalnoj mreži.

- **Dopusti višeodredišnu adresnu razlučivost u pouzdanoj zoni (LLMNR)** – LLMNR (Link-Local Multicast Name Resolution) protokol je koji se temelji na DNS paketu koji dopušta glavnim računalima IPv4 i IPv6 rješavanje naziva za glavna računala na istoj lokalnoj vezi bez konfiguriranja DNS servera ili DNS klijenta. Ova opcija dopušta dolazne multicast DNS zahtjeve iz pouzdane zone kroz firewall.

- **Podrška za Windows HomeGroup** – Aktivira se HomeGroup podrška za Windows 7 i novije operacijske sustave. Unutar osnovne grupe moguće je dijeliti datoteke i pisače na kućnoj mreži. Da biste konfigurirali Homegroup, prijeđite na **Start** > **Upravljačka ploča** > **Mreža i internet** > **HomeGroup**.

Otkrivanje upada

Otkrivanje upada nadzire zlćudne aktivnosti u mrežnoj komunikaciji uređaja. Te postavke možete urediti u odjeljku **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Zaštita od mrežnog napada** > **Napredne opcije** > **Otkrivanje upada**.

- **Protokol SMB** – Otkriva i blokira razne sigurnosne probleme u SMB protokolu.

- **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 gore).

- **ARP Otkrivanje napada onečišćenjem** – otkrivanje napada ARP onečišćenjem koje se aktivira posredničkim napadima vrste "man-in-the-middle" ili otkrivanje prisluškivanja na mrežnom preklopniku. ARP (Address Resolution Protocol – protokol za razrješavanje adrese) koriste mrežne aplikacije ili uređaji za utvrđivanje Ethernet adrese.

- Otkrivanje napada skeniranjem **TCP/UDP porta** – Otkrivaju se napadi koje vrši softver/aplikacija koja skenira portove i koja je osmišljena da traži otvorene portove na hostu slanjem klijentskih zahtjeva određenom rasponu adresa portova s ciljem pronalaženja aktivnih portova te iskorištavanja slabosti servisa. Više o toj vrsti napada pročitajte u rječniku.

- **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

Vrsta analize paketa koja filtrira prijenos podataka putem mreže. Te postavke možete urediti u odjeljku **Napredno podešavanje** (F5) > **Mrežna zaštita** > **Zaštita od mrežnog napada** > **Napredne opcije** > **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$*ADMIN$*). 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.

- **Zabrani otvaranje izvršnih datoteka na serveru izvan pouzdane zone u SMB protokolu** – Odbija se veza kad pokušavate pokrenuti izvršnu datoteku (.exe, .dll...) iz zajedničke mape na serveru koji ne pripada pouzdanoj zoni u firewallu. Imajte na umu da kopiranje izvršnih datoteka iz pouzdanih izvora može biti legitimno. Napominjemo da kopiranje izvršnih datoteka iz pouzdanih izvora može biti legitimno. Međutim, ovo bi otkrivanje trebalo umanjiti rizik neželjenog otvaranja datoteke na zlonamjernom serveru (primjerice, klikom hiperveze na zajedničku zlonamjernu izvršnu datoteku).

- **Zabrani NTLM autentikaciju u SMB protokolu za povezivanje servera u/izvan pouzdane zone** – Protokoli koji koriste NTLM sheme autentikacije (obje verzije) podliježu napadu prosljeđivanjem korisničkih podataka (poznatom i kao „SMB Relay" kada se radi o SMB protokolu). Zabrana NTLM autorizacije pri povezivanju sa serverom izvan pouzdane zone trebala bi umanjiti rizik da će zlonamjerni server izvan poudane zone proslijediti podatke. Na sličan se način može zabraniti i NTLM autorizacija pri povezivanju sa serverima u pouzdanoj zoni.

- **Dopusti komunikaciju sa servisom Security Account Manager** – Više informacija o ovom servisu pogledajte ovdje [MS-SAMR].

- **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** – Drugi MSRPC servisi.

Povezane mreže

Prikazuje mreže na koje su povezani mrežni prilagodnici. **Povezane mreže** možete pronaći u glavnom izborniku pod **Podešavanje** > **Mrežna zaštita**. Nakon što kliknete link ispod naziva mreže, od vas će se zatražiti da odaberete vrstu zaštite za povezanu mrežu.

Postoje dva načina mrežne zaštite koja možete odabrati u prozoru za konfiguriranje mrežne zaštite:

- **Da** – za pouzdanu mrežu (kućnu ili uredsku mrežu). Vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi su drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži. Preporučujemo upotrebu ove postavke prilikom pristupa sigurnoj lokalnoj mreži.

- **Ne** – za nepouzdanu mrežu (javnu mrežu). Datoteke i mape u vašem sustavu ne dijele se s drugim korisnicima na mreži niti su im vidljive i deaktivirano je dijeljenje resursa sustava. Preporučujemo upotrebu ove postavke prilikom pristupa bežičnim mrežama.

Kliknite ikonu zupčanika pokraj mreže da biste odabrali jednu od sljedećih opcija (za nepouzdane mreže dostupna je samo opcija **Uredi mrežu**):

- **Uredi mrežu** – otvara Uređivač mreže.

- **Skeniranje mreže pomoću Mrežne provjere** – otvara Mrežnu provjeru za pokretanje skeniranja mreže.

- **Označi kao "Moja mreža"** – dodaje oznaku Moja mreža na mrežu. Ova oznaka će se prikazivati pored mreže u cijelom programu ESET Internet Security radi bolje identifikacije i sigurnosti.

- **Poništi označavanje kao "Moja mreža"** – uklanja oznaku Moja mreža. Dostupno samo ako je mreža već označena.

Za prikaz pojedinog mrežnog adaptera i njemu dodijeljenog profila firewalla i pouzdane zone kliknite **Mrežni**

adapteri. Detaljne informacije potražite u odjeljku Mrežni adapteri.

Mrežni adapteri

U prozoru mrežnih adaptera prikazuju se sljedeće informacije o mrežnim adapterima:

- Naziv mrežnog adaptera i vrsta veze (žičana, virtualna itd.)
- IP adresa s MAC adresom
- Povezana mreža (prikazuje oznaku Moja mreža)
- IP adresa pouzdane zone s podmrežom
- Aktivni profil (pogledajte stavku Profili dodijeljeni mrežnim adapterima)

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 Internet Security 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).

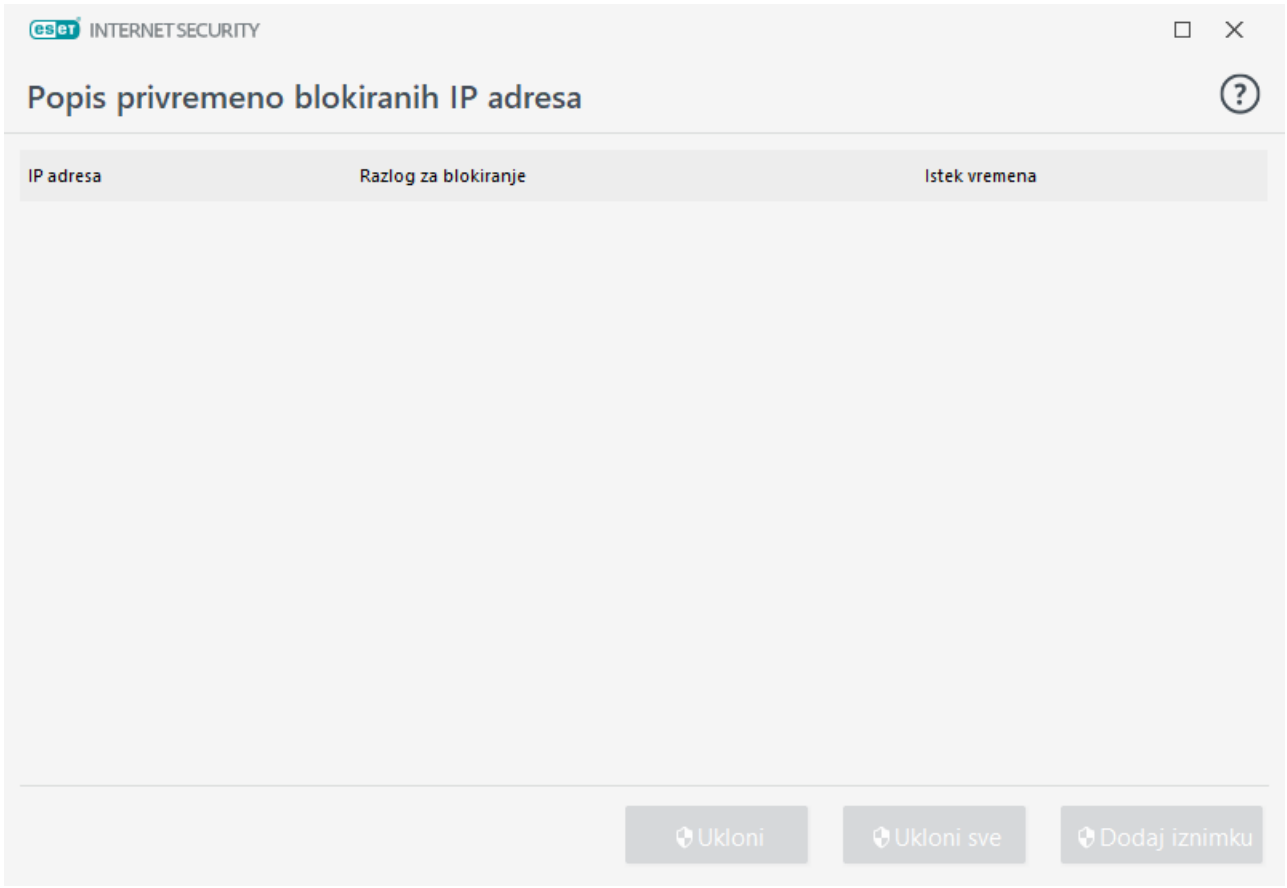
Istek vremena – Prikazuje vrijeme i datum do kada će adresa biti na popisu blokiranih adresa.

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.



Dnevnik mrežne zaštite

Mrežna zaštita programa ESET Internet Security sprema sve važne događaje u dnevnik koji je moguće prikazati izravno iz glavnog izbornika. Kliknite **Alati** > **Više alata** > **Dnevnici**, a zatim odaberite **Mrežna zaštita** iz padajućeg izbornika **Dnevnik**.

Dnevnici se mogu upotrijebiti za otkrivanje pogrešaka i provala u sustav. ESET-ovi dnevnici mrežne zaštite sadrže sljedeće podatke:

- Datum i vrijeme događaja
- Naziv događaja
- Izvor
- Ciljna mrežna adresa
- Protokol mrežne komunikacije
- Primijenjeno pravilo ili naziv crva, ako je otkriven
- Aplikacija koja je sudjelovala u događaju
- Korisnik

Podrobna analiza tih podataka može pridonijeti otkrivanju pokušaja ugrožavanja sigurnosti sustava. Mnogi drugi čimbenici ukazuju na moguće sigurnosne rizike i omogućuju korisniku minimiziranje njihova učinka: prečeste veze s nepoznatim mjestima, višestruki pokušaji uspostave veza, komunikacija nepoznatih aplikacija i korištenje

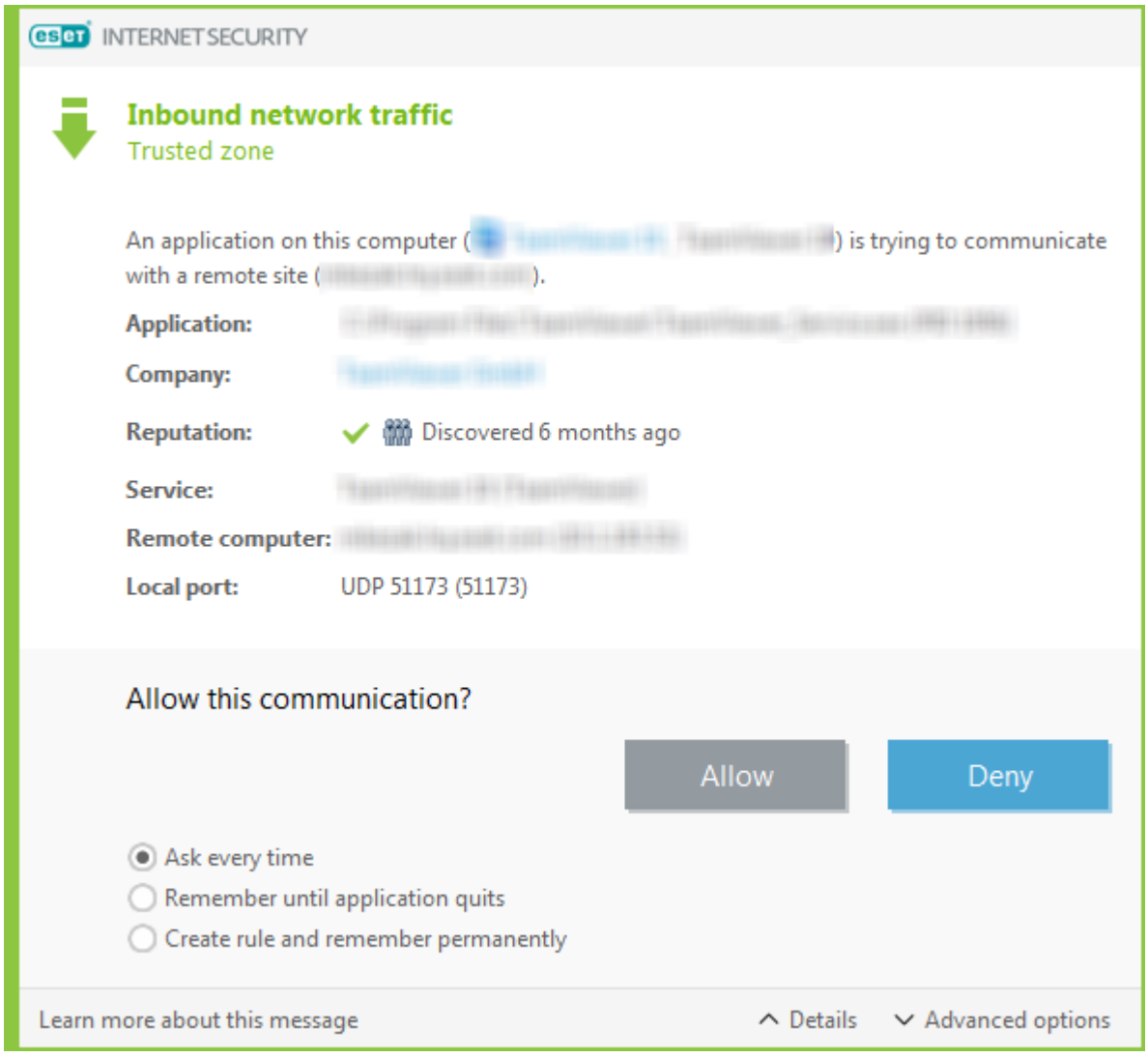
neobičnih brojeva portova.

> **Iskorištavanje sigurnosnog propusta**
> Poruka o iskorištavanju sigurnosnog propusta zapisuje se u dnevnik čak i ako je određena ranjivost već zakrpana jer je pokušaj iskorištavanja otkriven i blokiran na razini mreže prije nego što može doći do stvarnog iskorištavanja.

Uspostava veze – otkrivanje

Firewall otkriva sve novostvorene mrežne veze. Aktivnim su načinom rada firewalla određene radnje koje se provode za novo pravilo. Ako je aktiviran **Automatski način** ili **Način na temelju pravila**, firewall će izvršiti prethodno definirane radnje bez korisničke interakcije.

U **interaktivnom načinu rada** prikazuje informativni prozor u kojem se izvješćuje o otkrivanju nove mrežne veze i navode detaljne informacije o njoj. Odabrati možete **Dopusti** ili **Odbij** (blokiraj) vezu. Ako korisnik opetovano dopušta istu vezu u tom dijaloškom prozoru, preporučujemo mu da za nju stvori novo pravilo. Odaberite opciju **Stvori pravilo i trajno ga zapamti** i spremite tu radnju kao novo pravilo firewalla. Ako firewall nakon toga prepozna istu vezu, primijenit će postojeće pravilo bez potrebe za intervencijom korisnika.



Tijekom stvaranja novih pravila budite oprezni i dopustite samo veze koje su sigurne. Ako su sve veze dopuštene, firewall ne može ostvariti svoju svrhu. Evo važnih parametara veza:

Aplikacija – mjesto izvršne datoteke i ID-ja procesa. Nemojte dopustiti veze za nepoznate aplikacije i procese.

Tvrtka – naziv izdavača aplikacije. Kliknite tekst da bi se prikazao sigurnosni certifikat za tvrtku.

Reputacija – razina rizika veze. Vezama je dodijeljena razina rizika: U redu (zeleno), Nepoznato (narančasto) ili Rizično (crveno), pomoću niza heurističkih pravila koja ispituju karakteristike svake veze, broj korisnika i vrijeme otkrivanja. Te podatke prikuplja tehnologija ESET LiveGrid®.

Usluga – naziv usluge ako je aplikacija usluga sustava Windows.

Udaljeno računalo – adresa udaljenog uređaja. Dopustite samo veze s pouzdanim i poznatim adresama.

Udaljeni port – komunikacijski port. Komunikacija putem uobičajenih portova (na primjer, web promet – broj porta 80.443) može pod normalnim okolnostima biti dopuštena.

Računalne infiltracije često se šire putem skrivenih i internetskih veza, što im pomaže da zaraze udaljene sustave. Ako se pravila ispravno konfiguriraju, firewall postaje koristan alat za zaštitu od mnogih napada zlonamjernog koda.

Rješavanje problema s ESET firewallom

Ako doživite probleme s povezivanjem s instaliranim programom ESET Internet Security, postoji nekoliko načina za otkrivanje uzrokuje li ESET Firewall problem. Nadalje, ESET firewall može vam pomoći u stvaranju novih pravila ili izuzetaka za rješavanje problema u povezivanju.

Pogledajte sljedeće teme za pomoć u rješavanju problema s ESET firewallom:

- Čarobnjak za otklanjanje poteškoća
- Zapisivanje i stvaranje pravila ili izuzetaka iz dnevnika
- Stvaranje izuzetaka od obavijesti firewalla
- Napredno vođenje dnevnika Mrežne zaštite
- Rješavanje problema s filtriranjem protokola

Čarobnjak za otklanjanje poteškoća

Čarobnjak za otklanjanje poteškoća neprimjetno nadzire sve blokirane veze i vodi vas kroz proces otklanjanja poteškoća kako bi se otklonili problemi s firewallom za određene aplikacije ili uređaje. Sljedeće, čarobnjak će predložiti novi niz pravila koja se mogu primijeniti ako ih odobrite. **Čarobnjak za otklanjanje poteškoća** može se pronaći u glavnom izborniku pod stavkom **Podešavanje** > **Mrežna zaštita**.

Zapisivanje i stvaranje pravila ili izuzetaka iz dnevnika

Prema standardnim postavkama ESET Firewall ne zapisuje sve blokirane veze u dnevnik. Ako želite vidjeti što je blokirala Mrežna zaštita, omogućite vođenje dnevnika u odjeljku **Napredno podešavanje**, pod stavkom **Alati** > **Dijagnostika** > **Napredno vođenje dnevnika** > **Aktiviraj napredno vođenje dnevnika mrežne zaštite**. Ako u

dnevniku vidite nešto što ne želite da firewall blokira, možete stvoriti pravilo ili IDS pravilo desnim klikom te stavke i odabirom opcije **Ubuduće ne blokiraj slične događaje**. Imajte na umu da dnevnik svih blokiranih veza može sadržavati tisuće stavki te može biti teško pronaći određenu vezu u tom dnevniku. Vođenje dnevnika možete isključiti nakon što otklonite problem.

Dodatne informacije o dnevniku potražite u stavci Dnevnici.

Upotrijebite vođenje dnevnika da biste vidjeli redoslijed u kojem je Mrežna zaštita blokirao određene veze. Nadalje, stvaranje pravila iz dnevnika omogućuje stvaranje pravila koja čine upravo ono što želite.

Stvori pravilo iz dnevnika

Nova verzija programa ESET Internet Security omogućuje vam stvaranje pravila iz dnevnika. U glavnom izborniku kliknite **Alati** > **Više alata** > **Dnevnici**. Odaberite **Firewall** iz padajućeg izbornika, kliknite željeni unos u dnevniku desnom tipkom i odaberite **Nemoj blokirati slične događaje u budućnosti** iz kontekstnog izbornika. Prozor s obavijestima prikazat će vaše novo pravilo.

Kako biste omogućili stvaranje novih pravila iz dnevnika, ESET Internet Security mora biti konfiguriran prema sljedećim postavkama:

1. Postavite minimalnu opširnost zapisivanja na **Dijagnostičko** u **Naprednom podešavanju** (F5) > **Alati** > **Dnevnici**.

2. Aktivirajte opciju **"Prikaži obavijesti i za nadolazeće napade na sigurnosne propuste"** u odjeljku **"Napredno podešavanje"** (F5) > **"Mrežna zaštita"** > **"Zaštita od mrežnog napada"** > **"Napredne opcije"** > **"Otkrivanje upada"**.

Stvaranje izuzetaka od obavijesti firewalla

Kada ESET Firewall otkrije zloćudnu mrežnu aktivnost, pojavit će se prozor s obavijesti koji opisuje događaj. Ova obavijest sadrži poveznicu koja će vam omogućiti da naučite više o događaju i ako želite, postavite pravilo za ovaj događaj.

Ako mrežna aplikacija ili uređaj ne primjenjuje ispravno mrežne standarde, može uzrokovati višestruke IDS obavijesti firewalla. Izuzetak možete stvoriti izravno iz obavijesti kako ESET firewall ne bi otkrivao tu aplikaciju ili uređaj.

Napredno vođenje dnevnika Mrežne zaštite

Ova funkcija namijenjena je za pružanje složenijih dnevnika za ESET-ovu tehničku podršku. Upotrebljavajte ovu funkciju samo kada od vas to zatraži ESET-ova tehnička podrška jer bi se mogao stvoriti velik dnevnik i usporiti rad vašeg računala.

1. Idite na **Napredno podešavanje** > **Alati** > **Dijagnostika** i aktivirajte **Aktiviraj napredno vođenje dnevnika mrežne zaštite**.

2. Pokušajte ponoviti problem koji ste imali.

3. Deaktivirajte napredno vođenje dnevnika mrežne zaštite.

4. Dnevnik PCAP zapisivanja koji je izrađen u okviru naprednog vođenja dnevnika mrežne zaštite može se pronaći u istoj mapi gdje se stvaraju dijagnostičke slike stanja memorije: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Rješavanje problema s filtriranjem protokola

Ako imate probleme s preglednikom ili klijentom e-pošte, prvi korak je provjeriti je li odgovorno filtriranje protokola. Da biste to učinili, pokušajte privremeno deaktivirati filtriranje protokola u naprednom podešavanju (ne zaboravite ponovno uključiti kada završite, inače će vaš preglednik i klijent e-pošte ostati nezaštićeni). Ako vaš problem nestane nakon isključivanja, ovdje je popis najčešćih problema i kako ih otkloniti:

Problemi s aktualizacijom ili sigurnosnom komunikacijom

Ako vaša aplikacija prigovara o nemogućnosti nadogradnja ili nezaštićenosti komunikacijskog kanala:

- Ako imate aktivirano filtriranje SSL protokola, pokušajte ga privremeno isključiti. Ako to pomaže, možete nastaviti koristiti SSL filtriranje i obaviti aktualizaciju izuzimanjem problematične komunikacije:
  Prebacite filtriranje SSL protokola na interaktivni način rada. Ponovno pokrenite aktualizaciju. Trebao bi se pojaviti dijaloški okvir koji vas informira o šifriranom mrežnom prometu. Provjerite odgovara li aplikacija onoj kojoj pokušavate otkloniti poteškoće i izgleda li certifikat kao da dolazi sa servera na kojem se izvršava aktualizacija. Zatim odaberite da se pamti akcija za ovaj certifikat i kliknite ignoriraj. Ako se ne prikazuje više važnih dijaloških okvira, možete prebaciti način filtriranja natrag na automatski i problem bi trebao biti otklonjen.

- Ako dotična aplikacija nije preglednik ili klijent e-pošte, možete ju potpuno izuzeti iz filtriranja protokola (da učinite ovako što za preglednik ili klijent e-pošte, bili biste izloženi riziku). Sve aplikacije čija se komunikacija filtrirala u prošlosti trebale bi već biti ponuđene u popisu kada dodajete izuzetke, tako da ručno dodavanje ne bi trebalo biti potrebno.

Problem u pristupanju uređaju na vašoj mreži

Ako ne možete koristiti uređaj na mreži (ovo može biti web stranica ili reprodukcija videozapisa na multimedijskom reproduktoru), pokušajte dodati njegove IPv4 i IPv6 adrese na popis izuzetih adresa.

Problemi s određenom web stranicom

Možete izuzeti određene web stranice iz filtriranja protokola korištenjem upravljanja URL adresa. Primjerice, ako ne možete pristupiti https://www.gmail.com/intl/en/mail/help/about.html, pokušajte dodati *gmail.com* na popis izuzetih adresa.

Pogreška „Još uvijek rade neke aplikacije koje mogu uvesti root certifikat”

Kad omogućite filtriranje SSL protokola, ESET Internet Security provjerava vjeruju li instalirane aplikacije načinu kako se filtrira SSL protokol uvezivanjem certifikata u njihovu pohranu certifikata. Za neke aplikacije ovo nije moguće dok se one izvršavaju. To uključuje aplikacije Firefox i Opera. Provjerite jesu li sve isključene (najbolji je način da otvorite upravitelj zadataka i provjerite da na kartici procesa ne postoje aktivni procesi firefox.exe ili opera.exe), a zatim pokušajte ponovno.

Pogreška o nepouzdanom izdavaču ili neispravnom potpisu

Ovo vjerojatno znači da je gore opisani uvoz bio neuspješan. Prvo provjerite da gore navedene aplikacije nisu aktivne. Zatim deaktivirajte filtriranje SSL protokola i ponovno aktivirajte. To će ponovno pokrenuti uvoz.

Informacije o tome kako upravljati filtriranjem protokola SSL/TLS u ESET-ovim Windows programima za kućnu upotrebu potražite u članku iz baze znanja.

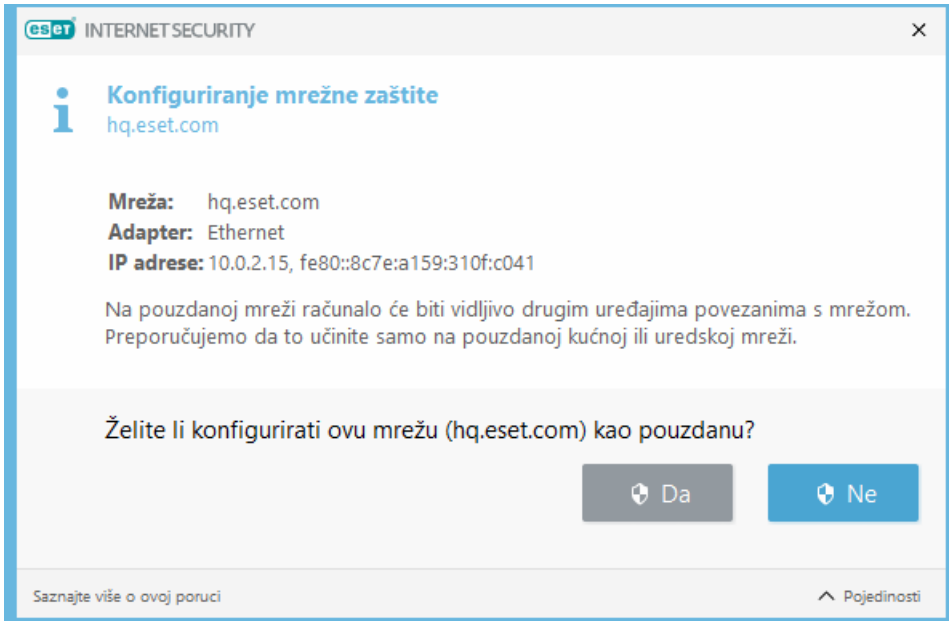
Otkrivena je nova mreža

Kad se otkrije mreža, ESET Internet Security standardno upotrebljava postavke Windowsa. Da bi se prikazao prozor kad se otkrije nova mreža, promijenite vrstu zaštite novih mreža u "Pitaj korisnika" u odjeljku Poznate mreže. Ako se zatim otkrije veza s novom mrežom, korisnik može odabrati razinu zaštite. Ta se postavka primjenjuje na sva udaljena računala iz određene mreže.

Postoje dva načina mrežne zaštite koja možete odabrati u prozoru za konfiguriranje mrežne zaštite:

- **Da** – za pouzdanu mrežu (kućnu ili uredsku mrežu). Vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi su drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži. Preporučujemo upotrebu ove postavke prilikom pristupa sigurnoj lokalnoj mreži.

- **Ne** – za nepouzdanu mrežu (javnu mrežu). Datoteke i mape u vašem sustavu ne dijele se s drugim korisnicima na mreži niti su im vidljive i deaktivirano je dijeljenje resursa sustava. Preporučujemo upotrebu ove postavke prilikom pristupa bežičnim mrežama.



Ako je mreža postavljena kao pouzdana, izravno povezane podmreže se automatski smatraju pouzdanima.

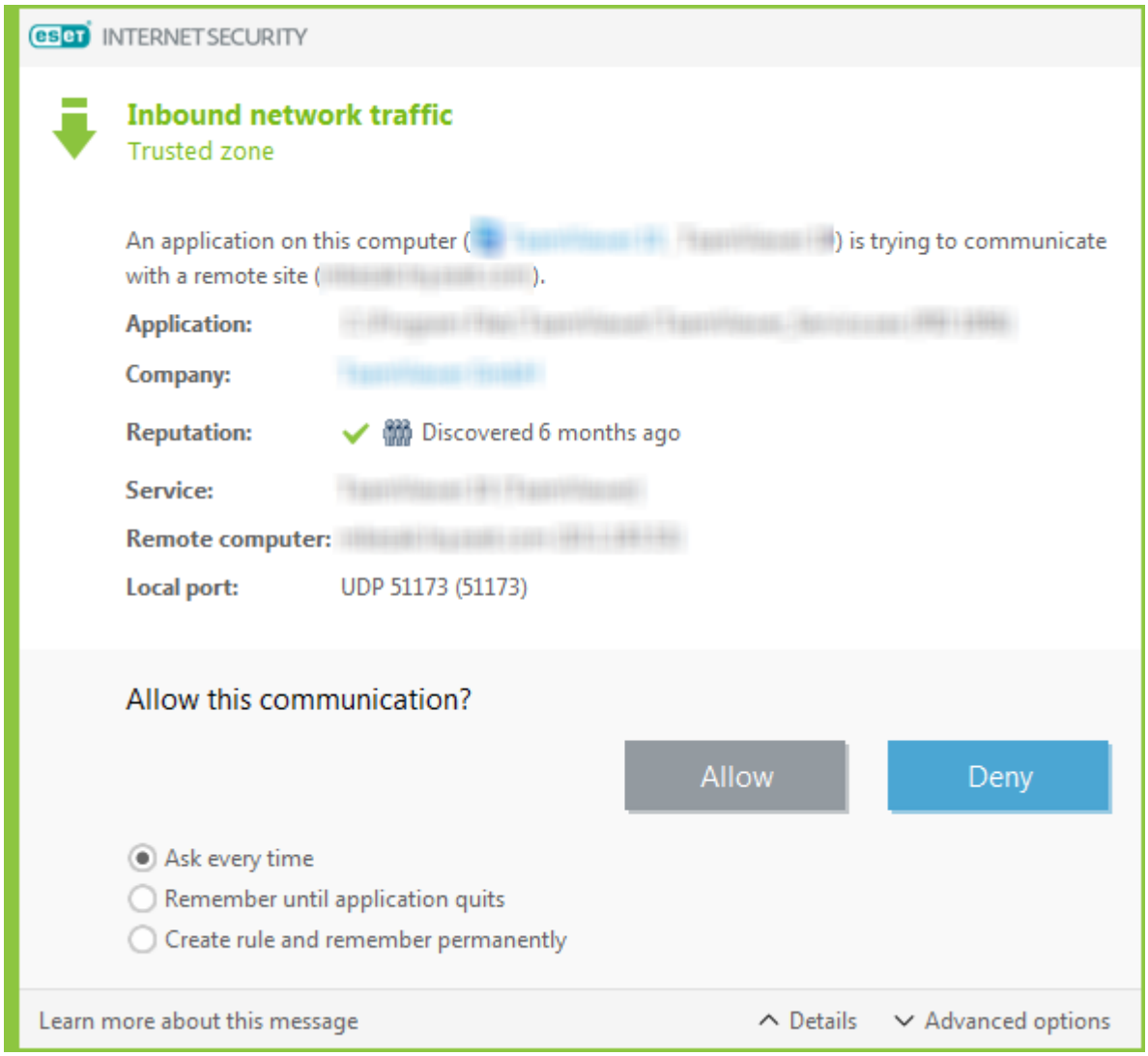
Promjena aplikacije

Firewall je u aplikaciji otkrio preinaku koja se koristi za uspostavljanje odlaznih veza s vašeg računala. Možda je aplikacija jednostavno nadograđena na novu verziju. No postoji i mogućnost da je preinaku izvršila zlonamjerna aplikacija. Ako niste sigurni da se radi o legitimnoj preinaci, preporučujemo da zabranite vezu i skenirate računalo

uz upotrebu najnovije baze podataka virusnih potpisa.

Dolazna pouzdana komunikacija

Primjer dolazne internetske veze u pouzdanoj zoni:
Udaljeno računalo iz pouzdane zone pokušava uspostaviti komunikaciju s lokalnom aplikacijom na vašem računalu.



Aplikacija – Aplikacija s kojom udaljeno računalo stupa u vezu.

Tvrtka – Izdavač aplikacije.

Reputacija – Reputacija koju je aplikacija dobila pomoću tehnologije ESET LiveGrid®.

Usluga – Naziv usluge koja se trenutačno koristi na vašem računalu.

Udaljeno računalo – Identifikacijski podaci udaljenog računala koje pokušava uspostaviti komunikaciju s aplikacijom na vašem računalu.

Lokalni port – Port koji se koristi za komunikaciju.

Pitaj svaki put – Ako je standardna radnja pravila postavljena na **Pitaj**, prilikom svakog pokretanja tog pravila

prikazuje se prozor.

Zapamti do zatvaranja aplikacije – ESET Internet Security zapamtit će odabranu radnju do sljedećeg ponovnog pokretanja.

Stvori pravilo i trajno ga zapamti – Ako odaberete tu opciju prije no što dopustite ili zabranite komunikaciju, ESET Internet Security zapamtit će radnju i koristiti je ako udaljeno računalo ponovno pokuša uspostaviti vezu s aplikacijom.

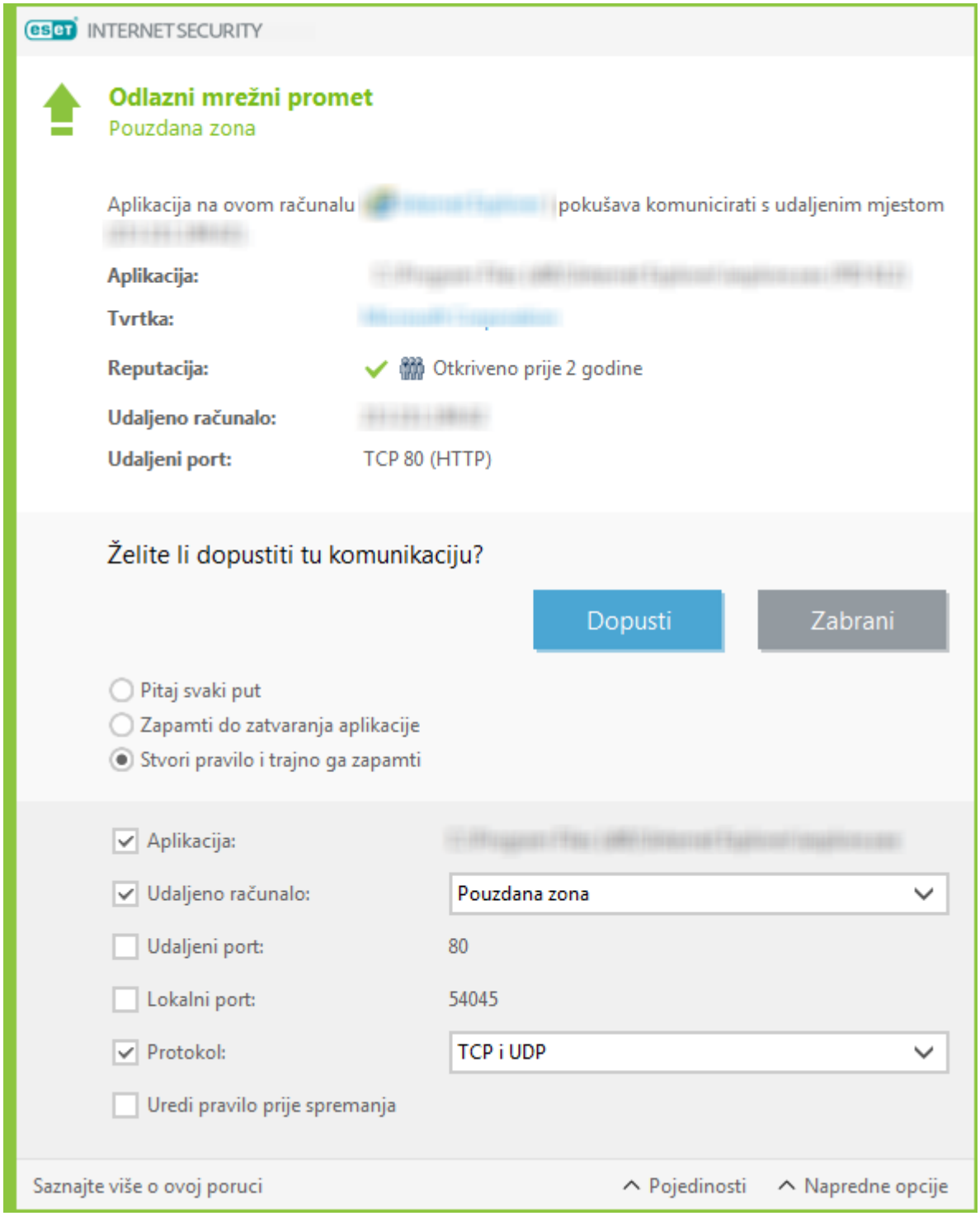
Dopusti – Dopušta dolaznu komunikaciju.

Zabrani – Zabranjuje dolaznu komunikaciju.

Napredne opcije – Omogućuje vam prilagodbu svojstava pravila.

Odlazna pouzdana komunikacija

Primjer odlazne internetske veze u pouzdanoj zoni:
Lokalna aplikacija pokušava uspostaviti vezu s nekim drugim računalom u lokalnoj mreži ili u mrežama u pouzdanoj zoni.



Aplikacija – Aplikacija s kojom udaljeno računalo stupa u vezu.

Tvrtka – Izdavač aplikacije.

Reputacija – Reputacija koju je aplikacija dobila pomoću tehnologije ESET LiveGrid®.

Usluga – Naziv usluge koja se trenutačno koristi na vašem računalu.

Udaljeno računalo – Identifikacijski podaci udaljenog računala koje pokušava uspostaviti komunikaciju s aplikacijom na vašem računalu.

Lokalni port – Port koji se koristi za komunikaciju.

Pitaj svaki put – Ako je standardna radnja pravila postavljena na **Pitaj**, prilikom svakog pokretanja tog pravila prikazuje se prozor.

Zapamti do zatvaranja aplikacije – ESET Internet Security zapamtit će odabranu radnju do sljedećeg ponovnog pokretanja.

Stvori pravilo i trajno ga zapamti – Ako odaberete tu opciju prije no što dopustite ili zabranite komunikaciju, ESET Internet Security zapamtit će radnju i koristiti je ako udaljeno računalo ponovno pokuša uspostaviti vezu s aplikacijom.

Dopusti – Dopušta dolaznu komunikaciju.

Zabrani – Zabranjuje dolaznu komunikaciju.

Napredne opcije – Omogućuje vam prilagodbu svojstava pravila.

Dolazna komunikacija

Primjer dolazne internetske veze:
Udaljeno računalo pokušava komunicirati s aplikacijom na vašem računalu.

Aplikacija – Aplikacija s kojom udaljeno računalo stupa u vezu.

Tvrtka – Izdavač aplikacije.

Reputacija – Reputacija koju je aplikacija dobila pomoću tehnologije ESET LiveGrid®.

Usluga – Naziv usluge koja se trenutačno koristi na vašem računalu.

Udaljeno računalo – Identifikacijski podaci udaljenog računala koje pokušava uspostaviti komunikaciju s aplikacijom na vašem računalu.

Lokalni port – Port koji se koristi za komunikaciju.

Pitaj svaki put – Ako je standardna radnja pravila postavljena na **Pitaj**, prilikom svakog pokretanja tog pravila prikazuje se prozor.

Zapamti do zatvaranja aplikacije – ESET Internet Security zapamtit će odabranu radnju do sljedećeg ponovnog pokretanja.

Stvori pravilo i trajno ga zapamti – Ako odaberete tu opciju prije no što dopustite ili zabranite komunikaciju, ESET Internet Security zapamtit će radnju i koristiti je ako udaljeno računalo ponovno pokuša uspostaviti vezu s aplikacijom.

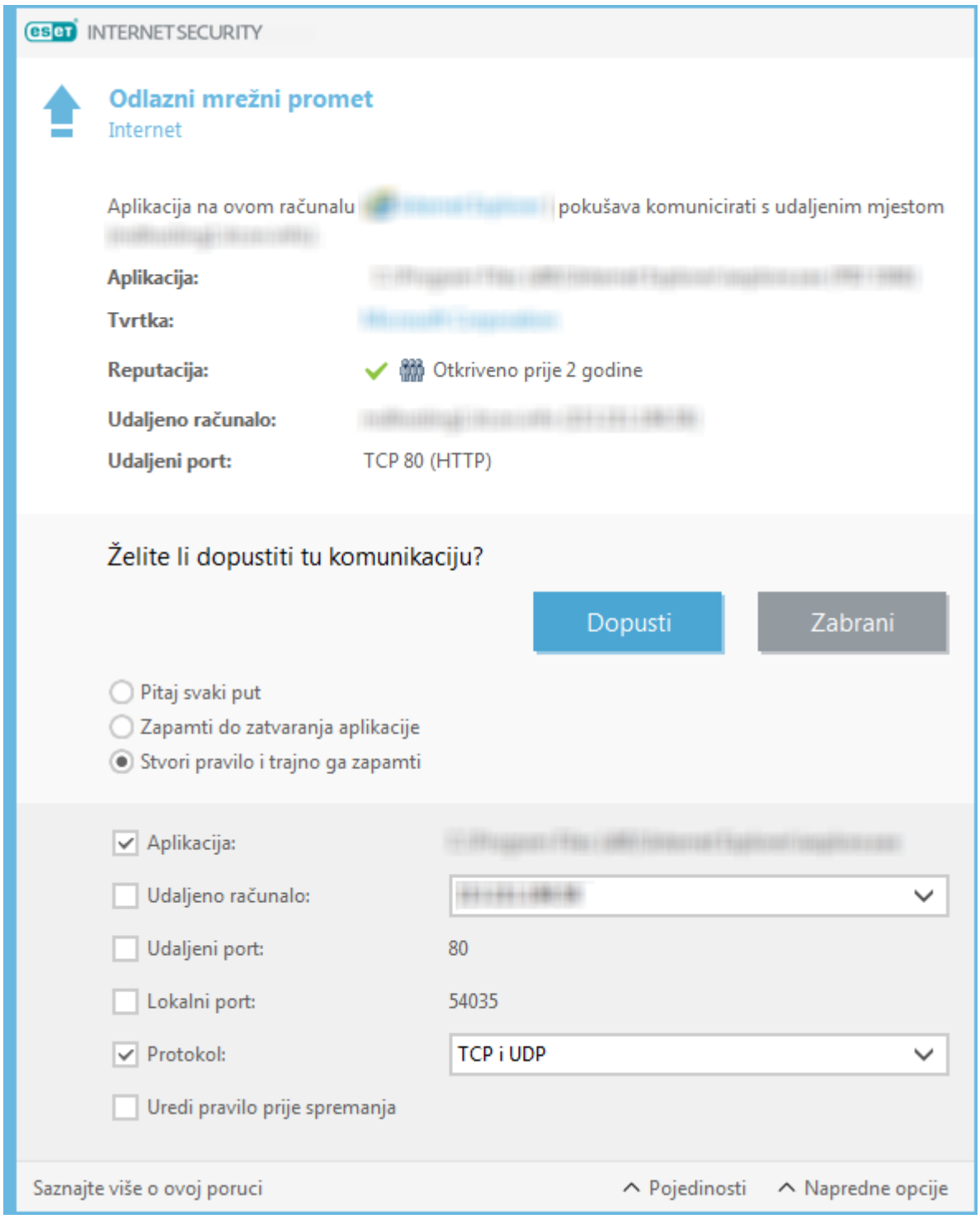
Dopusti – Dopušta dolaznu komunikaciju.

Zabrani – Zabranjuje dolaznu komunikaciju.

Napredne opcije – Omogućuje vam prilagodbu svojstava pravila.

Odlazna komunikacija

Primjer odlazne internetske veze:
Lokalna aplikacija pokušava uspostaviti vezu s internetom.



Aplikacija – Aplikacija s kojom udaljeno računalo stupa u vezu.

Tvrtka – Izdavač aplikacije.

Reputacija – Reputacija koju je aplikacija dobila pomoću tehnologije ESET LiveGrid®.

Usluga – Naziv usluge koja se trenutačno koristi na vašem računalu.

Udaljeno računalo – Identifikacijski podaci udaljenog računala koje pokušava uspostaviti komunikaciju s aplikacijom na vašem računalu.

Lokalni port – Port koji se koristi za komunikaciju.

Pitaj svaki put – Ako je standardna radnja pravila postavljena na **Pitaj**, prilikom svakog pokretanja tog pravila prikazuje se prozor.

Zapamti do zatvaranja aplikacije – ESET Internet Security zapamtit će odabranu radnju do sljedećeg ponovnog pokretanja.

Stvori pravilo i trajno ga zapamti – Ako odaberete tu opciju prije no što dopustite ili zabranite komunikaciju, ESET Internet Security zapamtit će radnju i koristiti je ako udaljeno računalo ponovno pokuša uspostaviti vezu s aplikacijom.

Dopusti – Dopušta dolaznu komunikaciju.

Zabrani – Zabranjuje dolaznu komunikaciju.

Napredne opcije – Omogućuje vam prilagodbu svojstava pravila.

Podešavanje pregleda veza

Kliknite vezu desnom tipkom miša da biste vidjeli dodatne mogućnosti koje obuhvaćaju:

Razriješi nazive hostova – Ako je moguće, sve mrežne adrese prikazuju se u DNS obliku, a ne u brojčanom obliku IP adresa.

Prikaži samo veze putem TCP protokola – Na popisu se prikazuju samo veze koje pripadaju TCP protokolu.

Prikaži veze koje se osluškuju – Odaberite ovu opciju da biste prikazali samo veze u kojima komunikacija trenutno nije uspostavljena, ali je sustav otvorio port i čeka vezu.

Prikaži veze unutar računala – Odaberite ovu opciju da biste prikazali samo one veze gdje je udaljena strana lokalni sustav – takozvane localhost veze.

Brzina osvježavanja – Odaberite učestalost osvježavanja aktivnih veza.

Osvježi sada – ponovno učitava prozor **Mrežne veze**.

