ESET Internet Security

Uporabniški priročnik

Če želite prikazati različico spletne pomoči tega dokumenta kliknite tukaj

Digital Security
Progress. Protected.

Izdelek ESET Internet Security je razvila družba ESET, spol. s r.o.

Za več informacij obiščite https://www.eset.com.

Tehnična podpora: https://support.eset.com

REV. 12.4.2024

1 ESET Internet Security 1
1.1 Novosti 2
1.2 Kateri izdelek imam? 2
1.3 Sistemske zahteve 3
1.3 Zastarela različica sistema Microsoft Windows 4
1.4 Preprečevanje 5
1.5 Strani pomoči 6
2 Namestitev 7
2.1 Namestitveni program Live 8
2.2 Namestitev brez povezave 9
2.2 Nadgradnja naročnine 11
2.2 Nadgradnja izdelka 12
2.2 Zamenjava naročnine s slabšo različico 12
2.2 Zamenjava izdelka s starejšo različico 13
2.3 Orodje za odpravljanje težav z namestitvijo 14
2.4 Prvi pregled po namestitvi 14
2.5 Nadgradnja na novejšo različico 15
2.5 Samodejna nadgradnja starejšega izdelka 16
2.5 Izdelek ESET Internet Security bo nameščen 16
2.5 Sprememba na drugo serijo izdelkov 16
2.5 Registracija 16
2.5 Potek aktiviranja 17
2.5 Aktiviranje je uspešno 17
3 Uvod 17
3.1 Ikona sistemske vrstice 17
3.2 Bližnjice na tipkovnici 18
3.3 Profili 18
3.4 Posodobitve 20
3.5 Konfiguriranje zaščite omrežja 21
3.6 Omogočite Zaščita pred krajo 22
3.7 Starševski nadzor 23
4 Aktiviranje izdelka 23
4.1 Vnos aktivacijske kode med aktiviranjem 24
4.2 Uporaba računa ESET HOME 24
4.3 Aktivacija brezplačne preizkusne licence 25
4.4 Brezplačna aktivacijska koda ESET 26
4.5 Aktiviranje ni uspelo – pogosti vzroki 26
4.6 Stanje naročnine 27
4.6 Aktiviranje ni uspelo zaradi prekomerne uporabe naročnine 28
5 Delo s programom ESET Internet Security 29
5.1 Pregled 30
5.2 Pregled računalnika 33
5.2 Zaganjalnik pregleda po meri 35
5.2 Napredovanje pregleda 37
5.2 Dnevnik pregleda računalnika 39
5.3 Posodabljanje 41
5.3 Pogovorno okno – zahtevan je vnovični zagon 43
5.3 Ustvarjanje opravil posodabljanja 43
5.4 Orodja 44
5.4 Dnevniške datoteke 45

5.4 Filtriranje dnevnika 48
5.4 Izvajajoči se procesi 49
5.4 Varnostno poročilo 51
5.4 Omrežne povezave 52
5.4 Dejavnost omrežja 54
5.4 ESET SysInspector 55
5.4 Razporejevalnik 56
5.4 Možnosti načrtovanega pregleda 58
5.4 Pregled razporejenih opravil 59
5.4 Podrobnosti opravila 59
5.4 Čas opravila 60
5.4 Čas opravila – enkrat 60
5.4 Čas opravila – dnevno 60
5.4 Čas opravila – tedensko 60
5.4 Čas opravila – ob dogodkih 60
5.4 Preskočeno opravilo 61
5.4 Podrobnosti opravila – posodobitev 61
5.4 Podrobnosti opravila – zagon programa 61
5.4 Sistemski čistilnik 62
5.4 Nadzornik omrežja 63
5.4 Omrežna naprava v nadzorniku omrežja 66
5.4 Obvestila | Nadzornik omrežja 67
5.4 Karantena 67
5.4 Izberi vzorec za analizo 70
5.4 Izberi vzorec za analizo – sumljiva datoteka 71
5.4 Izberi vzorec za analizo – sumljivo spletno mesto 71
5.4 Izberi vzorec za analizo – napačna pozitivna datoteka 72
5.4 Izberi vzorec za analizo – napačno pozitivno mesto 72
5.4 Izberi vzorec za analizo – drugo 72
5.5 Nastavitve 72
5.5 Zaščita računalnika 73
5.5 Zaznana je infiltracija 75
5.5 Zaščita na spletu 78
5.5 Preprečevanje lažnega predstavljanja 79
5.5 Starševski nadzor 81
5.5 Izjeme za spletno mesto 83
5.5 Kopiraj izjeme iz uporabnika 85
5.5 Kopiraj kategorije iz računa 85
5.5 Zaščita omrežja 85
5.5 Omrežne povezave 86
5.5 Podrobnosti omrežne povezave 87
5.5 Odpravljanje težav z dostopom do omrežja 88
5.5 Seznam začasno blokiranih naslovov IP 88
5.5 Dnevniki zaščite omrežja 89
5.5 Odpravljanje težav s požarnim zidom 90
5.5 Pisanje dnevnika in ustvarjanje pravil ali izjem iz dnevnika 90
5.5 Ustvarjanje pravila iz dnevnika 91
5.5 Ustvarjanje izjem iz obvestil osebnega požarnega zidu 91
5.5 Napredno beleženje zaščite omrežja 91
5.5 Odpravljanje težav s pregledovalnikom omrežnega prometa 92
5.5 Omrežna grožnja blokirana 93

5.5 Zaznano novo omrežje ... 93
5.5 Vzpostavljanje povezave – zaznavanje ... 94
5.5 Sprememba v programu ... 96
5.5 Dohodna zaupanja vredna komunikacija ... 96
5.5 Odhodna zaupanja vredna komunikacija ... 97
5.5 Dohodna komunikacija ... 99
5.5 Odhodna komunikacija ... 100
5.5 Nastavitve pogleda povezave ... 101
5.5 Varnostna orodja ... 101
5.5 Varno bančništvo in brskanje ... 102
5.5 Obvestilo v brskalniku ... 103
5.5 Zasebnost in varnost brskalnika ... 103
5.5 Zaščita pred krajo ... 105
5.5 Prijavite se v račun ESET HOME. ... 107
5.5 Nastavite ime naprave ... 108
5.5 Zaščita pred krajo omogočena/onemogočena ... 108
5.5 Dodajanje nove naprave ni uspelo ... 108
5.5 Uvoz in izvoz nastavitev ... 109
5.6 Pomoč in podpora ... 109
5.6 Vizitka izdelka ESET Internet Security ... 110
5.6 Novice družbe ESET ... 111
5.6 Pošlji podatke o konfiguraciji sistema ... 112
5.6 Tehnična podpora ... 112
5.7 ESET HOME račun ... 113
5.7 Povežite z računom ESET HOME ... 114
5.7 Prijava v račun ESET HOME ... 115
5.7 Prijava ni uspela – pogoste napake ... 116
5.7 Dodajanje naprave v račun ESET HOME ... 117
6 Napredne nastavitve ... 117
6.1 Pogon za zaznavo ... 118
6.1 Izključitve ... 119
6.1 Izključitve delovanja ... 119
6.1 Dodajanje ali urejanje izključitve delovanja ... 120
6.1 Oblika zapisa izključitve poti ... 122
6.1 Izključitve zaznav ... 122
6.1 Dodajanje ali urejanje izključitve zaznav ... 124
6.1 Čarovnik za ustvarjanje izključitev zaznav ... 125
6.1 Napredne možnosti pogona za zaznavo ... 126
6.1 Pregledovalnik omrežnega prometa ... 126
6.1 Zaščita v oblaku ... 126
6.1 Filter za izključevanje za zaščito v oblaku ... 129
6.1 Pregledi zlonamerne programske opreme ... 129
6.1 Profili pregleda ... 130
6.1 Cilji pregleda ... 130
6.1 Pregled v mirovanju ... 131
6.1 Zaznavanje stanja mirovanja ... 132
6.1 Zagonski pregled ... 132
6.1 Samodejni zagon pregledovanja datotek ... 132
6.1 Izmenljivi nosilci podatkov ... 133
6.1 Zaščita dokumentov ... 134
6.1 HIPS – Sistem za preprečevanje vdorov v gostitelja ... 134

6.1 Izključitve sistema HIPS ... 137
6.1 Napredne nastavitve HIPS ... 137
6.1 Gonilniki, ki se lahko vedno naložijo ... 137
6.1 Interaktivno okno HIPS ... 138
6.1 Način za učenje je končan ... 139
6.1 Zaznana morebitna programska oprema z zahtevo po odkupnini ... 139
6.1 Upravljanje pravil HIPS ... 140
6.1 Nastavitve pravil HIPS ... 141
6.1 Dodajanje poti do programa/registra za HIPS ... 144
6.2 Posodabljanje ... 144
6.2 Povrnitev prejšnjega stanja posodobitve ... 146
6.2 Časovni interval prejšnjega stanja posodobitve ... 148
6.2 Posodobitve izdelka ... 148
6.2 Možnosti povezave ... 148
6.3 Zaščite ... 149
6.3 Sprotna zaščita datotečnega sistema ... 153
6.3 Izključitve postopkov ... 155
6.3 Dodajanje ali urejanje izključitev procesov ... 156
6.3 Kdaj spremeniti konfiguracijo sprotne zaščite ... 156
6.3 Preverjanje sprotne zaščite ... 156
6.3 Kaj storiti, če sprotna zaščita ne deluje ... 156
6.3 Zaščita omrežnega dostopa ... 157
6.3 Profili omrežnih povezav ... 158
6.3 Dodajanje ali urejanje profilov omrežnih povezav ... 159
6.3 Aktivatorji ... 160
6.3 Nabori IP-jev ... 161
6.3 Urejanje naborov IP-jev ... 162
6.3 Nadzornik omrežja ... 162
6.3 Požarni zid ... 163
6.3 Nastavitve načina za učenje ... 165
6.3 Pravila za požarni zid ... 166
6.3 Dodajanje ali urejanje pravil za požarni zid ... 168
6.3 Zaznavanje sprememb v programih ... 170
6.3 Seznam programov, izključenih iz zaznavanja ... 170
6.3 Zaščita pred napadi iz omrežja (IDS) ... 171
6.3 Pravila IDS ... 171
6.3 Zaščita pred napadi z grobo silo ... 174
6.3 Pravila ... 175
6.3 Napredne možnosti ... 177
6.3 SSL/TLS ... 178
6.3 Pravila za pregled programov ... 180
6.3 Pravila za potrdila ... 181
6.3 Šifriran omrežni promet ... 182
6.3 Zaščita e-poštnega odjemalca ... 182
6.3 Zaščita prenosa e-pošte ... 182
6.3 Izključeni programi ... 184
6.3 Izključeni naslovi IP ... 185
6.3 Zaščita e-poštnega nabiralnika ... 186
6.3 Integracije ... 188
6.3 Orodna vrstica programa Microsoft Outlook ... 188
6.3 Pogovorno okno za potrditev ... 189

6.3 Vnovični pregled sporočil ... 189
6.3 Odziv ... 189
6.3 Upravljanje seznamov naslovov ... 190
6.3 Seznami naslovov ... 191
6.3 Dodaj/uredi naslov ... 192
6.3 Rezultat obdelave naslova ... 193
6.3 ThreatSense ... 193
6.3 Zaščita spletnega dostopa ... 196
6.3 Izključeni programi ... 198
6.3 Izključeni naslovi IP ... 199
6.3 Upravljanje seznama naslovov URL ... 200
6.3 Seznam naslovov ... 201
6.3 Ustvarjanje novega seznama naslovov ... 202
6.3 Kako dodati masko URL-ja ... 203
6.3 Pregledovanje prometa protokola HTTPS ... 204
6.3 ThreatSense ... 204
6.3 Starševski nadzor ... 207
6.3 Uporabniški računi ... 207
6.3 Nastavitve uporabniškega računa ... 208
6.3 Kategorije ... 210
6.3 Zaščita brskalnika ... 211
6.3 Varno bančništvo in brskanje ... 211
6.3 Nadzor naprave ... 212
6.3 Urejevalnik pravil za nadzor naprave ... 213
6.3 Zaznane naprave ... 214
6.3 Dodajanje pravil za nadzor naprav ... 214
6.3 Skupine naprav ... 217
6.3 Zaščita spletne kamere ... 218
6.3 Urejevalnik pravil zaščite spletne kamere ... 219
6.3 ThreatSense ... 219
6.3 Ravni čiščenja ... 222
6.3 Pripone datotek, izključenih iz pregledovanja ... 223
6.3 Dodatni parametri orodja ThreatSense ... 223
6.4 Orodja ... 224
6.4 Storitev Microsoft Windows® Update ... 224
6.4 Pogovorno okno – posodobitve sistema ... 225
6.4 Informacije o posodobitvi ... 225
6.4 ESET CMD ... 225
6.4 Dnevniške datoteke ... 227
6.4 Način za igranje ... 228
6.4 Diagnostika ... 228
6.4 Tehnična podpora ... 230
6.5 Povezljivost ... 230
6.6 Uporabniški vmesnik ... 231
6.6 Elementi uporabniškega vmesnika ... 232
6.6 Nastavitve dostopa ... 233
6.6 Geslo za napredne nastavitve ... 234
6.6 Podpora za bralnike zaslona ... 234
6.7 Obvestila ... 235
6.7 Pogovorno okno – stanja programa ... 236
6.7 Obvestila na namizju ... 236

6.7 Seznam obvestil na namizju 237
6.7 Interaktivna opozorila 239
6.7 Potrditvena sporočila 240
6.7 Posredovanje 242
6.8 Nastavitve zasebnosti 244
6.8 Povrnitev privzetih nastavitev 245
6.8 Povrnitev vseh nastavitev v trenutnem razdelku 245
6.8 Napaka pri shranjevanju konfiguracije 245
6.9 Pregledovalnik v ukazni vrstici 246
7 Pogosta vprašanja 248
7.1 Posodobitev izdelka ESET Internet Security 249
7.2 Odstranjevanje virusa iz računalnika 249
7.3 Kako dovoliti komunikacijo določenemu programu 250
7.4 Kako omogočiti starševski nadzor računa 250
7.5 Kako ustvariti novo opravilo v razporejevalniku 251
7.6 Kako razporediti tedensko pregledovanje računalnika 252
7.7 Odklepanje naprednih nastavitev 253
7.8 Kako razrešiti deaktivacijo izdelka s portala ESET HOME 253
7.8 Izdelek je deaktiviran, povezava z napravo je prekinjena 254
7.8 Izdelek ni aktiviran 254
8.1 Program za izboljšanje izkušenj strank 254
8.2 Licenčna pogodba za končnega uporabnika 255
8.3 Pravilnik o zasebnosti 266

ESET Internet Security

ESET Internet Security predstavlja nov pristop k resnično integrirani računalniški varnosti. Najnovejša različica orodja za pregledovanje ESET LiveGrid®, združena s prilagojenim požarnim zidom in moduli za preprečevanje neželene pošte, hitro in natančno varuje vaš računalnik. Rezultat je inteligenten sistem, ki omogoča nenehen pregled nad napadi in zlonamerno programsko opremo, ki lahko škodi vašemu računalniku.

ESET Internet Security je celovita varnostna rešitev, ki zagotavlja najvišjo raven zaščite pri najmanjšem odtisu v sistemu. Napredne tehnologije temeljijo na umetni inteligenci in preprečijo dostop virusom, vohunski programski opremi, trojanskim konjem, črvom, oglaševalnim programom, korenskim kompletom in drugim grožnjam, ne da bi omejevale učinkovitost delovanja sistema ali prekinile delovanje računalnika.

Funkcije in prednosti

Preoblikovan uporabniški vmesnik	Uporabniški vmesnik v tej različici smo korenito preoblikovali in poenostavili na podlagi rezultatov preskusov uporabnosti. Natančno smo pregledali besedilo in obvestila v grafičnem uporabniškem vmesniku, ki zdaj podpira tudi jezike, ki se pišejo od desne proti levi, kot sta hebrejščina in arabščina. Spletna pomoč je zdaj del izdelka ESET Internet Security in zagotavlja vsebine za podporo, ki se posodabljajo dinamično.
Temni način	Razširitev, s katero lahko hitro preklopite zaslon na temno temo. Želeno barvno shemo lahko izberete v razdelku Elementi uporabniškega vmesnika.
Zaščita pred virusi in vohunsko programsko opremo	Proaktivno zazna in izbriše več znanih in neznanih virusov, črvov, trojanskih konjev in korenskih kompletov. Napredna hevristika označi celo neznano zlonamerno programsko opremo, tako da vas zaščiti pred neznanimi grožnjami in jih odpravi, preden vam lahko škodijo. Zaščita spletnega dostopa in Preprečevanje lažnega predstavljanja delujeta na podlagi spremljanja komunikacije med spletnimi brskalniki in oddaljenimi strežniki (tudi SSL). Zaščita e-poštnega odjemalca omogoča nadzor e-poštne komunikacije, prejete prek protokolov POP3(S) in IMAP(S).
Redne posodobitve	Redno posodabljanje orodja za zaznavanje (prej zbirka virusnih definicij) in modulov programa je najboljši način zagotavljanja največje ravni varnosti v računalniku.
ESET LiveGrid® (Ugled v oblaku)	Ugled izvajajočih se procesov in datotek lahko preverite neposredno v programu ESET Internet Security.
Nadzor naprave	Samodejno pregleda vse pogone USB, pomnilniške kartice in CD-je/DVD-je. Blokira izmenljive nosilce podatkov glede na vrsto nosilca podatkov, izdelovalca, velikost in druge oznake.
Funkcije HIPS	Podrobneje lahko prilagodite delovanje sistema; določite pravila v sistemskem registru, aktivnih procesih in programih ter natančno nastavite varnostne nastavitve.
Način za igranje	Odloži vsa pojavna okna, posodobitve ali druge dejavnosti, ki bremenijo delovanje sistema, zaradi varčevanja sistemskih sredstev za igranje iger in drugih celozaslonskih dejavnosti.

Funkcije programa ESET Internet Security

Varno bančništvo in brskanje	Varno bančništvo in brskanje omogoča uporabo zaščitenega brskalnika pri dostopanju do prehodov storitev spletnega bančništva ali spletnega plačevanja ter tako zagotavlja, da vse spletne transakcije potekajo v zaupanja vrednem in varnem okolju.

Podpora za podpise omrežja	Podpisi omrežja omogočajo hitro prepoznavanje ter blokirajo zlonameren promet v uporabniške naprave in iz njih, kot so robotski računalniki in izkoriščevalska programska oprema. Ta funkcija je pravzaprav izboljšava zaščite pred omrežjem okuženih računalnikov.
Pametni požarni zid	Preprečuje dostop nepooblaščenim uporabnikom do vašega računalnika in zlorabo osebnih podatkov.
Zaščita pred neželeno pošto v e-poštnem odjemalcu	Predstavlja kar 50 odstotkov vse e-poštne komunikacije. Zaščita pred neželeno pošto v e-poštnem odjemalcu ščiti pred to težavo.
Zaščita pred krajo	Zaščita pred krajo zagotavlja razširjeno varnost za uporabnika v primeru izgube ali tatvine računalnika. Ko namestite ESET Internet Security in Zaščita pred krajo, bo vaša naprava navedena v spletnem vmesniku. V spletnem vmesniku lahko upravljate konfiguracijo izdelka Zaščita pred krajo in določate funkcije izdelka Zaščita pred krajo v napravi.
Starševski nadzor	Zaščiti družino pred morebitno žaljivo spletno vsebino, tako da blokira različne kategorije spletnih mest.

Naročnina mora biti aktivna za delovanje funkcij ESET Internet Security. Priporočamo, da naročnino podaljšate nekaj tednov pred potekom naročnine za izdelek ESET Internet Security.

Novosti

Novosti v različici ESET Internet Security 17.1

- Majhne izboljšave Nadzornika omrežja
- Majhne izboljšave Varnega bančništva in brskanja
- Drugi manjši popravki napak in izboljšave

Če želite onemogočiti **obvestila o novostih:**
1. Odprite Napredne nastavitve > **Obvestila** > **Obvestila na namizju**.
2. Kliknite **Uredi** poleg možnosti **Obvestila na namizju**.
3. Prekličite izbor možnosti **Prikaz obvestil o novostih** ter kliknite **V redu**.

Za več informacij o obvestilih si oglejte razdelek Obvestila.

Za podroben seznam sprememb v ESET Internet Security glejte Dnevniki sprememb ESET Internet Security.

Kateri izdelek imam?

ESET pri novih izdelkih zagotavlja več ravni varnosti od zmogljivih in hitrih protivirusnih rešitev do celovite varnostne rešitve z najmanjšim odtisom v sistemu:

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

Če želite ugotoviti, kateri izdelek imate nameščen, odprite glavno okno programa in na vrhu okna bo prikazano ime izdelka (glejte članek v zbirki znanja).

V spodnji tabeli so navedene funkcije, ki so na voljo v posameznem izdelku.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Pogon za zaznavo	✔	✔	✔	✔
Napredno strojno učenje	✔	✔	✔	✔
Ščit pred exploit programsko kodo	✔	✔	✔	✔
Zaščita pred napadi na podlagi skriptov	✔	✔	✔	✔
Preprečevanje lažnega predstavljanja	✔	✔	✔	✔
Zaščita spletnega dostopa	✔	✔	✔	✔
HIPS (vključno z Zaščito pred izsiljevalsko programsko opremo)	✔	✔	✔	✔
Preprečevanje neželene pošte		✔	✔	✔
Požarni zid		✔	✔	✔
Nadzornik omrežja		✔	✔	✔
Zaščita spletne kamere		✔	✔	✔
Zaščita pred napadi iz omrežja		✔	✔	✔
Zaščita pred omrežjem okuženih računalnikov		✔	✔	✔
Varno bančništvo in brskanje		✔	✔	✔
Zasebnost in varnost brskalnika		✔	✔	✔
Starševski nadzor		✔	✔	✔
Zaščita pred krajo		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Nekateri zgoraj navedeni izdelki morda niso na voljo za vaš jezik ali regijo.

Sistemske zahteve

Za optimalno delovanje programa ESET Internet Security, mora sistem izpolnjevati naslednje zahteve za strojno in programsko opremo:

Podprti procesorji

32-bitni (x86) ali 64-bitni (x64) procesor Intel oziroma AMD z naborom navodil SSE2 z, frekvenca 1 GHz ali višja procesor ARM64, 1 GHz ali višja

Podprti operacijski sistemi

Microsoft® Windows® 11

Microsoft® Windows® 10

Za namestitev ali nadgradnjo izdelkov ESET, izdanih po juliju 2023, mora biti v vseh operacijskih sistemih Windows nameščena podpora za Azure Code Signing. Več informacij.

Poskrbite, da je operacijski sistem vedno posodobljen.

Zahteve funkcij za ESET Internet Security

V spodnji tabeli so navedene sistemske zahteve za določene funkcije za ESET Internet Security:

Funkcija	Zahteve
Intel® Threat Detection Technology	Oglejte si podprte procesorje.
Varno bančništvo in brskanje	Oglejte si podprte spletne brskalnike.
Transparentno ozadje	Različica Windows 10 RS4 ali novejša.
Poseben program za odstranjevanje	Procesor, ki ne temelji na ARM64.
Sistemski čistilnik	Procesor, ki ne temelji na ARM64.
Ščit pred exploit programsko kodo	Procesor, ki ne temelji na ARM64.
Globoko preverjanje delovanja	Procesor, ki ne temelji na ARM64.

Ostalo

Za aktivacijo izdelka ESET Internet Security in ustrezno delovanje posodobitev potrebujete internetno povezavo.

Dva protivirusna programa, ki se hkrati izvajata v eni napravi, povzročata neizogibne spore v sistemskih virih, kot je upočasnitev sistema in nezmožnost operiranja.

Zastarela različica sistema Microsoft Windows

Težava

- Najnovejšo različico programa ESET Internet Security želite namestiti v računalnik s sistemom Windows 7, Windows 8 (8.1) ali Windows Home Server 2011
- ESET Internet Security med namestitvijo prikaže obvestilo o napaki **Zastarel operacijski sistem**

Podrobnosti

Za najnovejšo različico programa ESET Internet Security potrebujete operacijski sistem Windows 10 ali Windows 11.

Rešitev

Na voljo so naslednje rešitve:

Nadgradnja na Windows 10 ali Windows 11

Postopek nadgradnje je razmeroma enostaven in v mnogih primerih pri tem ne boste izgubili svojih datotek. Pred nadgradnjo na Windows 10:

1. Varnostno kopiranje pomembnih podatkov.

2. Preberite pogosta vprašanja o nadgradnji na Windows 10 ali pogosta vprašanja o nadgradnji na Windows 11 družbe Microsoft in posodobite operacijski sistem Windows.

Namestitev programa ESET Internet Security različice 16.0

Če ne morete nadgraditi sistema Windows, namestite različico 16.0 programa ESET Internet Security. Za več informacij glejte spletno pomoč za ESET Internet Security različice 16.0.

Preprečevanje

Pri delu z računalnikom in še posebej kadar brskate po spletu, ne pozabite, da noben protivirusni program ne more povsem preprečiti tveganja, povezanega z zaznavami in oddaljenimi napadi. Za zagotavljanje najvišje ravni zaščite in ustreznosti je zelo pomembno, da protivirusno rešitev uporabljate pravilno in da se držite nekaterih koristnih pravil:

Redno posodabljanje

Po statističnih podatkih, ki jih navaja ESET LiveGrid®, se vsak dan ustvari na tisoče novih in edinstvenih infiltracij z namenom, da bi zaobšle obstoječe varnostne ukrepe in avtorjem omogočile lahek zaslužek – na račun drugih uporabnikov. Strokovnjaki v raziskovalnem laboratoriju družbe ESET vsakodnevno analizirajo grožnje in pripravljajo ter izdajajo posodobitve, s katerimi želijo povišati raven zaščite za naše uporabnike. Za zagotavljanje največje učinkovitosti teh posodobitev, je pomembno, da so posodobitve ustrezno konfigurirane v vašem sistemu. Če želite več informacij o konfiguraciji posodobitev, si oglejte poglavje Nastavitve posodobitve.

Prenos varnostnih popravkov

Avtorji zlonamerne programske opreme običajno izrabljajo razne ranljivosti sistemov, da bi tako povečali učinkovitost širitve zlonamerne kode. Zato izdelovalci programske opreme pazljivo obravnavajo vse ranljivosti svojih programov, da bi objavili in izdali varnostne posodobitve ter tako redno preprečevali mogoče grožnje. Pomembno je, da varnostne posodobitve prenesete, takoj ko so izdane. Microsoft Windows in spletni brskalniki, kot je Internet Explorer, sta dva primera programov, za katera se redno izdajajo varnostne posodobitve.

Varnostno kopiranje pomembnih podatkov

Pisci zlonamerne programske opreme se po navadi ne zmenijo za potrebe uporabnikov, zato zlonamerni programi pogosto povzročijo popolno okvaro operacijskega sistema in izgubo pomembnih podatkov. Pomembno je redno varnostno kopirati pomembne in občutljive podatke na zunanji vir, kot je na primer DVD ali zunanji disk. Takšni ukrepi močno olajšajo in pospešijo obnovo podatkov, če pride do okvare sistema.

Redno pregledujte računalnik in preverite, ali so v njem virusi

Zaznavanje več znanih in neznanih virusov, črvov, trojanskih konjev in korenskih kompletov obravnava modul sprotne zaščite datotečnega sistema. To pomeni, da je datoteka ob vsakem dostopu ali odpiranju pregledana, ali se v njej nahaja zlonamerna programska oprema. Priporočamo, da pregled celotnega računalnika zaženete vsaj enkrat na mesec, saj so definicije zlonamerne programske opreme lahko različne in orodje za zaznavanje se vsak dan posodablja.

Sledite osnovnim varnostnim pravilom

Najbolj uporabno in učinkovito pravilo pa je – bodite vedno previdni. Danes številne infiltracije zahtevajo posredovanje uporabnika, da bi se izvedle in razposlale. Če ste pri odpiranju novih datotek previdni, boste prihranili precej časa in napora, ki bi ju sicer porabili za čiščenje infiltracij. Tukaj je nekaj koristnih priporočil:

- ne obiskujte sumljivih spletnih mest, kjer je več pojavnih in utripajočih oglasov;
- bodite previdni, kadar nameščate brezplačne programe, pakete kodekov itn. Uporabljajte le varne programe in obiskujte le varna spletna mesta v internetu.
- bodite previdni, kadar odpirate priloge e-poštnih sporočil, še posebej tistih, pripetih sporočilom, poslanim na več naslovov in sporočilom neznanih pošiljateljev;
- Ne uporabljajte računa skrbnika za vsakodnevno delo v računalniku.

Strani pomoči

Dobrodošli v uporabniškem priročniku izdelka ESET Internet Security. Z informacijami, ki so na voljo tukaj, boste bolje spoznali izdelek, hkrati pa bo delo z računalnikom varnejše.

Uvod

Preden začnete uporabljati izdelek ESET Internet Security, priporočamo, da se seznanite z različnimi vrstami zaznanih elementov in napadov na daljavo, na katere boste morda naleteli pri delu z računalnikom. Prav tako smo pripravili seznam novih funkcij, uvedenih v izdelku ESET Internet Security.

Najprej namestite ESET Internet Security. Če ste že namestili ESET Internet Security, glejte Delo s programom ESET Internet Security.

Uporaba strani s pomočjo za ESET Internet Security

Spletna pomoč je razdeljena na več poglavij in podpoglavij. Za informacije o trenutno odprtem oknu v programu ESET Internet Security pritisnite **F1**.

Program omogoča, da poiščete temo za pomoč po ključnih besedah ali iščete po vsebini tako, da vnašate besede ali besedne zveze. Ta načina iskanja se med seboj razlikujeta v tem, da je ključna beseda lahko logično povezana s stranmi pomoči, ki pa v svojih besedilih nimajo prav te ključne besede. Iskanje z besedami ali besednimi zvezami pa pomeni, da bo program preiskal vsebino vseh strani in prikazal le tiste, ki v dejanskih besedilih te besede ali besedne zveze vsebujejo.

Zaradi doslednosti in jasnosti je v tem vodniku uporabljena terminologija, ki se uporablja v uporabniškem vmesniku programa ESET Internet Security. Prav tako je uporabljen nabor simbolov za poudarjanje pomembnih tem ali tem, ki vas lahko zanimajo.

Opomba je le kratko opažanje. Opombe lahko izpustite, vendar vsebujejo dragocene informacije, kot so posebne funkcije ali povezave do povezanih tem.

To opozorilo zahteva vašo pozornost in priporočamo, da ga ne preskočite. Običajno zagotavlja nekritične, toda pomembne informacije.

Ta informacija zahteva posebno pozornost in previdnost. Opozorila so prikazana zato, da vas odvrnejo od napak, ki jih lahko storite in so lahko škodljive. Preberite in upoštevajte besedilo, saj se nanaša na izjemno občutljive sistemske nastavitve ali druga tveganja.

To je primer uporabe ali praktični primer, katerega namen je zagotavljanje pomoči pri razumevanju, kako lahko uporabite določeno funkcijo.

Dogovor	Pomen
Krepko	Imena elementov vmesnika, kot so polja in gumbi možnosti.
Ležeče	Označbe mesta za podatke, ki jih navedete. Tako na primer ime datoteke ali pot pomeni, da vnesete dejansko ime datoteke ali pot.
`Courier New`	Vzorci kode ali ukazi.
Hiperpovezava	Zagotavlja hiter in enostaven dostop do navzkrižno sklicevanih tem ali zunanjih spletnih mest. Hiperpovezave so označene z modro in so lahko podčrtane.
%ProgramFiles%	Sistemski imenik Windows, v katerem so shranjeni programi, nameščeni v sistemu Windows.

Spletna pomoč je glavni vir vsebine pomoči. Najnovejša različice spletne pomoči se pri vzpostavljeni internetni povezavi samodejno prikaže.

Namestitev

ESET Internet Security lahko v svoj računalnik namestite na več načinov. Načini namestitve se lahko razlikujejo glede na državo in način distribucije:

- Live Installer – prenesen s spletnega mesta ESET ali CD-ja/DVD-ja. Namestitveni paket je enoten za vse jezike (izberite ustrezni jezik). Live Installer je majhna datoteka, dodatne datoteke, ki jih potrebujete za namestitev programa ESET Internet Security, pa se prenesejo samodejno.

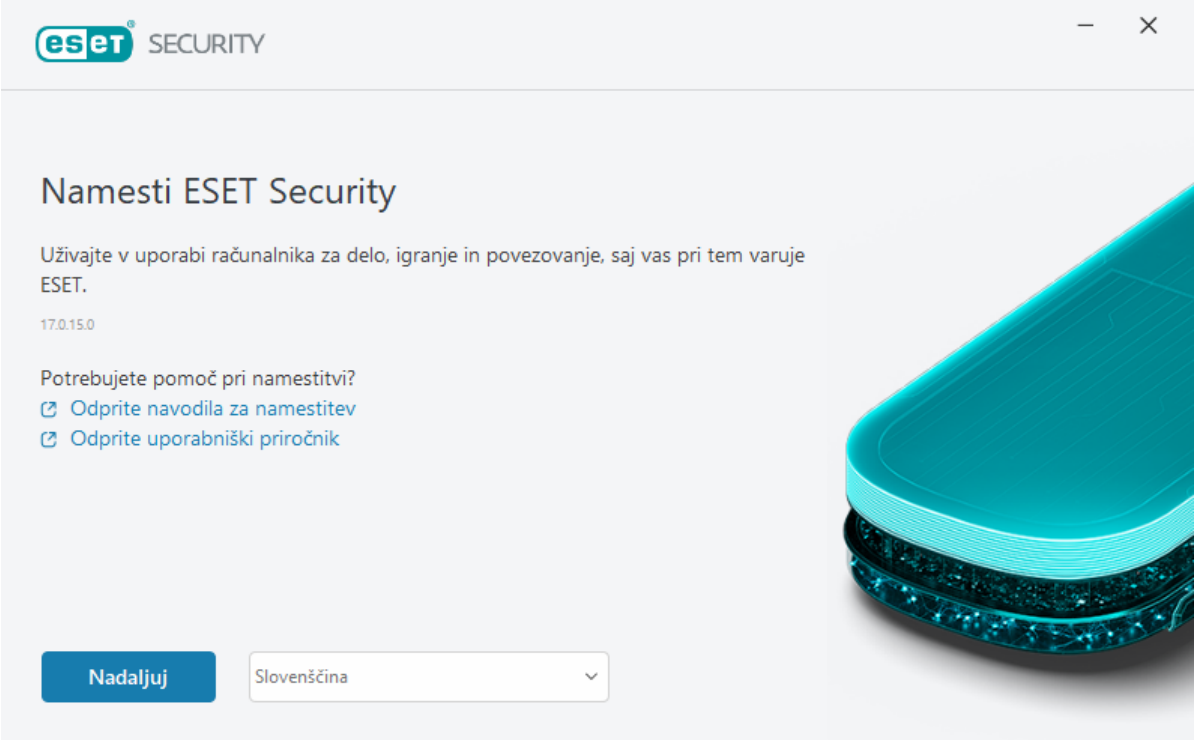
- Namestitev brez povezave – pri tej namestitvi je uporabljena datoteka .exe, ki je večja od datoteke Live Installer, in ne zahteva internetne povezave ali dodatnih datotek za dokončanje namestitve.

Pred namestitvijo programa ESET Internet Security se prepričajte, da v računalniku ni nameščen noben drug protivirusni program. Če sta v računalniku nameščeni dve protivirusni rešitvi ali več, bo med njima morda prihajalo do sporov. Priporočamo, da iz sistema odstranite vse druge protivirusne programe. Oglejte si naš članek v zbirki znanja ESET, kjer je prikazan seznam orodij za odstranjevanje pogoste protivirusne programske opreme (na voljo v angleščini in nekaterih drugih jezikih).

Namestitveni program Live

Ko prenesete namestitveni paket Live Installer, dvakrat kliknite namestitveno datoteko in upoštevajte navodila po korakih v čarovniku za namestitev.

Pri tej vrsti namestitve morate imeti vzpostavljeno povezavo z internetom.



1. S spustnega menija izberite primerni jezik in kliknite možnost **Nadaljuj**.

Če prek prejšnje različice nameščate novejšo različico z nastavitvami, zaščitenimi z geslom, vnesite svoje geslo. Nastavitve gesla lahko konfigurirate v nastavitvah dostopa.

2. Izberite nastavitve za te funkcije, preberite licenčno pogodbo za končnega uporabnika in pravilnik o zasebnosti ter kliknite možnost **Nadaljuj** ali pa možnost **Dovoli vse in nadaljuj**, da omogočite vse funkcije:

- sistem za povratne informacije ESET LiveGrid®
- Morebitno neželeni programi
- Program za izboljšanje izkušenj strank

Če kliknete možnost **Nadaljuj** ali **Dovoli vse in nadaljuj**, sprejemate licenčno pogodbo za končnega uporabnika in potrjujete pravilnik o zasebnosti.

3. Za aktivacijo, upravljanje in ogled varnosti naprave prek ESET HOME, povežite napravo z računom ESET HOME. Kliknite možnost **Preskoči prijavo** za nadaljevanje, ne da bi se povezali z računom ESET HOME. Napravo lahko povežete z računom ESET HOME pozneje.

4. Če nadaljujete brez povezave z računom ESET HOME, izberite možnost aktiviranja. Če nameščate novejšo različico namesto starejše, se vaša **aktivacijska koda** vnese samodejno.

5. Čarovnik za namestitev na podlagi vaše naročnine določi, kateri izdelek ESET se namesti. Vedno je vnaprej izbrana različica z največ varnostnimi funkcijami. Kliknite možnost **Spremeni izdelek**, če želite namestiti drugo različico izdelka ESET. Kliknite možnost **Nadaljuj**, da začnete postopek namestitve. To lahko traja nekaj trenutnkov.

Če obstajajo ostanki (datoteke ali mape) izdelkov ESET, odstranjenih v preteklosti, boste pozvani, da dovolite njihovo odstranitev. Za nadaljevanje kliknite možnost **Namesti**.

6. Za izhod iz čarovnika za namestitev kliknite **Dokončano**.

Orodje za odpravljanje težav z namestitvijo.

Po namestitvi in aktivaciji izdelka se začne prenos modulov. Zaščita se namešča in nekatere funkcije morda ne bodo v celoti delovale, dokler se prenos ne zaključi.

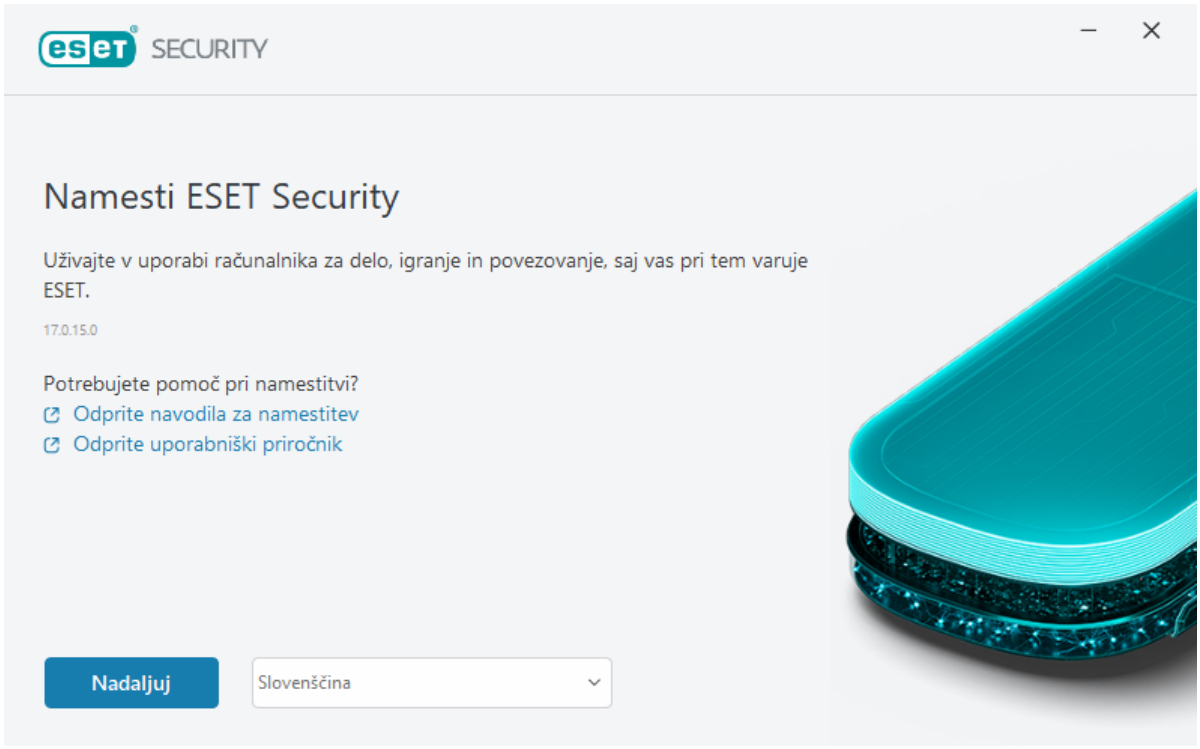
Namestitev brez povezave

Spodaj prenesite izdelek ESET za domačo uporabo za sistem Windows in ga namestite prek programa za namestitev (.exe) brez povezave. Izberite, katero različico izdelka ESET za domačo uporabo želite prenesti (32-bitno, 64-bitno ali ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Prenos 64-bitne različice Prenos 32-bitne različice Prenos različice ARM	Prenos 64-bitne različice Prenos 32-bitne različice Prenos različice ARM	Prenos 64-bitne različice Prenos 32-bitne različice Prenos različice ARM	Prenos 64-bitne različice Prenos 32-bitne različice Prenos različice ARM

Če imate vzpostavljeno aktivno internetno povezavo, namestite izdelek ESET prek programa Live Installer.

Ko zaženete program za namestitev brez povezave (.exe), med postopkom nastavitve upoštevajte navodila čarovnika za namestitev.



1. S spustnega menija izberite primerni jezik in kliknite možnost **Nadaljuj**.

Če prek prejšnje različice nameščate novejšo različico z nastavitvami, zaščitenimi z geslom, vnesite svoje geslo. Nastavitve gesla lahko konfigurirate v nastavitvah dostopa.

2. Izberite nastavitve za te funkcije, preberite licenčno pogodbo za končnega uporabnika in pravilnik o zasebnosti ter kliknite možnost **Nadaljuj** ali pa možnost **Dovoli vse in nadaljuj**, da omogočite vse funkcije:

- sistem za povratne informacije ESET LiveGrid®
- Morebitno neželeni programi
- Program za izboljšanje izkušenj strank

Če kliknete možnost **Nadaljuj** ali **Dovoli vse in nadaljuj**, sprejemate licenčno pogodbo za končnega uporabnika in potrjujete pravilnik o zasebnosti.

3. Kliknite možnost **Preskoči prijavo**. Ko vzpostavite povezavo z internetom, lahko svojo napravo povežete z računom ESET HOME .

4. Kliknite možnost **Preskoči aktivacijo**. Izdelek ESET Internet Security mora biti po namestitvi aktiviran, da lahko deluje v celoti. Za aktivacija izdelka je potrebna aktivna internetna povezava.

5. Čarovnik za namestitev na podlagi prenesenega programa za namestitev brez povezave prikaže, kateri izdelek ESET bo nameščen. Kliknite možnost **Nadaljuj**, da začnete postopek namestitve. To lahko traja nekaj trenutnkov.

Če obstajajo ostanki (datoteke ali mape) izdelkov ESET, odstranjenih v preteklosti, boste pozvani, da dovolite njihovo odstranitev. Za nadaljevanje kliknite možnost **Namesti**.

6. Za izhod iz čarovnika za namestitev kliknite **Dokončano**.

Orodje za odpravljanje težav z namestitvijo.

Nadgradnja naročnine

To okno z obvestilom se pokaže, ko se je naročnina, s katero ste aktivirali izdelek ESET, spremenila. S spremenjeno naročnino lahko aktivirate izdelek, ki ima več funkcij zaščite. Če ne izvedete nobene spremembe, bo program ESET Internet Security enkrat prikazal opozorilo z nazivom **Sprememba na izdelek z več funkcijami**.

Da (priporočeno) – samodejna namestitev izdelka z več funkcijami zaščite.

Ne, hvala – brez sprememb, obvestilo pa trajno izgine.

Za naknadno spremembo izdelka glejte zbirko znanja družbe ESET. Če želite več informacij o naročnini ESET, glejte Pogosta vprašanja o naročnini.

V spodnji tabeli so navedene funkcije, ki so na voljo v posameznem izdelku.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Pogon za zaznavo	✔	✔	✔	✔
Napredno strojno učenje	✔	✔	✔	✔
Ščit pred exploit programsko kodo	✔	✔	✔	✔
Zaščita pred napadi na podlagi skriptov	✔	✔	✔	✔
Preprečevanje lažnega predstavljanja	✔	✔	✔	✔
Zaščita spletnega dostopa	✔	✔	✔	✔
HIPS (vključno z Zaščito pred izsiljevalsko programsko opremo)	✔	✔	✔	✔
Preprečevanje neželene pošte		✔	✔	✔
Požarni zid		✔	✔	✔
Nadzornik omrežja		✔	✔	✔
Zaščita spletne kamere		✔	✔	✔
Zaščita pred napadi iz omrežja		✔	✔	✔
Zaščita pred omrežjem okuženih računalnikov		✔	✔	✔
Varno bančništvo in brskanje		✔	✔	✔
Zasebnost in varnost brskalnika		✔	✔	✔
Starševski nadzor		✔	✔	✔
Zaščita pred krajo		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Nadgradnja izdelka

Prenesli ste privzeti namestitveni program, ker želite spremeniti izdelek za aktivacijo ali zamenjati že nameščeni program s takim, ki ima več funkcij zaščite.

Spremenite izdelek med namestitvijo.

V spodnji tabeli so navedene funkcije, ki so na voljo v posameznem izdelku.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Pogon za zaznavo	✔	✔	✔	✔
Napredno strojno učenje	✔	✔	✔	✔
Ščit pred exploit programsko kodo	✔	✔	✔	✔
Zaščita pred napadi na podlagi skriptov	✔	✔	✔	✔
Preprečevanje lažnega predstavljanja	✔	✔	✔	✔
Zaščita spletnega dostopa	✔	✔	✔	✔
HIPS (vključno z Zaščito pred izsiljevalsko programsko opremo)	✔	✔	✔	✔
Preprečevanje neželene pošte		✔	✔	✔
Požarni zid		✔	✔	✔
Nadzornik omrežja		✔	✔	✔
Zaščita spletne kamere		✔	✔	✔
Zaščita pred napadi iz omrežja		✔	✔	✔
Zaščita pred omrežjem okuženih računalnikov		✔	✔	✔
Varno bančništvo in brskanje		✔	✔	✔
Zasebnost in varnost brskalnika		✔	✔	✔
Starševski nadzor		✔	✔	✔
Zaščita pred krajo		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Zamenjava naročnine s slabšo različico

To pogovorno okno se odpre, ko se je naročnina, s katero ste aktivirali izdelek ESET, spremenila. Spremenjeno naročnino lahko uporabljate samo z drugim izdelkom ESET, ki ima manj funkcij zaščite. Izdelek je bil samodejno zamenjan, da ne bi izgubili zaščite.

Če želite več informacij o naročnini ESET, glejte Pogosta vprašanja o naročnini.

V spodnji tabeli so navedene funkcije, ki so na voljo v posameznem izdelku.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Pogon za zaznavo	✔	✔	✔	✔
Napredno strojno učenje	✔	✔	✔	✔
Ščit pred exploit programsko kodo	✔	✔	✔	✔
Zaščita pred napadi na podlagi skriptov	✔	✔	✔	✔
Preprečevanje lažnega predstavljanja	✔	✔	✔	✔
Zaščita spletnega dostopa	✔	✔	✔	✔
HIPS (vključno z Zaščito pred izsiljevalsko programsko opremo)	✔	✔	✔	✔
Preprečevanje neželene pošte		✔	✔	✔
Požarni zid		✔	✔	✔
Nadzornik omrežja		✔	✔	✔
Zaščita spletne kamere		✔	✔	✔
Zaščita pred napadi iz omrežja		✔	✔	✔
Zaščita pred omrežjem okuženih računalnikov		✔	✔	✔
Varno bančništvo in brskanje		✔	✔	✔
Zasebnost in varnost brskalnika		✔	✔	✔
Starševski nadzor		✔	✔	✔
Zaščita pred krajo		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Zamenjava izdelka s starejšo različico

Trenutno nameščeni izdelek ima več funkcij zaščite kot tisti, ki ga nameravate aktivirati.Izgubili boste zaščito pred krajami in dostop do povezanih podatkov, shranjenih na ESET HOME.

V spodnji tabeli so navedene funkcije, ki so na voljo v posameznem izdelku.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Pogon za zaznavo	✔	✔	✔	✔
Napredno strojno učenje	✔	✔	✔	✔
Ščit pred exploit programsko kodo	✔	✔	✔	✔
Zaščita pred napadi na podlagi skriptov	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Preprečevanje lažnega predstavljanja	✔	✔	✔	✔
Zaščita spletnega dostopa	✔	✔	✔	✔
HIPS (vključno z Zaščito pred izsiljevalsko programsko opremo)	✔	✔	✔	✔
Preprečevanje neželene pošte		✔	✔	✔
Požarni zid		✔	✔	✔
Nadzornik omrežja		✔	✔	✔
Zaščita spletne kamere		✔	✔	✔
Zaščita pred napadi iz omrežja		✔	✔	✔
Zaščita pred omrežjem okuženih računalnikov		✔	✔	✔
Varno bančništvo in brskanje		✔	✔	✔
Zasebnost in varnost brskalnika		✔	✔	✔
Starševski nadzor		✔	✔	✔
Zaščita pred krajo		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Orodje za odpravljanje težav z namestitvijo

Če med namestitvijo pride do težav, čarovnik za namestitev zažene orodje za odpravljanje težav, ki odpravi težavo, če je to mogoče.

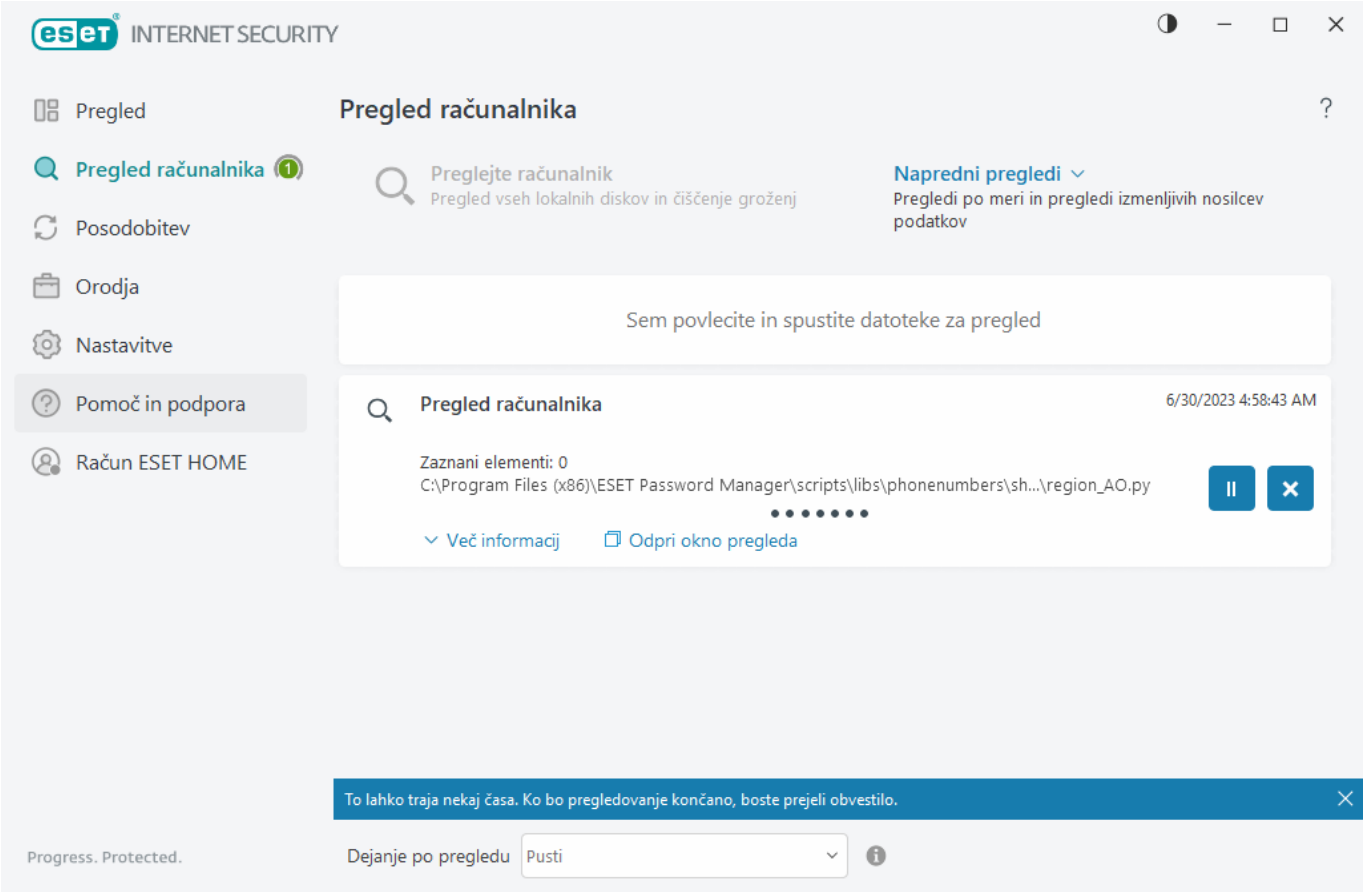
Če želite zagnati orodje za odpravljanje težav, kliknite možnost **Zaženi odpravljanje težav**. Ko se odpravljanje težav konča, ravnajte v skladu s predlagano rešitvijo.

Če se težava ne odpravi, si oglejte seznam, na katerem so pogoste napake pri namestitvi in rešitve.

Prvi pregled po namestitvi

Po namestitvi programa ESET Internet Security se po prvi uspešni posodobitvi zažene pregled računalnika, ki preveri, ali je v računalniku zlonamerna koda.

Pregled računalnika lahko zaženete tudi ročno v glavnem oknu programa tako, da kliknete **Pametni pregled** > **Preglejte računalnik**. Več informacij o pregledih računalnika najdete v razdelku Pregled računalnika.



Nadgradnja na novejšo različico

Nove različice izdelka ESET Internet Security so izdane za uvajanje izboljšav ali odpravljanje težav, ki jih ni mogoče razrešiti s samodejnimi posodobitvami modulov programa. Nadgradnjo na novejšo različico lahko izvedete na več načinov:

1. Samodejno s posodobitvijo programa.
Ker je nadgradnja programa distribuirana vsem uporabnikom in lahko vpliva na določene konfiguracije sistema, je izdana šele po dolgem obdobju preskušanja, s čimer je zagotovljeno brezhibno delovanje z vsemi konfiguracijami sistema. Če morate nadgraditi na novejšo različico takoj po izdaji, uporabite enega od spodnjih načinov.
Prepričajte se, da ste omogočili možnost **Posodobitve funkcij programa** v razdelku Napredne nastavitve > **Posodobitev** > **Profili** > **Posodobitve**.