Sigurnosni alati

Podešavanje **Sigurnosnih alata** omogućuje vam prilagođavanje sljedećih modula:

- **Zaštita bankarstva i plaćanja** – pruža dodatan sloj zaštite preglednika koji je osmišljen za zaštitu financijskih podataka tijekom online transakcija. Aktivirajte opciju **Zaštiti sve preglednike** da biste pokrenuli sve podržane web preglednike u sigurnom načinu rada. Više informacija potražite u odjeljku Zaštita bankarstva i plaćanja.

- **Roditeljska kontrola** – modul roditeljske kontrole štiti vašu djecu tako što blokira neprimjeren ili štetan

sadržaj na internetu.

- **Anti-Theft** – aktivirajte Anti-Theft da biste zaštitili računala u slučaju gubitka ili krađe.

Zaštita bankarstva i plaćanja

Zaštita bankarstva i plaćanja dodatni je sloj zaštite osmišljen za zaštitu financijskih podataka tijekom mrežnih transakcija.

U većini slučajeva zaštićeni preglednik Zaštite bankarstva i plaćanja pokreće se u pregledniku koji se trenutačno upotrebljava nakon što posjetite poznatu web stranicu za bankarstvo.

Odaberite jednu od sljedećih opcija konfiguracije ponašanja zaštićenog preglednika:

- **Zaštiti sve preglednike** – ako se ova opcija aktivira, svi podržani web preglednici se pokreću u sigurnom načinu rada. To vam omogućuje pregledavanje interneta, pristup internetskom bankarstvu te kupnju i izvršavanje transakcija na internetu u jednom prozoru zaštićenog preglednika, bez preusmjeravanja.

- **Preusmjeravanje web stranica** (standardno) – web stranice s popisa zaštićenih web stranica i internog popisa internetskog bankarstva se preusmjeravaju u zaštićeni preglednik. Možete odabrati koji se preglednik otvara (standardni ili zaštićeni).

- Obje prethodne opcije su deaktivirane – da biste pristupili zaštićenom pregledniku u programu ESET Internet Security, kliknite **Alati** > **Zaštita bankarstva i plaćanja** ili kliknite ikonu **Zaštita bankarstva i plaćanja** na radnoj površini. Preglednik koji je postavljen kao standardni u sustavu Windows pokreće se u sigurnom načinu rada.

Da biste konfigurirali ponašanje zaštićenog preglednika, pogledajte Napredno podešavanje zaštite bankarstva i plaćanja. Da biste aktivirali funkciju Zaštiti sve preglednike u programu ESET Internet Security, kliknite **Podešavanje** > **Sigurnosni alati** i aktivirajte traku klizača opcije **Zaštiti sve preglednike**.

Za sigurno pregledavanje weba nužna je upotreba šifrirane HTTPS komunikacije. Sljedeći preglednici podržavaju zaštitu bankarstva i plaćanja:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Više informacija o funkcijama zaštite bankarstva i plaćanja pročitajte u sljedećim člancima ESET-ove baze znanja dostupnima na engleskom i više drugih jezika:

- Kako koristiti ESET-ovu zaštitu bankovnih plaćanja?
- Aktiviranje ili deaktiviranje ESET-ove Zaštite bankarstva i plaćanja za određenu web-stranicu
- Pauziranje ili deaktivacija Zaštite bankarstva i plaćanja u ESET-ovim Windows programima za kućne korisnike

- ESET-ova Zaštita bankarstva i plaćanja – uobičajene pogreške
- ESET-ov rječnik | Zaštita bankarstva i plaćanja

Napredno podešavanje zaštite bankarstva i plaćanja

Ovo je podešavanje dostupno u odjeljku **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita bankarstva i plaćanja**.

Osnovno

Aktiviraj zaštitu bankarstva i plaćanja – čim se aktivira zaštita bankarstva i plaćanja, aktivira se i popis zaštićenih web stranica, omogućujući vam uređivanje popisa Zaštićene web stranice.

Zaštita preglednika

Osigurajte sve preglednike – omogućite ovu opciju za pokretanje svih podržanih web preglednika u sigurnom načinu rada.

Način rada za instalaciju proširenja – iz padajućeg izbornika možete odabrati koja proširenja će biti dopuštena za instalaciju u preglednik zaštićen ESET-om: Promjena načina rada za instalaciju proširenja ne utječe na prethodno instalirana proširenja preglednika:

- **Osnovna proširenja** – samo najvažnija proširenja koja je razvio određeni proizvođač preglednika.
- **Sva proširenja** – sva proširenja koja podržava određeni preglednik.

Preusmjeravanje web stranica

Aktiviraj preusmjeravanje zaštićenih web stranica – Ako je opcija aktivirana, web stranice s popisa zaštićenih web stranica i interni popis internetskog bankarstva preusmjerit će se na zaštićeni preglednik.

Zaštićene web stranice – popis web stranica za koje možete odabrati koji preglednik će se otvarati (uobičajeni ili zaštićeni). U okviru preglednika prikazat će se logotip ESET, što je znak da je sigurno pregledavanje aktivno. Za uređivanje popisa pogledajte zaštićene web stranice.

Zaštićeni preglednik

Aktiviraj poboljšanu zaštitu memorije – Ako je opcija aktivirana, memorija zaštićenog preglednika bit će zaštićena od inspekcije putem drugih procesa.

Aktiviraj zaštitu tipkovnice – ako je opcija aktivirana, podaci koje unesete tipkovnicom u zaštićeni preglednik će biti skriveni od drugih aplikacija. Time se povećava zaštita od keyloggera.

Zeleni okvir preglednika – ako je opcija deaktivirana, informativna obavijest u pregledniku i zeleni okvir oko preglednika kratko će se prikazati tijekom pokretanja preglednika, a zatim će nestati.

Zaštićene web stranice

ESET Internet Security sadrže ugrađeni popis web stranica koje će pokrenuti otvaranje zaštićenog preglednika. U odjeljku konfiguracije programa možete dodati web stranicu ili urediti popis web stranica.

Popis **zaštićenih web stranica** može se pregledati i urediti u odjeljku **Napredno podešavanje** (F5) > **Web i e-pošta** > **Zaštita bankarstva i plaćanja** > **Osnovno** > **Zaštićene web stranice** > **Uredi**. Prozor se sastoji od sljedećeg:

Stupci

Web stranica – Zaštićena web stranica.

Zaštićeni preglednik – Tijekom zaštićenog pregledavanja oko ruba vašeg preglednika prikazat će se logotip ESET.

Pitaj me – Kad je aktivirano, prozor s opcijama pretraživanja prikazat će se kad god se posjeti zaštićena web stranica. ESET Internet Security može zapamtiti vašu radnju ili možete ručno odabrati kako nastaviti.

Uobičajeni preglednik – Odaberite tu opciju za nastavak bankovne transakcije bez dodatne zaštite.

Kontrolni elementi

Dodaj – Omogućuje dodavanje web stranice popisu poznatih web stranica.

Uredi – Omogućuje uređivanje odabranih unosa.

Izbriši – Uklanja odabrane unose.

Uvoz/izvoz – omogućuje izvoz popisa zaštićenih web stranica i uvoz popisa na novi uređaj.

Obavijest u pregledniku

Zaštićeni preglednik informira vas o svojem trenutačnom statusu putem obavijesti u pregledniku i boje okvira preglednika.

Obavijesti u pregledniku prikazane su na kartici na desnoj strani.



Da biste proširili obavijest u pregledniku, kliknite ikonu ESET-a. Da biste smanjili obavijest, kliknite tekst obavijesti. Da biste odbacili obavijest, kliknite ikonu za zatvaranje.

Obavijesti u pregledniku

Vrsta obavijesti	Status
Informativna obavijest i zeleni okvir preglednika	Osigurana je maksimalna zaštita, a obavijest u pregledniku minimizirana je prema standardnim postavkama. Proširite obavijest u pregledniku za prikaz opcija konfiguracije: • **Sakrij zeleni okvir preglednika** – označite potvrdni okvir da biste sakrili zeleni okvir oko preglednika kada odbacite obavijest. Na zaslonu Napredno podešavanje zaštite bankarstva i plaćanja možete trajno deaktivirati informativnu obavijest u pregledniku i zeleni okvir oko preglednika. • **Postavke** – otvara podešavanje sigurnosnih alata.
Upozorenje i narančasti okvir preglednika	Zaštićeni preglednik zahtijeva vašu pažnju za nekritičan problem. Za više informacija o problemu ili rješenju slijedite upute u obavijesti u pregledniku.
Sigurnosno upozorenje i crveni okvir preglednika	Preglednik nije zaštićen ESET-ovom Zaštitom bankarstva i plaćanja. Ponovno pokrenite preglednik da biste osigurali da je zaštita aktivirana. Za rješavanje konflikta s datotekama koje su učitane u preglednik obratite se ESET-ovoj tehničkoj podršci tako da slijedite upute u našem članku iz Baze znanja.

Roditeljska kontrola

Modul roditeljske kontrole omogućuje konfiguriranje postavki roditeljske kontrole koja roditeljima pruža automatizirane alate pomoću kojih mogu zaštititi svoju djecu i postaviti ograničenja za korištenje uređaja i servisa. Cilj je onemogućiti djeci i tinejdžerima pristup stranicama s neprikladnim ili štetnim sadržajem.

Roditeljska kontrola omogućuje blokiranje web stranica s potencijalno uvredljivim sadržajima. Osim toga, roditelji mogu zabraniti pristup do 40 unaprijed definiranih kategorija web stranica i više od 140 podkategorija.

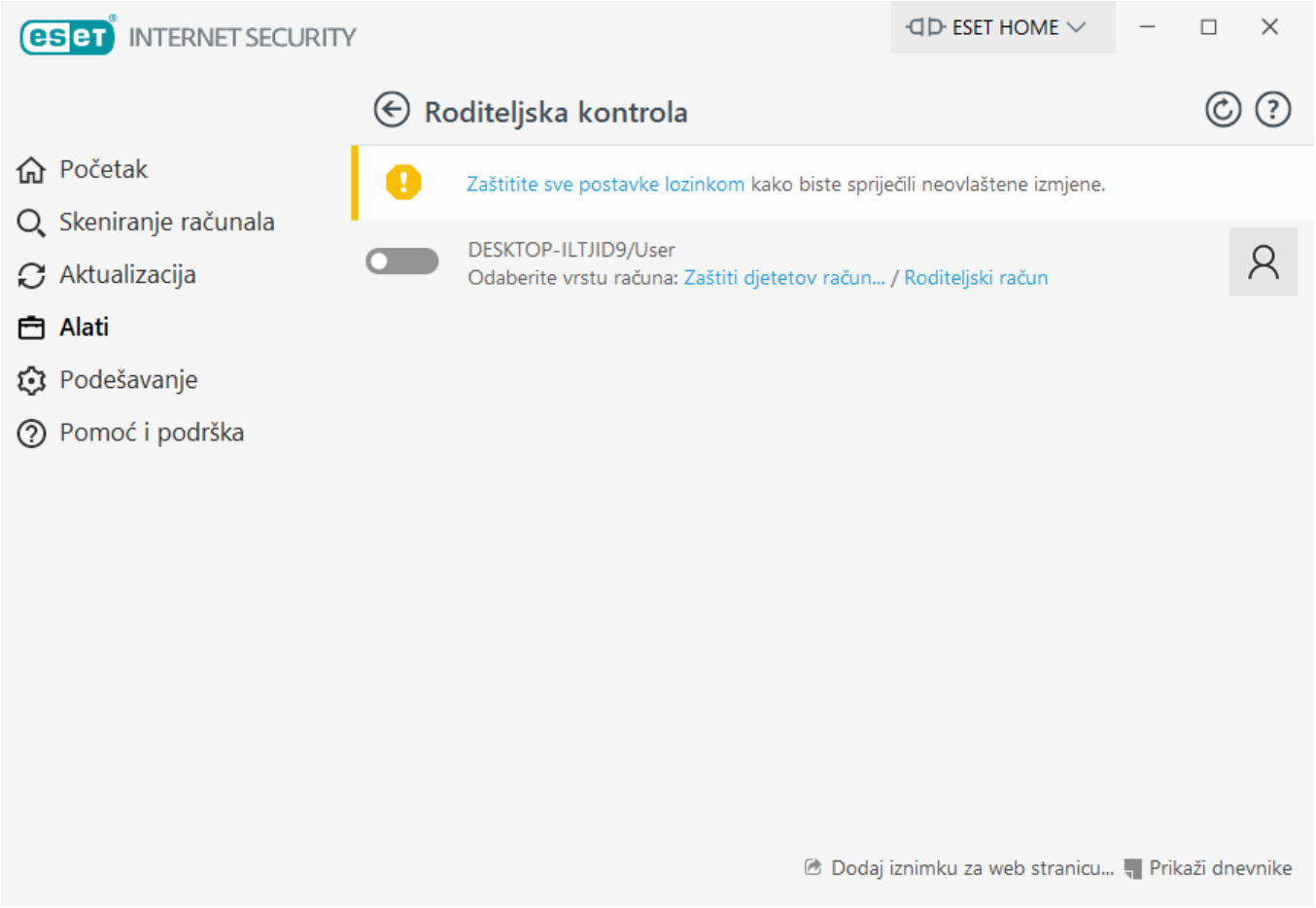
Da biste za određeni korisnički račun aktivirali roditeljsku kontrolu, pratite sljedeće korake:

1. Roditeljska je kontrola prema standardnim postavkama u programu ESET Internet Security deaktivirana. Roditeljsku kontrolu možete aktivirati na dva načina:

   • Kliknite  u oknu **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola** glavnog prozora programa i promijenite stanje roditeljske kontrole u aktivirano.

   • Pritisnite tipku F5 da biste pristupili stablu **Napredno podešavanje**, idite na **Web i e-pošta** > **Roditeljska kontrola**, a zatim aktivirajte traku klizača pokraj opcije **Aktiviraj roditeljsku kontrolu**.

2. Kliknite **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola** u glavnom prozoru programa. Premda se uz **roditeljsku kontrolu** pojavljuje stavka **Aktivno**, roditeljsku kontrolu za željeni račun morate konfigurirati tako da kliknete simbol strelice, a zatim u sljedećem prozoru odaberete **Zaštiti djetetov račun** ili **Roditeljski račun**. U sljedećem prozoru odaberite datum rođenja za određivanje razine pristupa i preporučene stranice prikladne za danu dob. Tada će za navedeni korisnički račun biti aktivirana roditeljska kontrola. Ispod naziva računa kliknite **Blokirani sadržaj i postavke** kako biste prilagodili kategorije koje želite dopustiti ili blokirati na kartici Kategorije. Da biste dopustili ili blokirali prilagođene stranice koje ne odgovaraju određenoj kategoriji, kliknite karticu Iznimke.



Ako kliknete **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola** u glavnom prozoru programa ESET Internet Security, vidjet ćete da glavni program sadrži sljedeće:

Korisnički računi sustava Windows

Ako ste stvorili ulogu za neki postojeći račun, ona će se prikazati ovdje. Kliknite klizač tako da se na njemu prikaže zelena potvrdna kvačica uz stavku roditeljske kontrole za račun. Pod aktivnim računom kliknite Blokirani sadržaj i postavke da biste prikazali popis dopuštenih kategorija stranica za ovaj račun te blokiranih i dopuštenih stranica.

Da biste stvorili novi račun (na primjer, za dijete), slijedite ove upute za sustav Windows 7 ili Windows Vista:
1.Otvorite **Korisničke račune** tako što ćete kliknuti gumb **Start** (nalazi se u donjem lijevom kutu vaše radne površine), **Upravljačka ploča** te potom i **Korisnički računi**.
2.Kliknite **Upravljanje drugim računom**. Ako dobijete zahtjev za administratorskom lozinkom ili potvrdom, upišite lozinku ili potvrdite.
3.Kliknite **Stvori novi račun**.
4.Upišite naziv koji želite dati korisničkom računu, kliknite vrstu računa, a zatim kliknite **Stvori račun**.
5.Ponovno otvorite okno Roditeljska kontrola tako da još jednom u glavnom prozoru programa ESET Internet Security kliknete na stavku **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola** i kliknete simbol strelice.

Donji dio prozora sadrži

Dodaj iznimku za web stranicu – Možete dopustiti ili blokirati određenu web stranicu za svaki roditeljski račun posebno u skladu sa svojim željama.

Prikaži dnevnik – Prikazuje detaljni dnevnik aktivnosti roditeljske kontrole (blokirane stranice, račun, razlog zbog kojega je stranica blokirana, kategoriju itd.). Taj dnevnik možete i filtrirati na temelju kriterija koje odaberete klikom na **Filtriraj**.

Roditeljska kontrola

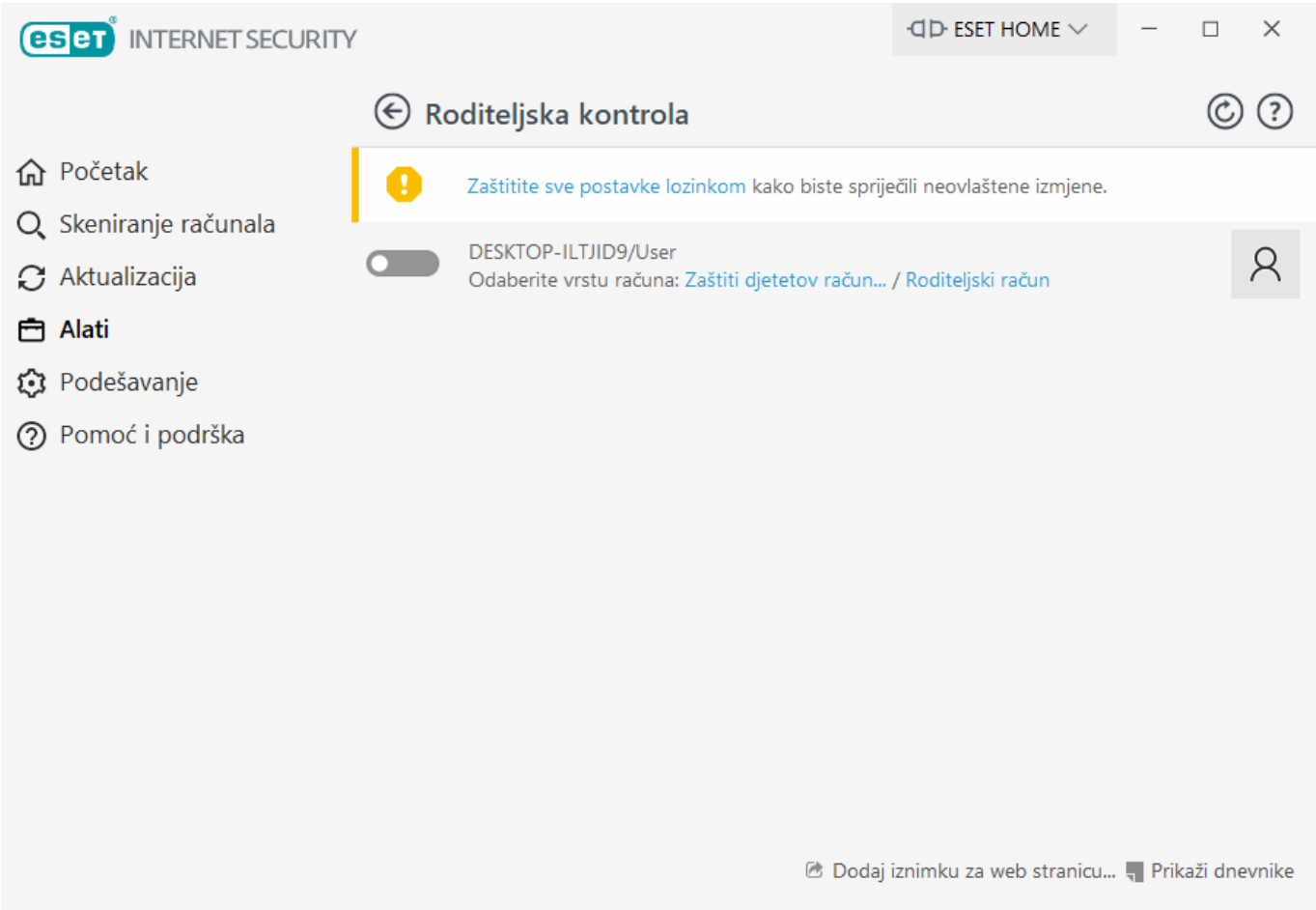
Nakon deaktiviranja roditeljske kontrole pojavit će se prozor **Deaktiviraj roditeljsku kontrolu**. Tu možete odrediti vremensko razdoblje tijekom kojega će zaštita biti deaktivirana. Mogućnost se potom mijenja u stavku **Pauzirano** ili **Trajno deaktivirano**.

Važno je postavke u programu ESET Internet Security zaštititi lozinkom. Ta lozinka može se postaviti u odjeljku Podešavanje pristupa. Ako lozinka nije postavljena, pojavit će se sljedeće upozorenje – **Zaštiti sve postavke lozinkom** kako biste spriječili neovlaštene promjene. Ograničenja postavljena u odjeljku Roditeljska kontrola utječu samo na standardne korisničke račune. Takva ograničenja nemaju nikakvog učinka jer administrator ima ovlasti za njihovo zaobilaženje.

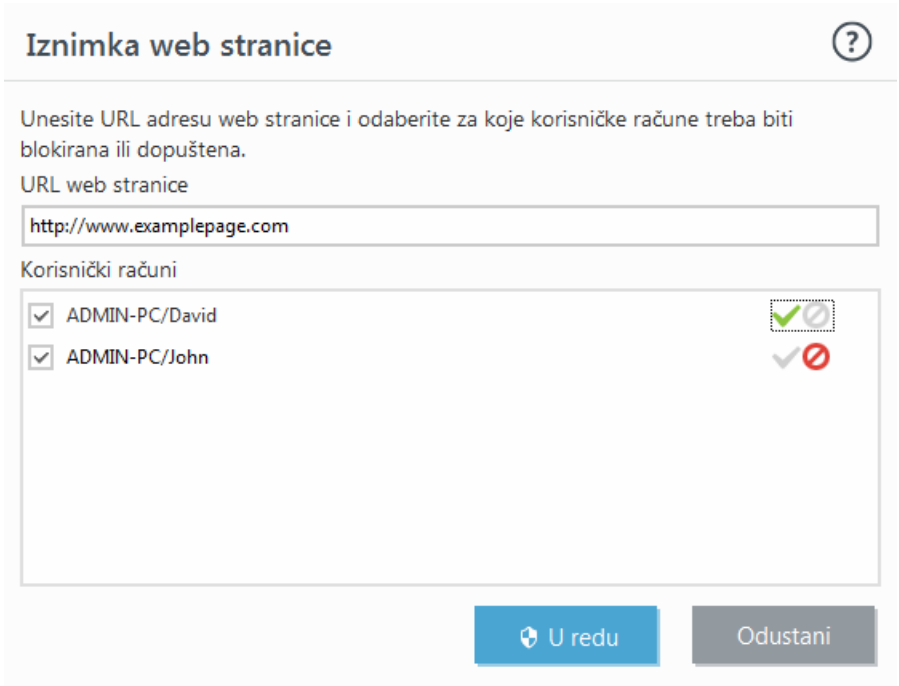
> Da bi ispravno funkcionirala, roditeljska kontrola zahtijeva aktiviranje Filtriranja sadržaja aplikacijskih protokola, Provjere HTTP protokola i firewalla. Sve te funkcije aktivirane su prema standardnim postavkama.

Iznimke web stranica

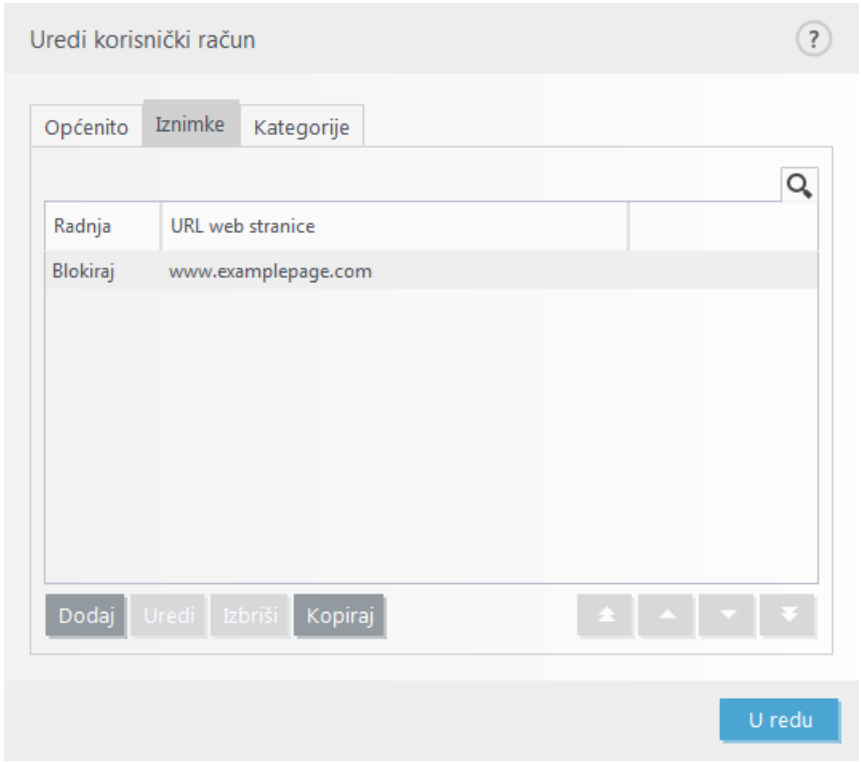
Da biste dodali iznimku za web stranicu, kliknite **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola,** a zatim kliknite **Dodaj iznimku za web stranicu**.



Unesite URL u polje **URL web stranice**, odaberite (dopušteno) ili (blokirano) za pojedini korisnički račun i zatim kliknite **U redu** da biste ga dodali na popis.



Za brisanje URL adrese s popisa kliknite **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola**, kliknite **Blokirani sadržaj i postavke** pod željenim korisničkim računom, kliknite karticu **Iznimka**, odaberite iznimku i kliknite **Ukloni**.



Na popisu URL adresa ne mogu se koristiti posebni simboli * (zvjezdica) i ? (upitnik). Na primjer, adrese web stranica s više TLD-ova moraju se unijeti ručno (stranicaprimjer.com*examplepage.com*, *examplepage.sk*stranicaprimjer.sk, itd.). Kada na popis dodate domenu, sav sadržaj koji se nalazi u toj domeni i svim poddomenama (npr, sub.examplepage.com*sub.examplepage.com*) bit će blokiran ili dopušten ovisno o vašem odabiru radnje na temelju URL-a.

Blokiranje ili dopuštanje određene web stranice može biti preciznije od blokiranja ili dopuštanja kategorije web stranica. Budite pažljivi pri mijenjanju tih postavki i dodavanju kategorije/web stranice na popis.

Korisnički računi

Ova postavka je dostupna pod **Napredno podešavanje** (F5) > **Web i e-pošta** > **Roditeljska kontrola** > **Korisnički računi** > **Uredi**.

U ovom odjeljku možete povezati Windows korisničke račune kojima se koristi Roditeljska kontrola za određene korisnike kako bi se ograničio njihov pristup neprikladnom ili štetnom sadržaju na internetu.

Stupci

Windows račun – Ime korisnika.

Aktivirano – Kada se aktivira ta opcija, aktiviraju se roditeljske kontrole za određeni korisnički račun.

Domena – Naziv korisnikove domene.

Rođendan – Dob korisnika kojemu taj račun pripada.

Kontrolni elementi

Dodaj – Prikazat će se prozor Rad s korisničkim računima.

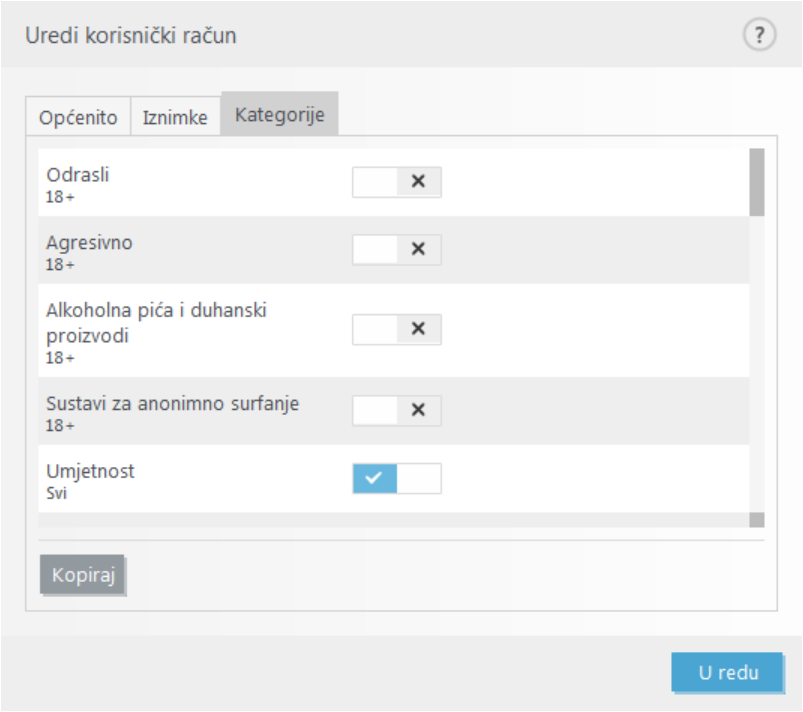
Uredi – Ta opcija omogućuje vam uređivanje odabranih računa.

Izbriši – Brisanje odabranog računa.

Osvježi – Ako ste dodali korisnički račun, ESET Internet Security može osvježiti popis korisničkih računa bez potrebe za ponovnim otvaranjem ovog prozora.

Kategorije

Označite potvrdni okvir u stupcu **Aktivirano** pored kategorije da biste je dopustili. Ako ne označite potvrdni okvir, kategorija neće biti dopuštena za ovaj račun.



Evo nekih primjera kategorija (grupa) s kojima korisnici možda nisu upoznati:

- **Razno** – Najčešće privatne (lokalne) IP adrese kao što su intranet, 127.0.0.0/8, 192.168.0.0/16 itd. Kad dobijete kod pogreške 403 ili 404, i web stranica će odgovarati toj kategoriji. Kad dobijete kôd pogreške 403 ili 404, i web stranica odgovarat će toj kategoriji.
- **Nije razriješeno** – Ta kategorija obuhvaća web stranice koje nisu razriješene zbog pogreške pri spajanju sa bazom podataka roditeljske kontrole.
- **Nekategorizirano** – Nepoznate web stranice koje još nisu u bazi podataka roditeljske kontrole.
- **Dinamičko** – Web stranice koje preusmjeravaju na druge stranice na drugim web stranicama.

Rad s korisničkim računima

Prozor ima tri kartice:

Općenito

Kliknite traku klizača pored opcije **Aktivirano** da biste uključili roditeljsku kontrolu za Windows račun odabran u nastavku.

Prvo **odaberite** Windows račun na svom računalu. Ograničenja postavljena u odjeljku Roditeljska kontrola utječu samo na standardne Windows račune. Administratorski računi mogu zaobići ograničenja.

Ako račun koristi roditelj, odaberite **Roditeljev račun**.

Postavite **datum rođenja djeteta** za račun da biste odredili njegovu razinu pristupa i postavili pravila pristupa za web stranice koje su prikladne za određenu dob.

Minimalna opširnost zapisivanja

ESET Internet Security sprema sve važne događaje u dnevnik koji je moguće prikazati izravno iz glavnog izbornika. Kliknite **Alati** > **Više alata** > **Dnevnici**, a zatim odaberite **Roditeljska kontrola** u padajućem izborniku **Dnevnik**.

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa.
- **Informacije** – Zapisuju se informativne poruke, uključujući dopuštene i blokirane iznimke, kao i svi prethodno navedeni zapisi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke s upozorenjima.
- **Ništa** – neće se stvoriti dnevnici.

Iznimke

Stvaranjem iznimke može se korisniku dopustiti ili zabraniti pristup web stranicama koje se ne nalaze na popisu iznimki. To je korisno ako želite kontrolirati pristup određenim web stranicama umjesto upotrebe kategorija. Iznimke stvorene za jedan račun mogu se kopirati i koristiti za drugi račun. To može biti korisno kada želite stvoriti istovjetna pravila za djecu slične dobi.

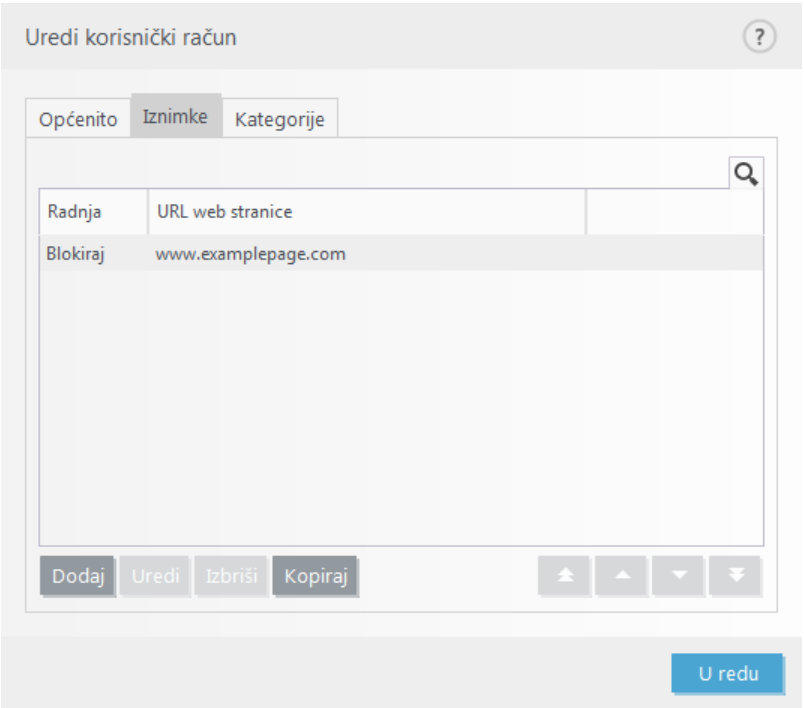
Kliknite **Dodaj** da biste stvorili novu iznimku. Naznačite **Radnju** (na primjer **Blokiraj**) pomoću padajućeg izbornika, upišite **URL web stranice** na koju se odnosi ova iznimka, a zatim kliknite **U redu**. Iznimka će biti dodana popisu postojećih iznimki, uz prikaz stanja.

Dodaj – Stvara novu iznimku.

Uredi – Možete urediti **URL web stranice** ili **Radnju** odabrane iznimke.

Ukloni – uklanja odabranu iznimku.

Kopiraj – Na padajućem izborniku odaberite korisnika iz kojeg želite kopirati stvorenu iznimku.



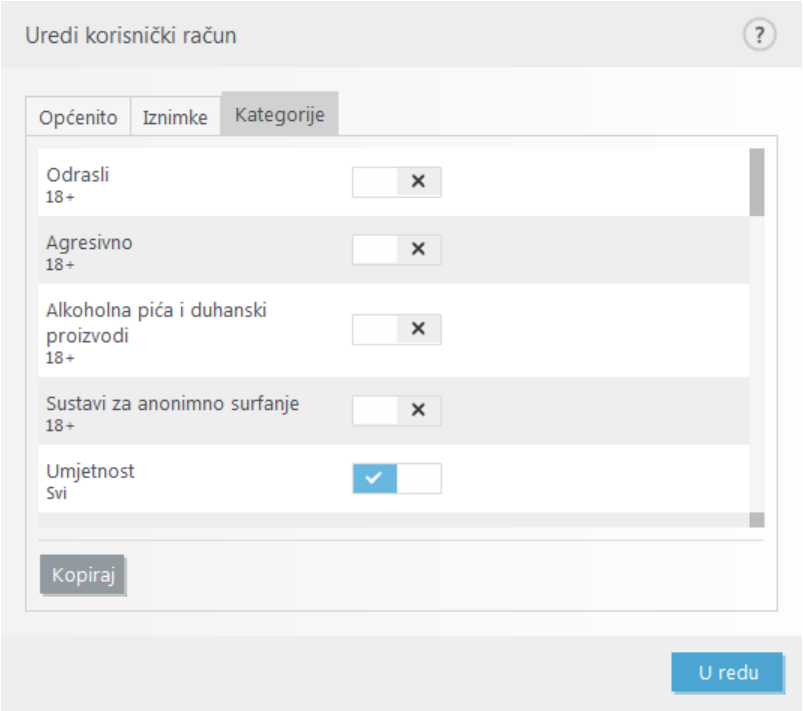
Definirane iznimke smatraju se važnijima od kategorija koje su definirane za odabrane račune. Na primjer, ako je na računu blokirana kategorija **Vijesti**, a vi ste definirali web stranicu vijesti kao dopuštenu iznimku, račun može

pristupiti dopuštenoj web stranici. Sve promjene koje su tu izvršene možete pregledati u odjeljku Iznimke.

Kategorije

U kartici **Kategorije** možete definirati opće kategorije web stranica koje želite blokirati ili dopustiti za svaki račun. Odaberite potvrdni okvir pored kategorije da biste je dopustili. Ako potvrdni okvir ostane prazan, kategorija neće biti dopuštena za taj račun.

Kopiraj – Omogućuje vam kopiranje popisa blokiranih ili dopuštenih kategorija iz postojećeg izmijenjenog računa.



Kopiranje iznimke od korisnika

Na padajućem izborniku odaberite korisnika iz kojeg želite kopirati stvorenu iznimku.

Kopiranje kategorija s računa

Omogućuje vam kopiranje popisa blokiranih ili dopuštenih kategorija iz postojećeg izmijenjenog računa.

Aktiviraj roditeljsku kontrolu

Opcija **Aktiviraj roditeljsku kontrolu** integrira roditeljsku kontrolu u program ESET Internet Security. Prikazat će se odjeljak Roditeljska kontrola u glavnom prozoru pod **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola**.

Anti-Theft

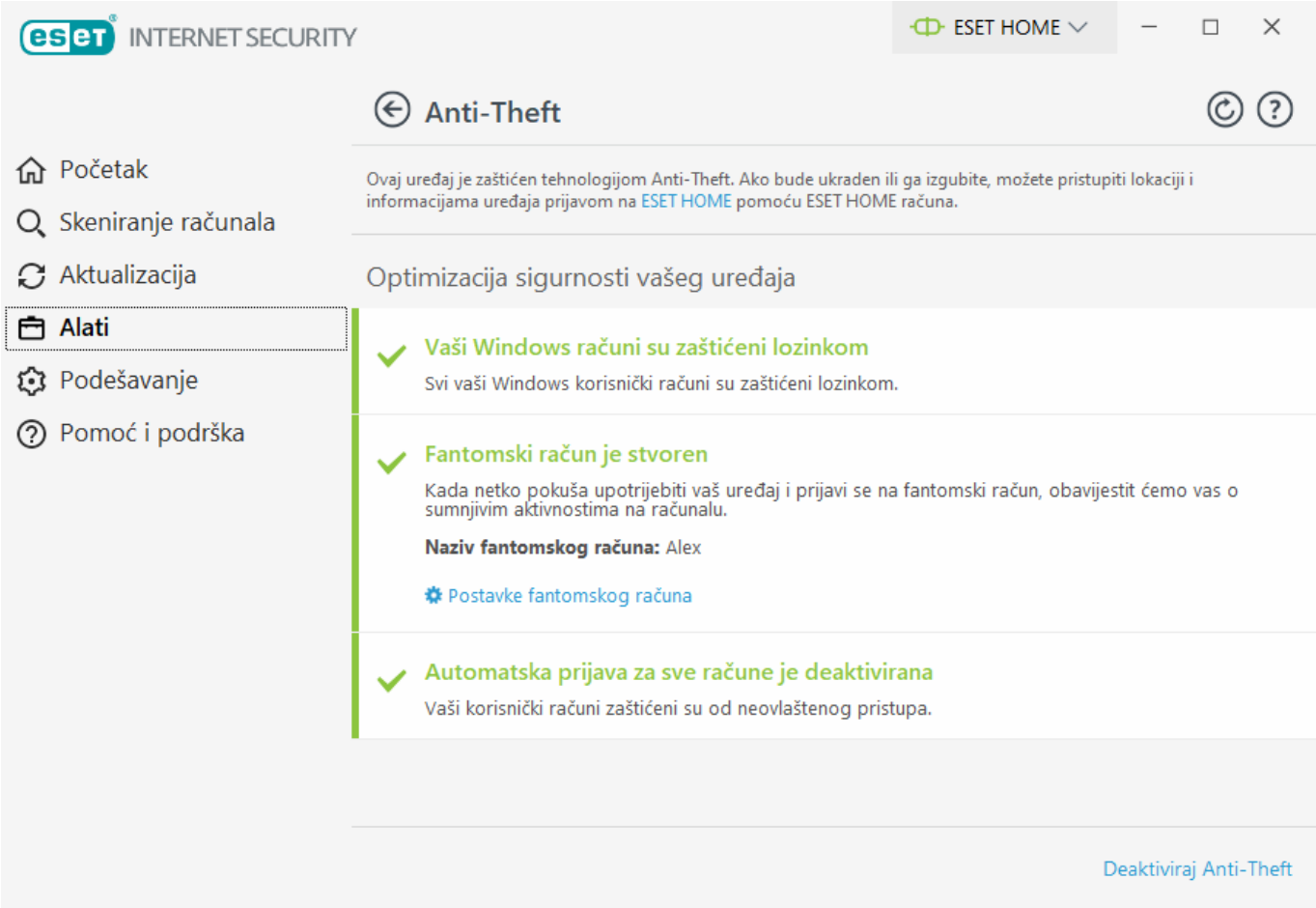
Za osobne uređaje stalno postoji rizik od gubljenja ili krađe tijekom puta od kuće na posao ili na drugim javnim mjestima. Anti-Theft je funkcija koja povećava sigurnost na korisničkoj razini u slučaju gubitka ili krađe uređaja.

Anti-Theft omogućuje nadziranje upotrebe uređaja i praćenje nestalog uređaja pomoću lokalizacije pomoću IP adrese u ESET HOME računu, čime vam pomaže da vratite uređaj i zaštitite osobne podatke.

Upotreba modernih tehnologija kao što su traženje geografske lokacije IP adrese, snimanje slike web-kamerom, zaštita korisničkog računa i nadzor uređaja Anti-Theft mogu pomoći vama i organima za provedbu zakona pri lociranju izgubljenog ili ukradenog računala ili uređaja. U ESET HOME računu možete vidjeti koje se aktivnosti odvijaju na vašem računalu ili uređaju.

Dodatne informacije o programu Anti-Theft u ESET HOME računu potražite u pomoći na mreži za ESET HOME.

Nakon što aktivirate Anti-Theft možete optimizirati sigurnost svojeg uređaja na glavnom prozoru programa > **Alati** > **Anti-Theft**.



Opcije optimizacije

Fantomski račun nije stvoren

Stvaranje fantomskog računa povećava mogućnosti utvrđivanja lokacije izgubljenog ili ukradenog uređaja. Ako označite da vaš uređaj nedostaje, Anti-Theft će blokirati pristup vašim aktivnim korisničkim računima radi zaštite osjetljivih podataka. Svatko tko pokuša upotrijebiti uređaj moći će upotrebljavati samo fantomski račun. Fantomski račun je oblik gostujućeg računa s ograničenim dopuštenjima. Upotrebljavat će se kao standardni račun sustava dok se uređaj ne označi kao oporavljen – time se onemogućuje bilo kome da se prijavi na druge korisničke račune ili pristupi korisničkim podacima.

Svaki put kada se netko prijavi na fantomski račun kada je vaše računalo u normalnom stanju, stići će vam e-poruka s obavijesti i informacijama o sumnjivim aktivnostima na računalu. Nakon primitka obavijesti e-poštom možete odlučiti želite li označiti računalo kao nestalo.

Da biste stvorili fantomski račun, kliknite **Stvori fantomski račun**, upišite **Naziv fantomskog računa** u tekstno polje i kliknite **Stvori**.

Kada stvorite fantomski račun, kliknite **Postavke fantomskog računa** da biste ga preimenovali ili uklonili.

Zaštita Windows računa lozinkom

Vaš korisnički račun nije zaštićen lozinkom. Ovo upozorenje o optimizaciji ćete dobiti ako najmanje jedan korisnički račun nije zaštićen lozinkom. Stvaranjem lozinke za sve korisnike (osim **fantomskog računa**) na računalu će se riješiti taj problem.

Da biste stvorili lozinku za korisnički račun, kliknite **Upravljanje Windows računima** i promijenite lozinku ili slijedite upute u nastavku:

1. Pritisnite CTRL+Alt+Delete na tipkovnici.
2. Kliknite **Promijeni lozinku**.
3. Ostavite polje **Stara lozinka** prazno.
4. Upišite lozinku u polja **Nova lozinka** i **Potvrda lozinku** i pritisnite **Enter**.

Automatska prijava za Windows račune

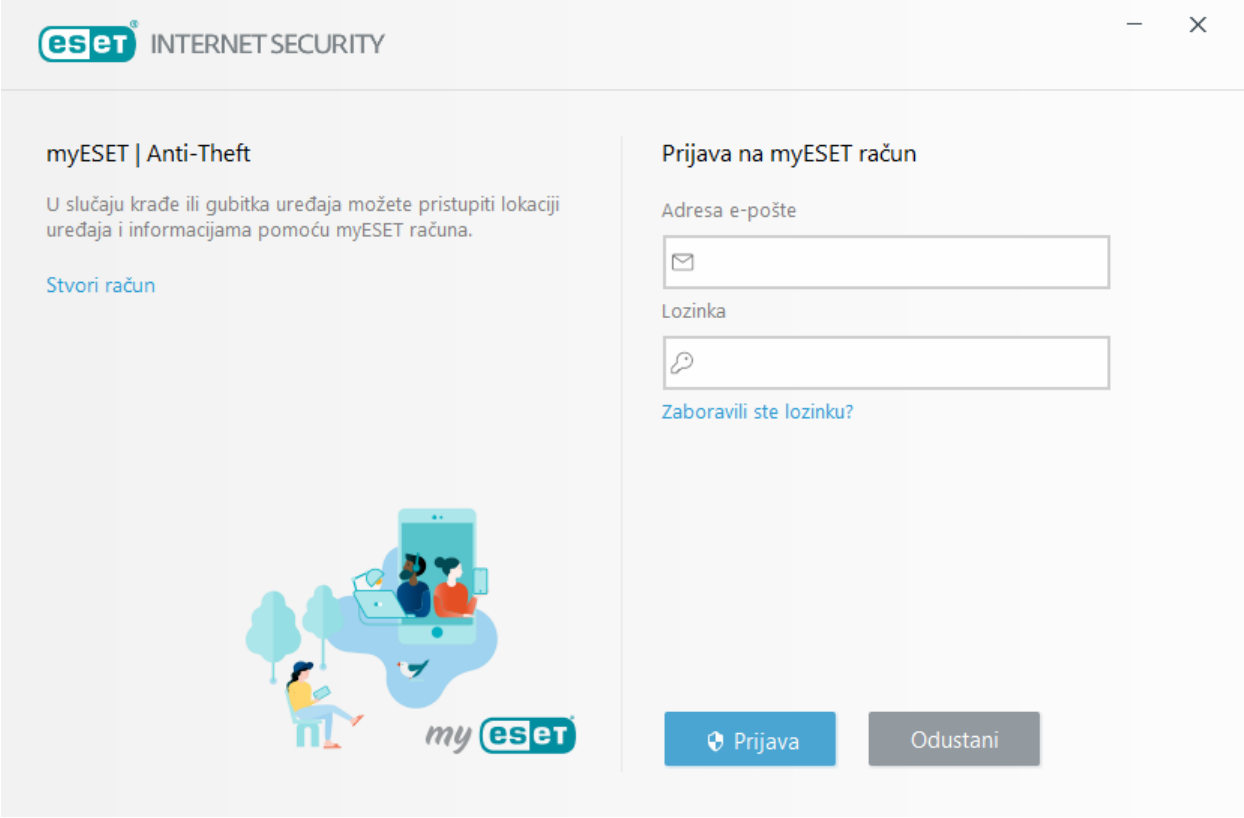
Vaš korisnički račun ima aktiviranu automatsku prijavu; stoga vaš račun nije zaštićen od neovlaštenog pristupa. Ovo upozorenje o optimizaciji ćete primiti ako je aktivirana automatska prijava na najmanje jednom korisničkom računu. Kliknite **Deaktiviraj automatsku prijavu** da biste riješili taj problem s optimizacijom.

Automatska prijava za fantomski račun

Automatska prijava je aktivirana za **fantomski račun** na vašem uređaju. Kada je uređaj u normalnom stanju, ne preporučujemo da upotrebljavate automatsku prijavu jer može uzrokovati probleme s pristupom vašem stvarnom korisničkom računu ili poslati lažne alarme o stanju vašeg nestalog računala. Kliknite **Deaktiviraj automatsku prijavu** da biste riješili taj problem s optimizacijom.

Prijavite se na svoj račun ESET HOME.

Da biste aktivirali/deaktivirali Anti-Theft i pristupili lokaciji uređaja i informacijama u ESET HOME računu, prijavite se u svoj ESET HOME račun.



Postoji nekoliko načina prijave na vaš ESET HOME račun:

- **Upotrijebite svoj adresu e-pošte i lozinku za ESET HOME** – upišite **adresu e-pošte** i **lozinku** koju ste upotrijebili za stvaranje svojeg ESET HOME računa i kliknite **Prijava**.

- **Upotrijebite svoj račun sa servisa Google / AppleID** – kliknite **Nastavi sa servisom Google** ili **Nastavi sa servisom Apple** i prijavite se u odgovarajući račun. Nakon uspješne prijave bit ćete preusmjereni na stranicu za potvrdu ESET HOME. Za nastavak se prebacite natrag na prozor ESET-ova programa. Za više informacija o prijavi putem računa servisa Google / AppleID pogledajte upute u online pomoći za ESET HOME.

- **Skenirajte QR kôd** – kliknite **Skeniraj QR kôd** za prikaz QR kôda. Otvorite mobilnu aplikaciju ESET HOME i skenirajte QR kôd ili usmjerite kameru uređaja na QR kôd. Dodatne informacije potražite u online pomoći za ESET HOME.

Prijava nije uspjela – česte pogreške.

Ako nemate ESET HOME račun, kliknite **Stvori račun** da biste se registrirali ili proučite upute u online pomoći za ESET HOME.
Ako ste zaboravili lozinku, kliknite **Zaboravio/la sam lozinku** i slijedite korake na zaslonu ili proučite upute u online pomoći za ESET HOME.

Anti-Theft ne podržava Microsoft Windows Home Server.

Postavi naziv uređaja

Polje **Naziv uređaja** predstavlja naziv računala (uređaja) koji će se prikazati kao identifikator na svim ESET HOME servisima. Naziv vašeg računala je standardan. Upišite naziv uređaja ili upotrijebite standardni i kliknite **Nastavi**.

Anti-Theft aktiviran/deaktiviran

Ovaj prozor sadržava poruku za potvrdu kada aktivirate/deaktivirate Anti-Theft:

- Aktivirano – vaš uređaj je sada zaštićen programom Anti-Theft, a njegovom sigurnosti možete daljinski upravljati naESET HOME portalu pomoću svojeg računa.
- Deaktiviran Anti-Theft – deaktiviran je na ovom uređaju, a svi podaci povezani s programom <%ESET_ANTTHEFT%> za ovaj uređaj se uklanjaju s ESET HOME portala.

Dodavanje novog uređaja nije uspjelo

Dobili ste poruku o pogrešci pri pokušaju aktivacije programa Anti-Theft.

Najčešći scenariji su:

- Pogreška pri prijavi u ESET HOME
- Nema povezivosti s internetom (ili internet trenutačno nije u funkciji)

Ako ne možete riješiti problem, obratite se ESET-ovoj tehničkoj podršci.

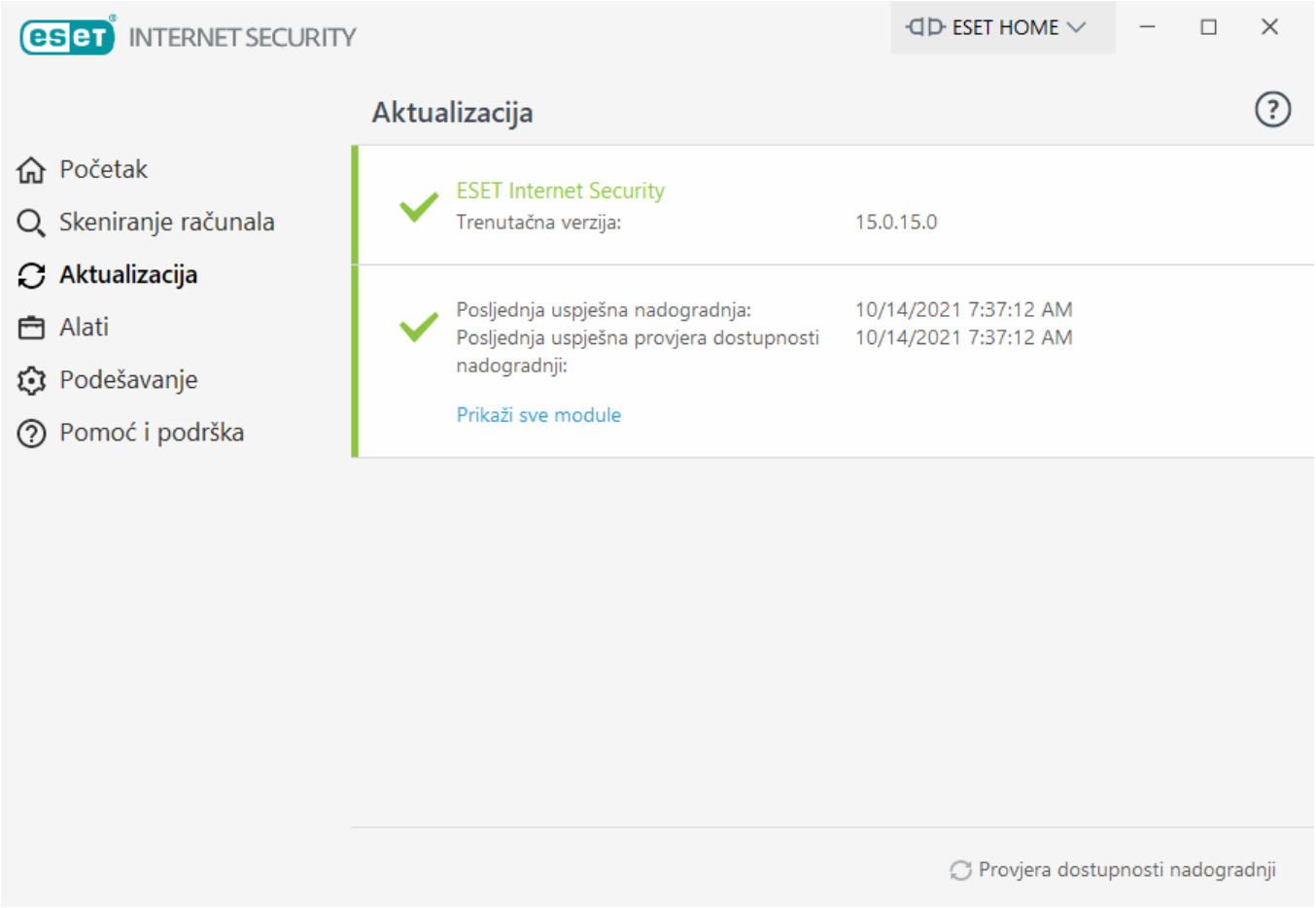
Aktualizacija programa

Redovita nadogradnja programa ESET Internet Security najbolji je način osiguravanja maksimalne razine sigurnosti na računalu. Modul nadogradnje osigurava da su moduli programa i komponente sustava uvijek aktualni.

Klikom gumba **Aktualizacija** u glavnom prozoru programa možete provjeriti status trenutačne nadogradnje, datum i vrijeme zadnje uspješne nadogradnje te je li nadogradnja potrebna.

Osim automatskih nadogradnji, možete kliknuti opciju **Potraži nadogradnje** da biste pokrenuli ručnu nadogradnju. Redovite nadogradnje modula programa i komponenata imaju važnu ulogu u održavanju potpune zaštite od zlonamjernog koda. Obratite pozornost na konfiguraciju i rad modula programa. Za primanje nadogradnji morate aktivirati program pomoću licenčnog ključa. Ako to niste učinili tijekom instalacije, trebat ćete unijeti licenčni ključ kako biste aktivirali program i pristupili serverima za nadogradnju tvrtke ESET tijekom nadogradnje.

Licenčni ključ primili ste e-poštom od tvrtke ESET nakon kupnje programa ESET Internet Security.



Trenutačna verzija – Prikazuje broj verzije trenutačne verzije programa koju ste instalirali.

Posljednja uspješna nadogradnja – Prikazuje datum zadnje uspješne nadogradnje. Ako ne vidite neki noviji datum, moguće je da su vaši moduli programa zastarjeli.

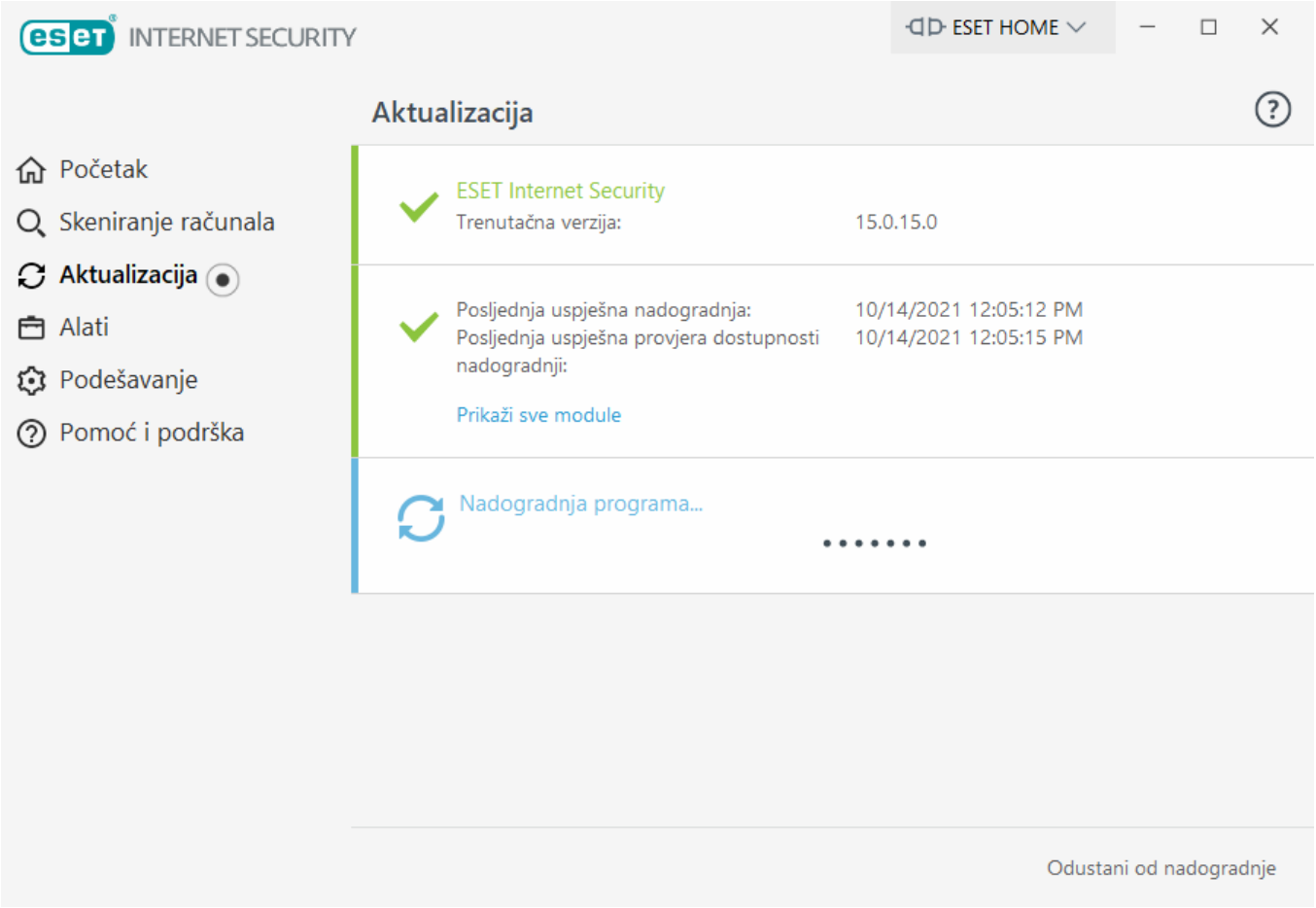
Posljednja uspješna provjera dostupnosti nadogradnji – Prikazuje datum zadnjeg pretraživanja novih nadogradnji.

Prikaži sve module – Prikazuje popis instaliranih modula programa.

Kliknite **Provjera dostupnosti nadogradnji** da biste otkrili najnoviju dostupnu verziju programa ESET Internet Security.

Proces aktualizacije

Nadogradnja započinje kada kliknete stavku **Potraži nadogradnje**. Prikazat će se traka napretka i preostalo vrijeme za preuzimanje. Da biste prekinuli aktualizaciju, kliknite **Odustani od aktualizacije**.



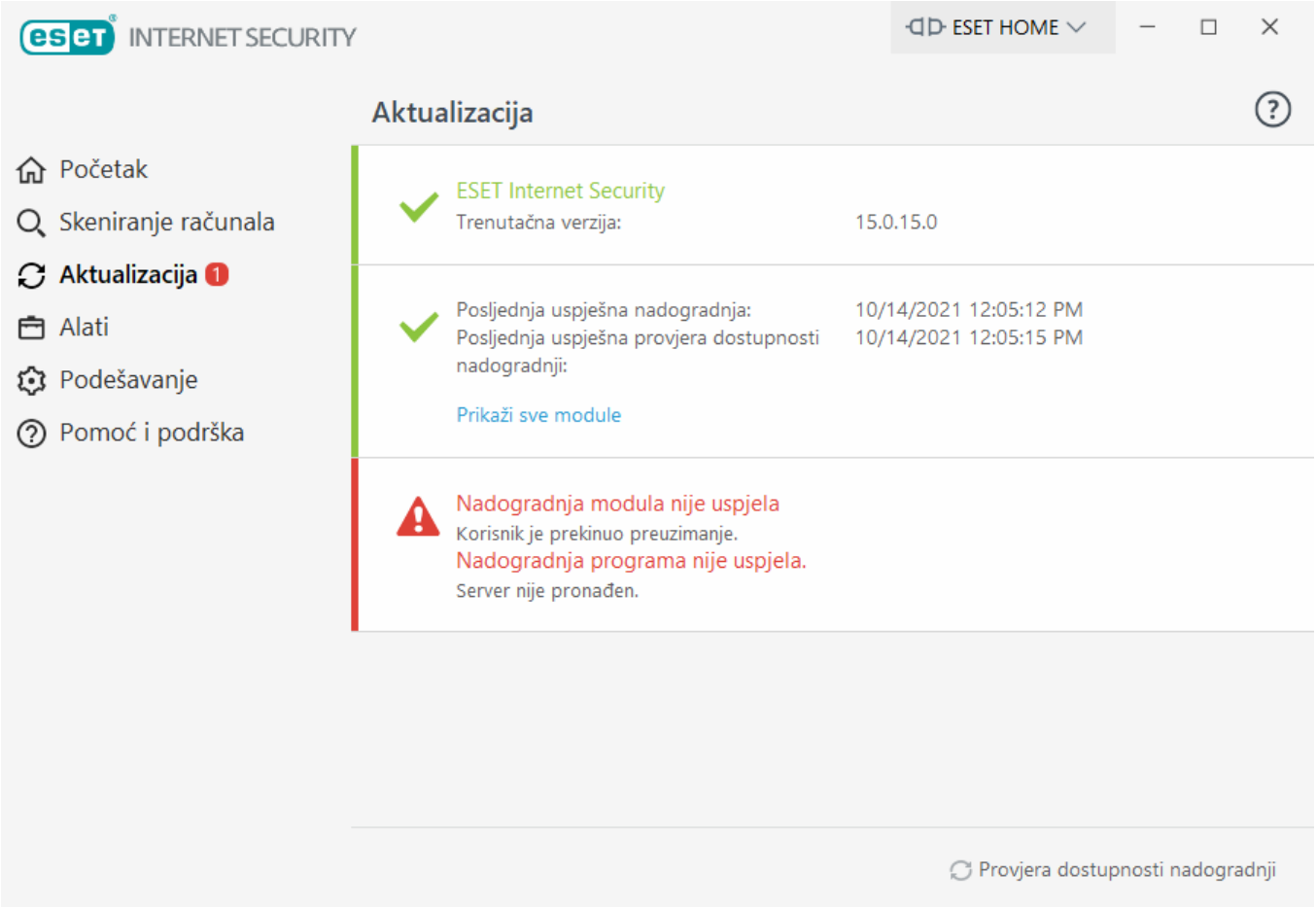
Pod uobičajenim okolnostima možete vidjeti zelenu oznaku potvrde u prozoru **Nadogradnja** koja označava da je program nadograđen. Ako ne vidite zelenu oznaku potvrde, program je zastario i izloženiji zarazama. Nadogradite module programa što prije.

Neuspješna nadogradnja

Ako dobijete poruku o neuspješnoj nadogradnji modula, to može biti uzrokovano sljedećim problemima:

1. **Neispravna licenca** – licenca koja se upotrebljava za aktivaciju nije ispravna ili je istekla. U glavnom prozoru programa kliknite **Pomoć i podrška** > **Promijeni licencu** i unesite novi licenčni ključ.

2. **Tijekom preuzimanja datoteka nadogradnje došlo je do pogreške** – uzrok tome mogu biti neispravne 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).



Preporučujemo da ponovno pokrenete računalo nakon uspješne nadogradnje programa ESET Internet Security na noviju verziju programa kako biste osigurali da su svi moduli programa ispravno nadograđeni. Nije potrebno ponovno pokretati računalo nakon redovitih nadogradnji modula.

Dodatne informacije potražite u Otklanjanje poteškoća za poruku „Nadogradnja modula nije uspjela”.

Podešavanje aktualizacije

Mogućnosti podešavanja nadogradnje dostupne su na stablu **Napredno podešavanje** (F5), u odjeljku **Nadogradnja** > **Osnovno**. U ovom odjeljku navode se informacije o izvoru aktualizacije, na primjer aktualizacijski serveri i podaci za autorizaciju za te servere.

Osnovno

Profil nadogradnje koji je trenutačno u upotrebi (osim ako određeni profil nije postavljen u opcijama **Napredno podešavanje** > **Firewall** > **Poznate mreže**) prikazuje se u padajućem izborniku **Odaberite standardni profil nadogradnje**.

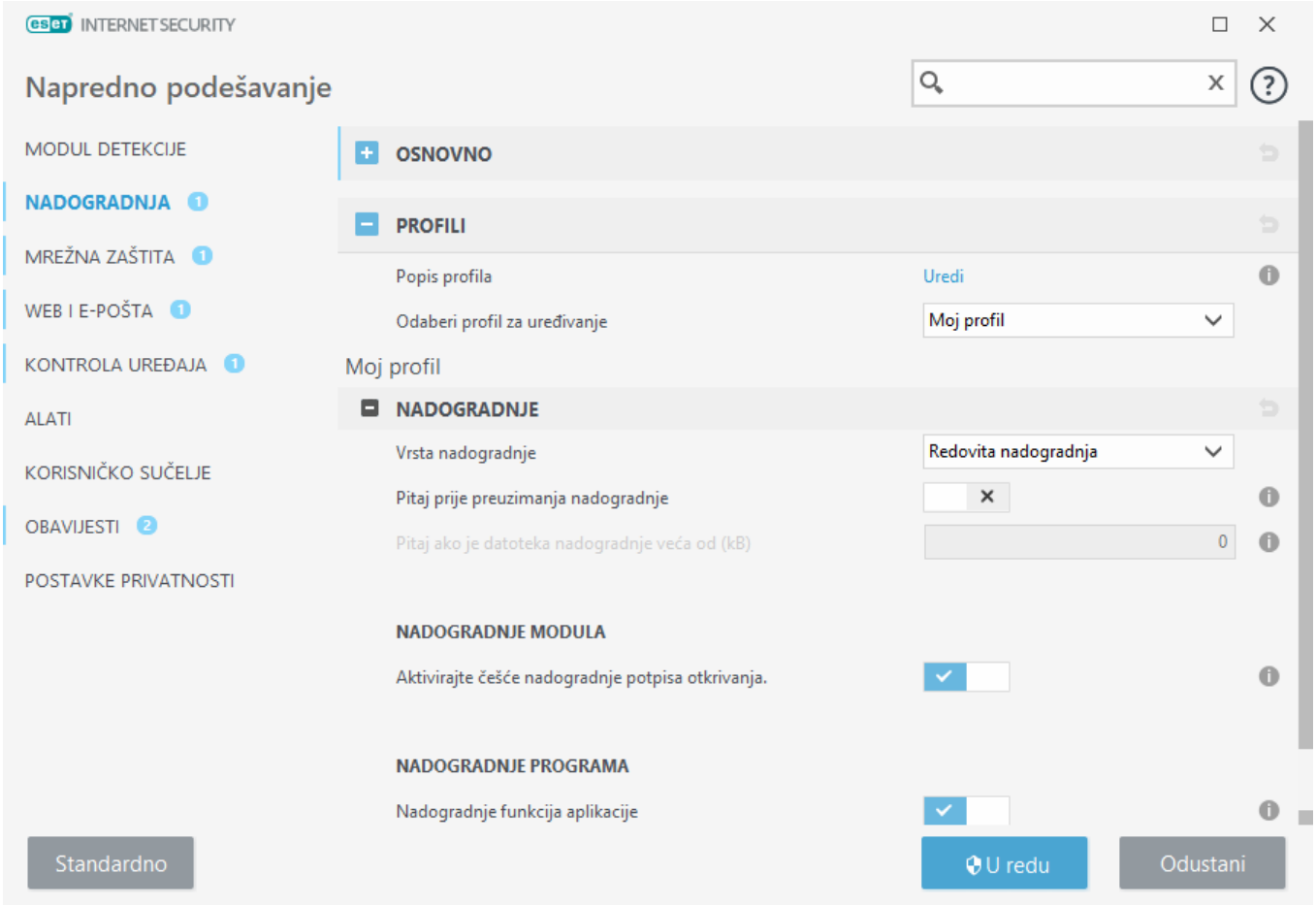
Da biste stvorili novi profil, pogledajte odjeljak Profili nadogradnje.

Automatsko prebacivanje profila – Omogućuje vam promjenu profila za određenu mrežu.

Ako dođe do problema s preuzimanjem nadogradnja modula detekcije i drugih modula, kliknite gumb **Očisti** da biste izbrisali privremene datoteke nadogradnje / predmemoriju.

Povrat 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.



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 HTTP-a).

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.

Pitaj prije preuzimanja nadogradnje – program će prikazati obavijest u kojoj možete potvrditi ili odbiti preuzimanja datoteka nadogradnje.

Pitaj ako je datoteka nadogradnje veća od (kB) – Program će prikazati upit za potvrdu ako je datoteka nadogradnje veća od navedene vrijednosti. Ako je veličina datoteke za nadogradnju postavljena na 0 kB, program će uvijek prikazati upit za potvrdu.

Deaktiviraj obavijest o uspješnoj nadogradnji – Isključuje obavijesti na traci sustava u donjem desnom kutu zaslona. Korisno je odabrati tu mogućnost ako je pokrenuta aplikacija ili igra na cijelom zaslonu. Imajte na umu da su u načinu rada za igranje isključene sve obavijesti.

Nadogradnje modula

Aktiviraj češće nadogradnje potpisa za otkrivanje – Potpisi za otkrivanje bit će nadograđivani u kraćim intervalima. Deaktivacija ove postavke može negativno utjecati na stopu otkrivanja.

Nadogradnje programa

Nadogradnje funkcija aplikacije – automatski instalirajte nove verzije programa ESET Internet Security.

Opcije veze

Kako biste upotrebljavali proxy server za preuzimanje nadogradnji, pogledajte odjeljak Opcije veze.

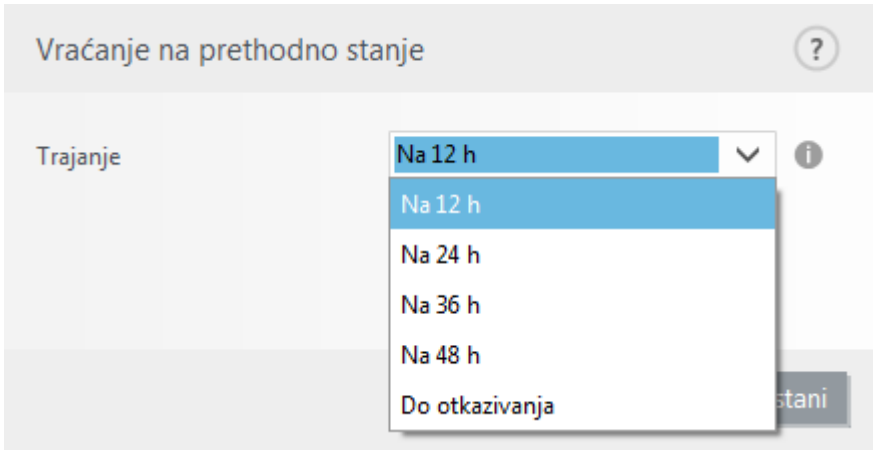
Vraćanje aktualizacije

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 Internet Security bilježi snimke modula detekcije i modula programa za upotrebu s funkcijom vraćanja na prethodno stanje. Da biste stvorili snimke baze podataka virusa, funkcija **Stvori snimke modula** mora ostati aktivirana. Kada je aktivirana funkcija **Stvori 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.

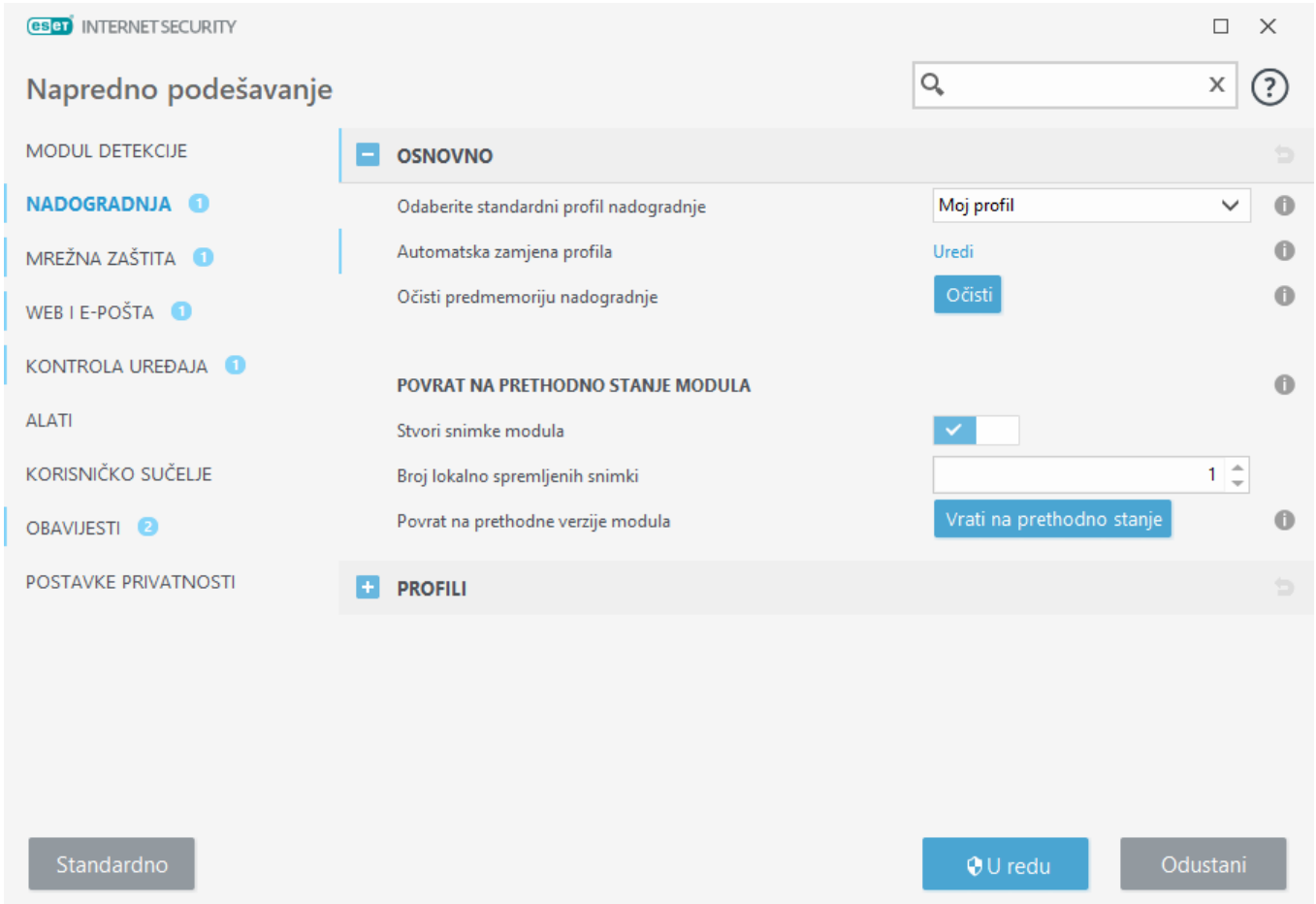
> Kada se dosegne maksimalna količina snimki (na primjer, tri), najstarija snimka zamjenjuje se novom svakih 48 sati. ESET Internet Security vraća modul detekcije i verzije nadogradnji modula programa na najstariju snimku.

Ako kliknete **Povrat** (**Napredno podešavanje** (F5) > **Nadogradnja** > **Općenito**), morate s padajućeg izbornika **Trajanje** odabrati vremenski interval koji predstavlja razdoblje tijekom kojeg će nadogradnje modula za otkrivanje virusa i programskih modula biti zaustavljene.



Odaberite **Do otkazivanja** da biste odgodili redovne nadogradnje na neodređeno vrijeme dok ručno ne vratite funkciju nadogradnje. ESET ne preporučuje odabir ove opcije jer ona predstavlja mogući sigurnosni rizik.

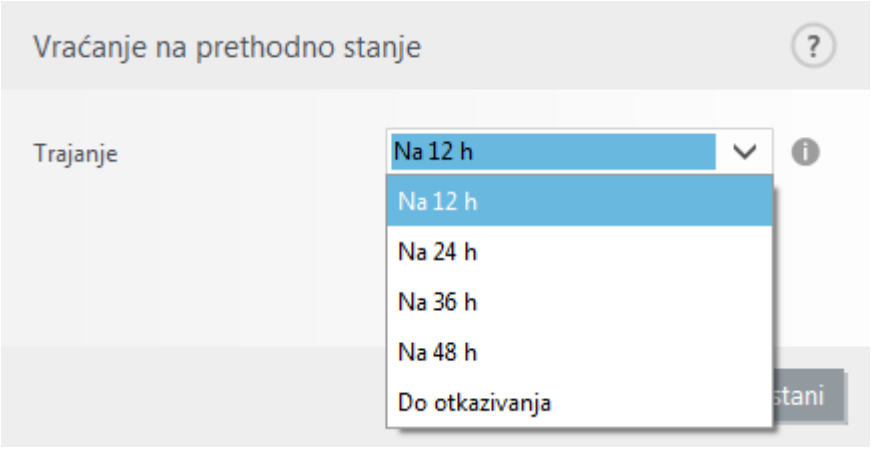
Ako se vrši vraćanje na prethodno stanje, gumb **Vrati na prethodno stanje** pretvara se u **Dopusti nadogradnje**. Tijekom vremenskog intervala odabranog iz padajućeg izbornika **Obustava nadogradnji** nisu dopuštene nadogradnje. Verzija modula detekcije vraćena je na najstariju dostupnu verziju i spremljena 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.

Vremenski interval povrata

Ako kliknete **Povrat** (**Napredno podešavanje** (F5) > **Nadogradnja** > **Općenito**), morate s padajućeg izbornika **Trajanje** odabrati vremenski interval koji predstavlja razdoblje tijekom kojeg će nadogradnje modula za otkrivanje virusa i programskih modula biti zaustavljene.



Odaberite **Do otkazivanja** da biste odgodili redovne nadogradnje na neodređeno vrijeme dok ručno ne vratite funkciju nadogradnje. ESET ne preporučuje odabir ove opcije jer ona predstavlja mogući sigurnosni rizik.

Nadogradnje programa

Odjeljak **Nadogradnje programa** omogućuje automatsku instalaciju novih nadogradnji funkcija kada su dostupne.

Nadogradnje funkcija aplikacije uvode nove funkcije ili mijenjaju one koje već postoje u prethodnim verzijama. Moguće ih je izvršiti automatski bez korisničke intervencije, ali korisnik može odabrati da ga se o tome obavijesti. Nakon instalacije nadogradnje funkcije aplikacije možda će biti potrebno restartanje računala.

Nadogradnje funkcija aplikacije – kada su omogućene, nadogradnje funkcija aplikacije izvodit će se automatski.

Opcije veze

Da biste pristupili opcijama podešavanja proxy servera za određeni profil nadogradnje, kliknite **Nadogradnja** na stablu **Napredno podešavanje** (F5) i zatim kliknite **Profili** > **Nadogradnje** > **Opcije povezivanja**. 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 Internet Security ne koristi proxy server.

Mogućnost **Veza putem proxy servera** treba se odabrati ako:

• Drugačiji proxy server od onog definiranog pod **Alati** > **Proxy server** upotrebljava se za nadogradnju programa ESET Internet Security. 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 Internet Security 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.

Polja **Korisničko ime** i **Lozinka** u ovom odjeljku specifična su za proxy server. Ispunite ova polja samo ako su korisničko ime i lozinka potrebni za pristup proxy serveru. Ta polja trebate ispuniti samo ako trebate lozinku za pristup internetu putem proxy servera.

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 zakazani zadatak, kliknite **Alati** > **Više alata** > **Planer**. Prema standardnim se postavkama u programu ESET Internet Security 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 zadataka nadogradnje potražite u odjeljku Planer.

Dijaloški prozor – potrebno je restartati računalo

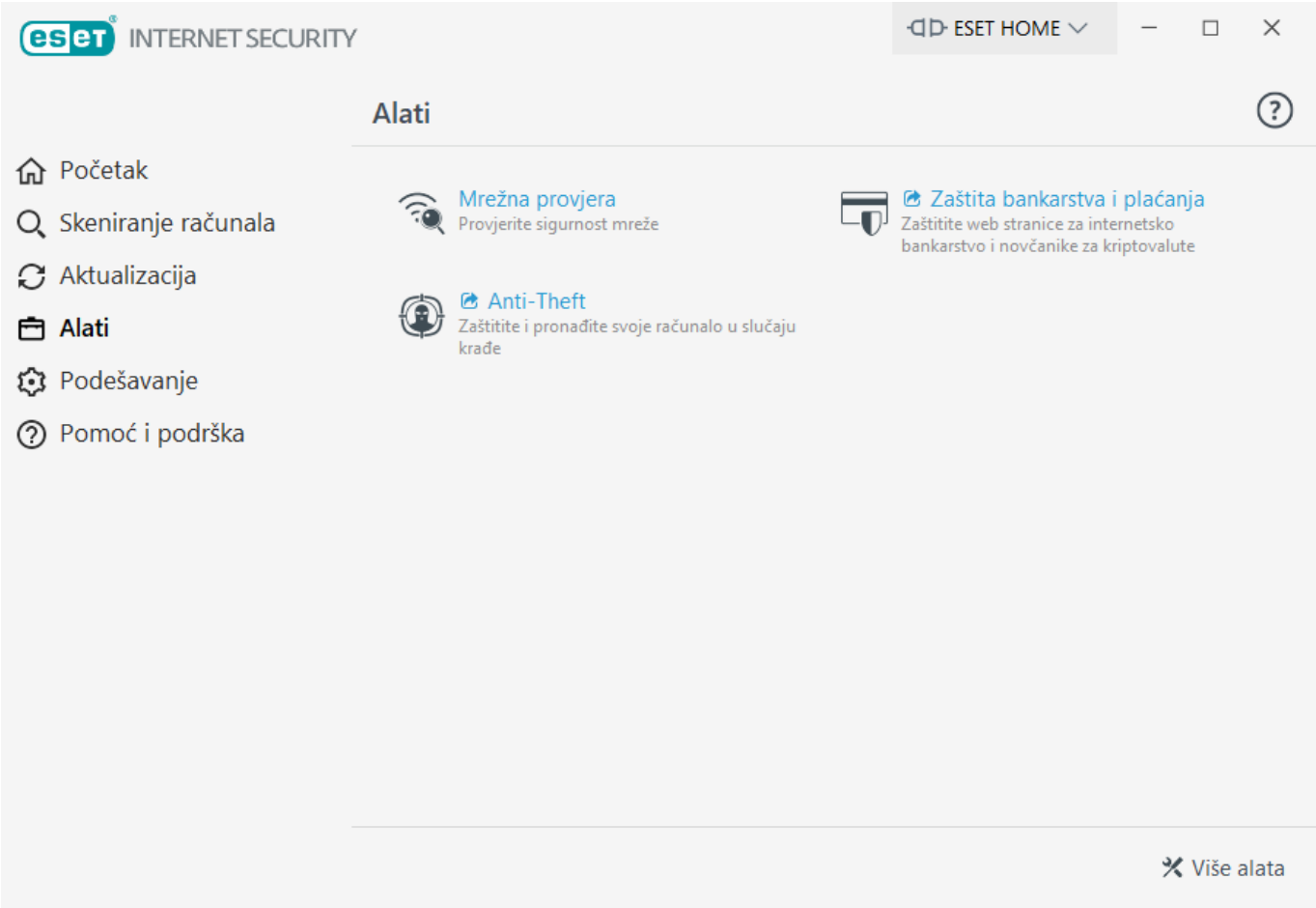
Nakon nadogradnje programa ESET Internet Security na novu verziju potrebno je restartati računalo. Nove verzije programa ESET Internet Security izdaju se radi instalacije poboljšanja ili popravka problema koji se ne mogu riješiti automatskom nadogradnjom modula programa.

Nova verzija programa ESET Internet Security se može instalirati automatski, na temelju postavki nadogradnje programa ili ručno preuzimanjem i instalacijom novije verzije u odnosu na prethodnu.

Kliknite **Restartaj odmah** da biste restartali računalo. Ako planirate restartati računalo kasnije, kliknite **Podsjeti me kasnije**. Kasnije možete ručno restartati računalo iz odjeljka **Početak** u glavnom prozoru programa.

Alati

Izbornik **Alati** sadrži module koji pojednostavnjuju administriranje programa i nude dodatne mogućnosti naprednim korisnicima.



Mrežna provjera – smanjuje rizik od sigurnosnih problema kada ste povezani s mrežom. Više informacija potražite u odjeljku Mrežna provjera.

Zaštita bankarstva i plaćanja – ESET Internet Security štiti vaše brojeve kreditnih kartica i druge osjetljive osobne podatke dok se koristite mrežnim bankarstvom ili web stranicama za plaćanje. Pokrenut će se zaštićeni preglednik koji omogućava sigurnije bankovne transakcije.

Anti-Theft – locira vaš uređaj u slučaju gubitka ili krađe i pomaže vam da ga pronađete.

Kliknite Više alata za prikaz drugih alata za zaštitu računala (kao što je Karantena).

Mrežna provjera

Mrežna provjera može pomoći u prepoznavanju ranjivosti vaše pouzdane (kućne ili uredske) mreže (na primjer, otvoreni portovi ili slaba lozinka routera). Također pruža popis povezanih uređaja na kojem su uređaji kategorizirani prema vrsti (na primjer, pisač, router, mobilni uređaj itd.) kako biste vidjeli što je povezano na vašu mrežu (npr. igraća konzola, uređaj interneta stvari (IoT) ili drugi pametni kućni uređaji).

Mrežna provjera pomaže vam identificirati ranjivost routera i povećava vašu razinu zaštite kada ste povezani na mrežu.

Mrežna provjera ne izvršava ponovnu konfiguraciju vašeg routera za vas. Sami ćete napraviti promjene upotrebom specijaliziranog sučelja vašeg routera. Kućni routeri vrlo su izloženi zlonamjernim programima koji se upotrebljavaju za pokretanje distribuiranog napada uskraćivanja usluge (DDoS). Ako korisnik nije promijenio standardnu lozinku routera, hakeri je mogu jednostavno pogoditi i prijaviti se na vaš router te ga ponovno konfigurirati ili ugroziti vašu mrežu.

Toplo preporučujemo izradu jake lozinke koja je dovoljno dugačka i uključuje brojeve, simbole ili velika slova. Kako bi lozinku bilo teže probiti, upotrijebite mješavinu različitih vrsta znakova.

Ako je mreža s kojom ste povezani konfigurirana kao pouzdana, mrežu možete označiti kao "Moja mreža". Kliknite **Označi kao "Moja mreža"** da biste na mrežu dodali oznaku Moja mreža. Ova oznaka će se prikazivati pored mreže u cijelom programu ESET Internet Security radi bolje identifikacije i sigurnosti. Kliknite **Poništi označavanje kao "Moja mreža"** da biste uklonili oznaku.

Svaki uređaj koji je povezan na vašu mrežu se prikazuje s osnovnim informacijama u prikazu popisa. Kliknite određeni uređaj da biste uredili uređaj ili pogledali detaljne informacije o uređaju.

Padajući izbornik **Mreže** omogućuje filtriranje uređaja na temelju sljedećih kriterija:

- Uređaji povezani s određenom mrežom
- Uređaji povezani sa **Svim mrežama**
- nekategorizirani uređaji

Za prikaz svih povezanih uređaja u sonarnom prikazu kliknite ikonu sonara . Pomaknite pokazivač preko ikone uređaja za prikaz osnovnih informacija poput naziva mreže i datuma posljednjeg pregleda.

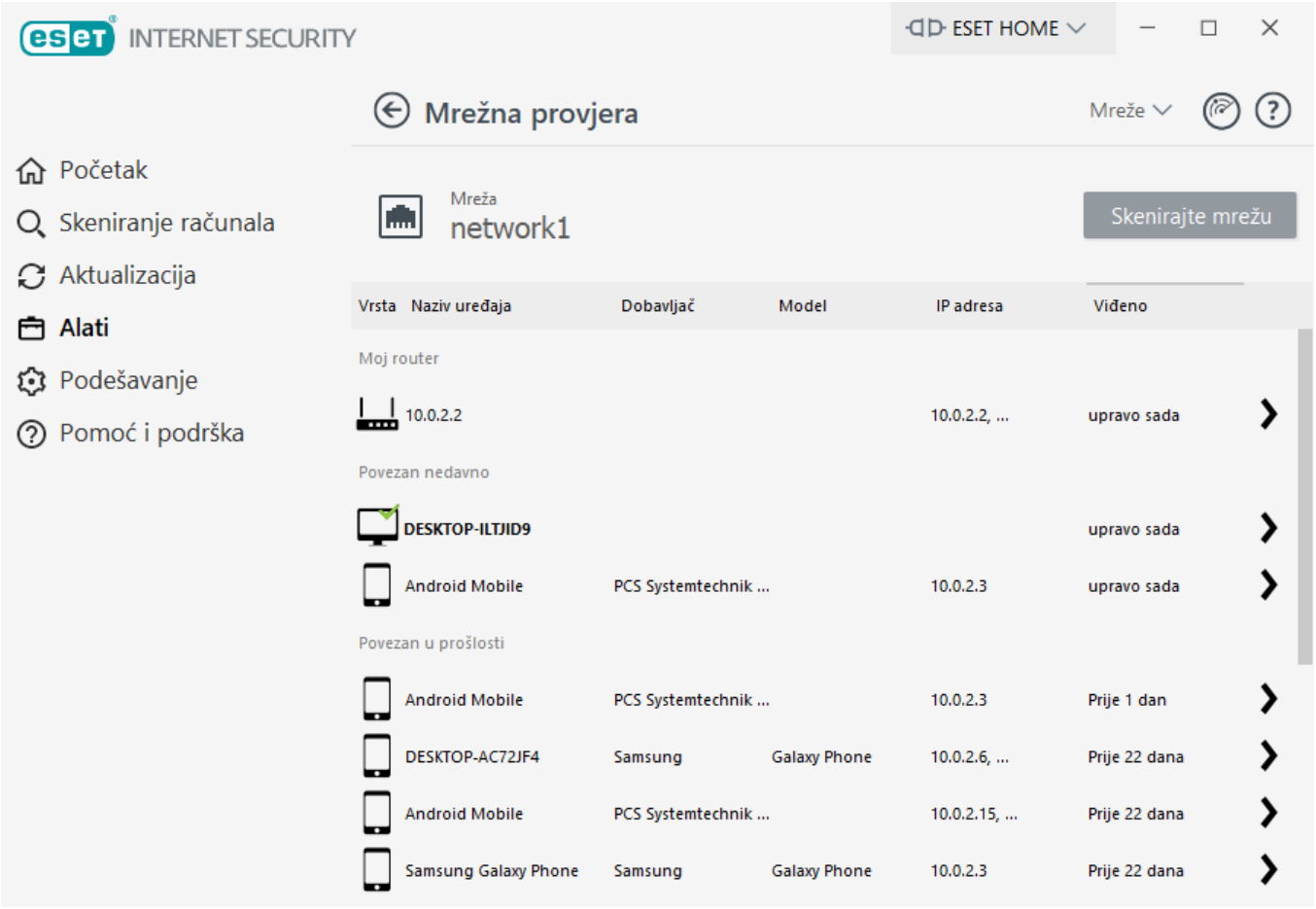
Kliknite ikonu uređaja za uređivanje uređaja ili prikaz detaljnih informacija o uređaju. Nedavno povezani uređaji prikazani su bliže routeru tako da ih možete lakše uočiti.

Kliknite **Skeniraj mrežu** da biste ručno izvršili skeniranje mrežu na koju ste trenutačno povezani. **Skeniranje mreže** je dostupno samo za pouzdanu mrežu. Pogledajte Poznate mreže za pregled ili uređivanje mrežnih postavki.

Možete odabrati jednu od sljedećih opcija skeniranja:

- Skeniraj sve
- Skeniraj samo usmjerivač
- Skeniraj samo uređaje

Izvršite skeniranje mreže samo na pouzdanoj mreži! Ako ovo učinite na nepouzdanim mrežama, budite svjesni potencijalne opasnosti.



Kad je skeniranje dovršeno, prikazat će se obavijest s linkom na osnovne informacije o uređaju ili možete dvokliknuti sumnjiv uređaj na popisu ili sonarnom prikazu. Kliknite **Otklanjanje poteškoća** za prikaz nedavno blokiranih komunikacija. Dodatne informacije o otklanjanju poteškoća s firewallom.

Dvije su vrste obavijesti koje se prikazuju u modulu Mrežna provjera:

- **Novi uređaj povezan s mrežom** – prikazuje se ako se prethodno neviđeni uređaj poveže s mrežom dok je korisnik povezan.
- **Pronađeni su novi mrežni uređaji** – prikazuje se ako se ponovno povežete na pouzdanu mrežu, a prisutan je prethodno neviđeni uređaj.