2. Ročno lahko to storite tako, da v glavnem oknu programa v razdelku **Posodobitev** kliknete **Poišči posodobitve**.

3. Ročno s prenosom in namestitvijo novejše različice prek starejše.

Za dodatne informacije in ilustrirana navodila glejte:

- Posodobitev izdelkov ESET – preverjanje najnovejših modulov izdelkov
- Katere so različne vrste posodobitev in izdaj izdelkov ESET?

Samodejna nadgradnja starejšega izdelka

Vaša različica izdelka ESET ni več podprta, zato je bil vaš izdelek nadgrajen na najnovejšo različico.

Pogoste težave z namestitvijo

Vsaka nova različica izdelkov ESET vključuje veliko popravkov in izboljšav. Obstoječe stranke z veljavno naročnino za izdelek ESET lahko na novo različico tega izdelka nadgradijo brezplačno.

Za dokončanje postopka namestitve:

1. Za sprejem licenčne pogodbe za končnega uporabnika kliknite možnost **Sprejmi in nadaljuj**, nato sprejmite še pravilnik o zasebnosti. Če se z licenčno pogodbo za končnega uporabnika ne strinjate, kliknite možnost **Odstrani**. Vrnitev na prejšnjo različico ni več mogoča.

2. Kliknite **Dovoli vse in nadaljuj**, da omogočite Sistem za povratne informacije ESET LiveGrid® in Program za izboljšanje izkušenj strank, ali pa kliknite **Nadaljuj**, če ne želite sodelovati.

3. Ko z aktivacijsko kodo aktivirate novi izdelek ESET, se prikaže stran s pregledom. Če podatkov o naročnini ni mogoče najti, nadaljujte z brezplačnim preskusom. Če naročnina, ki ste jo uporabljali za prejšnji izdelek, ni veljavna, aktivirajte izdelek ESET.

4. Za dokončanje namestitve je potreben ponovni zagon naprave.

Izdelek ESET Internet Security bo nameščen

To pogovorno okno se lahko prikaže:

- Med postopkom namestitve – kliknite možnost **Nadaljuj**, da namestite izdelek ESET Internet Security.

- Ko spreminjate naročnino v izdelku ESET Internet Security – kliknite **Aktiviraj**, da spremenite naročnino in aktivirate ESET Internet Security.

Možnost **Spremeni izdelek** omogoča preklop med izdelki za domačo uporabo ESET za Windows na podlagi vaše naročnine ESET. Za več informacij glejte razdelek Kateri izdelek imam?.

Sprememba na drugo serijo izdelkov

Možen je preklop med različnimi izdelki za domačo uporabo ESET za Windows na podlagi vaše naročnine ESET. Za več informacij glejte razdelek Kateri izdelek imam?.

Registracija

Naročnino registrirajte tako, da izpolnite polja, ki jih vsebuje obrazec za registracijo, in kliknete možnost **Aktiviraj**. Polja, ki so v oklepaju označena z »obvezno«, morate izpolniti. Ti podatki bodo uporabljeni samo za namene, povezane z vašo naročnino družbe ESET.

Potek aktiviranja

Postopek aktiviranja traja nekaj sekund (čas je lahko različen, odvisno od hitrosti internetne povezave v računalniku).

Aktiviranje je uspešno

Aktivacija je končana. Za dokončanje namestitve programa ESET Internet Security upoštevajte navodila čarovnika po namestitvi.

Posodobitev modulov se bo nadaljevala čez nekaj sekund. Redne posodobitve programa ESET Internet Security se bodo začele takoj.

Prvi pregled se bo samodejno zagnal 20 minut po končani posodobitvi modulov.

Postopek aktivacije se lahko prekine, če ponudba ni povezana z računom ESET HOME. Prijavite se v svoj račun ESET HOME ali ustvarite račun.

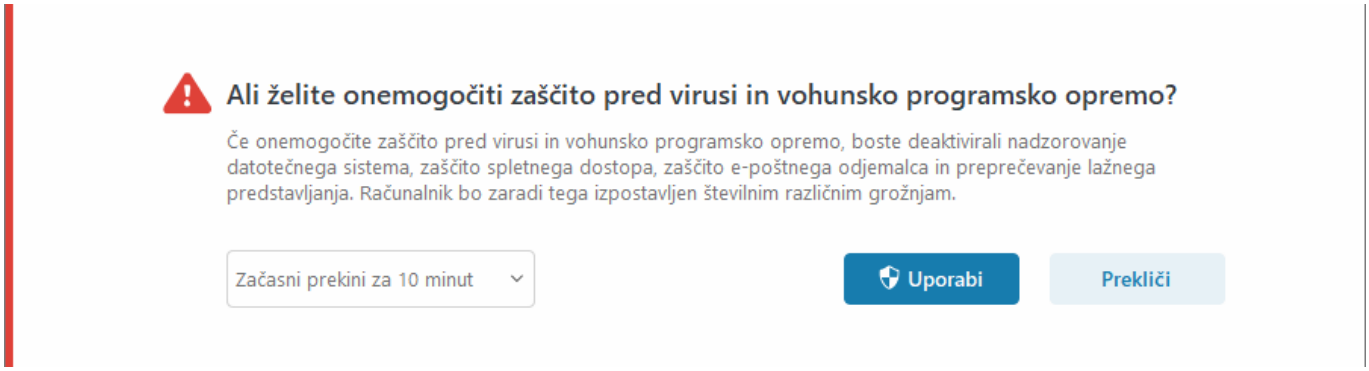
Priročnik za začetnike

V tem poglavju je podan uvodni pregled izdelka ESET Internet Security z osnovnimi nastavitvami.

Ikona sistemske vrstice

Nekatere najpomembnejše možnosti nastavitev in funkcije so na voljo, če z desno tipko miške kliknete ikono sistemske vrstice .

Začasno onemogoči zaščito – prikaže potrditveno pogovorno okno, ki onemogoči orodje za zaznavanje, ki ščiti sistem pred zlonamernimi napadi tako, da nadzoruje datoteko, splet in e-poštno komunikacijo. V spustnem meniju **Časovni interval** lahko določite, kako dolgo bo zaščita onemogočena.



Začasno onemogoči požarni zid (dovoli ves promet) – preklopi požarni zid v neaktivno stanje. Z več informacij glejte Omrežje.

Blokiraj ves omrežni promet – blokira ves omrežni promet. Omrežni promet znova omogočite tako, da kliknete **Prenehaj blokirati ves omrežni promet**.

Napredne nastavitve – odpre napredne nastavitve programa ESET Internet Security. Če želite odpreti napredne nastavitve v glavnem oknu izdelka, pritisnite F5 na tipkovnici ali kliknite **Nastavitve** > **Napredne nastavitve**.

Dnevniške datoteke – dnevniške datoteke zagotavljajo informacije o pomembnih dogodkih programa, ki so se zgodili, prav tako pa je na voljo predogled zaznanih elementov.

Odpri ESET Internet Security – odpre glavno okno programa ESET Internet Security.

Ponastavi postavitev okna – ponastavi okno programa ESET Internet Security na privzeto velikost in položaj na zaslonu.

Barvni način – odpre nastavitve uporabniškega vmesnika, kjer lahko spremenite njegovo barvo.

Poišči posodobitve – zažene posodobitev modula ali izdelka, da vam zagotovi zaščito. ESET Internet Security samodejno večkrat na dan preveri, ali so na voljo posodobitve.

Vizitka – navaja informacije o sistemu, podrobnosti o nameščeni različici programa ESET Internet Security, nameščene module programa in informacije o operacijskem sistemu ter sistemskih sredstvih.

Bližnjice na tipkovnici

Za boljšo krmarjenje v programu ESET Internet Security lahko uporabite te bližnjice na tipkovnici:

Bližnjice na tipkovnici	Dejanje
F1	odpre strani s pomočjo
F5	odpre napredne nastavitve
Puščica navzgor/puščica navzdol	krmarjenje v spustnih menijih
TAB	premik na naslednji element grafičnega uporabniškega vmesnika v oknu
Shift+TAB	premik na prejšnji element grafičnega uporabniškega vmesnika v oknu
ESC	zapre aktivno pogovorno okno
Ctrl+U	prikaže podatke o naročnini izdelka ESET in vašem računalniku (podrobnosti za tehnično podporo)
Ctrl+R	ponastavi okno izdelka na privzeto velikost in položaj na zaslonu
ALT + Puščica levo	krmarjenje nazaj
ALT + Puščica desno	krmarjenje naprej
ALT+Home	krmarjenje domov

Za krmarjenje lahko uporabite tudi gumba nazaj ali naprej.

Profili

Upravitelj profila se uporablja na dveh mestih v programu ESET Internet Security – v razdelku **Pregled na zahtevo** in v razdelku **Posodobitev**.

Pregled računalnika

V programu ESET Internet Security so 4 vnaprej določeni profili pregleda:

- **Pametni pregled**: to je privzeti napredni profil pregleda. Profil pametnega pregleda uporablja tehnologijo pametne optimizacije, ki preskoči datoteke, ki so bile med prejšnjim pregledom neproblematične in od takrat niso bile spremenjene. To omogoča krajši čas pregleda z najmanjšim možnim vplivom na varnost sistema.

- **Pregled priročnega menija** – zahtevate lahko pregled katere koli datoteke iz priročnega menija. Profil pregleda priročnega menija omogoča, da določite konfiguracijo pregleda, ki se uporablja pri tovrstnem zagonu pregleda.

- **Poglobljen pregled** – profil poglobljenega preglede privzeto ne uporablja pametne optimizacije, zato pri uporabi tega profila niso izpuščene nobene datoteke.

- **Pregled računalnika** – to je privzeti profil, ki se uporablja pri standardnem pregledu računalnika.

Prednostne parametre pregleda lahko shranite za pregledovanje v prihodnje. Priporočamo, da za vsak pregled, ki ga redno uporabljate, ustvarite drugačen profil (z različnimi cilji in načini pregleda ter drugimi parametri).

Če želite ustvariti nov profil, odprite okno razdelek Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** > **Pregled na zahtevo** > **Seznam profilov** > **Uredi**. V oknu **Upravitelj profila** je spustni meni **Izbrani profil** z obstoječimi profili pregleda in možnost za ustvarjanje novega profila. Če želite ustvariti profil pregleda, ki bo ustrezal vašim potrebam, glejte razdelek ThreatSense, v katerem boste našli opis vseh parametrov nastavitev pregleda.

> Recimo, da želite ustvariti lasten profil pregleda in konfiguracija **Preglejte računalnik** deloma ustreza vašim potrebam, vendar ne želite pregledati samoustvarjenih arhivov ali morebitno nevarnih programov, poleg tega pa želite uporabiti še možnost **Vedno popravi zaznani element**. V okno **Upravitelj profila** vnesite ime svojega novega profila in kliknite **Dodaj**. Iz spustnega menija **Izbrani profil** izberite svoj novi profil in preostale parametre prilagodite tako, da ustrezajo vašim zahtevam, nato za shranjevanje kliknite možnost **V redu**.

Posodabljanje

Upravitelj profila v razdelku Nastavitve posodobitve omogoča uporabnikom ustvarjanje novih profilov posodabljanja. Ustvarite in uporabite lasten profil po meri (to pomeni profil, ki ni privzeti **Moj profil**), le če računalnik vzpostavlja povezavo s strežniki za posodabljanje na več načinov.

Na primer prenosni računalnik, ki normalno vzpostavlja povezavo z lokalnim strežnikom (zrcalnim strežnikom) v lokalnem omrežju, a prenaša posodobitve neposredno iz ESET-ovih strežnikov za posodabljanje, ko ni povezan z lokalnim omrežjem (na poslovni poti), lahko uporablja dva profila: prvega za vzpostavitev povezave z lokalnim strežnikom, drugega pa za vzpostavitev povezave z ESET-ovimi strežniki. Ko sta profila konfigurirana, se pomaknite do možnosti **Orodja** > **Razporejevalnik** in uredite parametre opravila posodabljanja. Določite en profil kot primarni in drugega kot sekundarni.

Profil posodobitev – trenutno uporabljeni profil posodobitev. Če ga želite spremeniti, izberite profil iz spustnega menija.

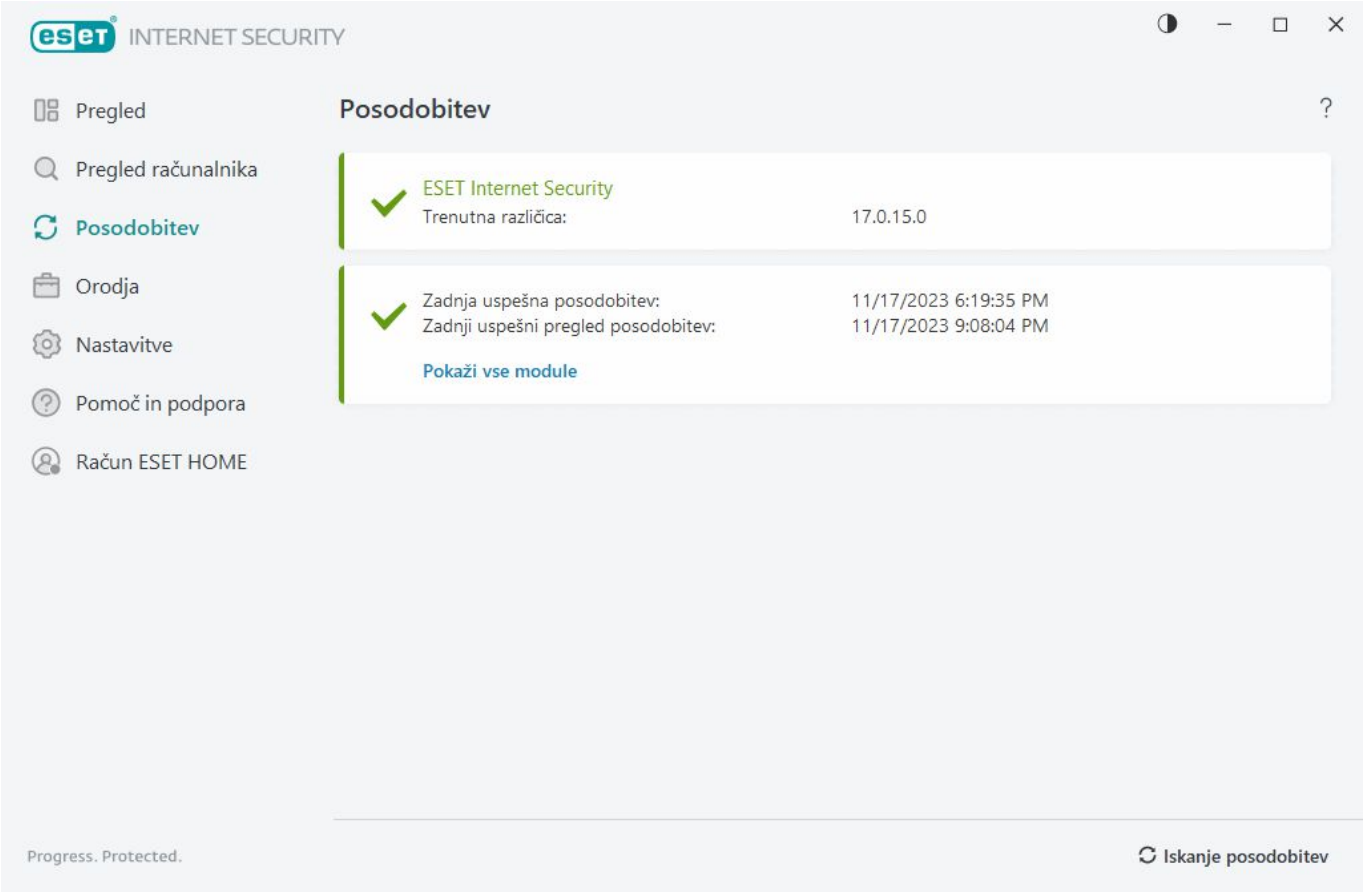
Seznam profilov – ustvarite nove profile posodobitev ali odstranite obstoječe.

Posodobitve

Z rednim posodabljanjem programa ESET Internet Security najbolje zagotovite največjo raven zaščite v računalniku. Modul za posodobitev zagotavlja, da so tako programski moduli kot sistemske komponente vedno posodobljeni.

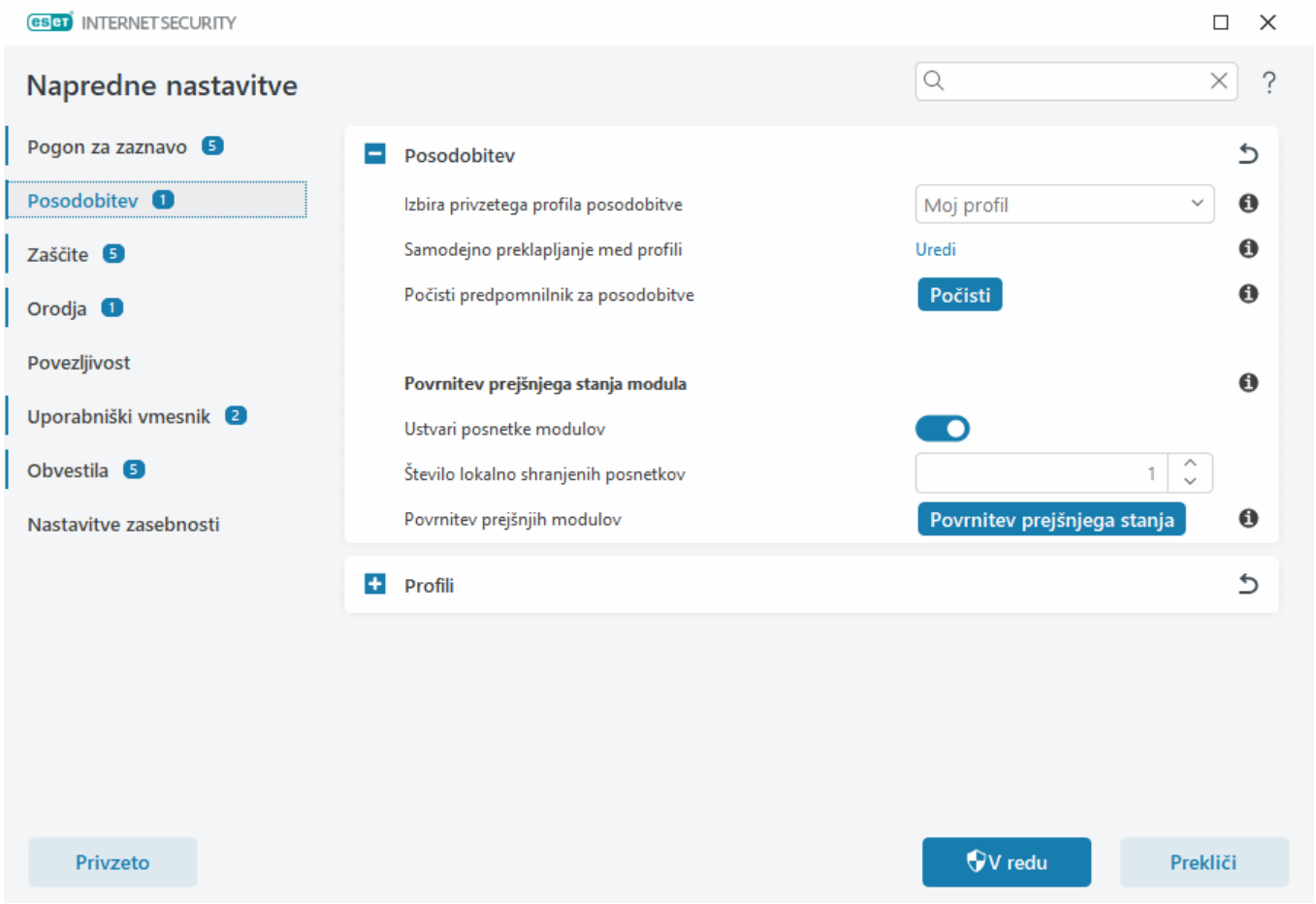
Če v glavnem oknu programa kliknete **Posodobitev**, lahko poiščete trenutno stanje posodobitve, vključno z datumom in časom zadnje uspešne posodobitve in v primeru, da potrebujete posodobitev.

Poleg samodejnih posodobitev lahko kliknete možnost **Preveri, ali so na voljo posodobitve**, da sprožite ročno posodobitev.



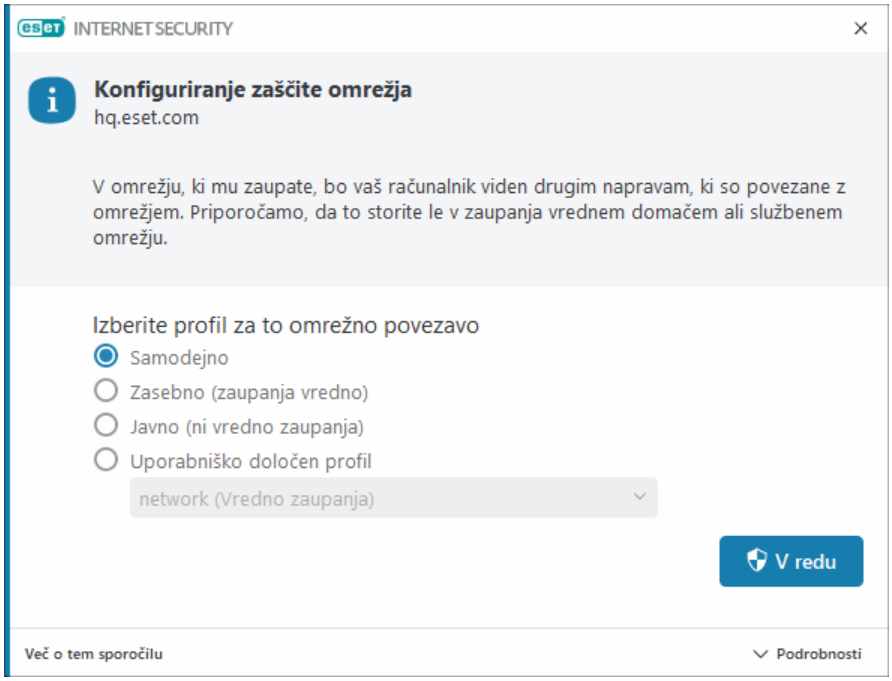
Razdelek Napredne nastavitve > **Posodobitev** vsebuje dodatne možnosti posodobitve, kot so način posodobitve, dostop do strežnika proxy in povezave z lokalnim omrežjem.

Če pri posodobitvi prihaja do težav, kliknite **Počisti**, da počistite predpomnilnik za posodobitve. Če modulov programa še vedno ni mogoče posodobiti, glejte razdelek Odpravljanje težav za sporočilo »Posodobitev modulov ni uspela«.



Konfiguriranje zaščite omrežja

Program ESET Internet Security pri zaznavi novega omrežja privzeto uporabi nastavitve sistema Windows. Če želite prikazati pogovorno okno, ko je zaznano novo omrežje, spremenite dodelitev profila zaščite omrežja na možnost **Vprašaj**. Konfiguracija zaščite omrežja se prikaže vedno, ko se računalnik poveže z novim omrežjem.



Izbirate lahko med naslednjimi profili omrežnih povezav:

Samodejno – program ESET Internet Security bo samodejno izbral profil na podlagi aktivatorjev, konfiguriranih za vsak profil.

Zasebno – za zaupanja vredna omrežja (domače ali službeno omrežje). Računalnik in datoteke v skupni rabi, shranjene v računalniku, so vidne drugim uporabnikom omrežja, sistemski viri pa so dostopni drugim uporabnikom v omrežju (omogočen je dostop do datotek in tiskalnikov v skupni rabi, omogočena je dohodna komunikacija RPC in na voljo je skupna raba oddaljenega namizja). Priporočamo uporabo te nastavitve pri dostopu do varnega lokalnega omrežja. Ta profil je samodejno dodeljen omrežni povezavi, če je konfiguriran kot domena ali zasebno omrežje v sistemu Windows.

Javno – za omrežja, ki niso vredna zaupanja (javno omrežje). Datoteke in mape v vašem sistemu niso v skupni rabi ali vidne drugim uporabnikom v omrežju in deljenje sistemskih virov je deaktivirano. Pri dostopu do brezžičnih omrežij priporočamo uporabo te nastavitve. Ta profil je samodejno dodeljen kateri koli omrežni povezavi, ki ni konfigurirana kot domena ali zasebno omrežje v sistemu Windows.

Uporabniško določen profil – v spustnem meniju lahko izberete profil, ki ste ga ustvarili. Ta možnost je na voljo le, če ste ustvarili vsaj en profil po meri.

Nepravilna konfiguracija omrežja lahko predstavlja varnostno tveganje za računalnik.

Omogočite Zaščita pred krajo

Na poti od doma do službe in na druga javna mesta, ki jih vsakodnevno obiskujemo, so naše osebne naprave ves čas v nevarnosti, da jih izgubimo ali da nam jih ukradejo. Zaščita pred krajo je funkcija, ki razširja varnost na ravni uporabnika v primeru izgubljene ali ukradene naprave. S funkcijo Zaščita pred krajo lahko nadzirate uporabo naprave in izsledite izgubljeno napravo tako, da jo poiščete prek naslova IP v računu ESET HOME, kar vam omogoča, da jo znova pridobite in zaščitite osebne podatke.

S sodobnimi tehnologijami, kot so iskanje zemljepisne lokacije prek naslova IP, zajemanje slik s spletno kamero, zaščita uporabniškega računa in nadziranje naprave, lahko z uporabo funkcije Zaščita pred krajo vi in organi kazenskega pregona hitreje poiščete računalnik ali napravo, ki je izgubljena ali ukradena. V računu ESET HOME lahko vidite, katere dejavnosti se izvajajo v računalniku ali napravi.

Če želite izvedeti več o funkciji Zaščita pred krajo v računu ESET HOME, si oglejte spletno pomoč ESET HOME.

Funkcija Zaščita pred krajo zaradi omejitev pri upravljanju uporabniških računov morda ne bo delovala pravilno v računalnikih v domenah.

Če želite omogočiti funkcijo Zaščita pred krajo in zaščititi svojo napravo pred izgubo ali krajo, izberite eno od naslednjih možnosti:

- V glavnem oknu programa > **Pregled** kliknite možnost **NASTAVI** zraven **Zaščita pred krajo**.
- Če v glavnem oknu programa > **Pregled** zaslon opazite sporočilo »Funkcija Anti-Theft je na voljo«, kliknite možnost **Omogoči Zaščita pred krajo**.
- V glavnem oknu programa kliknite razdelek **Nastavitve** > **Varnostna orodja**. Omogočite gumb za preklop **Zaščita pred krajo** in upoštevajte navodila na zaslonu.

Če naprava ni povezana z računom ESET HOME, storite naslednje:
1. Ko omogočite funkcijo Zaščita pred krajo, se prijavite se v račun ESET HOME.
2. Nastavite ime naprave.

Zaščita pred krajo ne podpira Microsoft Windows Home Server.

Ko omogočite funkcijo Zaščita pred krajo, lahko optimizirate varnost svoje naprave v glavnem oknu programa > **Nastavitve** > **Varnostna orodja** > **Zaščita pred krajo**.

Starševski nadzor

Če ste v programu ESET Internet Security funkcijo starševskega nadzora že omogočili, morate starševski nadzor konfigurirati tudi za vse povezane uporabniške račune.

Če je funkcija starševskega nadzora aktivna, uporabniški računi pa niso konfigurirani, se na zaslonu **Pregled** v izdelku ESET Internet Security prikaže obvestilo »Starševski nadzor ni nastavljen«. Kliknite možnost **Nastavi pravila**, več pa si preberite v razdelku Starševski nadzor.

Aktiviranje izdelka

Na voljo je več načinov za aktivacijo izdelka. Razpoložljivost določenega scenarija aktivacije v oknu za aktivacijo je odvisna od države in načina distribucije (CD/DVD, spletna stran družbe ESET itn.):

- Če ste kupili maloprodajno različico izdelka v embalaži ali prejeli e-poštno sporočilo s podatki o naročnini, aktivirajte izdelek tako, da kliknete možnost **Uporabite kupljeni aktivacijsko kodo**. Aktivacijska koda morate vnesti tako, kot je naveden, sicer aktivacija ne bo uspešna. Aktivacijska koda – enoličen niz v obliki XXXX-XXXX-XXXX-XXXX-XXXX ali XXXX-XXXXXXXX, ki se uporablja za identifikacijo lastnika naročnine in aktivacijo naročnine. Aktivacijska koda je po navadi naveden na zadnji strani škatle z izdelkom.

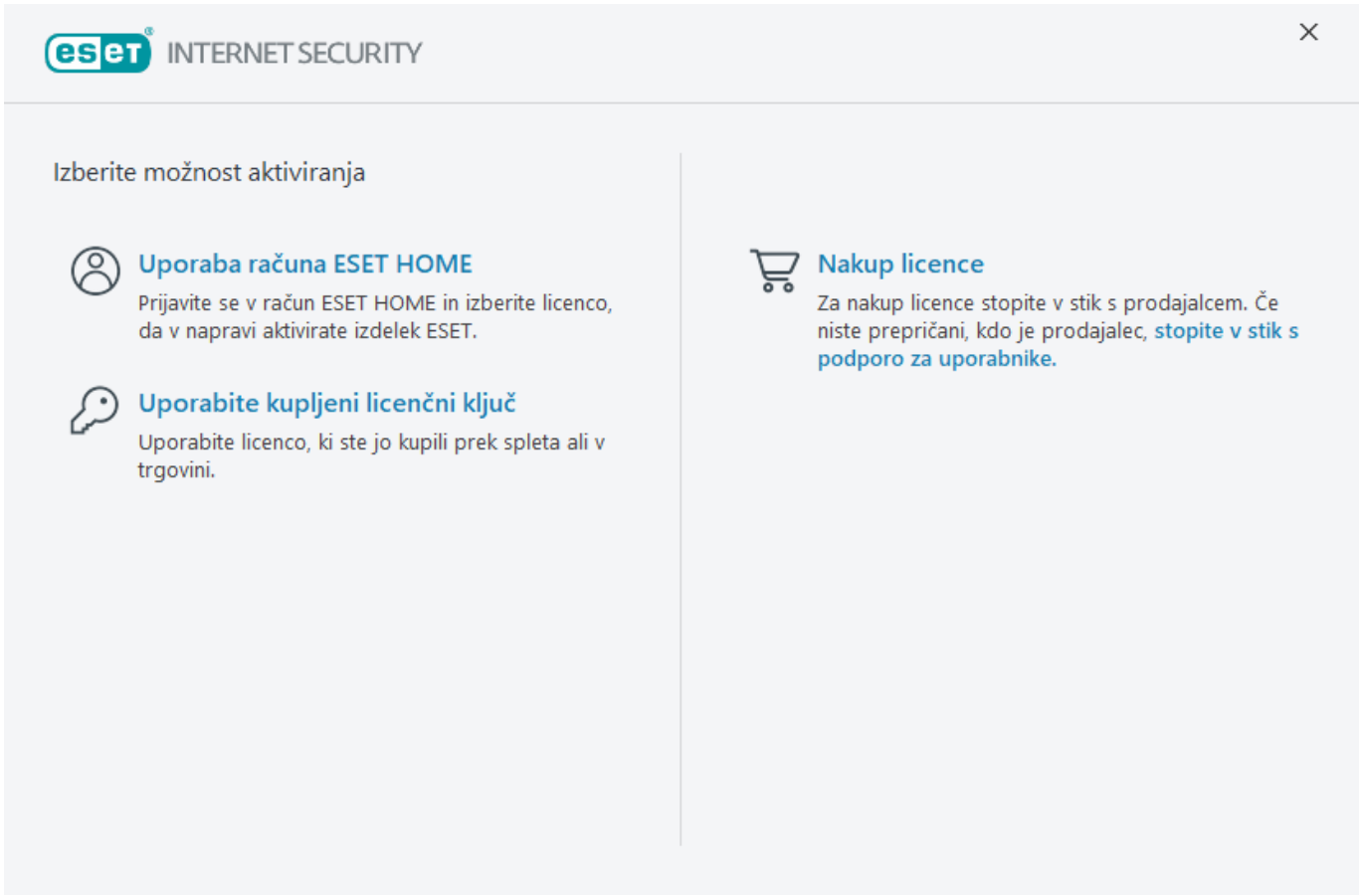
- Ko izberete možnost Uporaba računa ESET HOME, boste pozvani k prijavi v račun ESET HOME.

- Če želite izdelek ESET Internet Security pred nakupom preizkusiti, izberite možnost Brezplačni preizkus. Vnesite e-poštni naslov in državo, da izdelek ESET Internet Security aktivirate za omejen čas. Brezplačno preskusno različico vam bomo poslali po e-pošti. Brezplačno preskusno različico je mogoče aktivirati samo enkrat na stranko.

- Če nimate naročnine in jo želite kupiti, kliknite možnost »**Nakup naročnine**«. S tem boste preusmerjeni na spletno mesto lokalnega dobavitelja izdelkov podjetja ESET. Naročnine na izdelke ESET Windows Home niso brezplačne.

Naročnino za izdelek lahko kadar koli spremenite. To storite tako, da v glavnem oknu programa kliknete **Pomoč in podpora** > **Spremeni naročnino**. Videli boste javni ID, ki ga oddelek za podporo družbe ESET uporablja za identifikacijo naročnine.

Ali aktivacija izdelka ni uspela?



Vnos aktivacijske kode med aktiviranjem

Samodejne posodobitve so pomembne za varnost. ESET Internet Security bo prejel posodobitve šele, ko ga aktivirate.

Aktivacijska koda vnesite natančno, tako, kot je zapisan. Aktivacijska koda je enoličen niz v obliki XXXX-XXXX-XXXX-XXXX-XXXX, ki se uporablja za identifikacijo lastnika naročnine in aktiviranje naročnine.

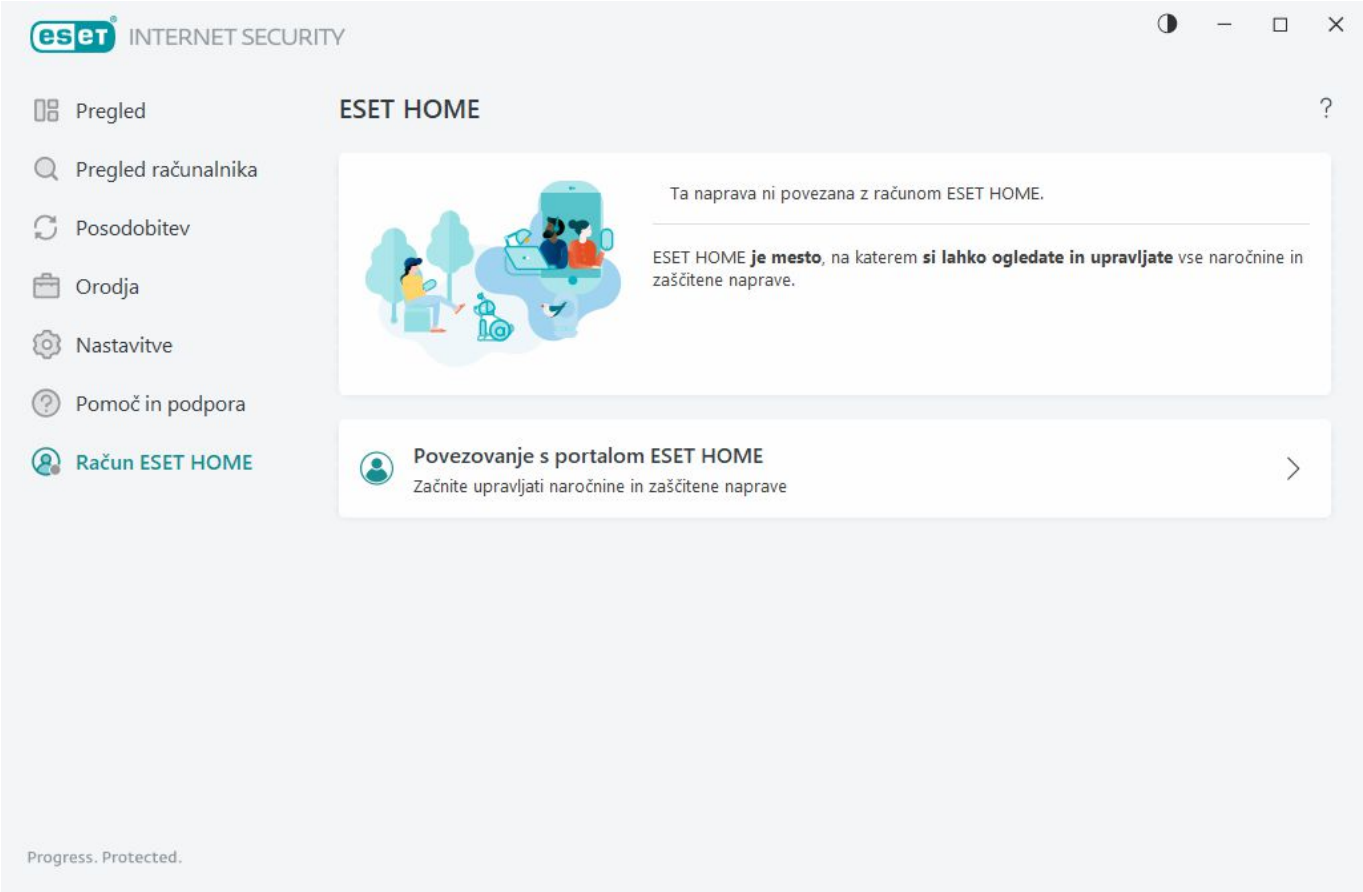
Priporočamo, da aktivacijsko kodo kopirate iz e-poštnega sporočila za registracijo in ga prilepite.

Če aktivacijske kode niste vnesli po namestitvi, izdelek ne bo aktiviran. Program ESET Internet Security lahko aktivirate v glavnem oknu programa > **Pomoč in podpora** > **Aktiviraj naročnino**.

Naročnine na izdelke ESET Windows Home niso brezplačne.

Uporaba računa ESET HOME

Napravo povežite s ESET HOME, da preverite in upravljate vse svoje aktivirane naročnine ESET ter naprave. Naročnino lahko obnovite, nadgradite ali podaljšate in si ogledate pomembne podrobnosti naročnine. V mobilni aplikaciji ali na portalu za upravljanje računa ESET HOME lahko dodate različne naročnine, prenesete izdelke v svoje naprave, preverite varnostno stanje izdelka ali delite naročnino prek e-pošte. Za več informacij obiščite spletno pomoč za račun ESET HOME.



Ko za način aktiviranja izberete možnost **Uporaba računa ESET HOME** ali ko se med namestitvijo povežete z računom ESET HOME:

1. Prijavite se v račun ESET HOME.

> Če nimate računa ESET HOME, kliknite možnost **Ustvari račun**, da ga registrirate, ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.
> Če ste pozabili geslo, kliknite **Pozabljeno geslo** in upoštevajte navodila na zaslonu ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.

2. Nastavite **ime naprave** za napravo, ki se bo uporabljala za vse storitve računa ESET HOME, in kliknite možnost **Nadaljuj**.

3. Izberite naročnino, ki jo želite aktivirati, ali dodajte novo naročnino. Kliknite možnost **Nadaljuj**, da aktivirate izdelek ESET Internet Security.

Aktivacija brezplačne preizkusne licence

Za aktivacijo preskusne različice izdelka ESET Internet Security vnesite veljaven e-poštni naslov v polji **E-poštni naslov** in **Potrdite e-poštni naslov**. Po aktivaciji bo naročnina ESET, ustvarjena in poslana na vaš e-poštni naslov. Na ta e-poštni naslov boste prejeli tudi obvestila o poteku veljavnosti izdelka in druga sporočila družbe ESET. Brezplačno preskusno različico je mogoče aktivirati samo enkrat.

Če želite izdelek ESET Internet Security registrirati pri lokalnem distributerju, ki vam bo nudil tehnično podporo, izberite državo v spustnem meniju **Država**.

Brezplačna aktivacijska koda ESET

Naročnina za izdelek ESET Internet Security ni brezplačna.

Aktivacijska koda ESET je enolična kombinacija črk in številk, ločenih s pomišljajem, ki jo zagotovi družba ESET za zakonito uporabo izdelka ESET Internet Security v skladu z licenčno pogodbo za končnega uporabnika. Vsak končni uporabnik lahko uporablja aktivacijska koda le v obsegu, v katerem ima pravico do uporabe izdelka ESET Internet Security na podlagi števila licenc, ki mu jih izda družba ESET. Aktivacijska koda je zaupna in je ni mogoče deliti z drugimi; lahko pa daste naročnino v skupno rabo z aplikacijo ESET HOME.

Morda vam bodo internetni viri ponujali »brezplačne« aktivacijske kode ESET, vendar si zapomnite:

- Če kliknete oglas »Brezplačna naročnina ESET«, lahko ogrozite varnost računalnika ali naprave, saj se lahko okuži z zlonamerno programsko opremo. Zlonamerna programska oprema se lahko skriva v neuradni spletni vsebini (npr. v videoposnetkih), na spletnih mestih, ki prikazujejo oglase in služijo z obiski itd. Običajno so to pasti.
- Družba ESET ima pravico onemogočiti ponarejene naročnine in to tudi izvaja.
- Uporaba ponarejenega aktivacijske kode ni v skladu z licenčno pogodbo za končnega uporabnika, s katero morate soglašati, če želite namestiti izdelek ESET Internet Security.
- Naročnine ESET kupite le prek uradnih kanalov, kot so spletno mesto www.eset.com in pooblaščeni dobavitelji ali prodajalci izdelkov ESET (ne kupujte naročnin na neuradnih spletnih mestih tretjih oseb, kot je eBay, ali skupnih naročnin tretjih oseb).
- Prenos izdelka ESET Internet Security je brezplačen, vendar je za aktivacijo med namestitvijo potrebna veljavna aktivacijska koda ESET (izdelek lahko prenesete in namestite, vendar brez aktivacije ne bo deloval).
- Svoje naročnine ne delite z drugimi v internetu ali na družabnih omrežjih (lahko se razširi).

Za navodila o prepoznavanju in prijavi ponarejenih naročnin ESET glejte članek v naši zbirki znanja.

Če niste prepričani glede nakupa varnostnega izdelka ESET, lahko najprej preskusite preskusno različico, da se lažje odločite:

1. Aktivirajte ESET Internet Security z brezplačnim preizkusom
2. Sodelujte v beta programu ESET
3. Namestite ESET Mobile Security, če uporabljate mobilno napravo s sistemom Android (brezplačno z omejitvami)

Za pridobitev popusta/podaljšanje licence obnovite licenco ESET.

Aktiviranje ni uspelo – pogosti vzroki

Če aktivacija izdelka ESET Internet Security ni uspešna, so najpogostejši vzroki:

- Aktivacijska koda je že v uporabi.
- Vnesli ste neveljavno serijsko številko.
- Podatki v obrazcu za aktiviranje manjkajo ali so neveljavni.
- Komunikacija s strežnikom za aktiviranje ni uspela.
- Povezava s strežniki družbe ESET za aktivacijo ni vzpostavljena ali je onemogočena.

Preverite, ali ste vnesli ustrezno aktivacijsko kodo in ali je internetna povezava aktivna. Znova poskusite aktivirati izdelek ESET Internet Security. Če za aktivacijo uporabljate račun ESET HOME, glejte Naročnine in upravljanje naročnin ESET HOME – Spletna pomoč.

Če se prikaže določena napaka (na primer »Začasno onemogočena naročnina« ali »Prekomerna uporaba naročnine«), sledite navodilom v stanju naročnine.

Če aktivacija ESET Internet Security še vedno ne uspe, vas bo naše orodje za odpravljanje težav pri aktivaciji ESET vodilo skozi pogosta vprašanja, napake in težave pri aktivaciji ter licenciranju (na voljo v angleščini in nekaterih drugih jezikih).

Stanje naročnine

Vaša naročnina ima lahko različna stanja. Stanje naročnine najdete v aplikaciji ESET HOME. Če želite dodati naročnino v račun ESET HOME, glejte Dodajanje naročnine.

Če nimate računa ESET HOME, lahko ustvarite nov račun ESET HOME.

Če stanje naročnine ni **Aktivno**, se med aktiviranjem prikaže napaka ali obvestilo v glavnem oknu programa.

Če želite onemogočiti obvestila o stanju naročnine, odprite Napredne nastavitve > **Obvestila** > **Stanja programa**. Kliknite **Uredi** poleg možnosti **Stanja programa**, razširite **Licenciranje** in počistite potrditveno polje poleg obvestila, ki ga želite onemogočiti. Z onemogočenjem obvestila ne rešite težave.

V spodnji tabeli si oglejte opise in priporočene rešitve za različna stanja naročnine:

Stanje naročnine	Opis	Rešitev
Aktivna	Naročnina je veljavna in ni potrebe po ukrepanju. Izdelek ESET Internet Security lahko aktivirate, podrobnosti o naročnini pa so na voljo v glavnem oknu programa > **Pomoč in podpora**.	
Prekomerna uporaba	To naročnino uporablja več naprav, kot je dovoljeno. Prikaže se napaka pri aktiviranju.	Za več informacij glejte Aktiviranje ni uspelo zaradi prekomerne uporabe naročnine.

Stanje naročnine	Opis	Rešitev
Začasno prekinjena	Veljavnost naročnine je bila začasno prekinjena zaradi težav s plačilom. Če želite uporabiti naročnino, se prepričajte, da so vaši podatki za plačilo na portalu ESET HOME posodobljeni ali pa se obrnite na prodajalca naročnin. Ta napaka se lahko prikaže med aktiviranjem ali v glavnem oknu programa.	Nameščen izdelek – če imate račun ESET HOME, v obvestilu, prikazanem v glavnem oknu programa, kliknite **Upravljanje naročnine na portalu ESET HOME** in preglejte podatke za plačilo. V nasprotnem primeru se obrnite na prodajalca naročnine. Napaka pri aktiviranju – če imate račun ESET HOME, v oknu z napako pri aktiviranju kliknite **Odpri ESET HOME** in preglejte podatke za plačilo. V nasprotnem primeru se obrnite na prodajalca naročnine.
Potekla	Naročnina je potekla, zato je ne morete uporabiti za aktiviranje izdelka ESET Internet Security. Ta napaka se lahko prikaže med aktiviranjem ali v glavnem oknu programa. Če ste izdelek ESET Internet Security že namestili, računalnik ni zaščiten in posodobljen.	Nameščen izdelek – v obvestilu, ki je prikazano v glavnem oknu programa, kliknite **Obnovi naročnino** in upoštevajte navodila v razdelku Kako obnovim svojo naročnino? ali pa kliknite **Aktivirajte izdelek** in izberite način aktiviranja. Napaka pri aktiviranju – v oknu z napako pri aktiviranju kliknite **Obnovite naročnino** in upoštevajte navodila v razdelku Kako obnovim naročnino? ali pa vnesite novo ali obnovljeno aktivacijsko kodo in kliknite **Obnovi naročnino**.
Preklicana	Vašo naročnino je preklicala družba ESET ali prodajalec naročnine.	Če se prikaže napaka: »Naročnina preklicana v glavnem oknu programa ali med aktiviranjem« in »naročnina bi morala pravilno delovati«, se obrnite na prodajalca naročnine.

Aktiviranje ni uspelo zaradi prekomerne uporabe naročnine

Težava

- Vaša naročnina se morda prekomerno uporablja ali zlorablja
- Aktiviranje ni uspelo zaradi prekomerne uporabe naročnine

Rešitev

Naročnino uporablja več naprav, kot je dovoljeno. Morda ste žrtev piratstva programske opreme ali ponaredbe. Naročnine ni mogoče uporabiti za aktivacijo nobenega drugega izdelka ESET. Če imate možnost upravljanja naročnine v računu za ESET HOME oziroma ste naročnino kupili pri uradnem viru, lahko težavo odpravite takoj. Če še nimate računa, ga ustvarite.

Če ste lastnik naročnine in niste bili pozvani, da vnesete svoj e-poštni naslov:

1. Če želite upravljati naročnino ESET, odprite spletni brskalnik in obiščite https://home.eset.com. Odprite funkcijo ESET License Manager in odstranite sedeže ali jih deaktivirajte. Za več informacij glejte razdelek Kaj storiti v primeru prekomerne uporabe naročnine.

2. Za navodila o prepoznavanju in prijavi ponarejenih naročnin ESET glejte članek v naši zbirki znanja o prepoznavanju in prijavljanju ponarejenih naročnin za izdelke ESET.

3. Če niste prepričani, kliknite **Nazaj** in pošljite e-poštno sporočilo tehnični podpori družbe ESET.

Če niste lastnik naročnine, stopite v stik z lastnikom naročnine in mu sporočite, da zaradi prekomerne uporabe naročnine ni mogoče aktivirati izdelka ESET. Lastnik lahko težavo odpravi na portalu ESET HOME.

Če ste pozvani, da potrdite e-poštni naslov, vnesite e-poštni naslov, prvotno uporabljen za nakup ali aktivacijo programa ESET Internet Security.

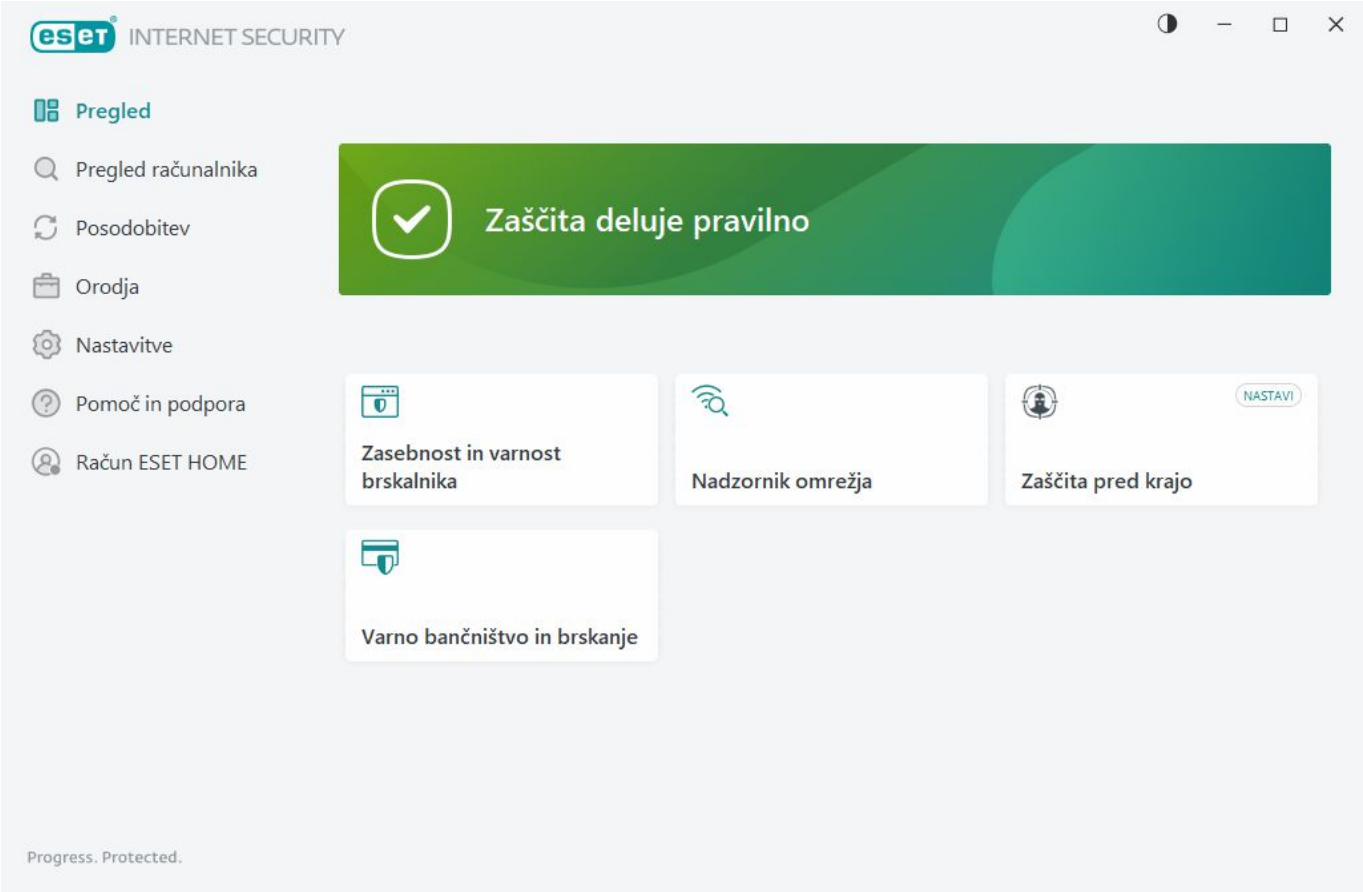
Delo s programom ESET Internet Security

Glavno okno programa ESET Internet Security je razdeljeno v dva razdelka. V primarnem oknu na desni so prikazane informacije, ki ustrezajo izbrani možnosti iz glavnega menija na levi.

> **Ilustrirana navodila**
> Oglejte si Odprtje glavnega okna programa za izdelke ESET v sistemu Windows za ilustrirana navodila, ki so na voljo v angleščini in v nekaterih drugih jezikih.

Barvno shemo grafičnega uporabniškega vmesnika programa ESET Internet Security lahko izberete v zgornjem desnem kotu glavnega okna programa. Kliknite ikono **Barvna shema** (ikona se spreminja na podlagi trenutno izbrane barvne sheme) poleg ikone **Minimiziraj** in v spustnem meniju izberite barvno shemo:

- **Enako kot sistemska barva** – nastavi barvno shemo programa ESET Internet Security na podlagi nastavitev operacijskega sistema.
- **Temno** – program ESET Internet Security bo imel temno barvno shemo (temni način).
- **Svetlo** – program ESET Internet Security bo imel standardno, svetlo barvno shemo.



Možnosti glavnega menija:

Pregled – navedene so informacije o stanju zaščite programa ESET Internet Security.

Pregled računalnika – konfigurirajte in zaženite pregled računalnika ali ustvarite pregled po meri.

Posodobitev – prikaže informacije o posodobitvah modula in pogona za zaznavo.

Orodja – zagotavlja dostop do funkcije Nadzornik omrežja in drugih funkcij , ki poenostavijo upravljanje programa in zagotavljajo dodatne možnosti za napredne uporabnike.

Nastavitve – ponuja možnosti konfiguracije za funkcije zaščite programa ESET Internet Security (zaščita računalnika, zaščita na spletu, zaščita omrežja in varnostna orodja) in dostop do naprednih nastavitev.

Pomoč in podpora – prikaže informacije o naročnini in nameščenem izdelku ESET ter povezave do spletne pomoči, zbirke znanja družbe ESET in tehnične podpore.