Obje vrste obavijesti obavještavaju vas da se neovlašteni uređaj pokušava povezati s vašom mrežom. Kliknite **prikaži uređaj** da bi se prikazale pojedinosti o uređaju.

Što znače ikone na uređajima u mrežnoj provjeri?

	Ikona žute zvijezde označava uređaje koji su novi u mreži ili koje je ESET prvi put otkrio.
	Žuta ikona opreza označava da vaš router možda sadrži ranjivosti. Kliknite ikonu u programu za detaljnije informacije o problemu.
	Crvena ikona upozorenja na uređajima označava da vaš router sadrži ranjivosti i da su možda zaraženi. Kliknite ikonu u programu za detaljnije informacije o problemu.

Plava ikona se može pojaviti kada ESET-ov program ima dodatne informacije za vaš router, ali ne zahtijeva hitnu pozornost jer nema sigurnosnih rizika. Kliknite ikonu u programu za detaljnije informacije.

Mrežni uređaj u Mrežnoj provjeri

Ovdje se mogu pronaći detaljne informacije o određenom mrežnom uređaju, uključujući sljedeće:

- Naziv uređaja
- Vrsta uređaja
- Zadnje viđen
- Naziv mreže
- IP adresa
- MAC adresa
- Operacijski sustavi

Ikona olovke označava da možete izmijeniti naziv ili vrstu uređaja.

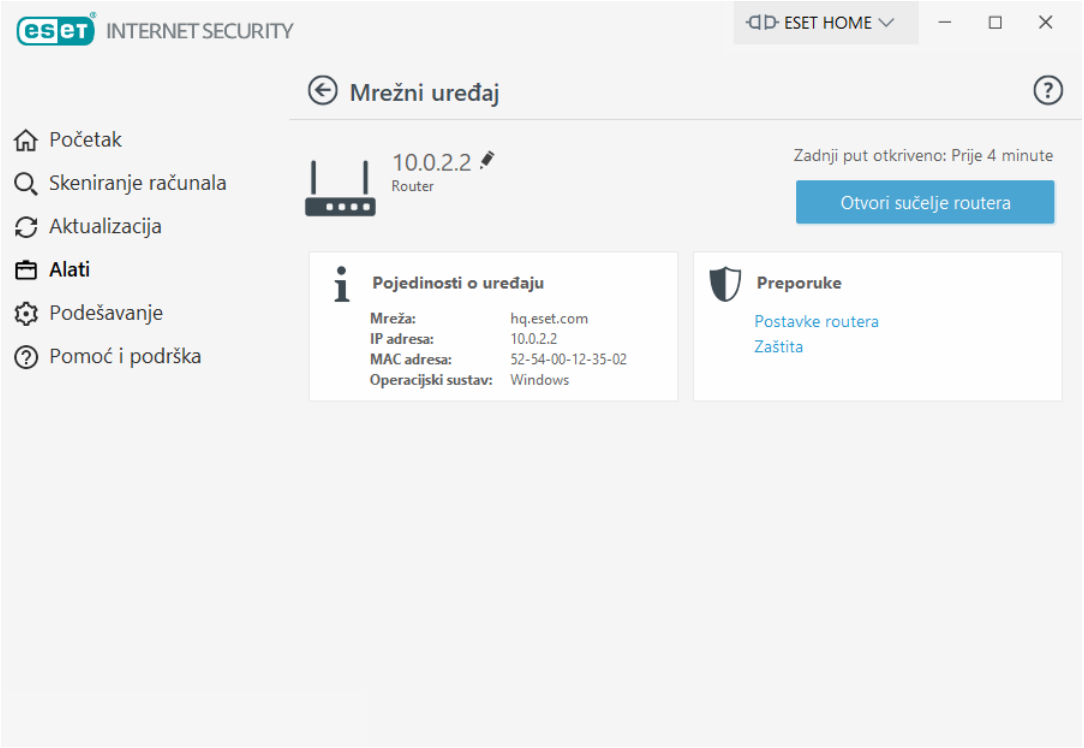
Ukloni iz povijesti – izbrišite uređaj s popisa uređaja. Ova opcija je dostupna samo za uređaje koji trenutačno nisu povezani na vašu mrežu.

Za svaku vrstu uređaja na raspolaganju su sljedeće radnje:

Router

Postavke routera – pristupajte postavkama routera iz web sučelja, iz mobilne aplikacije ili klikom na opciju **Otvori sučelje routera**. Ako vam je router dao davatelj internetskih usluga, možda ćete se trebati obratiti podršci davatelja internetskih usluga ili proizvođaču routera da biste riješili otkrivene sigurnosne probleme. Uvijek se pridržavajte odgovarajućih sigurnosnih mjera kako je navedeno u korisničkom vodiču routera.

Zaštita – Da biste zaštitili router i mrežu od mrežnih napada, slijedite osnovne preporuke navedene u nastavku.

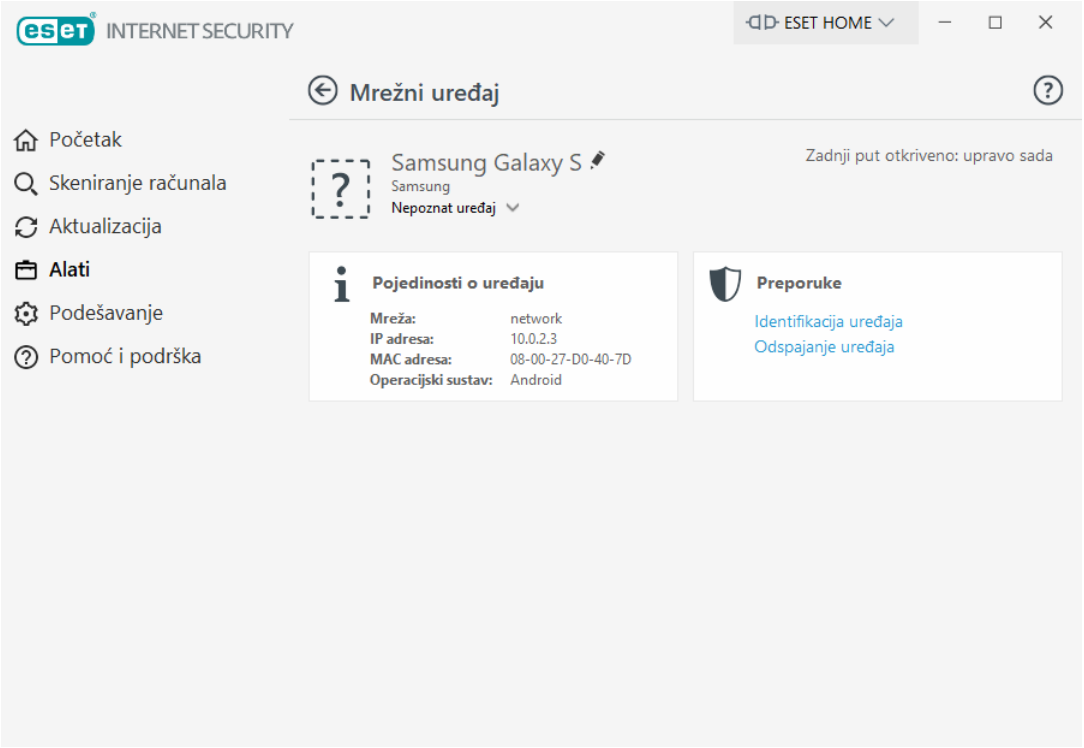


Mrežni uređaj

Identifikacija uređaja – ako niste sigurni za uređaj koji je povezan s vašom mrežom, provjerite naziv dobavljača ili proizvođača ispod naziva uređaja. To će vam pomoći da otkrijete o kakvom je uređaju riječ. Možete promijeniti naziv uređaja radi lakšeg prepoznavanja u budućnosti.

Odspajanje uređaja – ako niste sigurni je li povezani uređaj siguran za vašu mrežu ili uređaje, uredite pristup mreži za taj uređaj u postavkama routera ili promijenite lozinku mreže.

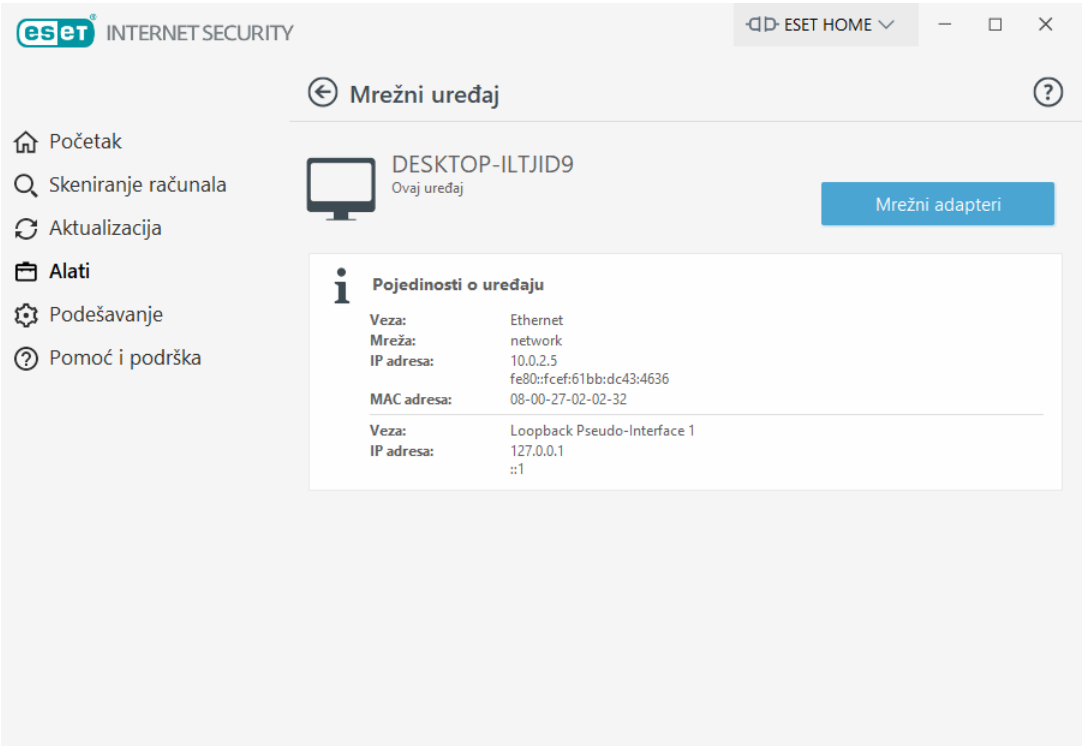
Zaštita – da biste zaštitili svoj uređaj od napada i zlonamjernog softvera, instalirajte mrežnu zaštitu na uređaju i pobrinite se da su operacijski sustav i instalirani softver uvijek nadograđeni. Da biste ostali zaštićeni, nemojte se povezivati s nezaštićenim Wi-Fi mrežama.



Ovaj uređaj

Ovaj uređaj predstavlja vaše računalo na mreži.

Mrežni adapteri – prikazuje informacije o vašim mrežnim adapterima.



Obavijesti | Mrežna provjera

U nastavku je popis nekoliko obavijesti koje se mogu prikazati kad ESET Internet Security otkrije neki problem ranjivosti na vašem routeru. Svaka obavijest sadrži kratak opis i pruža neko rješenje ili korake koje treba poduzeti kako bi se smanjio rizik ranjivosti vašeg routera. Ako vam promjene na routeru nisu poznate, preporučujemo da se obratite svojem proizvođaču routera ili davatelju internetskih usluga.

Pronađena je potencijalna slabost
Vaš router može sadržavati poznate slabosti koje mogu olakšati njegov napad i zloupotrebu. Nadogradite firmware routera.

Pronađena je slabost
Vaš router sadrži poznate slabosti koje olakšavaju njegov napad i zloupotrebu. Nadogradite firmware routera.

Pronađena je prijetnja
Vaš je router zaražen zlonamjernim softverom. Ponovno pokrenite router i ponovite skeniranje.

Slaba lozinka routera
Lozinka na vašem routeru slaba je i druge je osobe mogu lako pogoditi. Promijenite lozinku routera.

Zlonamjerno preusmjeravanje mreže
Čini se da je vaš internetski promet preusmjeren na zlonamjerne web stranice. To može značiti da je vaš router ugrožen. Promijenite postavku DNS servera na routeru.

Otvorene mrežne usluge
Vaš router pokreće mrežne usluge koje drugi mogu iskoristiti. To može biti uzrokovano lošom konfiguracijom ili ugroženim routerom. Provjerite konfiguraciju routera.

Osjetljive otvorene mrežne usluge
Vaš router pokreće osjetljive mrežne usluge koje drugi mogu iskoristiti. To može biti uzrokovano lošom konfiguracijom ili ugroženim routerom. Provjerite konfiguraciju routera.

Firmware je zastario
Firmver na vašem routeru zastario je i može sadržavati slabosti. Nadogradite firmver na routeru.

Zlonamjerna postavka routera
Ovaj DNS server koji vaš router upotrebljava je zlonamjeran i može vas slati na opasne web stranice. To može značiti da je vaš router ugrožen. Promijenite postavku DNS servera na routeru.

Mrežne usluge
Vaš router pokreće zajedničke mrežne usluge. Njih mreža treba i vjerojatno su sigurni. Provjerite konfiguraciju routera.

Alati u programu ESET Internet Security

Izbornik **Alati** sadrži module koji pojednostavnjuju administriranje programa i nude dodatne mogućnosti naprednim korisnicima. Ti alati su vidljivi samo ako u donjem desnom kutu kliknete **Više alata**.

Taj izbornik sadrži sljedeće alate:

 Dnevnici

 Sigurnosno izvješće

Pokrenuti procesi (ako je ESET LiveGrid® aktiviran u programu ESET Internet Security)

Mrežne veze (ako je firewall aktiviran u programu ESET Internet Security)

ESET SysInspector

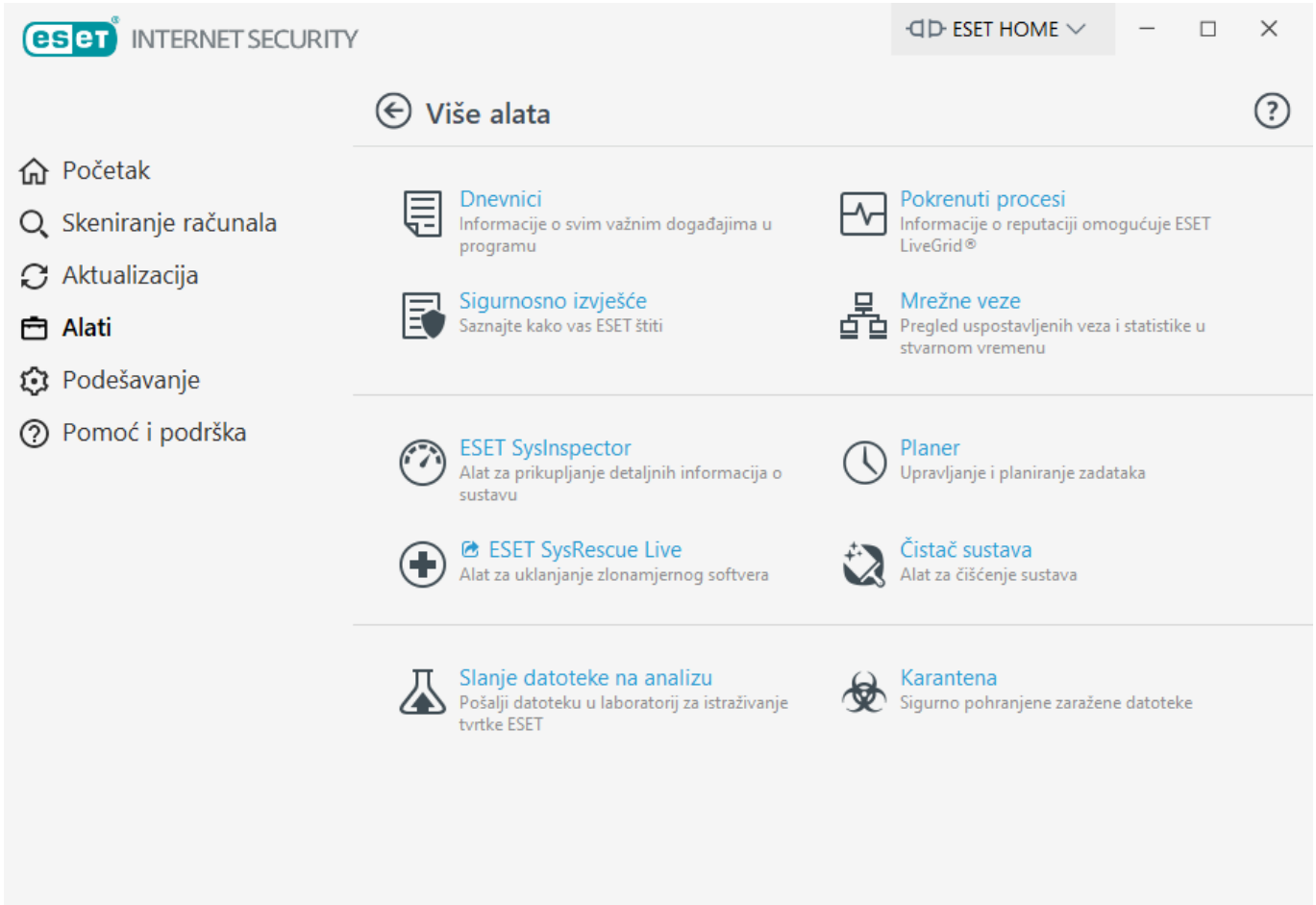
ESET SysRescue Live – Preusmjerava vas na stranicu ESET SysRescue Live, gdje možete preuzeti sliku CD-a/DVD-a za ESET SysRescue Live .iso.

Planer

Čistač sustava – Pomaže vam vratiti računalo u uporabno stanje nakon čišćenja prijetnje.

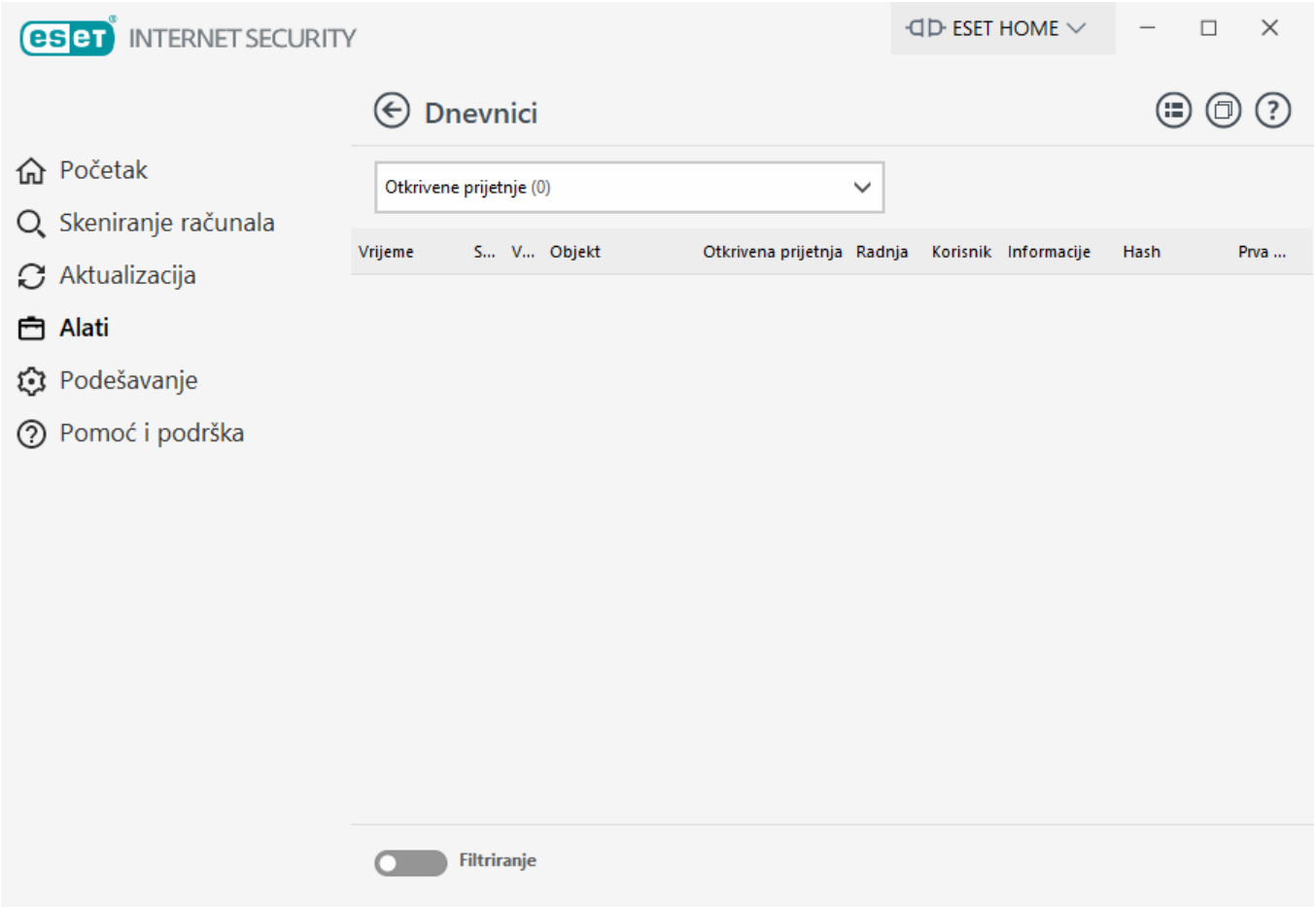
Slanje uzorka na analizu – Omogućuje slanje sumnjive datoteke na analizu u Laboratorij za istraživanje tvrtke ESET (možda neće biti dostupno ovisno o konfiguraciji za ESET LiveGrid®).

Karantena



Dnevnici

Dnevnici sadrže informacije o važnim događajima u programu koji su se pojavili i pružaju pregled otkrivenih prijetnji. Zapisivanje je ključan dio analize sustava, otkrivanja prijetnji i otklanjanja poteškoća. Zapisivanje se izvodi aktivno u pozadini bez korisničke intervencije. Podaci se bilježe na temelju trenutnih postavki opsega zapisivanja. Prikaz tekstualnih poruka i dnevnika moguć je izravno iz okruženja programa ESET Internet Security, kao i arhiviranje dnevnika.



Dnevnicima se pristupa iz glavnog prozora programa klikom na **Alati** > **Više alata** > **Dnevnici**. Odaberite željenu vrstu dnevnika s padajućeg izbornika **Dnevnik**. Dostupni su sljedeći dnevnici:

- **Otkrivene prijetnje** – u ovom dnevniku se navode detaljne informacije o otkrivenim prijetnjama i infiltracijama koje je otkrio program ESET Internet Security. Informacije dnevnika obuhvaćaju vrijeme otkrivanja, vrstu skenera, vrstu objekta, lokaciju objekta, naziv otkrivene prijetnje, provedenu radnju, ime korisnika prijavljenog u trenutku otkrivanja infiltracije, hash i prvo pojavljivanje. Neočišćene infiltracije su uvijek označene crvenim tekstom na svjetlo-crvenoj pozadini. Očišćene infiltracije su označene žutim tekstom na bijeloj pozadini. Neočišćene potencijalno nepoželjne aplikacije ili potencijalno nesigurne aplikacije su označene žutim tekstom na bijeloj pozadini.

- **Događaji** – sve važne radnje koje je obavio ESET Internet Security zabilježene su u dnevniku događaja. Dnevnik događaja sadrži informacije o događajima i pogreškama do kojih je došlo u programu Namijenjen je 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 prozoru prikazuju se rezultati svih prijašnjih skeniranja. Na popisu izvršenih skeniranja bit će prikazana i nedovršena skeniranja (prekinuta od strane korisnika). Dvokliknite bilo koju

stavku za prikaz detalja dotičnog skeniranja.

- **HIPS** – Sadrži zapise određenih HIPS pravila označenih za zapisivanje. Protokol pokazuje aplikaciju koja je pokrenula operaciju, rezultat (je li pravilo bilo dopušteno ili zabranjeno) i naziv pravila.

- **Mrežna zaštita** – dnevnik mrežne zaštite prikazuje sve udaljene napade koje su otkrili firewall, zaštita od mrežnog napada (IDS) i zaštita od botneta. Ovdje možete pronaći informacije o svakom napadu na vaše računalo. U stupcu Događaj nalazi se popis otkrivenih napada. Stupac Izvor sadrži dodatne informacije o napadaču. Stupac Protokol otkriva komunikacijski protokol upotrijebljen u napadu. Analiza dnevnika mrežne zaštite može vam pomoći da na vrijeme otkrijete pokušaje infiltracije sustava kako biste spriječili neovlašten pristup sustavu. Više detalja o mrežnim napadima potražite u odjeljku IDS i napredne opcije.

- **Filtrirane web stranice** – Taj je popis koristan kada želite pregledati popis web stranica koje je blokirala Zaštita web pristupa ili Roditeljska kontrola. Svaki dnevnik uključuje vrijeme, URL adresu, korisnika i aplikaciju koja je stvorila vezu s određenim web-mjestom.

- **Antispam zaštita** – Sadrži zapise koji se odnose na poruke e-pošte označene kao spam poruke.

- **Roditeljska kontrola** – Prikazuje web stranice koje blokira ili dopušta Roditeljska kontrola. Stupci Vrsta podudaranja i Vrijednosti podudaranja sadrže informacije o tome kako su primijenjena pravila filtriranja.

- **Kontrola uređaja** – Sadrži zapise izmjenjivih medija ili uređaja koji su priključeni na računalo. U dnevnik se zapisuju samo uređaji s odgovarajućim pravilima kontrole uređaja. Ako pravilo ne odgovara priključenom uređaju, neće se stvoriti stavka dnevnika za priključeni uređaj. Možete vidjeti i pojedinosti kao što su vrsta uređaja, serijski broj, naziv proizvođača i veličina medija (ako je dostupno).

- **Zaštita web kamere** – Sadrži zapise o aplikacijama koje su blokirane zaštitom web kamere.

Odaberite sadržaj bilo kojeg dnevnika i pritisnite **CTRL + C** kako biste ga kopirali u međuspremnik. Držite **CTRL** ili **SHIFT** da 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 filtriranje za određene stavke u dnevniku.

- **Aktiviraj filtar** – Aktivira postavke filtra.

- **Deaktiviraj filtar** – Poništava sve postavke filtra (kao što je gore opisano).

- **Kopiraj / Kopiraj sve** – kopira informacije o odabranim zapisima u prozoru.

- **Ukloni / Ukloni sve** – briše odabrane zapise ili sve prikazane zapise. Ova radnja zahtijeva administratorske ovlasti.

- **Izvoz / Izvezi sve** – izvozi informacije o odabranim zapisima ili svim zapisima u XML formatu.

- **Pronađi / Pronađi sljedeće / Pronađi prethodno** – nakon što kliknete ovu opciju, možete definirati kriterije za filtriranje da biste istaknuli određen unos s pomoću prozora Filtriranje dnevnika.

- **Opis otkrivene prijetnje** – otvara enciklopediju prijetnji tvrtke ESET koja sadrži detaljne informacije o opasnostima i simptomima zabilježene infiltracije.

- **Stvori izuzetak** – Stvorite novi izuzetak za detekciju pomoću čarobnjaka (nije dostupno za detekciju zlonamjernog softvera).

Filtriranje dnevnika

Kliknite **Filtriranje** u izborniku **Alati** > **Više alata** > **Dnevnici** za određivanje kriterija za filtriranje.

Značajka filtriranja dnevnika pomoći će vam da pronađete informacije koje tražite, posebice kada imate mnogo zapisa. Omogućuje vam sužavanje zapisa dnevnika, na primjer ako tražite određenu vrstu događaja, status ili vremensko razdoblje. Možete filtrirati zapise dnevnika navođenjem određenih opcija pretraživanja; u prozoru Dnevnika prikazat će se samo relevantni zapisi (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 zapisa iz padajućeg izbornika **Vrste zapisa 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 (riječ ili dio riječi). Prikazat će se samo zapisi koji sadrže taj niz. Ostali zapisi 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 zapisa

Odaberite jednu vrstu zapisa dnevnika ili više njih u padajućem izborniku:

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje 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).

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 potvrdni 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. Dnevnici 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 Internet Security može se pristupiti s glavnog prozora programa. Kliknite **Podešavanje** > **Napredno podešavanje** > **Alati** > **Dnevnici**. 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 konfiguriranje 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, firewallitd.).

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 dnevnike – Ako se označi, dnevnici će se automatski defragmentirati ako je postotak veći od onog definiranog vrijednošću značajke **Ako broj nekorištenih zapisa prelazi (%)**.

Kliknite **Optimiziraj** za pokretanje defragmentiranja dnevnika. Tijekom ovog procesa uklanjaju se svi prazni unosi u dnevnik, što poboljšava radne karakteristike i brzinu obrade dnevnika. Ovo poboljšanje primjećuje se osobito ako dnevnici sadrže velik broj unosa.

Mogućnost **Aktiviraj tekstualni protokol** omogućuje pohranu dnevnika u drugom formatu, zasebno od dnevnika:

- **Ciljni direktorij** – direktorij u kojem će se pohraniti dnevnici (odnosi se samo na tekstualne/CSV datoteke). Svaki odjeljak dnevnika ima vlastitu datoteku s unaprijed definiranim nazivom datoteke (primjerice, virlog.txt za odjeljak **Otkrivene prijetnje** u dnevniku ako želite upotrebljavati običan format tekstualne datoteke za pohranu dnevnika).

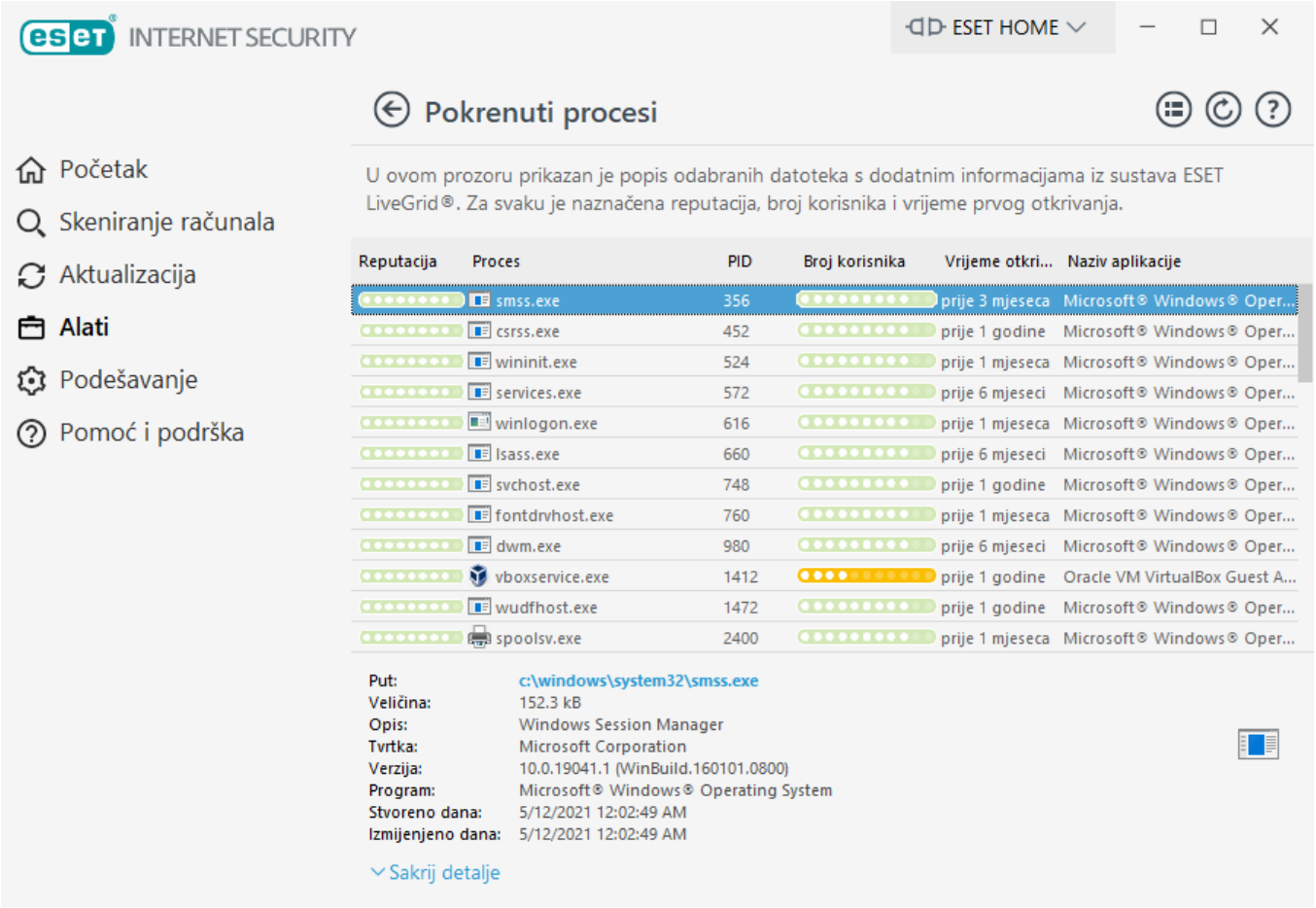
- **Vrsta** – ako odaberete format datoteke **Tekst**, dnevnici će se pohraniti u tekstualnoj datoteci i podaci će se razdvojiti na kartice. Isto se primjenjuje za podatke odvojene zarezom u **CSV** datoteci. Ako odaberete **Događaj**, dnevnici će se umjesto u datoteku pohranjivati u dnevnik Windows Event (može se pregledati uz pomoć programa Event Viewer na upravljačkoj ploči).

- **Izbriši sve dnevnike** – Briše sve pohranjene dnevnike koji su trenutačno odabrani u padajućem izborniku **Vrsta**. Prikazat će se obavijest o uspješnom brisanju dnevnika.

> Kako biste pomogli u bržem rješavanju problema, tvrtka ESET od vas može zatražiti dnevnike 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.

Procesi koji se izvršavaju

Procesi koji se izvršavaju prikazuju programe i procese pokrenute na računalu i ESET se odmah i neprekidno obavještava o novim infiltracijama. ESET Internet Security pruža detaljne informacije o procesima koji se izvršavaju kako bi zaštitio korisnike pomoću tehnologije ESET LiveGrid®.



Reputacija – U većini slučajeva ESET Internet Security i tehnologija ESET LiveGrid® dodjeljuju razine rizika objektima (datotekama, procesima, ključevima registra itd.) s pomoću serije heurističkih pravila koja provjeravaju značajke svakog objekta i zatim procjenjuju moguću zlonamjernu aktivnost. Prema toj heuristici objektima se dodjeljuje razina rizika od 1 – Dobro (zeleno) do 9 – Rizično (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.

Poznate aplikacije označene kao Dobro (zeleno) definitivno su čiste (nalaze se na popisu pouzdanih adresa) i neće biti skenirane kako bi se poboljšale performanse.

PID – Identifikacijski broj procesa može se upotrijebiti kao parametar u raznim funkcijama kao što je podešavanje prioriteta procesa.

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.

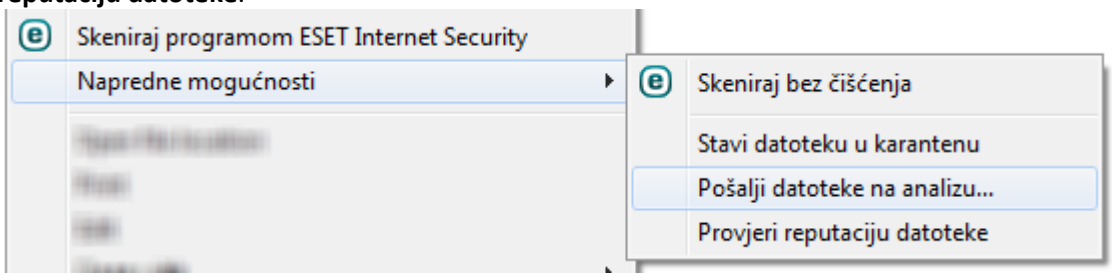
Aplikacija koja je označena kao Nepoznata (narančasto) nije nužno zlonamjerni softver. Obično je samo riječ o novijoj aplikaciji. Ako za neku datoteku niste sigurni, možete poslati datoteku na analizu u Laboratorij za istraživanje tvrtke ESET. Ako se pokaže da je datoteka ustvari zlonamjeran program, njezino će se otkrivanje dodati u jednu od sljedećih nadogradnja.

Naziv aplikacije – Zadani naziv programa ili procesa.

Kliknite aplikaciju za prikaz sljedećih detalja te aplikacije:

- **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/Izmijenjeno** – Datum i vrijeme stvaranja (izmjene).

Možete provjeriti i reputaciju datoteka koje ne rade kao pokrenuti programi/procesi. Da biste to učinili, kliknite na njih desnom tipkom miša u eksploreru za datoteke i odaberite **Napredne opcije** > **Provjeri reputaciju datoteke**.



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.
- **Blokirane web stranice u Roditeljskoj kontroli** – Prikazuje broj blokiranih web stranica u Roditeljskoj kontroli.
- **Otkrivene potencijalno nepoželjne aplikacije** – prikazuje broj potencijalno nepoželjnih aplikacija (PUA).
- **Otkrivene neželjene poruke e-pošte** – Prikazuje broj potencijalno neželjenih poruka e-pošte.
- **Blokirani pristupi web kameri** – prikazuje broj blokiranih pristupa web kameri.
- **Zaštićene veze s internetskim bankarstvom** – prikazuje broj zaštićenih pristupa web stranicama putem funkcije zaštita bankarstva i plaćanja.
- **Pregledani dokumenti** – Prikazuje broj skeniranih objekata dokumenata.
- **Skenirane aplikacije** – Prikazuje broj skeniranih izvršnih objekata.

- **Pregledani 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.

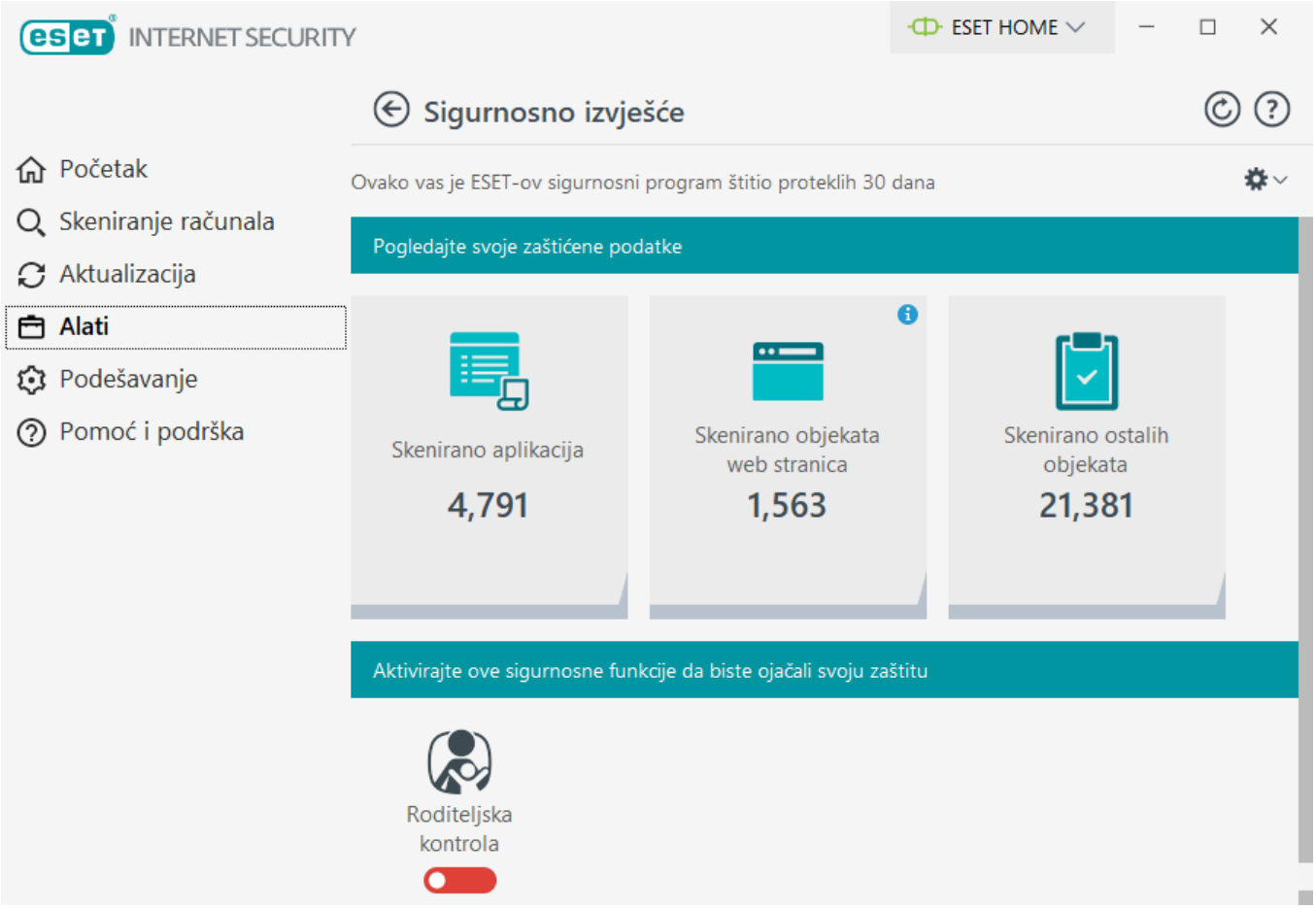
Redoslijed ovih kategorija temelji se na numeričkoj vrijednosti od najviše prema najnižoj. Kategorije s nultom vrijednošću nisu prikazane. Kliknite **Prikaži više** za proširivanje i prikaz skrivenih kategorija.

Zadnji dio sigurnosnog izvješća nudi mogućnost aktiviranja sljedećih funkcija:

- Roditeljska kontrola
- Anti-Theft

Kada je ova funkcija aktivirana, više se ne prikazuje kao nefunkcionalna u sigurnosnom izvješću.

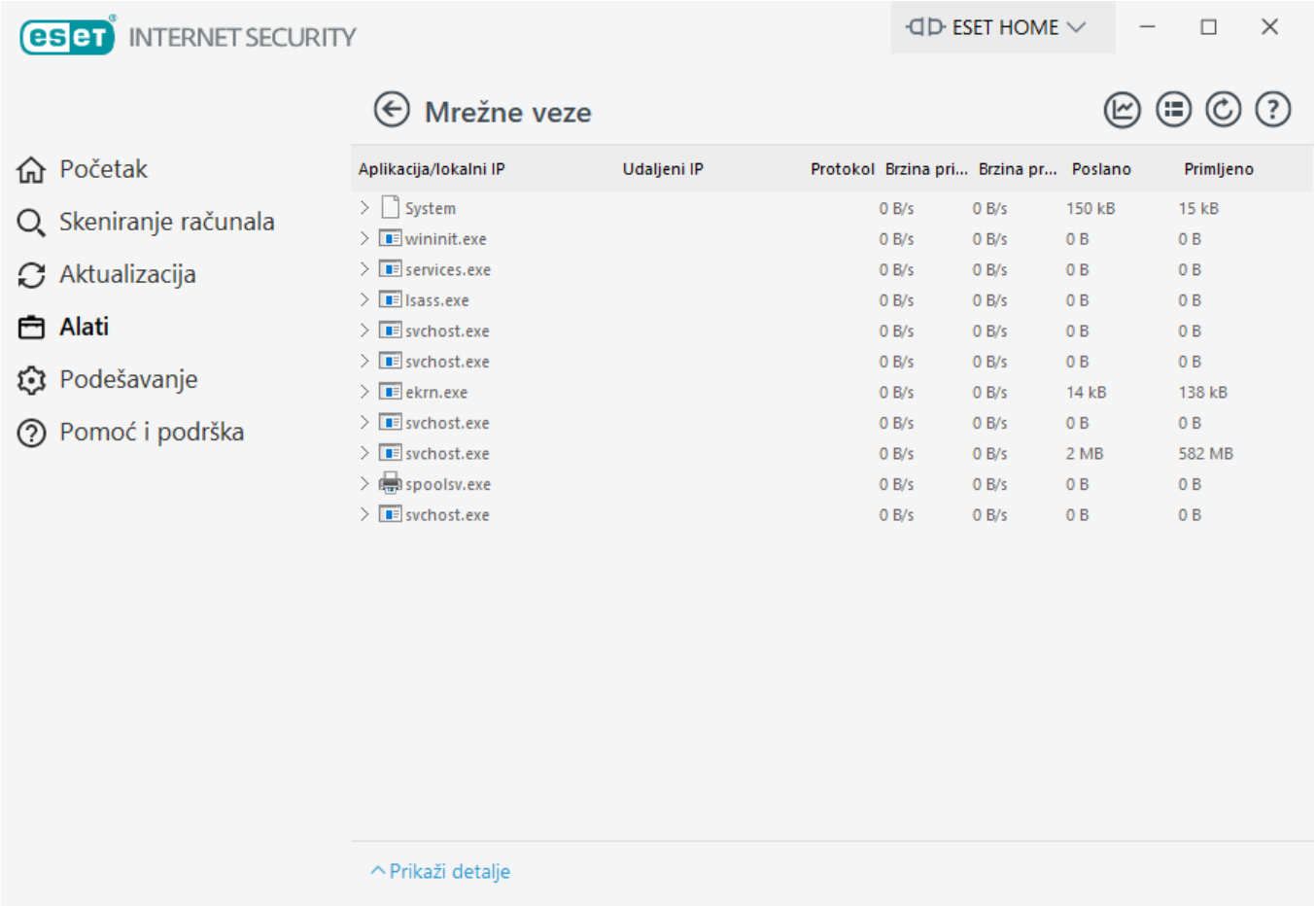
Ako kliknite zupčanik u gornjem desnom kutu, možete **aktivirati/deaktivirati obavijesti sigurnosnog izvješća** ili odabrati hoće li se prikazivati podaci za zadnjih 30 dana ili za razdoblje otkada je program aktiviran. Ako je ESET Internet Security instaliran manje od 30 dana, moguće je odabrati samo 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** > **Obavijesti** > **Interaktivna upozorenja** > **Poruke za potvrdu** > **Uredi**.

Mrežne veze

U odjeljku mrežnih veza prikazuje se popis aktivnih veza i veza na čekanju. To vam olakšava regulaciju svih aplikacija koje uspostavljaju odlazne veze.



Kliknite ikonu grafikona da biste otvorili Mrežnu aktivnost.

U prvom retku se prikazuju naziv aplikacije i brzina prijenosa podataka. Za prikaz popisa veza koje je uspostavila aplikacija (i za detaljne informacije) kliknite **>**.

Stupci

Aplikacija/lokalni IP – Naziv aplikacije, lokalne IP adrese i komunikacijski portovi.

Udaljeni IP – IP adresa i broj porta određenog udaljenog računala.

Protokol – Korišteni protokol prijenosa.

Brzina prijenosa / brzina preuzimanja – Trenutačna brzina prijenosa odlaznih i dolaznih podataka.

Poslano/primljeno – Količina podataka razmijenjenih tijekom trajanja veze.

Prikaži detalje – Odaberite ovu opciju za prikaz detaljnih informacija o odabranim vezama.

Kliknite vezu desnom tipkom miša da biste vidjeli dodatne mogućnosti koje obuhvaćaju:

Razriješi nazive hostova – Ako je moguće, sve mrežne adrese prikazuju se u DNS obliku, a ne u brojčanom obliku IP adresa.

Prikaži samo veze putem TCP protokola – Na popisu se prikazuju samo veze koje pripadaju TCP protokolu.