Račun ESET HOME – povežite svojo napravo z računom ESET HOME ali si oglejte stanje povezave z računom ESET HOME. Uporabite ESET HOME za ogled in upravljanje nastavitev Zaščita pred krajo ter aktiviranih naročnin ESET in naprav.

Pregled

V oknu **Pregled** so prikazane informacije o trenutni zaščiti računalnika skupaj s hitrimi povezavami do varnostnih funkcij v izdelku ESET Internet Security.

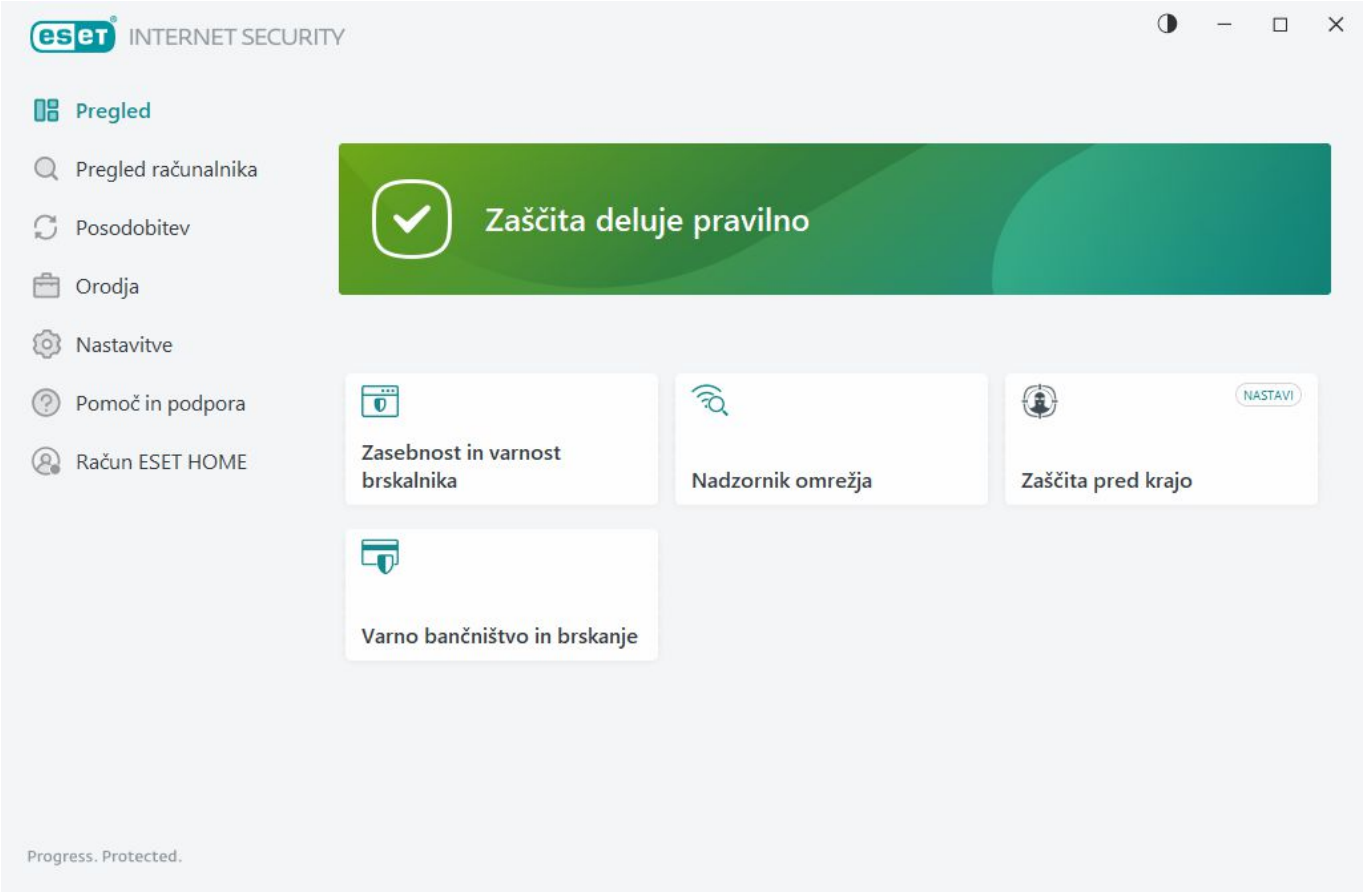
V oknu **Pregled** so prikazana obvestila s podrobnimi informacijami in priporočenimi rešitvami za izboljšanje varnosti izdelka ESET Internet Security, vklop dodatnih funkcij ali zagotavljanje največje zaščite. Če je obvestil več,

kliknite **Še X obvestil**, da razširite vsa.

Nadzornik omrežja – Preverite varnost omrežja.

Varno bančništvo in brskanje – zažene brskalnik, nastavljen kot privzeti v sistemu Windows, v varnem načinu.

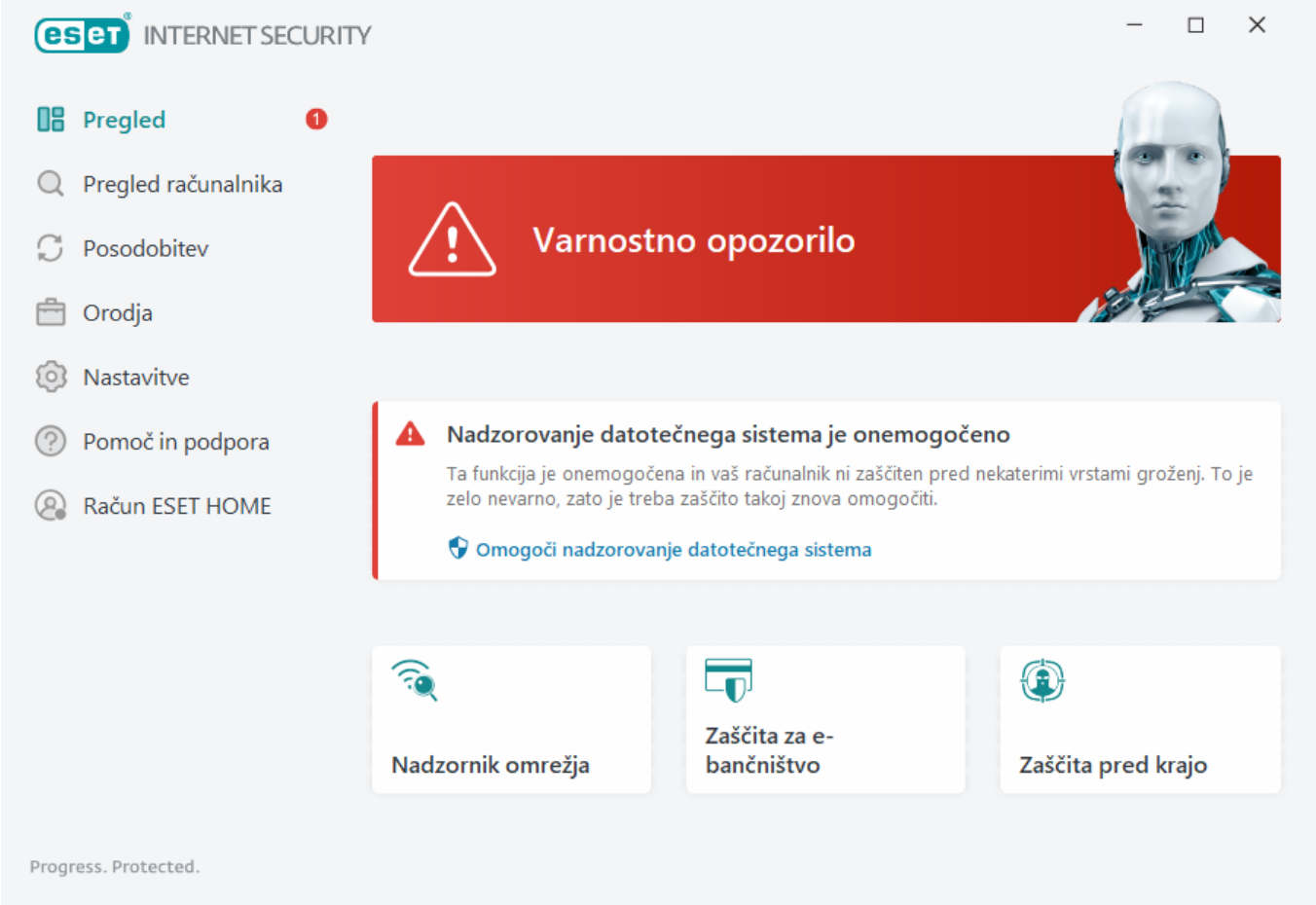
Zaščita pred krajo – zažene nastavitev za Zaščita pred krajo. Če ste Zaščita pred krajo že nastavili, hitra povezava odpre stran za Zaščita pred krajo.



Zelena ikona in zeleno stanje **Zaščiteni ste** označujeta največjo možno zaščito.

Kaj storiti, če program ne deluje pravilno

Če aktivni modul zaščite deluje pravilno, je ikona stanja zaščite zelene barve. Rdeč klicaj ali oranžna ikona za obveščanje pomeni, da ni zagotovljena največja zaščita. Dodatne informacije o stanju zaščite vsakega modula in predlogi rešitev za obnovitev popolne zaščite so prikazane v obliki obvestila v oknu **Pregled**. Če želite spremeniti stanje posameznih modulov, kliknite **Nastavitve** in izberite želeni modul.



Rdeča ikona in rdeče obarvano stanje **Varnostno opozorilo** opozarjata na kritične težave. To stanje se lahko prikaže zaradi več razlogov:

- **Izdelek ni aktiviran** ali **Naročnina je potekla** – to označuje ikona stanja zaščite rdeče barve. Programa po poteku naročnine ne bo več mogoče posodabljati. Upoštevajte navodila v oknu z opozorilom in obnovite svojo naročnino.
- **Orodje za zaznavanje je zastarelo** – ta napaka se prikaže po več neuspešnih poskusih posodobitve orodja za zaznavanje. Priporočamo vam, da preverite nastavitve posodobitev. Najpogostejši vzrok te napake so nepravilno vneseni podatki za preverjanje pristnosti ali nepravilno konfigurirane nastavitve povezave.
- **Sprotna zaščita datotečnega sistema je onemogočena** – sprotno zaščito je onemogočil uporabnik. Vaš računalnik ni zaščiten pred grožnjami. Kliknite **Omogoči sprotno zaščito datotečnega sistema**, da znova omogočite to funkcijo.
- **Protivirusna zaščita je onemogočena** – zaščito pred virusi in vohunsko programsko opremo lahko znova omogočite tako, da kliknete **Omogoči zaščito pred virusi in vohunsko programsko opremo**.
- **Osebni požarni zid ESET je onemogočen** – na to težavo opozarja tudi varnostno obvestilo ob elementu **Omrežje** na namizju. Zaščito računalniškega omrežja lahko znova omogočite tako, da kliknete **Omogoči požarni zid**.

Oranžna ikona označuje omejeno zaščito. Na primer, da je morda prišlo do težave pri posodobitvi programa ali da bo vaša naročnina morda kmalu potekla.
To stanje se lahko prikaže zaradi več razlogov:

- **Opozorilo za optimizacijo zaščite pred krajo** – naprava ni optimizirana za Zaščita pred krajo. V

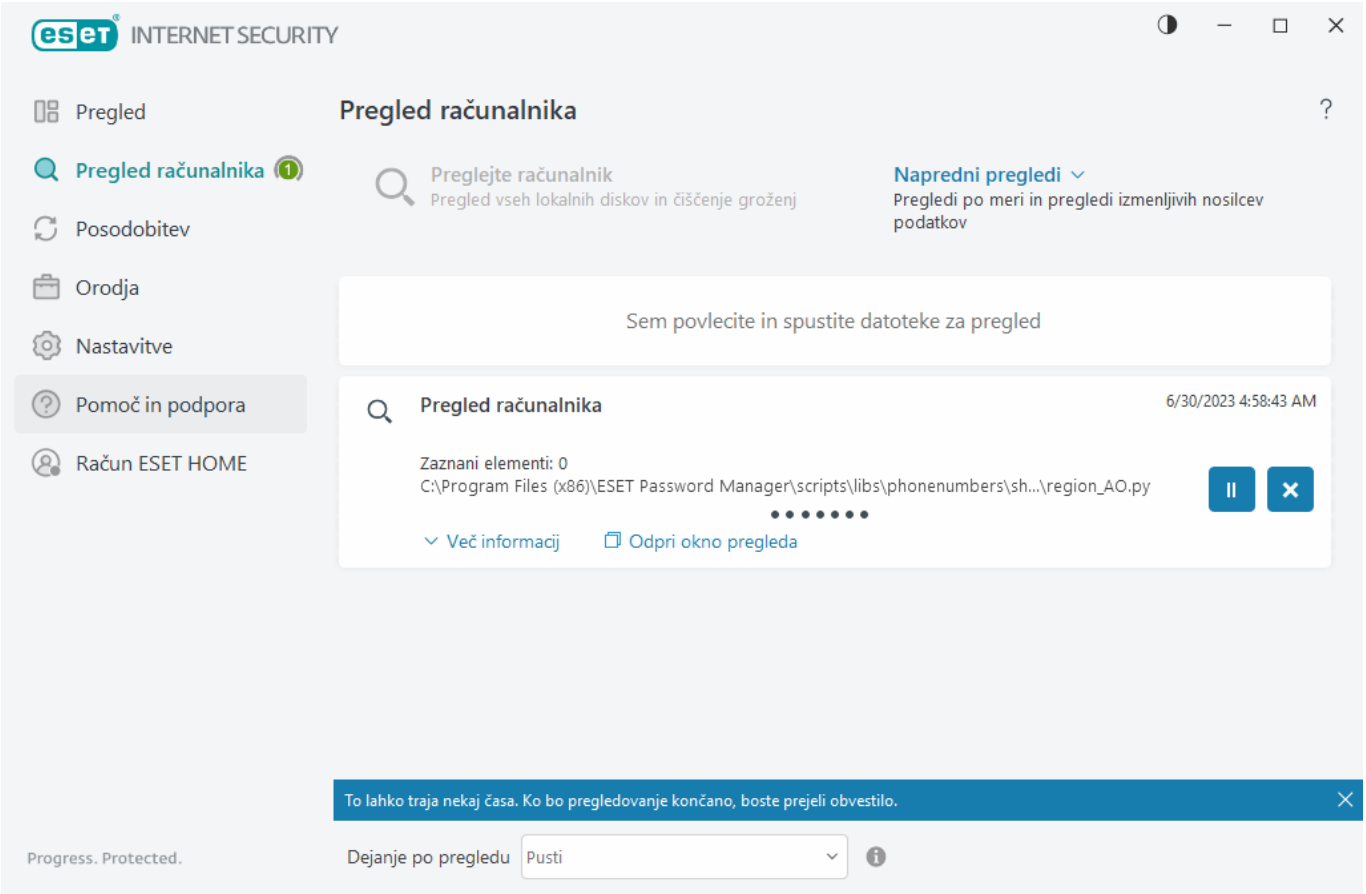
računalniku na primer ni mogoče ustvariti fantomskega računa (varnostne funkcije, ki se sproži samodejno, ko označite napravo kot izgubljeno). Fantomski račun lahko ustvarite s funkcijo optimiziranja v spletnem vmesniku programa Zaščita pred krajo.

- **Način za igranje je aktiven** – če omogočite Način za igranje, je to lahko morebitno varnostno tveganje. Če omogočite to funkcijo, bodo onemogočena vsa okna z obvestili in opozorili ter ustavljena morebitna razporejena opravila.
- **Naročnina bo kmalu potekla/Vaša naročnina poteče danes** – na to težavo opozarja ikona stanja zaščite, v kateri je prikazan klicaj zraven sistemske ure. Ko naročnina poteče, programa ne bo več mogoče posodabljati in ikona stanja zaščite bo postala rdeče barve.

Če s predlaganimi rešitvami ne odpravite težave, kliknite možnost **Pomoč in podpora**, da odprete datoteke pomoči ali začnete iskati v zbirki znanja družbe ESET. Če še vedno potrebujete pomoč, lahko oddate zahtevo za podporo. Tehnična podpora ESET bo na vaša vprašanja hitro odgovorila in vam pomagala najti rešitev.

Pregled računalnika

Pregledovalnik na zahtevo je pomemben del protivirusne rešitve. Z njim lahko pregledujete datoteke in mape v računalniku. S stališča varnosti je zelo pomembno, da preglede računalnika izvajate redno kot del ustaljenih varnostnih ukrepov, ne le takrat, kadar menite, da je prišlo do okužbe. Priporočamo, da izvajate redne poglobljene preglede sistema, s katerimi zaznate viruse, ki jih Sprotna zaščita datotečnega sistema ne zazna, ko so zapisani na disk. To se lahko zgodi, če je sprotna zaščita datotečnega sistema trenutno onemogočena, če je orodje za zaznavanje zastarelo ali če datoteka pri shranjevanju na disk ni zaznana kot virus.



Na voljo sta dve vrsti **Pregled računalnika**. Možnost **Preglejte računalnik** opravi hiter pregled sistema, pri čemer ni treba določiti parametrov pregleda. Možnost **Pregled po meri** (v možnosti Napredni pregledi) vam omogoči, da

izberete med vnaprej določenimi profili pregleda, ki so zasnovani za določene ciljne lokacije, in določene cilje pregleda.

Če želite več informacij o postopku pregleda, glejte razdelek Napredovanje pregleda.

> Izdelek ESET Internet Security privzeto poskuša očistiti ali izbrisati zaznane elemente, najdene med pregledom računalnika. V nekaterih primerih, če ni mogoče izvesti nobenega dejanja, prejmete interaktivno opozorilo in morate izbrati dejanje čiščenja (na primer »izbriši« ali »prezri«). Za spreminjanje ravni čiščenja ali podrobnejše informacije glejte razdelek Čiščenje. Za pregled prejšnjih pregledov glejte razdelek Dnevniške datoteke.

Preglejte računalnik

Možnost »**Preglejte računalnik**« uporabniku omogoča hiter zagon pregleda računalnika in čiščenje okuženih datotek brez njegovega posredovanja. Prednost možnosti »**Preglejte računalnik**« je preprosta uporaba, poleg tega pa ne zahteva podrobne konfiguracije pregleda. Ta pregled omogoča preverjanje vseh datotek na lokalnih pogonih in samodejno čiščenje ali brisanje zaznanih infiltracij. Raven čiščenja je samodejno nastavljena na privzeto vrednost. Če želite podrobnejše informacije o vrstah čiščenja, glejte razdelek Čiščenje.

Funkcijo **pregleda »povleci in spusti«** lahko uporabite za ročni pregled datoteke ali mape tako, da kliknete datoteko ali mapo, kazalec miške premaknete na označeno območje, pri čemer držite gumb miške in ga nato sprostite. S tem se program premakne v ospredje.

V možnosti **Napredni pregledi**so na voljo naslednje možnosti pregleda:

Pregled po meri

Pregled po meri omogoča določitev parametrov pregleda, kot so cilji pregleda in načini. Prednost **pregleda po meri** je, da lahko parametre podrobno konfigurirate. Konfiguracije lahko shranite v uporabniško določene profile pregleda, kar pride prav, če pogosto izvajate preglede z istimi parametri.

Pregled izmenljivih nosilcev podatkov

Podobno kot »**Pregled računalnika**« – hitro zažene pregled izmenljivih nosilcev podatkov (kot so CD/DVD/USB), ki so trenutno povezani z računalnikom. To je lahko uporabno, ko priključite pogon USB v računalnik ter želite pregledati njegovo vsebino in preveriti, ali je v njem zlonamerna programska oprema ali druge morebitne grožnje.

To vrsto pregleda lahko zaženete tudi tako, da kliknete **Pregled po meri** in v spustnem meniju **Cilji pregleda** izberete možnost **Izmenljivi nosilci podatkov** ter kliknete **Preglej**.

Ponovi zadnji pregled

Omogoča vam hiter zagon prejšnjega pregleda pri enakih nastavitvah.

V spustnem meniju **Dejanje po pregledu** lahko nastavite dejanje, ki bo samodejno izvedeno po končanem pregledu:

- **Ne naredi ničesar** – po končanem pregledu se ne izvede nobeno dejanje.
- **Zaustavitev sistema** – računalnik se po končanem pregledu izklopi.

• **Ponovni zagon po potrebi** – računalnik se znova zažene le, če je to potrebno za izvedbo čiščenja zaznanih groženj.

• **Vnovičen zagon** – po končanem pregledu se vsi odprti programi zaprejo, računalnik pa se znova zažene.

• **Prisilen ponovni zagon po potrebi** – računalnik se znova zažene le, če je to potrebno za izvedbo čiščenja zaznanih groženj.

• **Prisilen vnovičen zagon** – Prisilno zapre vse odprte programe, ne da bi čakal na interakcijo uporabnika, in po končanem pregledovanju znova zažene računalnik.

• **Stanje pripravljenosti** – vaša seja se shrani, računalnik pa preklopi v stanje nizke porabe, iz katerega lahko hitro nadaljujete z delom.

• **Stanje mirovanja** – vse, kar se izvaja v pomnilniku RAM, se premakne v posebno datoteko na trdem disku. Računalnik se zaustavi, vendar ob naslednjem zagonu obnovi svoje prejšnje stanje.

i Dejanji **Stanje pripravljenosti** ali **Stanje mirovanja** sta na voljo glede na nastavitve napajanja in stanja pripravljenosti operacijskega sistema ali lastnosti vašega računalnika/prenosnika. Upoštevajte, da računalnik v stanju pripravljenosti še deluje. V njem se še vedno izvajajo osnovne funkcije, poleg tega se porablja energija akumulatorja, če se računalnik napaja prek akumulatorja. Če želite podaljšati čas delovanja akumulatorja, ko na primer zapustite pisarno, priporočamo, da računalnik preklopite v stanje mirovanja.

Izbrano dejanje se bo začelo, ko bodo vsi pregledi v izvajanju končani. Ko izberete možnost **Zaustavitev** ali **Vnovični zagon**, bo v potrditvenem pogovornem oknu prikazano 30-sekundno odštevanje (kliknite možnost **Prekliči**, da deaktivirate zahtevano dejanje).

i Priporočamo, da pregled računalnika zaženete vsaj enkrat na mesec. Pregledovanje lahko konfigurirate kot načrtovano opravilo v možnosti **Orodja** > **Razporejevalnik**. Kako razporediti tedensko pregledovanje računalnika

Zaganjalnik pregleda po meri

Če želite pregledati delovni pomnilnik, omrežje ali samo določene dele diska, ne pa celotnega, lahko uporabite pregled po meri. Za ta postopek kliknite **Napredni pregledi** > **Pregled po meri** in izberite želene cilje v (drevesni) strukturi mape.

V spustnem meniju **Profil** lahko izberete profil, ki ga želite uporabiti za pregled posameznih ciljev. Privzeti profil je **Pametni pregled**. Na voljo so trije dodatni predhodno določeni profila pregleda, in sicer **Poglobljen pregled**, **Pregled priročnega menija** in **Pregled računalnika**. Ta profila pregleda uporabljata različne parametre orodja ThreatSense. Možnosti, ki so na voljo, so opisane v razdelku Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** > **Pregled na zahtevo** > ThreatSense.

Struktura mape (drevesa) vsebuje tudi določene cilje pregleda.

• **Delovni pomnilnik** – pregleda vse procese in podatke, ki jih trenutno uporablja delovni pomnilnik.

• **Zagonski sektorji/UEFI** – pregleda zagonske sektorje in UEFI za prisotnost zlonamerne programske opreme. Preberite več o pregledovalniku za UEFI v slovarčku.

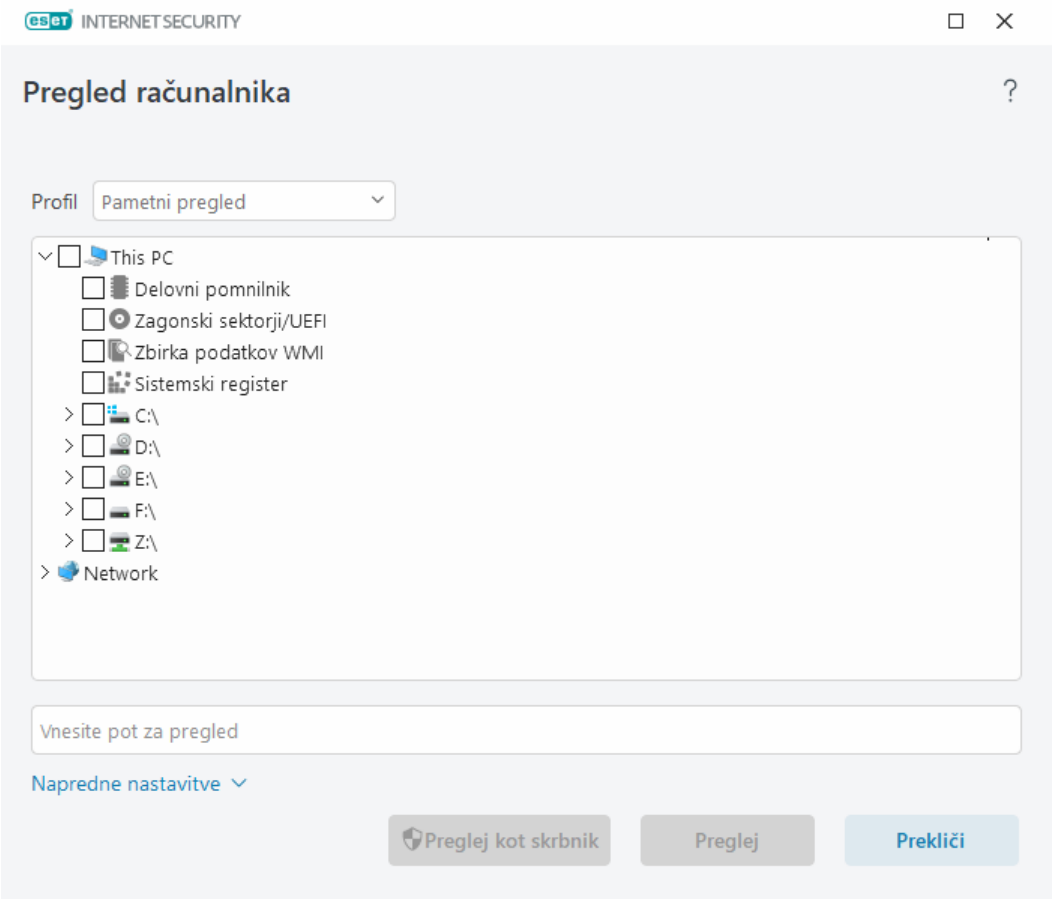
• **Zbirka podatkov WMI** – pregleda celotno zbirko podatkov Windows Management Instrumentation (WMI), vse imenske prostore, vse primerke razredov in vse lastnosti. Išče sklice na okuženo datoteko ali zlonamerno programsko opremo, vdelano kot podatke.

• **Sistemski register** – pregleda celoten sistemski register, vse ključe in podključe. Išče sklice na okuženo datoteko ali zlonamerno programsko opremo, vdelano kot podatke. Pri čiščenju zaznanih elementov ostane sklic v registru, da se zagotovi, da ne bodo izgubljeni nobeni pomembni podatki.

Če se želite hitro pomakniti na cilj pregleda (datoteka ali mapa), vnesite njegovo pot v besedilno polje pod drevesno strukturo. Pot razlikuje med malimi in veliki črkami. Če želite cilj vključiti v pregled, izberite njegovo potrditveno polje v drevesni strukturi.

Kako razporediti tedensko pregledovanje računalnika

Če želite razporediti redno opravilo, preberite poglavje Kako razporediti tedensko pregledovanje računalnika.



Parametre za čiščenje za pregled lahko konfigurirate v razdelku Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** > **Pregled na zahtevo** > **ThreatSense** > **Čiščenje**. Za pregled brez čiščenja kliknite **Napredne nastavitve** in izberite **Preglej brez čiščenja**. Zgodovina pregledov je shranjena v dnevnik pregledovanja.

Ko je izbrana možnost **Prezri izključitve**, bodo datoteke s priponami, ki so bile predhodno izključene, brez izjeme pregledane.

Kliknite **Preglej**, če želite izvesti pregled z nastavljenimi parametri po meri.

Možnost **Preglej kot skrbnik** omogoča izvajanje pregleda s skrbniškim računom. To možnost uporabite, če

trenutni uporabnik nima pravic za dostop do datotek, ki jih želite pregledati. Ta gumb ni na voljo, če trenutni uporabnik ne more priklicati operacij UAC kot skrbnik.

Po končanem pregledu si dnevnik pregleda računalnika si lahko ogledate tako, da kliknete Pokaži dnevnik.

Napredovanje pregleda

V oknu napredovanja pregleda so prikazani trenutno stanje pregleda in podatki o številu datotek, v katerih je bila odkrita zlonamerna koda.

Normalno je, da nekaterih datotek, kot so datoteke, zaščitene z geslom, ali datoteke, ki jih izključno uporablja sistem (običajno so to datoteke *pagefile.sys* in nekatere dnevniške datoteke), ni mogoče pregledati. Več podrobnosti najdete v našem članku v zbirki znanja družb.

Kako razporediti tedensko pregledovanje računalnika

Če želite razporediti redno opravilo, preberite poglavje Kako razporediti tedensko pregledovanje računalnika.

Napredovanje pregleda – vrstica napredka prikazuje stanje tekočih pregledov.

Cilj – ime predmeta, ki se trenutno pregleduje in njegovo mesto.

Zaznani so bili elementi – prikaže skupno število pregledanih datotek, najdenih groženj in groženj, ki so bile očiščene med pregledovanjem.

Kliknite možnost Več informacij, če želite prikazati naslednje informacije:

- **Uporabnik** – ime uporabniškega računa, ki je zagnal pregled.
- **Pregledani predmeti** – število že pregledanih predmetov.
- **Trajanje** – čas, ki je pretekel.

Ikona za začasno ustavitev – začasno ustavi pregled.

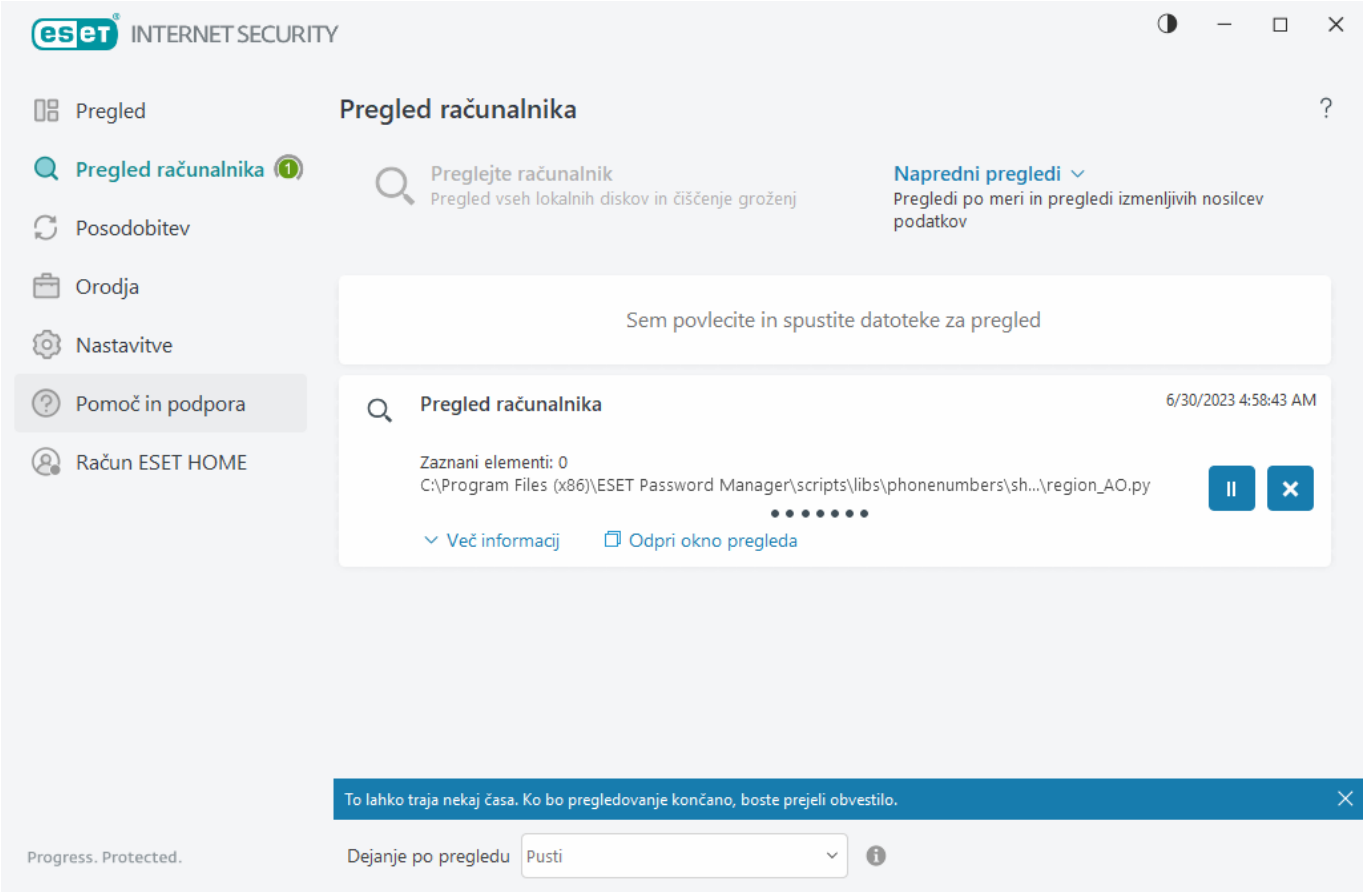
Ikona za nadaljevanje – to možnost lahko vidite, ko je napredovanje pregleda začasno ustavljeno. Kliknite ikono, da nadaljujete s pregledom.

Ikona za zaustavitev – konča pregled.

Kliknite možnost **Odpri okno pregleda**, da odprete Dnevnik pregleda računalnika z več podrobnosti o pregledu.

Preglej dnevnik pregleda – če je možnost omogočena, se ob dodajanju novih vnosov dnevnik pregleda samodejno premakne navzdol, tako da lahko vidite najnovejše vnose.

Kliknite lupo ali puščico, da se prikažejo podrobnosti o trenutno zagnanem pregledu. Zaženete lahko dodatni vzporedni pregled in sicer tako, da kliknete možnost **Preglejte računalnik** ali odprete razdelek **Napredni pregledi** > **Pregled po meri**.



V spustnem meniju **Dejanje po pregledu** lahko nastavite dejanje, ki bo samodejno izvedeno po končanem pregledu:

- **Ne naredi ničesar** – po končanem pregledu se ne izvede nobeno dejanje.
- **Zaustavitev sistema** – računalnik se po končanem pregledu izklopi.
- **Ponovni zagon po potrebi** – računalnik se znova zažene le, če je to potrebno za izvedbo čiščenja zaznanih groženj.
- **Vnovičen zagon** – po končanem pregledu se vsi odprti programi zaprejo, računalnik pa se znova zažene.
- **Prisilen ponovni zagon po potrebi** – računalnik se znova zažene le, če je to potrebno za izvedbo čiščenja zaznanih groženj.
- **Prisilen vnovičen zagon** – Prisilno zapre vse odprte programe, ne da bi čakal na interakcijo uporabnika, in po končanem pregledovanju znova zažene računalnik.
- **Stanje pripravljenosti** – vaša seja se shrani, računalnik pa preklopi v stanje nizke porabe, iz katerega lahko hitro nadaljujete z delom.
- **Stanje mirovanja** – vse, kar se izvaja v pomnilniku RAM, se premakne v posebno datoteko na trdem disku. Računalnik se zaustavi, vendar ob naslednjem zagonu obnovi svoje prejšnje stanje.

Dejanji **Stanje pripravljenosti** ali **Stanje mirovanja** sta na voljo glede na nastavitve napajanja in stanja pripravljenosti operacijskega sistema ali lastnosti vašega računalnika/prenosnika. Upoštevajte, da računalnik v stanju pripravljenosti še deluje. V njem se še vedno izvajajo osnovne funkcije, poleg tega se porablja energija akumulatorja, če se računalnik napaja prek akumulatorja. Če želite podaljšati čas delovanja akumulatorja, ko na primer zapustite pisarno, priporočamo, da računalnik preklopite v stanje mirovanja.

Izbrano dejanje se bo začelo, ko bodo vsi pregledi v izvajanju končani. Ko izberete možnost **Zaustavitev** ali **Vnovični zagon**, bo v potrditvenem pogovornem oknu prikazano 30-sekundno odštevanje (kliknite možnost **Prekliči**, da deaktivirate zahtevano dejanje).

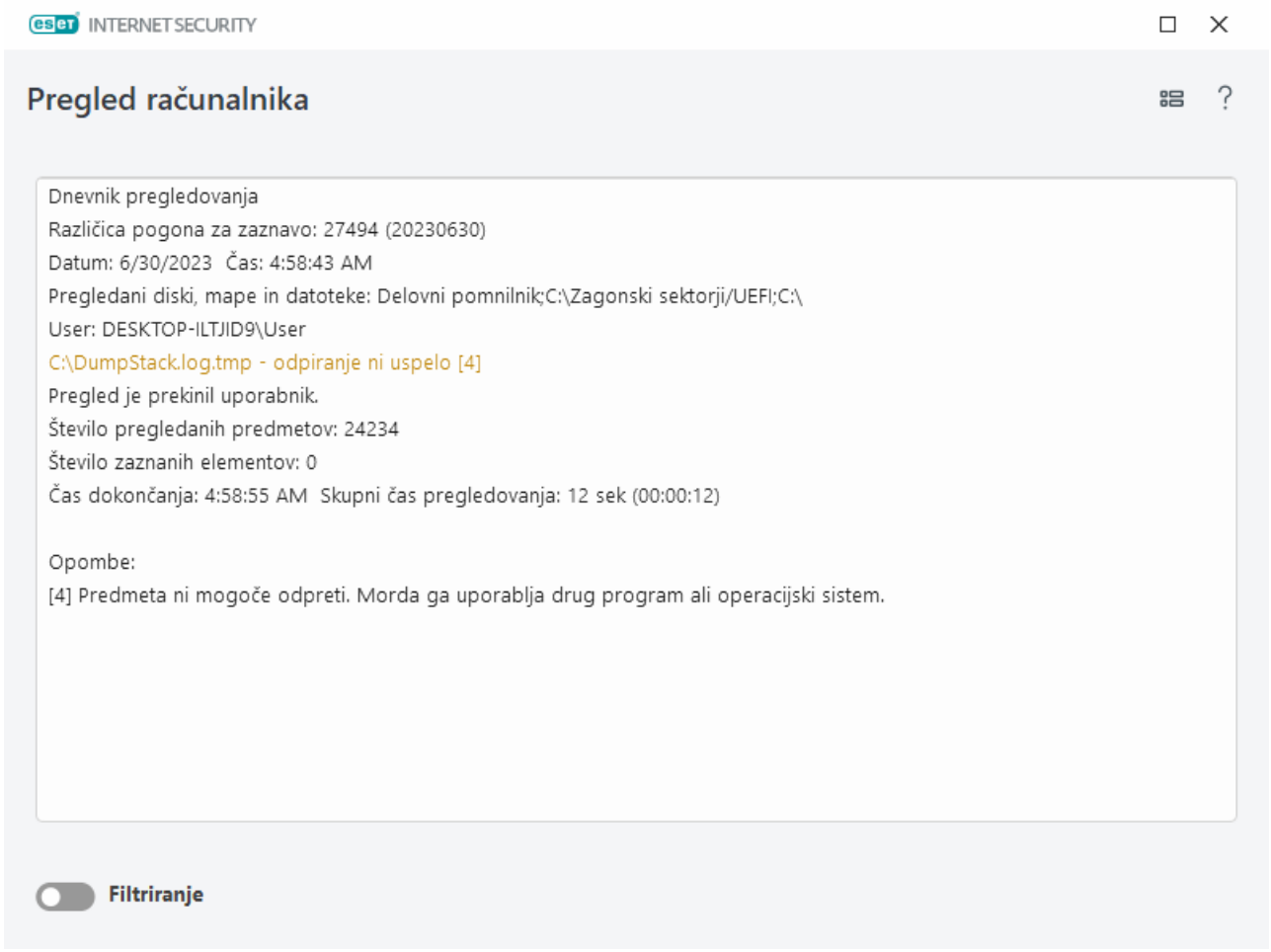
Dnevnik pregleda računalnika

Podrobne informacije, povezane z določenim pregledom, si lahko ogledate v dnevniških datotekah. Dnevnik pregledovanja vsebuje naslednje informacije:

- Različica orodja za zaznavanje
- Datum in ura začetka
- Seznam pregledanih diskov, map in datotek
- Ime načrtovanega pregleda (samo načrtovani pregled)
- Uporabnik, ki je zagnal pregled.
- Stanje pregleda
- Število pregledanih predmetov
- Število zaznanih elementov
- Čas dokončanja
- Skupni čas pregledovanja

Nov začetek razporejenega opravila pregleda v računalniku se preskoči, če se isto razporejeno opravilo, ki je bilo izvedeno prej, še vedno izvaja. Preskočeno razporejeno opravilo pregleda bo ustvarilo dnevnik pregleda računalnika z 0 pregledanimi predmeti in stanje **Pregled ni bil zagnan, ker se je še vedno izvajal prejšnji pregled.**.

Če si želite ogledati prejšnje dnevnike pregledov, v glavnem oknu programa izberite **Orodja** > **Dnevniške datoteke**. V spustnem meniju izberite **Pregled računalnika** in dvokliknite želeni zapis.



Če želite izvedeti več o zapisih »odpiranje ni uspelo«, »napaka pri odpiranju« in/ali »arhiv je poškodovan«, si oglejte Članek iz zbirke znanja družbe ESET.

Za odpiranje okna Filtriranje dnevnika, kliknite ikono gumba za preklop **Filtriranje**, v katerem lahko zožite iskanje z merili po meri. Za prikaz priročnega menija z desno tipko miške kliknite posamezen vnos v dnevniku:

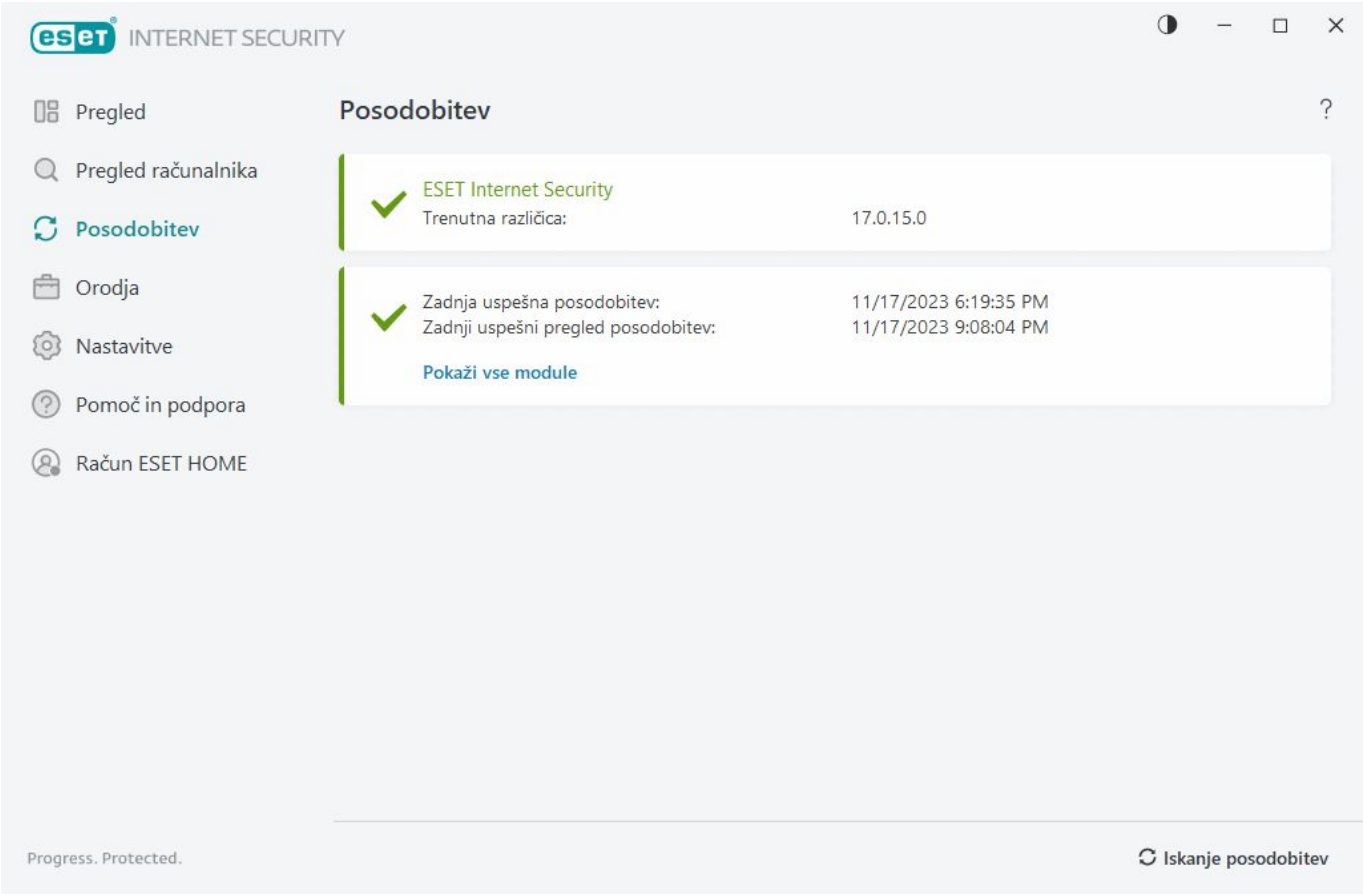
Dejanje	Uporaba
Filtriraj enake zapise	Aktivira filtriranje dnevnika. V tem dnevniku bodo prikazani samo zapisi enake vrste kot je izbrani zapis.
Filter	Ta možnost odpre okno Filtriranje dnevnika in omogoča opredelitev meril za posamezne vnose v dnevniku. Bližnjica: `Ctrl+Shift+F`
Omogoči filter	Aktivira nastavitve filtriranja. Če filtriranje aktivirate prvič, morate določiti nastavitve. Odpre se okno Filtriranje dnevnika.
Onemogoči filter	Izklopi filtriranje (enako kot stikalo na dnu).
Kopiraj	Kopira označene zapise v odložišče. Bližnjica: `Ctrl+C`
Kopiraj vse	Kopira vse zapise v oknu.
Izvozi	Izvozi označene zapise v datoteko XML.
Izvozi vse	Ta možnost izvozi vse zapise v oknu v datoteko XML.
Opis zaznanega elementa	Odpre enciklopedijo groženj družbe ESET, v kateri najdete podrobne informacije o nevarnostih in simptomih, povezanih z različnimi vrstami poudarjene infiltracije.

Posodabljanje

Z rednim posodabljanjem programa ESET Internet Security najbolje zagotovite največjo raven zaščite v računalniku. Modul za posodobitev zagotavlja, da so tako programski moduli kot sistemske komponente vedno posodobljeni.

Če v glavnem oknu programa kliknete **Posodobitev**, lahko poiščete trenutno stanje posodobitve, vključno z datumom in časom zadnje uspešne posodobitve in v primeru, da potrebujete posodobitev.

Poleg samodejnih posodobitev lahko kliknete možnost **Preveri, ali so na voljo posodobitve**, da sprožite ročno posodobitev. Redno posodabljanje modulov in komponent programov je pomemben del vzdrževanja celovite zaščite pred zlonamerno kodo. Bodite pozorni na konfiguracijo in delovanje modulov izdelka. Izdelek morate aktivirati z aktivacijsko kodo, da boste lahko prejemali posodobitve. Če tega niste storili med namestitvijo, boste morali aktivirati ESET Internet Security za dostop do strežnikov za posodobitev ESET. Aktivacijsko kodo vam je po nakupu izdelka ESET Internet Security po e-pošti posredoval ESET.



Trenutna različica – prikaz številke trenutne nameščene različice.

Zadnja uspešna posodobitev – prikaz datuma zadnje uspešne posodobitve. Če nedavni datum ni prikazan, morda nimate najnovejših modulov programov.

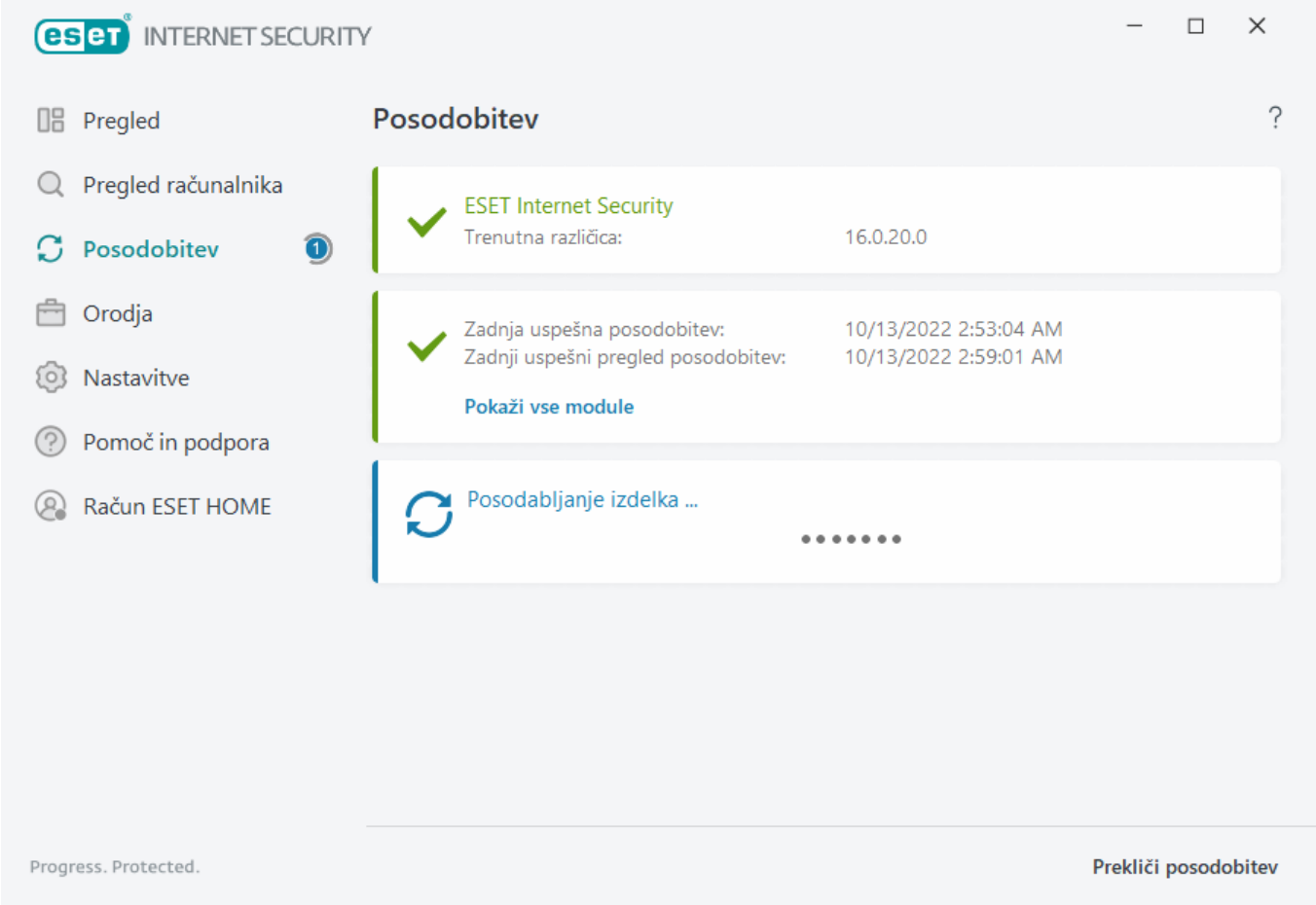
Zadnji uspešen pregled posodobitev – datum zadnjega uspešnega pregleda posodobitev.

Pokaži vse module – prikaže sezname nameščenih programskih modulov.

Če želite poiskati najnovejšo različico programa ESET Internet Security, ki je na voljo, kliknite **Iskanje posodobitev**.

Proces posodabljanja

Prenos se začne, ko kliknete **Iskanje posodobitev**. Prikazana bosta vrstica napredka prenašanja in preostali čas do dokončanja tega procesa. Če želite prekiniti posodabljanje, kliknite **Prekliči posodobitev**.



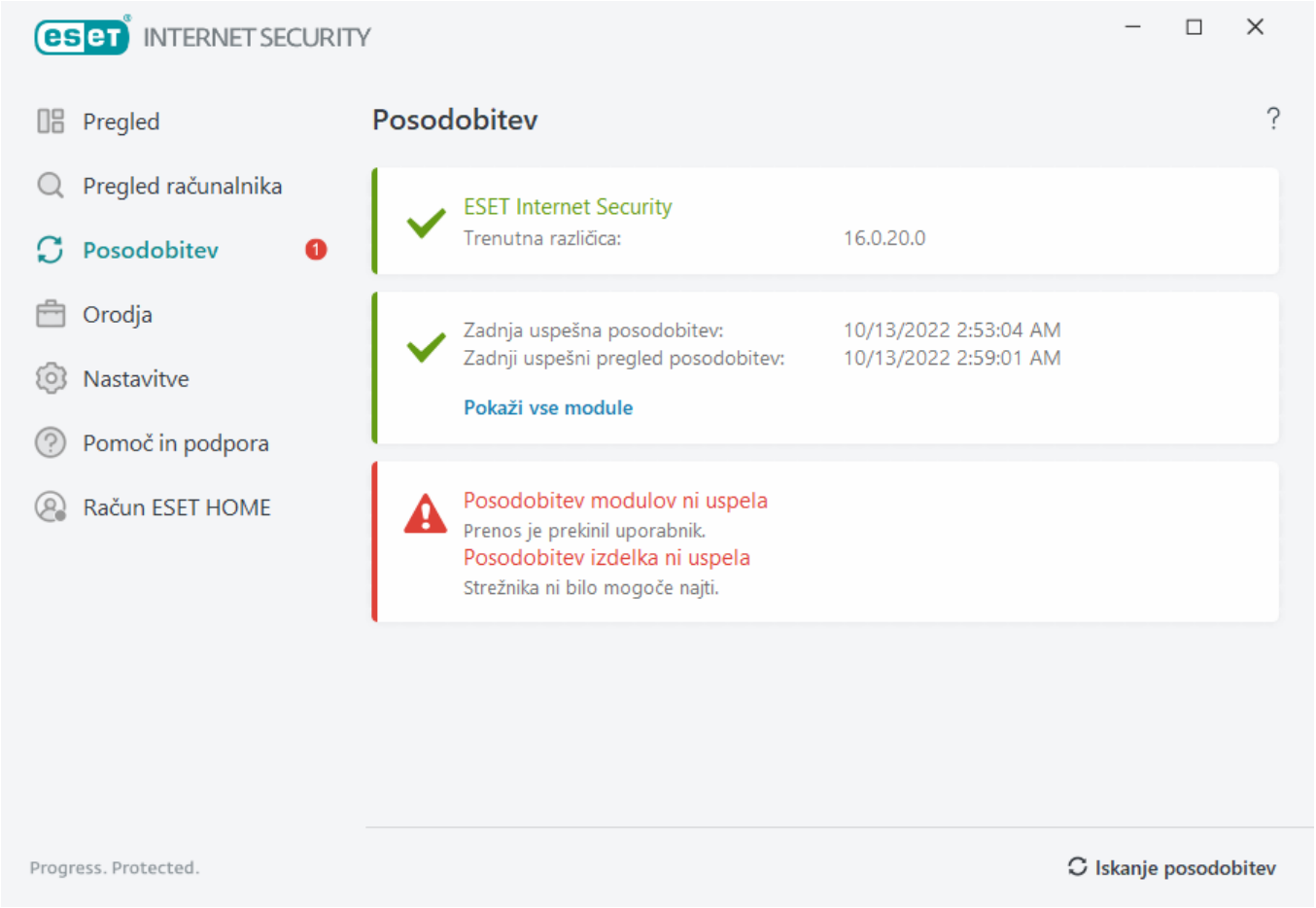
V običajnih okoliščinah lahko vidite zeleno kljukico v oknu **Posodobi**, ki označuje, da je program posodobljen na najnovejšo različico. Če zelene kljukice ne vidite, je program zastarel in bolj dovzeten za okužbe. Čim prej posodobite module programa.

Posodobitev ni uspela

Če prejmete sporočilo o neuspešni posodobitvi modulov, je razlog lahko:

1. **Neveljavna naročnina** – naročnina, uporabljena za aktivacijo, ni veljavna ali je potekla. V glavnem oknu programa kliknite možnost **Pomoč in podpora** > **Spremeni naročnino** in aktivirajte izdelek.

2. **Pri prenosu datotek za posodobitev je prišlo do napake** – vzrok napake so morda nepravilne nastavitve internetne povezave. Priporočamo vam, da preverite povezavo z internetom (tako da s spletnim brskalnikom odprete poljubno spletno mesto). Če se spletno mesto ne odpre, se verjetno ni vzpostavila internetna povezava ali pa je prišlo do težav, povezanih s povezavo z računalnikom. Pri svojem ponudniku internetnih storitev preverite, ali je internetna povezava aktivna.



Po uspešni posodobitvi programa ESET Internet Security na novejšo različico morate znova zagnati računalnik, da se vsi moduli programa ustrezno posodobijo. Po rednih posodobitvah modulov ni treba znova zagnati računalnika.

Za več informacij glejte Odpravljanje težav za sporočilo »Posodobitev modulov ni uspela«.

Pogovorno okno – zahtevan je vnovični zagon

Po posodobitvi programa ESET Internet Security na novo različico je zahtevan vnovični zagon računalnika. Nove različice programa ESET Internet Security so izdane za uvajanje izboljšav ali odpravljanje težav, ki jih samodejne posodobitve modulov programa ne morejo razrešiti.

Novo različico programa ESET Internet Security lahko namestite samodejno na podlagi nastavitev posodobitve programa ali ročno s prenosom in namestitvijo novejše različice prek starejše.

Če želite znova zagnati računalnik, kliknite možnost **Znova zaženi zdaj**. Če nameravate računalnik znova zagnati pozneje, kliknite možnost **Opomni me pozneje**. Pozneje lahko računalnik znova zaženete ročno v razdelku **Pregled**« v glavnem oknu programa.

Ustvarjanje opravil posodabljanja

Posodobitve lahko sprožite ročno tako, da v primarnem oknu, ki se prikaže, ko v glavnem meniju kliknete **Posodobi**, kliknete še **Iskanje posodobitev**.

Posodobitve lahko zaženete kot razporejena opravila. Če želite konfigurirati razporejeno opravilo, kliknite **Orodja** > **Razporejevalnik**. V programu ESET Internet Security so privzeto aktivirana naslednja opravila posodabljanja:

- **Redno samodejno posodabljanje**
- **Samodejna posodobitev po prijavi uporabnika**

Vsako opravilo posodabljanja lahko spremenite tako, da ustreza vašim potrebam. Poleg privzetih opravil posodabljanja lahko ustvarite nova opravila posodabljanja z uporabniško določeno konfiguracijo. Če želite več podrobnosti o ustvarjanju in konfiguriranju opravil posodabljanja, glejte poglavje Razporejevalnik.

Orodja

V meniju **Orodja** so funkcije, ki ponujajo dodatno varnost in pomoč pri poenostavitvi skrbništva za ESET Internet Security. Na voljo so naslednja orodja:

 Dnevniške datoteke

 Izvajajoči se procesi (če je omogočeno orodje ESET LiveGrid® v programu ESET Internet Security)

 Varnostno poročilo

 Omrežne povezave (če je požarni zid omogočen v programu ESET Internet Security)

 ESET SysInspector

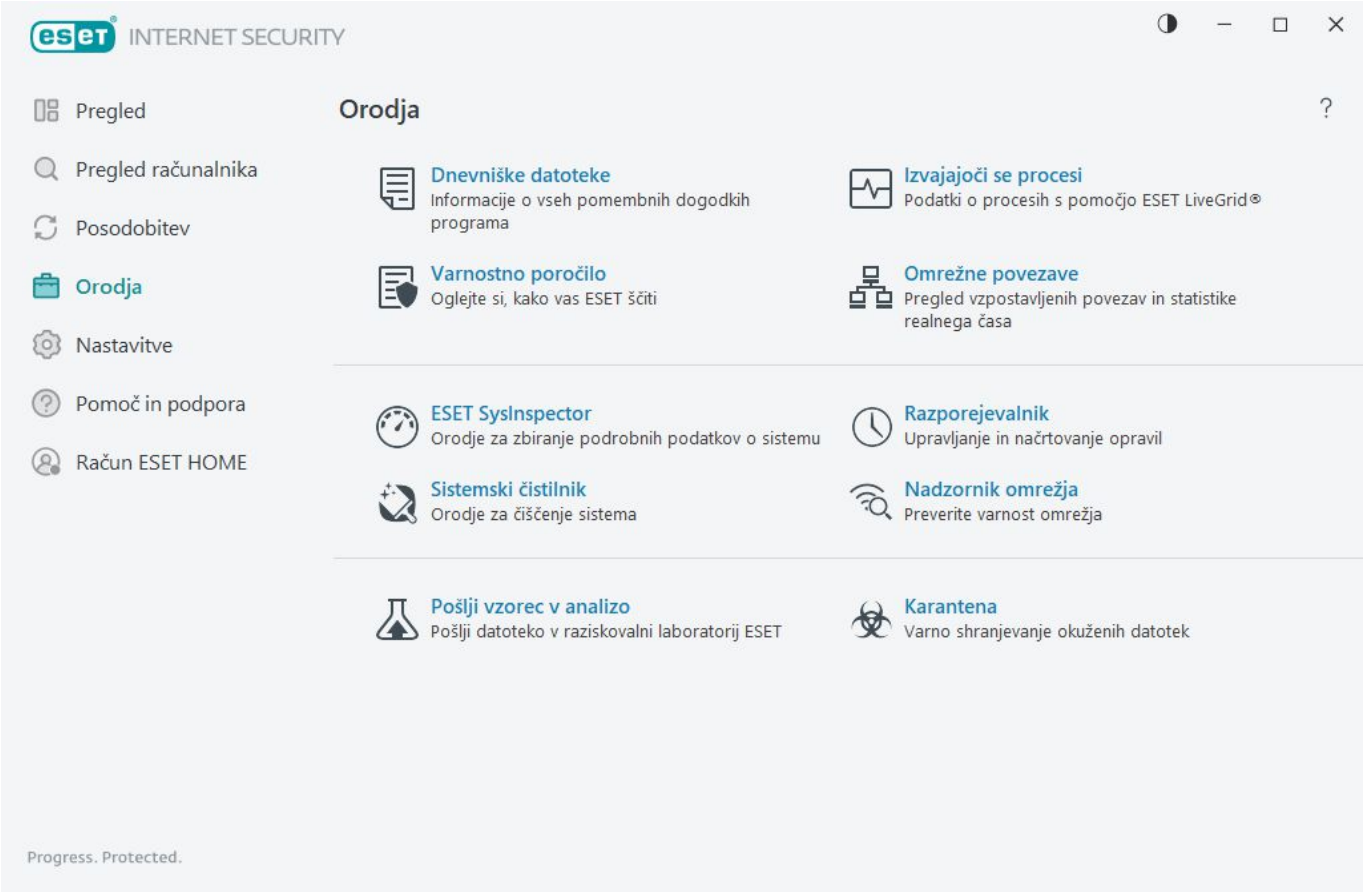
 Razporejevalnik

 Sistemski čistilnik

 Nadzornik omrežja

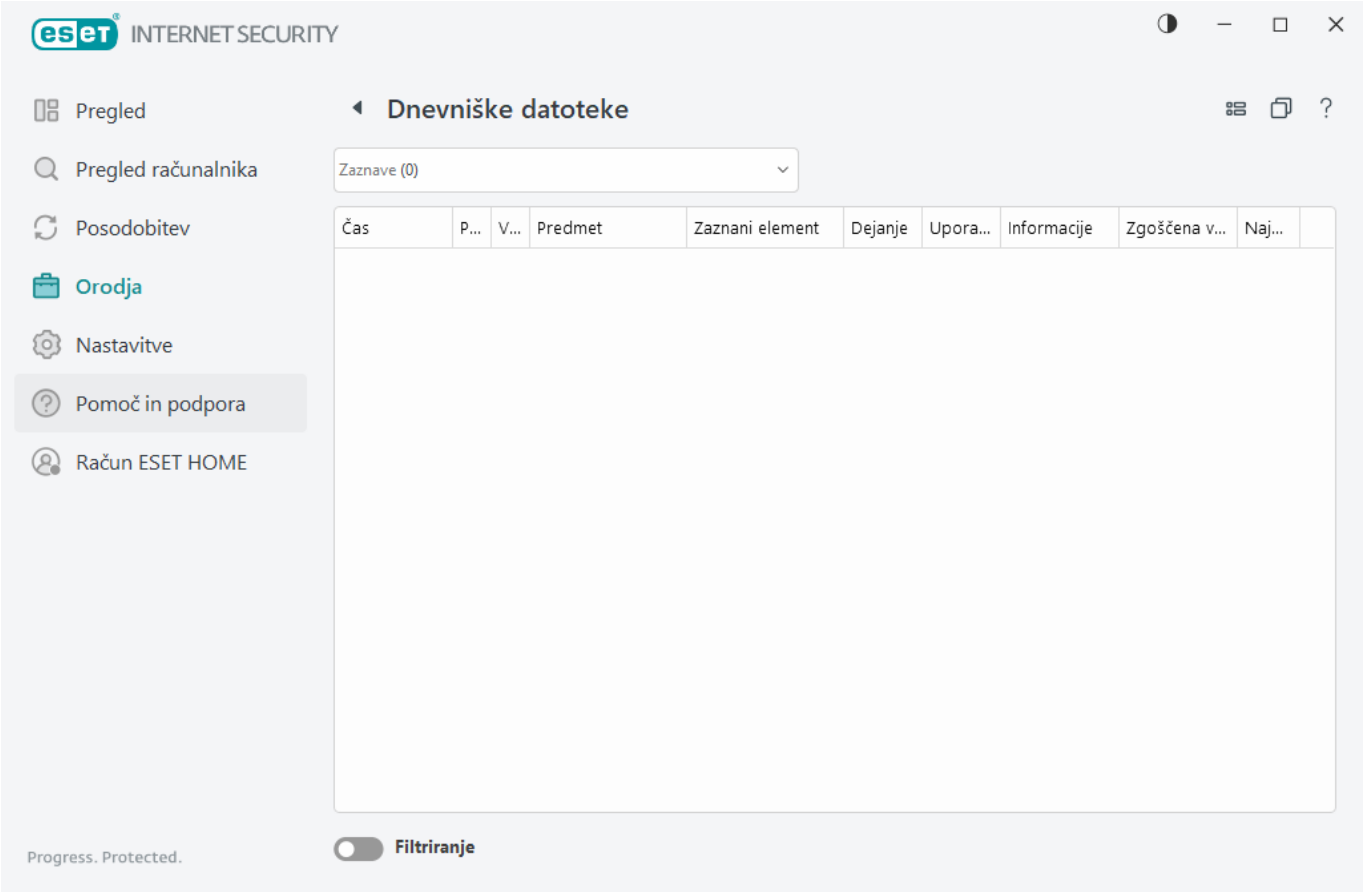
 Pošlji vzorec v analizo (razpoložljivost te možnosti je odvisna od konfiguracije za ESET LiveGrid®).

 Karantena



Dnevniške datoteke

V dnevniških datotekah so podatki o pomembnih dogodkih programa, ki so se zgodili, in pregled zaznanih groženj. Pisanje dnevnika je pomemben del analize sistema, zaznavanja groženj in odpravljanja težav. Zapisovanje v dnevnik se aktivno izvaja v ozadju brez interakcije uporabnika. Podatki so zabeleženi glede na trenutne nastavitve ravni podrobnosti pri pisanju v dnevnik. Besedilna sporočila in dnevnike si lahko ogledate neposredno iz okolja programa ESET Internet Security, pa tudi iz arhivskih dnevnikov.



Dostop do dnevniških datotek je mogoč iz glavnega okna programa, tako da kliknete **Orodja** in nato še **Dnevniške datoteke**. Iz spustnega menija Dnevnik izberite želeno vrsto dnevnika.

- **Zaznave** – ta dnevnik zagotavlja podrobne informacije o zaznavah in infiltracijah, ki jih je zaznal ESET Internet Security. Podatki vključujejo čas zaznave, vrsto pregledovalnika, vrsto predmeta, mesto predmeta, ime zaznave, izvedeno dejanje, ime uporabnika, ki je bil prijavljen v času, ko je bila zaznana infiltracija, zgoščeno vrednost in prvo pojavitev. Neočiščene infiltracije so vedno navedene z rdečimi črkami na svetlo rdečem ozadju. Očiščene infiltracije so označene z rumenimi črkami na belem ozadju. Neočiščeni morebitno nevarni programi so navedeni z rumenimi črkami na belem ozadju.

- **Dogodki** – vsi pomembni postopki, ki jih opravi ESET Internet Security, se zabeležijo v dnevnik dogodkov. V dnevniku dogodkov so podatki o dogodkih in napakah, do katerih je prišlo v programu. Skrbniki sistema in uporabniki si z njim pomagajo pri reševanju težav. Pogosto lahko s podatki v tem dnevniku poiščete rešitev za težavo, do katere pride v programu.

- **Pregled računalnika** – v tem oknu so prikazani rezultati vseh prejšnjih pregledov. Vsaka vrstica ustreza enemu računalniškemu pregledu. Če si želite ogledati podrobnosti izbranega pregleda, dvokliknite kateri koli vnos.

- **HIPS** – vsebuje zapise določenih pravil HIPS, ki so označena za zapisovanje. V tem protokolu je prikazan program, ki je sprožil postopek, rezultat (ali je pravilo dovoljeno ali prepovedano) in ime pravila.

- **Zaščita brskalnika** – vsebuje zapise datotek, ki niso preverjene ali vredne zaupanja, naložene v brskalniku.

- **Zaščita omrežjal** – v dnevniku zaščite omrežja so prikazani vsi oddaljeni napadi, ki jih zaznajo požarni zid ter funkciji zaščite pred napadi iz omrežja (IDS) in preprečevanja napadov iz omrežja (Botnet). Tukaj najdete informacije o vseh napadih v računalniku. V stolpcu Dogodek so navedeni vsi znani napadi. V stolpcu Vir so podatki o napadalcu. V stolpcu Protokol je naveden protokol komunikacije, ki je bil uporabljen za napad.

Analiza zaščite omrežja vam omogoča pravočasno zaznavo poskusov infiltracije v računalnik, s čimer lahko preprečite nepooblaščen dostop do računalnika. Za več podrobnosti o omrežnih napadih glejte poglavje IDS in napredne možnosti.

- **Filtrirana spletna mesta** – Ta seznam je uporaben, če si želite ogledati seznam spletnih mest, ki jih je blokirala zaščita spletnega dostopa ali starševski nadzor. V vsakem dnevniku je zapisan čas, naslov URL, uporabnik in program, ki je vzpostavil povezavo z določenim spletnim mestom.

- **Zaščita pred neželeno pošto v e-poštnem odjemalcu** – vsebuje zapise o e–poštnih sporočilih, ki so bila označena kot neželena pošta.

- **Starševski nadzor** – prikaže spletne strani, ki jih je blokiral ali dovolil starševski nadzor. V stolpcih Vrsta ujemanja in Vrednosti ujemanja je naveden način uporabe pravil za filtriranje.

- **Nadzor naprav** – vsebuje zapise izmenljivih nosilcev podatkov ali naprav, priključenih v računalnik. V dnevniško datoteko bodo zapisane le naprave z ustreznimi pravili za nadzor naprav. Če se pravilo ne ujema s priključeno napravo, vnos v dnevnik za priključeno napravo ne bo ustvarjen. Lahko si ogledate tudi podrobnosti, kot so vrsta naprave, serijska številka, ime dobavitelja in velikost nosilcev podatkov (če je na voljo).

- **Zaščita spletne kamere** – vsebuje zapise o programih, ki jih je funkcija zaščite spletne kamere blokirala.

Izberite vsebino katerega koli dnevnika in pritisnite **CTRL + C** za kopiranje v odložišče. Za izbiro več vnosov zadržite **CTRL** ali **SHIFT**.

Kliknite  **Filtriranje**, če želite odpreti okno Filtriranje dnevnika, v katerem lahko določite merila filtriranja.

Z desno tipko miške kliknite določen zapis, da odprete priročni meni. V priročnem meniju so na voljo te možnosti:

- **Pokaži** – pokaže podrobne podatke o izbranem dnevniku v novem oknu.

- **Filtriraj enake zapise** – ko aktivirate ta filter, boste videli le zapise iste vrste (diagnostika, opozorila itd.).

- **Filtriraj** – ko kliknete to možnost, lahko v oknu Filtriranje dnevnika določite merila filtriranja za posamezne vnose v dnevniku.

- **Omogoči filter** – aktivira nastavitve filtra.

- **Onemogoči filter** – počisti vse nastavitve filtra (kot je opisano zgoraj).

- **Kopiraj/Kopiraj vse** – kopira informacije o vseh izbranih zapisih.

- **Kopiraj celico** – kopira vsebino celice, ki ste jo kliknili z desno tipko miške.

- **Izbriši/Izbriši vse** – izbriše izbrane zapise ali vse prikazane zapise. Za to dejanje potrebujete skrbniške pravice.

- **Izvozi/Izvozi vse** – izvozi informacije o izbranih zapisih ali vseh zapisih v obliki zapisa XML.

- **Najdi/Najdi naslednje/Najdi prejšnje** ko kliknete to možnost, lahko v oknu Filtriranje dnevnika določite merila filtriranja, da poudarite določen vnos.

- **Opis zaznanega elementa** – odpre enciklopedijo groženj družbe ESET, v kateri najdete podrobne

informacije o nevarnostih in simptomih, povezanih z različnimi vrstami zabeležene infiltracije.

• **Ustvari izključitev** – ustvari novo izključitev zaznav s čarovnikom (ni na voljo za zaznave zlonamerne programske opreme).

• **Dodaj na seznam dovoljenih datotek za zaščito brskalnika**– odpre okno seznama dovoljenih datotek za zaščito brskalnika in doda element na seznam.

Filtriranje dnevnika

Kliknite **Filtriranje** v možnosti **Orodja** > **Dnevniške datoteke** in določite merila filtriranja.

S funkcijo filtriranja dnevnika lahko poiščete želene podatke, če je npr. na voljo preveč zapisov. Omogoča, da zožite nabor zapisov, ko npr. iščete določeno vrsto dogodka, stanje ali časovno obdobje. Zapise dnevnika lahko filtrirate z določanjem različnih možnosti iskanja, da se v oknu z dnevniškimi datotekami prikažejo samo ustrezni zapisi (v skladu z določenimi možnostmi iskanja).

Vnesite ključno besedo, ki jo želite poiskati, v polje **Najdi besedilo**. V spustnem meniju **Išči v stolpcih** natančneje določite možnosti iskanja. V spustnem meniju **Vrste dnevniških zapisov** izberite enega ali več zapisov. Določite **Časovno obdobje**, za katerega želite prikaz rezultatov. Uporabite lahko tudi nadaljnje možnosti iskanja, npr. **Najdi samo cele besede** ali **Razlikovanje med velikimi/malimi črkami**.

Najdi besedilo

Vnesite niz (besedo ali del besede). Prikazani bodo zapisi, ki vsebujejo ta niz. Drugi zapisi ne bodo vključeni.

Išči v stolpcih

Izberite stolpce, v katerih naj poteka iskanje. Izberete lahko enega ali več stolpcev, ki se nato uporabijo za iskanje.

Vrste zapisov

Izberite eno ali več vrst zapisov dnevnika iz spustnega menija:

• **Diagnostika** – zabeleži podatke, ki so potrebni za natančno prilagajanje programa in vseh zgornjih zapisov.

• **Informativno** – zabeleži informativna sporočila, vključno s sporočili o uspešnem posodabljanju in vsemi zgornjimi zapisi.

• **Opozorila** – zabeleži kritične napake in opozorilna sporočila o grožnjah.

• **Napake** – zabeleži napake, kot je »Napaka pri prenosu datoteke«, in kritične napake.

• **Kritično** – v dnevnik zabeleži le kritične napake (napake pri zagonu protivirusne zaščite

Časovno obdobje

določite časovno obdobje, iz katerega želite prikazati rezultate:

• **Ni navedeno** (privzeto) – iskanje ne poteka znotraj določenega časovnega obdobja, ampak po celotnem dnevniku.

• **Prejšnji dan**

• **Prejšnji teden**

• **Prejšnji mesec**

• **Časovno obdobje** – določite lahko točno obdobje (Od:/Do:), s čimer filtrirate zapise samo za določeno časovno obdobje.

Najdi samo cele besede

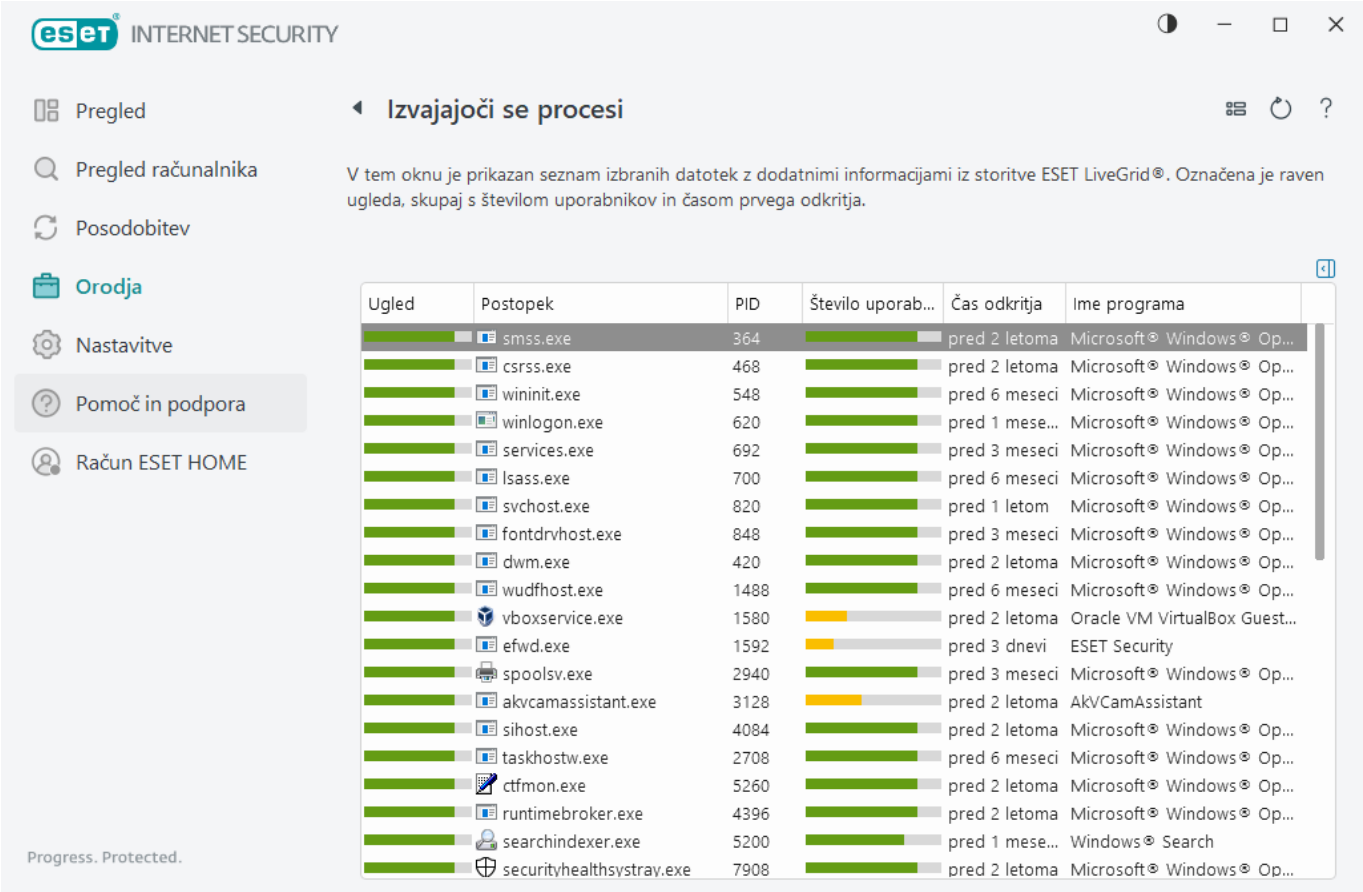
Potrdite to polje, če želite poiskati določene cele besede za natančnejše rezultate.

Razlikovanje med velikimi/malimi črkami

To možnost omogočite, če želite pri filtriranju uporabiti male ali velike črke. Ko konfigurirate možnosti filtriranja/iskanja, kliknite **OK**, da se prikažejo filtrirani zapisi dnevnika ali **Najdi**, če želite začeti iskanje. Iskanje dnevniških datotek poteka od vrha proti dnu z začetkom na vašem trenutnem položaju (zapisu, ki je poudarjen). Iskanje se preneha, ko je najdem prvi ustrezen zapis. Za iskanje naslednjega zapisa pritisnite **F3** ali kliknite z desno tipko miške, izberite **Najdi** in natančneje določite možnosti iskanja.

Izvajajoči se procesi

Izvajajoči se procesi prikazujejo programe ali procese, ki se izvajajo v računalniku, in družbo ESET nemudoma in stalno obveščajo o novih infiltracijah. ESET Internet Security omogoča podrobne informacije o procesih, ki se izvajajo, s čimer ščiti uporabnike s tehnologijo ESET LiveGrid®.



Ugled – v večini primerov program ESET Internet Security in tehnologija ESET LiveGrid® predmetom dodelita raven tveganja (datotekam, procesom, registrskim ključem itd.) z nizom hevrističnih pravil, ki pregledujejo lastnosti vsakega posameznega predmeta in nato pretehtajo možnosti za njihovo zlonamerno aktivnost. Glede na ta hevristična pravila so predmeti dodeljeni ravni tveganja od 1 – Ustrezno (zelena) do 9 – Tvegano (rdeča).

Proces – ime slike programa ali procesa, ki se trenutno izvaja v računalniku. Vse izvajajoče se procese v računalniku si lahko ogledate tudi z upraviteljem opravil v sistemu Windows. Če želite odpreti upravitelja opravil, z desno tipko miške v opravilni vrstici kliknite prazno območje, nato kliknite **Upravitelj opravil** ali na tipkovnici pritisnite kombinacijo tipk **Ctrl**+**Shift**+**Esc**.

Znani programi, označeni z Ustrezno (zeleno) so zagotovo čisti (na seznamu dovoljenih) in bodo izključeni iz pregledovanja za izboljšanje delovanja.

PID – številka identifikatorja procesa je lahko uporabljena kot parameter v različnih klicih funkcij, kot je prilagajanje pomembnosti postopka.

Število uporabnikov – število uporabnikov, ki uporabljajo dani program. Te informacije zbira tehnologija ESET LiveGrid®.

Čas odkritja – čas, odkar je tehnologija ESET LiveGrid® zaznala program.

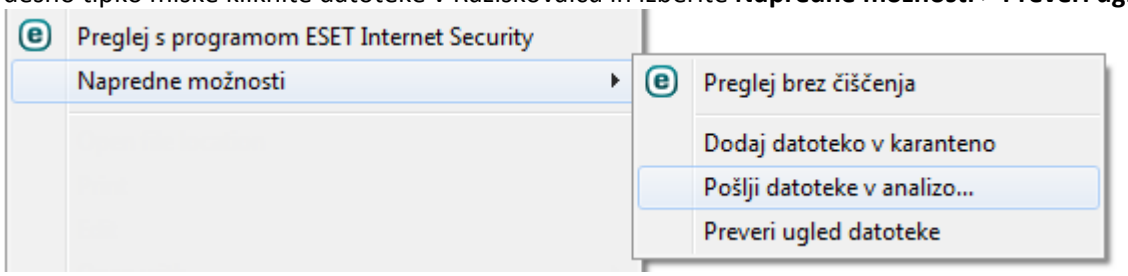
Če je program označen z Neznano (oranžno), to še ne pomeni, da gre za zlonamerno programsko opremo. Po navadi gre le za nov program. Če ne veste, za kakšno datoteko gre, lahko pošljete datoteko v analizo in jo posredujete raziskovalnemu laboratoriju družbe ESET. Če ugotovimo, da je datoteka zlonamerna, bo dodana v eno od naslednjih posodobitev.

Ime programa – ime programa ali procesa.

Kliknite program za prikaz naslednjih podrobnosti tega programa:

- **Pot** – mesto programa v računalniku.
- **Velikost** – velikost datoteke v KB (kilobajtih) ali MB (megabajtih).
- **Opis** – značilnosti datoteke na osnovi opisa iz operacijskega sistema.
- **Podjetje** – ime dobavitelja ali procesa programa.
- **Različica** – informacije založnika programa.
- **Izdelek** – ime programa in/ali ime podjetja.
- **Ustvarjeno dne/Spremenjeno dne** – datum in čas nastanka (spremembe).

Preverite lahko tudi ugled datotek, ki ne delujejo kot izvajajoči se program/proces. Če želite to storiti, z desno tipko miške kliknite datoteke v Raziskovalcu in izberite **Napredne možnosti** > **Preveri ugled datotek**.



Varnostno poročilo

Ta funkcija omogoča pregled statističnih podatkov za naslednje kategorije:

- **Blokirane spletne strani** – prikazuje število blokiranih spletnih strani (URL na seznamu blokiranih zaradi morebitno neželenega programa, lažnega predstavljanja, usmerjevalnika, v katerega je nekdo vdrl, IP-ja ali digitalnega potrdila).
- **Zaznani okuženi predmeti e-pošte** – prikazuje število zaznanih okuženih predmetov e-pošte.
- **Blokirane spletne strani v starševskem nadzoru** – prikazuje število blokiranih spletnih strani v starševskem nadzoru.
- **Zaznani morebitni neželeni programi** – prikazuje število morebitno neželenih programov (PUA).
- **Zaznana neželena e-pošta** – prikazuje število zaznanih neželenih e-poštnih sporočil.
- **Blokiran dostop do spletne kamere** – prikazuje število blokiranih dostopov do spletne kamere.
- **Pregledani dokumenti** – prikazuje število pregledanih predmetov dokumentov.
- **Pregledani programi** – prikazuje število pregledanih izvedljivih predmetov.
- **Pregledani drugi predmeti** – prikazuje število drugih pregledanih predmetov.
- **Pregledani predmeti spletnih strani** – prikazuje število pregledanih predmetov spletnih strani.

- **Pregledani predmeti e-pošte** – prikazuje število pregledanih predmetov e-poštnih sporočil.

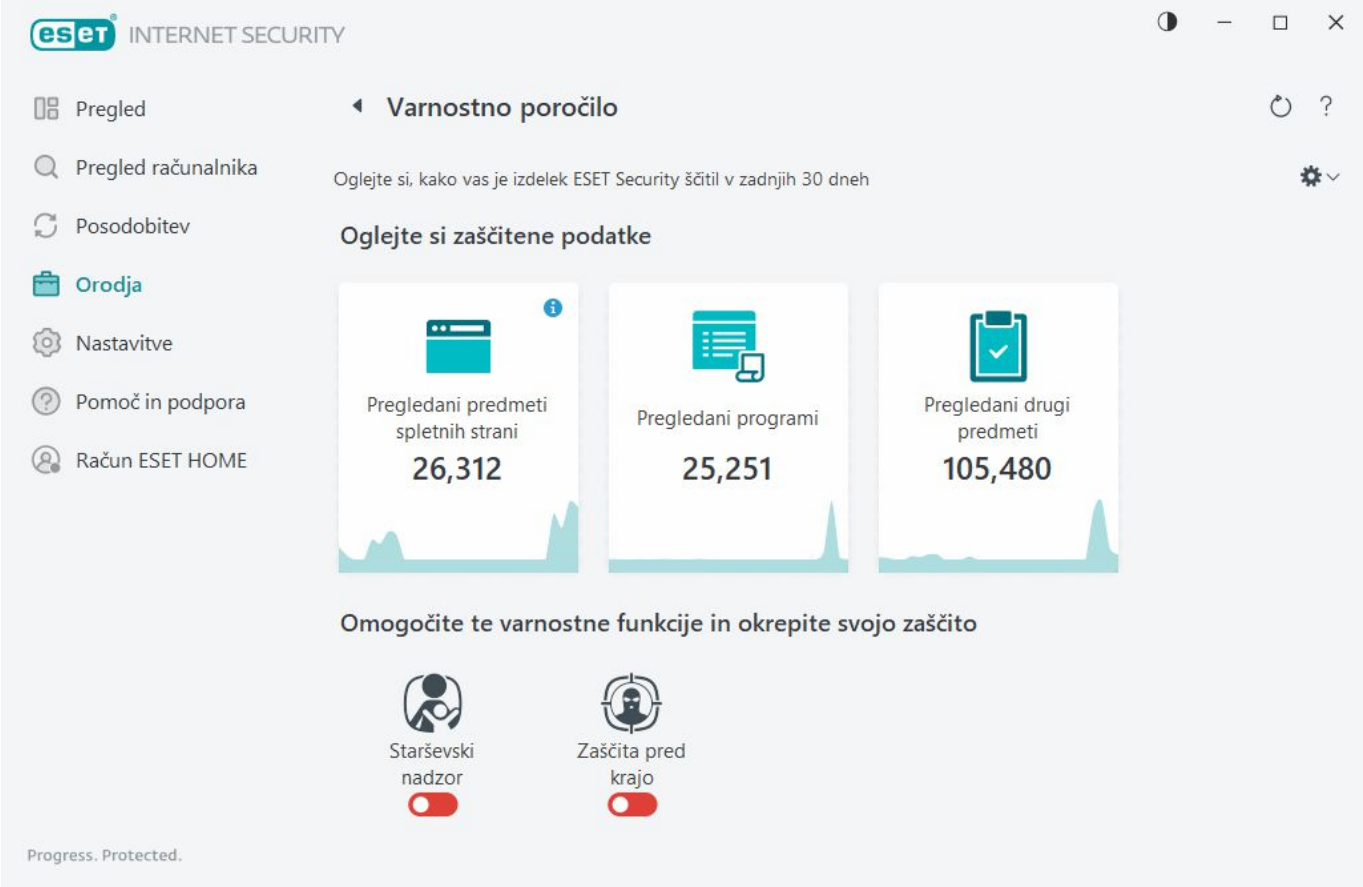
Vrstni red teh kategorij temelji na številski vrednosti od najvišje do najnižje. Kategorije brez vrednosti niso prikazane. Če želite razširiti prikaz in prikazati skrite kategorije, kliknite »**Pokaži več**«.

V zadnjem delu varnostnega poročila lahko aktivirate naslednje funkcije:

- Starševski nadzor
- Zaščita pred krajo

Ko funkcijo omogočite, v varnostnem poročilu ne bo več prikazana kot nedelujoča.

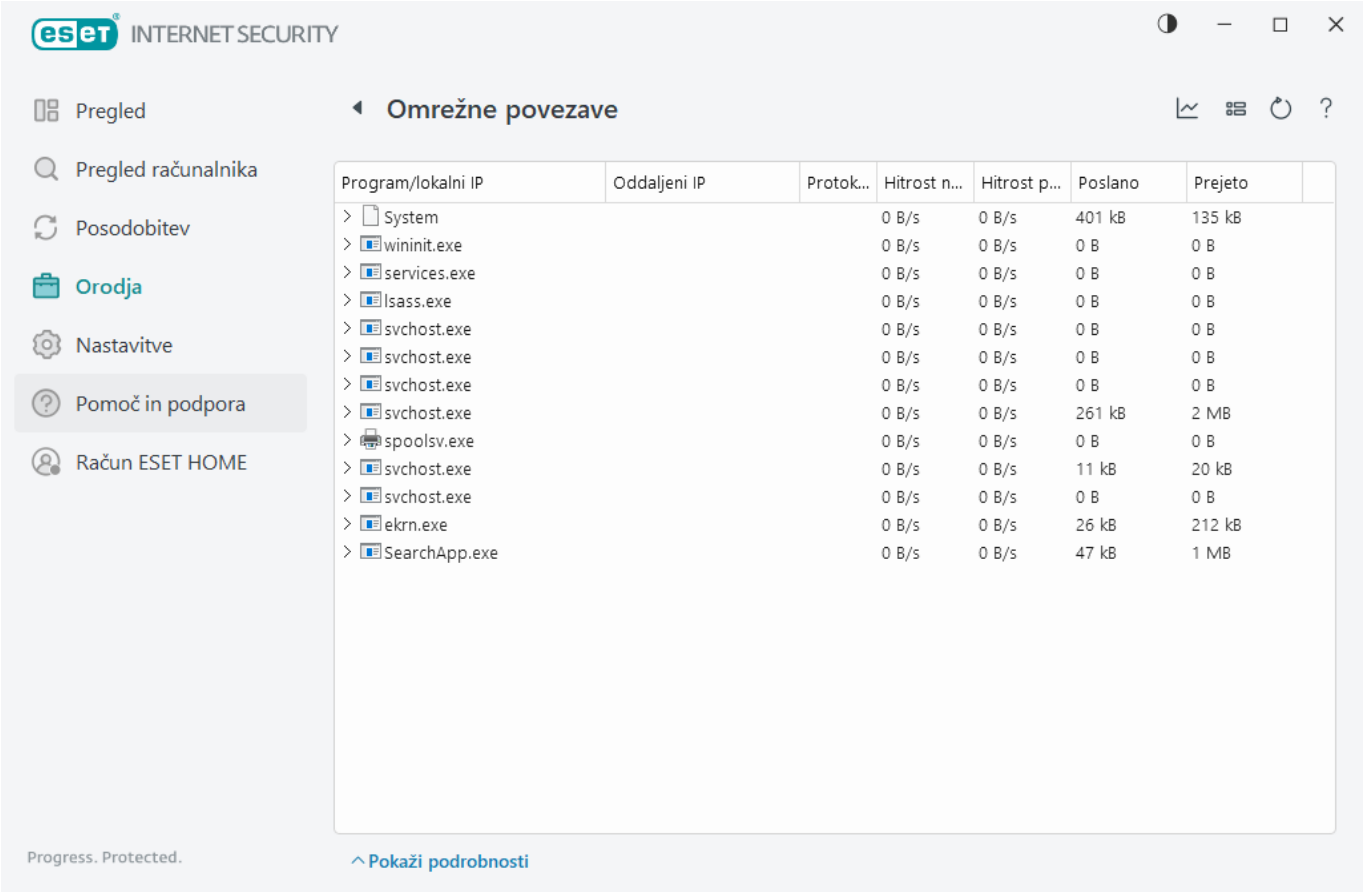
Če kliknite ikono zobnika v zgornjem desnem kotu, lahko **omogočite/onemogočite obvestila za varnostna poročila** in izberete, ali bodo podatki prikazani za zadnjih 30 dni ali od aktivacije izdelka. Če je izdelek ESET Internet Security nameščen manj kot 30 dni, lahko izberete le število dni od namestitve. Privzeto je nastavljeno obdobje 30 dni.



Možnost **Ponastavitev podatkov** izbriše vso statistiko in odstrani obstoječe podatke za varnostno poročilo. To dejanje morate potrditi, razen če onemogočite možnost **Vprašaj pred ponastavitvijo statistike** v razdelku Napredna nastavitev > **Obvestila** > **Interaktivna opozorila** > **Potrditvena sporočila** > **Uredi**.

Omrežne povezave

V razdelku omrežnih povezav je seznam aktivnih in čakajočih povezav. Tako lahko nadzorujete vse programe, ki vzpostavljajo odhodne povezave.



Kliknite ikono grafa , da odprete dejavnost omrežja.

V prvi vrstici je prikazano ime programa in hitrost prenosa podatkov. Če želite videti seznam povezav, ki jih je ustvaril program (in podrobnejše informacije), kliknite **>**.

Stolpci

Program/lokalni IP – ime programa, lokalni naslovi IP in vrata za komunikacijo.

Oddaljeni IP – naslov IP in številka vrat določenega oddaljenega računalnika.

Protokol – uporabljen protokol za prenos.

Hitrost nalaganja/Hitrost prenosa – trenutna hitrost dohodnih in izhodnih podatkov.

Poslano/prejeto – količina izmenjanih podatkov med povezavo.

Pokaži podrobnosti – to možnost izberite, če želite prikazati podrobne podatke o izbrani povezavi.

Z desno tipko miške kliknite povezavo, če si želite ogledati dodatne možnosti, vključno z:

Razreši imena gostiteljev – če je mogoče, so vsi omrežni naslovi prikazani v obliki zapisa DNS, ne v številski obliki naslova IP.

Pokaži samo povezave prek protokola TCP – na seznamu so prikazane samo povezave, ki pripadajo zbirki protokolov TCP.

Pokaži povezave, ki poslušajo – to možnost izberite, če želite prikazati le povezave, v katerih trenutno ni

komunikacije, vendar je sistem odprl vrata in čaka povezavo.

Pokaži povezave v računalniku – to možnost izberite, če želite prikazati le povezave, v katerih je oddaljena stran lokalni sistem – tako imenovane povezave localhost.

Hitrost osveževanja – izberite frekvenco, s katero osvežite aktivne povezave.

Osveži zdaj – znova naloži okno **omrežnih povezav**.

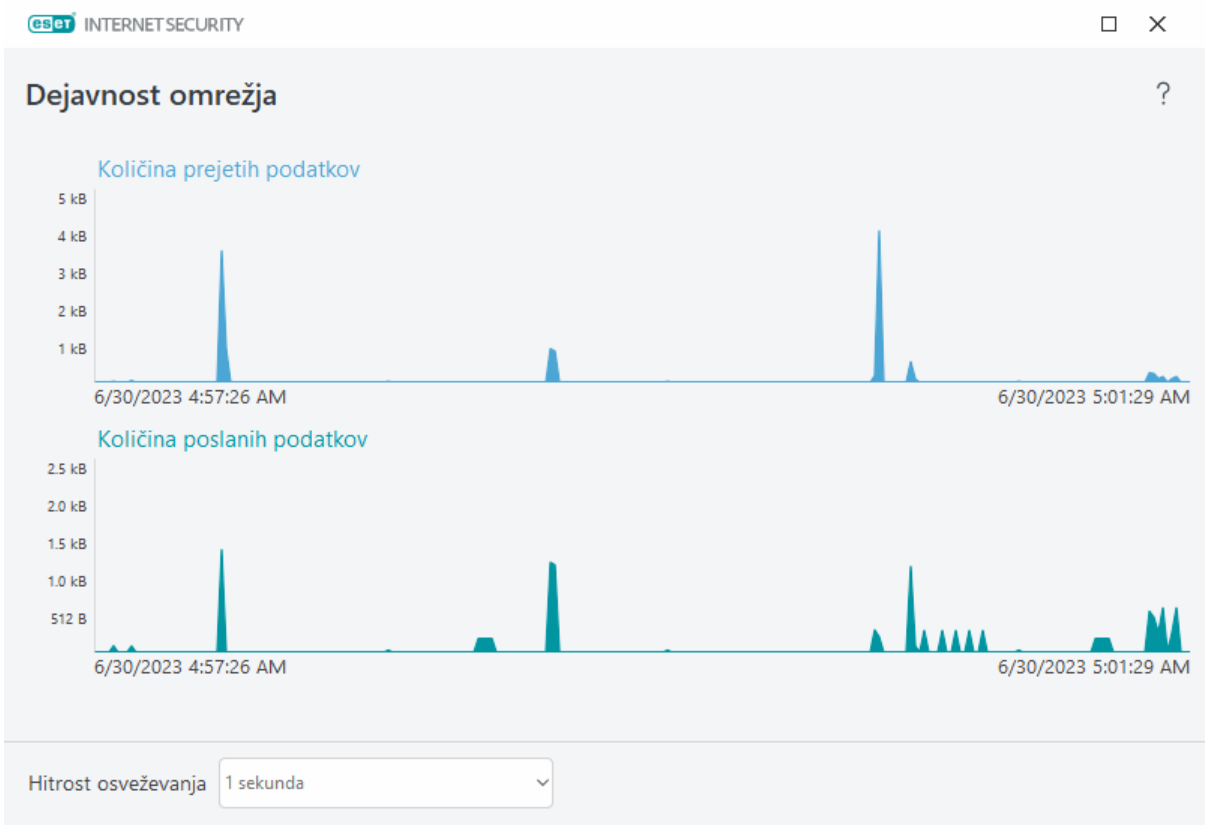
Te možnosti so na voljo le, ko kliknete program ali proces, ne aktivne povezave:

Začasno zavrni komunikacijo za postopek – zavrne trenutne povezave izbranega programa. Če je vzpostavljena nova povezava, požarni zid uporabi vnaprej določeno pravilo. Opis nastavitev najdete v razdelku Pravila za požarni zid.

Začasno omogoči komunikacijo za postopek – dovoli trenutne povezave izbranega programa. Če je vzpostavljena nova povezava, požarni zid uporabi vnaprej določeno pravilo. Opis nastavitev najdete v razdelku Pravila za požarni zid.

Dejavnost omrežja

Če želite trenutno **dejavnost omrežja** videti v obliki grafikona, kliknite **Orodja** > **Omrežne povezave** in kliknite ikono grafa . Na dnu grafikona je časovnica, ki na podlagi izbranega časovnega razpona sproti beleži dejavnost omrežja. Če želite spremeniti časovni razpon, v spustnem meniju izberite ustrezno vrednost za **Hitrost osveževanja**.



Na voljo so naslednje možnosti:

- **1 sekunda** – grafikon se osveži vsako sekundo, časovna premica pa pokriva zadnjih 4 minut.

- **1 minuta (zadnjih 24 ur)** – grafikon se osveži vsako minuto, časovna premica pa pokriva zadnjih 24 ur.
- **1 ura (zadnji mesec)** – grafikon se osveži vsako uro, časovna premica pa pokriva zadnji mesec.

Navpična os predstavlja količino prejetih ali poslanih podatkov. Če si želite ogledati točno količino prejetih/poslanih podatkov ob določenem času, se z miško pomaknite na grafikon.

ESET SysInspector

ESET SysInspector je program, ki omogoča temeljit pregled računalnika in zbiranje podrobnih informacij o sistemskih komponentah, kot so gonilniki in programi, omrežne povezave ali pomembni vnosi v register, ter ocenjevanje ravni tveganja za vsako posamezno komponento. Te informacije so lahko v pomoč pri ugotavljanju vzroka sumljivega delovanja sistema, ki je morda posledica nezdružljivosti programske ali strojne opreme ali okužbe z zlonamerno programsko opremo. Če želite izvedeti, kako uporabljati program ESET SysInspector, glejte spletno pomoč za ESET SysInspector.

V oknu programa ESET SysInspector so prikazani naslednji podatki o dnevnikih:

- **Čas** – čas nastanka dnevnika.
- **Komentar** – kratek komentar.
- **Uporabnik** – ime uporabnika, ki je ustvaril dnevnik.
- **Stanje** – stanje nastanka dnevnika.

Na voljo so naslednja dejanja:

- **Pokaži** – odpre izbrani dnevnik v programu ESET SysInspector. Izbrano dnevniško datoteko lahko kliknete z desno tipko miške in v priročnem meniju izberete možnost **Pokaži**.
- **Ustvari** – ustvari nov dnevnik. Preden poskusite dostopati do dnevnika počakajte, da se ustvari ESET SysInspector (stanje **Ustvarjeno**). Dnevnik je shranjen v C:\ProgramData\ESET\ESET Security\SysInspector.
- **Izbriši** – s seznama odstrani izbrane dnevnike.

Ko je izbrana ena ali več dnevniških datotek, so v priročnem meniju na voljo naslednji elementi:

- **Pokaži** – odpre izbrani dnevnik v programu ESET SysInspector (ista funkcija kot dvoklik dnevnika).
- **Ustvari** – ustvari nov dnevnik. Preden poskusite dostopati do dnevnika počakajte, da se ustvari ESET SysInspector (stanje **Ustvarjeno**).
- **Izbriši** – s seznama odstrani izbrane dnevnike.
- **Izbriši vse** – izbriše vse dnevnike.
- **Izvozi** – izvozi dnevnik v datoteko .xml ali stisnjeno datoteko .xml.

Razporejevalnik

Razporejevalnik upravlja in zažene razporejena opravila z vnaprej določeno konfiguracijo in lastnostmi.

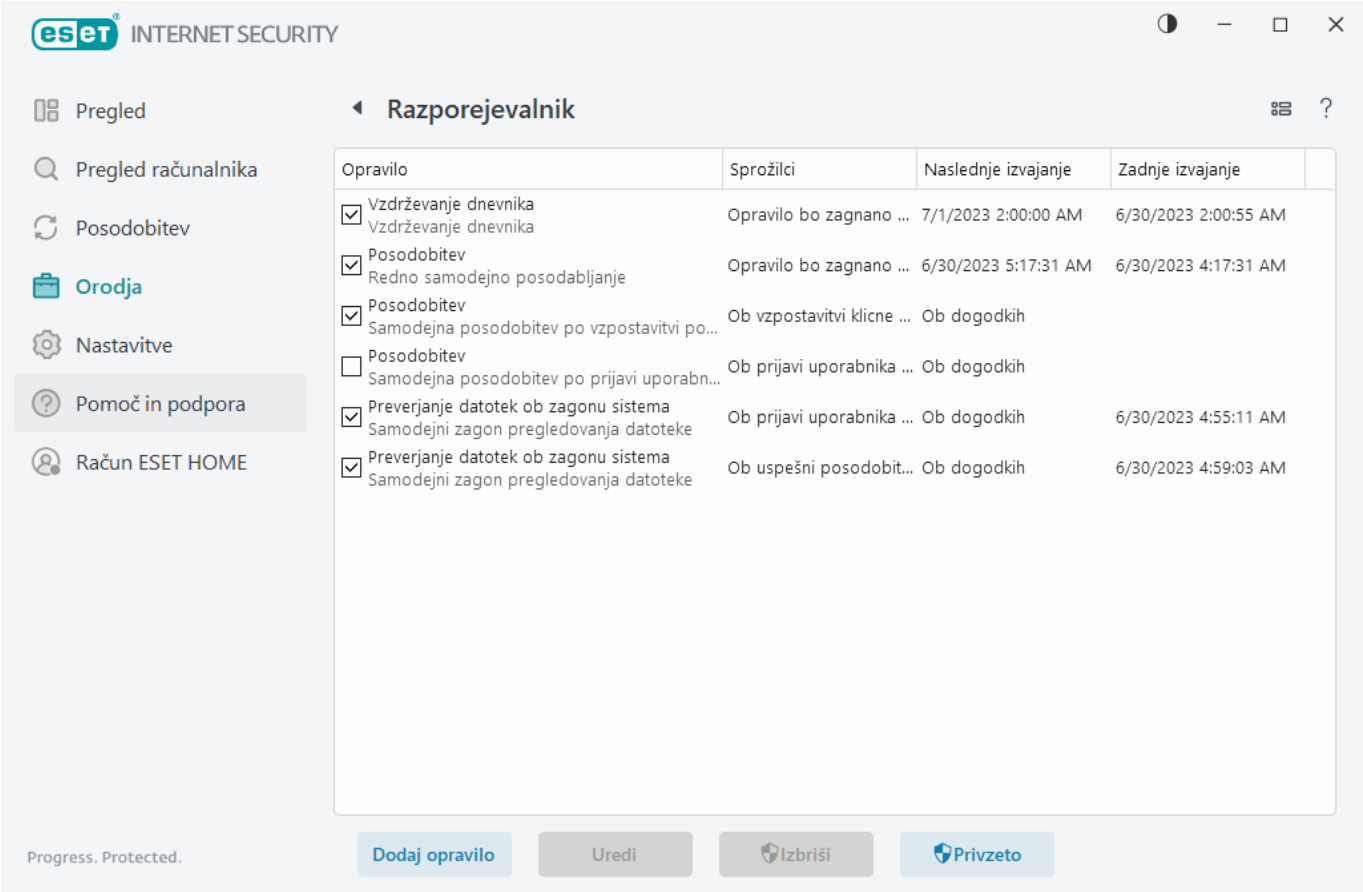
Dostop do razporejevalnika je mogoč iz glavnega okna programa ESET Internet Security tako, da kliknete **Orodja** > **Razporejevalnik**. V **razporejevalniku** je seznam načrtovanih opravil in lastnosti konfiguracije, na primer vnaprej določen datum, čas in uporabljeni profil pregleda.

Z razporejevalnikom lahko razporejate ta opravila: posodobitev modulov, opravilo pregledovanja, preverjanje datotek za zagon sistema in vzdrževanje dnevnika. Opravila lahko dodajate in brišete neposredno prek glavnega okna razporejevalnika (na dnu kliknite **Dodaj opravilo** ali **Izbriši**). Seznam načrtovanih opravil lahko ponastavite na privzetega in izbrišite vse spremembe tako, da kliknete **Privzeto**. Z desno tipko miške kliknite kamor koli v oknu razporejevalnika, če želite izvesti ta dejanja: prikazati podrobne podatke, takoj izvesti opravilo, dodati novo opravilo in izbrisati obstoječe opravilo. S potrditvenimi polji na začetku posameznega vnosa aktivirate/deaktivirate opravila.