Prikaži veze koje se osluškuju – Odaberite ovu opciju da biste prikazali samo veze u kojima komunikacija trenutno nije uspostavljena, ali je sustav otvorio port i čeka vezu.

Prikaži veze unutar računala – Odaberite ovu opciju da biste prikazali samo one veze gdje je udaljena strana lokalni sustav – takozvane localhost veze.

Brzina osvježavanja – Odaberite učestalost osvježavanja aktivnih veza.

Osvježi sada – ponovno učitava prozor **Mrežne veze**.

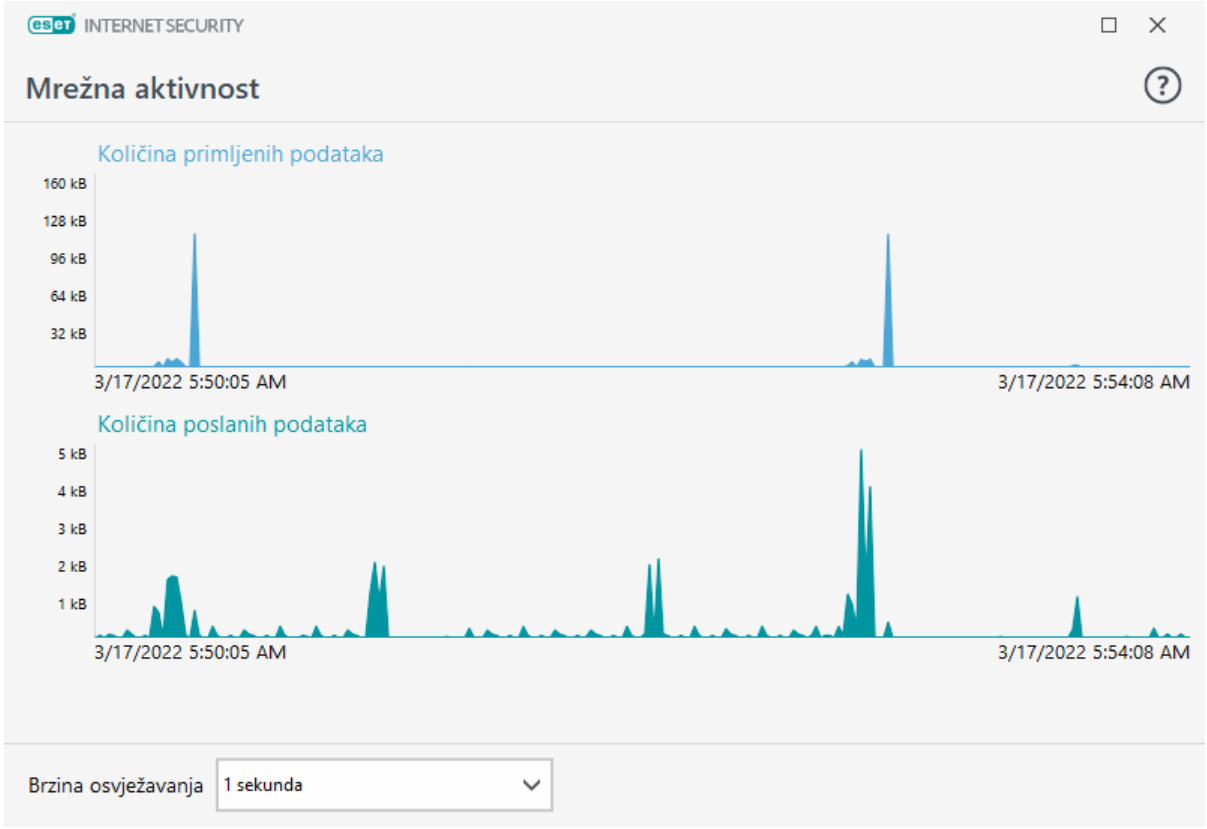
Sljedeće mogućnosti dostupne su samo ako kliknete na aplikaciju ili proces, ne na aktivnu vezu:

Privremeno zabrani komunikaciju za proces – Time se odbijaju trenutačne veze za određenu aplikaciju. Ako se uspostavi nova veza, firewall primjenjuje unaprijed definirano pravilo. Opis postavki možete pronaći u odjeljku Konfiguriranje i korištenje pravila.

Privremeno dopusti komunikaciju za proces – Time se dopuštaju trenutačne veze za određenu aplikaciju. Ako se uspostavi nova veza, firewall primjenjuje unaprijed definirano pravilo. Opis postavki možete pronaći u odjeljku Konfiguriranje i korištenje pravila.

Mrežna aktivnost

Da biste vidjeli trenutačnu **mrežnu aktivnost** u obliku grafikona, kliknite **Alati** > **Više alata** > **Mrežne veze** i kliknite ikonu grafikona . Na dnu grafikona nalazi se vremenska crta koja bilježi mrežnu aktivnost u stvarnom vremenu na temelju odabranog vremenskog raspona. Da biste promijenili vremenski raspon, odaberite primjenjivu vrijednost iz padajućeg izbornika **Brzina osvježavanja**.



Dostupne su sljedeće opcije:

- **1 sekunda** – Graf se osvježava svake sekunde, a vremenska crta pokriva posljednjih 4 minuta.
- **1 minuta (zadnja 24 sata)** –Graf se osvježava svake minute, a vremenska crta pokriva posljednja 24 sata.
- **1 sat (zadnji mjesec)** – Graf se osvježava svakog sata, a vremenska crta pokriva posljednjih mjesec dana.

Okomita os grafikona predstavlja količinu primljenih ili poslanih podataka. Zadržite pokazivač miša iznad grafikona da biste vidjeli točnu količinu primljenih/poslanih podataka u određeno vrijeme.

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 softverom. Da biste saznali kako upotrebljavati ESET SysInspector, pogledajte ESET SysInspector pomoć na mreži.

Prozor ESET SysInspector prikazuje sljedeće podatke o 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 odabranu prijavu u sustav ESET SysInspector. Možete i desnom tipkom miša kliknuti dotični dnevnik i odabrati mogućnost **Prikaži** na kontekstnom izborniku.
- **Usporedi** – uspoređuje dva postojeća dnevnika.
- **Stvori** – Stvara novi dnevnik. Pričekajte dok se ESET SysInspector ne generira (status **Stvoreno**) prije nego što pokušate pristupiti dnevniku.
- **Izbriši** – Briše odabrane dnevnike 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).
- **Usporedi** – uspoređuje dva postojeća dnevnika.
- **Stvori** – Stvara novi dnevnik. Pričekajte dok se ESET SysInspector ne generira (status **Stvoreno**) prije nego što pokušate pristupiti dnevniku.
- **Izbriši** – Briše odabrane dnevnike s popisa.
- **Izbriši sve** – Briše sve dnevnike.
- **Izvezi** – Izvozi dnevnik u .xml datoteku ili komprimiranu .xml datoteku. Dnevnik se izvozi u C:\ProgramData\ESET\ESET Security\SysInspector.

Planer

Planer upravlja planiranim zadacima s unaprijed definiranom konfiguracijom i svojstvima i pokreće ih.

Planeru se može pristupiti iz glavnog prozora programa ESET Internet Security klikom na **Alati** > **Više alata** > **Planer**. **Planer** sadrži popis svih zakazanih zadataka i njihova konfiguracijska svojstva, primjerice unaprijed definirani datum i vrijeme te profil skeniranja koji se upotrebljava.

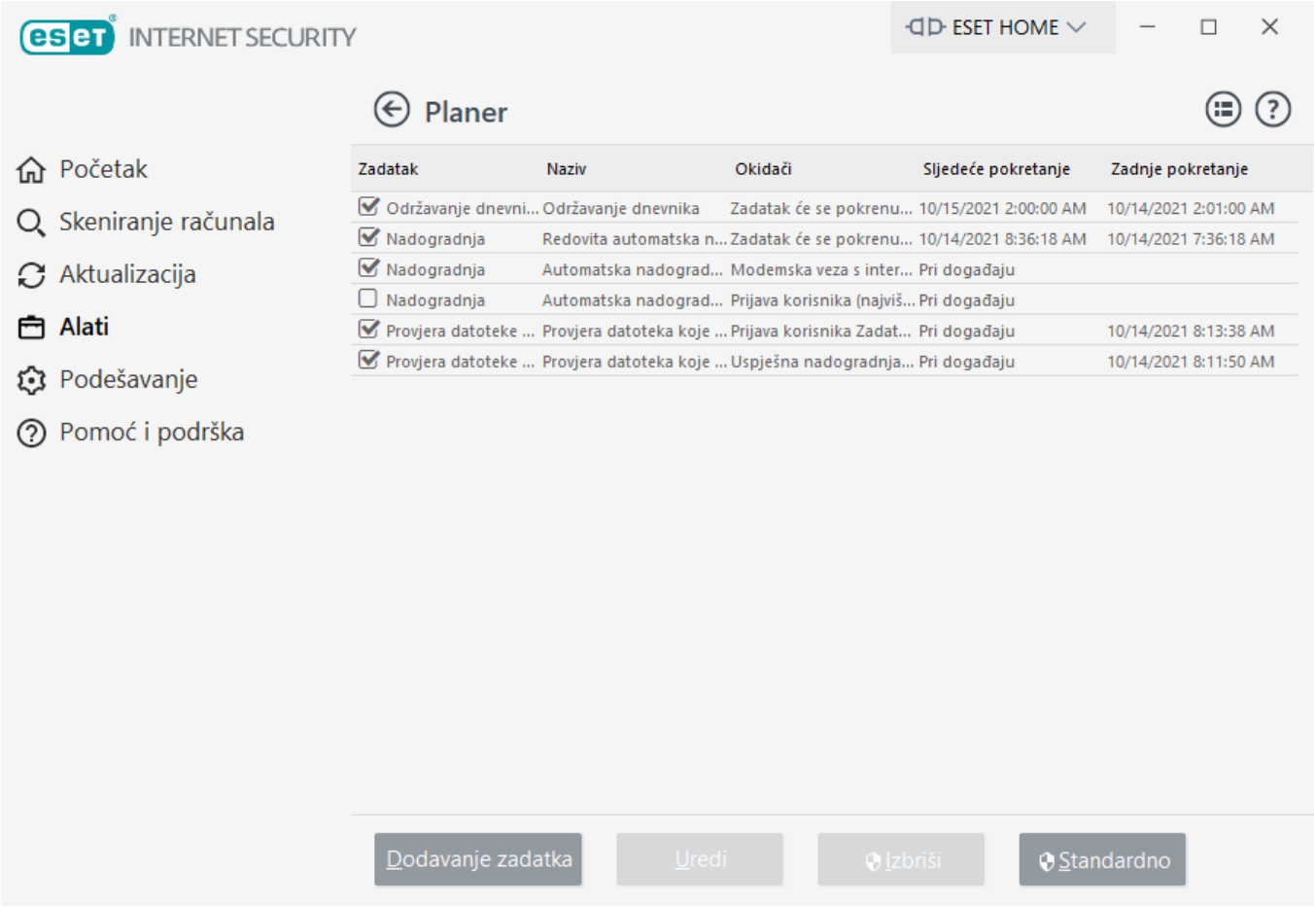
Planer služi za planiranje sljedećih zadataka: nadogradnje modula, poslova skeniranja, provjere datoteka pri pokretanju sustava te održavanja dnevnika. Možete dodavati i brisati zadatke izravno iz glavnog prozora Planera (klikom na gumb **Dodaj zadatak** ili **Izbriši** koji se nalaze u donjem dijelu). Možete vratiti popis planiranih zadataka na standardnu postavku i izbrisati sve promjene klikom na **Standardno**. 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. Potvrdnim 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 pokretačkih datoteka** (nakon uspješne nadogradnje modula za otkrivanje virusa)

Da biste uredili konfiguraciju postojećeg planiranog zadatka (standardnu ili korisnički definiranu), desnom tipkom miša kliknite zadatak i kliknite **Uredi** ili odaberite zadatak koji želite izmijeniti pa kliknite **Uredi**.



Dodavanje novog zadatka

1. Kliknite **Dodaj zadatak** na dnu prozora.
2. Unesite naziv zadatka.
3. Odaberite željeni zadatak s padajućeg izbornika:
   - **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
   - **Održavanje dnevnika** – Dnevnici 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.
- **Nadogradnja** – Planira zadatak nadogradnje nadogradnjom modula.

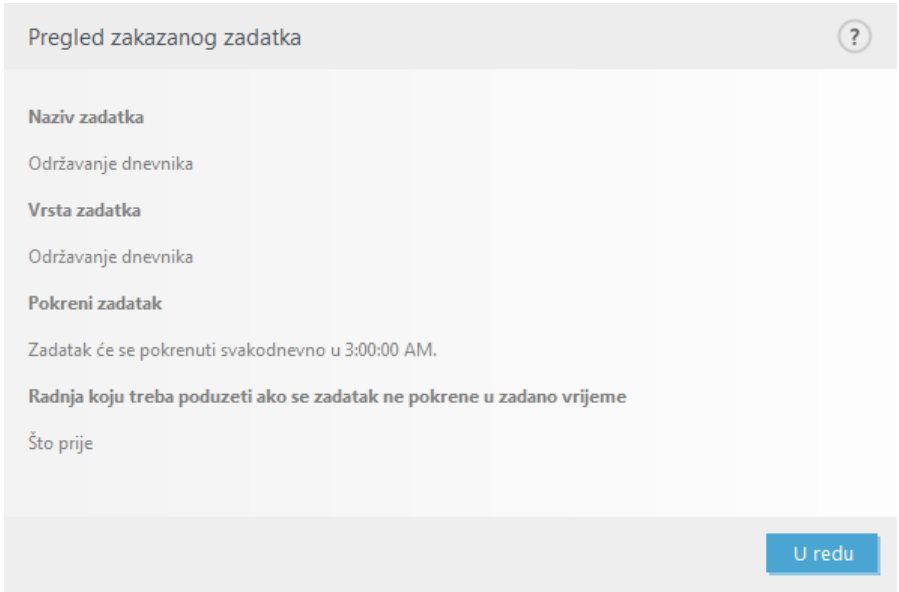
4. Kliknite traku klizača uz **Aktiviraj** ako želite aktivirati zadatak (to možete učiniti kasnije označavanjem/poništavanjem potvrdnog okvira na popisu planiranih zadataka), a zatim kliknite **Dalje** i odaberite jednu od vremenskih mogućnosti:

- **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 zadatka**. 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 je vrijeme od posljednjeg pokretanja više od (sati)** – predstavlja vrijeme proteklo od prvog preskočenog izvođenja zadatka. Ako se ovo vrijeme prekorači, zadatak će se odmah pokrenuti. Postavite vrijeme pomoću okretnog gumba u nastavku.

Možete pregledati planirane zadatke desnim klikom i odabirom **Prikaži detalje zadatka**.



Opcije planiranog skeniranja

U ovom prozoru možete odrediti napredne opcije za zadatak zakazanog skeniranja računala.

Da biste pokrenuli skeniranje bez radnje čišćenja, kliknite **Napredne postavke** i odaberite **Skeniraj bez čišćenja**. Povijest skeniranja sprema 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 pomoću padajućeg izbornika možete postaviti radnju tako da se automatski izvršava nakon što se skeniranje dovrši:

- **Bez radnje** – Kada skeniranje završi, neće se izvršiti nijedna radnja.
- **Isključi** – Kada skeniranje završi, računalo se isključuje.
- **Ponovno pokreni** – Zatvara sve otvorene programe i restarta računalo kada završi skeniranje.
- **Ponovno pokreni po potrebi** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Prisilno ponovno pokreni** – prisilno zatvara sve otvorene programa bez čekanja interakcije korisnika i ponovno pokreće računalo nakon što se skeniranje dovrši.
- **Prisilno ponovno pokrenite ako je potrebno** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **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.

> Radnje **Mirovanje** ili **Hibernacija** dostupne su na temelju postavki operacijskog sustava na vašem računalu za uštedu energije i stanje mirovanja ili na temelju mogućnosti stolnog/prijenosnog računala. Imajte na umu da računalo koje je u stanju mirovanja i dalje radi. I dalje pokreće osnovne funkcije i troši električnu energiju dok se napaja putem baterije. Da bi baterija dulje trajala, na primjer, kada se nalazite izvan ureda, preporučujemo da upotrijebite opciju Hibernacija.

Odaberite opciju **Skeniranje se ne može otkazati** da biste korisnicima koji nemaju posebne ovlasti onemogućili prekidanje radnji koje se poduzimaju 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.

Također pogledajte Napredak skeniranja.

Pregled zakazanog zadatka

Dijaloški prozor prikazuje detaljne informacije o označenim zakazanim zadacima kada dvokliknete na prilagođeni zadatak ili desnim klikom kliknete na prilagođeni zadatak planera i kliknete **Prikaži detalje zadatka**.

Pojedinosti zadatka

Upišite **naziv zadatka**, odaberite jednu od opcija **vrste zadataka**, a zatim kliknite **Dalje**:

- **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
- **Održavanje dnevnika** – Dnevnici 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.
- **Nadogradnja** – Planira zadatak nadogradnje nadogradnjom modula.

Vrijeme pokretanja zadatka

Zadatak će se izvršavati opetovano u navedenim vremenskim intervalima. Odaberite jednu od vremenskih mogućnosti:

- **Jednom** – Zadatak će se izvršiti samo jednom, na unaprijed definirani datum i u unaprijed definirano vrijeme.
- **Opetovano** – Zadatak će se izvršavati u navedenim vremenskim intervalima (u satima).
- **Svakodnevno** – Zadatak će se izvršavati svakog dana u isto vrijeme.
- **Tjedno** – Zadatak će se izvršavati jednom ili nekoliko puta tjedno i to u odabrane dane i odabrano vrijeme.
- **Pri događaju** – Zadatak će se izvršiti nakon pojave određenog događaja.

Nemoj izvršavati zadatak ako računalo koristi bateriju – Zadatak se neće pokrenuti ako se računalo u trenutku pokretanja zadatka napaja iz baterije. To vrijedi i za računala koja se napajaju iz UPS-a.

Vrijeme pokretanja zadatka – jednom

Pokretanje zadatka – Određeni zadatak pokrenut će se samo jednom na određeni datum i u određeno vrijeme.

Vrijeme pokretanja zadatka – svakodnevno

Zadatak će se izvršavati svakog dana u isto vrijeme.

Vrijeme pokretanja zadatka – tjedno

Zadatak će se iznova pokretati svaki tjedan na odabrani dan ili dane i u odabrano vrijeme.

Vrijeme pokretanja zadatka – pokretanje prilikom događaja

Zadatak će se pokrenuti prilikom jednog od sljedećih događaja:

- **Prilikom svakog pokretanja računala**
- **Svakodnevno prilikom prvog pokretanja računala**
- **Modemska veza s internetom/VPN-om**
- **Uspješna nadogradnja modula**
- **Uspješna nadogradnja programa**
- **Prijava korisnika**
- **Otkrivanje prijetnji**

Prilikom zakazivanja zadatka koji će se pokrenuti s pojavom nekog događaja, možete navesti minimalni interval između dva dovršenja zadatka. Ako se, primjerice, na računalo prijavljujete nekoliko puta dnevno, odaberite 24 sata da bi se taj zadatak izvršio samo prilikom prve prijave u danu, a zatim ponovno sljedećeg dana.

Preskočeni zadatak

Zadatak se može preskočiti kada se računalo napaja putem baterije ili je isključeno. Odaberite kada se preskočeni zadatak treba izvršiti putem jedne od ovih opcija i kliknite **Dalje**:

- **U sljedećem zakazanom terminu** – zadatak će se pokrenuti ako je računalo uključeno u sljedećem zakazanom terminu.
- **Što prije** – zadatak će se pokrenuti kada je računalo uključeno.
- **Odmah, ako je vrijeme od posljednjeg zakazanog pokretanja više od (sati)** – predstavlja vrijeme proteklo od prvog preskočenog izvođenja zadatka. Ako se ovo vrijeme prekorači, zadatak će se odmah pokrenuti.

Odmah ako vrijeme od posljednjeg zakazanog pokretanja premašuje (u satima) – primjeri

Primjer zadatka je postavljen za izvođenje više puta svakih sat vremena. Opcija **Odmah, ako je vrijeme od zadnjeg zakazanog izvođenja dulje od (sati)** je odabrana i prekoračeno vrijeme je postavljeno na dva sata. Zadatak se pokreće u 13:00 h, a po završetku računalo odlazi u stanje mirovanja:

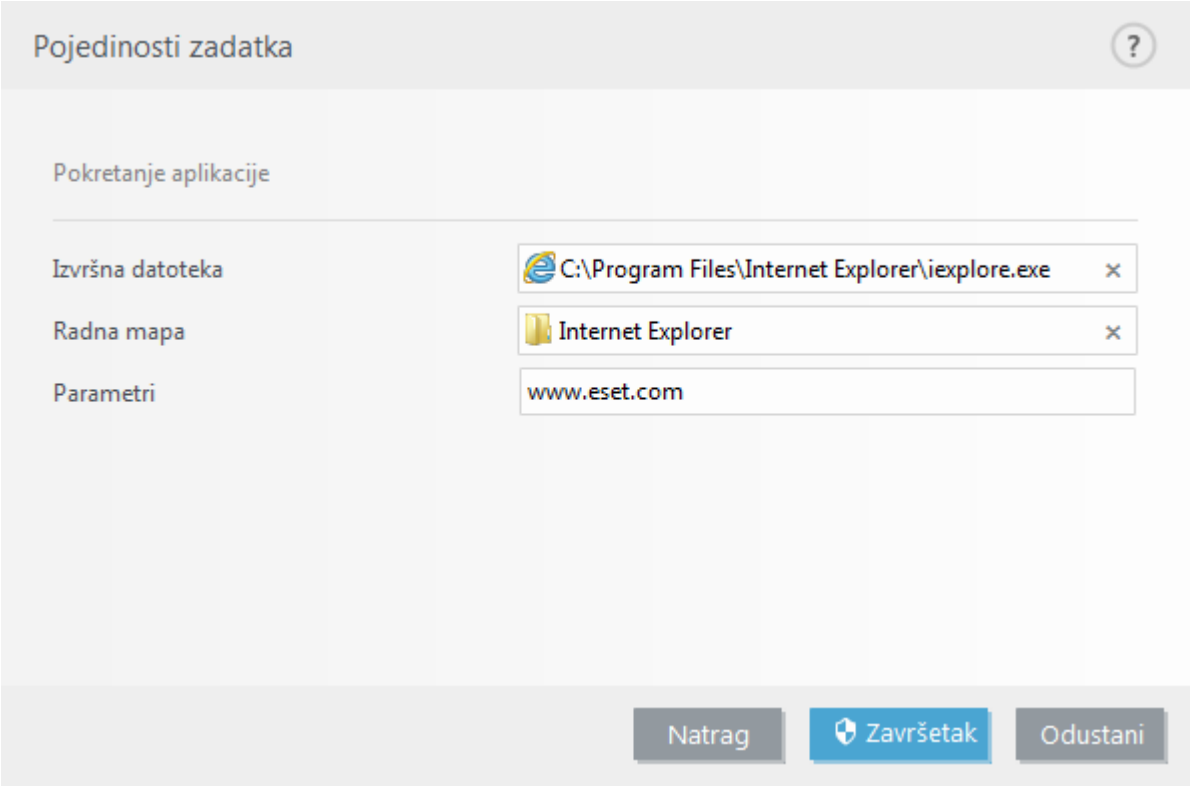
- Računalo se budi u 15:30 h. Prvo preskočeno pokretanje zadatka je bilo u 14:00 h. Prošlo je samo 1,5 sata od 14:00 h, tako da će se zadatak pokrenuti u 16:00 h.
- Računalo se budi u 16:30 h. Prvo preskočeno pokretanje zadatka je bilo u 14:00 h. Prošla su dva i pol sata od 14:00 h, tako da će se zadatak odmah pokrenuti.

Detalji o zadatku – nadogradnja

Ako program želite aktualizirati pomoću dva aktualizacijska servera, morate stvoriti dva različita aktualizacijska profila. Ako prvi server ne uspije u preuzimanju datoteka aktualizacije, program će se automatski prebaciti na drugi server. To je primjerice pogodno za prijenosna računala čija se aktualizacija obično vrši putem aktualizacijskog servera na lokalnom LAN-u, no njihovi se vlasnici često povezuju s internetom pomoću drugih mreža. Dakle, ako prvi profil ne uspije, drugi će automatski preuzeti aktualizacijske datoteke s ESET-ovih aktualizacijskih servera.

Detalji o zadatku – pokretanje aplikacije

Ovaj zadatak zakazuje pokretanje vanjske aplikacije.



Izvršna datoteka – Odaberite izvršnu datoteku iz stabla direktorija, kliknite opciju **...** ili unesite put ručno.

Radna mapa – Definirajte radni direktorij vanjske aplikacije. Sve privremene datoteke odabrane **Izvršne datoteke** stvorit će se u tom direktoriju.

Parametri – Parametri naredbenog retka za aplikaciju (nije obavezno).

Kliknite **Završetak** da biste primijenili zadatak.

Čistač sustava

Čistač sustava alat je koji vam pomaže vratiti računalo u uporabno stanje nakon čišćenja prijetnje. Zlonamjerni softver može onemogućiti uslužne programe sustava kao što su Registry Editor, upravitelj zadataka ili ažuriranja za sustav Windows. Čistač sustava vraća standardne vrijednosti i postavke za određeni sustav jednim klikom.

Čistač sustava prijavljuje probleme iz pet kategorija postavki:

- **Sigurnosne postavke**: promjene u postavkama koje mogu uzrokovati povećanu ranjivost vašeg računala, poput ažuriranja sustava Windows
- **Postavke sustava**: promjene u postavkama sustava koje mogu promijeniti ponašanje vašeg računala, poput pridruživanja datoteka
- **Izgled sustava**: postavke koje mijenjaju izgled sustava, kao što je pozadina radne površine
- **Deaktivirane funkcije**: važne funkcije i aplikacije koje se mogu deaktivirati
- **Vraćanje sustava Windows**: postavke za funkciju Vraćanje sustava Windows koja vam omogućuje vraćanje sustava u prethodno stanje

Čišćenje sustava može se zatražiti:

- kad se pronađe prijetnja
- kad korisnik klikne **Poništi**

Možete pregledati promjene i poništiti postavke prema potrebi.



Samo korisnik s administratorskim pravima može izvršiti radnje u čistaču sustava.

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

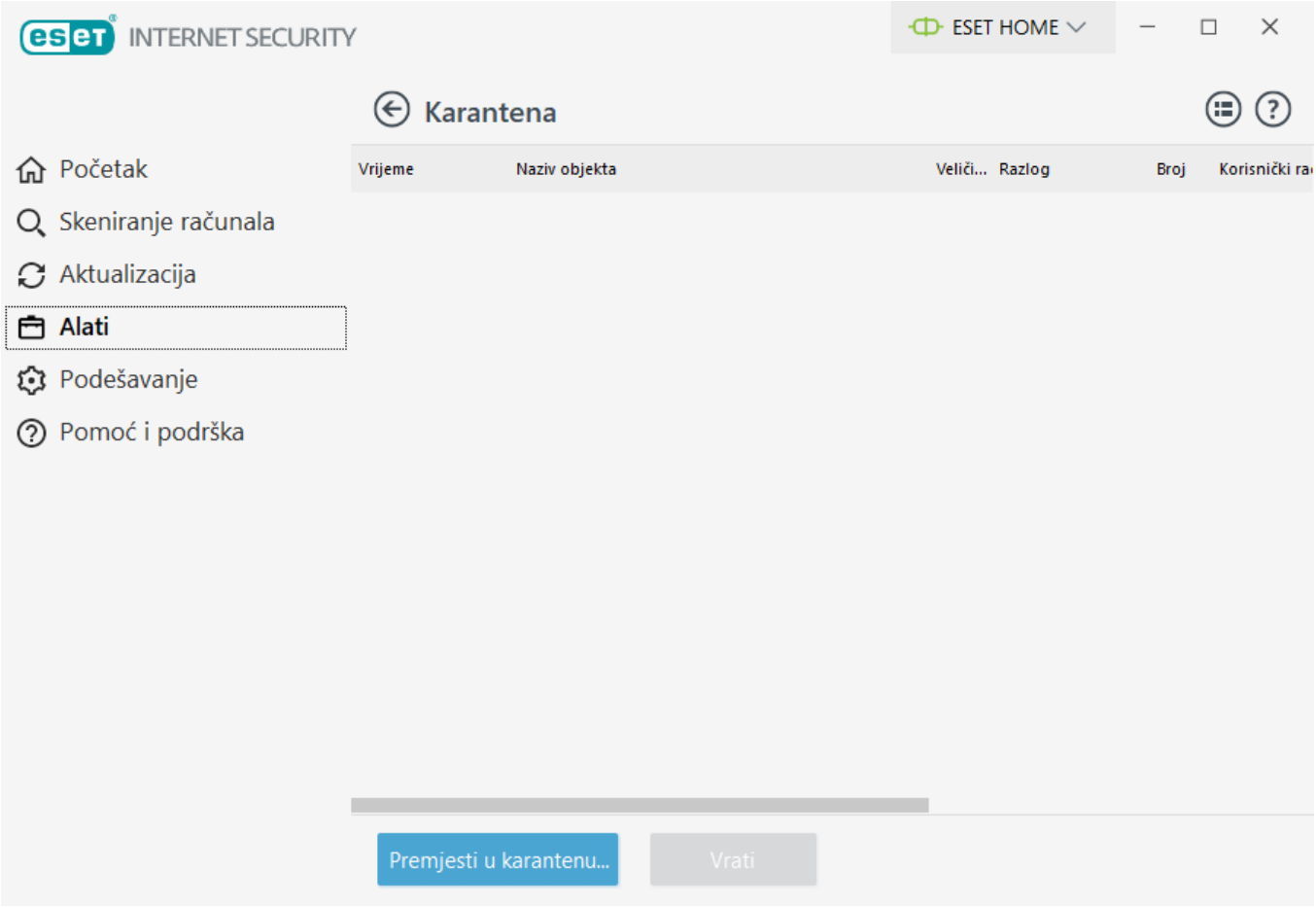
Karantena

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 Internet Security klikom na **Alati** > **Više alata** > **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).



Stavljanje datoteka u karantenu

ESET Internet Security automatski stavlja obrisane datoteke u karantenu (ako niste onemogućili ovu opciju u prozoru s upozorenjima).

Dodatne datoteke treba staviti u karantenu:

a.ako se ne mogu izbrisati,

b.ako ih nije sigurno ili preporučljivo obrisati,

c.ako ih ESET Internet Security 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.Desnom tipkom miša kliknite datoteku > kliknite **Napredne opcije** > **Stavi datoteku u karantenu**.

c.Kliknite **Prebaci u karantenu** u prozoru **Karantena**.

d.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 stavljena 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**.

Opis prijetnje

Kliknite desnom tipkom miša na stavku i kliknite **Opis otkrivene prijetnje** da biste otvorili enciklopediju prijetnji tvrtke ESET koja sadrži detaljne informacije o opasnostima i simptomima zabilježene infiltracije.

Ilustrirane upute

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

- Vraćanje datoteke u karanteni u programu ESET Internet Security
- Brisanje datoteke u karanteni u programu ESET Internet Security
- ESET-ov program obavijestio me o prijetnji – što trebam učiniti?

Stavljanje u karantenu nije uspjelo

Nekoliko je razloga zbog kojih se određene datoteke ne mogu prebaciti u karantenu:

- **Nemate dopuštenja za čitanje** – to znači da ne možete vidjeti sadržaj datoteke.
- **Nemate dopuštenja za pisanje** – to znači da ne možete mijenjati sadržaj datoteke, odnosno dodavati novi sadržaj ili brisati postojeći.
- **Datoteka koju pokušavate staviti u karantenu je prevelika** – trebate smanjiti datoteku.

Kada primite poruku o pogrešci "Stavljanje u karantenu nije uspjelo", kliknite **Više informacija**. Prikazat će se prozor s popisom pogrešaka povezanih s karantenom i vidjet ćete naziv datoteke i razlog zbog kojeg se datoteku ne može staviti u karantenu.

Proxy server

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 Internet Security 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 Internet Security. Parametre koji se tu nalaze koristit će svi moduli kojima je potrebna internetska veza.

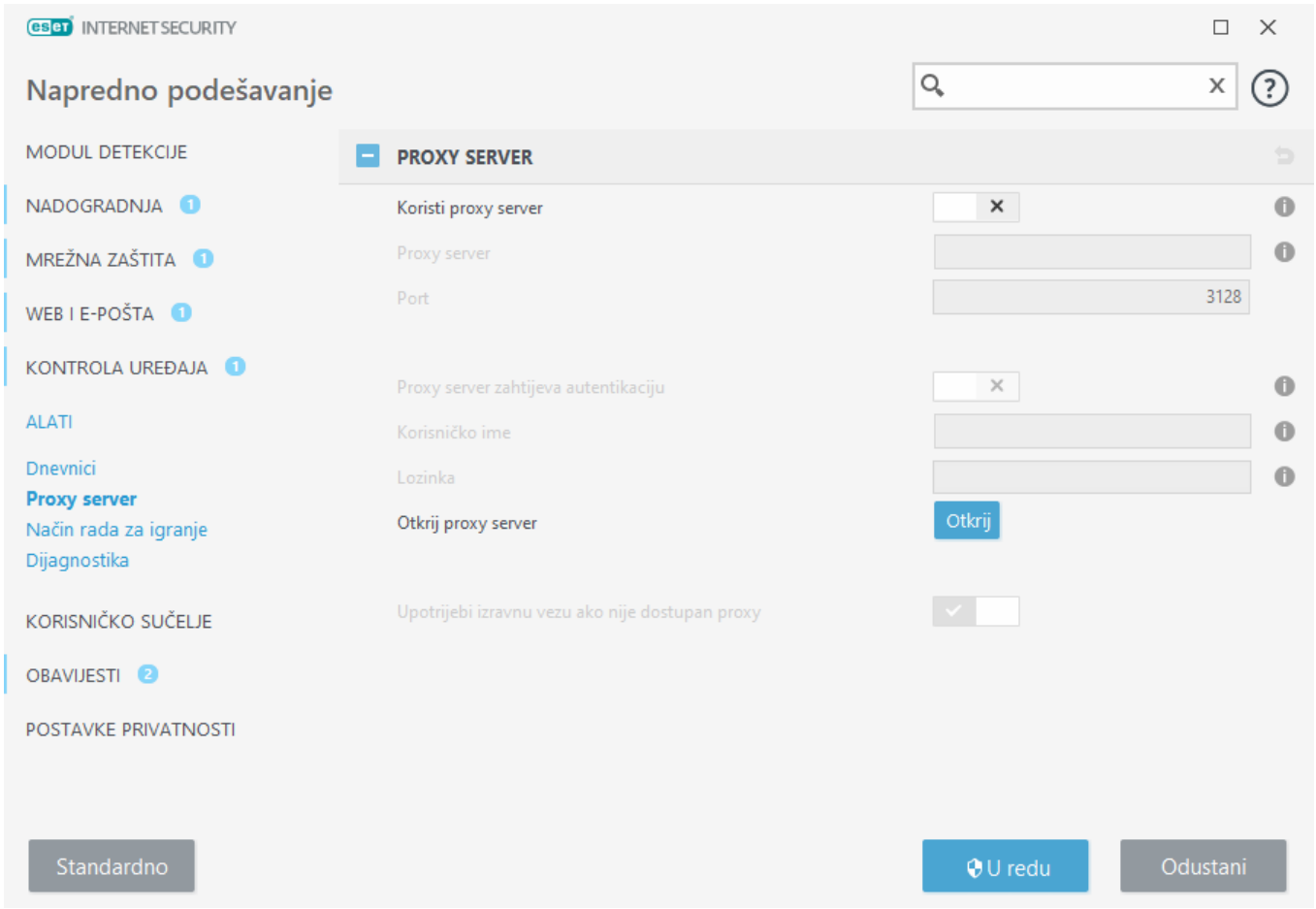
Da biste odredili postavke proxy servera za tu razinu, odaberite potvrdni okvir **Koristi proxy server** i zatim unesite adresu proxy servera u polje **Proxy server**, zajedno s brojem **porta** proxy servera.

Ako je za komunikaciju s proxy serverom potrebna prijava, odaberite potvrdni okvir **Proxy server zahtijeva 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.

Korisničko ime i lozinku morate ručno unijeti u postavke **proxy servera**.

Upotrijebi izravnu vezu ako nije dostupan proxy – ako je ESET Internet Security konfiguriran za povezivanje putem proxyja, a proxy nije dostupan, program ESET Internet Security 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 različitih lokacija primaju nadogradnje virusnih potpisa. Dodatne informacije o toj postavci potražite u odjeljku Napredno podešavanje nadogradnje.



Odabir uzorka za 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®).

Prije slanja uzoraka tvrtki ESET

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).

Uzorak (datoteku ili web stranicu) možete poslati ESET-u radi analize jednom od sljedećih metoda:

1. Upotrijebite obrazac za slanje uzoraka u svom programu. Nalazi se u izborniku **Alati** > **Više alata** > **Slanje uzorka na analizu**. Maksimalna veličina poslanog uzorka je 256 MB.

2. Datoteku možete poslati i e-poštom. Ako želite upotrijebiti tu mogućnost, datoteku zapakirajte s pomoću programa WinRAR/WinZIP, arhivsku datoteku zaštitite lozinkom "infected" i pošaljite je na adresu samples@eset.com.

3. Da biste prijavili spam sadržaj, neispravno identificirani spam sadržaj ili web stranice koje je modul roditeljske kontrole pogrešno kategorizirao, pročitajte članak ESET-ove baze znanja.

U obrascu **Odabir uzorka za analizu** iz padajućeg izbornika **Razlog za slanje uzorka** odaberite opis koji najbolje odgovara svrsi vaše poruke:

- Sumnjiva datoteka
- Sumnjiva stranica (web stranica koja je zaražena bilo kojim zlonamjernim softverom),
- Neispravno identificirana web stranica
- Neispravno identificirana datoteka (datoteka koja je otkrivena kao zaražena, ali zapravo nije),
- 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.

> **Možda nećete dobiti odgovor ESET-a**
> 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

Primijećeni 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 – Tu možete unijeti dodatne informacije ili opis koji će nam pomoći pri pronalaženju ili obradi sumnjive datoteke.

> Prvi parametar – **Primijećeni znakovi i simptomi zaraze zlonamjernim softverom** – obavezan je, no navođenje dodatnih informacija našim će laboratorijima uvelike pomoći pri identifikaciji i obradi uzoraka.

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 distribuira 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. Neispravno identificirane stranice (FP-ovi) mogu se pojaviti kad uzorak datoteke odgovara istom uzorku sadržanom u modulu za otkrivanje virusa.

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, multimedijski reproduktor...) i njena funkcionalnost.

Napomene i dodatne informacije – Ovdje možete unijeti dodatne informacije ili opis koji će nam pomoći pri obradi sumnjive datoteke.

> 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 uzoraka.

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.

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 Internet Security 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 nadogradnje 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.

Dijaloški prozor – nadogradnja sustava

Ako su dostupne nadogradnje za vaš operacijski sustav, ESET Internet Security početni prozor prikazuje obavijest. Kliknite **Više informacija** za otvaranje prozora nadogradnje sustava.

U prozoru o sistemskim nadogradnjama prikazan je popis dostupnih nadogradnji koje su spremne za preuzimanje i instalaciju. Vrsta nadogradnje prikazana je pokraj naziva nadogradnje.

Dvaput kliknite bilo koji redak nadogradnje kako bi se prikazao prozor Informacije o nadogradnji s dodatnim informacijama.

Kliknite **Pokreni nadogradnju sustava** da biste pokrenuli preuzimanje i instalaciju nadogradnje operacijskog sustava.

Aktualiziranje podataka

Informacije o aktualizacijama sustava Windows. Naziv i broj aktualizacije prikazuju se pri vrhu prozora zajedno s prioritetom i opisom poteškoće koju aktualizacija otklanja.

Korisničko sučelje

Da biste konfigurirali ponašanje grafičkog korisničkog sučelja programa (GUI), u glavnom prozoru programa kliknite **Podešavanje** > **Napredno podešavanje** (F5) > **Korisničko sučelje**.

Vizualni izgled programa i efekte možete podesiti u odjeljku Elementi korisničkog sučelja na zaslonu Napredno podešavanje.

Za maksimalnu sigurnost sigurnosnog softvera možete spriječiti deinstalaciju ili bilo koje neovlaštene promjene tako da zaštitite postavke putem lozinke s pomoću alata Podešavanje pristupa.

Da biste konfigurirali ponašanje obavijesti sustava, upozorenja o prijetnjama i statusa aplikacije, pogledajte odjeljak Obavijesti.

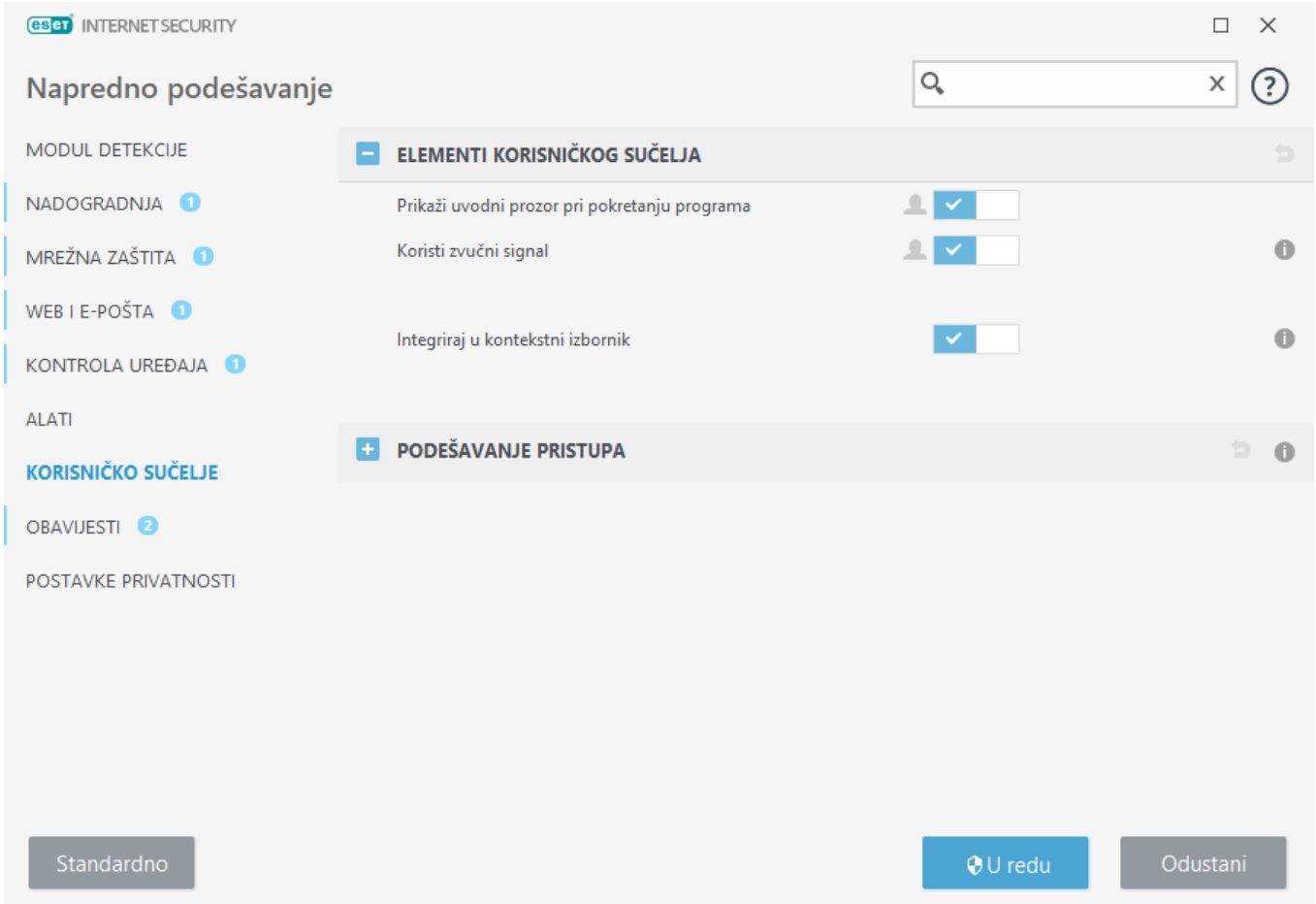
Elementi korisničkog sučelja

Mogućnosti konfiguriranja korisničkog sučelja u programu ESET Internet Security omogućuju vam da radno okruženje prilagodite svojim potrebama. Tim konfiguracijskim opcijama može se pristupiti u opcijama **Napredno podešavanje** (F5) > **Korisničko sučelje** > **Elementi korisničkog sučelja**.

Ako želite deaktivirati uvodni prozor programa ESET Internet Security, poništite odabir **Prikaži uvodni prozor pri pokretanju programa**.

Upotrijebi zvučni signal – ESET Internet Security reproducira zvučni signal u slučaju važnih događaja tijekom skeniranja, na primjer, kada se otkrije prijetnja ili se skeniranje dovrši.

Integriraj u kontekstni izbornik – Integrirajte kontrolne elemente programa ESET Internet Security u kontekstni izbornik.



Podešavanje pristupa

ESET Internet Security postavke su ključan dio vaših sigurnosnih pravila. Neovlaštene izmjene mogu ugroziti stabilnost i zaštitu vašeg sustava. Da bi se izbjegle neovlaštene preinake, parametre podešavanja programa ESET Internet Security i njegovu deinstalaciju moguće je zaštititi lozinkom.

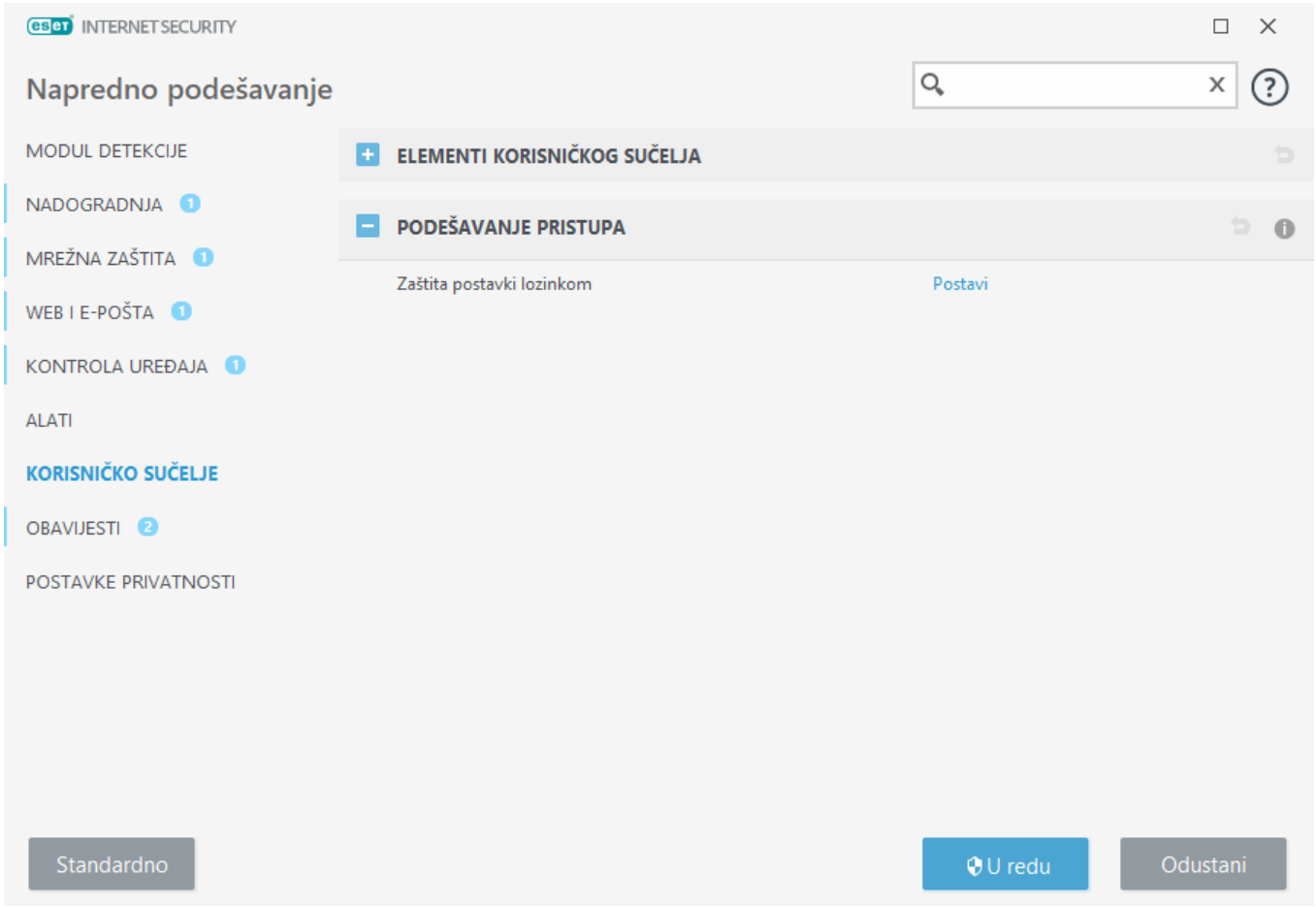
Da biste postavili lozinku za zaštitu parametara podešavanja programa ESET Internet Security i njegovu deinstalaciju, kliknite **Postavi** pored stavke **Zaštita postavki lozinkom**.