Privzeto so v **razporejevalniku** prikazana ta načrtovana opravila:

- **vzdrževanje dnevnika**
- **Redno samodejno posodabljanje**
- **Samodejna posodobitev po prijavi uporabnika**
- **samodejni zagon pregleda datoteke** (po prijavi uporabnika)
- **Samodejni zagon pregleda datoteke** (po uspešni posodobitvi orodja za zaznavanje)

Če želite urediti konfiguracijo obstoječega razporejenega opravila (privzetega in uporabniško določenega), z desno tipko miške kliknite opravilo in nato kliknite **Uredi** ali pa izberite opravilo, ki ga želite spremeniti, in kliknite **Uredi**.



Dodaj novo opravilo

1. Kliknite **Dodaj opravilo** na dnu okna.

2. Vnesite ime opravila.

3. Izberite želeno opravilo v spustnem meniju:

   • **Zaženi zunanji program** – razporedi izvajanje zunanjega programa.

   • **Vzdrževanje dnevnika** – v dnevniških datotekah so tudi ostanki iz izbrisanih zapisov. S tem opravilom redno optimizirate zapise v dnevniških datotekah in tako omogočite učinkovito delovanje.

   • **Preverjanje datotek ob zagonu sistema** – preveri datoteke, ki se lahko zaženejo ob zagonu sistema ali prijavi.

   • **Ustvari posnetek stanja računalnika** – ustvari posnetek računalnika s programom ESET SysInspector; zbere podrobne informacije o sistemskih komponentah (na primer gonilnikih, programih) in oceni raven tveganja za vsako posamezno komponento.

   • **Pregled računalnika na zahtevo** – izvede pregled datotek in map v računalniku.

   • **Posodobi** – razporedi opravilo posodabljanja tako, da posodobi module.

4. Omogočite gumb za preklop ob možnosti **Omogočeno**, da aktivirate opravilo (to lahko storite pozneje tako, da izberete/počistite potrditveno polje na seznamu načrtovanih opravil), kliknite **Naprej** in izberite eno od časovnih možnosti:

- **Enkrat** – opravilo se izvede ob vnaprej določenem datumu in uri.
- **Večkrat** – opravilo se izvede v določenih časovnih intervalih.
- **Dnevno** – opravilo se izvede vsak dan ob določeni uri.
- **Tedensko** – opravilo se zažene ob izbranem dnevu in času.
- **Ob dogodkih** – opravilo se izvede ob določenem dogodku.

5. Izberite **Preskoči opravilo, ko se naprava napaja iz akumulatorja**, da zmanjšate sistemske vire, kadar se prenosnik napaja iz akumulatorja. Opravilo bo zagnano ob datumu in uri, ki sta določena v poljih **Izvedba opravil**. Če opravila ni bilo mogoče izvesti ob določenem času, lahko določite, kdaj naj bo znova opravljeno:

- **Ob naslednjem razporejenem času**
- **Takoj, ko je mogoče**
- **Takoj, če čas od zadnjega zagona presega (ure)** – predstavlja čas, ki je pretekel od prvega preskočenega zagona opravila. Če je ta čas presežen, se opravilo izvede takoj. Čas nastavite s spodnjim vrtljivim kolescem.

Če si želite ogledati načrtovano opravilo, z desno tipko miške kliknite opravilo in nato **Pokaži podrobnosti opravila**.

Možnosti načrtovanega pregleda

V tem oknu lahko določite napredne možnosti za razporejeno opravilo pregleda računalnika.

Za pregled brez čiščenja kliknite **Napredne nastavitve** in izberite **Preglej brez čiščenja**. Zgodovina pregledov je shranjena v dnevnik pregledovanja.

Ko je izbrana možnost **Prezri izključitve**, bodo datoteke s priponami, ki so bile predhodno izključene iz pregleda, brez izjeme pregledane.

V spustnem meniju **Dejanje po pregledu** lahko nastavite dejanje, ki bo samodejno izvedeno po končanem pregledu:

- **Ne naredi ničesar** – po končanem pregledu se ne izvede nobeno dejanje.
- **Zaustavitev sistema** – računalnik se po končanem pregledu izklopi.
- **Ponovni zagon po potrebi** – računalnik se znova zažene le, če je to potrebno za izvedbo čiščenja zaznanih groženj.
- **Vnovičen zagon** – po končanem pregledu se vsi odprti programi zaprejo, računalnik pa se znova zažene.
- **Prisilen ponovni zagon po potrebi** – računalnik se znova zažene le, če je to potrebno za izvedbo čiščenja zaznanih groženj.
- **Prisilen vnovičen zagon** – Prisilno zapre vse odprte programe, ne da bi čakal na interakcijo uporabnika, in po končanem pregledovanju znova zažene računalnik.

• **Stanje pripravljenosti** – vaša seja se shrani, računalnik pa preklopi v stanje nizke porabe, iz katerega lahko hitro nadaljujete z delom.

• **Stanje mirovanja** – vse, kar se izvaja v pomnilniku RAM, se premakne v posebno datoteko na trdem disku. Računalnik se zaustavi, vendar ob naslednjem zagonu obnovi svoje prejšnje stanje.

Dejanji **Stanje pripravljenosti** ali **Stanje mirovanja** sta na voljo glede na nastavitve napajanja in stanja pripravljenosti operacijskega sistema ali lastnosti vašega računalnika/prenosnika. Upoštevajte, da računalnik v stanju pripravljenosti še deluje. V njem se še vedno izvajajo osnovne funkcije, poleg tega se porablja energija akumulatorja, če se računalnik napaja prek akumulatorja. Če želite podaljšati čas delovanja akumulatorja, ko na primer zapustite pisarno, priporočamo, da računalnik preklopite v stanje mirovanja.

Izbrano dejanje se bo začelo, ko bodo vsi pregledi v izvajanju končani. Ko izberete možnost **Zaustavitev** ali **Vnovični zagon**, bo v potrditvenem pogovornem oknu prikazano 30-sekundno odštevanje (kliknite možnost **Prekliči**, da deaktivirate zahtevano dejanje).

Izberite možnost **Pregleda ni mogoče preklicati**, če želite onemogočiti uporabnikom brez pravic, da bi zaustavili izvajanje dejanj po pregledu.

Izberite možnost **Uporabnik lahko ustavi pregled za (min)**, če želite omogočiti uporabniku z omejenimi pravicami, da ustavi pregled računalnika za določeno časovno obdobje.

Glejte tudi Napredovanje pregleda.

Pregled razporejenih opravil

Če dvakrat kliknete opravilo po meri ali z desno tipko miške kliknete opravilo razporejevalnika po meri in izberete možnost **Pokaži podrobnosti opravila**, se v tem pogovornem oknu prikažejo podrobne informacije o izbranem načrtovanem opravilu.

Podrobnosti opravila

Vnesite **Ime opravila**, v razdelku **Vrsta opravila** izberite eno možnost ter nato kliknite **Naprej**:

• **Zaženi zunanji program** – razporedi izvajanje zunanjega programa.

• **Vzdrževanje dnevnika** – v dnevniških datotekah so tudi ostanki iz izbrisanih zapisov. S tem opravilom redno optimizirate zapise v dnevniških datotekah in tako omogočite učinkovito delovanje.

• **Preverjanje datotek ob zagonu sistema** – preveri datoteke, ki se lahko zaženejo ob zagonu sistema ali prijavi.

• **Ustvari posnetek stanja računalnika** – ustvari posnetek računalnika s programom ESET SysInspector; zbere podrobne informacije o sistemskih komponentah (na primer gonilnikih, programih) in oceni raven tveganja za vsako posamezno komponento.

• **Pregled računalnika na zahtevo** – izvede pregled datotek in map v računalniku.

• **Posodobi** – razporedi opravilo posodabljanja tako, da posodobi module.

Čas opravila

Opravilo se izvede večkrat, v določenih časovnih intervalih. Izberite eno od časovnih možnosti:

- **Enkrat** – opravilo se izvede le enkrat, ob vnaprej določenem datumu in uri.
- **Večkrat** – opravilo se izvaja v določenih intervalih (v urah).
- **Dnevno** – opravilo se izvede vsak dan ob določeni uri.
- **Tedensko** – opravilo se izvede enkrat ali večkrat tedensko ob izbranih dnevih in urah.
- **Ob dogodkih** – opravilo se izvede po določenem dogodku.

Preskoči opravilo, ko se naprava napaja iz akumulatorja – opravilo se ne zažene, če se računalnik napaja iz akumulatorja v času, ko bi se moralo opravilo zagnati. To velja tudi za računalnike, ki delujejo na neprekinjeno napajanje.

Čas opravila – enkrat

Izvedba opravil – opravilo bo zagnano samo enkrat, ob določenem datumu in uri.

Čas opravila – dnevno

Opravilo se izvede vsak dan ob določeni uri.

Čas opravila – tedensko

Opravilo se bo izvedlo vsak teden ob izbranih dnevih in urah.

Čas opravila – ob dogodkih

Opravilo sproži eden od teh dogodkov:

- **Vsak zagon računalnika**
- **Prvi zagon računalnika v dnevu**
- **Povezava na klic z internetom/omrežjem VPN**
- **Posodobitev modula je uspela**
- **Posodobitev izdelka je uspela**
- **Prijava uporabnika**
- **Zaznavanje groženj**

Ko razporejate opravilo, ki ga sproži dogodek, lahko določite minimalen interval med dvema dokončanima opraviloma. Če se na primer večkrat dnevno prijavite v računalnik, izberite interval 24 ur, da se opravilo izvede le ob prvi prijavi v dnevu in nato znova naslednji dan.

Preskočeno opravilo

Opravilo je mogoče preskočiti, če je računalnik izklopljen ali se napaja iz akumulatorja. Izberite eno od naslednjih možnost, da določite, kdaj naj se izvajajo preskočena opravila, in kliknite **Naprej**:

- **Ob naslednjem razporejenem času** – opravilo se bo zagnalo, če je računalnik vklopljen ob naslednjem razporejenem času.
- **Takoj, ko je mogoče** – opravilo se bo zagnalo, ko bo računalnik vklopljen.
- **Takoj, če čas od zadnjega načrtovanega zagona presega (ure)** – predstavlja čas, ki je pretekel od prvega preskočenega zagona opravila. Če je ta čas presežen, se opravilo izvede takoj.

Takoj, če čas od zadnjega načrtovanega zagona presega (ure) – primeri

Primer opravila je nastavljen tako, da se vsako uro ponavlja. Izbrana je možnost **Takoj, če čas od zadnjega načrtovanega zagona presega (ure)** in presežen čas je nastavljen na dve uri. Opravilo se izvaja ob 13.00 in ko je končano, računalnik preklopi v stanje pripravljenosti:

- Računalnik se zbudi ob 15.30. Prvi preskočeni zagon opravila je bil ob 14.00. Od 14.00 je minilo le 1,5 ure, tako da se bo opravilo zagnalo ob 16.00.
- Računalnik se zbudi ob 16.30. Prvi preskočeni zagon opravila je bil ob 14.00. Od 14.00 sta minili dve uri in pol, tako da se bo opravilo zagnalo takoj.

Podrobnosti opravila – posodobitev

Če želite posodobiti program iz dveh strežnikov za posodabljanje, potem je potrebno ustvariti dva različna profila posodobitve. Če prenos posodobitvenih datotek v prvem poskusu ne uspe, potem program samodejno preklopi na drug strežnik. To je primerno na primer za prenosnike, ki običajno posodabljajo iz strežnika za posodabljanje v krajevnem omrežju, njihovi lastniki pa imajo pogosto vzpostavljeno povezavo z internetom v drugih omrežjih. Torej če prvi profil ne uspe, bo drugi samodejno prenesel posodobitvene datoteke iz strežnikov ESET za posodabljanje.

Podrobnosti opravila – zagon programa

To opravilo razporedi izvajanje zunanjega programa.

Izvedljiva datoteka – izberite izvedljivo datoteko iz drevesa imenika, kliknite možnost **...** ali ročno vnesite pot.

Delovna mapa – določite delovni imenik zunanjega programa. Vse začasne datoteke izbrane **izvedljive datoteke** bodo ustvarjene v tem imeniku.

Parametri – parametri ukazne vrstice za program (izbirno).

Če želite uporabiti opravilo, kliknite **Dokončaj**.

Sistemski čistilnik

Sistemski čistilnik je orodje, ki vam pomaga obnoviti računalnik v uporabno stanje po čiščenju grožnje. Zlonamerna programska oprema lahko onemogoči sistemske pripomočke, kot so urejevalnik registra, upravitelj opravil ali posodobitve za Windows. Sistemski čistilnik obnovi privzete vrednosti in nastavitve za ustrezni sistem z enim samim klikom.

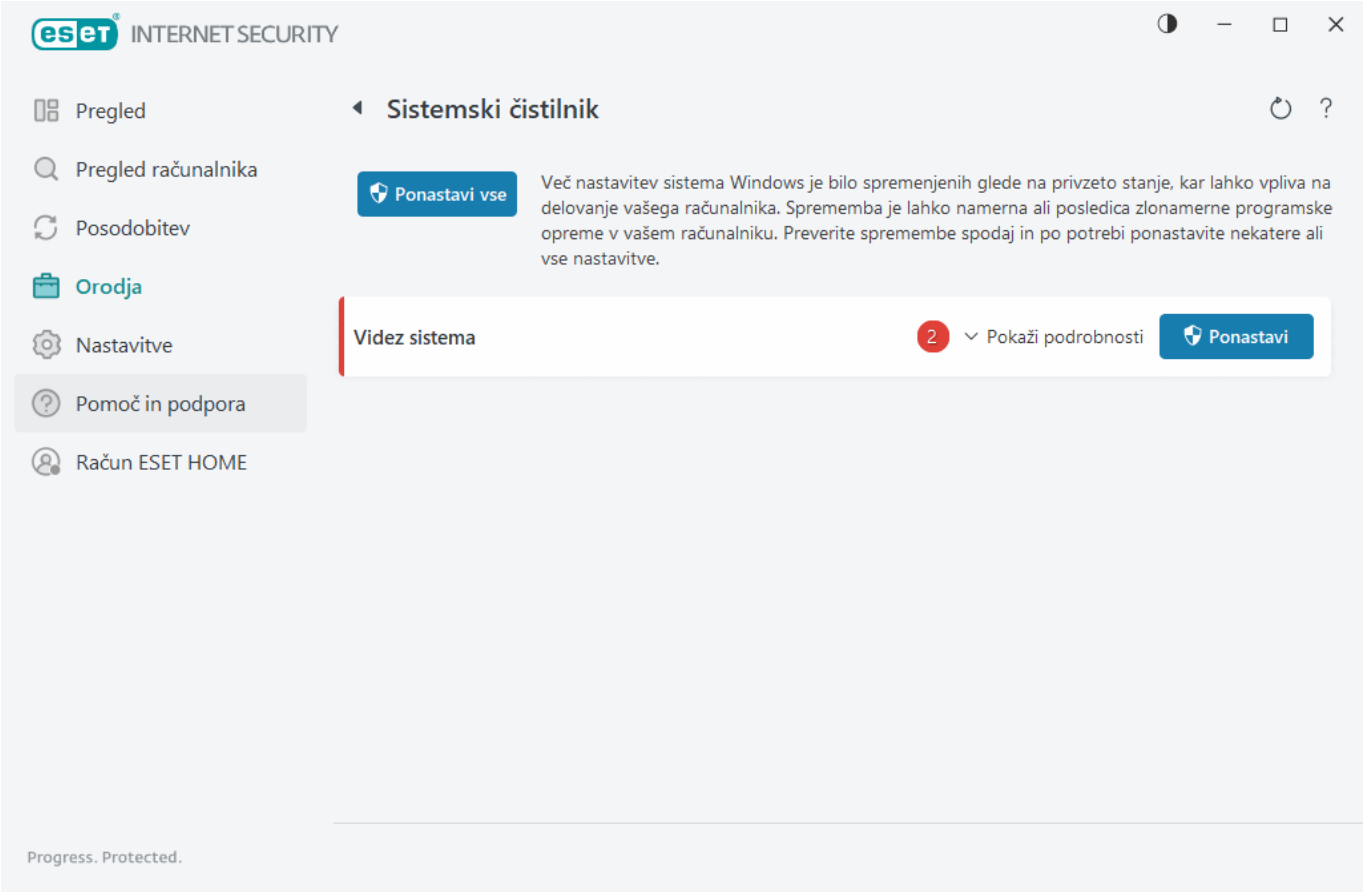
Sistemski čistilnik poroča o težavah iz petih kategorij nastavitev:

- **Varnostne nastavitve**: spremembe nastavitev, ki lahko povečajo ranljivost vašega računalnika, na primer posodobitev sistema Windows
- **Nastavitve sistema**: spremembe nastavitev sistema, ki lahko spremenijo vedenje računalnika, na primer povezave datotek
- **Videz sistema**: nastavitve, ki spremenijo videz sistema, na primer ozadje namizja
- **Onemogočene funkcije**: nekatere pomembne funkcije in aplikacije, ki so morda onemogočene.
- **Obnovitev sistema Windows**: nastavitve funkcije obnovitve sistema Windows, ki omogočajo, da sistem povrnete v prejšnje stanje

Sistemski čistilnik je mogoče zagnati:

- ko je najdena grožnja
- ko uporabnik klikne **Ponastavi**

Spremembe lahko pregledate in po potrebi ponastavite nastavitve.



Samo uporabniki s skrbniškimi pravicami lahko izvajajo dejanja v sistemskem čistilniku.

Nadzornik omrežja

Nadzornik omrežja pomaga odkriti ranljivosti v vašem zaupanja vrednem (domačem ali službenem) omrežju (npr. odprta vrata ali šibko geslo usmerjevalnika). Zagotavlja tudi seznam povezanih naprav, razvrščenih glede na vrsto (npr. tiskalnik, usmerjevalnik, mobilna naprava), ter vam tako omogoča, da imate pregled nad napravami, ki so povezane z vašim domačim omrežjem (npr. igralna konzola, naprave IoT ali druge domače pametne naprave).

Nadzornik omrežja vam pomaga odkriti ranljivosti usmerjevalnika ter povečuje raven zaščite, ko ste povezani s omrežjem.

Nadzornik omrežja usmerjevalnika ne konfigurira znova namesto vas. Spremembe morate s pomočjo posebnega vmesnika usmerjevalnika izvesti sami. Domači usmerjevalniki so lahko močno izpostavljeni zlonamerni programski opremi, ki se uporablja za distribuirane napade zavrnitve storitve (DDoS). Če uporabnik ne spremeni privzetega gesla usmerjevalnika, ga lahko napadalci preprosto uganejo in se prijavijo v vaš usmerjevalnik ter znova konfigurirajo ali ogrozijo vaše omrežje.

Priporočamo vam, da ustvarite močno geslo, ki je dovolj dolgo in vsebuje številke, simbole in velike črke. Če uporabite mešanico različnih vrst znakov, bo geslo težje uganiti.

Če je omrežje, s katerim ste povezani, konfigurirano kot zaupanja vredno, lahko omrežje označite kot »Moje omrežje«. Kliknite možnost **Označi kot »Moje omrežje«**, da v omrežje dodate oznako »Moje omrežje«. Ta oznaka bo prikazana poleg omrežja v programu ESET Internet Security za lažje prepoznavanje in varnostni pregled. Če želite odstraniti oznako, kliknite možnost **Odstrani oznako »Moje omrežje«**.

Vsaka naprava, ki je povezana z omrežjem, je prikazana v pogledu seznama z osnovnimi informacijami. Kliknite določeno napravo, da jo uredite ali si ogledate podrobne informacije o napravi.

Spustni meni **Omrežja** vam omogoča, da naprave filtrirate na podlagi naslednjih kriterijev:

- Naprave, ki so povezane z določenim omrežjem
- Naprave, ki so povezane z **Vsemi omrežji**
- Nekategorizirane naprave

Kliknite ikono za urejanje naprave ali ogled podrobnih informacij o napravi. Nedavno povezane naprave so prikazane bližje usmerjevalnika, da jih lahko zlahka opazite.

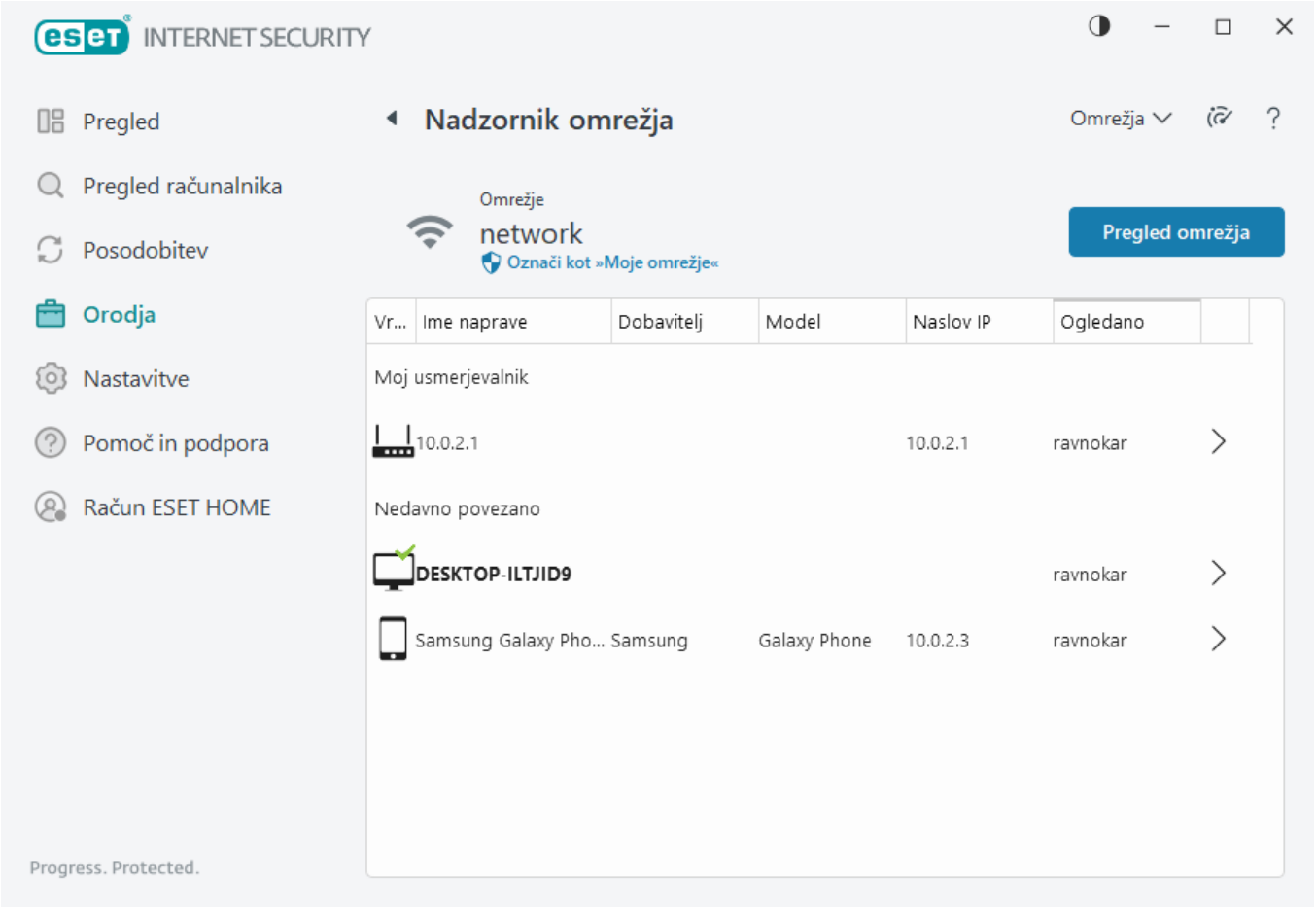
Kliknite zobnik ⚙ v zgornjem desnem kotu in izberite, ali želite prejeti obvestilo, ko je v omrežju odkrita nova naprava.

Če želite ročno zagnati pregled omrežja, s katerim ste povezani, kliknite **Pregled omrežja**. Možnost **Pregled omrežja** je na voljo le za zaupanja vredno omrežje. Za pregled ali urejanje nastavitev omrežja glejte Profili omrežnih povezav.

Izbirate lahko med naslednjimi možnostmi pregledov:

- Preglej vse
- Preglej samo usmerjevalnik
- Preglej samo naprave

⚠ Preglede omrežij izvajajte samo v zaupanja vrednem omrežju. Če jih izvedete v omrežjih, ki niso vredna zaupanja, se zavedajte morebitne nevarnosti.



Po končanem pregledu se bo prikazalo obvestilo s povezavo do osnovnih informacij o napravi, lahko pa tudi dvokliknete sumljivo napravo v pogledu seznama ali sonarja. Če si želite ogledati nedavno blokirane komunikacije, kliknite **Odpravljanje težav**. Več informacij o odpravljanju težav s požarnim zidom.

Modul nadzornika omrežja prikaže dve vrsti obvestil:

- **Nova naprava, povezana z omrežjem** – če se z omrežjem medtem, ko je z njim povezan uporabnik, poveže nepoznana naprava, bo prikazano obvestilo.
- **Najdene nove naprave v omrežju** – če se ponovno povežete z zaupanja vrednim omrežjem in je v njem tudi nepoznana naprava, bo prikazano splošno obvestilo.

Obe vrsti obvestil vas obvestita, če se z vašim omrežjem poskuša povezati nepooblaščena naprava. Za ogled podrobnosti o napravi kliknite možnost **ogled naprave**.

Kaj pri napravah v nadzorniku omrežja pomenijo ikone?

	Ikona rumene zvezdice označuje naprave, ki so nove v omrežju ali pa jih je ESET prvič zaznal.
	Rumena ikona za previdnost pomeni, da ima usmerjevalnik morda ranljivosti. Za prikaz podrobnejših informacij o težavi kliknite ikono v izdelku.
	Rdeča opozorilna ikona pomeni, da imajo naprave, ki jih vsebuje vaš usmerjevalnik, ranljivosti in je morda okužen. Za prikaz podrobnejših informacij o težavi kliknite ikono v izdelku.
	Modra ikona se lahko prikaže, ko ima izdelek ESET dodatne informacije glede vašega usmerjevalnika, ki pa ne zahtevajo vašega takojšnjega ukrepanja, ker ni varnostnega tveganja. Za prikaz podrobnejših informacij kliknite ikono v izdelku.

Omrežna naprava v nadzorniku omrežja

Tukaj so na voljo podrobne informacije o napravi, vključno z naslednjim:

- Ime naprave
- Vrsta naprave
- Zadnji ogled
- Ime omrežja
- Naslov IP
- Naslov MAC
- Operacijski sistemi

Ikona svinčnika označuje, da lahko spremenite ime naprave ali vrsto naprave.

Odstranitev iz zgodovine – izbrišite napravo s seznama naprav. Ta možnost je na voljo samo za naprave, ki trenutno niso povezane z vašim omrežjem.

Za vsako vrsto naprave so na voljo naslednja dejanja:

Usmerjevalnik

Nastavitve usmerjevalnika – do nastavitev usmerjevalnika lahko dostopate v spletnem vmesniku, programu za mobilne naprave ali tako, da kliknete možnost **Odprite vmesnik usmerjevalnika**. Če imate usmerjevalnik, ki vam ga zagotavlja internetni ponudnik, se boste za odpravljanje zaznanih varnostnih težav morda morali obrniti na vire podpore internetnega ponudnika ali proizvajalca usmerjevalnika. Vedno upoštevajte ustrezne varnostne ukrepe, navedene v uporabniškem priročniku usmerjevalnika.
Zaščita – Če želite zaščititi usmerjevalnik in omrežje pred spletnimi napadi, upoštevajte ta osnovna navodila.

Omrežna naprava

Prepoznavanje naprave – če niste prepričani, katera naprava je povezana v vaše omrežje, si oglejte ime dobavitelja ali proizvajalca pod imenom naprave. To vam lahko pomaga prepoznati vrsto naprave. Ime naprave lahko spremenite za poznejšo uporabo.
Prekinjanje povezave z napravo – če niste prepričani, ali je povezana naprava varna za omrežje ali naprave, lahko v nastavitvah usmerjevalnika upravljajte dostop do omrežja za to napravo ali spremenite geslo omrežja.
Zaščita – če želite zaščititi napravo pred napadi in zlonamerno programsko opremo, v napravi namestite spletno zaščito in poskrbite, da sta operacijski sistem in nameščena programska oprema vedno posodobljena. Ne vzpostavljajte povezave z nezaščitenimi omrežji Wi-Fi, da boste še naprej zaščiteni.

Ta naprava

Ta naprava v omrežju predstavlja vaš računalnik.
Omrežne kartice – prikazuje podatke o vaših omrežnih karticah.

Obvestila | Nadzornik omrežja

Spodaj je navedenih več obvestil, ki jih lahko program ESET Internet Security prikaže v primeru zaznanih težav z ranljivostjo v usmerjevalniku. Vsako obvestilo vsebuje kratek opis in navaja rešitev ali priporočljive ukrepe za zmanjšanje ranljivosti usmerjevalnika. Če ne prepoznate sprememb v usmerjevalniku, priporočamo, da stopite v stik s proizvajalcem usmerjevalnika ali ponudnikom internetnega omrežja.

Najdena morebitna ranljivost
Usmerjevalnik lahko vsebuje znane ranljivosti, zaradi katerih bi lahko lažje prišlo do napadov in izkoriščanj. Posodobite vdelano programsko opremo usmerjevalnika.

Najdena ranljivost
Usmerjevalnik vsebuje znane ranljivosti, zaradi katerih lažje pride do napadov in izkoriščanj. Posodobite vdelano programsko opremo usmerjevalnika.

Najdena je bila grožnja
Usmerjevalnik je okužen z zlonamerno programsko opremo. Znova zaženite usmerjevalnik in ponovite pregled.

Šibko geslo usmerjevalnika
Geslo v vašem usmerjevalniku je šibko in ga kdo drug lahko hitro ugane. Spremenite geslo v usmerjevalniku.

Zlonamerno preusmerjanje v omrežju
Zdi se, da je vaš internetni promet preusmerjen na zlonamerna spletna mesta. To lahko pomeni, da je vaš usmerjevalnik okužen. Spremenite nastavitev strežnika DNS v usmerjevalniku.

Storitve odprtega omrežja
Vaš usmerjevalnik izvaja omrežne storitve, ki jih morda drugi izkoriščajo. Razlog za to je lahko slaba konfiguracija ali okužen usmerjevalnik. Preverite konfiguracijo usmerjevalnika.

Občutljive storitve odprtega omrežja
Vaš usmerjevalnik izvaja občutljive omrežne storitve, ki jih morda drugi izkoriščajo. Razlog za to je lahko slaba konfiguracija ali okužen usmerjevalnik. Preverite konfiguracijo usmerjevalnika.

Zastarela vdelana programska oprema
Vdelana programska oprema v vašem usmerjevalniku je zastarela in je lahko ranljiva. Posodobite vdelano programsko opremo v usmerjevalniku.

Zlonamerna nastavitev usmerjevalnika
Strežnik DNS, ki ga uporablja vaš usmerjevalnik, je zlonameren in vas lahko pošlje na nevarna spletna mesta. To lahko pomeni, da je vaš usmerjevalnik okužen. Spremenite nastavitev strežnika DNS v usmerjevalniku.

Omrežne storitve
Vaš usmerjevalnik izvaja običajne omrežje storitve. Te so potrebne za omrežje in so verjetno varne. Preverite konfiguracijo usmerjevalnika.

Karantena

Glavna funkcija karantene je varna hramba prepoznanih predmetov (kot so zlonamerna programska oprema ali morebitno neželeni programi).

Dostop do karantene je mogoč iz glavnega okna programa ESET Internet Security tako, da kliknete **Orodja** > **Karantena**.

Datoteke, shranjene v mapi karantene, si lahko ogledate v tabeli, v kateri je prikazano naslednje:

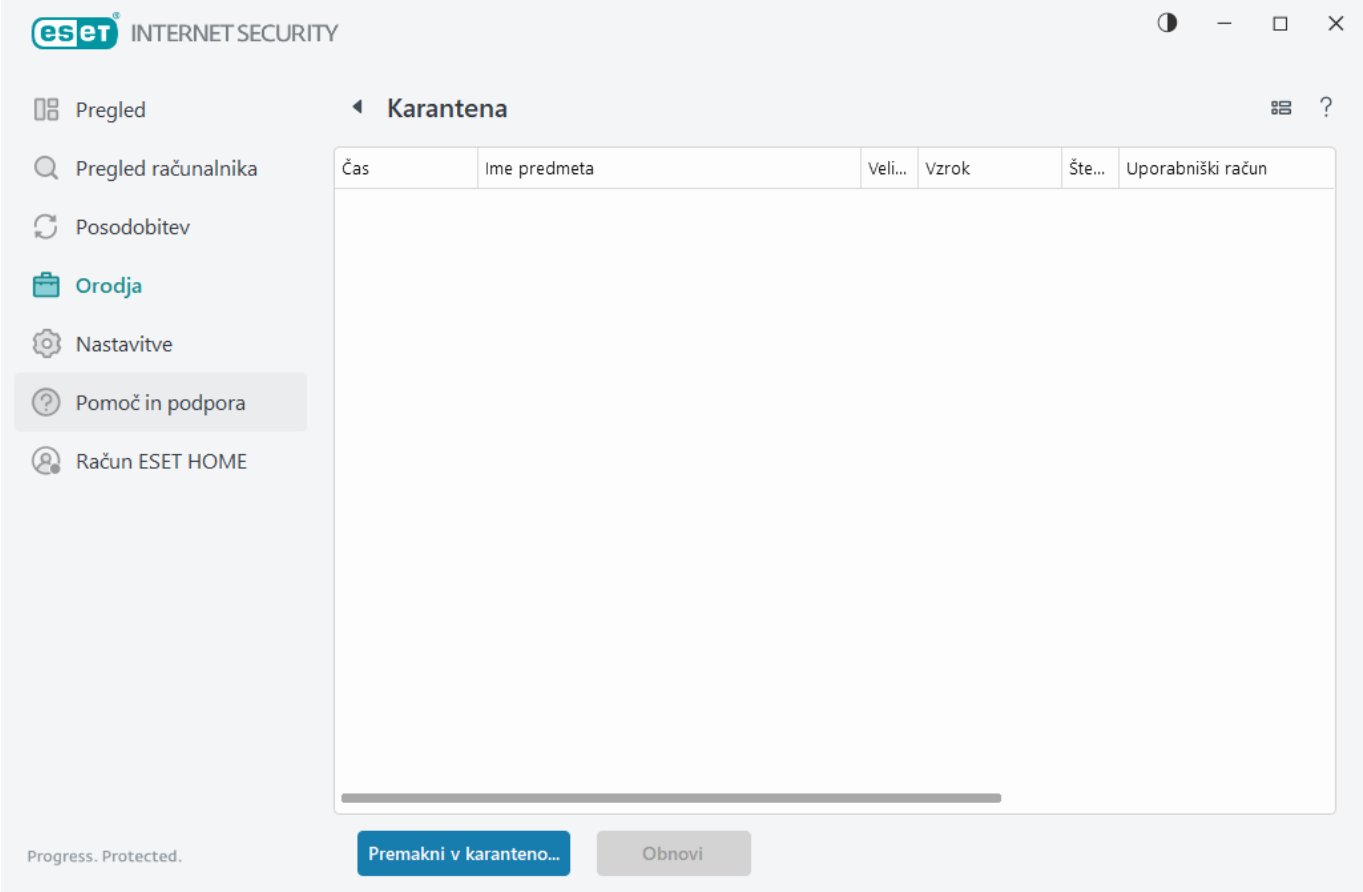
• datum in čas karantene,

• pot do izvirnega mesta okužene datoteke,

• njena velikost v bajtih,

• razlog (npr. predmet je dodal uporabnik),

• in število zaznav (če gre na primer za podvojene zaznave iste datoteke ali gre za arhiv, ki vsebuje več infiltracij).



Dodajanje datotek v karanteno

ESET Internet Security c karanteno samodejno doda izbrisane datoteke (če te možnosti niste preklicali v oknu z opozorilom).

Dodatne datoteke bi bilo treba dati v karanteno, če:

a.jih ni mogoče očistiti,

b.njihovo brisanje ni varno ali priporočljivo,

c.če jih je program ESET Internet Security napačno zaznal ali

d.se datoteka sumljivo vede, vendar je zaščita ne zazna.

Za premik datoteke v karanteno imate več možnosti:

a.Datoteko lahko ročno dodate v karanteno s funkcijo »povleci in spusti« tako, da kliknete datoteko,

kazalec miške premaknete na označeno območje, pri čemer držite gumb miške in ga nato spustite. S tem se program premakne v ospredje.

b.Z desno tipko miške kliknite datoteko in kliknite razdelek **Napredne možnosti** > **Dodaj datoteko v karanteno**.

c.V oknu **Karantena** kliknite možnost **Premakni v karanteno**.

d.To lahko naredite tudi s priročnim menijem – kliknite z desno tipko v oknu **Karantena** in izberite **Dodaj v karanteno**.

Obnavljanje iz karantene

Datoteke iz karantene je mogoče obnoviti na njihovo prvotno lokacijo:

- V ta namen uporabite funkcijo **Obnovi**, ki je na voljo v priročnem meniju, ko v karanteni z desno tipko miške kliknete določeno datoteko.

- Če je datoteka označena kot morebitno neželen program, je možnost **Obnovi in izključi iz pregledovanja** omogočena. Glejte tudi Izključitve.

- Priročni meni vsebuje tudi možnost **Obnovi v**, s katero lahko obnovite datoteko na drugo mesto in ne na prvotno lokacijo, s katere je bila izbrisala.

- Funkcija obnovitve v nekaterih primerih ni na voljo, na primer za datoteke, ki so bile locirane na omrežnem pogonu samo za branje.

Brisanje iz karantene

Z desno tipko miške kliknite izbran element in izberite **Izbriši iz karantene**, ali pa izberite element, ki ga želite izbrisati, in na tipkovnici pritisnite **Izbriši**. Če želite izbrati in izbrisati vse elemente v karanteni, lahko pritisnete **Ctrl + A** in nato **Delete** na tipkovnici. Izbrisani elementi bodo trajno odstranjeni iz naprave in karantene.

Pošiljanje datoteke iz karantene

Če ste v karanteno prenesli sumljivo datoteko, ki je program ni zaznal, ali če je bila datoteka nepravilno določena kot okužena (npr. s hevristično analizo kode) in posledično poslana v karanteno, pošljite vzorec v raziskovalni laboratorij ESET za analizo. Če želite poslati datoteko, jo kliknite z desno tipko miške in v priročnem meniju izberite **Pošlji v analizo**.

Opis zaznanega elementa

Z desno tipko miške kliknite element in kliknite možnost **Opis zaznanega elementa**, da odprete enciklopedijo groženj družbe ESET, v kateri najdete podrobne informacije o nevarnostih in simptomih, povezanih z različnimi vrstami zabeležene infiltracije.

Ilustrirana navodila

Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:

- Obnovitev datoteke v karanteni v programu ESET Internet Security
- Brisanje datoteke v karanteni v programu ESET Internet Security
- Moj izdelek ESET me je obvestil o zaznanem elementu – kaj naj storim?

Karantena ni uspela

Obstajajo naslednji razlogi, zakaj določenih datotek ni mogoče dodati v karanteno:

- **Nimate dovoljenja za branje** – pomeni, da si ne morete ogledati vsebine ali datoteke.
- **Nimate dovoljenja za zapisovanje** – pomeni, da ne morete urejati vsebine ali datotek, na primer ne morete dodajati nove vsebine ali izbrisati obstoječe vsebine.
- **Datoteka, ki jo želite dodati v karanteno je prevelika** – zmanjšati morate velikost datoteke.

Ko prejmete sporočilo o napaki »Karantena ni uspela«, kliknite možnost **Več informacij**. Pojavi se okno s seznamom napak, kjer si lahko ogledati ime datoteke in razlog, zakaj ga ni mogoče premakniti v karanteno.

Izberi vzorec za analizo

Če najdete sumljivo datoteko v računalniku ali sumljivo mesto v internetu, ju lahko pošljete v raziskovalni laboratorij družbe ESET v analizo (razpoložljivost te možnosti je odvisna od konfiguracije tehnologije ESET LiveGrid®).

Pred pošiljanjem vzorcev družbi ESET

Vzorec pošljite le, če izpolnjuje vsaj enega od naslednjih pogojev:

- Izdelek ESET vzorca sploh ni zaznal
- Vzorec je bil napačno zaznan kot grožnja
- Ne sprejemamo vzorcev iz vaših osebnih datotek, ki bi jih želeli poslati družbi ESET v pregled (raziskovalni laboratorij ESET ne izvaja pregledov na zahtevo za uporabnike)
- Uporabite opisno zadevo in vključite čim več informacij o datoteki (na primer posnetek zaslona ali spletno mesto, s katerega ste jo prenesli)

Vzorec (datoteko ali spletno mesto) lahko družbi ESET pošljete v analizo na naslednje načine:

1. Uporabite obrazec za pošiljanje vzorcev v izdelku. Najdete ga v razdelku **Orodja** > **Pošlji vzorec v analizo**. Največja dovoljena velikost poslanega vzorca je 256 MB.

2. Datoteko lahko pošljete tudi po e-pošti. Če želite izbrati to možnost, datoteko zapakirajte s programom WinRAR/WinZIP, zaščitite arhiv z geslom »infected« in jo pošljite na naslov samples@eset.com.

3. Če želite prijaviti neželeno pošto, napačno pozitivno prepoznano e-pošto ali spletna mesta, ki jih modul starševskega nadzora uvrsti v napačno kategorijo, glejte naš članek v zbirki znanja družbe ESET.

V obrazcu **Izberi vzorec za analizo** v spustnem meniju **Razlog za pošiljanje vzorca** izberite opis, ki najbolje ustreza vašemu sporočilu:

- Sumljiva datoteka

- Sumljivo spletno mesto (spletno mesto, ki je okuženo z zlonamerno programsko opremo)
- Napačna pozitivna prepoznava spletnega mesta
- Napačna pozitivna prepoznava datoteke (datoteka, ki je zaznana kot okužba, a ni okužena)
- Drugo

Datoteka/mesto – pot do datoteke ali spletnega mesta, ki ga želite poslati.

E-poštni naslov za stik – e-poštni naslov za stik je skupaj s sumljivimi datotekami poslan družbi ESET in prek njega lahko stopimo v stik z vami, če bi potrebovali dodatne informacije za analizo. E-poštnega naslova za stik ni treba vnesti. Izberite **Pošlji anonimno**, če želite polje pustiti prazno.

> **Od družbe ESET morda ne boste prejeli odgovora**
> Družba ESET vam ne bo odgovorila, razen če bo potrebovala dodatne informacije. Naši strežniki vsak dan prejmejo več deset tisoč datotek, zato je nemogoče odgovoriti na vsa poslana sporočila.
> Če ugotovimo, da vzorec vsebuje zlonameren program ali zlonamerno spletno mesto, bomo njegovo zaznavanje vključili v naslednjo posodobitev izdelkov ESET.

Izberi vzorec za analizo – sumljiva datoteka

Zaznani znaki in simptomi okužbe z zlonamerno programsko opremo – vnesite svoja opažanja glede dejanj okužene datoteke v računalniku.

Izvor datoteke (naslov URL ali dobavitelj) – vnesite izvor datoteke (izvirno datoteko) in kako ste naleteli nanjo.

Opombe in dodatne informacije – tukaj lahko vnesete dodatne informacije ali opis, ki bo v pomoč pri obdelavi sumljive datoteke.

> Prvi parameter – **Zaznani znaki in simptomi okužbe z zlonamerno programsko opremo** – je obvezen, vendar boste z dodatnimi informacijami močno pomagali laboratorijem pri prepoznavanju in obdelavi vzorcev.

Izberi vzorec za analizo – sumljivo spletno mesto

V spustnem meniju **Kaj je narobe z mestom** izberite eno od teh možnosti:

- **Okuženo** – spletno mesto, ki vsebuje viruse ali drugo zlonamerno programsko opremo, ki se posreduje na različne načine.
- **Lažno predstavljanje** se pogosto uporablja za dostop do občutljivih podatkov, kot so številke bančnih računov, številke PIN ipd. Več o tej vrsti napadov preberite v slovarju izrazov.
- **Prevara** – prevarantsko ali lažno spletno mesto, namenjeno zlasti ustvarjanju hitrega dobička.
- Izberite **Drugo**, če zgornje možnosti ne ustrezajo spletnemu mestu, ki ga želite poslati.

Opombe in dodatne informacije – tukaj lahko vnesete dodatne informacije ali opise, ki bodo v pomoč pri analizi sumljivega spletnega mesta.

Izberi vzorec za analizo – napačna pozitivna datoteka

Prosimo vas, da nam pošljete datoteke, ki so zaznane kot okužene, a v resnici niso okužene. S tem želimo izboljšati našo zaščito pred virusi in vohunsko programsko opremo in obenem zaščititi vse uporabnike. Do napačnih pozitivnih prepoznav lahko pride, ko se vzorec datoteke ujema z vzorcem, ki je v zbirki pogon za zaznavo.

Ime in različica programa – naslov programa in njegova različica (na primer številka, vzdevek ali ime kode).

Izvor datoteke (naslov URL ali dobavitelj) – vnesite izvor datoteke (izvirno datoteko) in zabeležite, kako ste naleteli nanjo.

Namen programa – splošni opis programa, vrsta programa (na primer brskalnik, predvajalnik predstavnosti ...) in njegovo delovanje.

Opombe in dodatne informacije – tukaj lahko vnesete dodatne informacije ali opis, ki bo v pomoč pri obdelavi sumljive datoteke.

> prvi trije parametri so obvezni za prepoznavanje zakonitih programov in njihovo razlikovanje v primerjavi z zlonamerno kodo. S pošiljanjem dodatnih informacij močno pomagate našim laboratorijem pri prepoznavanju in obdelavi vzorcev.

Izberi vzorec za analizo – napačno pozitivno mesto

Prosimo vas, da nam pošljete mesta, ki so zaznana kot okužbe, prevare ali lažno predstavljanje, a v resnici niso. Do napačnih pozitivnih prepoznav lahko pride, ko se vzorec datoteke ujema z vzorcem, ki je v zbirki pogon za zaznavo. Prosimo pošljite nam to napačno pozitivno mesto, kajti želimo izboljšati našo zaščito pred virusi in preprečevanje lažnega predstavljanja ter obenem zaščititi vse uporabnike.

Opombe in dodatne informacije – tukaj lahko vnesete dodatne informacije ali opise, ki bodo v pomoč pri obdelavi sumljivega spletnega mesta.

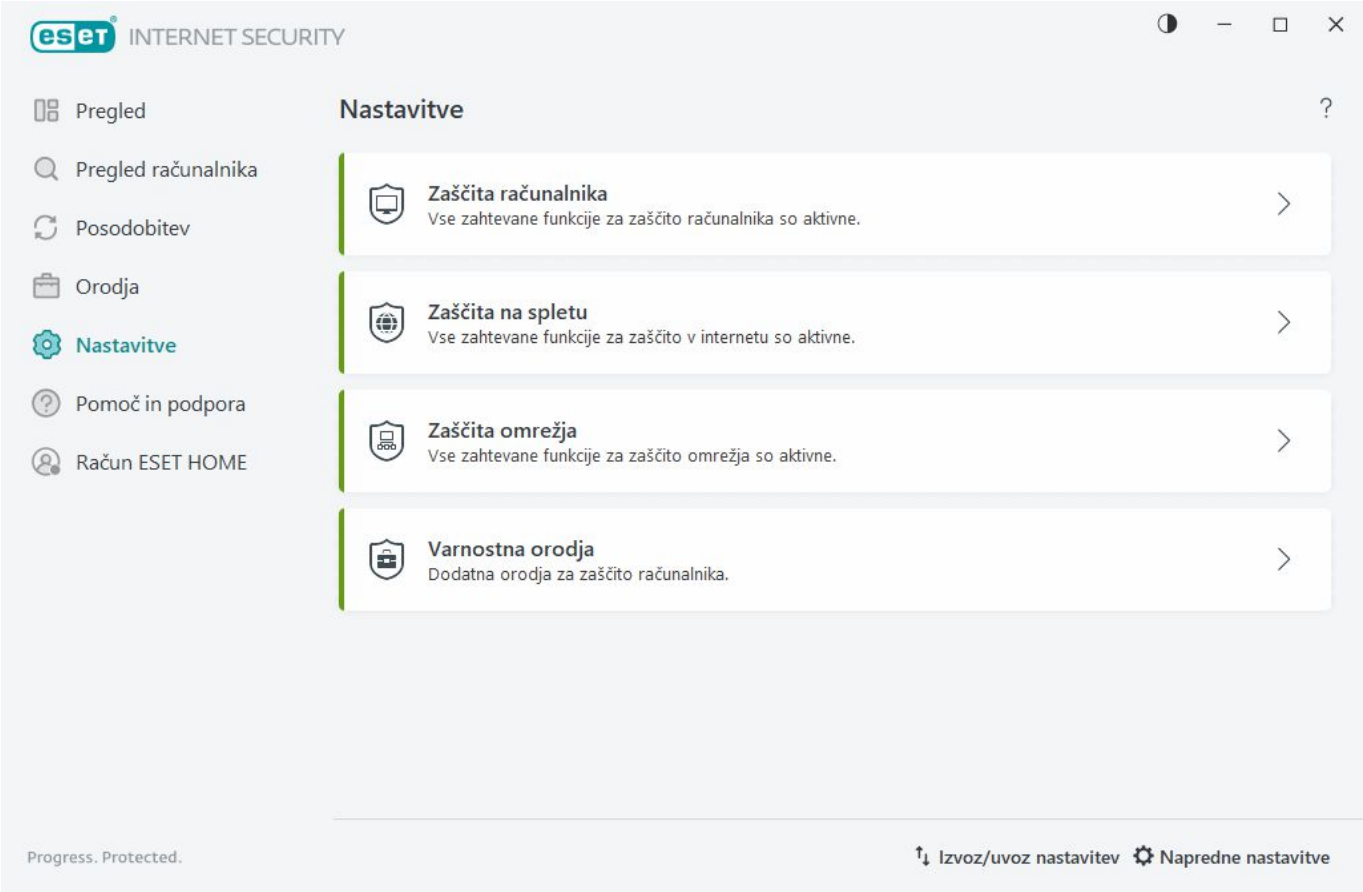
Izberi vzorec za analizo – drugo

Uporabite ta obrazec, če datoteke ni mogoče razvrstiti kot **sumljivo datoteko** ali **napačno pozitivno prepoznavo**.

Razlog za pošiljanje datoteke – vnesite podroben opis in razlog za pošiljanje datoteke.

Nastavitve

Skupine razpoložljivih funkcij zaščite najdete v glavnem oknu programa > **Nastavitve**.



Meni **Nastavitve** sestavljajo naslednji razdelki:

Zaščita računalnika

Zaščita na spletu

Zaščita omrežja

Varnostna orodja

Na dnu okna z nastavitvami so na voljo dodatne možnosti. Kliknite Napredne nastavitve, da konfigurirate podrobnejše parametre za vsak modul. Uporabite možnost Uvoz/izvoz nastavitev, če želite naložiti parametre nastavitev s konfiguracijsko datoteko .xmlali shraniti trenutne parametre nastavitev v konfiguracijsko datoteko.

Zaščita računalnika

Za ogled pregleda vseh modulov zaščite kliknite **Zaščita računalnika** v glavnem oknu programa > **Nastavitve**:

- Nadzorovanje datotečnega sistema – v vseh datotekah preveri prisotnost zlonamerne kode, ko jih odprete, ustvarite ali izvajate.

- Nadzor naprav – s tem modulom lahko pregledate, blokirate ali prilagodite razširjene filtre/dovoljenja in izberete način, kako bo uporabnik dostopal do naprave in jo uporabljal (CD/DVD/USB itn.).

- HIPS – sistem HIPS nadzira dogodke v operacijskem sistemu in se nanje odziva v skladu s prilagojenim

nizom pravil.

- Način za igranje – omogoči ali onemogoči Način za igranje. Ko omogočite način za igranje, prejmete sporočilo z opozorilom (morebitno varnostno tveganje) in glavno okno se obarva oranžno.

- Zaščita spletne kamere – nadzira postopke in programe, ki dostopajo do spletne kamere.

Če želite začasno ustaviti ali onemogočiti posamezne module zaščite, kliknite ikono gumba za preklop  .

Izklop zaščitnih modulov lahko zmanjša raven zaščite računalnika.

Kliknite ikono zobnika zraven modula zaščite ter si tako zagotovite dostop do naprednih nastavitev za ta modul.

Za **Nadzorovanje datotečnega sistema** kliknite ikono zobnika in izberite eno od naslednjih možnosti:

- **Konfiguriraj** – odpre napredne nastavitve nadzorovanja datotečnega sistema.

- **Uredi izključitve** – odpre okno z nastavitvami izključitev, tako da lahko datoteke in mape izključite iz pregledovanja.

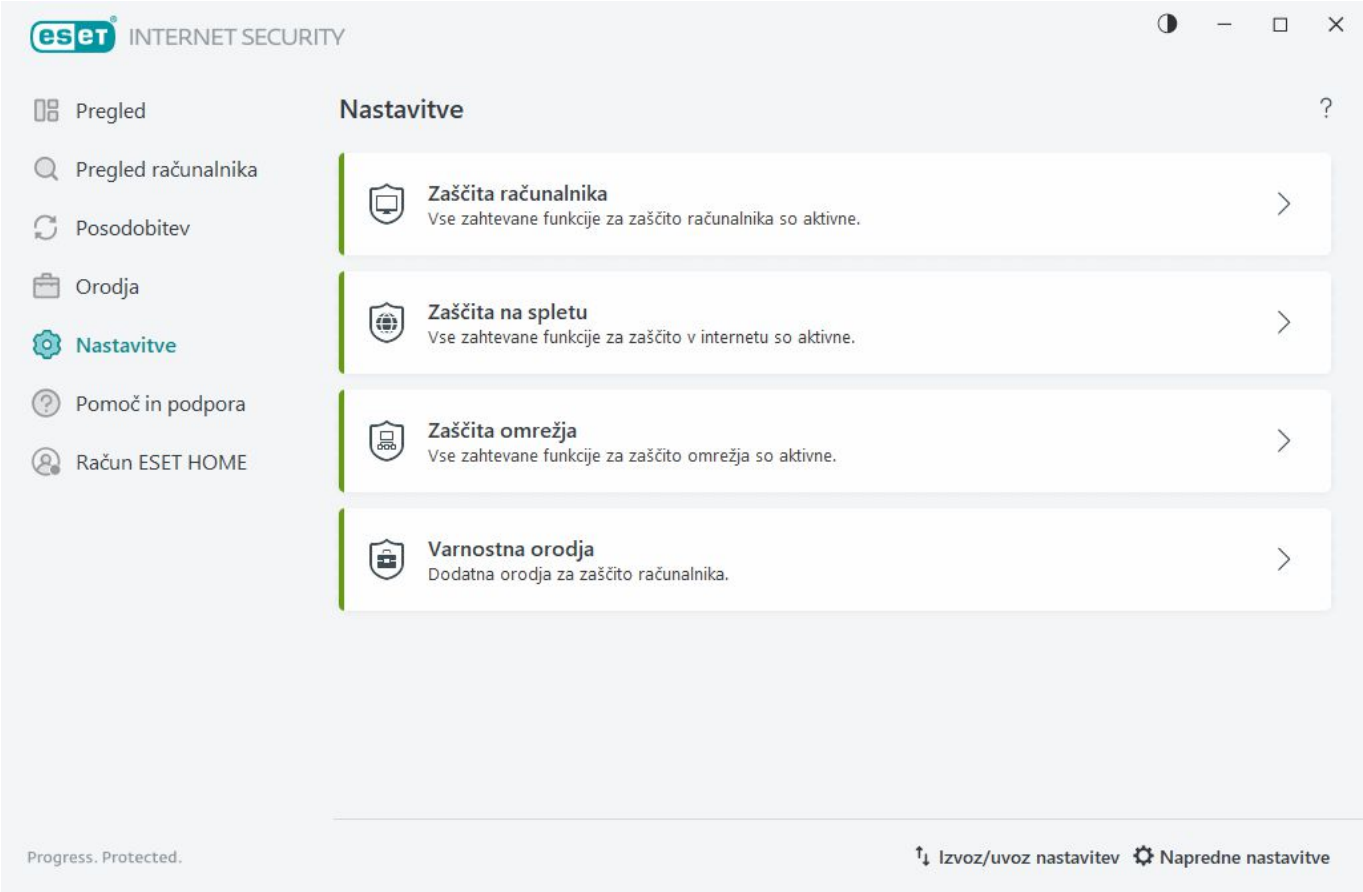
Za možnost **Zaščita spletne kamere** kliknite ikono zobnika in izberite eno od naslednjih možnosti:

- **Konfiguriraj** – odpre napredne nastavitve zaščite spletne kamere.

- **Blokiraj ves dostop do ponovnega zagona** – blokira dostop do spletne kamere, dokler se računalnik znova ne zažene.

- **Trajno blokiraj ves dostop** – blokira dostop do spletne kamere, dokler ta nastavitev ni onemogočena.

- **Prenehaj blokirati vse dostope** – onemogoči možnost blokiranja dostopa do spletne kamere. Ta možnost je na voljo samo, če je dostop do spletne kamere blokiran.



Začasno onemogoči protivirusno in protivohunsko zaščito – onemogoči vse module protivirusne in protivohunske zaščite. Ko onemogočite zaščito, se odpre okno, v katerem lahko v spustnem meniju **Časovni interval** določite, kako dolgo naj bo zaščita onemogočena. To možnost uporabite samo, če ste izkušeni uporabnik ali če imate pooblastila tehnične podpore družbe ESET.

Zaznana je infiltracija

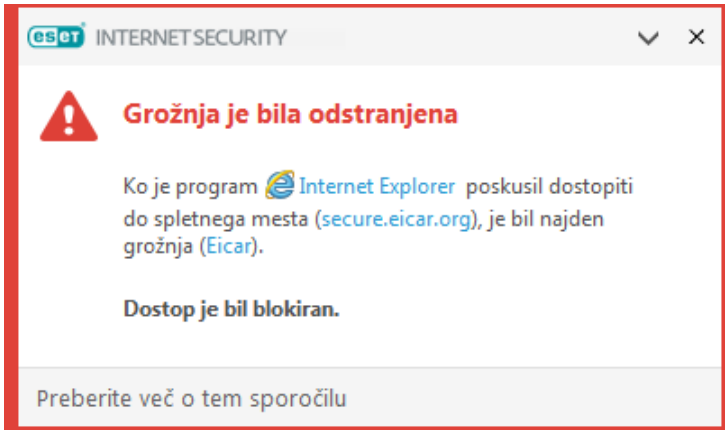
Infiltracije lahko pridejo v sistem iz različnih vstopnih mest, na primer s spletnih strani, iz map v skupni rabi, po e-pošti ali iz izmenljivih naprav (USB-jev, zunanjih diskov, CD-jev, DVD-jev, disket itd.).

Standardno delovanje

Če vzamemo splošen primer obravnave infiltracij s programom ESET Internet Security, so infiltracije zaznane na te načine:

- Sprotna zaščita datotečnega sistema
- Zaščita spletnega dostopa
- Zaščita e-poštnega odjemalca
- Pregled računalnika na zahtevo

Vsak od naštetih načinov uporablja standardno raven čiščenja in bo poskusil očistiti datoteko in jo premaknil v karanteno oz. prekinil povezavo. V območju obvestil v spodnjem desnem kotu zaslona se prikaže okno z obvestilom. Za podrobne informacije o zaznanih/očiščenih elementih si oglejte dnevniške datoteke. Če želite več informacij o ravneh čiščenja in delovanju, glejte razdelek Raven čiščenja.



Pregledovanje, ali računalnik vsebuje okužene datoteke

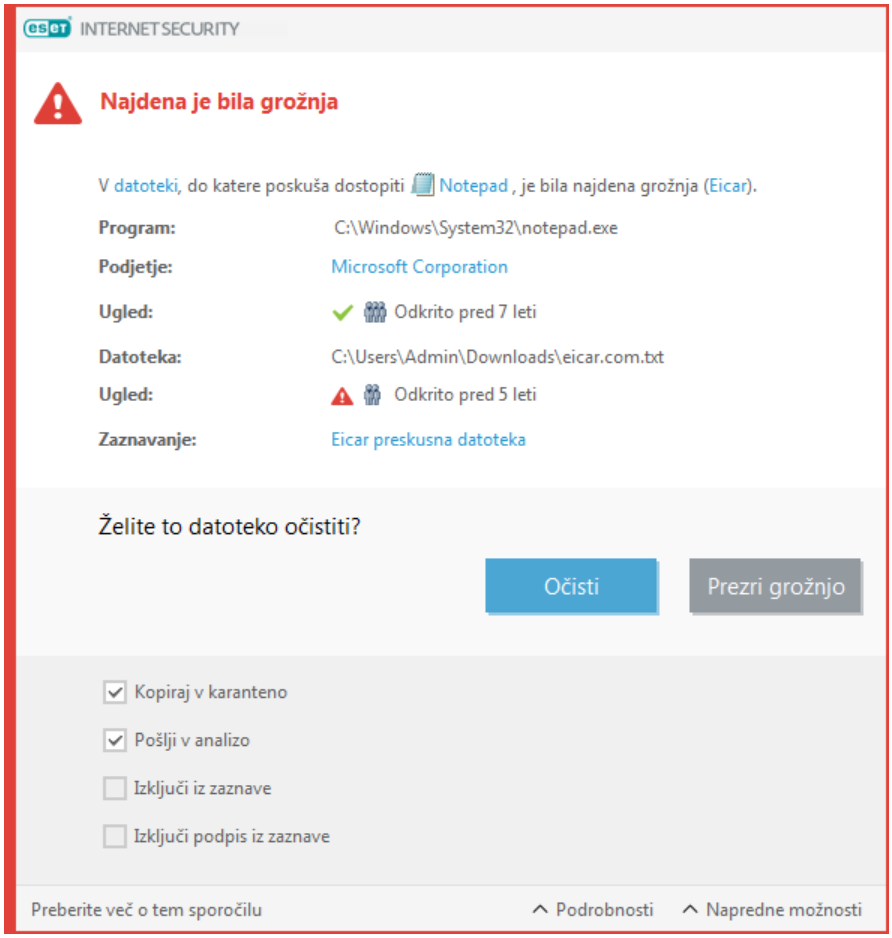
Če menite, da je v vašem računalniku prišlo do okužbe z zlonamerno programsko opremo, na primer, če računalnik deluje počasneje, pogosto zamrzne itn., vam priporočamo, da naredite to:

1. Odprite ESET Internet Security in kliknite **Pametni pregled**.
2. Kliknite **Preglejte računalnik** (več informacij najdete v razdelku Pametni pregled).
3. Ko je pregled končan, v dnevniku preverite, koliko datotek je pregledanih, okuženih in očiščenih.

Če želite pregledati le določeni del diska, izberite možnost **Pregled po meri** in izberite cilje, ki jih želite pregledati in ugotoviti, ali so v njih virusi.

Čiščenje in brisanje

Če v sprotni zaščiti datotečnega sistema ni vnaprej določenega dejanja, ki naj se izvede, vas bo program pozval, da v oknu z opozorilom izberete poljubno možnost. Običajno so na voljo možnosti **Očisti**, **Izbriši** in **Pusti**. Priporočamo, da možnosti **Pusti** ne izberete, saj bodo tako okužene datoteke ostale neočiščene. To možnost izberite le, če ste prepričani, da taka datoteka ni nevarna in da je bila zaznana pomotoma.



Če je datoteko napadel virus in ji priložil zlonamerno kodo, uporabite čiščenje. V tem primeru najprej poskusite očistiti okuženo datoteko, da bi obnovili njeno prvotno stanje. Če je vsebina datoteke izključno zlonamerna koda, bo datoteka izbrisana.

Če je okužena datoteka »zaklenjena« ali jo uporablja sistemski proces, jo program običajno le izbriše, potem ko ni več zaklenjena ali v uporabi (običajno po vnovičnem zagonu sistema).

Obnavljanje iz karantene

Dostop do karantene je mogoč iz glavnega okna programa ESET Internet Security tako, da kliknete **Orodja** > **Karantena**.

Datoteke iz karantene je mogoče obnoviti na njihovo prvotno lokacijo:

- V ta namen uporabite funkcijo **Obnovi**, ki je na voljo v priročnem meniju, ko v karanteni z desno tipko miške kliknete določeno datoteko.
- Če je datoteka označena kot morebitno neželen program, je možnost **Obnovi in izključi iz pregledovanja** omogočena. Glejte tudi Izključitve.
- Priročni meni vsebuje tudi možnost **Obnovi v**, s katero lahko obnovite datoteko na drugo mesto in ne na prvotno lokacijo, s katere je bila izbrisala.
- Funkcija obnovitve v nekaterih primerih ni na voljo, na primer za datoteke, ki so bile locirane na omrežnem pogonu samo za branje.

Več groženj

Če med pregledom računalnika katera od okuženih datotek ni bila očiščena (ali pa je bila možnost Raven čiščenja nastavljena na **Brez čiščenja**), se prikaže okno z opozorilom, ki vas poziva, da izberete dejanja za te datoteke. Izberite dejanja za datoteke (dejanja so nastavljena posamezno za vsako datoteko na seznamu) in nato kliknite **Dokončaj**.

Brisanje datotek v arhivih

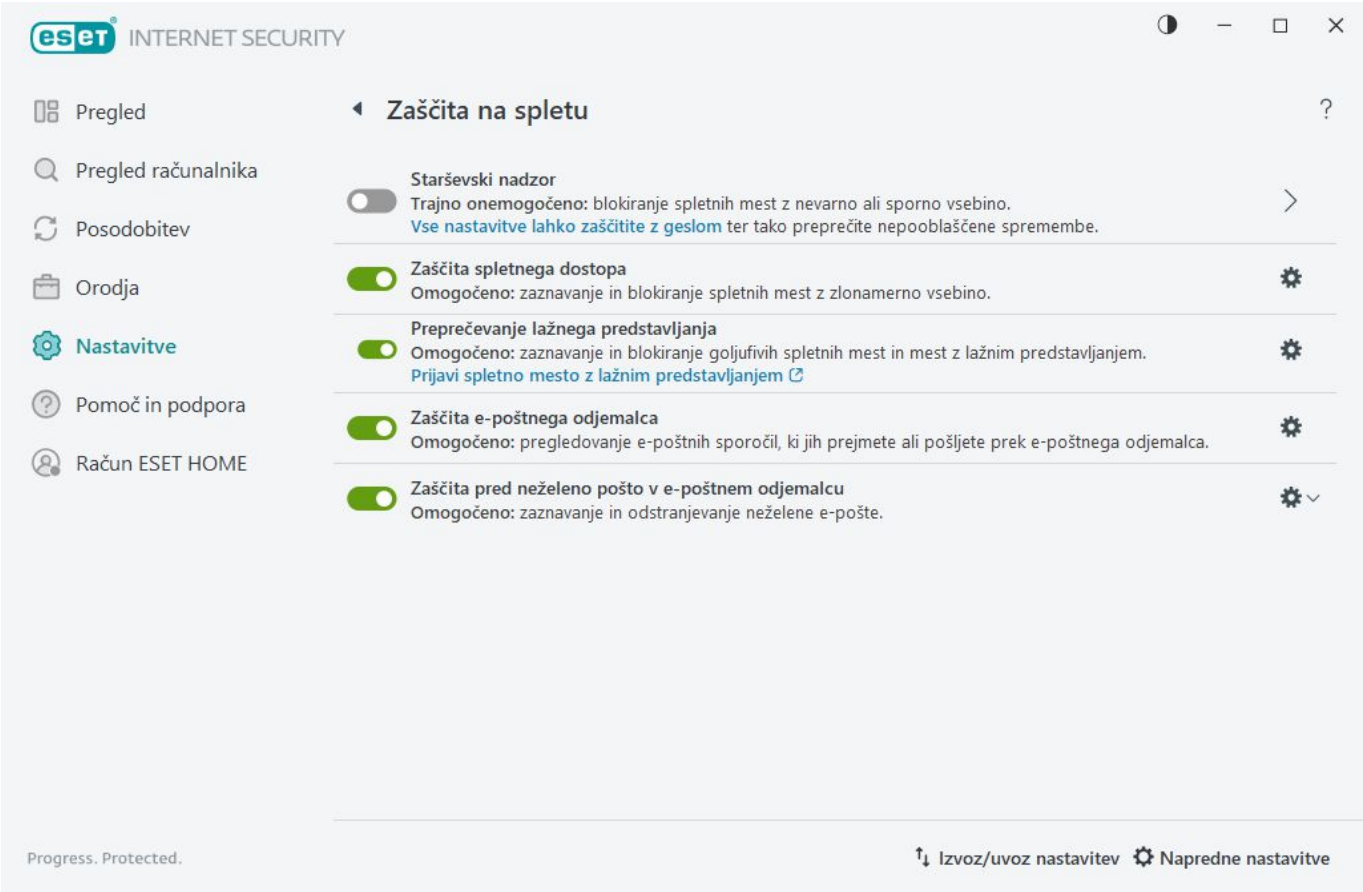
V privzetem načinu čiščenja bo celoten arhiv izbrisan le, če so v njem okužene datoteke in nobene čiste datoteke. To pomeni, da arhivi niso izbrisani, če so v njih tudi čiste datoteke, ki niso nevarne. Pri izvajanju strogega čiščenja bodite previdni – če je možnost strogega čiščenja omogočena, to pomeni, da bodo arhivi izbrisani, če je v njih vsaj ena okužena datoteka ne glede na stanje drugih datotek v posameznem arhivu.

Zaščita na spletu

Internetna povezljivost je standardna funkcija osebnega računalnika. Na žalost je postala tudi glavni način za prenos zlonamerne kode. Odprite glavno okno programa > **Nastavitve** > **Zaščita na spletu**, da konfigurirate funkcije v ESET Internet Security, ki povečajo vašo zaščito na spletu.

Če želite začasno ustaviti ali onemogočiti posamezne module zaščite, kliknite ikono gumba za preklop .

Izklop zaščitnih modulov lahko zmanjša raven zaščite računalnika.



Kliknite ikono zobnika zraven modula zaščite ter si tako zagotovite dostop do naprednih nastavitev za ta

modul.

Modul starševskega nadzora ščiti vaše otroke tako, da v spletu blokira neprimerno ali škodljivo vsebino.

Zaščita spletnega dostopa pregleda komunikacijo HTTP/HTTPS za zlonamerno programsko opremo in lažno predstavljanje. Za odpravljanje težav je treba izklopiti zaščito spletnega dostopa.

Preprečevanje lažnega predstavljanja omogoča blokiranje spletnih strani, za katere je znano, da posredujejo vsebino lažnega predstavljanja. Priporočamo, da pustite funkcijo preprečevanja lažnega predstavljanja omogočeno.

Prijavi spletno mesto z lažnim predstavljanjem – prijavite spletno mesto z lažnim predstavljanjem/zlonamerno spletno mesto družbi ESET za analizo.

> Preden pošljete spletno mesto družbi ESET, mora izpolnjevati enega od teh pogojev:
> • Spletnega mesta ni bilo mogoče zaznati.
> • Spletno mesto je nepravilno zaznano kot grožnja. V tem primeru lahko prijavite nepravilno blokirane strani.

Zaščita e-poštnega odjemalca omogoča nadzor nad e-poštno komunikacijo, prejeto prek protokolov POP3(S) in IMAP(S). Če uporabljate vtičnik za svojega e-poštnega odjemalca, omogoča program ESET Internet Security nadzor nad celotno komunikacijo tega e-poštnega odjemalca.

Zaščita pred neželeno pošto v e-poštnem odjemalcu filtrira vsiljena e-poštna sporočila.

Za možnost **Zaščita pred neželeno pošto v e-poštnem odjemalcu** kliknite ikono zobnika in izberite eno od naslednjih možnosti:

- **Konfiguriranje** – odpre napredne nastavitve za zaščito pred neželeno pošto v e-poštnem odjemalcu.
- **Seznam naslovov uporabnika** (če je omogočen) – odpre pogovorno okno, v katerega lahko dodate, uredite ali izbrišete naslove, da določite pravila za preprečevanje neželene pošte. Pravila na tem seznamu bodo veljala za trenutnega uporabnika.
- **Globalni seznam naslovov** (če je omogočen) – odpre pogovorno okno, v katerega lahko dodate, uredite ali izbrišete naslove, da določite pravila za preprečevanje neželene pošte. Pravila na tem seznamu bodo veljala za vse uporabnike.

Preprečevanje lažnega predstavljanja

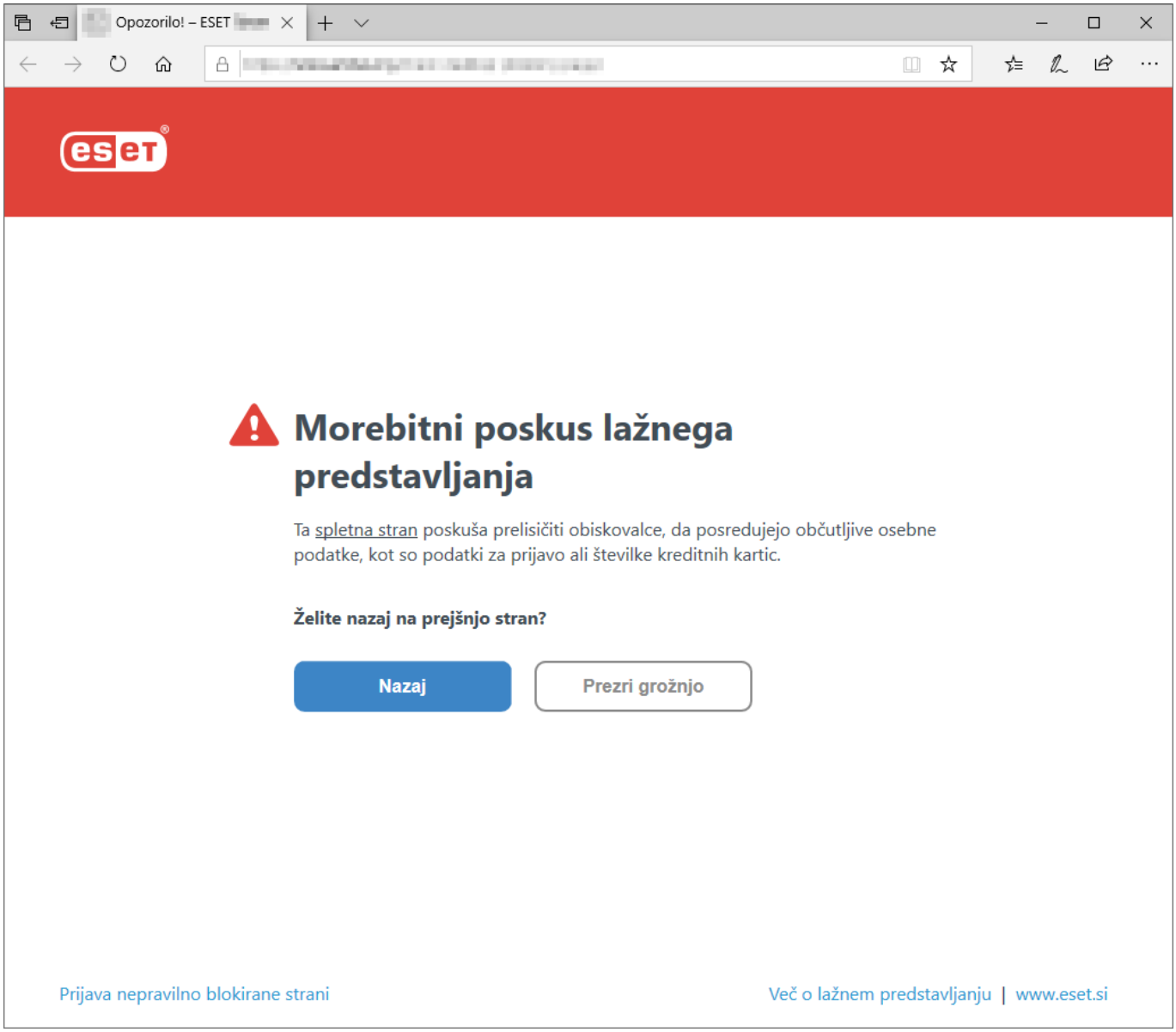
Lažno predstavljanje je kazniva dejavnost s tehnikami socialnega inženiringa (preračunljivo ravnanje z uporabniki, da bi prišli do zaupnih informacij). Lažno predstavljanje se uporablja za dostop do občutljivih podatkov, kot so številke bančnih računov, številke PIN itd. Za več informacij glejte slovar izrazov. ESET Internet Security zagotavlja zaščito pred preprečevanjem lažnega predstavljanja, ki lahko blokira spletne strani, za katere je znano, da posredujejo to vrsto vsebine.

Zaščita pred preprečevanjem lažnega predstavljanja je privzeto omogočena. To nastavitev je mogoče konfigurirati v razdelku Napredne nastavitve > **Zaščite** > **Zaščita spletnega dostopa**.

Za več informacij o preprečevanju lažnega predstavljanja v programu ESET Internet Security preberite članek v naši zbirki znanja.

Dostop do spletnega mesta z lažnim predstavljanjem

Ko odprete spletno mesto s prepoznanim lažnim predstavljanjem, se v spletnem brskalniku prikaže naslednje pogovorno okno. Če kljub temu želite dostopati do spletnega mesta, kliknite **Prezri grožnjo** (ni priporočeno).



Morebitna spletna mesta z lažnim predstavljanjem, ki so na seznamu varnih pošiljateljev, privzeto potečejo po nekaj urah. Spletno mesto lahko trajno dovolite z orodjem Upravljanje naslovov URL. V polju Napredne nastavitve > **Zaščite** > **Zaščita spletnega dostopa** > **Upravljanje naslovov URL** > **Seznam naslovov** > **Uredi** ter dodajte spletno mesto, ki ga želite urediti, na ta seznam.

Prijavi spletno mesto z lažnim predstavljanjem

Povezava **Prijava nepravilno blokirane strani** omogoča da prijavo spletnega mesta, ki je nepravilno zaznano kot grožnja.

Spletno mesto pa lahko pošljete tudi po e-pošti. Svoj e-poštni naslov pošljite na samples@eset.com. Ne pozabite dodati zadeve z opisom in priložite čim več informacij o spletnem mestu (navedite na primer spletno mesto, s katerega ste ga odprli, kako ste izvedeli za to mesto itn.).

Starševski nadzor

V modulu starševskega nadzora lahko konfigurirate nastavitve starševskega nadzora. Starši imajo tako na voljo avtomatizirana orodja, s katerimi lahko zaščitijo otroke in nastavijo omejitve za naprave in storitve. Cilj je otrokom in mladoletnim osebam preprečiti dostop do strani z neustrezno ali škodljivo vsebino.

S starševskim nadzorom lahko blokirate spletne strani, na katerih je lahko potencialno žaljiva vsebina. Poleg tega lahko starši preprečijo dostop do več kot 40 vnaprej določenih kategorij spletnih mest in več kot 140 podkategorij.

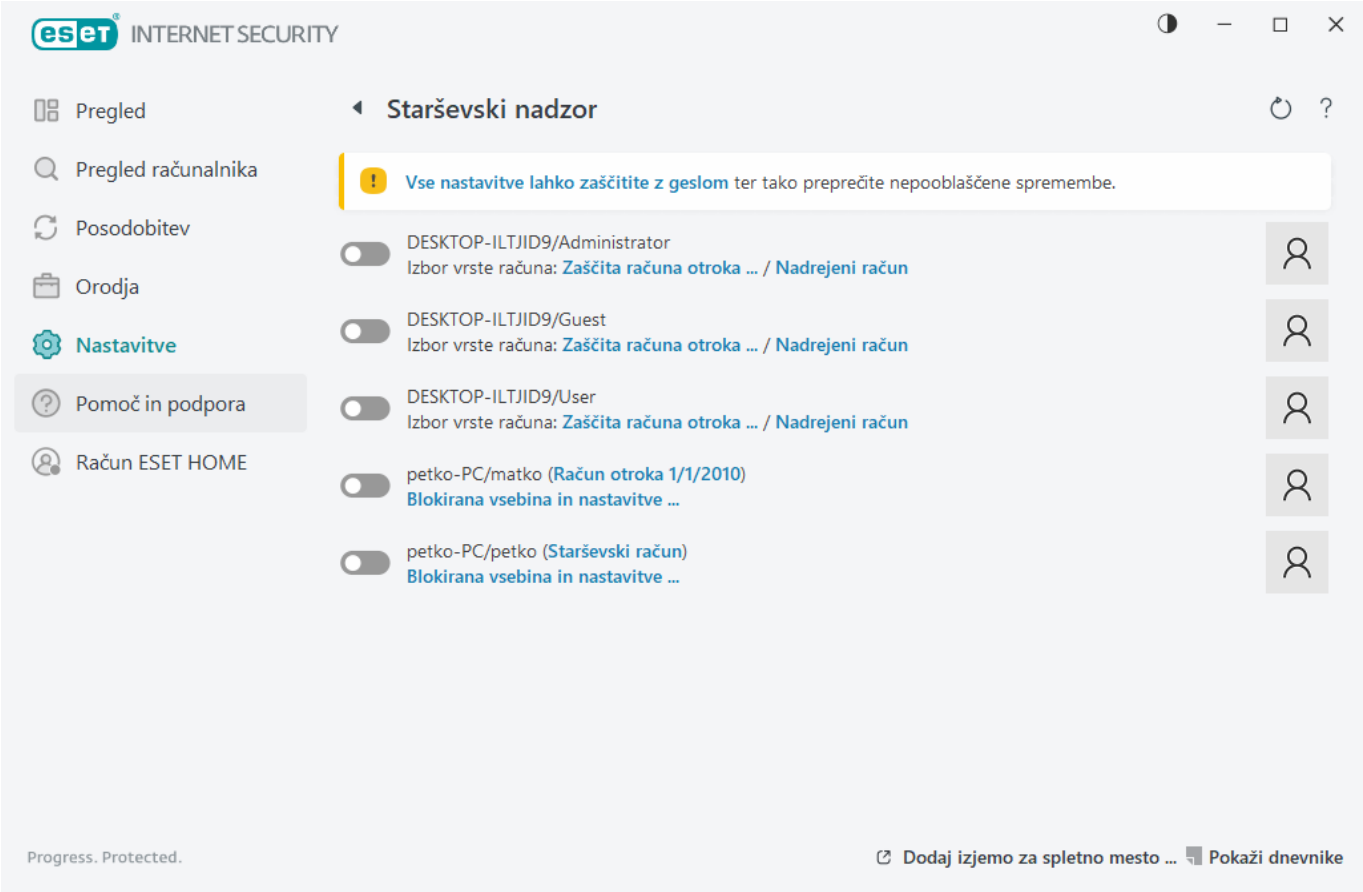
Če želite aktivirati starševski nadzor določenega uporabniškega računa, sledite spodnjim navodilom:

1. Starševski nadzor je privzeto onemogočen v programu ESET Internet Security. Starševski nadzor lahko aktivirate na dva načina:

   • V glavnem oknu programa kliknite ikono gumba za preklop v razdelku **Nastavitve** > **Zaščita na spletu** > **Starševski nadzor** in spremenite stanje starševskega nadzora na omogočeno.

   • Odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita spletnega dostopa** > **Starševski nadzor** in nato omogočite gumb za preklop zraven možnosti **Omogoči starševski nadzor**.

2. V glavnem oknu programa kliknite **Nastavitve** > **Zaščita na spletu** > **Starševski nadzor**. Čeprav je ob možnosti **Starševski nadzor** prikazano **Omogočeno**, morate konfigurirati starševski nadzor za želeni račun tako, da kliknete simbol puščice in nato v naslednjem oknu izberete **Zaščita računa otroka** ali **Nadrejeni račun**. V naslednjem oknu izberite rojstni datum, da določite raven dostopa in priporočene spletne strani, primerne za določeno starost. Starševski nadzor je omogočen za navedeni uporabniški račun. Pod imenom računa kliknite **Blokirana vsebina in nastavitve**, da prilagodite kategorije, ki jih želite dovoliti ali blokirati na zavihku Kategorije. Če želite dovoliti ali blokirati spletne strani po meri, ki se ne ujemajo s kategorijo, kliknite zavihek Izjeme.



Če kliknete **Nastavitve** > **Zaščita na spletu** > **Starševski nadzor** v glavnem oknu izdelka ESET Internet Security, se bo v glavnem oknu prikazalo naslednje:

Uporabniški računi sistema Windows

Če ste ustvarili vlogo za obstoječi račun, bo prikazan tukaj. Kliknite gumb za preklop tako, da se prikaže zelena kljukica poleg možnosti Starševski nadzor za račun. V aktivnem računu kliknite Blokirana vsebina in nastavitve za ogled seznama dovoljenih kategorij spletnih strani za ta račun ter blokiranih in dovoljenih spletnih strani.

Spodnji del okna vsebuje naslednje:

Dodaj izjemo za spletno mesto – posamezno spletno mesto lahko dovolite ali blokirate po svojih željah za vsak starševski račun posebej.

Pokaži dnevnike – funkcija pokaže dnevnik s podrobnimi podatki dejavnosti starševskega nadzora (blokirane strani, račun, za katerega je bila stran blokirana, kategorijo itn.). Ta dnevnik lahko tudi filtrirate glede na izbrane pogoje, in sicer tako, da kliknete **Filtriranje**.

Starševski nadzor

Ko onemogočite starševski nadzor, se pojavi okno **Onemogoči starševski nadzor**. Tukaj lahko nastavite časovni interval, v katerem bo onemogočena zaščita. Možnost se nato spremeni v **Začasno ustavljeno** ali **Trajno onemogočeno**.

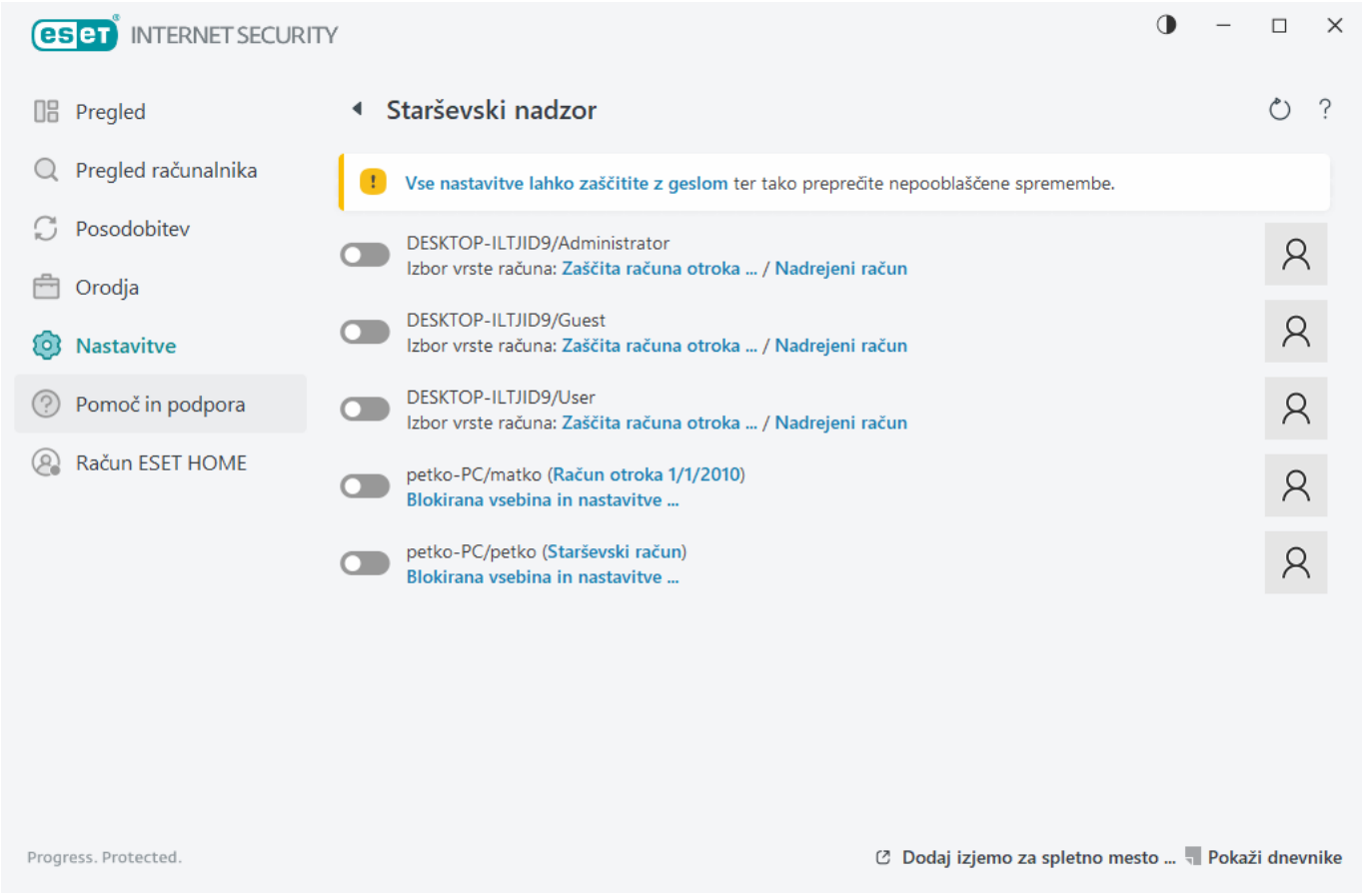
Pomembno je, da nastavitve v programu ESET Internet Security zaščitite z geslom. Geslo lahko nastavite v

razdelku Nastavitve dostopa. Če geslo ni nastavljeno, se bo prikazalo naslednje opozorilo – **Zaščitite vse nastavitve z geslom**, da preprečite nepooblaščene spremembe. Omejitve, nastavljene v starševskem nadzoru, vplivajo le na standardne uporabniške račune. Skrbnik lahko preglasi vsako omejitev, zato omejitve ne bodo vplivale na skrbnike.

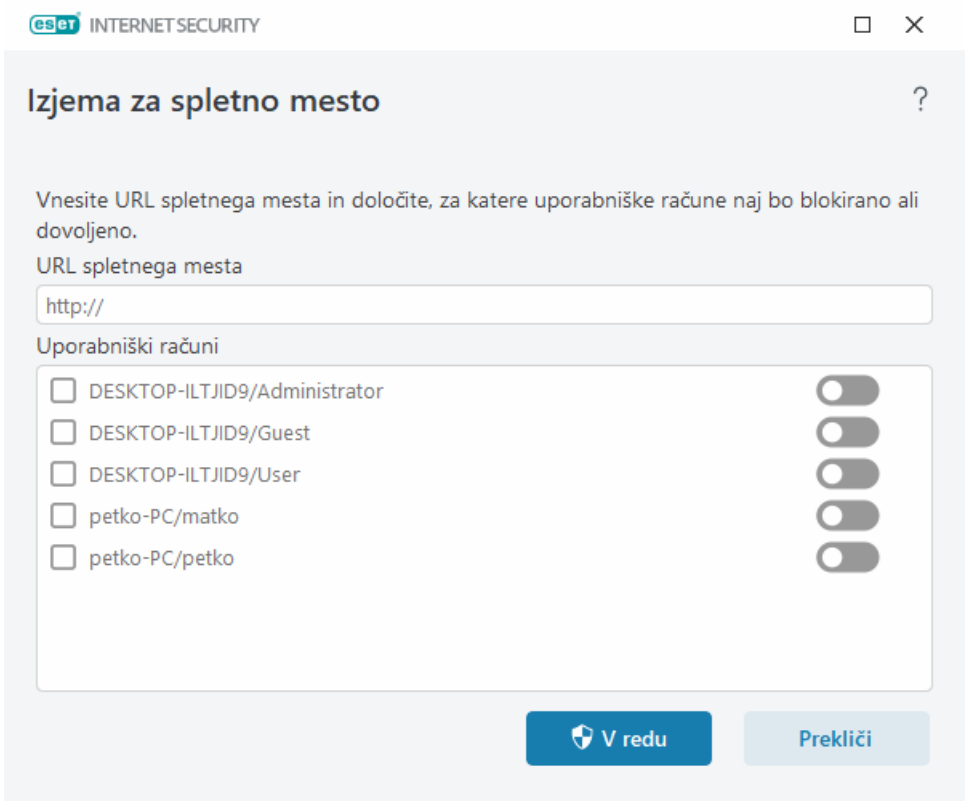
Starševski nadzor za pravilno delovanje zahteva omogočanje možnosti Pregledovalnik omrežnega prometa, Pregledovanje prometa protokola HTTPS in Požarni zid. Vse te funkcije so privzeto omogočene.

Izjeme za spletno mesto

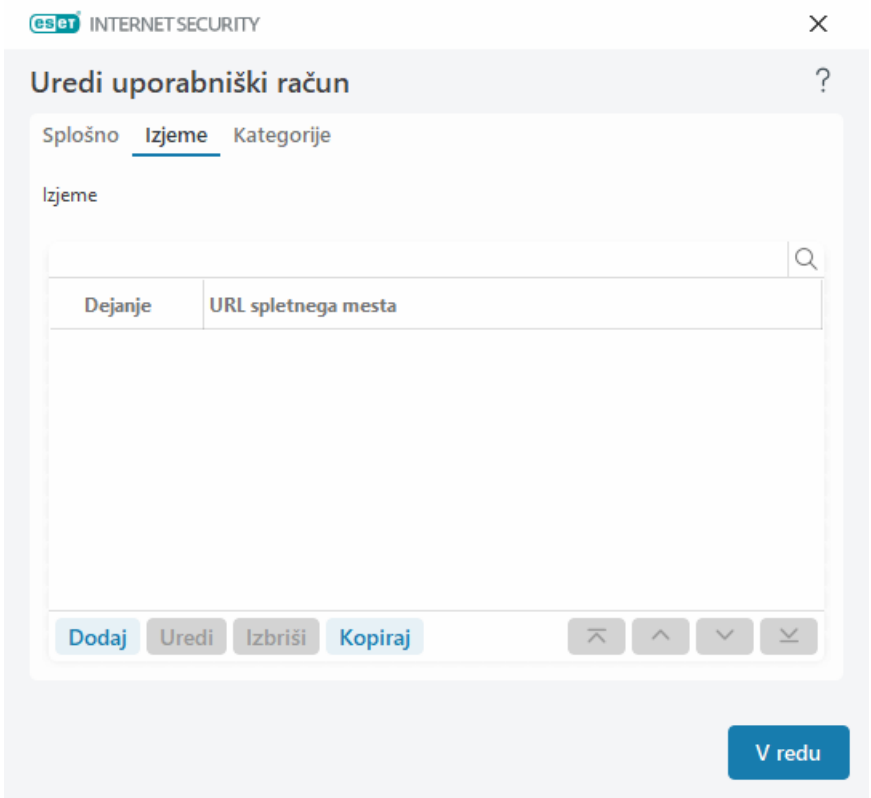
Če želite za spletno mesto dodati izjemo, kliknite **Nastavitve** > **Zaščita na spletu** > **Starševski nadzor** in nato kliknite **Dodaj izjemo za spletno mesto**.



V polje **URL spletnega mesta** vnesite URL in izberite (dovoljeno) ali (blokirano) za vsak posamezni uporabniški račun, nato pa kliknite možnost **V redu**, da ga dodate na seznam.



Če želite s seznama izbrisati naslov URL, kliknite **Nastavitve** > **Zaščita na spletu** > **Starševski nadzor**, nato pod želenim uporabniškim računom kliknite **Blokirana vsebina in nastavitve** in kliknite zavihek **Izjema** ter izberite izjemo, nato kliknite **Odstrani**.



Na seznamu spletnih naslovov ni mogoče uporabiti posebnih simbolov »*« (zvezdice) in »?« (vprašaja). Naslove spletnih strani z več domenami najvišje ravni je denimo treba vnesti ročno (*examplepage.com*, *examplepage.sk* itd.). Ko na seznam dodate domeno, bo vsa vsebina te domene in poddomen (npr. *sub.examplepage.com*) blokirana ali dovoljena glede na izbrano dejanje na osnovi URL-ja.

Blokiranje ali dovoljevanje določenih spletnih strani je lahko bolj natančno od blokiranja ali dovoljevanja kategorije spletnih strani. Bodite previdni, ko spreminjate te nastavitve in dodajate kategorijo/spletno stran na seznam.

Kopiraj izjeme iz uporabnika

Izberite uporabnika v spustnem meniju, iz katerega želite kopirati ustvarjeno izjemo.

Kopiraj kategorije iz računa

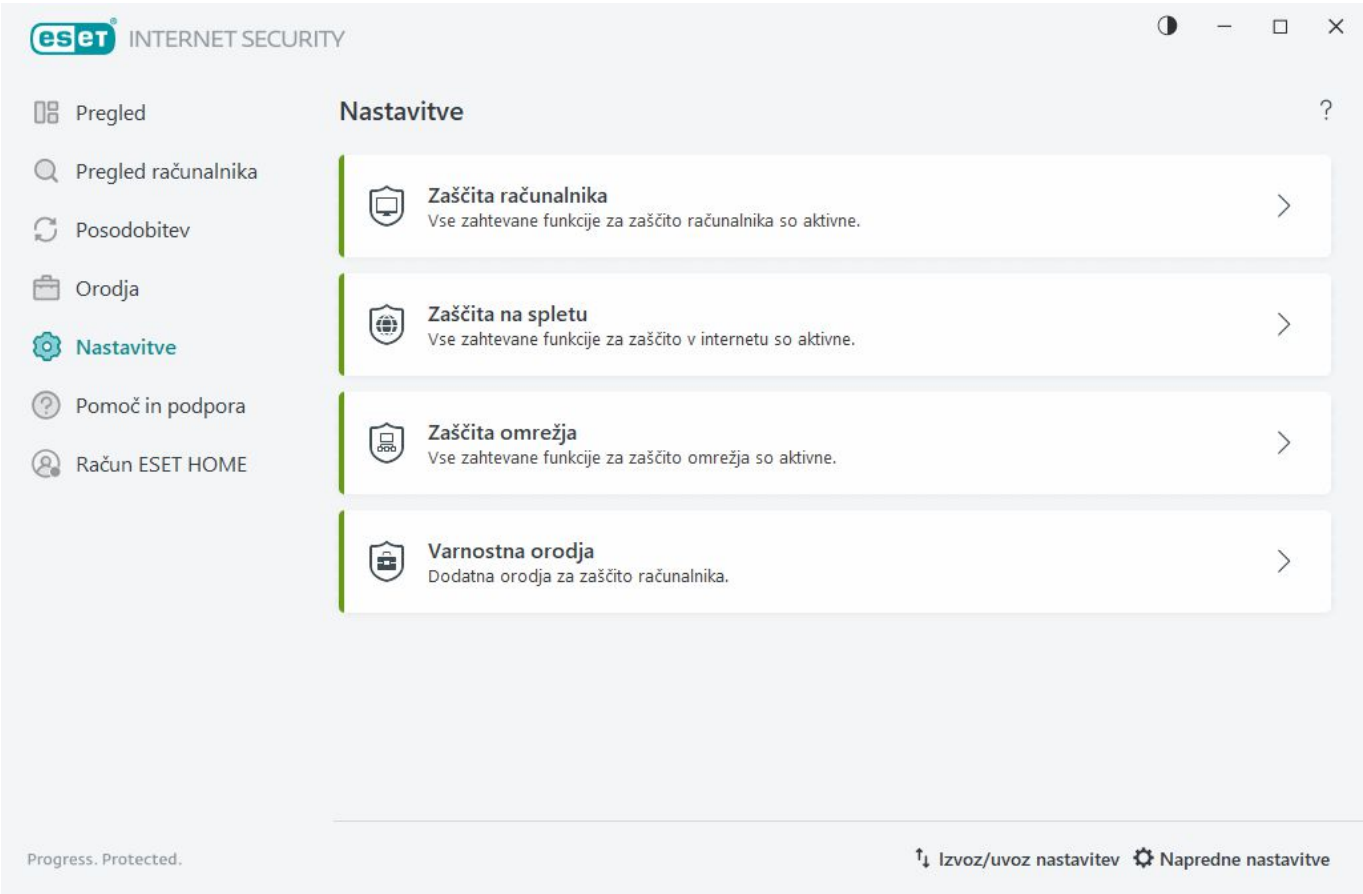
Ta možnost omogoča kopiranje seznama blokiranih ali dovoljenih kategorij iz obstoječega spremenjenega računa.

Zaščita omrežja

Odprite glavno okno programa > **Nastavitve** > **Zaščita omrežja**, da konfigurirate osnovne nastavitve zaščite omrežja ali odpravite težave z omrežno komunikacijo.

Če želite začasno ustaviti ali onemogočiti posamezne module zaščite, kliknite ikono gumba za preklop .

Izklop zaščitnih modulov lahko zmanjša raven zaščite računalnika.



Kliknite ikono zobnika zraven modula zaščite ter si tako zagotovite dostop do naprednih nastavitev za ta modul.

Požarni zid – filtrira vso omrežno komunikacijo na podlagi konfiguracije ESET Internet Security.

Konfiguriranje – odpre Napredne nastavitve požarnega zidu, kjer lahko določite, kako bo požarni zid obravnaval omrežno komunikacijo.

Začasno onemogoči požarni zid (dovoli ves promet) – vse možnosti filtriranja požarnega zidu in tako omogočite vse dohodne in odhodne povezave. Kliknite **Omogoči požarni zid**, da znova omogočite požarni zid, ko je »Filtriranje omrežnega načina« v tem načinu.

Blokiraj ves promet – požarni zid blokira vso dohodno in odhodno komunikacijo. To možnost uporabite le, če sumite, da morate zaradi hudih varnostnih tveganj prekiniti povezavo sistema z omrežjem. Ko je »Filtriranje omrežnega prometa« v načinu **Ves promet je blokiran**, kliknite možnost **Prenehaj blokirati ves promet**, da povrnete normalno delovanje požarnega zidu.

Samodejni način – (ko je omogočen drug način filtriranja) – kliknite, da način filtriranja spremenite v samodejni način (s pravili, ki jih je določil uporabnik).

Interaktivni način – (ko je omogočen drug način filtriranja) – kliknite, da način filtriranja spremenite v interaktivni način.

Zaščita pred napadi iz omrežja (IDS) – analizira vsebino omrežnega prometa in ščiti pred napadi iz omrežja. Ves promet, ki bi lahko bil škodljiv, se blokira. ESET Internet Security vas obvesti, ko je vzpostavljena povezava z nezaščitenim brezžičnim omrežjem ali s slabo zaščitenim omrežjem.

Zaščita pred omrežjem okuženih računalnikov – hitro in natančno poišče zlonamerno programsko opremo v sistemu.

Omrežne povezave – prikaže omrežja, s katerimi so povezane omrežne kartice, s podrobnimi informacijami.

Razrešitev blokirane komunikacije – pomaga odpraviti težave s povezljivostjo, ki jih povzroča požarni zid ESET. Za več podrobnih informacij glejte razdelek Čarovnik za odpravljanje težav.

Razrešitev začasno blokiranih naslovov IP – Oglejte si seznam naslovov IP, ki so bili zaznani kot vir napadov in dodani na seznam blokiranih naslovov, zaradi česar je povezava z njimi nekaj časa blokirana.

Pokaži dnevnike – odpre dnevniško datoteko zaščite omrežja.

Omrežne povezave

Prikaže omrežja, s katerimi so povezane omrežne kartice. Za ogled omrežnih povezav odprite glavno okno programa > **Nastavitve** > **Zaščita omrežja** > **Omrežne povezave**.

Dvakrat kliknite povezavo na seznamu, da prikažete podrobnosti in podrobnosti omrežne kartice.

Pomaknite se na določeno omrežno povezavo in kliknite ikono menija ⋮ v stolpcu **Vredno zaupanja**, da izberete eno od naslednjih možnosti:

- **Uredi** – odpre okno Konfiguriranje zaščite omrežja, v katerem lahko določenemu omrežju dodelite profil zaščite omrežja
- **Pozabi** – ponastavi konfiguracijo omrežne povezave na privzeto
- **Pregled omrežja z modulom Nadzornik omrežja** – odpre modul Nadzornik omrežja za zagon pregleda

omrežja

- **Označi kot »Moje omrežje«** – omrežju doda oznako »Moje omrežje«; ta oznaka bo prikazana poleg omrežja v programu ESET Internet Security za lažje prepoznavanje in varnostni pregled
- **Odstrani oznako »Moje omrežje«** – odstrani oznako »Moje omrežje«; na voljo samo, če je omrežje že označeno

Podrobnosti omrežne povezave

Dvakrat kliknite povezavo na seznamu omrežnih povezav, da prikažete podrobnosti skupaj s podrobnostmi omrežne kartice. Podrobnosti o omrežni povezavi in kartici vam lahko pomagajo prepoznati omrežje, ki ga skušate konfigurirati v zaščiti omrežnega dostopa.

Podrobnosti omrežne povezave:

- Stanje omrežne povezave
- Datum in ura prvega zaznavanja omrežja
- Zadnja aktivnost omrežja
- Skupni čas, porabljen v tem omrežju
- Profil omrežnih povezav
- Profil omrežne povezave, določen v sistemu Windows
- Konfiguracija zaščite omrežja (ali je omrežje zaupanja vredno)

Podrobnosti omrežne kartice:

- Vrsta povezave (žična, navidezna itd.)
- Ime omrežnega vmesnika
- Opis omrežne kartice
- Naslov IP z naslovom MAC
- Naslov IPv4 in IPv6 omrežja s podomrežjem
- Pripona DNS
- IP strežnika DNS
- IP strežnika DHCP
- IP privzetega prehoda in naslov MAC
- Naslov MAC kartice

Odpravljanje težav z dostopom do omrežja

Čarovnik za odpravljanje težav vam pomaga odpraviti težave s povezljivostjo, ki jih povzroča požarni zid. **Odpravljanje težav z dostopom do omrežja** lahko najdete v glavnem oknu programa > **Nastavitve** > **Zaščita omrežja** > **Razrešitev blokirane komunikacije**.

Izberite, če želite prikazati komunikacijo, blokirano za **lokalne programe**, ali blokirano komunikacijo iz **oddaljenih naprav**.

V spustnem meniju izberite časovno obdobje, med katerim je bila komunikacija blokirana. Seznam nedavno blokiranih komunikacij omogoča vpogled v vrste programov ali naprav, ugled ter skupno število programov in naprav, ki so bili blokirani v tem časovnem obdobju. Če želite več informacij o blokiranih komunikacijah, kliknite **Podrobnosti**. Naslednji korak je, da odblokirate program ali napravo, v zvezi s katerim prihaja do težav s povezljivostjo.

Če kliknete **Odblokiraj**, dovolite predhodno blokirano komunikacijo. Če še naprej prihaja do težav v zvezi s programom oz. naprava ne deluje kot običajno, kliknite **ustvarjanje drugega pravila** in vsa predhodno blokirana komunikacija za to napravo bo zdaj dovoljena. Če težave ne morete odpraviti, znova zaženite računalnik.

Kliknite **Odpri pravila za požarni zid**, da si ogledate pravila, ki jih je ustvaril čarovnik. Pravila, ki jih je ustvaril čarovnik, si lahko ogledate tudi v možnosti Napredna nastavitev > **Zaščite** > **Zaščita omrežnega dostopa** > **Požarni zid** > **Pravila** > **Uredi**.

Če pravila ni mogoče ustvariti, se prikaže sporočilo o napaki. Kliknite **Poskusi znova** in ponovite postopek za odblokiranje komunikacije ali pa ustvarite drugo pravilo s seznama blokirane komunikacije.

Seznam začasno blokiranih naslovov IP

Če si želite ogledati naslove IP, ki so bili zaznani kot viri napadov in dodani na seznam blokiranih pošiljateljev, tako da je povezava z njimi za določeno časovno obdobje blokirana, odprite glavno okno programa > **Nastavitve** > **Zaščita omrežja** > **Razrešitev začasno blokiranih naslovov IP**. Začasno blokirani naslovi IP so blokirani 1 uro.

Stolpci

Naslov IP – prikaže naslov IP, ki je blokiran.

Razlog blokiranja – prikaže vrsto napada, ki je bil preprečen z naslova (na primer napad na pregled vrat TCP).

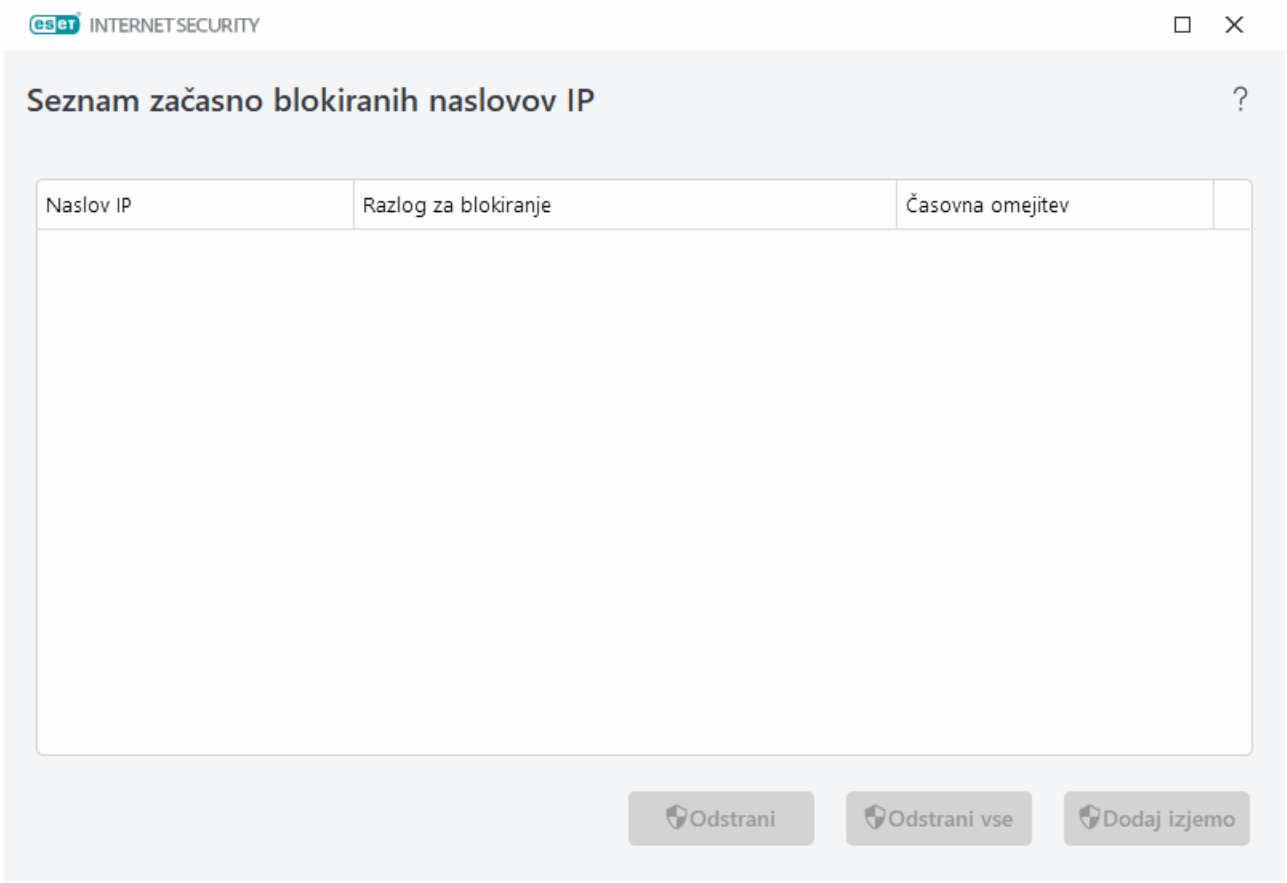
Časovna omejitev – prikaže čas in datum, ko bo naslov odstranjen s seznama blokiranih naslovov.