Kada želite pristupiti zaštićenom Naprednom podešavanju, prikazuje se prozor za unos lozinke. Ako zaboravite ili izgubite lozinku, kliknite opciju **Vrati lozinku** u nastavku i unesite adresu e-pošte kojom ste se koristili za registraciju licence. ESET će vam poslati poruku e-pošte s kodom za potvrdu i upute za poništavanje lozinke.

- Kako otključati Napredno podešavanje

Da biste promijenili lozinku, kliknite **Promijeni lozinku** pored stavke **Zaštita postavki lozinkom**.

Da biste uklonili lozinku, kliknite **Ukloni** pored stavke **Zaštita postavki lozinkom**.



Lozinka za napredno podešavanje

Da biste zaštitili napredno podešavanje programa ESET Internet Security i izbjegli neželjene preinake, morate postaviti novu lozinku.

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**.

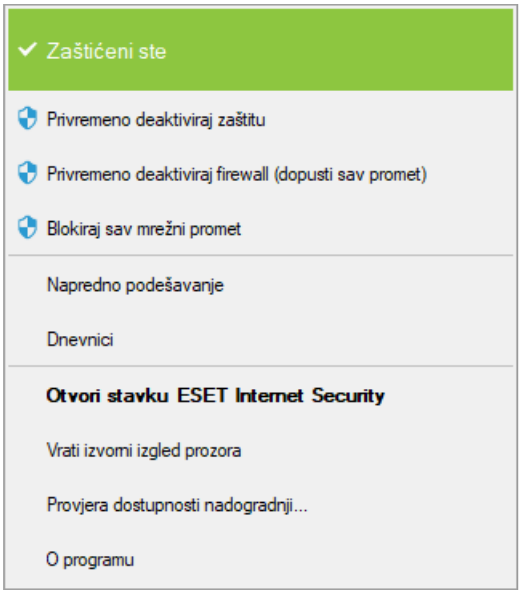
Ta lozinka morat će se unijeti prilikom budućih preinaka programa ESET Internet Security.

Ako zaboravite lozinku, pristup naprednim postavkama moguće je vratiti načinom „Vrati lozinku”.

Da biste vratili izgubljeni ESET-ov licenčni ključ, datum isteka licence ili druge informacije o licenci za ESET Internet Security, pogledajte naš članak iz baze znanja.

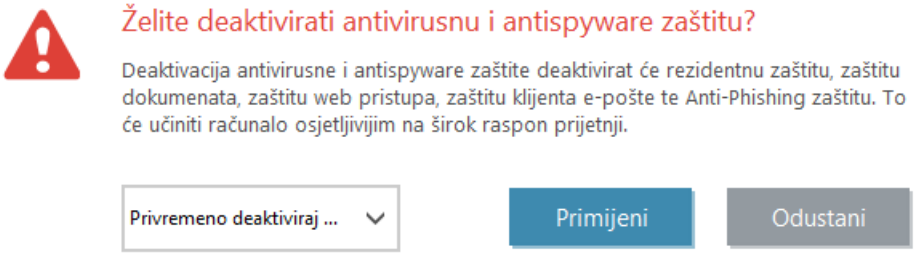
Ikona trake sustava

Neke od najvažnijih mogućnosti i značajki podešavanja dostupne su kada desnom tipkom miša kliknete ikonu trake sustava .



Privremeno deaktiviraj zaštitu – prikazuje upit za potvrdu kojim se deaktivira Modul detekcije, koji štiti od zloćudnih napada sustava kontrolirajući komunikaciju datoteka, weba i e-pošte.

Padajući izbornik **Vremensko razdoblje** predstavlja vremensko razdoblje tijekom kojeg će zaštita biti deaktivirana.



Pauziraj firewall (dopusti sav promet) – Prebacuje firewall u neaktivno stanje. Dodatne informacije potražite u odjeljku Mreža.

Blokiraj sav mrežni promet – Ta opcija blokira sav mrežni promet. Možete ga ponovno aktivirati tako da kliknete

Prestani blokirati sav mrežni promet.

Napredno podešavanje – odaberite ovu opciju da biste ušli u stablo **Napredno podešavanje**. Ima i drugih načina otvaranja Naprednog podešavanja, npr. pritiskom tipke F5 ili odlaskom na **Podešavanje** > **Napredno podešavanje**.

Dnevnici – dnevnici sadrže informacije o važnim događajima u programu koji su se pojavili i pružaju pregled otkrivenih prijetnji.

Otvori program ESET Internet Security – Otvara glavni prozor programa ESET Internet Security s ikone trake.

Poništi raspored prozora – Vraća prozor programa ESET Internet Security na standardnu veličinu i položaj na zaslonu.

Potraži nadogradnje – Počinje nadograđivati modul za otkrivanje (prethodno poznat kao „baza podataka virusnih potpisa") kako bi osigurao vašu razinu zaštite od zlonamjernog koda.

O programu – Pruža informacije o sustavu, detalje o instaliranoj verziji programa ESET Internet Security i instaliranim modulima programa. Tu se nalaze i informacije o datumu isteka licence te o operacijskom sustavu i sistemskim resursima.

Podrška za čitač zaslona

ESET Internet Security se može upotrebljavati zajedno s čitačima zaslona kako bi se ESET-ovim korisnicima oštećenog vida omogućila navigacija programom ili konfiguriranje postavki. Podržani su sljedeći čitači zaslona: (JAWS, NVDA, Narrator).

Da biste bili sigurni da softver čitača zaslona može ispravno pristupiti GUI-ju programa ESET Internet Security, slijedite upute u našem članku u bazi znanja.

Pomoć i podrška

ESET Internet Security sadrži alate za otklanjanje poteškoća i informacije za podršku koje će vam pomoći u rješavanju problema koji se mogu pojaviti.

Licenca

- **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. Ako je vaš uređaj povezan s programom ESET HOME, odaberite licencu iz ESET HOME računa ili dodajte novu.

Instalirani program

- **Novosti** – ovo kliknite da biste otvorili prozor s informacijama o novim i poboljšanim funkcijama.
- **O programu ESET Internet Security** – Prikazuje informacije o vašoj kopiji programa ESET Internet Security.
- **Otklanjanje poteškoća s programima** – kliknite ovaj link da biste pronašli rješenja za najčešće probleme.

• **Promjena programa** – Kliknite da vidite može li se ESET Internet Security promijeniti u drugu liniju programa s trenutačnom licencom.

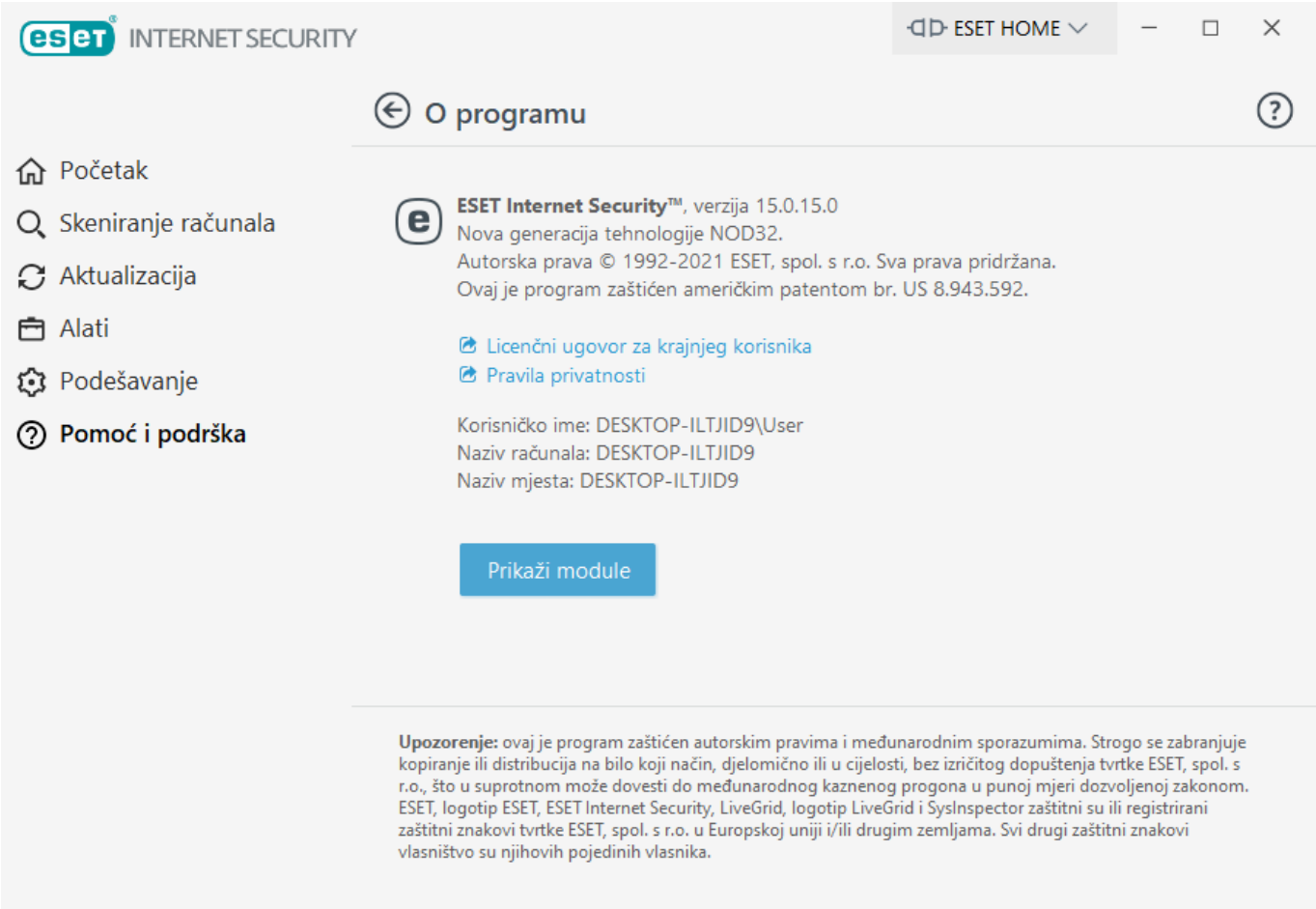
Stranica pomoći – Kliknite ovaj link da biste pokrenuli stranice pomoći programa ESET Internet Security.

Tehnička podrška

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 Internet Security

U ovom prozoru se navode pojedinosti o instaliranoj verziji programa ESET Internet Security i vašem računalu.



Kliknite **Prikaži module** da biste vidjeli informacije o popisu učitanih modula programa.

• Informacije o modulima možete kopirati u međuspremnik tako da kliknete **Kopiraj**. To može biti korisno prilikom otklanjanja poteškoća ili kontaktiranja s tehničkom podrškom.

• Kliknite **Modul detekcije** u prozoru Moduli da biste otvorili ESET-ov virusni radar koji sadrži informacije o svakoj verziji ESET-ovog modula detekcije.

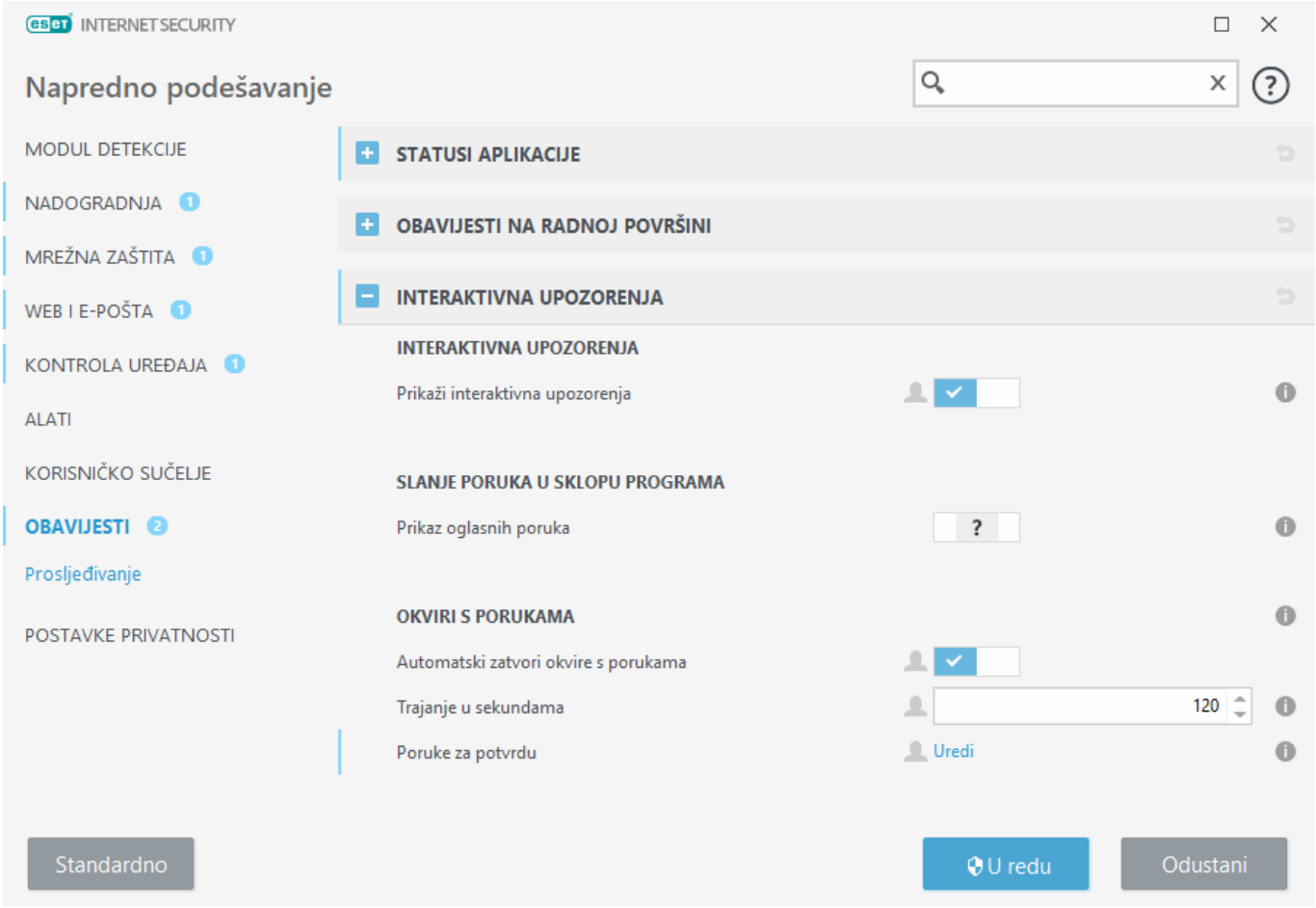
ESET vijesti

U ovom vas prozoru ESET Internet Security redovito obavještava o novostima iz ESET-a.

Prikaz poruka u programu namijenjen je informiranju korisnika o novostima i ostalim informacijama iz tvrtke ESET. Za slanje marketinških poruka potreban je pristanak korisnika. Marketinške poruke zato se ne šalju korisniku prema standardnoj postavci (prikazano kao upitnik). Aktivacijom ove opcije pristajete na primanje marketinških poruka tvrtke ESET. Ako niste zainteresirani za primanje marketinškog materijala tvrtke ESET, deaktivirajte opciju **Prikaz marketinških poruka**.

Da biste aktivirali ili deaktivirali primanje marketinških poruka u skočnim prozorima, slijedite upute u nastavku.

1. Otvorite glavni prozor ESET-ova programa.
2. Pritisnite tipku **F5** da biste pristupili odjeljku **Napredno podešavanje**.
3. Kliknite **Obavijesti** > **Interaktivna upozorenja**.
4. Izmijenite opciju **Prikaz marketinških poruka**.



Slanje podataka o sistemskoj konfiguraciji

Radi pružanja što brže i preciznije pomoći, tvrtki ESET potrebne su informacije o konfiguraciji programa ESET Internet Security, 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 opciju **Uvijek pošalji ove podatke** ako želite da se ta radnja zapamti za ovaj proces. Za slanje obrasca bez ikakvih podataka kliknite **Nemoj slati podatke** i obratite se tehničkoj podršci tvrtke ESET putem online obrasca za podršku.

Ovu postavku možete konfigurirati i u odjeljku **Napredno podešavanje** > **Alati** > **Dijagnostika** > Tehnička podrška.

> 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

U glavnom prozoru programa kliknite **Pomoć i podrška** > **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).

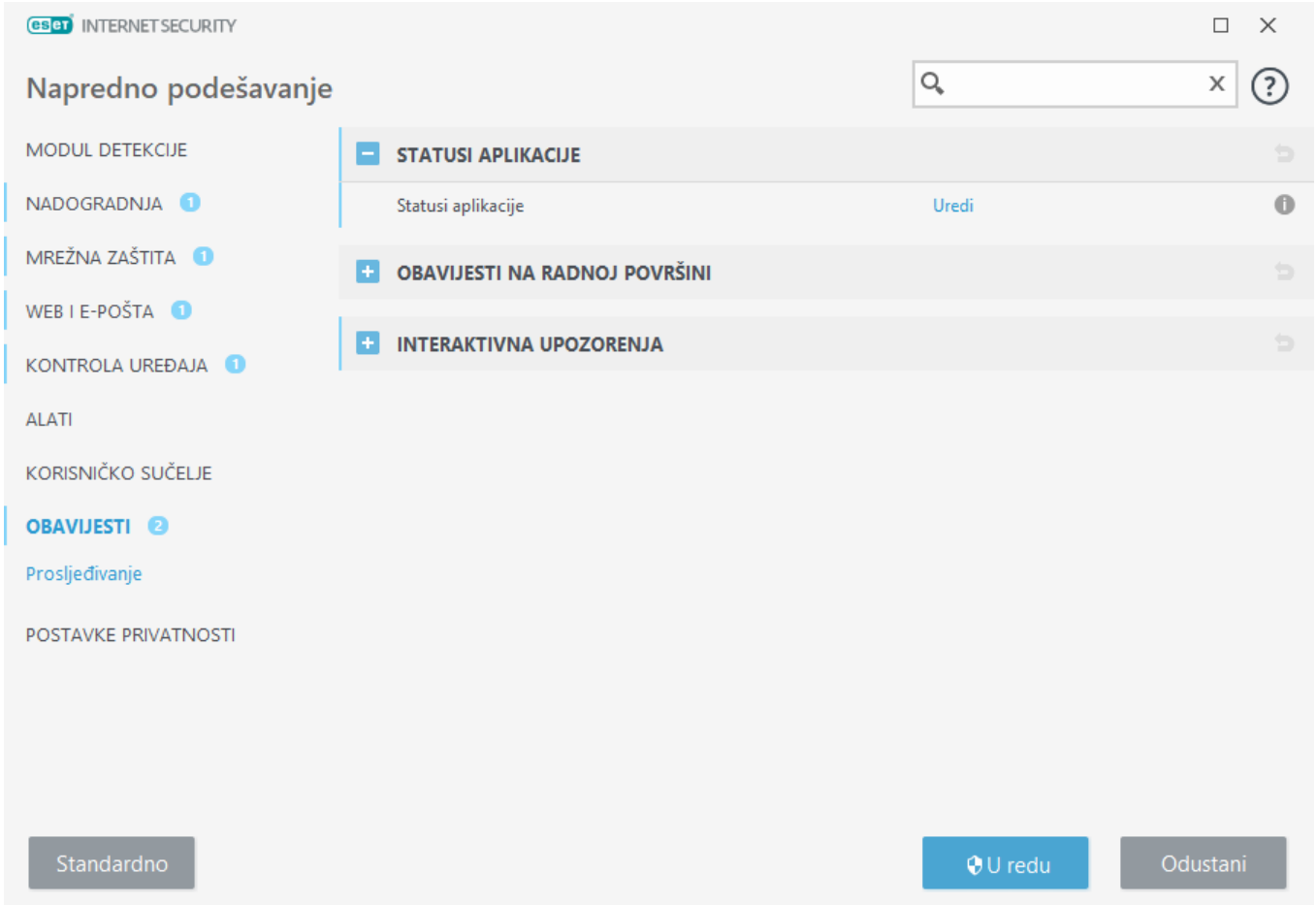
ESET Log Collector – Veza na članak iz ESET-ove baze znanja na kojem možete preuzeti uslužni alat ESET Log Collector, aplikaciju koja automatski prikuplja informacije i dnevnike s računala i omogućuje brže rješavanje problema. Za više informacija pogledajte mrežni korisnički priručnik za ESET Log Collector.

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 dnevnici, prikazat će se prozor obavijesti koji pruža izravan pristup mapi Dijagnostike s izrađenim dnevnicima.

Obavijesti

Da biste upravljali obavijestima programa ESET Internet Security, otvorite **Napredno podešavanje** (F5) > **Obavijesti**. Možete konfigurirati sljedeće vrste obavijesti:

- Statusi aplikacije – obavijesti prikazane u početnom odjeljku glavnog prozora programa.
- Obavijesti na radnoj površini – mali skočni prozori pokraj programske trake sustava.
- Interaktivna upozorenja – prozori s upozorenjima i okviri s porukama koji zahtijevaju interakciju korisnika.
- Prosljeđivanje (obavijesti e-poštom) – obavijesti e-poštom šalju se na određenu adresu e-pošte.



Statusi aplikacije

Statusi aplikacije – kliknite **Uredi** da biste odabrali koji će se statusi aplikacije prikazivati u početnom odjeljku glavnog prozora programa.

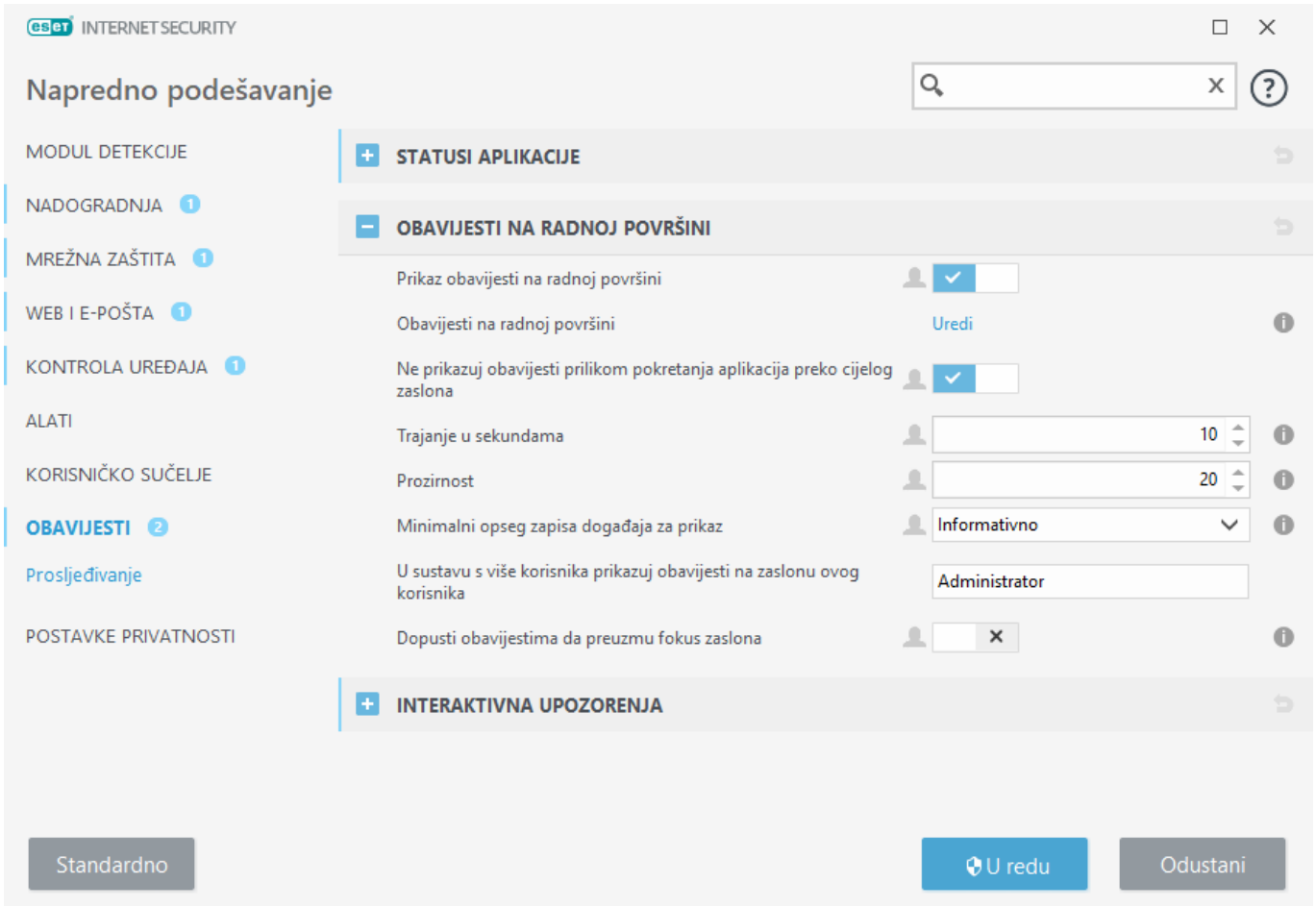
Dijaloški prozor – statusi aplikacije

U ovom dijaloškom prozoru možete odabrati koji će se statusi aplikacije prikazati. Na primjer, kada pauzirate antivirusnu i antispyware zaštitu ili aktivirate način rada za igranje.

Status aplikacije prikazat će se i ako program nije aktiviran ili ako je licenca istekla.

Obavijesti na radnoj površini

Obavijesti na radnoj površini se prikazuju kao mali skočni prozor pokraj programske trake sustava. Prema standardnim postavkama, prikazuje se na 10 sekundi, a zatim postupno nestaje. Obavijesti obuhvaćaju uspješne nadogradnje programa, nove povezane uređaje, završene zadatke skeniranja virusa ili nove pronađene prijetnje.



Prikaži obavijesti na radnoj površini – preporučujemo da ne deaktivirate tu opciju da biste mogli primati obavijesti programa o novim događajima.

Obavijesti na radnoj površini – kliknite **Uredi** da biste aktivirali ili deaktivirali određene Obavijesti na radnoj površini.

Ne prikazuj obavijesti prilikom pokretanja aplikacija preko cijelog zaslona – isključite sve obavijesti koje nisu interaktivne prilikom pokretanja aplikacija preko cijelog zaslona.

Trajanje u sekundama – postavite trajanje vidljivosti obavijesti. Vrijednost mora biti između 3 i 30 sekundi.

Prozirnost – postavite postotak prozirnosti obavijesti. Podržani raspon je od 0 (nema prozirnosti) do 80 (vrlo visoka prozirnost).

Minimalni opseg zapisa događaja za prikaz – postavite razinu ozbiljnosti prikazane obavijesti. U padajućem izborniku odaberite jednu od sljedećih opcija:

- **Dijagnostički** – prikazuje sve informacije potrebne za detaljno konfiguriranje programa te sve prethodno navedene zapise.
- **Informacije** – prikazuje sve informativne poruke kao što su nestandardni mrežni događaji, uključujući uspješne nadogradnje, te sve prethodno navedene zapise.
- **Upozorenja** – prikazuje poruke upozorenja, pogreške i kritične pogreške (na primjer, antistealth tehnologija ne funkcionira ispravno ili nadogradnja nije uspjela).
- **Pogreške** – prikazuje pogreške (na primjer, zaštita dokumenta nije pokrenuta) i kritične pogreške.

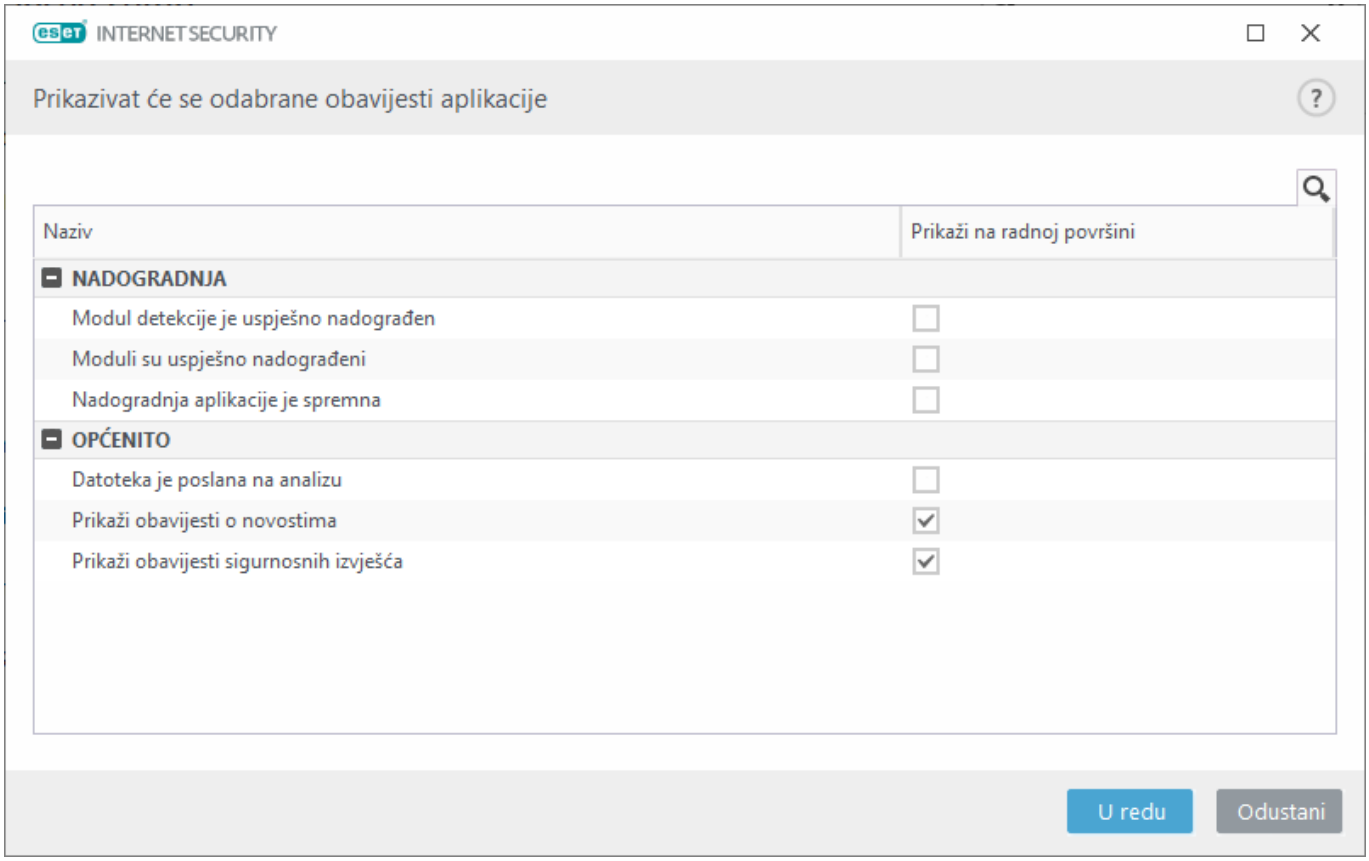
- **Kritično** – prikazuje samo kritične pogreške (pogreške pri pokretanju antivirusne zaštite, ako je sustav zaražen itd.).

U sustavu s više korisnika prikazuj obavijesti na zaslonu ovog korisnika – dopušta odabranom računu da prima obavijesti na radnoj površini. Na primjer, ako ne upotrebljavate administratorski račun, upišite puni naziv računa i obavijesti na radnoj površini prikazat će se za navedeni račun. Samo jedan korisnički račun može primati obavijesti na radnoj površini.

Dopusti obavijestima da preuzmu fokus zaslona – dopušta obavijestima da preuzmu fokus zaslona i dostupne su u izborniku **ALT + Tab.**

Popis obavijesti na radnoj površini

Da biste podesili vidljivost obavijesti na radnoj površini (koje se prikazuju u donjem desnom kutu zaslona), otvorite **Napredno podešavanje** (F5) > **Obavijesti** > **Obavijesti na radnoj površini**. Kliknite **Uredi** pored **Obavijesti na radnoj površini** i odaberite odgovarajući potvrdni okvir **Prikaži**.



Općenito

Prikaži obavijesti sigurnosnog izvješća – prikazat će se obavijest kad se stvori novo sigurnosno izvješće.

Prikaži obavijesti o novostima – obavijesti o svim novim i poboljšanim funkcijama najnovije verzije programa.

Datoteka je poslana na analizu – prikazat će se obavijest svaki put kada ESET Internet Security pošalje datoteku na analizu.

Nadogradnja

Nadogradnja aplikacije je spremna – prikazat će se obavijest kada je spremna nadogradnja programa ESET Internet Security na novu verziju.

Modul detekcije je uspješno nadograđen – prikazat će se obavijest kada program nadogradi module detekcije.

Moduli su uspješno ažurirani – prikazat će se obavijest kada program nadogradi komponente programa.

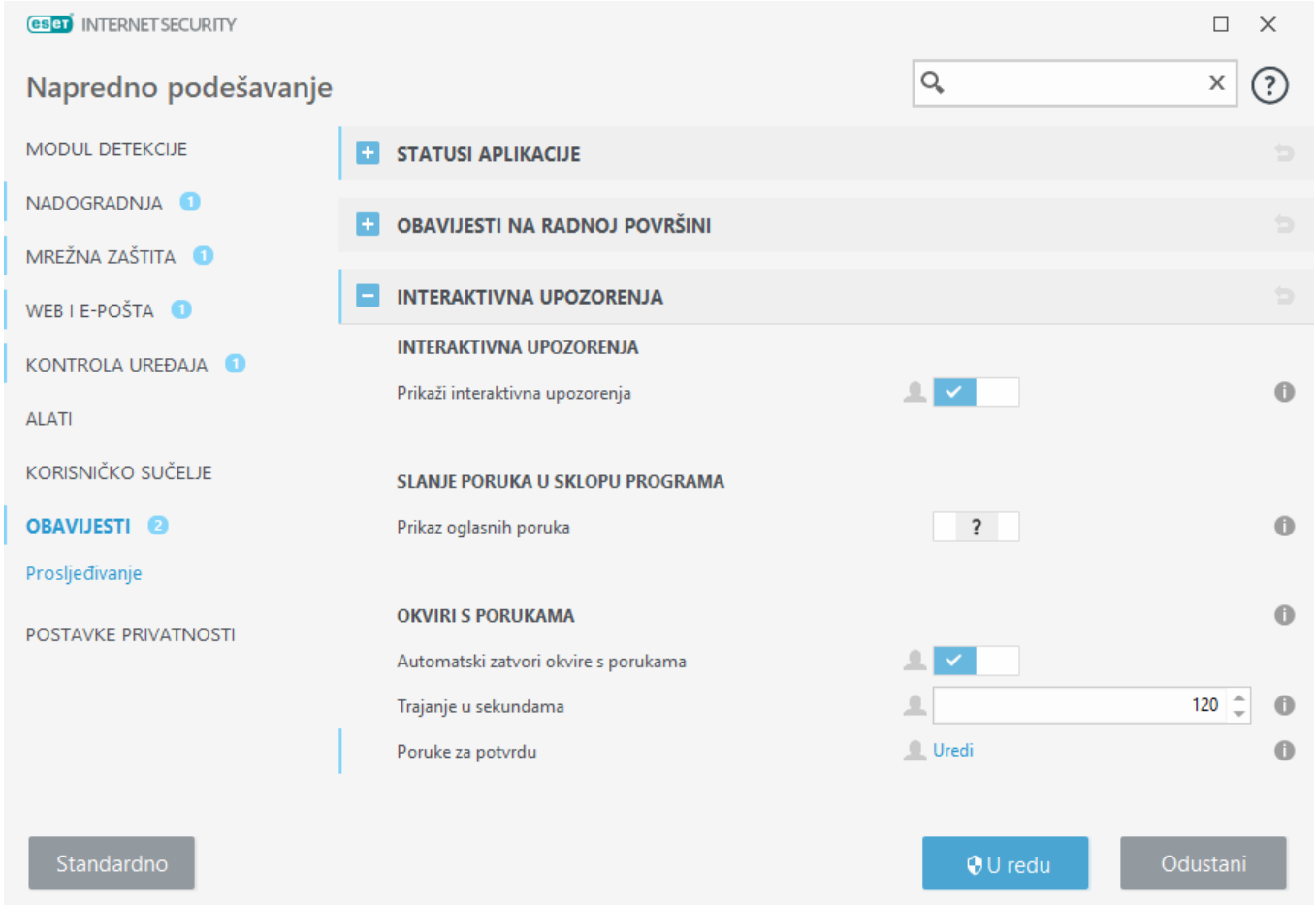
Da biste postavili opće postavke za obavijesti na radnoj površini, primjerice, koliko će se dugo prikazivati poruka ili minimalni opseg događaja za prikaz, pogledajte stavku Obavijesti na radnoj površini u izborniku **Napredno podešavanje** (F5) > **Obavijesti**.

Interaktivna upozorenja

Tražite informacije o čestim upozorenjima i obavijestima?

- Pronađena je prijetnja
- Adresa je blokirana
- Program nije aktiviran
- Promjena u program s više funkcija
- Prelazak na nižu liniju programa
- Dostupna je nadogradnja
- Informacije o nadogradnji nisu dosljedne
- Otklanjanje poteškoća za poruku "Nadogradnja modula nije uspjela"
- Rješavanje pogrešaka nadogradnje modula
- Blokirana je mrežna prijetnja
- Odbijen certifikat web stranice

Odjeljak **Interaktivna upozorenja** u dijelu **Napredno podešavanje** (F5) > **Obavijesti** omogućuje vam da konfigurirate kako ESET Internet Security upravlja okvirima s porukama i interaktivnim upozorenjima za prijetnje u slučaju kada korisnik treba donijeti odluku (na primjer, potencijalna web stranica za phishing).



Interaktivna upozorenja

Deaktiviranjem opcije **Prikaži interaktivna upozorenja** sakrit će se svi prozori upozorenja i dijaloški okviri u pregledniku, što je prikladno samo za ograničen broj specifičnih situacija. ESET preporučuje da ova opcija ostane aktivirana.

Slanje poruka u sklopu proizvoda

Prikaz poruka u programu namijenjen je informiranju korisnika o novostima i ostalim informacijama iz tvrtke ESET. Za slanje marketinških poruka potreban je pristanak korisnika. Marketinške poruke zato se ne šalju korisniku prema standardnoj postavci (prikazano kao upitnik). Aktivacijom ove opcije pristajete na primanje marketinških poruka tvrtke ESET. Ako niste zainteresirani za primanje marketinškog materijala tvrtke ESET, deaktivirajte opciju **Prikaz marketinških poruka**.

Okviri s porukama

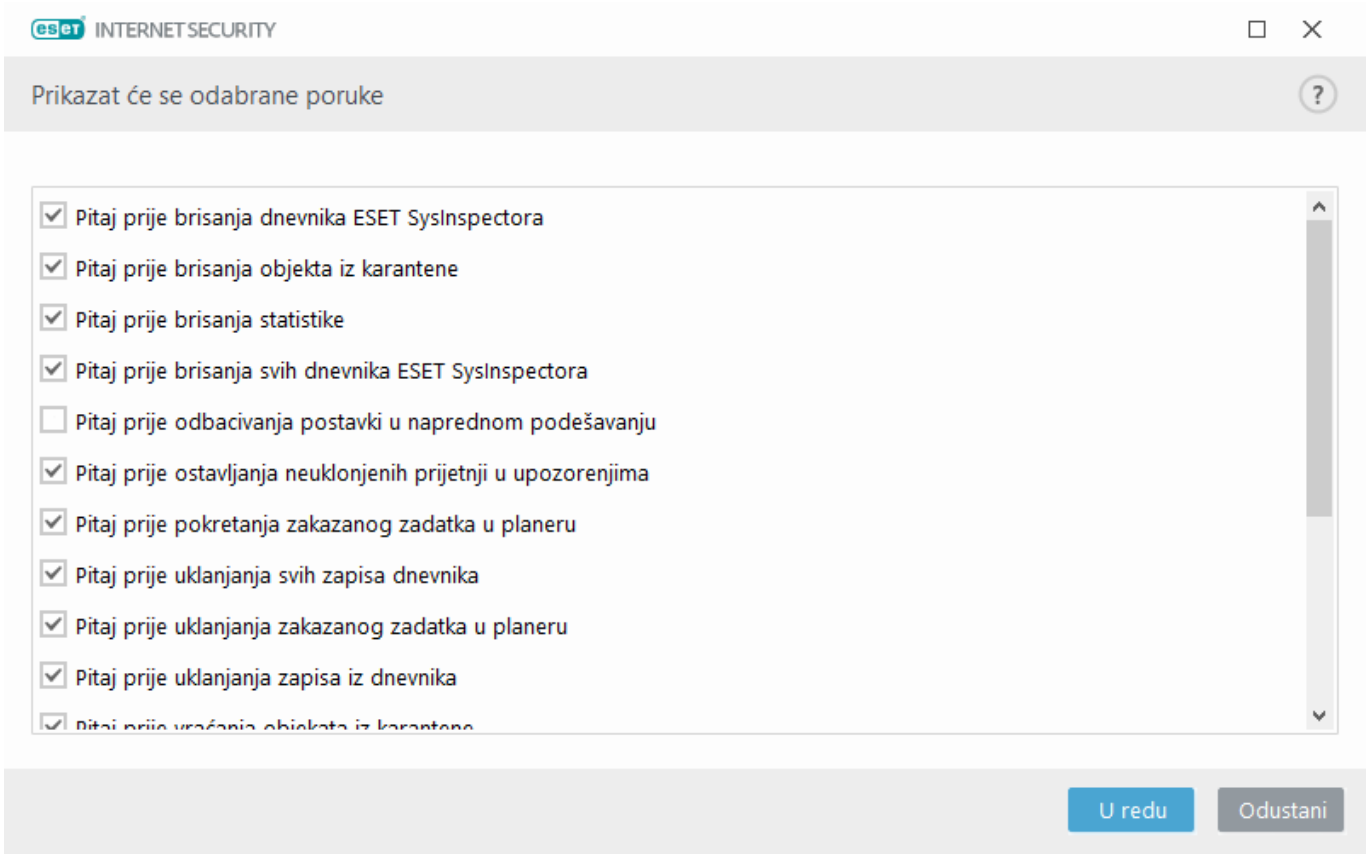
Da biste automatski zatvorili okvire s porukama nakon određenog vremena, odaberite opciju **Automatski zatvori okvire s porukama**. Ako se okviri ne zatvore ručno, prozori upozorenja automatski se zatvaraju nakon isteka određenog vremenskog razdoblja.

Istek vremena u sekundama – postavlja trajanje vidljivosti upozorenja. Vrijednost mora biti između 10 i 999 sekundi.

Poruke za potvrdu – kliknite **Uredi** za prikaz popisa poruka za potvrdu na kojem možete odabrati hoće li se poruke prikazivati ili ne.

Poruke za potvrdu

Da biste podesili poruke za potvrdu, idite na **Napredno podešavanje** (F5) > **Obavijesti** > **Interaktivna upozorenja** i kliknite **Uredi** pored opcije **Poruke za potvrdu**.



U ovom se dijaloškom prozoru prikazuju poruke za potvrdu koje program ESET Internet Security 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:

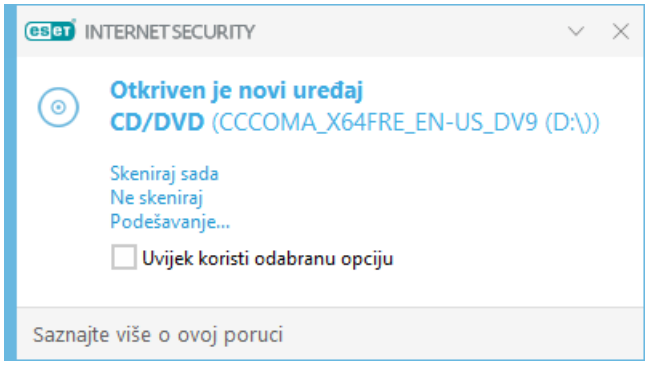
- Pitaj prije brisanja dnevnika ESET SysInspectora
- Pitaj prije brisanja svih dnevnika ESET SysInspectora
- Pitaj prije brisanja objekta iz karantene
- Pitaj prije odbacivanja postavki u naprednom podešavanju
- Pitaj prije ostavljanja neuklonjenih prijetnji u upozorenjima
- Pitaj prije uklanjanja zapisa 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 obavijesti s rezultatima antispam obrade
- Prikaži obavijesti s rezultatima antispam obrade za klijente e-pošte
- Prikaži potvrdne dijaloške okvire za Outlook Express i Windows Mail
- Prikaži potvrdne dijaloške okvire za Windows Live Mail
- Prikaži potvrdne dijaloške okvire za Outlook

Izmjenjivi mediji

ESET Internet Security 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 Internet Security, prikazuje se sljedeći prozor:



Opcije za ovaj prozor:

- **Skeniraj odmah** – Pokreće skeniranje izmjenjivih medija.
- **Ne skeniraj** – izmjenjivi mediji neće se skenirati.
- **Podešavanje** – Otvara odjeljak **Napredno podešavanje**.
- **Uvijek koristi odabranu opciju** – Ako je odabrana ova opcija, ista će se radnja izvršiti i kada se izmjenjivi medij umetne i drugi put.

Osim toga, ESET Internet Security 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.