Elementi kontrolnika

Odstrani – kliknite, če želite odstraniti naslov s seznama blokiranih naslovov pred določenim datumom.

Odstrani vse – kliknite, če želite takoj odstraniti vse naslove s seznama blokiranih naslovov.

Dodaj izjemo – kliknite, če želite dodati izjemo požarnega zidu v filtriranje IDS.



Dnevniki zaščite omrežja

Zaščita omrežja ESET Internet Security vse pomembne dogodke shrani v dnevniško datoteko. Če si želite ogledati dnevniško datoteko, odprite glavno okno programa > **Nastavitve** > **Zaščita omrežja** > **Pokaži dnevnike**.

Z dnevniškimi datotekami lahko odkrivate napake in razkrivate vdore v sistem. Dnevniki zaščite omrežja vključujejo naslednje podatke:

- Datum in čas dogodka
- Ime dogodka
- Vir
- Ciljni omrežni naslov
- Protokol omrežne komunikacije
- Uporabljeno pravilo ali ime črva (če je bil zaznan)
- Pot in ime programa
- Zgoščena vrednost
- Uporabnik
- Podpisnik programa (založnik)

- Ime paketa
- Ime storitve

S temeljito analizo teh podatkov je mogoče zaznati poskuse ogrožanja varnosti računalnika. Na morebitna varnostna tveganja lahko opozori veliko drugih dejavnikov lahko, tako da lahko v največji možni meri zmanjšate njihov učinek: pogoste povezave z neznanih mest, več poskusov vzpostavitve povezave, komunikacije neznanih programov ali uporaba nenavadnih številk vrat.

> **Izkoriščanje varnostne ranljivosti**
> Sporočilo o izkoriščanju varnostne ranljivosti se zabeleži, četudi je posamezna ranljivost že oskrbljena, saj je poskus izkoriščanja zaznan in blokiran na ravni omrežja, še preden pride do dejanskega izkoriščanja.

Odpravljanje težav s požarnim zidom

Če imate težave s povezavo z nameščenim programom ESET Internet Security, lahko na več načinov ugotovite, ali težave povzroča požarni zid. Požarni zid vam lahko pomaga tudi ustvariti nova pravila ali izjeme, s katerimi boste odpravili težave s povezljivostjo.

Za pomoč pri odpravljanju težav s požarnim zidom glejte naslednje teme:

- Odpravljanje težav z dostopom do omrežja
- Pisanje dnevnika in ustvarjanje pravil ali izjem iz dnevnika
- Ustvarjanje izjem iz obvestil požarnega zidu
- Napredno beleženje zaščite omrežja
- Odpravljanje težav s pregledovalnikom omrežnega prometa

Pisanje dnevnika in ustvarjanje pravil ali izjem iz dnevnika

Požarni zid ESET privzeto ne beleži vseh blokiranih povezav. Odprite razdelek Napredne nastavitve > **Orodja** > **Diagnostika** > **Napredno beleženje** in omogočite možnost **Omogoči napredno beleženje zaščite omrežja**, da si ogledate, kaj je blokirala zaščita omrežja. Če v dnevniku opazite elemente, za katere ne želite, da jih požarni zid blokira, lahko zanje ustvarite pravilo ali pravilo IDS, tako da nanje kliknete z desno tipko miške in izberete možnost **V prihodnje ne blokiraj podobnih dogodkov**. Upoštevajte, da lahko dnevnik vseh blokiranih povezav vsebuje tisoče elementov in da je iskanje posamezne povezave v dnevniku zahtevno. Ko odpravite težavo, lahko funkcijo beleženja v dnevnik izklopite.

Za več informacij o dnevnikih glejte Dnevniške datoteke.

> Če želite videti vrstni red posameznih povezav, ki jih je blokiral Zaščitu omrežja, uporabite pisanje dnevnika. Ustvarjanje pravil iz dnevnika pa vam omogoča, da ustvarite taka pravila, ki vam najbolj ustrezajo.

Ustvarjanje pravila iz dnevnika

Nova različica programa ESET Internet Security omogoča, da iz dnevnika ustvarite pravilo. V glavnem meniju kliknite možnost **Orodja** > **Dnevniške datoteke**. V spustnem meniju izberite možnost **Zaščita omrežja**, z desno tipko miške kliknite želeni vnos v dnevniku in v priročnem meniju izberite **V prihodnje ne blokiraj podobnih dogodkov**. Novo pravilo bo prikazano v oknu z obvestilom.

Če želite omogočiti ustvarjanje novih pravil iz dnevnika, mora biti program ESET Internet Security konfiguriran z naslednjimi nastavitvami:

1. Najmanjšo dovoljeno raven podrobnosti v možnosti **Napredne nastavitve** > Orodja > **Dnevniške datoteke** nastavite na **Diagnostika**.

2. Omogočite možnost **Obvesti me o dohodnih napadih na varnostne luknje** v razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Zaščita pred napadi iz omrežja** > **Napredne možnosti** > **Zaznavanje vdorov**.

Ustvarjanje izjem iz obvestil požarnega zidu

Ko požarni zid ESET zazna zlonamerno dejavnost omrežja, bo prikazano okno z obvestilom, ki opisuje dogodek. To obvestilo vsebuje povezavo, na kateri lahko najdete več informacij o dogodku in po želji nastavite pravilo za ta dogodek.

i če omrežni program ali naprava ne izvaja omrežnih standardov pravilno, lahko pride do ponavljanja obvestil sistema za zaznavanje vdorov (IDS) požarnega zidu. Izjemo lahko ustvarite neposredno iz obvestila in tako preprečite, da bi požarni zid ESET zaznal ta program ali napravo.

Napredno beleženje zaščite omrežja

Ta funkcija ustvari bolj kompleksne dnevniške datoteke za tehnično podporo družbe ESET. To funkcijo uporabite samo takrat, ko to zahteva tehnična podpora družbe ESET, saj lahko ustvari ogromno dnevniško datoteko in upočasni delovanje vašega računalnika.

1. Pomaknite se v razdelek Napredne nastavitve > **Orodja** > **Diagnostika** > **Napredno beleženje** in omogočite možnost **Omogoči napredno beleženje zaščite omrežja**.

2. Poskusite poustvariti težave, ki se pojavljajo.

3. Onemogočite napredno beleženje zaščite omrežja.

4. Dnevniško datoteko PCAP, ki jo ustvari napredno beleženje zaščite omrežja, lahko najdete v mapi z izvozi diagnostičnega pomnilnika s potjo: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Odpravljanje težav s pregledovalnikom omrežnega

prometa

Če v zvezi s spletnim brskalnikom ali e-poštnim odjemalcem naletite na težave, najprej določite, če je za to kriv pregledovalnik omrežnega prometa. To storite tako, da v razdelku Napredne nastavitve > **Pogon za zaznavo** > **Pregledovalnik omrežnega prometa** začasno onemogočite pregledovalnik omrežnega prometa (ne pozabite ga znova vklopiti, potem ko končate, sicer bo vaš spletni brskalnik ali e-poštni odjemalec ostal nezaščiten). Če je težava po izklopu odpravljena, glejte spodnji seznam običajnih težav s podatki o tem, kako težave odpraviti:

Težave s posodobitvami ali varno komunikacijo

Vaš program javlja, da ne more izvajati posodobitev ali da komunikacijski kanal ni varen:

- Če je omogočena možnost SSL/TLS, jo začasno izklopite. Če je težava s tem odpravljena, lahko SSL/TLS še naprej uporabljate, posodobitve pa bodo delovale, če izločite težavno komunikacijo:
  Onemogoči SSL/TLS. Ponovno zaženite posodobitve. Pojaviti se mora pogovorno okno, ki vas obvešča o šifriranem omrežnem prometu. Prepričajte se, da se program ujema s tistim, kjer odpravljate težave, in da je certifikat videti, kot bi bil poslan iz strežnika, od koder se izvajajo posodobitve. Nato izberite možnost, ki omogoča, da si sistem zapomni dejanje za ta certifikat ter kliknite »Prezri«. Če zadevna pogovorna okna niso več prikazana, lahko način filtriranja nastavite nazaj na »samodejno« in težava bi morala biti odpravljena.

- Če zadevni program ni brskalnik ali e-poštni odjemalec, ga lahko v celoti izločite iz zaščite spletnega dostopa (če to storite za brskalnik ali e-poštnega odjemalca, bi bili izpostavljeni tveganjem). Vsak program, ki je imel v preteklosti že filtrirano komunikacijo, bi že moral biti vključen na seznam, ki je na voljo, ko dodajate izjemo, tako da ročno dodajanje praviloma ni potrebno.

Težava z dostopanjem do naprave prek omrežja

Če ne morete uporabiti nobene funkcije naprave v svojem omrežju (npr. odpreti spletne strani spletne kamere ali predvajati videoposnetka prek domačega predvajalnika predstavnosti), poskusite dodati ustrezna naslova IPv4 in IPv6 na seznam izključenih naslovov.

Težave z določeno spletno stranjo

Določene spletne strani lahko iz zaščite spletnega dostopa odstranite z upravljanjem naslova URL. Če, na primer, ne morete dostopati do naslednjega naslova https://www.gmail.com/intl/en/mail/help/about.html, na seznam izključenih naslovov poskusite dodati *gmail.com*.

Napaka »Nekatere aplikacije, potrebne za uvoz korenskih certifikatov, so še vedno odprte«

Ko omogočite SSL/TLS, se program ESET Internet Security prepriča, da nameščeni programi zaupajo načinu filtriranja protokola SSL, tako da v njihovo trgovino s potrdili uvozi potrdilo. Nekateri programi lahko zahtevajo ponovni zagon za uvoz potrdila. Sem sta vključena programa Firefox in Opera. Prepričajte se, da se noben od teh programov ne izvaja (to lahko storite tako, da odprete »Upravitelja opravil« in v zavihku »Procesi« preverite, da element firefox.exe ali opera.exe ni prisoten), nato izberite »Poskusi znova«.

Napaka v zvezi z izdajateljem, ki ni vreden zaupanja, ali neveljavnim podpisom

To najverjetneje pomeni, da uvoz, opisan zgoraj, ni uspel. Najprej se prepričajte, da se noben od omenjenih programov ne izvaja. Nato onemogočite možnost SSL/TLS in jo znova omogočite. Tako znova zaženete uvoz.

Glejte članek v zbirki znanja o tem, kako upravljati pregledovalnik omrežnega prometa z izdelki za domačo uporabo ESET za Windows.

Omrežna grožnja blokirana

Do tega lahko pride, če program v vašem računalniku poskuša prenesti zlonameren promet v drugo napravo v omrežju ter pri tem izkorišča varnostno luknjo ali celo če je zaznan poskus pregledovanja vrat v sistemu.

V obvestilu lahko najdete vrsto grožnje in naslov IP povezane naprave. Kliknite **Spremeni obravnavo te grožnje**, da se prikažejo te možnosti:

Nadaljuj z blokiranjem – blokira zaznano grožnjo. Če želite prenehati prejemati obvestila o tej vrsti grožnje z določenega oddaljenega naslova, izberite izbirni gumb pri možnosti **Ne obveščaj**, preden kliknete **Nadaljuj z blokiranjem**. Tako boste ustvarili pravilo za storitev zaznavanja vdorov (IDS) z naslednjo konfiguracijo: **Blokiraj** – privzeto, **Obvesti** – ne, **Beleži v dnevnik** – ne.

Dovoli – ustvari pravilo za storitev zaznavanja vdorov (IDS), ki dovoli zaznano grožnjo. Preden kliknete **Dovoli**, izberite eno od naslednjih možnosti za določanje nastavitev pravila:

- **Obvesti me samo, ko je ta grožnja blokirana** – konfiguracija pravila: **Blokiraj** – ne, **Obvesti** – ne, **Beleži v dnevnik** – ne.
- **Obvesti vedno, ko se pojavi ta grožnja** – konfiguracija pravila: **Blokiraj** – ne, **Obvesti** – privzeto, **Beleži v dnevnik** – privzeto.
- **Ne obvesti** – konfiguracija pravila: **Blokiraj** – ne, **Obvesti** – ne, **Beleži v dnevnik** – ne.

Informacije, prikazane v tem oknu z obvestilom, se lahko razlikujejo glede na vrsto zaznane grožnje.
Če želite več informacij o grožnjah in drugih povezanih izrazih, preberite razdelek Vrste oddaljenih napadov ali Vrste zaznav.
Če želite rešiti dogodek **Podvojeni naslovi IP v omrežju**, preberite naš članek zbirke znanja družbe ESET.

Zaznano novo omrežje

Program ESET Internet Security pri zaznavi novega omrežja privzeto uporabi nastavitve sistema Windows. Če želite prikazati pogovorno okno, ko je zaznano novo omrežje, spremenite dodelitev profila zaščite omrežja na možnost **Vprašaj**. Konfiguracija zaščite omrežja se prikaže vedno, ko se računalnik poveže z novim omrežjem.

Izbirate lahko med naslednjimi profili omrežnih povezav:

Samodejno – program ESET Internet Security bo samodejno izbral profil na podlagi aktivatorjev, konfiguriranih za vsak profil.

Zasebno – za zaupanja vredna omrežja (domače ali službeno omrežje). Računalnik in datoteke v skupni rabi, shranjene v računalniku, so vidne drugim uporabnikom omrežja, sistemski viri pa so dostopni drugim uporabnikom v omrežju (omogočen je dostop do datotek in tiskalnikov v skupni rabi, omogočena je dohodna komunikacija RPC in na voljo je skupna raba oddaljenega namizja). Priporočamo uporabo te nastavitve pri dostopu do varnega lokalnega omrežja. Ta profil je samodejno dodeljen omrežni povezavi, če je konfiguriran kot domena ali zasebno omrežje v sistemu Windows.

Javno – za omrežja, ki niso vredna zaupanja (javno omrežje). Datoteke in mape v vašem sistemu niso v skupni rabi ali vidne drugim uporabnikom v omrežju in deljenje sistemskih virov je deaktivirano. Pri dostopu do brezžičnih omrežij priporočamo uporabo te nastavitve. Ta profil je samodejno dodeljen kateri koli omrežni povezavi, ki ni konfigurirana kot domena ali zasebno omrežje v sistemu Windows.

Uporabniško določen profil – v spustnem meniju lahko izberete enega od profilov, ki ste jih ustvarili. Ta možnost je na voljo le, če ste ustvarili vsaj en profil po meri.

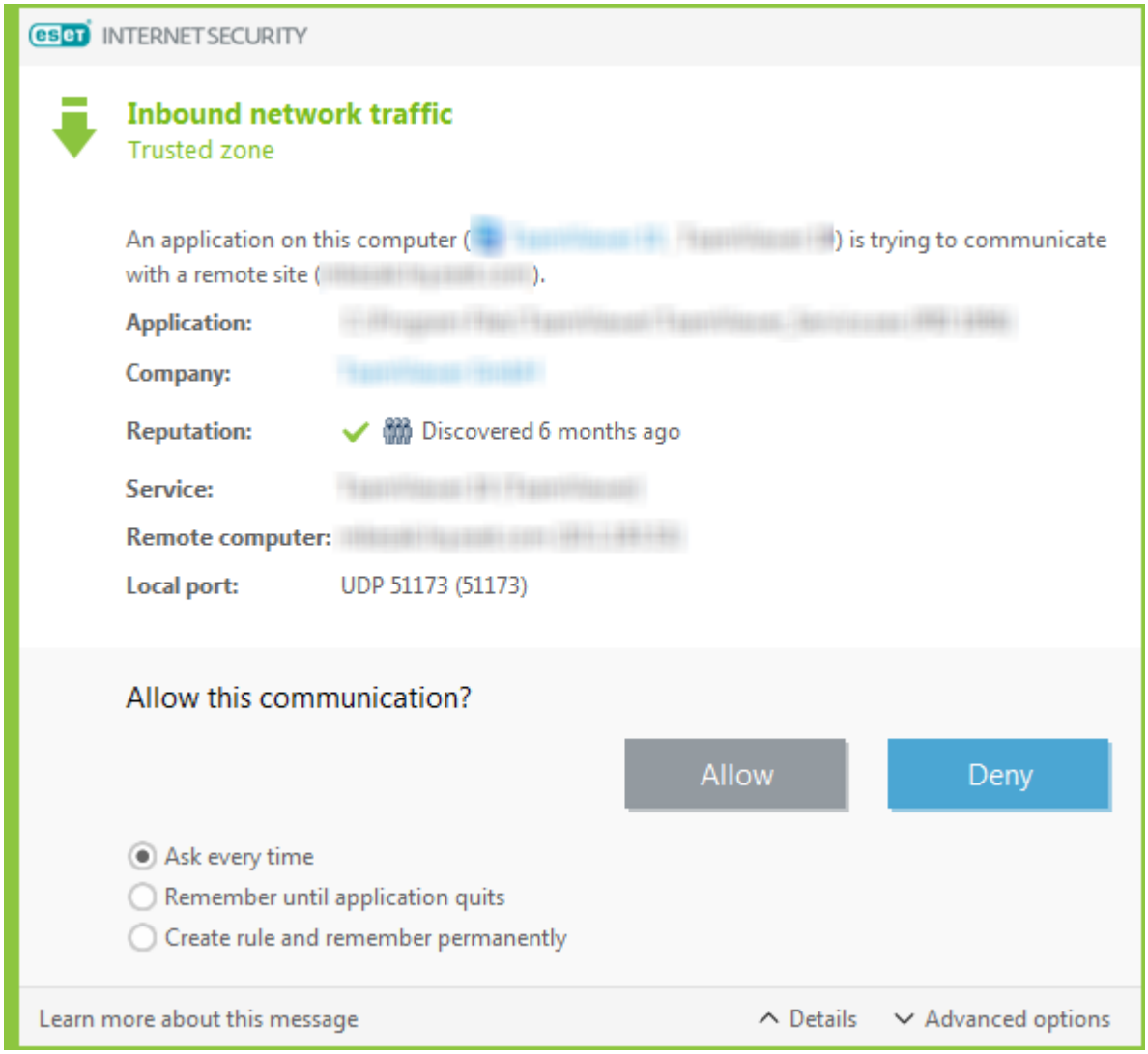
⚠ Nepravilna konfiguracija omrežja lahko predstavlja varnostno tveganje za računalnik.

Vzpostavljanje povezave – zaznavanje

Požarni zid zazna vse novo ustvarjene omrežne povezave. Aktivni način požarnega zidu ugotovi, katera dejanja so izvedena za novo pravilo. Če je aktiviran **Samodejni način** ali **Način na podlagi pravilnika**, požarni zid izvede vnaprej določena dejanja brez posredovanja uporabnika.

Interaktivni način prikaže okno z informacijami o zaznavi nove omrežne povezave in podrobne informacije o povezavi. Izberete lahko možnost **Dovoli** ali **Zavrni** (blokiraj) povezavo. Če v pogovornem oknu večkrat omogočite isto povezavo, priporočamo, da za povezavo ustvarite novo pravilo. Izberite možnost **Ustvari pravilo in si ga trajno zapomni** in shranite dejanje kot novo pravilo za požarni zid. Če požarni zid v prihodnosti prepozna isto

povezavo, bo uporabil obstoječe pravilo brez posredovanja uporabnika.



Ko ustvarjate nova pravila, dovolite samo povezave, za katere veste, da so varne. Če omogočite vse povezave, požarni zid ne more izpolniti svojega namena. Spodaj so navedeni pomembni parametri za povezave:

Program – mesto izvedljive datoteke in ID postopka. Ne dovolite povezav za neznane programe in postopke.

Podpisnik – ime založnika programa. Kliknite besedilo, če želite pokazati varnostno potrdilo za podjetje.

Ugled – raven tveganja povezave. Povezavam je dodeljena raven tveganja: ustrezna (zelena), neznana (oranžna) ali tvegana (rdeča), z nizom hevrističnih pravil, ki pregledujejo lastnosti vsake povezave, število uporabnikov in čas odkrivanja. Te informacije zbira tehnologija ESET LiveGrid®.

Storitev – ime storitve, če je program storitev sistema Windows.

Oddaljeni računalnik – naslov oddaljene naprave. Omogoči le vzpostavitev povezave z zaupanja vrednimi in znanimi naslovi.

Oddaljena vrata – komunikacijska vrata. Komunikacija prek znanih vrat (npr. spletni promet – številka vrat 80,443) naj bo dovoljena v normalnih okoliščinah.

Infiltracije v računalniku pogosto za svojo širitev uporabljajo internetne in skrite povezave, s katerimi lahko okužijo oddaljene sisteme. Če so pravila pravilno konfigurirana, postane požarni zid uporabno orodje za zaščito

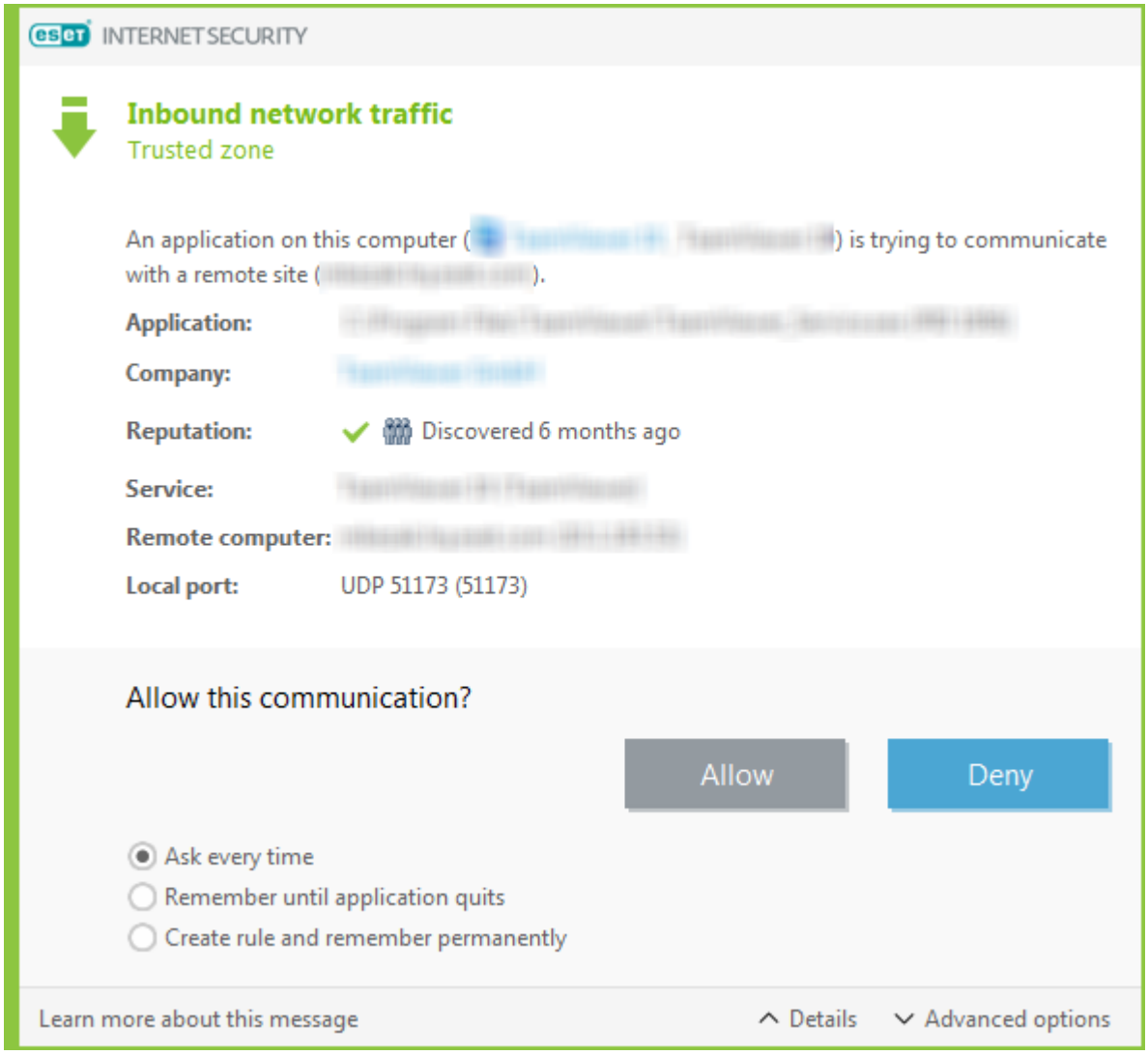
pred različnimi napadi zlonamerne kode.

Sprememba v programu

Požarni zid je zaznal spremembo v programu, ki vzpostavlja izhodne povezave iz računalnika. Morda je bil program preprosto posodobljen na novo različico. Morda pa je spremembo povzročil zlonameren program. Če se ne spomnite nobenega zakonitega spreminjanja, vam priporočamo, da zavrnete povezavo in pregledate računalnik z najnovejšo zbirko virusnih definicij.

Dohodna zaupanja vredna komunikacija

Primer dohodne povezave v zaupanja vrednem območju:
Oddaljeni računalnik v zaupanja vrednem območju poskuša vzpostaviti komunikacijo z lokalnim programom, ki se izvaja v računalniku.



Program – program, s katerim je stopila v stik oddaljena naprava.

Pot do programa – lokacija programa.

Program trgovine Microsoft Store – ime programa v trgovini Microsoft Store.

Podpisnik – ime založnika programa. Kliknite besedilo, če želite pokazati varnostno potrdilo za podjetje.

Ugled – ugled programa, pridobljen s tehnologijo ESET LiveGrid®.

Storitev – ime storitve, ki se trenutno izvaja v računalniku.

Oddaljeni računalnik – oddaljeni računalnik, ki poskuša vzpostaviti komunikacijo s programom v računalniku.

Oddaljena vrata – vrata, ki se uporabljajo za komunikacijo.

Vedno vprašaj – če je privzeto dejanje za pravilo nastavljeno na možnost **Vprašaj**, se prikaže pogovorno okno vsakič, ko se sproži to pravilo.

Zapomni si, dokler se program ne zapre – program ESET Internet Security si bo zapomnil izbrano dejanje do naslednjega vnovičnega zagona.

Ustvari pravilo in si ga trajno zapomni – če izberete to možnost, preden dovolite ali zavrnete komunikacijo, si program ESET Internet Security zapomni dejanje in ga uporabi, če oddaljeni računalnik znova stopi v stik s programom.

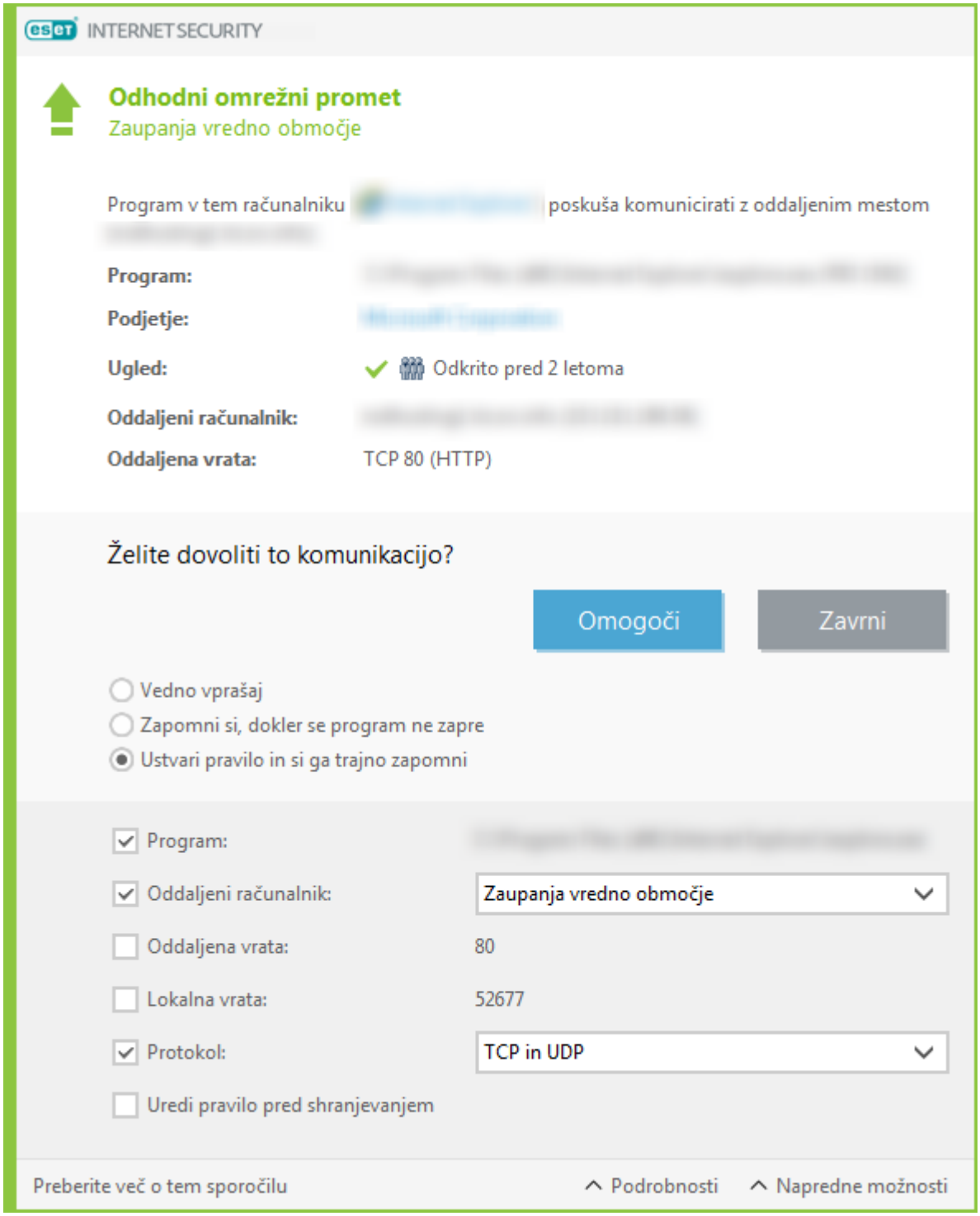
Dovoli – dovoli dohodno komunikacijo.

Zavrni – zavrne dohodno komunikacijo.

Uredi pravilo – omogoča prilagajanje lastnosti pravil z urejevalnikom pravil za požarni zid.

Odhodna zaupanja vredna komunikacija

Primer odhodne povezave v zaupanja vrednem območju:
Lokalni program poskuša vzpostaviti povezavo z drugim računalnikom v lokalnem omrežju ali v omrežju v zaupanja vrednem območju.



Program – program, s katerim je stopila v stik oddaljena naprava.

Pot do programa – lokacija programa.

Program trgovine Microsoft Store – ime programa v trgovini Microsoft Store.

Podpisnik – ime založnika programa. Kliknite besedilo, če želite pokazati varnostno potrdilo za podjetje.

Ugled – ugled programa, pridobljen s tehnologijo ESET LiveGrid®.

Storitev – ime storitve, ki se trenutno izvaja v računalniku.

Oddaljeni računalnik – oddaljeni računalnik, ki poskuša vzpostaviti komunikacijo s programom v računalniku.

Oddaljena vrata – vrata, ki se uporabljajo za komunikacijo.

Vedno vprašaj – če je privzeto dejanje za pravilo nastavljeno na možnost **Vprašaj**, se prikaže pogovorno okno vsakič, ko se sproži to pravilo.

Zapomni si, dokler se program ne zapre – program ESET Internet Security si bo zapomnil izbrano dejanje do naslednjega vnovičnega zagona.

Ustvari pravilo in si ga trajno zapomni – če izberete to možnost, preden dovolite ali zavrnete komunikacijo, si program ESET Internet Security zapomni dejanje in ga uporabi, če oddaljeni računalnik znova stopi v stik s programom.

Dovoli – dovoli dohodno komunikacijo.

Zavrni – zavrne dohodno komunikacijo.

Uredi pravilo – omogoča prilagajanje lastnosti pravil z urejevalnikom pravil za požarni zid.

Dohodna komunikacija

Primer dohodne vzpostavitve povezave z internetom:
Oddaljeni računalnik poskuša komunicirati s programom, ki se izvaja v računalniku.

Program – program, s katerim je stopila v stik oddaljena naprava.

Pot do programa – lokacija programa.

Program trgovine Microsoft Store – ime programa v trgovini Microsoft Store.

Podpisnik – ime založnika programa. Kliknite besedilo, če želite pokazati varnostno potrdilo za podjetje.

Ugled – ugled programa, pridobljen s tehnologijo ESET LiveGrid®.

Storitev – ime storitve, ki se trenutno izvaja v računalniku.

Oddaljeni računalnik – oddaljeni računalnik, ki poskuša vzpostaviti komunikacijo s programom v računalniku.

Oddaljena vrata – vrata, ki se uporabljajo za komunikacijo.

Vedno vprašaj – če je privzeto dejanje za pravilo nastavljeno na možnost **Vprašaj**, se prikaže pogovorno okno vsakič, ko se sproži to pravilo.

Zapomni si, dokler se program ne zapre – program ESET Internet Security si bo zapomnil izbrano dejanje do naslednjega vnovičnega zagona.

Ustvari pravilo in si ga trajno zapomni – če izberete to možnost, preden dovolite ali zavrnete komunikacijo, si program ESET Internet Security zapomni dejanje in ga uporabi, če oddaljeni računalnik znova stopi v stik s programom.

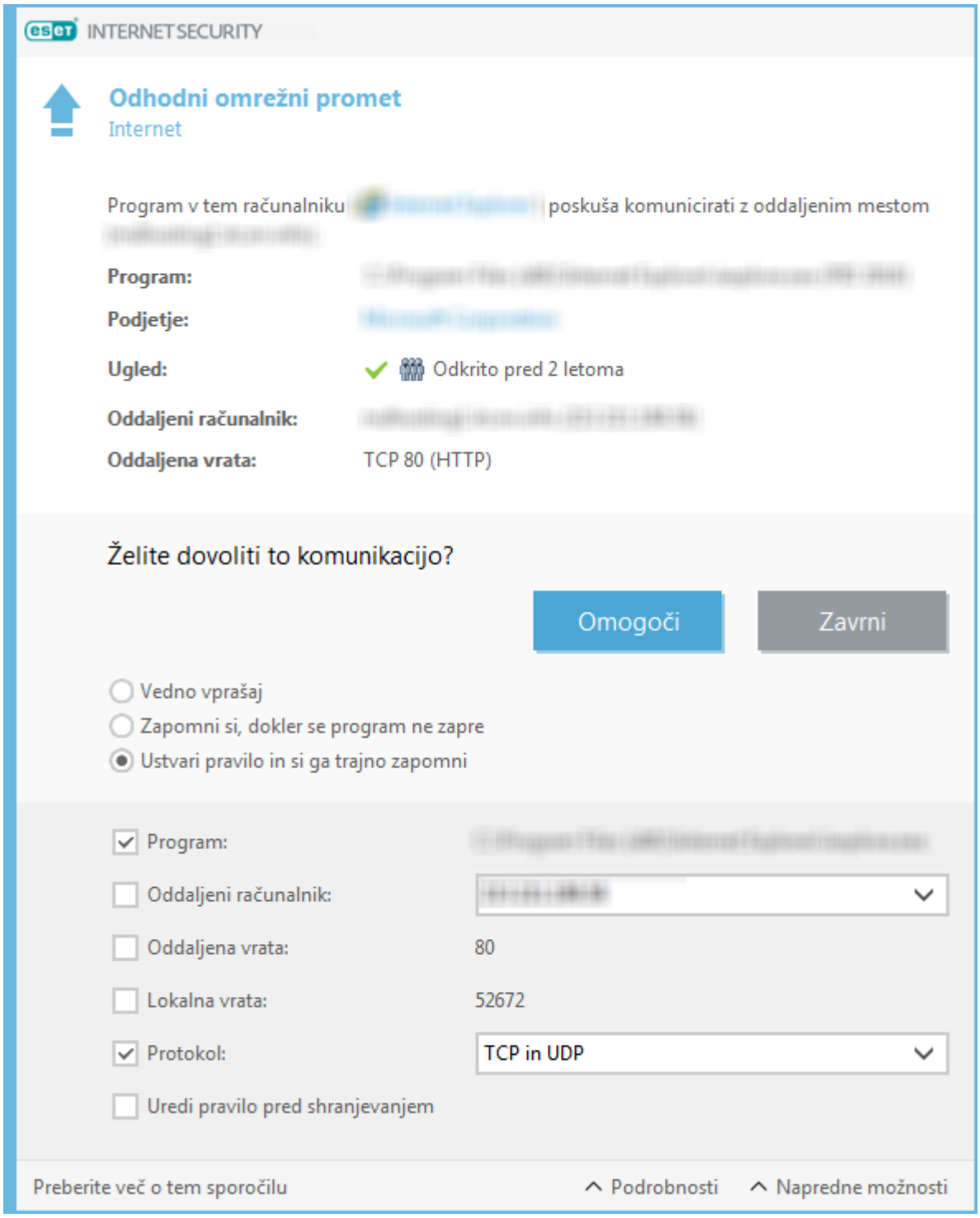
Dovoli – dovoli dohodno komunikacijo.

Zavrni – zavrne dohodno komunikacijo.

Uredi pravilo – omogoča prilagajanje lastnosti pravil z urejevalnikom pravil za požarni zid.

Odhodna komunikacija

Primer odhodne vzpostavitve povezave z internetom:
Lokalni program, ki poskuša vzpostaviti internetno povezavo.



Program – program, s katerim je stopila v stik oddaljena naprava.

Pot do programa – lokacija programa.

Program trgovine Microsoft Store – ime programa v trgovini Microsoft Store.

Podpisnik – ime založnika programa. Kliknite besedilo, če želite pokazati varnostno potrdilo za podjetje.

Ugled – ugled programa, pridobljen s tehnologijo ESET LiveGrid®.

Storitev – ime storitve, ki se trenutno izvaja v računalniku.

Oddaljeni računalnik – oddaljeni računalnik, ki poskuša vzpostaviti komunikacijo s programom v računalniku.

Oddaljena vrata – vrata, ki se uporabljajo za komunikacijo.

Vedno vprašaj – če je privzeto dejanje za pravilo nastavljeno na možnost **Vprašaj**, se prikaže pogovorno okno vsakič, ko se sproži to pravilo.

Zapomni si, dokler se program ne zapre – program ESET Internet Security si bo zapomnil izbrano dejanje do naslednjega vnovičnega zagona.

Ustvari pravilo in si ga trajno zapomni – če izberete to možnost, preden dovolite ali zavrnete komunikacijo, si program ESET Internet Security zapomni dejanje in ga uporabi, če oddaljeni računalnik znova stopi v stik s programom.

Dovoli – dovoli dohodno komunikacijo.

Zavrni – zavrne dohodno komunikacijo.

Uredi pravilo – omogoča prilagajanje lastnosti pravil z urejevalnikom pravil za požarni zid.

Nastavitve pogleda povezave

Z desno tipko miške kliknite povezavo, če si želite ogledati dodatne možnosti, vključno z:

Razreši imena gostiteljev – če je mogoče, so vsi omrežni naslovi prikazani v obliki zapisa DNS, ne v številski obliki naslova IP.

Pokaži samo povezave prek protokola TCP – na seznamu so prikazane samo povezave, ki pripadajo zbirki protokolov TCP.

Pokaži povezave, ki poslušajo – to možnost izberite, če želite prikazati le povezave, v katerih trenutno ni komunikacije, vendar je sistem odprl vrata in čaka povezavo.

Pokaži povezave v računalniku – to možnost izberite, če želite prikazati le povezave, v katerih je oddaljena stran lokalni sistem – tako imenovane povezave localhost.

Hitrost osveževanja – izberite frekvenco, s katero osvežite aktivne povezave.

Osveži zdaj – znova naloži okno **omrežnih povezav**.

Varnostna orodja

Odprite glavno okno programa > **Nastavitve** > **Varnostna orodja** za prilagoditev naslednjih modulov:

Varno bančništvo in brskanje – doda dodatno raven zaščite brskalnika, ki je zasnovana za zaščito finančnih

podatkov pri spletnih transakcijah. Omogočite funkcijo **Zaščiti vse brskalnike** v naprednih nastavitvah funkcije Varno bančništvo in brskanje, da se vsi podprti spletni brskalniki zaženejo v varnem načinu.

Zasebnost in varnost brskalnika – poskrbi za zasebno in varno uporabo spleta, ki ne pusti digitalnega odtisa.

Anti-Theft – omogočite funkcijo Zaščita pred krajo, da zaščitite svoj računalnik v primeru izgube ali kraje.

Varno bančništvo in brskanje

Varno bančništvo in brskanje je dodatna zaščita, zasnovana za zaščito finančnih podatkov med spletnimi transakcijami.

Vsi podprti spletni brskalniki se privzeto zaženejo v varnem načinu. To omogoča samodejno brskanje po internetu, dostop do spletnega bančništva ter opravljanje spletnih nakupov in transakcij v enem zaščitenem brskalniku.

Sistem ugleda ESET LiveGrid® mora biti omogočen (privzeto omogočen), da se zagotovi pravilno delovanje funkcije Varno bančništvo in brskanje.

Če želite konfigurirati delovanje zaščitenega brskalnika, glejte Napredne nastavitve funkcije Varno bančništvo in brskanje. Če onemogočite možnost **Zaščiti vse brskalnike**, lahko do zaščitenega brskalnika dostopate v glavnem oknu programa > **Pregled** > **Varno bančništvo in brskanje** ali tako, da kliknete namizno ikono **Varno bančništvo in brskanje**. Brskalnik, ki je privzet v sistemu Windows, se zažene v varnem načinu.

Za zaščiteno brskanje je nujna uporaba šifrirane komunikacije s protokolom HTTPS. Varno bančništvo in brskanje podpirajo naslednji brskalniki:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

V napravah s procesorji ARM sta podprta samo brskalnika Firefox in Microsoft Edge.

Dodatne podrobnosti o funkcijah Varno bančništvo in brskanje najdete v tem članku zbirke znanja družbe ESET, ki ne na voljo v angleščini in nekaterih drugih jezikih:

- Kako uporabljam Varno bančništvo in brskanje ESET?
- Začasna zaustavitev ali onemogočanje funkcije Varno bančništvo in brskanje izdelkih ESET Windows Home
- Varno bančništvo in brskanje ESET – pogoste napake
- Glosar ESET | Varno bančništvo in brskanje

Obvestilo v brskalniku

Zaščiten brskalnik vas o svojem trenutnem stanju obvešča z obvestili v brskalniku in barvo okvirja brskalnika.

Obvestila v brskalniku so prikazana na zavihku na desni strani.

Če želite razširiti obvestilo v brskalniku, kliknite ikono ESET. Če želite obvestilo zmanjšati, kliknite besedilo obvestila. Če želite opustiti obvestilo in okvir zelenega brskalnika, kliknite ikono za zapiranje.

Samo informativno obvestilo in okvir zelenega brskalnika je mogoče opustiti.

Obvestila v brskalniku

Vrsta obvestila	Stanje
Informativno obvestilo in zeleni okvir brskalnika	Zagotovljena je največja zaščita, obvestilo v brskalniku pa je privzeto zmanjšano. Razširite obvestilo v brskalniku in kliknite **Nastavitve**, da odprete nastavitev varnostnih orodij.
Opozorilo in oranžni okvir brskalnika	Zaščiten brskalnik zahteva vašo pozornost zaradi nekritične težave. Za več informacij o težavi ali rešitev sledite navodilom v obvestilu v brskalniku.
Varnostno opozorilo in rdeči okvir brskalnika	Brskalnik ni zaščiten s funkcijo Varno bančništvo in brskanje ESET. Znova zaženite brskalnik, če želite zagotoviti, da je zaščita aktivna. Če želite odpraviti spor z datotekami, naloženimi v brskalniku, odprite možnost Dnevniške datoteke > **Varno bančništvo in brskanje** in poskrbite, da zapisane datoteke ne bodo naložene, ko boste naslednjič zagnali brskalnik. Če težave ne odpravite, se obrnite na tehnično podporo ESET in sledite navodilom v našem članku v zbirki znanja.

Zasebnost in varnost brskalnika

Funkcijo Zasebnost in varnost brskalnika lahko omogočite prek razširitve po meri, ki je na voljo v podprtih brskalnikih (samo Google Chrome, Mozilla Firefox in Microsoft Edge).

Nameščanje in omogočanje razširitve:

1. Prepričajte se, da uporabljate najnovejšo različico izdelka ESET Internet Security in uspešno znova zaženite računalnik po posodobitvi.
2. Odprite brskalnik.
3. Razširitev je nameščena v vašem brskalniku.
4. Omogočite razširitev in prikaže se stran s podrobnostmi razširitve brskalnika.

Glavni meni razširitve brskalnika Zasebnost in varnost brskalnika je razdeljen na naslednje razdelke:

Pregled

Varno iskanje

Kliknite ikono preklopnega stikala  poleg možnosti **Pregled rezultatov iskanja**, da omogočite funkcijo in si ogledate, katere rezultate lahko varno kliknete. Funkcija Varno iskanje oceni navedene naslove povezav in ne pomeni nujno, da spletno mesto ne vsebuje zlonamerne programske opreme. Naš pogon za zaznavo nato zazna morebitno zlonamerno programsko opremo na spletnem mestu.

Čiščenje brskalnika

Izbrišite podatke brskanja ali nastavite redna čiščenja. Dodate lahko spletna mesta, kjer želite sprejeti piškotke in ostati prijavljeni tudi po čiščenju brskalnika, tako da **jih dodate na seznam**.

- **Enkratno čiščenje –** v spustnem meniju izberite časovno obdobje in vrsto podatkov, ki jo želite izbrisati. Izbirate lahko med možnostmi: vsi podatki, zasebni podatki in izbire po meri.

- **Redno čiščenje** – kliknite ikono preklopnega stikala  poleg možnosti **Redno čiščenje**, da omogočite funkcijo. V spustnem meniju izberite časovno obdobje in vrsto podatkov, ki jo želite redno brisati. Izbirate lahko med možnostmi: vsi podatki, zasebni podatki in izbire po meri.

Možnost **Podatki po meri** vsebuje te kategorije:

- Zgodovina brskanja
- Zgodovina prenosov
- Piškotki in podatki spletnega mesta
- Predpomnjene slike in datoteke
- Gesla in podatki za vpis
- Podatki za samodejno izpolnjevanje obrazcev

Pregled nastavitev za spletna mesta

Dostopajte do dovoljenj za spletna mesta in jih upravljajte, da imate nadzor na tem, katere informacije lahko spletna mesta uporabljajo.

- **Obvestila** – preglejte, katera spletna mesta želite **dovoliti/blokirati** obvestila ali če želite, da vas razširitev brskalnika **vsakič vpraša**.

Napredne nastavitve

Čiščenje brskalnika

Napredne nastavitve piškotkov

Seznam spletnih mest, kjer želite sprejeti piškotke in ostati prijavljeni tudi po čiščenju brskalnika. V besedilno polje vnesite naslov URL in kliknite **Dodaj**. S seznama ga lahko kadar koli odstranite, tako da kliknete ikono minusa  poleg določenega spletnega mesta.

Na dnu strani je seznam predlaganih domen, ki so trenutno odprte v brskalniku. Če določenega spletnega mesta ne vidite, kliknite **osveži seznam** in ga dodajte na seznam sprejetih piškotkov s klikom na ikono plusa  .

Pregled nastavitev za spletna mesta

Dostopajte do dovoljenj za spletna mesta in jih upravljajte, da imate nadzor na tem, katere informacije lahko spletna mesta uporabljajo.

- **Obvestila** – preglejte, katera spletna mesta želite **dovoliti/blokirati** obvestila ali če želite, da vas razširitev brskalnika **vsakič vpraša**.

Videz

Prilagodite barvno shemo vmesnika, da ustreza vašim željam. Želeno barvno shemo izberete tako, da izberete potrditveno polje **Svetlo** ali **Temno**.

Zaščita pred krajo

Na poti od doma do službe in na druga javna mesta, ki jih vsakodnevno obiskujemo, so naše osebne naprave ves čas v nevarnosti, da jih izgubimo ali da nam jih ukradejo. Zaščita pred krajo je funkcija, ki razširja varnost na ravni uporabnika v primeru izgubljene ali ukradene naprave. S funkcijo Zaščita pred krajo lahko nadzirate uporabo naprave in izsledite izgubljeno napravo tako, da jo poiščete prek naslova IP v računu ESET HOME, kar vam omogoča, da jo znova pridobite in zaščitite osebne podatke.

S sodobnimi tehnologijami, kot so iskanje zemljepisne lokacije prek naslova IP, zajemanje slik s spletno kamero, zaščita uporabniškega računa in nadziranje naprave, lahko z uporabo funkcije Zaščita pred krajo vi in organi kazenskega pregona hitreje poiščete računalnik ali napravo, ki je izgubljena ali ukradena. V računu ESET HOME lahko vidite, katere dejavnosti se izvajajo v računalniku ali napravi.

Če želite izvedeti več o funkciji Zaščita pred krajo v računu ESET HOME, si oglejte spletno pomoč ESET HOME.

Funkcija Zaščita pred krajo zaradi omejitev pri upravljanju uporabniških računov morda ne bo delovala pravilno v računalnikih v domenah.

Ko omogočite funkcijo Zaščita pred krajo, lahko optimizirate varnost svoje naprave v glavnem oknu programa > **Nastavitve** > **Varnostna orodja** > **Zaščita pred krajo**.

Možnosti optimizacije

Fantomski račun ni ustvarjen

Ustvarjanje fantomskega računa poveča možnost za iskanje izgubljene ali ukradene naprave. Če napravo označite kot izgubljeno, Zaščita pred krajo blokira dostop do aktivnih uporabniških računov, da zaščiti vaše občutljive podatke. Vsi, ki poskušajo uporabljati napravo, bodo lahko uporabljali samo fantomski račun. Fantomski račun je oblika račun gosta z omejenimi dovoljenji. Uporablja se kot privzeti sistemski račun, dokler naprava ni označena kot najdena, kar bo osebam preprečilo prijavo v druge uporabniške račune ali dostop do podatkov uporabnika.

Kadarkoli se nekdo prijavi v fantomski račun, ko je vaš računalnik v normalnem stanju, boste prejeli obvestilo s podatkom o sumljivi dejavnosti v računalniku. Po prejemu e-poštnega obvestila se lahko odločite, ali želite računalnik označiti kot manjkajoč.

Če želite ustvariti fantomski račun, kliknite možnost **Ustvari fantomski račun**, v besedilno polje vnesite **ime fantomskega računa** in kliknite možnost **Ustvari**.

Ko ustvarite fantomski račun, kliknite možnost **Nastavitve fantomskega računa**, da preimenujete ali izbrišete račun.

Zaščita gesel računov Windows

Vaš uporabniški račun ni zaščiten z geslom. To opozorilo optimizacije boste prejeli, če vsaj en uporabniški račun ni zaščiten z geslom. Ustvarjanje gesla za vse uporabnike (razen za **fantomski račun**) v računalniku bo razrešilo to težavo.

Če želite ustvariti geslo za uporabniški račun, kliknite **Upravljaj račune Windows** in spremenite geslo ali upoštevajte spodnja navodila:

1. Pritisnite CTRL+Alt+Delete na tipkovnici.
2. Kliknite možnost **Spremeni geslo**.
3. Polje **Staro geslo** pustite prazno.
4. Vnesite geslo v polji **Novo geslo** in **Potrdi geslo** ter pritisnite **Vnesi**.

Samodejna prijava za račune Windows

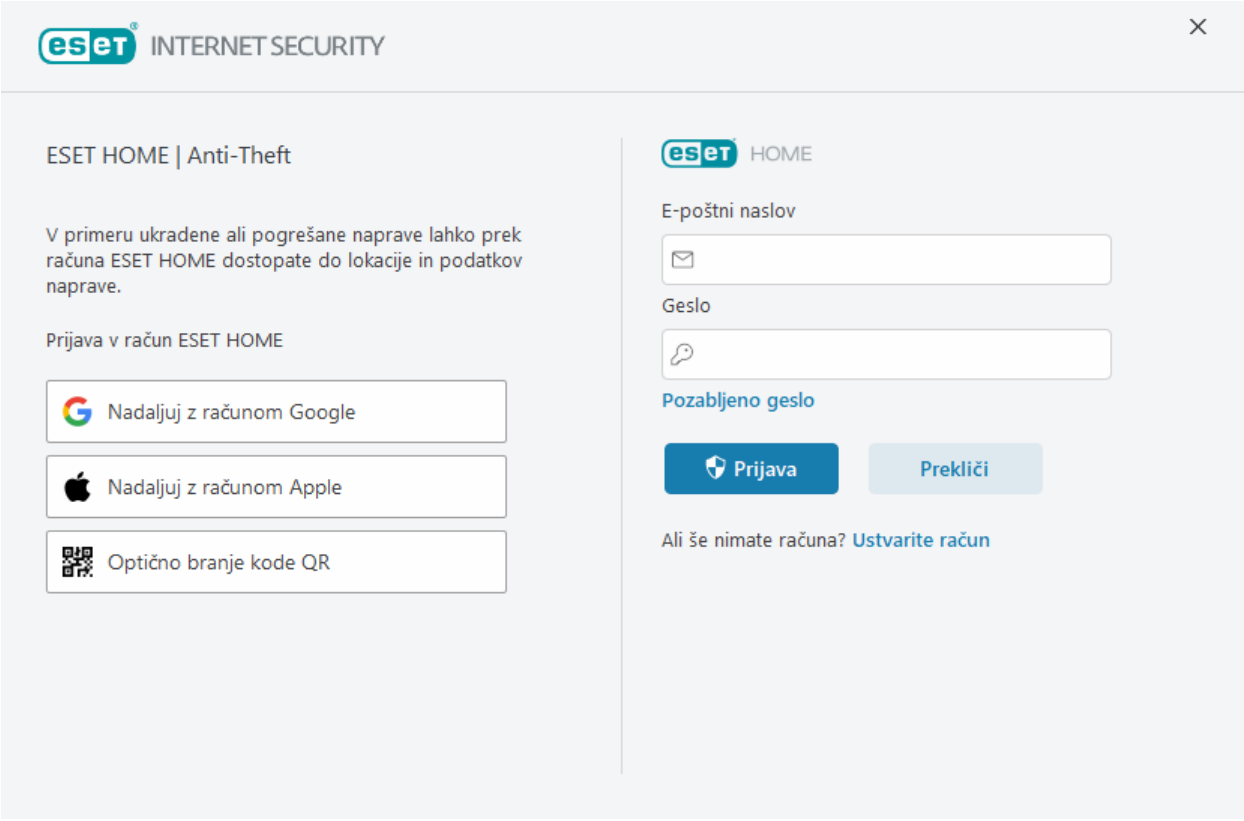
Vaš uporabniški račun ima omogočeno samodejno prijavo, zato vaš račun ni zaščiten pred nepooblaščenim dostopom. To opozorilo optimizacije boste prejeli, če ima omogočeno samodejno prijavo vsaj en uporabniški račun. Kliknite možnost **Onemogoči samodejno prijavo**, da razrešite to težavo z optimizacijo.