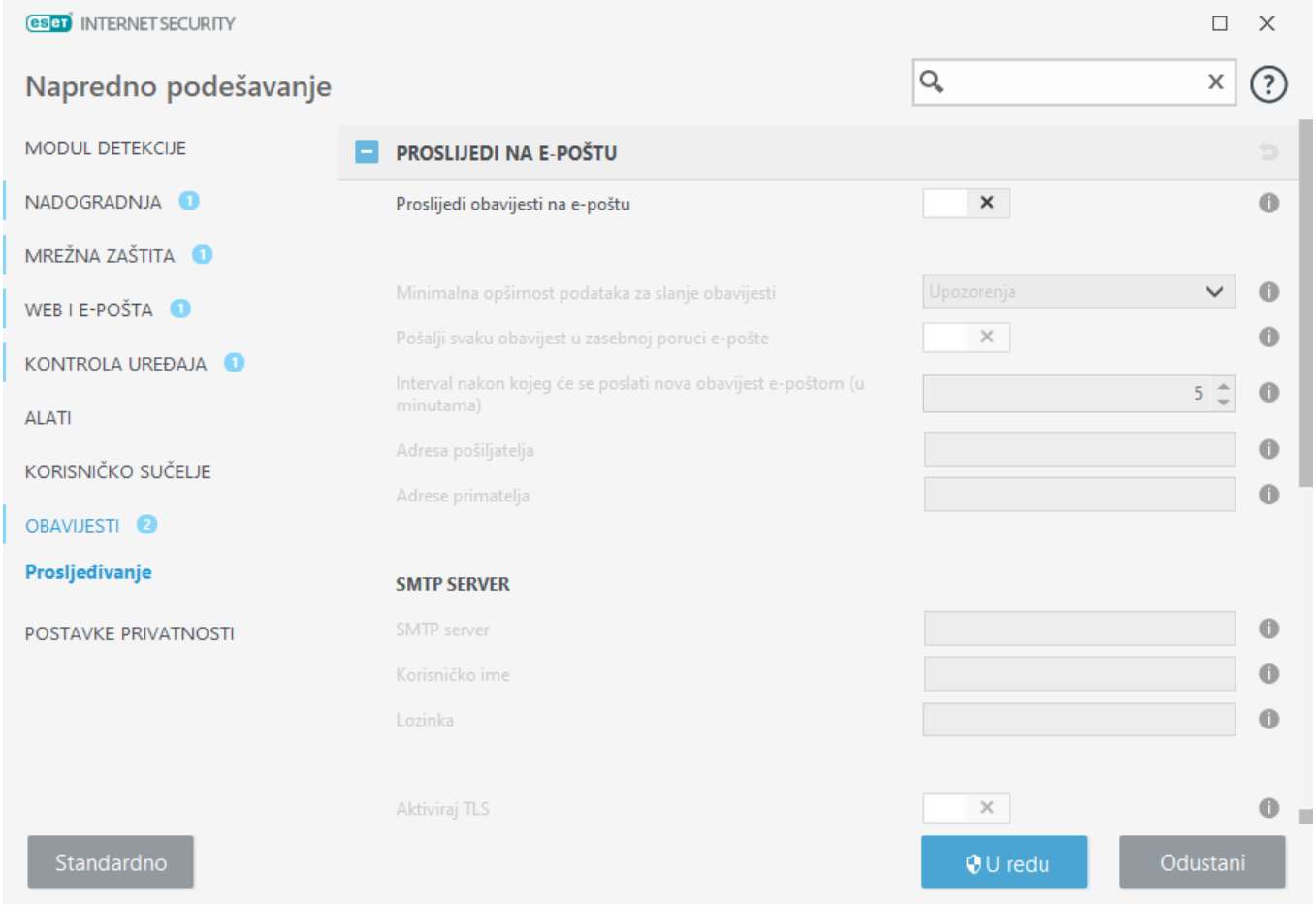
Otvorite Napredno podešavanje (**F5**) > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Izmjenjivi mediji** da biste pristupili postavkama skeniranja izmjenjivih medija.

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**.

Prosljeđivanje

ESET Internet Security može automatski slati obavijesti e-poštom ako dođe do događaja s odabranom razinom opširnosti. Otvorite **Napredno podešavanje** (F5) > **Obavijesti** > **Prosljeđivanje** i aktivirajte opciju **Proslijedi obavijesti na e-poštu** da biste aktivirali obavijesti e-poštom.



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** – bilježi samo kritične pogreške (na primjer, Pogreška pri pokretanju antivirusne zaštite ili Pronađena prijetnja).

Pošalji svaku obavijest u zasebnoj poruci e-pošte – kada je ova opcija aktivirana, primatelj će primiti 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.

Adresa pošiljatelja – U tom se polju navodi adresa pošiljatelja koja se prikazuje u zaglavlju poruka e-pošte s obavijestima.

Adrese primatelja – u tom se polju navode adrese primatelja koje se prikazuju u zaglavlju poruka e-pošte s obavijestima. Podržano je više vrijednosti. Upotrijebite točku sa zarezom za odvajanje.

SMTP server

SMTP server – SMTP server koji se upotrebljava za slanje obavijesti (na primjer, smtp.provider.com:587, prethodno definirani port je 25).

Program ESET Internet Security podržava SMTP servere s TLS šifriranjem.

Korisničko ime i **lozinka** – Ako SMTP zahtjeva autentikaciju, ova se polja trebaju popuniti ispravnim korisničkim imenom i lozinkom kako bi se moglo pristupiti SMTP serveru.

Aktiviraj TLS – Secure Alert i obavijesti koje koriste TLS šifriranje.

Testiraj SMTP vezu – Probna poruka e-pošte poslat će se na adresu e-pošte primatelja. Treba popuniti polja za SMTP server, korisničko ime, lozinku, adresu pošiljatelja i adresu primatelja.

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 ćete okolnostima 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 – poruke s upozorenjem o prijetnji i poruke s obavijestima imaju unaprijed definirani standardni oblik. ESET preporučuje da ne mijenjate taj oblik. Međutim, u nekim ćete okolnostima (na primjer, ako upotrebljavate automatizirani sustav 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 "?".

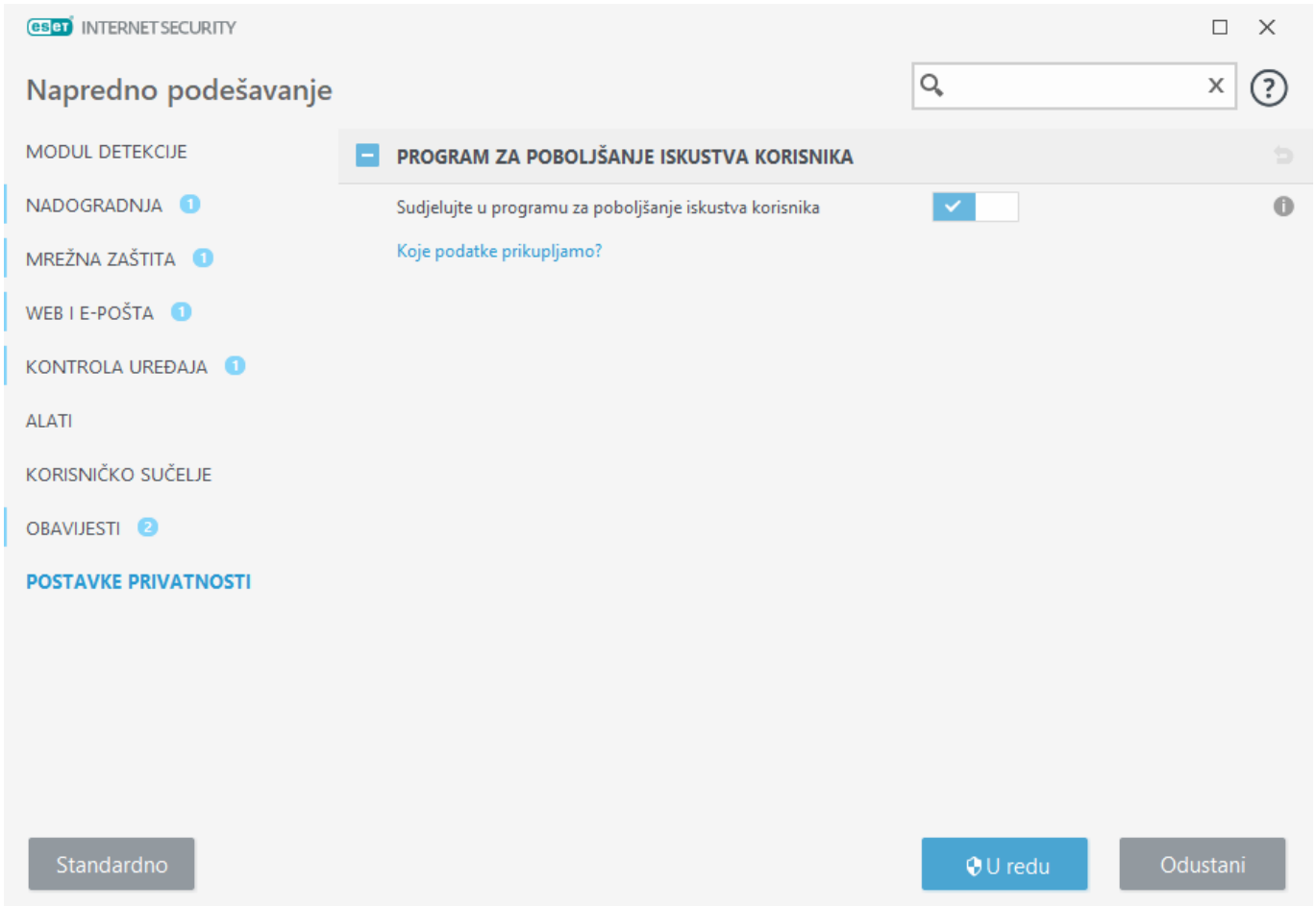
Koristi Quoted-printable kodiranje znakova – Izvor poruke e-pošte bit će kodiran u oblik Quoted-printable (QP) koji koristi ASCII znakove i može ispravno e-poštom prenijeti posebne znakove u 8-bitnom obliku (čććžšđ).

- **%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.

Postavke privatnosti

U glavnom prozoru programa kliknite **Podešavanje** > **Napredno podešavanje** (F5) > **Postavke privatnosti**.



Program za poboljšanje iskustva korisnika

Aktivirajte traku klizača pored opcije **Sudjelovanje u programu za poboljšanje iskustva korisnika** da biste se pridružili Programu za poboljšanje iskustva korisnika. Ako se pridružite, ESET-u pružate anonimne informacije povezane s upotrebom ESET-ovih programa. Podaci koje prikupimo pomoći će nam da poboljšamo vaše iskustvo i nikada ih nećemo dijeliti s trećim stranama. Koje podatke prikupljamo?

Profili

Upravljanje profilima koristi se na dva mjesta u programu ESET Internet Security – u odjeljku **Skeniranje računala na zahtjev** i u odjeljku **Aktualizacija**.

Skeniranje računala

U programu ESET Internet Security 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.

Pretpostavimo 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 primijeniti **Uvijek ukloni prijetnju**. 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 Internet Security možete upotrijebiti sljedeće tipkovne prečace:

Tipkovnički prečaci	Akcija
F1	otvara stranice pomoći
F5	otvara Napredno podešavanje
Strelica gore / strelica dolje	navigacija u stavkama padajućeg izbornika
TAB	prelazi na sljedeći element GUI-ja u prozoru
Shift+TAB	premješta na prethodni element GUI-ja u prozoru
ESC	zatvara aktivni dijaloški prozor

Tipkovnički prečaci	Akcija
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
ALT + Strelica lijevo	vraća natrag
ALT + Strelica desno	kreće se naprijed
ALT+Home	ide na početak

Za navigaciju možete upotrebljavati i tipke miša naprijed ili natrag.

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 Internet Security 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 pomoću 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*.

Stvori dijagnostički dump – kliknite **Stvori** da biste stvorili dijagnostičke datoteke slike stanja memorije u **ciljnom direktoriju**.

Napredno vođenje dnevnika

Aktiviraj napredno vođenje dnevnika u marketinškim porukama – bilježi sve događaje povezane s marketinškim porukama unutar programa.

Aktiviraj napredno vođenje dnevnika modula za nadogradnju – Bilježi sve događaje koji se dogode tijekom skeniranja protiv spama. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s ESET Antispam modulom.

Aktiviraj napredno vođenje dnevnika Anti-Theft modula – Bilježi sve događaje koji se dogode u sustavu Anti-Theft kako bi se omogućilo dijagnosticiranje i rješavanje problema.

Aktiviraj napredno vođenje dnevnika za zaštitu bankarstva i plaćanja – bilježi sve događaje koji se dogode u zaštiti bankarstva i plaćanja.

Aktiviraj napredno vođenje dnevnika skenera računala – Bilježi sve događaje koji se dogode tijekom skeniranja datoteka i mapa pomoću skeniranja računala.

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 o programu Direct Cloud – bilježi sve događaje koji se dogode u programu ESET LiveGrid®. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s programom ESET LiveGrid®.

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 zaštite klijenta e-pošte – zabilježite sve događaje koji se dogode u zaštiti klijenta e-pošte i dodatku za klijent e-pošte kako biste dopustili dijagnosticiranje i rješavanje problema.

Aktiviraj napredno vođenje dnevnika za Kernel – bilježi sve događaje koji se događaju u usluzi ESET Kernel (ekrn).

Aktiviraj napredno vođenje dnevnika licenciranja – bilježi svu komunikaciju programa s ESET-ovim aktivacijskim ili ESET License Manager serverima.

Aktiviraj praćenje memorije – bilježi sve događaje koji razvojnim programerima pomažu pri 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 – bilježi dodatne informacije o operacijskom sustavu kao što su pokrenuti procesi, aktivnost procesora i operacije diska. To razvojnim programerima može pomoći u dijagnostici i otklanjanju problema povezanih s ESET-ovim programom koji je pokrenut na vašem operacijskom sustavu.

Aktiviraj napredno vođenje dnevnika roditeljske kontrole – Bilježi sve događaje koji se dogode u roditeljskoj kontroli. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s roditeljskom kontrolom.

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 automatskih poruka – bilježi sve događaje koji se događaju tijekom slanja automatskih poruka.

Aktiviraj napredno vođenje dnevnika rezidentne zaštite sistemskih datoteka – bilježi sve događaje koji se događaju tijekom skeniranja datoteka i mapa s pomoću rezidentne zaštite sistemskih datoteka.

Aktiviraj napredno vođenje dnevnika modula za nadogradnju – Bilježi sve događaje do kojih dolazi tijekom nadogradnje. To može pomoći razvojnim programerima u dijagnostici i otklanjaju problema povezanih s modulom za nadogradnju.

Dnevnici se nalaze u mapi *C:**ProgramData**ESET**ESET Security**Diagnostics*\.

Tehnička podrška

Kada se obratite ESET-ovoj tehničkoj podršci iz programa ESET Internet Security, možete poslati podatke o sistemskoj konfiguraciji. Odaberite **Uvijek pošalji** iz padajućeg izbornika **Slanje podataka o sistemskoj konfiguraciji** da biste automatski poslali podatke ili odaberite **Pitaj prije slanja** da bi vam se poslao upit prije slanja podataka.

Uvoz i izvoz postavki

Možete uvesti ili izvesti svoju prilagođenu ESET Internet Security .xml konfiguracijsku datoteku na izborniku **Podešavanje**.

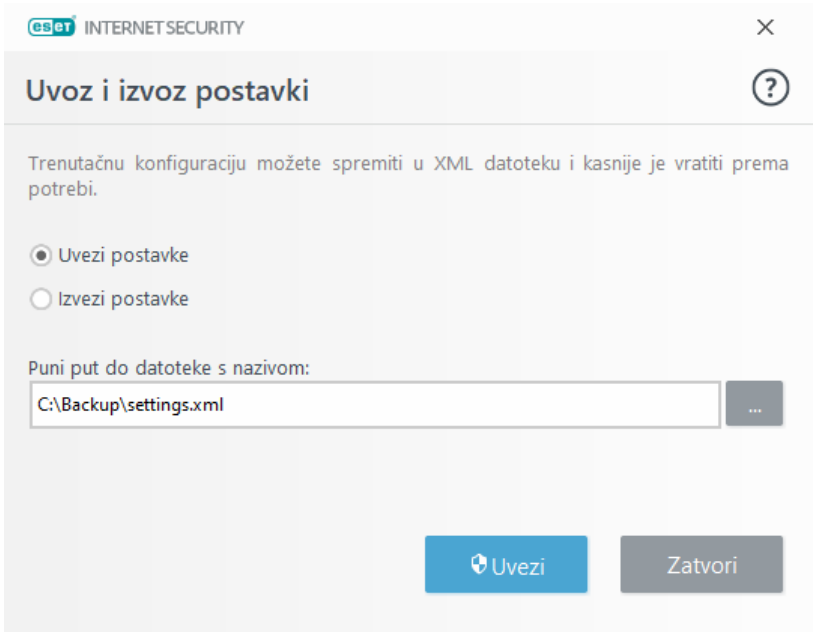
> **Ilustrirane upute**
> Pogledajte Uvoz ili izvoz postavki konfiguracije ESET-a pomoću .xml datoteke za ilustrirane upute dostupne na engleskom i nekoliko drugih jezika.

Uvoz i izvoz konfiguracijskih datoteka korisni su ako trebate izraditi sigurnosnu kopiju trenutne konfiguracije programa ESET Internet Security da biste je mogli koristiti kasnije. Opcija izvoza postavki je praktična i kada želite koristiti svoju preferiranu konfiguraciju u više sustava. Možete uvesti .xml datoteku za prijenos tih postavki.

Za uvoz konfiguracije u glavnom programskom prozoru kliknite **Podešavanje** > **Uvoz ili izvoz postavki**, a zatim odaberite **Uvezi postavke**. Unesite naziv konfiguracijske datoteke ili kliknite gumb **...** da biste pronašli konfiguracijsku datoteku koju želite uvesti.

Za izvoz konfiguracije u glavnom programskom prozoru kliknite **Podešavanje** > **Uvoz ili izvoz postavki**. Odaberite **Izvezi postavke** i unesite puni put datoteke s nazivom. Kliknite **...** da biste otišli na mjesto na računalu gdje želite spremiti konfiguracijsku datoteku.

> Tijekom izvoza postavki može se pojaviti pogreška ako nemate dostatna prava za pisanje izvezene datoteke u navedeni direktorij.



Želite li vratiti sve postavke u ovom odjeljku

Kliknite zakrivljenu 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.

Vraćanje na standardne postavke

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.

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.

Skener naredbenog retka

Modul za antivirusnu zaštitu programa ESET Internet Security 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 heuristiku (standardno)
/no-heur	deaktiviraj heuristiku
/adv-heur	aktiviraj naprednu heuristiku (standardno)
/no-adv-heur	deaktiviraj naprednu heuristiku
/ext-exclude=EKSTENZIJE	izuzmi iz skeniranja EKSTENZIJE datoteka razgraničene dvotočkom
/clean-mode=NAČIN	koristi NAČIN čišćenja za zaražene objekte Dostupne su sljedeće opcije: • `none` (standardno) – Automatsko čišćenje neće se izvršiti. • `standard` – ecls.exe automatski će pokušati očistiti ili izbrisati zaražene datoteke. • `strict (strogo)` – ecls.exe automatski će pokušati očistiti ili izbrisati zaražene datoteke bez intervencije korisnika (neće se prikazati odzivnik prije brisanja datoteka). • `rigorous (rigorozno)` – ecls.exe će izbrisati datoteke bez pokušaja čišćenja, neovisno o tome o kakvim se datotekama radi. • `delete (brisanje)` – ecls.exe će izbrisati datoteke bez pokušaja čišćenja, ali neće izbrisati osjetljive datoteke poput onih sustava Windows.
/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 Internet Security 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 uvesti novu konfiguraciju. Ako podešavanje pristupa nije aktivirano, lozinka ne odgovara ili konfiguracijska datoteka .xml nije potpisana, konfiguracija se neće uvesti.

Kad se aktivira ESET CMD, možete upotrijebiti naredbeni redak za uvoz ili izvoz konfiguracija ESET Internet Security. 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.

Naredba izvoza postavki:
```
ecmd /getcfg c:\config\settings.xml
```

Naredba uvoza postavki:
```
ecmd /setcfg c:\config\settings.xml
```

Napredne ecmd naredbe mogu se pokrenuti samo lokalno.

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 `xmlsigntool.exe`

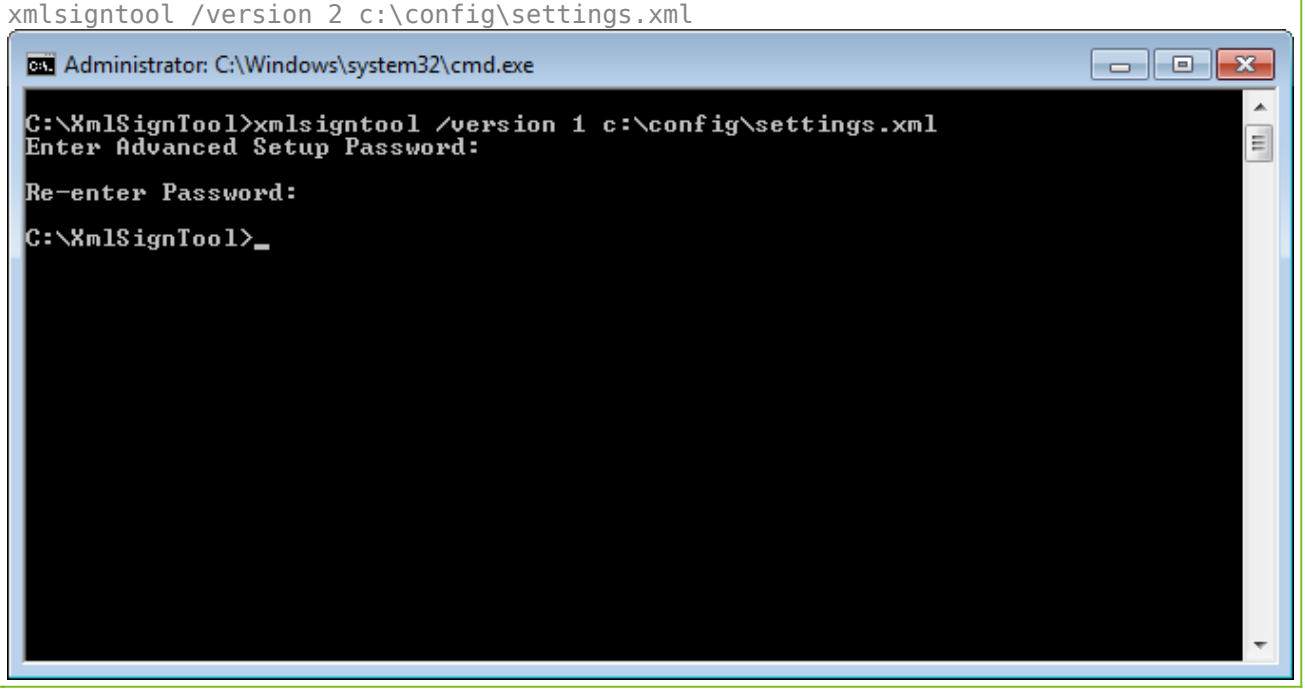
4. Izvršite naredbu da biste potpisali konfiguracijsku datoteku *.xml*, upotreba: `xmlsigntool /version 1|2 <xml_file_path>`

Vrijednost parametra `/version` ovisi o vašoj verziji programa ESET Internet Security. Upotrebljavajte `/version 1` za verzije programa ESET Internet Security starije od 11.1. Upotrebljavajte `/version 2` za trenutačnu verziju programa ESET Internet Security.

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 Internet Security programom ESET CMD upotrebom metode autorizacije lozinkom.

Potpišite izvezenu naredbu konfiguracijske datoteke:

```
xmlsigntool /version 2 c:\config\settings.xml
```



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 Internet Security 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.

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:

- **Isključen zaslon ili čuvar zaslona**
- **Zaključano računalo**
- **Odjava korisnika**

Pomoću traka klizača za svako stanje aktivirajte ili deaktivirajte različite pokretače otkrivanja stanja mirovanja.

Najčešća pitanja

Neka od najčešćih pitanja i problema s kojima se možete susresti možete pronaći u nastavku. Kliknite naslov teme da biste saznali rješenje problema:

- Kako nadograditi program ESET Internet Security
- Uklanjanje virusa s računala
- Dopuštanje komunikacije za određene aplikacije
- Kako aktivirati roditeljsku kontrolu za neki račun
- Stvaranje novog zadatka u Planeru
- Zakazivanje skeniranja (tjedno)
- Kako riješiti pogrešku "Zaštita bankarstva i plaćanja nije preusmjerena na traženu web stranicu"
- Kako otključati Napredno podešavanje
- Kako riješiti deaktivaciju programa s ESET HOME portala

Ako vaš problem nije naveden na prethodno navedenom popisu, pokušajte pretražiti pomoć na mreži programa ESET Internet Security.

Ako u pomoći na mreži programa ESET Internet Security ne možete pronaći rješenje svojeg problema ili odgovor na pitanje, pokušajte u redovito ažuriranoj internetskoj ESET-ovoj bazi znanja. Veze na najpopularnije članke iz naše baze znanja navedene su u nastavku:

- Kako mogu obnoviti licencu?
- Dobio sam poruku o pogreški aktivacije prilikom instalacije ESET-ovog programa. Što to znači?
- Aktiviraj moj ESET-ov Windows program za kućnu upotrebu s pomoću mog korisničkog imena, lozinke ili licenčnog ključa.
- Deinstaliraj ili ponovno instaliraj moj ESET-ov program za kućnu upotrebu.
- Dobivam poruku da je ESET instalacija završila preuranjeno
- Što trebam učiniti nakon obnove licence? (kućni korisnici)
- Što ako promijenim svoju adresu e-pošte?
- Prijenos ESET-ovog programa na novo računalo ili uređaj
- Kako se pokreće sustav Windows u sigurnom načinu rada ili u sigurnom načinu rada s umrežavanjem
- Izuzmi sigurne web stranice od blokiranja
- Dopusti čitačima zaslona pristup ESET-ovom grafičkom korisničkom sučelju

Ako je potrebno, sa svojim se pitanjima ili problemima možete obratiti našoj tehničkoj podršci.

Kako nadograditi program ESET Internet Security

Program ESET Internet Security 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 promijeniti interval, idite na stavku **Alati** > **Planer**.

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 **Skeniraj računalo** da biste pokrenuli skeniranje sustava.

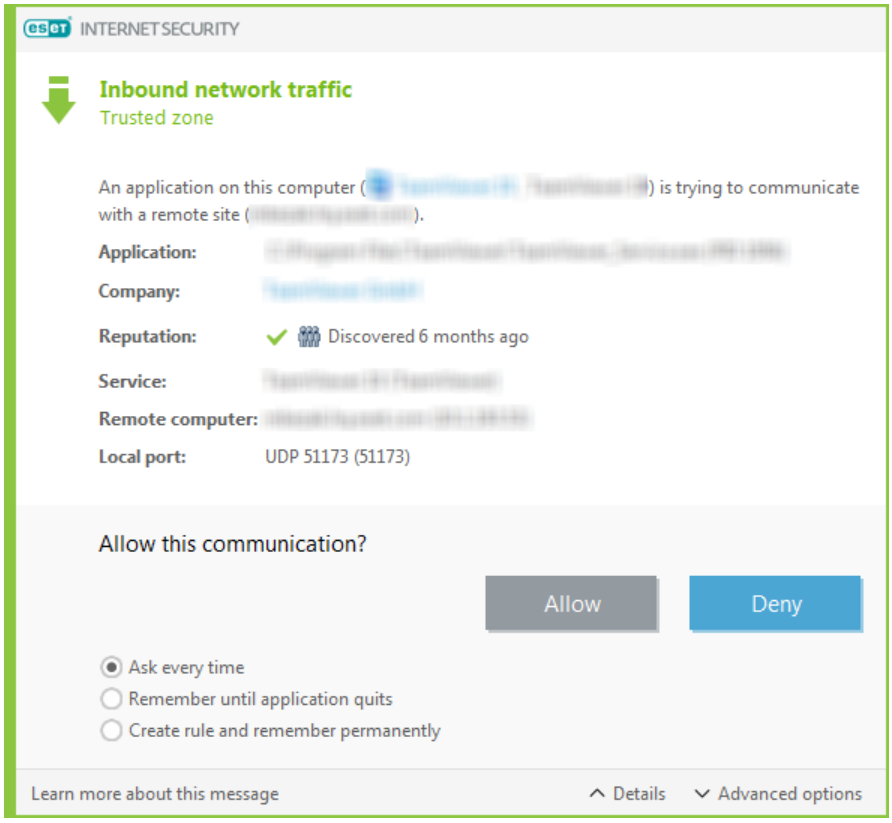
3. Nakon završetka skeniranja u dnevniku pogledajte koliko je skeniranih, zaraženih i očišćenih datoteka.

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.

Dopuštanje komunikacije za određene aplikacije

Ako se u interaktivnom načinu otkrije nova veza za koju ne postoji pravilo, prikazat će se odzivnik o tome želite li je dopustiti ili zabraniti. Želite li da ESET Internet Security izvrši istu akciju svaki put kad aplikacija pokuša uspostaviti vezu, potvrdite okvir **Stvori pravilo i trajno ga zapamti**.



Možete stvoriti nova pravila firewalla za aplikacije prije nego što ih program ESET Internet Security otkrije u prozoru za podešavanje firewalla. Otvorite glavni prozor programa > **Podešavanje** > **Mrežna zaštita** > kliknite ⚙ pored opcije **Firewall** > **Konfiguriraj** > **Napredno** > **Pravila** > **Uredi**.

Kliknite gumb **Dodaj** i na kartici **Općenito** unesite naziv, smjer i komunikacijski protokol za pravilo. Taj prozor vam omogućuje definiranje radnje koju treba provesti kada se pravilo primijeni.

Na kartici **Lokalno** unesite put do izvršne datoteke aplikacije i lokalni komunikacijski port. Kliknite na karticu **Udaljeno** i unesite udaljenu adresu i port (ako je moguće). Novostvoreno pravilo primijenit će se čim aplikacija ponovno pokuša komunicirati.

Kako aktivirati roditeljsku kontrolu za neki račun

Da biste za određeni korisnički račun aktivirali roditeljsku kontrolu, pratite sljedeće korake:

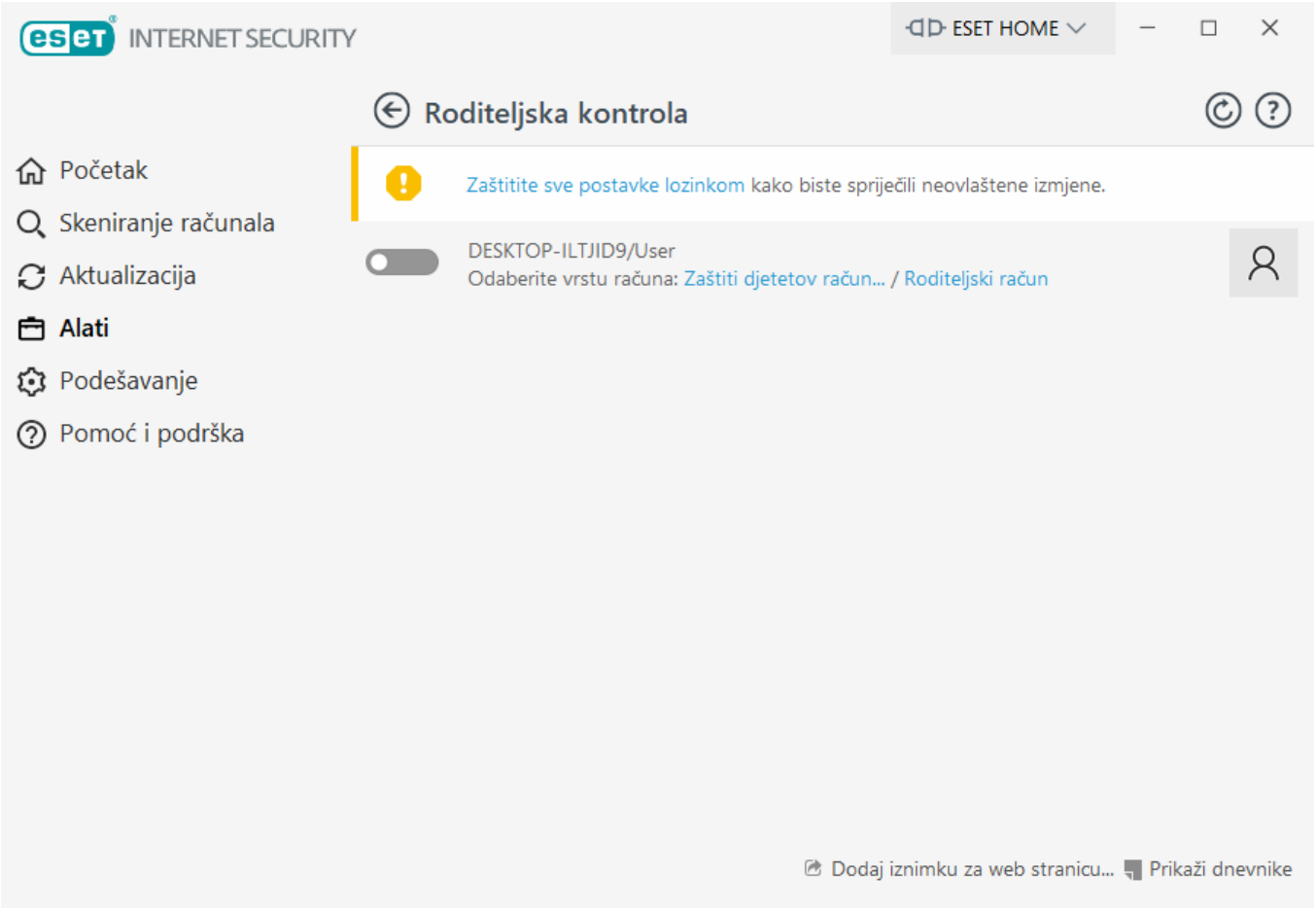
1. Roditeljska je kontrola prema standardnim postavkama u programu ESET Internet Security deaktivirana. Roditeljsku kontrolu možete aktivirati na dva načina:

   • Kliknite ◯ u oknu **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola** glavnog prozora programa i promijenite stanje roditeljske kontrole u aktivirano.

   • Pritisnite tipku F5 da biste pristupili stablu **Napredno podešavanje**, idite na **Web i e-pošta** > **Roditeljska kontrola**, a zatim aktivirajte traku klizača pokraj opcije **Aktiviraj roditeljsku kontrolu**.

2. Kliknite **Podešavanje** > **Sigurnosni alati** > **Roditeljska kontrola** u glavnom prozoru programa. Premda se uz **roditeljsku kontrolu** pojavljuje stavka **Aktivno**, roditeljsku kontrolu za željeni račun morate konfigurirati tako da kliknete simbol strelice, a zatim u sljedećem prozoru odaberete **Zaštiti djetetov račun** ili **Roditeljski račun**. U sljedećem prozoru odaberite datum rođenja za određivanje razine pristupa i preporučene stranice prikladne

za danu dob. Tada će za navedeni korisnički račun biti aktivirana roditeljska kontrola. Ispod naziva računa kliknite **Blokirani sadržaj i postavke** kako biste prilagodili kategorije koje želite dopustiti ili blokirati na kartici Kategorije. Da biste dopustili ili blokirali prilagođene stranice koje ne odgovaraju određenoj kategoriji, kliknite karticu Iznimke.



Stvaranje novog zadatka u Planeru

Kako biste stvorili novi zadatak u opciji **Alati** > **Više alata** > **Planer**, kliknite **Dodaj** ili desnom tipkom miša kliknite i odaberite **Dodaj** iz kontekstualnog izbornika. Na raspolaganju je sedam vrsta planiranih zadataka:

- **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
- **Održavanje dnevnika** – Dnevnici 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.
- **Nadogradnja** – Planira zadatak nadogradnje nadogradnjom 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. Dostupne su sljedeće opcije: **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 satima)**).

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** > **Više alata** > **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. Unesite naziv zadatka i odaberite opciju **Skeniranje računala na zahtjev** iz padajućeg izbornika **Vrsta zadatka**.
3. Odaberite **Tjedno** kao 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.

Kako riješiti pogrešku "Zaštita bankarstva i plaćanja nije preusmjerena na traženu web stranicu"

Upotreba opcije Zaštiti sve preglednike umjesto preusmjeravanja web stranica

Prema standardnim postavkama, zaštićeni preglednik Zaštite bankarstva i plaćanja pokreće se u pregledniku koji se trenutačno upotrebljava nakon posjeta poznatoj web stranici za bankarstvo. Umjesto preusmjeravanja web stranica možete upotrijebiti opciju Zaštiti sve preglednike da biste pokrenuli sve podržane preglednike u sigurnom načinu rada. To vam omogućuje pregledavanje interneta, pristup internetskom bankarstvu i izvršavanje transakcija na internetu u jednom prozoru zaštićenog preglednika, bez preusmjeravanja.

Da biste upotrijebili opciju Zaštiti sve preglednike, otvorite glavni prozor programa, idite na **Podešavanje** > **Sigurnosni alati** i aktivirajte traku klizača pokraj opcije **Zaštiti sve preglednike**.

Da biste riješili pogrešku preusmjeravanja web stranica, slijedite upute u nastavku:

Kada dovršite svaki korak, provjerite funkcionira li Zaštita bankarstva i plaćanja.

Ako prozor preglednika i dalje ne funkcionira, dovršite sljedeći korak dok ne počne funkcionirati.

1. Ponovno pokrenite računalo.

2. Provjerite upotrebljavate li najnoviju verziju operacijskog sustava Windows i ESET Internet Security: nadogradite ESET-ove Windows programe za kućne korisnike na najnoviju verziju.

3. Možda je došlo do sukoba sa sigurnosnim softverom, VPN-om ili firewallom treće strane. Privremeno deaktivirajte ili deinstalirajte ovaj softver.

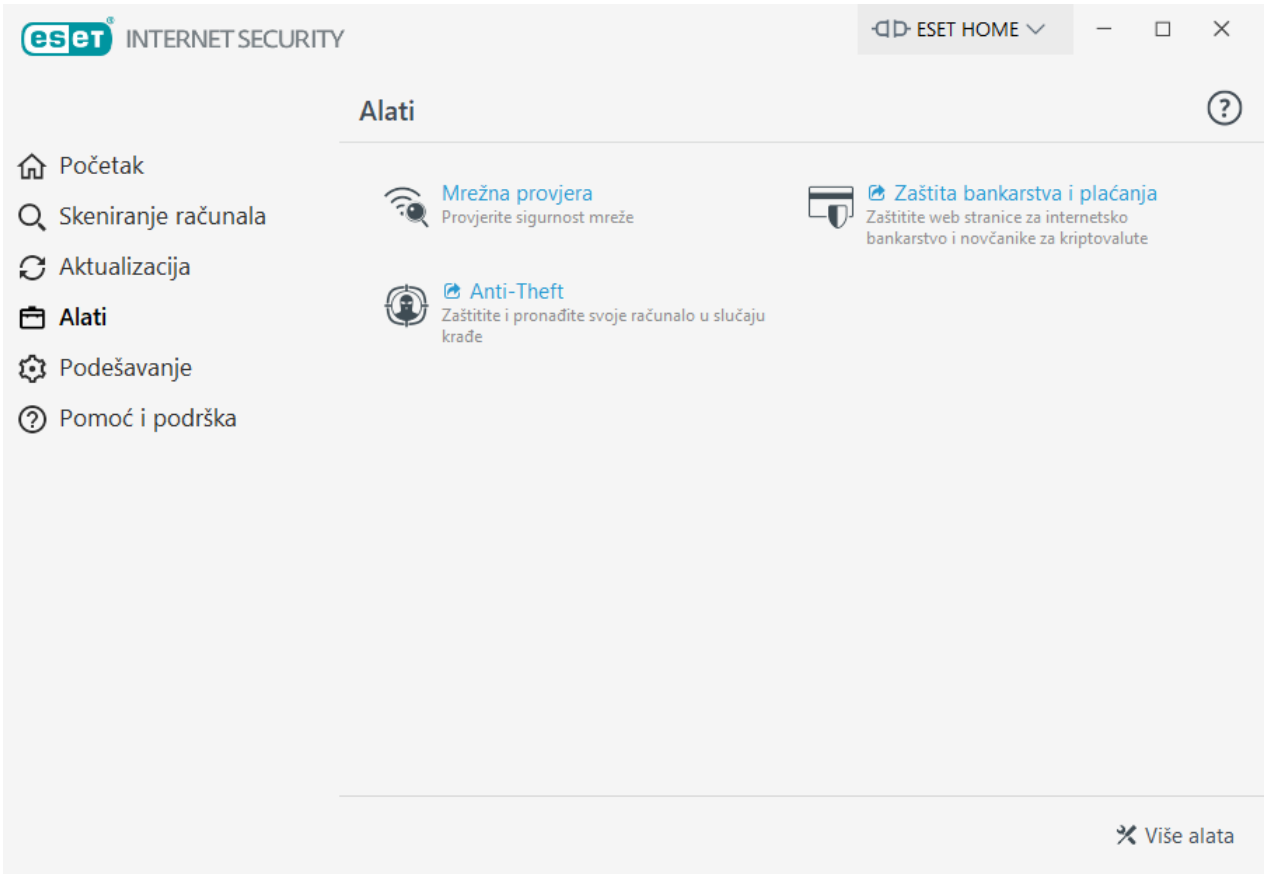
4. Deaktivirajte sva proširenja preglednika treće strane.

5. Izbrišite predmemoriju preglednika. Kako izbrisati predmemoriju preglednika Firefox ili izbrisati predmemoriju preglednika Google Chrome u svom pregledniku?

6. Pobrinite se da vaš standardni preglednik nije izuzet u izborniku **Napredno podešavanje** > **Web i e-pošta** > **Filtriranje protokola** > **Izuzete aplikacije**. Otvorite Napredno podešavanje.

7. Ako niste nadogradili ESET-ov program u prethodnim koracima, deinstalirajte i ponovno instalirajte ESET-ov program. Ponovno pokrenite računalo nakon instalacije.

8. Ako se problem nastavi, možete aktivirati opciju Zaštiti sve preglednike ili pristupiti zaštićenom pregledniku u glavnom prozoru programa > **Alati** > **Zaštita bankarstva i plaćanja**.



Zaštita bankarstva i plaćanja dodatni je sloj zaštite osmišljen za zaštitu financijskih podataka tijekom mrežnih transakcija.

U većini slučajeva zaštićeni preglednik Zaštite bankarstva i plaćanja pokreće se u pregledniku koji se trenutačno upotrebljava nakon što posjetite poznatu web stranicu za bankarstvo.

Odaberite jednu od sljedećih opcija konfiguracije ponašanja zaštićenog preglednika:

- **Zaštiti sve preglednike** – ako se ova opcija aktivira, svi podržani web preglednici se pokreću u sigurnom načinu rada. To vam omogućuje pregledavanje interneta, pristup internetskom bankarstvu te kupnju i izvršavanje transakcija na internetu u jednom prozoru zaštićenog preglednika, bez preusmjeravanja.

- **Preusmjeravanje web stranica** (standardno) – web stranice s popisa zaštićenih web stranica i internog popisa internetskog bankarstva se preusmjeravaju u zaštićeni preglednik. Možete odabrati koji se preglednik otvara (standardni ili zaštićeni).

- Obje prethodne opcije su deaktivirane – da biste pristupili zaštićenom pregledniku u programu ESET Internet Security, kliknite **Alati** > **Zaštita bankarstva i plaćanja** ili kliknite ikonu **Zaštita bankarstva i plaćanja** na radnoj površini. Preglednik koji je postavljen kao standardni u sustavu Windows pokreće se u sigurnom načinu rada.

Da biste konfigurirali ponašanje zaštićenog preglednika, pogledajte Napredno podešavanje zaštite bankarstva i plaćanja. Da biste aktivirali funkciju Zaštiti sve preglednike u programu ESET Internet Security, kliknite **Podešavanje** > **Sigurnosni alati** i aktivirajte traku klizača opcije **Zaštiti sve preglednike**.

Za sigurno pregledavanje weba nužna je upotreba šifrirane HTTPS komunikacije. Sljedeći preglednici podržavaju zaštitu bankarstva i plaćanja:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Više informacija o funkcijama zaštite bankarstva i plaćanja pročitajte u sljedećim člancima ESET-ove baze znanja dostupnima na engleskom i više drugih jezika:

- Kako koristiti ESET-ovu zaštitu bankovnih plaćanja?
- Aktiviranje ili deaktiviranje ESET-ove Zaštite bankarstva i plaćanja za određenu web-stranicu
- Pauziranje ili deaktivacija Zaštite bankarstva i plaćanja u ESET-ovim Windows programima za kućne korisnike
- ESET-ova Zaštita bankarstva i plaćanja – uobičajene pogreške
- ESET-ov rječnik | Zaštita bankarstva i plaćanja

Ako i dalje ne možete riješiti problem, pošaljite poruku e-pošte ESET-ovoj tehničkoj podršci.

Kako otključati Napredno podešavanje zaštićeno lozinkom

Kada želite pristupiti zaštićenom naprednom podešavanju, prikazuje se prozor za unos lozinke. Ako zaboravite ili izgubite lozinku, kliknite **Vrati lozinku** i unesite adresu e-pošte kojom ste se koristili za registraciju licence. ESET će vam poslati e-poruku s kodom za potvrdu. Unesite kod za potvrdu i zatim upišite i potvrdite novu lozinku. Kod za potvrdu vrijedi sedam dana.

Vraćanje lozinke putem ESET HOME računa – koristite ovu opciju ako je licenca koja se upotrebljava za aktivaciju povezana s vašim ESET HOME računom. Upišite adresu e-pošte koju koristite za prijavu na svoj ESET HOME račun.

Ako se ne možete sjetiti svoje adrese e-pošte ili imate poteškoća s vraćanjem lozinke, kliknite **Obratite se tehničkoj podršci**. Bit ćete preusmjereni na ESET-ovu web stranicu kako biste se obratili našem odjelu tehničke podrške.

Generiraj kod za tehničku podršku – ova opcija generira kod za tehničku podršku. Kopirajte kod koji vam je pružila tehnička podrška i kliknite **Imam kod za potvrdu**. Unesite kod za potvrdu i zatim upišite i potvrdite novu lozinku. Kod za potvrdu vrijedi sedam dana.

Dodatne informacije potražite u članku Otključavanje lozinke za postavke u ESET-ovim Windows programima za kućne korisnike.

Kako riješiti deaktivaciju programa s ESET HOME portala

Program nije aktiviran

Ova poruka o pogrešci se prikazuje kada vlasnik licence deaktivira vaš program ESET Internet Security s ESET HOME portala ili kada se licenca koja se dijeli s vašim ESET HOME računom više ne dijeli. Da biste riješili ovaj problem:

- Kliknite **Aktiviraj** i upotrijebite jednu od metoda aktivacije da biste aktivirali program ESET Internet Security.
- Obavijestite vlasnika licence da je vlasnik licence deaktivirao vaš program ESET Internet Security ili da se licenca više ne dijeli s vama. Vlasnik može riješiti problem u programu ESET HOME.

Program deaktiviran, uređaj odspojen

Ova poruka o pogrešci se prikazuje nakon uklanjanja uređaja s ESET HOME računa. Da biste riješili ovaj problem:

- Kliknite **Aktiviraj** i upotrijebite jednu od metoda aktivacije da biste aktivirali program ESET Internet Security.
- Obavijestite vlasnika licence da je vaš program ESET Internet Security deaktiviran i da je uređaj odspojen s ESET HOME portala.
- Ako ste vi vlasnik licence i niste upoznati s ovim promjenama, pregledajte Sažetak sadržaja aktivnosti za ESET HOME. Ako uočite bilo kakvu sumnjivu aktivnost, promijenite svoju lozinku za ESET HOME račun i obratite se ESET-ovoj tehničkoj podršci.

Program deaktiviran, uređaj odspojen

Ova poruka o pogrešci se prikazuje nakon uklanjanja uređaja s ESET HOME računa. Da biste riješili ovaj problem:

- Kliknite **Aktiviraj** i upotrijebite jednu od metoda aktivacije da biste aktivirali program ESET Internet Security.
- Obavijestite vlasnika licence da je vaš program ESET Internet Security deaktiviran i da je uređaj odspojen s ESET HOME portala.
- Ako ste vi vlasnik licence i niste upoznati s ovim promjenama, pregledajte Sažetak sadržaja aktivnosti za ESET HOME. Ako uočite bilo kakvu sumnjivu aktivnost, promijenite svoju lozinku za ESET HOME račun i obratite se ESET-ovoj tehničkoj podršci.

Program nije aktiviran

Ova poruka o pogrešci se prikazuje kada vlasnik licence deaktivira vaš program ESET Internet Security s ESET HOME portala ili kada se licenca koja se dijeli s vašim ESET HOME računom više ne dijeli. Da biste riješili ovaj

problem:

• Kliknite **Aktiviraj** i upotrijebite jednu od metoda aktivacije da biste aktivirali program ESET Internet Security.

• Obavijestite vlasnika licence da je vlasnik licence deaktivirao vaš program ESET Internet Security ili da se licenca više ne dijeli s vama. Vlasnik može riješiti problem u programu ESET HOME.

Program za poboljšanje iskustva korisnika

Pridruživanjem Programu za poboljšanje iskustva korisnika pružate ESET-u anonimne informacije o upotrebi naših programa. Više informacija o obradi podataka dostupno je u našim Pravilima privatnosti.

Vaš pristanak

Sudjelovanje u spomenutom programu dobrovoljno je i temelji se na vašem pristanku. Nakon što se pridružite, sudjelovanje je pasivno, što znači da ne trebate poduzeti nikakve daljnje radnje. Svoj pristanak možete povući u bilo kojem trenutku promjenom postavki programa. Tako ćete spriječiti daljnju obradu svojih anonimnih podataka.

Svoj pristanak možete povući u bilo kojem trenutku promjenom postavki programa:

- Promijenite postavke programa za poboljšanje iskustva korisnika u ESET-ovim Windows programima za kućnu upotrebu

Koje vrste informacija prikupljamo?

Podaci o interakciji s programima

Te informacije govore nam više o načinu na koji se naši programi upotrebljavaju. Zahvaljujući njima znamo, na primjer, koje se funkcije upotrebljavaju često, koje postavke korisnici mijenjaju ili koliko vremena potroše koristeći se programom.

Podaci o uređajima

Te informacije prikupljamo da bismo razumjeli gdje se naši programi upotrebljavaju i na kojim uređajima. Uobičajeni primjeri uključuju model uređaja, zemlju, verziju i naziv operacijskog sustava.

Dijagnostički podaci o pogreškama

Prikupljaju se i informacije o pogreškama i padovima sustava. Na primjer, koja se pogreška pojavila i koje su radnje dovele do nje.

Zašto prikupljamo te informacije?

Te anonimne informacije omogućuju nam da poboljšamo svoje programe za korisnike. Pomažu nam da povećamo relevantnost i jednostavnost upotrebe svojih programa i smanjimo učestalost njihovih pogrešaka.

Tko upravlja tim informacijama?

ESET, spol. s r.o. jedini je voditelj obrade podataka prikupljenih u sklopu Programa. Te informacije ne dijele se s trećim stranama.

Licenčni ugovor za krajnjeg korisnika

Stupa na snagu 19. listopada 2021..

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 („Ugovor”) sklopljenog između tvrtke ESET, spol. s r. o., sa sjedištem na adresi Einsteinova 24, 85101 Bratislava, Slovak Republic, registrirane u trgovačkom registru Okružnog suda u Bratislavi I, odjeljak Sro, unos br. 3586/B, registracijski broj tvrtke: 31333532 (dalje u tekstu: „ESET” ili „dobavljač”) i vas, fizičke ili pravne osobe („vi” ili „krajnji korisnik”), imate pravo na upotrebu softvera utvrđenog 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 daljnjem tekstu.

OVO 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 izražavate suglasnost s uvjetima i odredbama ovog Ugovora i slažete se s Pravilima privatnosti. Ako se ne slažete s nekim od uvjeta ili nekom od odredbi Ugovora i/ili Pravila privatnosti, 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 pojam „Softver” znači sljedeće: (i) računalni program koji se isporučuje s ovim Ugovorom i svi njegovi dijelovi; (ii) cjelokupan 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 („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 konfigurirano 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 stanice, 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 i odredbama ovog Ugovora i poštujete sve ugovorne uvjete i odredbe, Dobavljač Vam dodjeljuje sljedeća prava ("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, „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 prihvaća 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) **Home/Business Edition.** Home Edition verzija softvera mora se upotrebljavati isključivo u privatnim i/ili nekomercijalnim okruženjima i isključivo za osobne ili obiteljske potrebe. Za korištenje softvera u komercijalnom okruženju te za korištenje softvera na serverima za poštu, relejima za poštu, pristupnicima za poštu ili internetskim pristupnicima potrebno je nabaviti Business Edition verziju softvera.

d) **Trajanje Licence.** Vaše pravo korištenja Softvera vremenski je ograničeno.

e) **OEM Softver.** Softver klasificiran kao „OEM” ograničen 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 lijek dostupan Dobavljaču u takvom slučaju. U slučaju poništavanja 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 ili nadogradnje softvera („aktualizacije"), ali nije obvezan nuditi aktualizacije. Ta je funkcija aktivirana u standardnim postavkama softvera te se aktualizacije instaliraju automatski, osim ako krajnji korisnik deaktivira automatsko instaliranje aktualizacija. U svrhu pružanja aktualizacija potrebno je provjeriti autentičnost licence, uključujući podatke o računalu i/ili platformi na kojoj je instaliran softver u skladu s Pravilima privatnosti.

Pružanje aktualizacija može biti podložno Pravilima o isteku vijeka trajanja („Pravila o isteku vijeka trajanja") koja su dostupna na https://go.eset.com/eol_home. Aktualizacije se neće pružati nakon što softver ili bilo koja njegova funkcija dosegne datum isteka vijeka trajanja koji je naveden u Pravilima o isteku vijeka trajanja.

b) **Prosljeđivanje infiltracija i informacija Dobavljaču.** Softver sadrži funkcije koje prikupljaju uzorke 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 („Infiltracije"), a zatim ih šalju Dobavljaču, uključujući, ali ne isključivo, informacije o instalacijskom postupku, Računalu i/ili platformi na kojoj je Softver instaliran te informacije o operacijama i funkcionalnosti Softvera („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 prihvaćanja 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.

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 prenositi 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 dupliciranih 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. Vaše pravo na korištenje softvera i svih njegovih funkcija može biti podložno Pravilima o isteku vijeka trajanja. Nakon što softver ili bilo koja njegova funkcija dosegne datum isteka vijeka trajanja koji je naveden u Pravilima o isteku vijeka trajanja, nećete više imati pravo na korištenje softvera. Bez obzira na način prekida ovog Ugovora, odredbe članaka 7., 8., 11., 13., 19. i 21. primjenjuju se bez vremenskog ograničenja.

11. **IZJAVE KRAJNJEG KORISNIKA**. KAO KRAJNJI KORISNIK PRIHVAĆATE ČINJENICU DA SE SOFTVER ISPORUČUJE „U ZATEČENOM STANJU“, BEZ IKAKVOG 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 MJERODAVNIM ZAKONIMA, NI DOBAVLJAČ, NI NJEGOVI ZAPOSLENICI NI DAVATELJI LICENCE NE SNOSE 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 INSTALACIJOM, KORIŠTENJEM ILI NEMOGUĆNOŠĆU KORIŠTENJA SOFTVERA, ČAK I U SLUČAJU DA SU DOBAVLJAČ ILI NJEGOVI DAVATELJI LICENCE ILI POVEZANA DRUŠTVA 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. Tehnička podrška se prestaje pružati nakon što softver ili bilo koja njegova funkcija dosegne datum isteka vijeka trajanja koji je naveden u Pravilima o isteku vijeka trajanja. 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 ("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 („Zakoni kontrole izvoza”) te

ii. bilo koje ekonomske, 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.

(zakonski akti navedeni u točkama i. i ii. iznad zajednički se nazivaju „Zakoni o kontroli trgovine”).

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 trpjeti 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, 85101 Bratislava, Slovak Republic, ne dovodeći u pitanje pravo tvrtke ESET da vam priopći bilo kakve izmjene ovog Ugovora, Pravila privatnosti, Pravila o isteku vijeka trajanja i dokumentacije u skladu s čl. 22. Ugovora. ESET vam može slati e-poruke, obavijesti u aplikacijama putem softvera ili objaviti komunikaciju na svojoj web stranici. Pristajete primati komunikaciju o pravnim pitanjima od ESET-a u elektroničkom obliku, uključujući svaku komunikaciju koja se odnosi na izmjene Uvjeta, posebnih uvjeta ili Pravila privatnosti, sve prijedloge/prihvaćanja ugovora ili pozive na ponudu, obavijesti ili druge vrste komunikacije o pravnim pitanjima. Takva elektronička komunikacija smatra se primljenom u pisanom obliku, osim ako važeći zakoni izričito ne zahtijevaju drugačiji oblik komunikacije.

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. Ovaj je Ugovor sklopljen na engleskom jeziku. U slučaju prevođenja Ugovora radi praktičnosti ili bilo koje druge svrhe ili u slučaju odstupanja između različitih jezičnih verzija ovog Ugovora, mjerodavna je verzija na engleskom jeziku.

ESET zadržava pravo izmjene softvera te izmjene uvjeta ovog Ugovora, njegovih priloga, dodataka, Pravila privatnosti, Pravila o isteku vijeka trajanja i dokumentacije ili bilo kojih njihovih dijelova u svakom trenutku tako da ažurira relevantni dokument (i) u svrhu odražavanja izmjena softvera ili načina na koji ESET posluje, (ii) iz pravnih, regulatornih ili sigurnosnih razloga ili (iii) u svrhu sprječavanja zloupotrebe ili štete. O svakoj izmjeni ovog Ugovora bit ćete obaviješteni putem e-pošte, obavijesti unutar aplikacije ili drugim elektroničkim putem. Ako se ne slažete s predloženim izmjenama Ugovora, možete ga raskinuti u skladu s čl. 10. u roku od 30 dana od primitka obavijesti o promjeni. Ako ne raskinete Ugovor u tom roku, predložene promjene smatrat će se prihvaćenima i stupit će na snagu od datuma primitka obavijesti o promjeni.

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.

DODATAK UGOVORU

Sigurnosna procjena uređaja povezanih na mrežu. Na sigurnosnu procjenu uređaja povezanih na mrežu primjenjuju se dodatne odredbe kako slijedi:

Softver sadrži funkciju za provjeru sigurnosti lokalne mreže Krajnjeg korisnika i sigurnosti uređaja u lokalnoj mreži. Za ovu su funkciju potrebni naziv lokalne mreže i podaci o uređajima u lokalnoj mreži, kao što su prisutnost, vrsta, naziv, IP adresa i MAC adresa uređaja u lokalnoj mreži u vezi s podacima o licenci. Ovi podaci također uključuju vrstu zaštite bežične mreže i vrstu šifriranja bežične mreže za routere. Ova funkcija također može pružiti informacije o dostupnosti sigurnosnog softverskog rješenja radi zaštite uređaja u lokalnoj mreži.

Zaštita od zlouporabe podataka Na zaštitu od zlouporabe podataka primjenjuju se dodatne odredbe kako slijedi:

Softver sadrži funkciju koja sprečava gubitak ili zlouporabu kritičnih podataka u izravnoj vezi s krađom Računala. Ta funkcija isključena je prema standardnim postavkama Softvera. Za aktivaciju je potrebno stvoriti ESET HOME račun. Pomoću tog računa funkcija aktivira prikupljanje podataka u slučaju krađe računala. Ako odlučite aktivirati

ovu funkciju Softvera, prikupljat će se podaci o ukradenom Računalu i slati Dobavljaču. Oni mogu sadržavati podatke o mrežnoj lokaciji Računala, podatke o sadržaju prikazanom na zaslonu Računala, podatke o konfiguraciji Računala i/ili podatke snimljene kamerom povezanom s Računalom (u daljnjem tekstu: "Podaci"). Krajnji korisnik ima pravo upotrebljavati Podatke koji su prikupljeni pomoću ove funkcije i koji su pruženi putem ESET HOME računa isključivo za rješavanje negativnih posljedica koje su nastale uslijed krađe Računala. Samo u svrhu te funkcije Dobavljač obrađuje Podatke kao što je navedeno u Pravilima privatnosti i definirano važećim zakonskim propisima. Dobavljač je dužan omogućiti Krajnjem korisniku pristup Podacima za razdoblje potrebno za ostvarenje svrhe za koju su Podaci prikupljeni, a koje ne smije biti dulje od razdoblja zadržavanja podataka navedenog u Pravilima privatnosti. Zaštita od zlouporabe podataka upotrebljava se isključivo na Računalima i računima kojima Krajnji korisnik ima legitiman pristup. Svaka nezakonita upotreba prijavit će se nadležnom tijelu. Dobavljač je dužan poštovati odgovarajuće zakone i surađivati s nadležnim tijelima u slučaju zlouporabe. Slažete se i prihvaćate odgovornost za zaštitu lozinke za pristup ESET HOME računu i slažete se da nećete dijeliti lozinku s trećim stranama. Krajnji korisnik odgovoran je za svaku aktivnost prilikom koje se upotrebljava funkcija Zaštite od zlouporabe podataka i ESET HOME račun, bez obzira na autorizaciju. Ako je račun za ESET HOME ugrožen, odmah obavijestite Dobavljača. Dodatne odredbe za zaštitu od zlouporabe podataka primjenjuju se isključivo na krajnje korisnike programa ESET Internet Security i ESET Smart Security Premium.

ESET Secure Data. Na ESET Secure Data se primjenjuju dodatne odredbe kako slijedi:

1. Definicije. U ovim dodatnim odredbama za program ESET Secure Data riječi u nastavku imaju sljedeće značenje:

a) „Informacije” bilo koje informacije ili podaci koji su šifrirani ili dešifrirani pomoću softvera;

b) „Proizvodi” softver i dokumentacija programa ESET Secure Data;

c) „ESET Secure Data” softver odnosno softveri koji se upotrebljavaju za šifriranje i dešifriranje elektroničkih podataka;

Sva pozivanja na množinu uključuju jedninu, a sva pozivanja na muški rod uključuju ženski i srednji rod te obratno. Riječi bez određenih definicija upotrebljavat će se u skladu s definicijama navedenim u Ugovoru.

2. Dodatna izjava Krajnjeg korisnika. Potvrđujete i prihvaćate sljedeće:

a) dužni ste štititi, održavati i sigurnosno kopirati informacije;

b) trebate u potpunosti sigurnosno kopirati sve Informacije i podatke (uključujući, bez ograničenja, sve kritične informacije i podatke) na svojem Računalu prije instalacije softvera ESET Secure Data;

c) morate održavati sigurnu evidenciju svih lozinki i drugih informacija koje se upotrebljavaju za podešavanje i upotrebu softvera ESET Secure Data te morate sigurnosno kopirati sve ključeve za šifriranje, licenčne kodove, datoteke s ključevima i ostale podatke koji se generiraju na zaseban medij za pohranu;

d) odgovorni ste za upotrebu Proizvoda. Dobavljač nije odgovoran ni za koji gubitak, potraživanje ni štetu koji su pretrpljeni kao posljedica bilo kojeg neovlaštenog ili pogrešnog šifriranja ili dešifriranja Informacija ili drugih podataka gdje god i na koji se god način te Informacije ili drugi podaci pohranjuju;

e) premda je Dobavljač poduzeo sve razumne korake za osiguravanje integriteta i sigurnosti softvera ESET Secure Data, Proizvodi (ili bilo koji pojedinačan proizvod) ne smiju se upotrebljavati ni u kojem području koje ovisi o sigurnosnoj razini zaštićenoj od zakazivanja („fail-safe”) ili koje je potencijalno rizično ili opasno, uključujući bez ograničenja nuklearna postrojenja, navigaciju letjelica, kontrolne ili komunikacijske sustave, sustave oružja i obrane te sustave za nadzor ili održavanje životnih funkcija;

f) Krajnji korisnik dužan je provjeriti je li razina sigurnosti i šifriranja koju pružaju proizvodi primjerena za Vaše potrebe;

g) odgovorni ste za vlastitu upotrebu Proizvoda ili bilo kojeg pojedinačnog proizvoda, što obuhvaća bez ograničenja provjeru je li ta upotreba u skladu sa svim primjenjivim zakonima i propisima Slovačke Republike ili neke druge zemlje, regije ili države u kojoj se upotrebljava Proizvod. Prije bilo koje upotrebe Proizvoda morate potvrditi da ta upotreba nije u suprotnosti s bilo kojim vladinim (u Slovačkoj Republici ili negdje drugdje) embargom;

h) softver ESET Secure Data može povremeno kontaktirati s Dobavljačevim serverima kako bi provjerio postoje li informacije o licenci, dostupne zakrpe, servisni paketi i druge nadogradnje koje mogu poboljšati, održati, izmijeniti ili unaprijediti rad softvera ESET Secure Data i može slati informacije o sustavu povezane sa svojim radom u skladu s Pravilima privatnosti.

i) Dobavljač nije odgovoran ni za kakav gubitak, štetu, trošak ili potraživanje koji proizlaze iz gubitka, krađe, zloupotrebe, kvarenja, oštećenja ili uništenja lozinki, informacija o podešavanju, ključeva za šifriranje, aktivacijskih kodova licence i drugih podataka koji se generiraju ili pohranjuju tijekom upotrebe Softvera.

Dodatne odredbe za ESET Secure Data primjenjuju se isključivo na krajnje korisnike programa ESET Smart Security Premium.

Softver Password Manager. Na softver Password Manager primjenjuju se dodatne odredbe kako slijedi:

1. Dodatna izjava Krajnjeg korisnika. Potvrđujete i prihvaćate da ne smijete činiti sljedeće:

a) upotrebljavati softver Password Manager ni za koju primjenu od ključne važnosti u kojoj mogu biti ugroženi ljudski životi ili imovina. Razumijete da softver Password Manager nije osmišljen u te svrhe i da kvar u tim slučajevima može dovesti do smrti, osobnih ozljeda ili ozbiljne štete po imovinu ili okoliš, za što Dobavljač nije odgovoran.

SOFTVER PASSWORD MANAGER NIJE OSMIŠLJEN, NAMIJENJEN NI LICENCIRAN ZA UPOTREBU U OPASNIM OKRUŽENJIMA U KOJIMA SU POTREBNE KONTROLE ZA ZAŠTITU OD ZAKAZIVANJA, UKLJUČUJUĆI, ALI NE ISKLJUČIVO, DIZAJN, KONSTRUKCIJU, ODRŽAVANJE ILI RAD NUKLEARNIH POSTROJENJA, NAVIGACIJSKIH ILI KOMUNIKACIJSKIH SUSTAVA ZA LETJELICE, KONTROLE ZRAČNOG PROMETA, SUSTAVA ZA ODRŽAVANJE ŽIVOTNIH FUNKCIJA ILI SUSTAVA ORUŽJA. DOBAVLJAČ SE POSEBNO ODRIČE SVIH IZRIČITIH ILI PODRAZUMIJEVANIH JAMSTAVA POGODNOSTI ZA TAKVE SVRHE.

b) upotrebljavati softver Password Manager na način koji je u suprotnosti s ovim ugovorom ili zakonima Slovačke Republike ili vaše nadležnosti. Posebice ne smijete upotrebljavati softver Password Manager za provođenje ili promicanje bilo kakvih nezakonitih aktivnosti, uključujući učitavanje podataka štetnog sadržaja ili sadržaja koji se može upotrijebiti za bilo koje nezakonite aktivnosti ili koji na bilo koji način krši zakon ili prava bilo koje treće strane (uključujući sva prava intelektualnog vlasništva), uključujući bez ograničenja bilo koje pokušaje ostvarenja pristupa računima u spremištu (u svrhu ovih dodatnih uvjeta za softver Password Manager „spremište" se odnosi na prostor za pohranu podataka kojim upravlja dobavljač ili treća strana koja nije dobavljač i korisnik u svrhu aktiviranja sinkronizacije i sigurnosnog kopiranja korisničkih podataka) ili bilo kojim računima i podacima drugih korisnika softvera Password Manager ili spremišta. Ako prekršite bilo koju navedenu odredbu, Dobavljač ima pravo odmah raskinuti ovaj ugovor i zatražiti od vas naknadu troškova bilo kojeg potrebnog pravnog lijeka i poduzeti potrebne korake da bi spriječio vašu daljnju upotrebu softvera Password Manager bez mogućnosti povrata novca.

2. OGRANIČENJE ODGOVORNOSTI. SOFTVER PASSWORD MANAGER PRUŽA SE „KAKAV JEST". NE POSTOJI IZRIČITO ILI PODRAZUMIJEVANO JAMSTVO BILO KOJE VRSTE. SOFTVER UPOTREBLJAVATE NA VLASTITI RIZIK. PROIZVOĐAČ NIJE ODGOVORAN ZA GUBITAK PODATAKA, ŠTETU I OGRANIČENJE DOSTUPNOSTI USLUGE, UKLJUČUJUĆI BILO KOJE PODATKE KOJE SOFTVER PASSWORD MANAGER POŠALJE VANJSKOM SPREMIŠTU RADI SINKRONIZACIJE I SIGURNOSNOG KOPIRANJA PODATAKA. ŠIFRIRANJE PODATAKA POMOĆU SOFTVERA PASSWORD MANAGER NE PODRAZUMIJEVA NIKAKVU ODGOVORNOST DOBAVLJAČA U POGLEDU SIGURNOSTI PODATAKA. IZRIČITO SE

SLAŽETE DA SE PODACI KOJI SE DOBIVAJU, UPOTREBLJAVAJU, ŠIFRIRAJU, SINKRONIZIRAJU ILI ŠALJU POMOĆU SOFTVERA PASSWORD MANAGER TAKOĐER MOGU POHRANITI NA SERVERIMA TREĆIH STRANA (PRIMJENJUJE SE SAMO NA UPOTREBU SOFTVERA PASSWORD MANAGER U KOJOJ SU OMOGUĆENE USLUGE SINKRONIZACIJE I SIGURNOSNOG KOPIRANJA). AKO DOBAVLJAČ PO SVOM NAHOĐENJU ODLUČI UPOTRIJEBITI SPOMENUTO SPREMIŠTE, WEB-STRANICU, WEB-PORTAL, SERVER ILI USLUGU TREĆE STRANE, ON NIJE ODGOVORAN ZA KVALITETU, SIGURNOST ILI DOSTUPNOST TE USLUGE TREĆE STRANE I NI U KOJOJ MJERI NE SNOSI ODGOVORNOST PREMA VAMA ZA BILO KOJE KRŠENJE UGOVORNIH ILI ZAKONSKIH OBVEZA TREĆE STRANE KAO NI ZA ŠTETU, GUBITAK PROFITA, FINANCIJSKU ILI NEFINACIJSKU ŠTETU ILI BILO KOJU DRUGU VRSTU GUBITKA NASTALU ZA VRIJEME UPOTREBE OVOG SOFTVERA. DOBAVLJAČ NIJE ODGOVORAN ZA SADRŽAJ BILO KOJIH PODATAKA KOJI SE DOBIVAJU, UPOTREBLJAVAJU, ŠIFRIRAJU, POHRANJUJU, SINKRONIZIRAJU ILI ŠALJU POMOĆU SOFTVERA PASSWORD MANAGER ILI U SPREMIŠTU. POTVRĐUJETE DA DOBAVLJAČ NEMA PRISTUP SADRŽAJU POHRANJENIH PODATAKA I NIJE U MOGUĆNOSTI NADZIRATI GA ILI UKLONITI ZAKONSKI ŠTETAN SADRŽAJ.

Dobavljač posjeduje sva prava na poboljšanja, nadogradnje i popravke povezane sa softverom Password MANAGER („poboljšanja”), čak i ako su ta poboljšanja stvorena na temelju povratnih informacija, ideja ili prijedloga koje ste vi poslali u bilo kojem obliku. Nećete imati pravo ni na kakvu naknadu, uključujući bilo koje autorske naknade povezane s takvim poboljšanjima.

TVRTKE I DAVATELJI LICENCE DOBAVLJAČA NISU NI NA KOJI NAČIN ODGOVORNI ZA VAŠA POTRAŽIVANJA I ZAHTJEVE BILO KOJE VRSTE KOJI PROIZLAZE IZ VAŠE UPOTREBE SOFTVERA ILI SU NA BILO KOJI NAČIN POVEZANI S VAŠOM UPOTREBOM SOFTVERA PASSWORD MANAGER ILI NJEGOVOM UPOTREBOM OD STRANE TREĆIH STRANA, S UPOTREBOM ILI NEUPOTREBOM BILO KOJEG BROKERSKOG DRUŠTVA ILI TRGOVCA, ILI S PRODAJOM ILI KUPNJOM BILO KOJEG OSIGURANJA, NEOVISNO O TOME TEMELJE LI SE NAVEDENA POTRAŽIVANJA I OBVEZE NA ZAKONU ILI PRAVIČNOSTI.

SUBJEKTI I IZDAVAČI LICENCE DOBAVLJAČA NE SNOSE ODGOVORNOST PREMA VAMA NI ZA KOJU IZRAVNU, SLUČAJNU, POSEBNU, NEIZRAVNU ILI POSLJEDIČNU ŠTETU KOJA PROIZLAZI IZ ILI JE POVEZANA S BILO KOJIM SOFTVEROM TREĆE STRANE, BILO KOJIM PODACIMA KOJIMA JE PRISTUPLJENO PUTEM SOFTVERA PASSWORD MANAGER, VAŠOM UPOTREBOM ILI NEMOGUĆNOSTI UPOTREBE ILI PRISTUPA SOFTVERU PASSWORD MANAGER, ILI BILO KOJIM PODACIMA KOJI SE PRUŽE PUTEM SOFTVERA PASSWORD MANAGER, NEOVISNO O TOME TEMELJE LI SE NAVEDENI ODŠTETNI ZAHTJEVI NA ZAKONU ILI PRAVIČNOSTI. ŠTETA KOJA NIJE OBUHVAĆENA OVOM KLAUZULOM UKLJUČUJE, BEZ OGRANIČENJA, ŠTETU UZROKOVANU GUBITKOM POSLOVNE DOBITI, OSOBNIM OZLJEDAMA ILI OŠTEĆENJEM IMOVINE, PREKIDOM POSLOVANJA, GUBITKOM POSLOVANJA ILI OSOBNIH INFORMACIJA. NEKE NADLEŽNOSTI NE DOPUŠTAJU OGRANIČAVANJE SLUČAJNE ILI POSLJEDIČNE ŠTETE PA SE TO OGRANIČENJE NE MORA ODNOSITI NA VAS. U TOM ĆE SLUČAJU OPSEG ODGOVORNOSTI DOBAVLJAČA BITI JEDNAK MINIMUMU DOPUŠTENOM PRIMJENJIVIM ZAKONOM.

INFORMACIJE KOJE SE PRUŽAJU PUTEM SOFTVERA PASSWORD MANAGER, UKLJUČUJUĆI BURZOVNE KOTACIJE, ANALIZU, INFORMACIJE O TRŽIŠTU, VIJESTI I FINANCIJSKE PODATKE, MOGU BITI ZAKAŠNJELI, NETOČNI ILI SADRŽAVATI POGREŠKE ILI PROPUSTE, ZA ŠTO TVRTKE I DAVATELJI LICENCE DOBAVLJAČA NE SNOSE ODGOVORNOST. DOBAVLJAČ MOŽE PROMIJENITI ILI UKINUTI BILO KOJI ASPEKT ILI ZNAČAJKU SOFTVERA PASSWORD MANAGER ILI UPOTREBU SVIH ILI POJEDINIH ZNAČAJKI ILI TEHNOLOGIJE SOFTVERA PASSWORD MANAGER U BILO KOJEM TRENUTKU, A DA VAS O TOME NE MORA PRETHODNO OBAVIJESTITI.

AKO SU ODREDBE OVOG ČLANKA NIŠTAVNE IZ BILO KOJEG RAZLOGA ILI AKO SE UTVRDI DA JE DOBAVLJAČ ODGOVORAN ZA GUBITKE, ŠTETU ITD. PREMA PRIMJENJIVIM ZAKONIMA, STRANE SE SLAŽU DA ĆE DOBAVLJAČEVA ODGOVORNOST PREMA VAMA BITI OGRANIČENA NA UKUPAN IZNOS LICENČNIH NAKNADA KOJE STE PLATILI.

SLAŽETE SE DA ĆETE OBEŠTETITI, ŠTITITI I OSLOBODITI ODGOVORNOSTI DOBAVLJAČA I NJEGOVE ZAPOSLENIKE, PODRUŽNICE, POVEZANA DRUŠTVA, REBRANDING I DRUGE PARTNERE OD I PROTIV BILO KOJIH POTRAŽIVANJA, OBVEZA, ŠTETA, GUBITAKA, TROŠKOVA, IZDATAKA I NAKNADA TREĆIH STRANA (UKLJUČUJUĆI VLASNIKE UREĐAJA ILI STRANE NA ČIJA SU PRAVA UTJECALI PODACI UPOTRIJEBLJENI U SOFTVERU PASSWORD MANAGER ILI

SPREMIŠTU) KOJE TE STRANE MOGU PRETRPJETI KAO REZULTAT VAŠE UPOTREBE SOFTVERA PASSWORD MANAGER.

3. Podaci u softveru Password Manager. Ako izričito ne odaberete drukčije, svi podaci koje unesete i koji se spremaju u bazu podataka softvera Password Manager pohranjuju se u šifriranom obliku na vaše računalo ili na drugi uređaj za pohranu koji odredite. Razumijete da će se u slučaju brisanja ili oštećenja bilo koje baze podataka ili drugih datoteka softvera Password Manager svi podaci koji se nalaze ondje nepovratno izgubiti te shvaćate i prihvaćate rizik tog gubitka. Činjenica da se vaši osobni podaci pohranjuju na računalo u šifriranom obliku ne znači da te informacije ne može ukrasti ili zloupotrijebiti netko tko otkrije glavnu lozinku ili ostvari pristup korisnički definiranom aktivacijskom uređaju za otvaranje baze podataka. Dužni ste brinuti se za sigurnost svih pristupnih metoda.

4. Slanje osobnih podataka dobavljaču ili spremištu. Ako to odaberete, isključivo u svrhu osiguranja pravovremene sinkronizacije i sigurnosnog kopiranja podataka, softver Password Manager Software šalje osobne podatke, točnije lozinke, informacije za prijavu, račune i identitete, internetskim putem iz baze podataka softvera u spremište. Podaci se šalju isključivo u šifriranom obliku. Upotreba softvera Password Manager za popunjavanje internetskih obrazaca lozinkama, podacima za prijavu i drugim podacima može zahtijevati slanje informacija internetskim putem na web-stranicu koju odredite. To slanje podataka ne pokreće softver Password Manager i zato Dobavljač nije odgovoran za sigurnost navedenih interakcija s bilo kojom web-stranicom koju podržavaju različiti dobavljači. Bilo koje transakcije putem interneta, neovisno o tome jesu li povezane sa softverom Password Manager, vršite po svom nahođenju i snosite rizik za njih te ćete snositi isključivu odgovornost za bilo koju štetu na svom računalom sustavu ili gubitak podataka koji proizlazi iz preuzimanja i/upotrebe bilo kojeg navedenog materijala ili usluge. Kako bi se smanjio rizik od gubitka vrijednih podataka, Dobavljač preporučuje korisnicima redovito sigurnosno kopiranje baze podataka i drugih osjetljivih datoteka na vanjske pogone. Dobavljač vam ni na koji način ne može pomoći da vratite izgubljene ili oštećene podatke. Ako Dobavljač pruža uslugu sigurnosnog kopiranja datoteka iz korisnikove baze podataka za slučaj oštećenja ili brisanja datoteka na korisnikovom računalu, ta usluga sigurnosnog kopiranja nije zajamčena i ne podrazumijeva nikakvu odgovornost Dobavljača prema vama.

Upotrebom softvera Password Manager slažete se da softver može povremeno kontaktirati s Dobavljačevim serverima kako bi provjerio postoje li informacije o licenci, dostupne zakrpe, servisni paketi i druge nadogradnje koje mogu poboljšati, održati, izmijeniti ili unaprijediti rad softvera Password Manager. Softver može slati opće informacije o sustavu povezane s funkcioniranjem softvera Password Manager u skladu s Pravilima privatnosti.

5. Informacije i upute za deinstalaciju. Sve informacije iz baze podataka koje želite zadržati trebate izvesti prije deinstalacije softvera Password Manager.

Dodatne odredbe za softver Password Manager primjenjuju se isključivo na krajnje korisnike programa ESET Smart Security Premium.

ESET LiveGuard. Na ESET LiveGuard se primjenjuju dodatne odredbe kako slijedi:

Softver sadrži funkciju dodatne analize datoteka koje je poslao krajnji korisnik. Dobavljač će datoteke koje je poslao krajnji korisnik i rezultate analize koristiti samo u skladu s Pravilima privatnosti i važećim zakonskim propisima.

Dodatne odredbe za ESET LiveGuard primjenjuju se isključivo na krajnje korisnike programa ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Pravila privatnosti

Zaštita osobnih podataka vrlo je važna tvrtki ESET, spol. s.r.o., s registriranim uredom na adresi Einsteinova 24, 851 01 Bratislava, Slovak Republic, registriranoj u trgovačkom registru Okružnog suda u Bratislavi I, odjeljak Sro, unos br. 3586/B, broj poslovne registracije: 31333532 kao voditelju obrade podataka („ESET" ili „mi"). Želimo se pridržavati zahtjeva transparentnosti koji je zakonski standardiziran na temelju Opće uredbe EU-a o zaštiti podataka („OUZP"). Radi postizanja tog cilja objavljujemo ova Pravila privatnosti isključivo u svrhu informiranja svojih korisnika („krajnji korisnik" ili „vi") kao ispitanika o sljedećim temama zaštite osobnih podataka:

- Pravna osnova za obradu osobnih podataka,
- Dijeljenje podataka i povjerljivost,
- Sigurnost podataka,
- Vaša prava kao ispitanika,
- Obrada vaših osobnih podataka
- Kontaktni podaci.

Pravna osnova za obradu osobnih podataka

Samo je nekoliko pravnih osnova za obradu podataka koje upotrebljavamo u skladu s primjenjivim zakonodavnim okvirom koji se odnosi na zaštitu osobnih podataka. Obrada osobnih podataka u ESET-u uglavnom je potrebna za izvršenje Licenčni ugovor za krajnjeg korisnika („EULA") s krajnjim korisnikom (članak 6. stavak 1. točka (b) OUZP-a), koji se primjenjuje na pružanje ESET-ovih programa ili usluga, osim ako je izričito navedeno drugačije, npr.:

- Pravnom osnovom legitimnog interesa (članak 6. stavak 1. točka (f) OUZP-a) koja nam omogućuje da obrađujemo podatke o tome kako naši korisnici upotrebljavaju naše usluge i podatke o njihovom zadovoljstvu da bismo im pružili najbolju moguću zaštitu, podršku i iskustvo koje možemo ponuditi. Primjenjivi zakoni kao legitiman interes prepoznaju čak i marketing, stoga se obično oslanjamo na taj interes u svrhu marketinške komunikacije sa svojim korisnicima.
- Privolom (članak 6. stavak 1. točka (a) OUZP-a) koju možemo zatražiti od vas u određenim situacijama kada tu pravnu osnovu smatramo najprikladnijom ili kada je propisana zakonom.
- Usklađenošću s pravnom obvezom (članak 6. stavak 1. točka (c) OUZP-a), npr. propisanim zahtjevima za elektroničku komunikaciju, zadržavanje za fakturiranje ili dokumentaciju za naplatu.

Dijeljenje podataka i povjerljivost

Vaše podatke ne dijelimo s trećim stranama. Međutim, ESET je tvrtka koja djeluje diljem svijeta putem povezanih tvrtki ili partnera kao dio svoje mreže za prodaju, usluge i podršku. Informacije o licenciranju, naplati i tehničkoj podršci koje ESET obrađuje mogu se prenijeti povezanim subjektima ili preuzeti od njih radi provedbe Licenčnog ugovora za krajnjeg korisnika, uključujući npr. pružanje usluga ili podrške.

ESET daje prednost obradi svojih podataka u Europskoj uniji (EU). Međutim, ovisno o vašoj lokaciji (upotreba naših programa i/ili usluga izvan EU-a) i/ili usluzi koju odaberete, možda će biti potrebno prenijeti vaše podatke u zemlju izvan EU-a. Na primjer, koristimo usluge trećih strana u vezi s računalstvom u cloudu. U tim slučajevima pažljivo odabiremo davatelje usluga i osiguravamo odgovarajuću razinu zaštite podataka putem ugovornih,

tehničkih i organizacijskih mjera. U pravilu prihvaćamo upotrebu standardnih ugovornih odredbi EU-a, uz dodatne ugovorne propise prema potrebi.

Za neke zemlje izvan EU-a, kao što su Ujedinjena Kraljevina i Švicarska, EU je već utvrdio usporedivu razinu zaštite podataka. Zbog usporedive razine zaštite podataka za prijenos podataka u te zemlje nije potrebno nikakvo posebno odobrenje ni sporazum.

Sigurnost podataka

ESET provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao odgovarajuću razinu sigurnosti za potencijalne opasnosti. Dajemo sve od sebe kako bismo osigurali trajnu povjerljivost, integritet, dostupnost i otpornost sustava za obradu i usluga. Međutim, u slučaju povrede osobnih podataka koja uzrokuje opasnosti za Vaša prava i slobode, spremni smo obavijestiti relevantno nadzorno tijelo, kao i pogođene krajnje korisnike čiji se podaci obrađuju.

Pravima ispitanika.

Prava svakog krajnjeg korisnika važna su i želimo vas obavijestiti da ESET jamči sljedeća prava svim krajnjim korisnicima (iz bilo koje zemlje EU-a ili izvan njega). Da biste ostvarili svoja prava kao ispitanik, možete nam se obratiti putem obrasca za podršku ili porukom e-pošte na dpo@eset.sk. U svrhu identifikacije molimo da navedete sljedeće informacije: Ime, adresa e-pošte i – ako su dostupni – licenčni ključ ili broj kupca i pripadnost tvrtki. Nemojte nam slati druge osobne podatke, primjerice datum rođenja. Želimo istaknuti da ćemo, da bismo mogli obraditi vaš zahtjev, kao i u svrhe identifikacije, obrađivati vaše osobne podatke.

Pravo na povlačenje privole. Pravo na povlačenje privole primjenjuje se samo u slučaju obrade na temelju privole. Ako obrađujemo vaše osobne podatke na temelju vaše privole, imate pravo povući privolu u bilo kojem trenutku bez navođenja razloga. Povlačenje vaše privole ima učinak samo u budućnosti i ne utječe na zakonitost podataka obrađenih prije povlačenja privole.

Pravo na prigovor. Pravo na prigovor na obradu primjenjivo je u slučaju obrade na temelju legitimnog interesa ESET-a ili treće strane. Ako obrađujemo vaše osobne podatke da bismo zaštitili legitiman interes, vi kao ispitanik u bilo kojem trenutku imate pravo prigovoriti na legitimni interes koji smo naveli i na obradu vaših osobnih podataka. Vaš prigovor ima učinak samo u budućnosti i ne utječe na zakonitost podataka obrađenih prije upućivanja prigovora. Ako vaše osobne podatke obrađujemo u svrhe izravnog marketinga, nije potrebno navesti razloge za prigovor. To vrijedi i za izradu profila ako je povezana s takvim izravnim marketingom. U svim ostalim slučajevima molimo vas da nas ukratko obavijestite o svojim prigovorima na legitimni interes ESET-a za obradu vaših osobnih podataka.

Imajte na umu da u nekim slučajevima, unatoč vašem povlačenju privole, imamo pravo dalje obrađivati vaše osobne podatke na temelju druge pravne osnove, na primjer za izvršenje ugovora.

Pravo na pristup. Kao ispitanik imate pravo u bilo kojem trenutku besplatno dobiti informacije o svojim podacima koje pohranjuje ESET.

Pravo na ispravak. Ako nenamjerno obrađujemo vaše netočne osobne podatke, imate ih pravo ispraviti.

Pravo na brisanje i pravo na ograničenje obrade. Kao ispitanik imate pravo zatražiti brisanje ili ograničenje obrade svojih osobnih podataka. Ako obrađujemo vaše osobne podatke, na primjer uz vašu privolu, koju povučete i ne postoji druga pravna osnova, na primjer ugovor, odmah brišemo vaše osobne podatke. Vaše osobne podatke također ćemo obrisati čim više ne budu potrebni u svrhe navedene za njih na kraju razdoblja u kojem ih zadržavamo.

Ako vaše osobne podatke koristimo isključivo u svrhu izravnog marketinga, a vi povučete svoju privolu ili uložite prigovor na temeljni legitimni interes ESET-a, ograničit ćemo obradu vaših osobnih podataka tako što ćemo vaše podatke za kontakt uvrstiti na internu crnu listu kako bismo izbjegli neželjeni kontakt. U suprotnom će vaši osobni podaci biti obrisani.

Imajte na umu da se od nas može tražiti da vaše podatke pohranjujemo do isteka obveza i razdoblja zadržavanja koje je odredio zakonodavac ili nadzorna tijela. Obveze i razdoblja zadržavanja također mogu proizaći iz slovačkog zakonodavstva. Nakon toga odgovarajući podaci bit će rutinski obrisani.

Pravo na prenosivost podataka. Rado ćemo vam, kao ispitaniku, pružiti osobne podatke koje ESET obrađuje u xls formatu.

Pravo na pritužbu. Kao ispitanik u bilo kojem trenutku imate pravo podnijeti pritužbu nadzornom tijelu. Tvrtka ESET podložna je zakonskim odredbama Slovačke Republike i obvezuje nas zakonodavstvo o zaštiti podataka kao dio Europske unije. Relevantno nadzorno tijelo za podatke je Ured za zaštitu osobnih podataka Slovačke Republike, koji se nalazi na adresi Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Obrada vaših osobnih podataka

Usluge koje pruža ESET implementirane u naš program pružaju se pod uvjetima 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 Licenčnom ugovoru za krajnjeg korisnika i dokumentaciji programa dokumentacija. Kako bi usluge funkcionirale, moramo prikupljati sljedeće podatke:

Podaci o licenciranju i naplati. ESET prikuplja i obrađuje ime, adresu e-pošte, licenčni ključ i (ako je primjenjivo) adresu, pripadnost tvrtki i podatke o plaćanju kako bi se olakšala aktivacija licence, isporuka licenčnog ključa, podsjetnici na istek, zahtjevi za podršku, provjera autentičnosti licence, pružanje naših usluga i drugih obavijesti, uključujući marketinške poruke, u skladu s primjenjivim zakonodavstvom ili vašom privolom. ESET je zakonski obvezan čuvati podatke o naplati u razdoblju od 10 godina, no podaci o licenciranju bit će anonimizirani najkasnije 12 mjeseci nakon isteka licence.

Statistika o nadogradnji i ostala statistika. Informacije koje se obrađuju obuhvaćaju informacije o procesu instalacije i vašem računalu, uključujući platformu na kojoj je instaliran naš program, a 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, postavke konfiguracije programa obrađuju se u svrhu pružanja usluga nadogradnje i u svrhu održavanja, sigurnosti i unaprjeđenja infrastrukture našeg pozadinskog servisa.

Te se informacije čuvaju odvojeno od identifikacijskih informacija potrebnih u svrhe licenciranja i naplate jer ne zahtijevaju identifikaciju krajnjeg korisnika. Razdoblje zadržavanja traje do 4 godine.

Sustav reputacije ESET LiveGrid®. Jednostrani hashevi povezani s infiltracijama obrađuju se u svrhu sustava reputacije ESET LiveGrid® koji poboljšava učinkovitost naših rješenja za zaštitu od zlonamjernih programa usporedbom skeniranih datoteka i baze podataka pouzdanih i nepoželjnih stavki u cloudu. Krajnji korisnik ne identificira se tijekom tog postupka.

Sustav za povratne informacije programa ESET LiveGrid®. 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

- Infiltracije 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;

- Informacije o upotrebi interneta kao što su IP adresa i geografske informacije, IP paketi, URL-ovi i ethernet okviri;

- Datoteke 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.

Sve informacije dobivene i obrađene putem sustava za povratne informacije programa ESET LiveGrid® namijenjene su upotrebi bez identifikacije krajnjeg korisnika.

Sigurnosna procjena uređaja povezanih na mrežu. Radi pružanja funkcije sigurnosne procjene obrađujemo naziv lokalne mreže i podatke o uređajima u vašoj lokalnoj mreži, kao što su prisutnost, vrsta, naziv, IP adresa i MAC adresa uređaja u vašoj lokalnoj mreži u vezi s podacima o licenci. Ovi podaci također uključuju vrstu zaštite bežične mreže i vrstu šifriranja bežične mreže za routere. Podaci o licenci kojima se identificira krajnji korisnik anonimizirat će se najkasnije 12 mjeseci nakon isteka licence.

Tehnička podrška. Informacije i podaci za kontakt i licenciranje sadržani u vašim zahtjevima za podršku mogu biti potrebni za pružanje usluge podrške. 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 zatražiti da nam pružite i druge podatke radi olakšavanja usluge podrške. Podaci koji se obrađuju za tehničku podršku pohranjuju se 4 godine.

Zaštita od zlouporabe podataka Ako se stvori ESET HOME račun na https://home.eset.com i krajnji korisnik aktivira funkciju u vezi s krađom računala, prikupljat će se i obrađivati sljedeći podaci: podaci o lokaciji, snimke zaslona, podaci o konfiguraciji računala i podaci snimljeni kamerom računala. Prikupljeni podaci pohranjuju se na našim serverima ili na serverima naših davatelja usluga uz razdoblje zadržavanja od 3 mjeseca.

Password Manager. Ako odlučite aktivirati funkciju Password Manager, podaci povezani s vašim podacima za prijavu pohranjuju se samo u šifriranom obliku na vašem računalu ili drugom određenom uređaju. Ako aktivirate uslugu sinkronizacije, šifrirani podaci pohranjuju se na našim serverima ili na serverima naših davatelja usluga kako bi se osigurala takva usluga. Ni ESET ni davatelj usluga nemaju pristup šifriranim podacima. Samo vi imate ključ za dešifriranje podataka. Podaci će biti uklonjeni nakon deaktivacije funkcije.

ESET LiveGuard. Ako odlučite aktivirati funkciju ESET LiveGuard, potrebno je slanje uzoraka kao što su datoteke koje je unaprijed definirao i odabrao krajnji korisnik. Uzorci koje odaberete za daljinsku analizu prenijet će se na ESET-ov servis, a rezultat analize bit će poslan na vaše računalo. Svi sumnjivi uzorci obrađuju se na isti način kao i informacije koje prikuplja sustav za povratne informacije ESET LiveGrid®.

Program za poboljšanje iskustva korisnika. Ako odlučite aktivirati Program za poboljšanje iskustva korisnika , anonimni podaci o telemetriji koji se odnose na upotrebu naših programa prikupljat će se i upotrebljavati na temelju vašeg pristanka.

Napominjemo da ako osoba koja koristi naše programe i usluge nije krajnji korisnik koji je kupio program ili uslugu i sklopio Licenčni ugovor za krajnjeg korisnika s nama (npr. zaposlenik krajnjeg korisnika, član obitelji ili osoba koju je krajnji korisnik na drugi način ovlastio za korištenje programa ili usluge u skladu s Licenčnim ugovorom za krajnjeg korisnika), obrada podataka provodi se u legitimnom interesu ESET-a u smislu članka 6. stavka 1. točke (f) OUZP-a kako bi se korisniku kojeg je ovlastio krajnji korisnik omogućilo korištenje programa i usluga koje pružamo u skladu s Licenčnim ugovorom za krajnjeg korisnika.

Kontaktni podaci

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