Samodejna prijava za fantomski račun

Samodejna prijava je omogočena za **fantomski račun** v vaši napravi. Ko je naprava v normalnem stanju, vam priporočamo, da ne uporabljate samodejne prijave, ker lahko povzroči težave z dostopom do vašega pravega uporabniškega računa ali pošlje lažne preplahe o stanju izgubljenega računalnika. Kliknite možnost **Onemogoči samodejno prijavo**, da razrešite to težavo z optimizacijo.

Prijavite se v račun ESET HOME.

Če želite omogočiti/onemogočiti funkcijo Zaščita pred krajo ter dostopati do lokacije naprave in podatkov v računu ESET HOME, se prijavite v svoj račun ESET HOME.



V račun ESET HOME se lahko prijavite na več načinov:

• **Uporabite e-poštni naslov in geslo za račun ESET HOME** – vnesite **E-poštni naslov** in **Geslo**, ki ste ju uporabili pri ustvarjanju računa ESET HOME, nato pa kliknite možnost **Prijava**.

• Uporabite svoj **računGoogle/AppleID** – kliknite **Nadaljuj z računomGoogle** ali **Nadaljuj z računomApple** in se prijavite v ustrezni račun. Po uspešni prijavi boste preusmerjeni na spletno stran ESET HOME za potrditev. Če želite nadaljevati, preklopite nazaj na okno izdelka ESET. Če želite več informacij o računu Google/AppleID, si oglejte navodila, ki jih vsebuje ESET HOMESpletna pomoč.

• **Skeniranje kode QR** – kliknite **Skeniranje kode QR** in prikazala se bo koda QR. Odprite mobilno aplikacijo ESET HOME in skenirajte kodo QR ali pa nanjo usmerite kamero svoje naprave. Če želite več informacij, si oglejte navodila, ki jih vsebuje Spletna pomoč ESET HOME.

Prijava ni uspela – pogoste napake.

Če nimate računa ESET HOME, kliknite možnost **Ustvari račun**, da ga registrirate, ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.
Če ste pozabili geslo, kliknite **Pozabljeno geslo** in upoštevajte navodila na zaslonu ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.

Zaščita pred krajo ne podpira Microsoft Windows Home Server.

Nastavite ime naprave

Polje **Ime naprave** predstavlja ime vašega računalnika (naprave), ki bo prikazano kot identifikator v storitvah ESET HOME. Privzeto je uporabljeno ime vašega računalnika. Vnesite ime naprave ali uporabite privzeto ime in kliknite možnost **Nadaljuj**.

Zaščita pred krajo omogočena/onemogočena

To okno vsebuje potrditveno sporočilo, ko omogočite/onemogočite funkcijo Zaščita pred krajo:

• Omogočeno – vaša naprava je zdaj zaščitena s funkcijo Zaščita pred krajo in lahko upravljate njeno varnost na daljavo na portalu ESET HOME z uporabo računa.

• Onemogočeno – funkcija Zaščita pred krajo je v tej napravi onemogočena in vsi podatki, povezani s funkcijo <%ESET_ANTTHEFT%> za to napravo, so odstranjeni s portala ESET HOME.

Dodajanje nove naprave ni uspelo

Med aktiviranjem programa Zaščita pred krajo je prišlo do napake.

Najpogostejši vzroki so:

• Napaka pri prijavi v račun ESET HOME

• Povezava z internetom ni na voljo (ali pa internet trenutno ne deluje)

Če težave ne morete razrešiti, se obrnite na tehnično podporo ESET.

Uvoz in izvoz nastavitev

Prilagojeno konfiguracijsko datoteko programa ESET Internet Security.xml lahko uvozite ali izvozite iz menija **Nastavitve**.

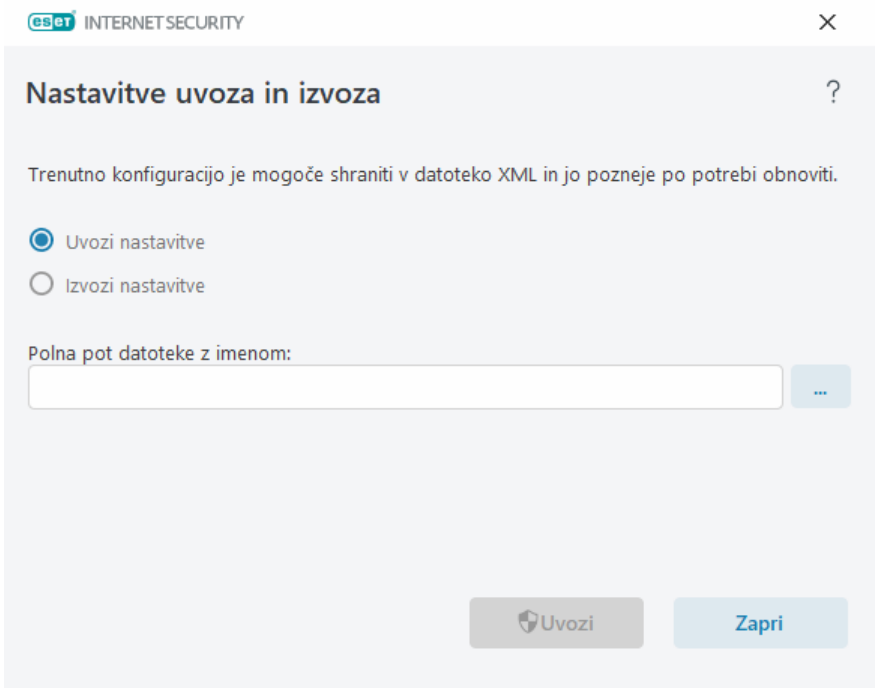
> **Ilustrirana navodila**
> Oglejte si Uvoz ali izvoz nastavitev konfiguracije za ESET ob uporabi datoteke .xml za ilustrirana navodila, ki so na voljo v angleščini ter v nekaterih drugih jezikih.

Uvoz in izvoz konfiguracijskih datotek sta koristna, če želite narediti varnostno kopijo trenutne konfiguracije za izdelek ESET Internet Security za poznejšo uporabo. Možnost nastavitev izvoza je prav tako priročna, ko želite želeno konfiguracijo uporabiti v več računalnikih. Datoteko .xml lahko uvozite ter tako prenesete nastavitve.

Če želite uvoziti konfiguracijo, izberite glavno okno programa in kliknite **Nastavitve** > **Uvoz/izvoz nastavitev**, nato pa izberite možnost **Uvozi nastavitve**. Vnesite ime konfiguracijske datoteke ali kliknite gumb **...**, če želite poiskati konfiguracijsko datoteko, ki jo boste uvozili.

Če želite izvoziti konfiguracijo, izberite **glavno okno programa** in kliknite Nastavitve > **Uvoz/izvoz nastavitev**. Izberite možnost **Izvozi nastavitve** in vnesite celotno pot datoteke, vključno z imenom. Kliknite **...**, če želite poiskati lokacijo na vašem računalniku, kamor boste shranili konfiguracijsko datoteko.

> Pri izvozu nastavitev lahko pride do napake, če nimate ustreznih pravic za zapisovanje izvoženih datotek v določen imenik.



Pomoč in podpora

Kliknite možnost **Pomoč in podpora** v glavnem oknu programa, da prikažete podatke o podpori in orodja za odpravljanje težav, ki vam pomagajo pri reševanju morebitnih težav.

Naročnina

• Odpravljanje težav z naročnino – kliknite to povezavo, da poiščete rešitve za težave z aktivacijo ali spremembo naročnine.

• Spremeni naročnino – kliknite, če želite zagnati okno za aktiviranje in aktivirati izdelek. Če je naprava povezana z računom ESET HOME, izberite naročnino iz svojega računa ESET HOME ali dodajte novega.

Nameščeni izdelek

• Novosti – kliknite to možnost, da se odpre okno z informacijami o novih in izboljšanih funkcijah.

• Več o programu ESET Internet Security – prikazuje podatke o vašem izvodu programa ESET Internet Security.

• Odpravljanje težav z izdelkom – kliknite to povezavo, da poiščete rešitve najpogostejših težav.

• **Spremeni izdelek** – kliknite, če želite izvedeti, ali je mogoče ESET Internet Security zamenjati za drug izdelek s trenutno naročnino.

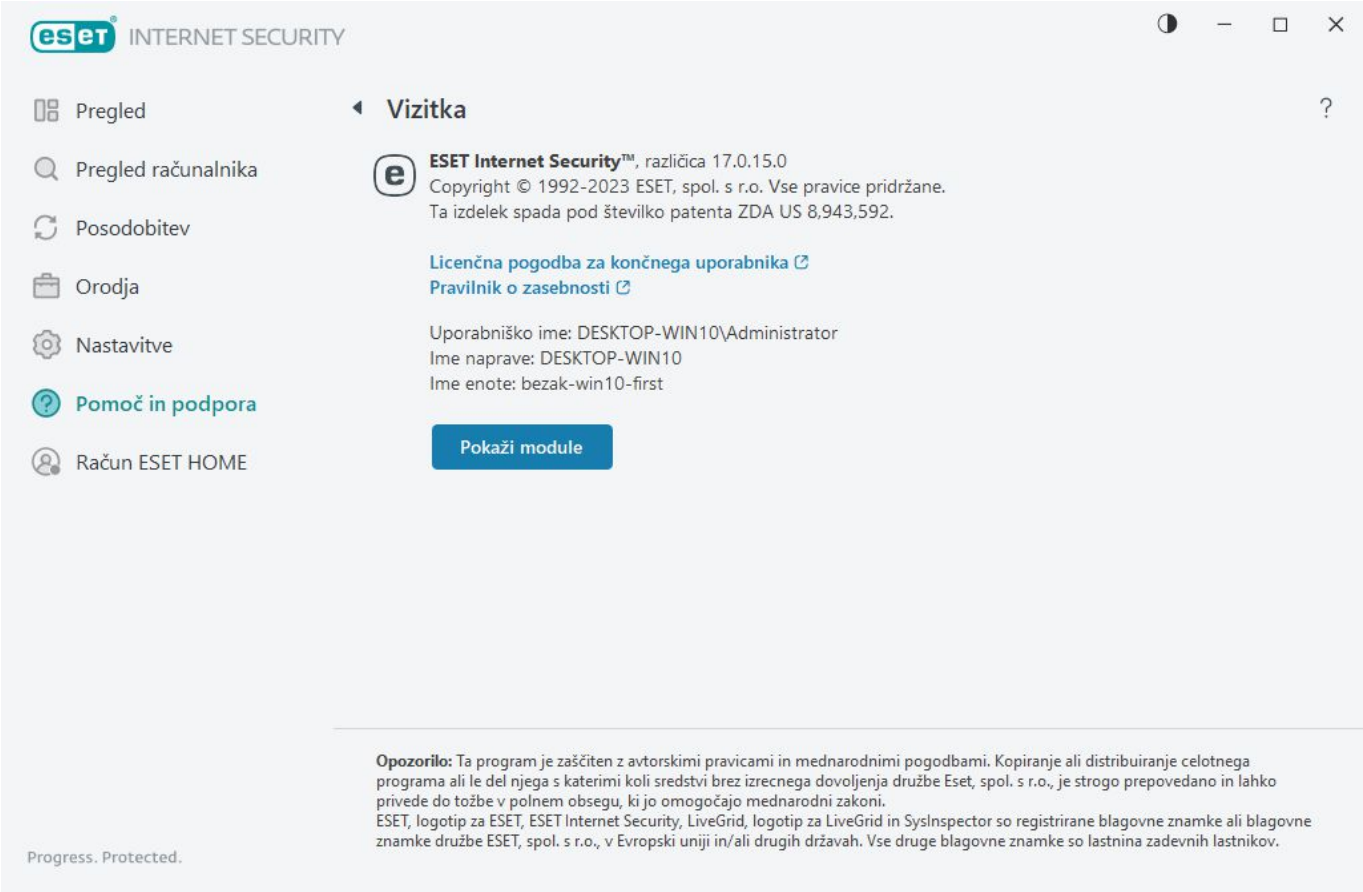
Stran za pomoč – kliknite to povezavo, če želite zagnati strani pomoči za ESET Internet Security.

Tehnična podpora

Zbirka znanja – zbirka znanja ESET vsebuje odgovore na najpogostejša vprašanja ter priporočene rešitve za različne težave. Zbirka znanja, ki jo tehnični strokovnjaki družbe ESET redno posodabljajo, je najbolj učinkovito orodje za odpravljanje raznih težav.

Vizitka izdelka ESET Internet Security

V tem oknu so na voljo podrobnosti o nameščeni različici izdelka ESET Internet Security in računalniku.



Če si želite ogledati informacije o seznamu nameščenih modulov programa, kliknite možnost **Pokaži module**.

- Podatke o modulih kopirate v odložišče tako, da kliknete **Kopiraj**. To je lahko uporabno pri odpravljanju težav ali stiku s tehnično podporo.

- V oknu Moduli kliknite **Pogon za zaznavo**, da odprete radar za viruse ESET, ki vsebuje podatke o posameznih različicah pogona za zaznavo ESET.

Novice družbe ESET

V tem oknu vas program ESET Internet Security redno obvešča o novicah družbe ESET.

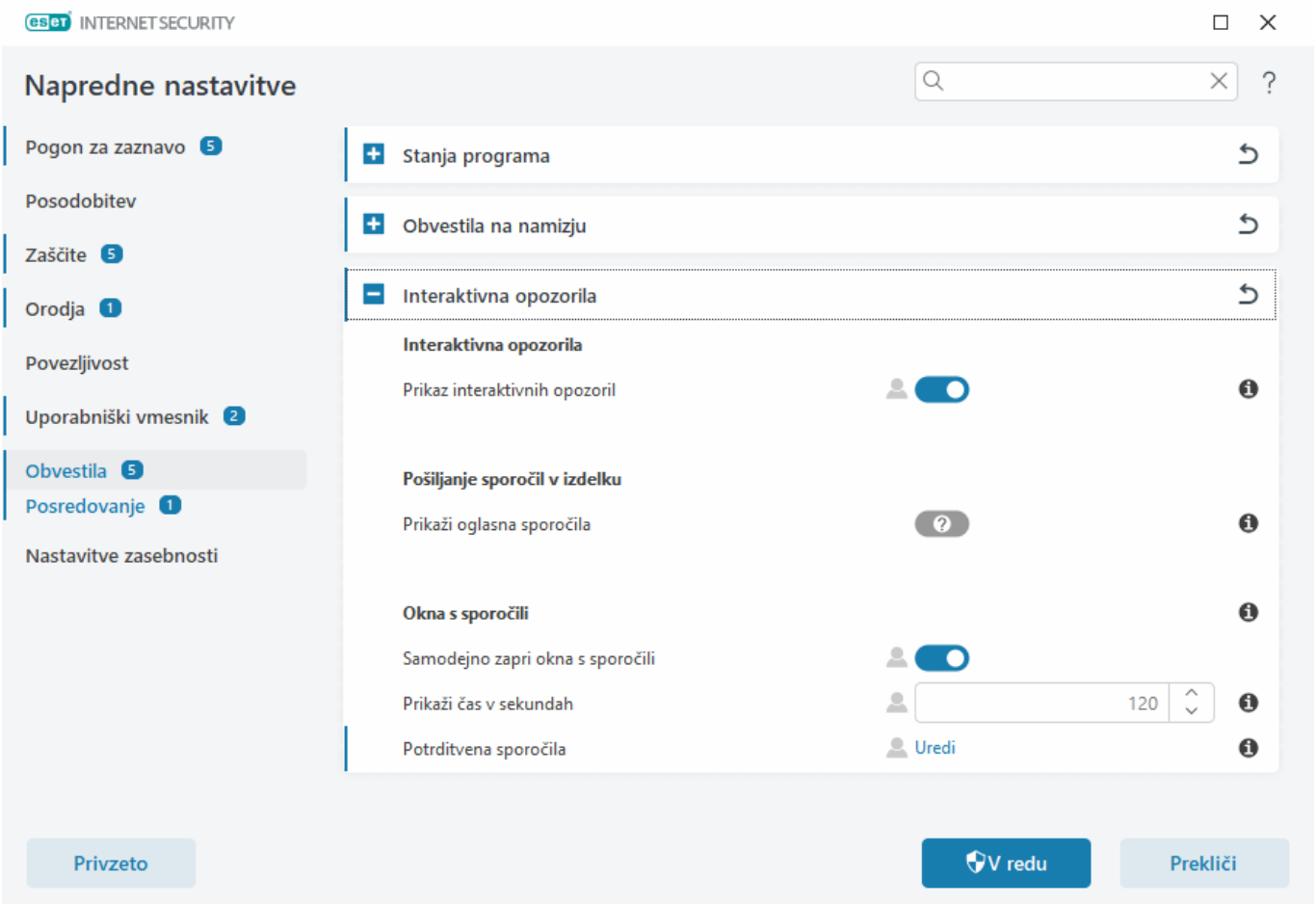
Pošiljanje sporočil v izdelku je namenjeno obveščanju uporabnikov o novicah družbe ESET in drugim sporočilom. Za pošiljanje oglaševalskih sporočil je potrebno soglasje uporabnika. Oglaševalska sporočila se zato privzeto ne pošiljajo uporabnikom (označeno z vprašajem). Če omogočite to možnost, soglašate s prejemanjem oglaševalskih sporočil družbe ESET. Če ne želite prejemati oglaševalskih vsebin družbe ESET, onemogočite možnost **Prikaži oglasna sporočila**.

Če želite omogočiti ali onemogočiti prejemanje oglasnih sporočil prek oken z obvestili, upoštevajte spodnja navodila.

1. Odpre napredne nastavitve.

2. Kliknite **Obvestila** > **Interaktivna opozorila**.

3. Uredite možnost **Prikaži oglasna sporočila**.



Pošlji podatke o konfiguraciji sistema

Družba ESET potrebuje podatke o konfiguraciji programa ESET Internet Security, podrobne podatke o sistemu in izvajajočih se postopkih (dnevniške datoteke ESET SysInspector) ter podatke registra, da lahko zagotovi čim hitrejšo in čim bolj natančno pomoč. ESET bo te podatke uporabil izključno za zagotavljanje tehnične podpore uporabniku.

Ko pošljete spletni obrazec, bodo podatki o konfiguraciji sistema poslani družbi ESET. Če želite, da si program zapomni to dejanje za ta postopek, izberite **Vedno pošlji te podatke**. Za pošiljanje spletnega obrazca brez pošiljanja podatkov kliknite **Ne pošlji podatkov** in nadaljujte.

Pošiljanje podatkov o konfiguraciji sistema lahko konfigurirate v razdelku Napredne nastavitve > **Orodja** > **Diagnostika** > Tehnična podpora.

Če ste se odločili za pošiljanje podatkov o konfiguraciji sistema, je potrebno izpolniti in poslati spletni obrazec. Sicer vaša vstopnica ne bo ustvarjena, podatki o konfiguraciji sistema pa bodo izgubljeni. Če podatkov o konfiguraciji sistema ni mogoče poslati, izpolnite spletni obrazec in počakajte na navodila tehnične podpore.

Tehnična podpora

V glavnem oknu programa kliknite možnost **Pomoč in podpora** > **Tehnična podpora**.

Obrnite se na tehnično podporo

Zahtevajte podporo – kadar ne najdete rešitve za težavo, lahko uporabite tudi ta obrazec na spletnem mestu družbe ESET in hitro stopite v stik z oddelkom za tehnično podporo družbe ESET. Na podlagi nastavitev se pred izpolnjevanjem spletnega obrazca prikaže okno za pošiljanje podatkov o konfiguraciji sistema.

Pridobite informacije za tehnično podporo

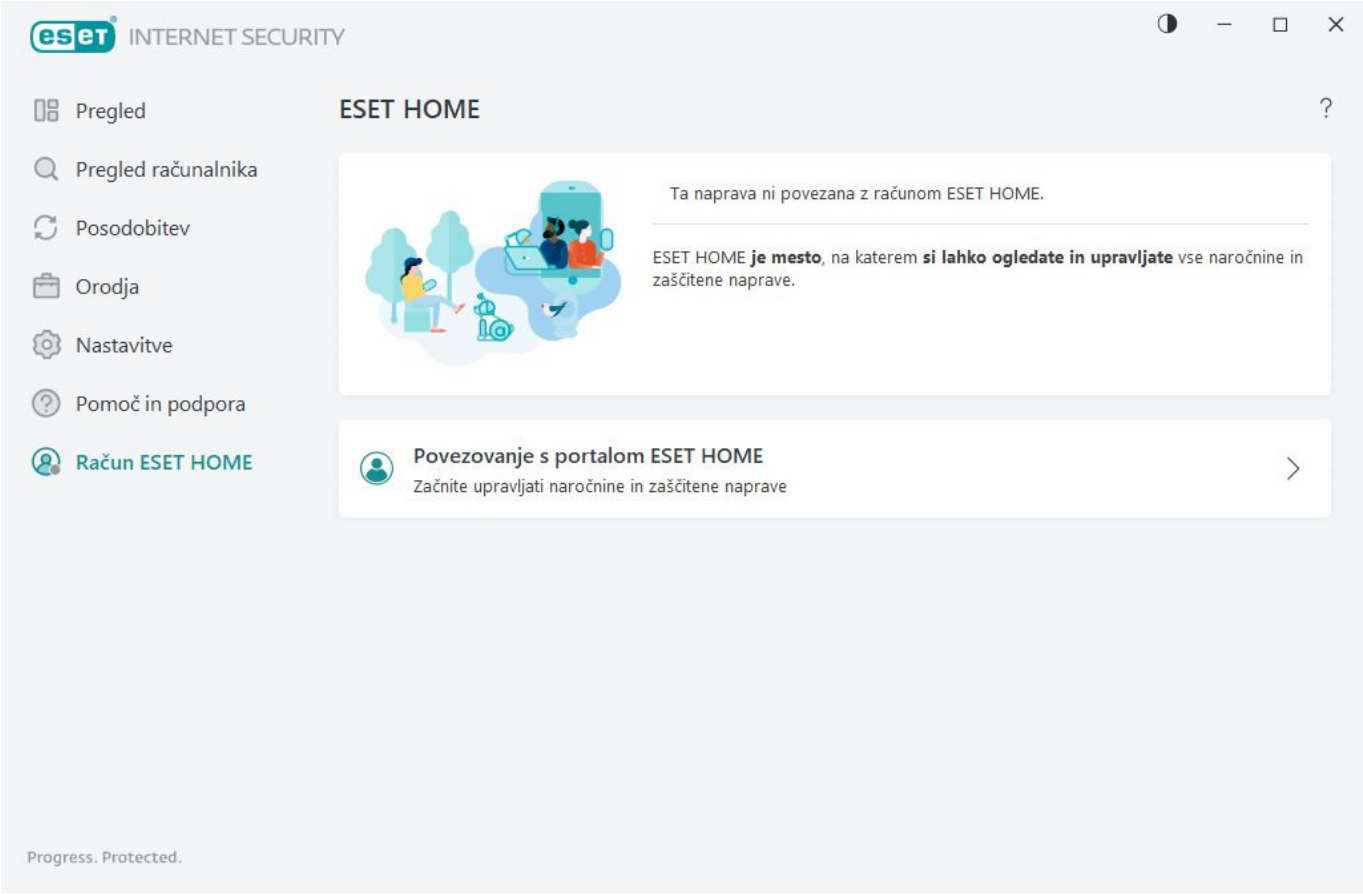
Podatki za tehnično podporo – ko ste pozvani, lahko podatke kopirate in pošljete tehnični podpori družbe ESET (na primer podatke o naročnini, ime in različico izdelka, operacijski sistem in podatke o računalniku).

ESET Log Collector – poveže se s člankom v zbirki znanja družbe ESET, kjer lahko prenesete program ESET Log Collector, ki samodejno zbira podatke in dnevnike iz računalnika za hitrejše odpravljanje težav. Za več informacij glejte spletni uporabniški priročnik za ESET Log Collector.

Omogočite pisanje naprednih dnevnikov, da ustvarite napredne dnevnike za vse razpoložljive funkcije in razvijalcem pomagate pri diagnosticiranju in odpravljanju težav. Najmanjša dovoljena raven podrobnosti pri pisanju v dnevnik je nastavljena na raven **Diagnostika**. Pisanje naprednih dnevnikov bo samodejno onemogočeno po dveh urah, če ga prej ne ustavite tako, da kliknete **Ustavi pisanje naprednih dnevnikov**. Ko so ustvarjeni vsi dnevniki, se pojavi okno z obvestilom in neposrednim dostopom do mape za diagnostiko, kjer so bili ustvarjeni dnevniki.

ESET HOME račun

Stanje povezave z računom ESET HOME lahko preverite v glavnem oknu programa > **Račun ESET HOME**.



Ta naprava ni povezana z računom ESET HOME

Če želite povezati napravo z računom ESET HOME ter upravljati svoje naročnine in zaščitene naprave, kliknite Poveži z računom ESET HOME. Naročnino lahko obnovite, nadgradite ali podaljšate in si ogledate pomembne podrobnosti. V mobilni aplikaciji ali na portalu za upravljanje računa ESET HOME lahko dodate različne naročnine, prenesete izdelke v svoje naprave, preverite varnostno stanje izdelka ali delite naročnino prek e-pošte. Za več informacij obiščite spletno pomoč za račun ESET HOME.

Ta naprava je povezana z računom ESET HOME

Na portalu za račun ESET HOME ali v mobilni aplikaciji lahko na daljavo upravljate varnost svoje naprave. Kliknite **App Store** ali **Google Play**, da se prikaže koda QR, ki jo lahko optično preberete z mobilnim telefonom in prenesete mobilno aplikacijo ESET HOME iz trgovine App Store ali Google Play.

Račun ESET HOME – ime vašega računa ESET HOME.

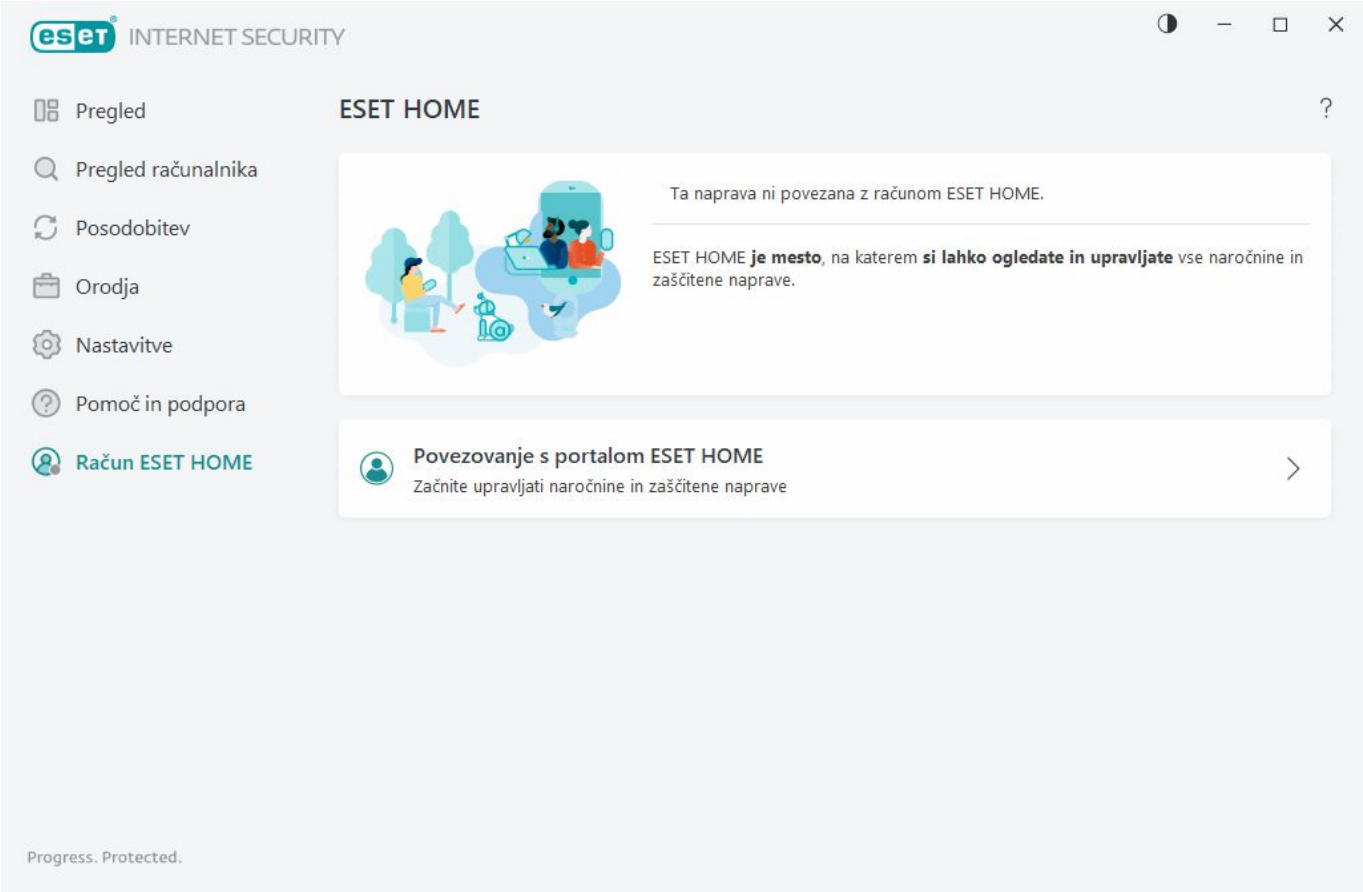
Ime naprave – ime te naprave, prikazano v računu ESET HOME.

Odpri ESET HOME – odpre portal za upravljanje računa ESET HOME.

Če želite prekiniti povezavo naprave z računom ESET HOME, kliknite **Prekini povezavo s portalom ESET HOME** > **Prekini povezavo**. Naročnina, uporabljena za aktivacijo, bo ostala aktivna in vaša naprava bo zaščitena.

Povežite z računom ESET HOME

Napravo povežite s ESET HOME, da preverite in upravljate vse svoje aktivirane naročnine ESET ter naprave. Naročnino lahko obnovite, nadgradite ali podaljšate in si ogledate pomembne podrobnosti naročnine. V mobilni aplikaciji ali na portalu za upravljanje računa ESET HOME lahko dodate različne naročnine, prenesete izdelke v svoje naprave, preverite varnostno stanje izdelka ali delite naročnino prek e-pošte. Za več informacij obiščite spletno pomoč za račun ESET HOME.



Če želite svojo napravo povezati z računom ESET HOME:

> Če se z računom ESET HOME povezujete med namestitvijo ali če kot metodo aktivacije izberete možnost **Uporaba računa ESET HOME**, upoštevajte navodila v temi Uporaba računa ESET HOME.
> Če ste izdelek ESET Internet Security že namestili in aktivirali z naročnino, dodano v vaš račun ESET HOME, lahko svojo napravo z računom ESET HOME povežete ob uporabi portala ESET HOME. Sledite navodilom v priročniku Spletni priročnik za pomoč za ESET HOME in dovolite povezavo v izdelku ESET Internet Security.

1. V glavnem oknu programa kliknite račun **ESET HOME** > **Vzpostavi povezavo z računom ESET HOME** oziroma kliknite možnost **Vzpostavi povezavo z računom ESET HOME** v obvestilu o **vzpostavljanju povezave med napravo in računom ESET HOME**.

2. Prijavite se v račun ESET HOME.

> Če nimate računa ESET HOME, kliknite možnost **Ustvari račun**, da ga registrirate, ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.
> Če ste pozabili geslo, kliknite **Pozabljeno geslo** in upoštevajte navodila na zaslonu ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.

3. Nastavite **ime naprave** in kliknite možnost **Nadaljuj**.

4. Ko je povezava uspešno vzpostavljena, se prikaže okno s podrobnostmi. Kliknite možnost **Dokončano**.

Prijava v račun ESET HOME

V račun ESET HOME se lahko prijavite na več načinov:

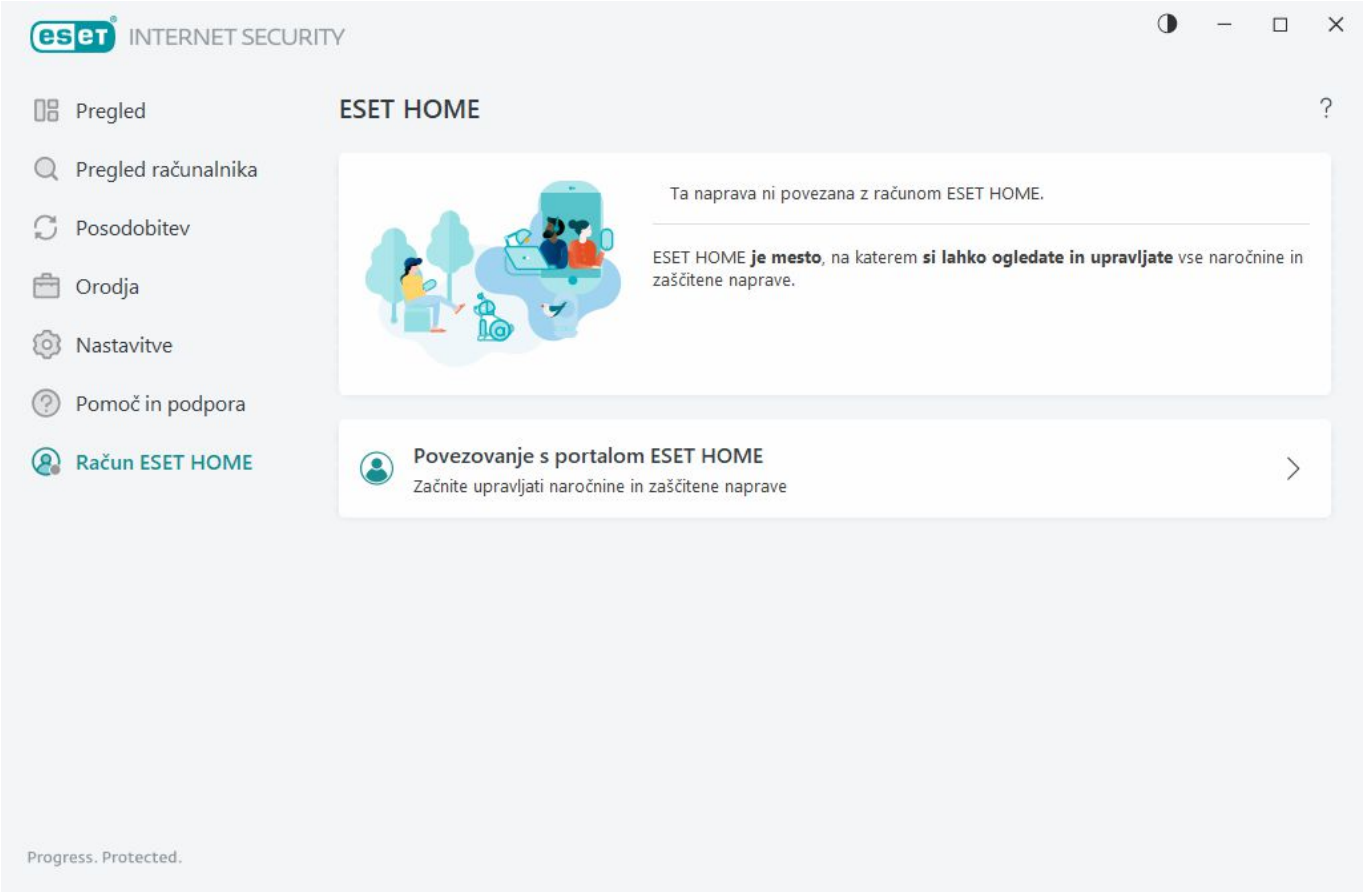
• **Uporabite e-poštni naslov in geslo za račun ESET HOME** – vnesite **E-poštni naslov** in **Geslo**, ki ste ju uporabili pri ustvarjanju računa ESET HOME, nato pa kliknite možnost **Prijava**.

• Uporabite svoj **računGoogle/AppleID** – kliknite **Nadaljuj z računomGoogle** ali **Nadaljuj z računomApple** in se prijavite v ustrezni račun. Po uspešni prijavi boste preusmerjeni na spletno stran ESET HOME za potrditev. Če želite nadaljevati, preklopite nazaj na okno izdelka ESET. Če želite več informacij o računu Google/AppleID, si oglejte navodila, ki jih vsebuje ESET HOMESpletna pomoč.

• **Skeniranje kode QR** – kliknite **Skeniranje kode QR** in prikazala se bo koda QR. Odprite mobilno aplikacijo ESET HOME in skenirajte kodo QR ali pa nanjo usmerite kamero svoje naprave. Če želite več informacij, si oglejte navodila, ki jih vsebuje Spletna pomoč ESET HOME.

Če nimate računa ESET HOME, kliknite možnost **Ustvari račun**, da ga registrirate, ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.
Če ste pozabili geslo, kliknite **Pozabljeno geslo** in upoštevajte navodila na zaslonu ali pa si oglejte navodila na straneh, na katerih je na voljo Spletna pomoč za ESET HOME.

Prijava ni uspela – pogoste napake.



Prijava ni uspela – pogoste napake

Ni bilo mogoče najti računa, ki bi ustrezal vnesenemu e-poštnemu naslovu

Vneseni e-poštni naslov se ne ujema z nobenim računom ESET HOME. Kliknite možnost **Nazaj** ter vnesite pravilen e-poštni naslov in geslo.

Če se želite prijaviti, morate ustvariti račun ESET HOME. Če nimate računa ESET HOME, kliknite **Nazaj** > **Ustvari račun** ali si oglejte temo Ustvarjanje novega računa ESET HOME.

Uporabniško ime in geslo se ne ujemata

Vneseno geslo se ne ujema z vnesenim e-poštnim naslovom. Kliknite **Nazaj**, vnesite pravilno geslo in preverite, ali je vneseni e-poštni naslov pravilen. Če prijava še vedno ni mogoča, kliknite **Nazaj** > **Pozabljeno geslo** ter ponastavite geslo in sledite navodilom na zaslonu ali pa si oglejte temo Pozabljeno geslo za račun ESET HOME.

Izbrana možnost prijave se ne ujema z vašim računom

Vaš račun je povezan z vašim računom na družbenih medijih. Če se želite prijaviti v račun ESET HOME, kliknite **Nadaljuj z računom Google** ali **Nadaljuj z računom Apple** ter se prijavite v ustrezni račun. Po uspešni prijavi boste preusmerjeni na spletno stran ESET HOME za potrditev. Na portalu ESET HOME lahko prekinete povezavo vašega računa ESET HOME z vašim računom z družbenega medija.

Geslo ni pravilno

Do te napake lahko pride, če je vaš izdelek ESET Internet Security že povezan z računom ESET HOME in če uvajate spremembe, za katere je potrebna prijava (npr. za onemogočenje možnosti Anti-Theft), pri čemer se vneseno geslo ne ujema z vašim računom. Kliknite možnost **Nazaj** in vnesite pravilno geslo. Če prijava še vedno ni mogoča, kliknite **Nazaj** > **Pozabljeno geslo** ter ponastavite geslo in sledite navodilom na zaslonu ali pa si oglejte temo Pozabljeno geslo za račun ESET HOME.

Dodajanje naprave v račun ESET HOME

Če ste izdelek ESET Internet Security že namestili in aktivirali z naročnino, dodano v vaš račun ESET HOME, lahko svojo napravo z računom ESET HOME povežete ob uporabi portala ESET HOME:

1. V napravo pošljite zahtevo za povezavo.

2. Izdelek ESET Internet Security prikaže pogovorno okno **Povezovanje naprave z računom ESET HOME** z imenom računa ESET HOME. Napravo z omenjenim računom ESET HOME povežete tako, da kliknete **Dovoli**.

Če do interakcije ne pride, bo zahteva za povezavo po približno 30 minutah samodejno preklicana.

Napredne nastavitve

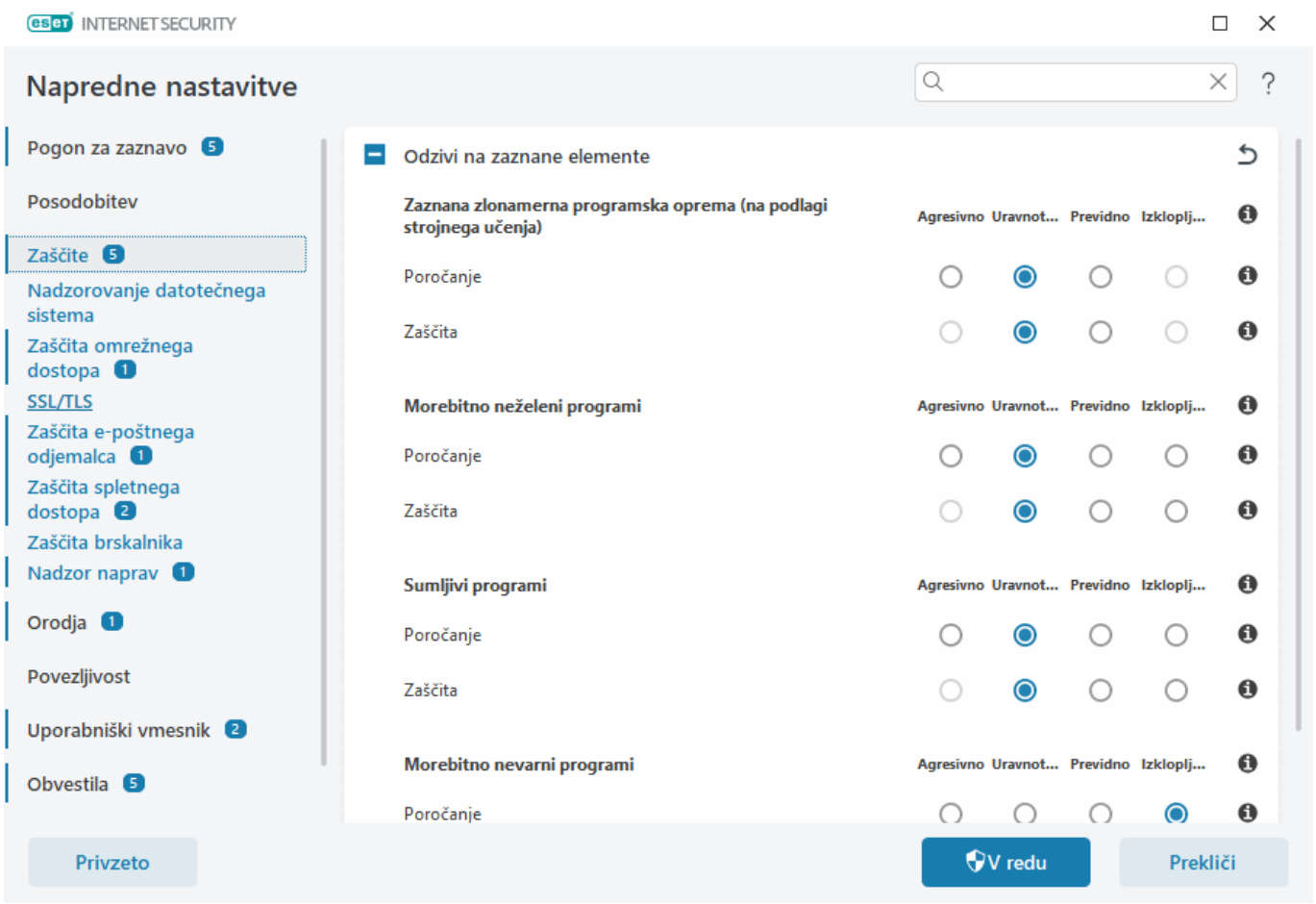
Napredne nastavitve omogočajo konfiguriranje podrobnih nastavitev za ESET Internet Security, ki ustrezajo vašim potrebam.

Če želite odpreti napredne nastavitve, odprite glavno okno programa in pritisnite tipko **F5** na tipkovnici ali pa kliknite **Nastavitve** > **Napredne nastavitve**.

Glede na vaše nastavitve dostopa boste morda pozvani, da vnesete geslo, če želite odpreti napredne nastavitve.

V naprednih nastavitvah lahko konfigurirate naslednje nastavitve:

- Pogon za zaznavo
- Posodabljanje
- Zaščite
- Orodja
- Povezljivost
- Uporabniški vmesnik
- Obvestila
- Nastavitve zasebnosti



Pogon za zaznavo

Napredne nastavitve > **Pogon za zaznavo** omogoča, da konfigurirate naslednje možnosti:

- Izključitve
- Napredne možnosti
- Pregledovalnik omrežnega prometa

Izključitve

Z **izključitvami** lahko izključite predmete iz pogona za zaznavo. Če želite zagotoviti, da pregleda vse predmete, priporočamo, da izključitve ustvarite samo v res nujnih primerih. Med primere, v katerih morate morda izključiti predmet, spada pregledovanje vnosov v veliki zbirki podatkov, ki bi upočasnilo delovanje računalnika, ali programske opreme, ki je v sporu s pregledom.

Izključitve delovanja – izključite datoteke in mape iz pregledovanja. Izključitve delovanja so uporabne za izključevanje pregledovanja programov za igre na ravni datotek ali v primeru neobičajnega delovanja sistema ali povečane učinkovitosti delovanja.

Izključitve zaznav vam omogočajo izključitev predmetov iz nabora zaznanih elementov ob uporabi imena, poti ali zgoščene vrednosti zaznav. Izključitve zaznav iz pregleda ne izključijo datotek in map tako kot izključitve delovanja. Izključitve zaznav elemente izključijo le, če slednje zazna pogon za zaznavo in če je na seznamu za izključitev ustrezno pravilo.

Ne smete jih zamenjati z drugimi vrstami izključitev:

- Izključitve postopkov – iz pregledovanja so izključeni postopki datotek, povezani s postopki izključenih programov (morda potrebno za izboljšanje hitrosti varnostnega kopiranja in razpoložljivosti storitev),
- Izključene datotečne pripone,
- Izključitve sistema HIPS,
- Filter za izključevanje za zaščito v oblaku.

Izključitve delovanja

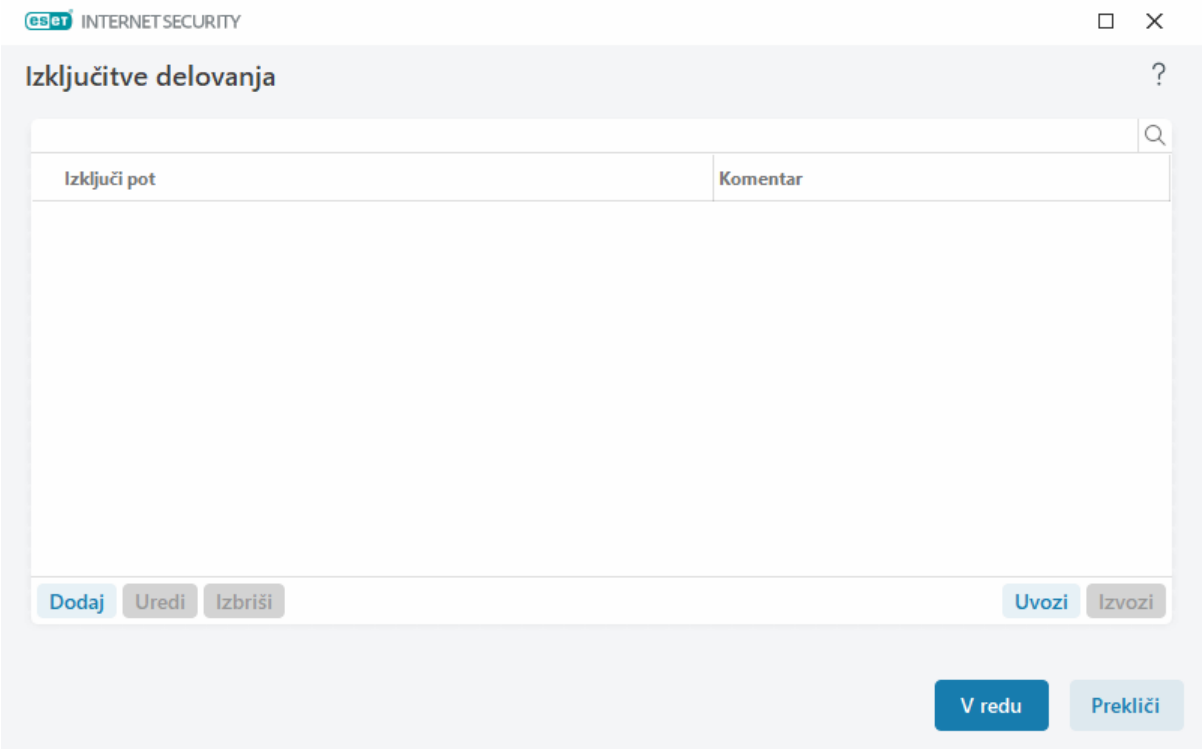
Z izključitvami delovanja lahko izključite datoteke in mape iz pregledovanja.

Če želite zagotoviti, da program pregleda vse predmete in preveri, ali so v njih grožnje, vam priporočamo, da izključitve ustvarite samo v res nujnih primerih. Vendar pa boste v nekaterih primerih morda morali izključiti predmet. Med te primere spadajo na primer vnosi v velike zbirke podatkov, zaradi katerih bi se lahko med pregledovanjem upočasnilo delovanje računalnika, ali programska oprema, ki je v sporu s pregledom.

Datoteke in mape, ki jih želite izključiti iz pregledovanja, lahko na seznam izključitev dodate tukaj: Napredne nastavitve > **Pogon za zaznavo** > **Izključitve** > **Izključitve delovanja** > **Uredi**.

> Ta funkcija ni enaka funkciji Izključitve delovanja, Izključene datotečne pripone, Izključitve sistema HIPS ali Izključitve postopkov.

Če želite izključiti predmet (pot: datoteka ali mapa) iz pregledovanja, kliknite **Dodaj** in vnesite ustrezno pot ali ga izberite v drevesni strukturi.



Modul **sprotne zaščite datotečnega sistema** ali modul **pregleda računalnika** ne bo zaznal grožnje v datoteki, če datoteka izpolnjuje pogoje za izključitev iz pregleda.

Elementi kontrolnika

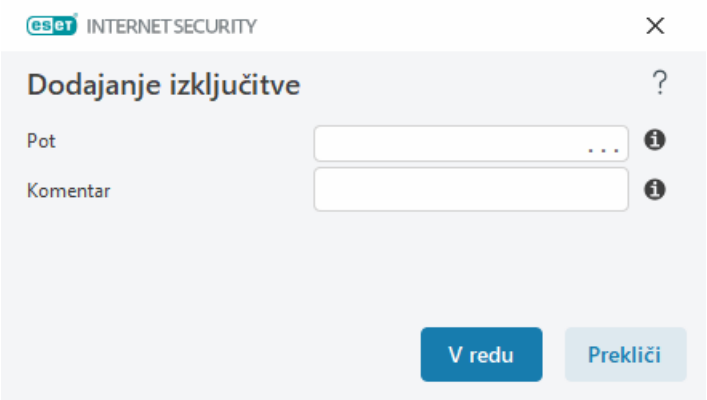
- **Dodaj** – izključi predmete iz zaznavanja.
- **Uredi** – omogoča urejanje izbranih vnosov.
- **Izbriši** – odstrani izbrane vnose (CTRL + kliknite za izbiro več vnosov).

Dodajanje ali urejanje izključitve delovanja

V tem pogovornem oknu lahko izključite določeno pot (datoteko ali imenik) za ta računalnik.

Izbira ali ročni vnos poti

Ustrezno pot lahko izberete tako, da kliknete **...** v polju **Pot**.
Za ročni vnos poti si spodaj oglejte več primerov oblike zapisa izključitve.



Skupino datotek lahko izključite z nadomestnimi znaki. Vprašaj (*?*) predstavlja en znak, medtem ko zvezdica (***) predstavlja niz z nič ali več znaki.

Oblika zapisa izključitev

- Če želite izključiti vse datoteke in podmape v mapi, vnesite pot do nje in uporabite masko ***
- Če želite izključiti le datoteke doc, uporabite masko **.doc*
- Če ima ime izvedljive datoteke določeno število znakov (in se ti znaki razlikujejo), vi pa poznate le prvi znak (recimo »D«), uporabite to obliko zapisa:
D????.exe (vprašaji nadomestijo manjkajoče/neznane znake)

Primeri:

- *C:\Tools** – pot se mora končati s poševnico nazaj (\) in zvezdico (*), kar označuje, da je to mapa, vsa vsebina mape (datoteke in podmape) pa bo izključena.
- *C:\Tools*.** – enako vedenje kot *C:\Tools**
- *C:\Tools* – mapa *Tools* ne bo izključena. Za pregledovalnik je *Tools* lahko tudi kot ime datoteke.
- *C:\Tools*.dat* – s tem bodo izključene datoteke .dat v mapi *Tools*.
- *C:\Tools\sg.dat* – s tem bo izključena točno ta datoteka na točno tej poti.

Sistemske spremenljivke v izključitvah

S sistemskimi spremenljivkami, npr. %PROGRAMFILES%, lahko določite iz pregleda.

- Če želite mapo Programske datoteke izključiti s to sistemsko spremenljivko, uporabite pot *%PROGRAMFILES%** (na koncu poti je treba dodati poševnico nazaj in zvezdico), ko dodajate izključitve.
- Če želite izključiti vse datoteke in mape v podimeniku *%PROGRAMFILES%*, uporabite pot *%PROGRAMFILES%\Excluded_Directory**

Razširjen seznam podprtih sistemskih spremenljivk

V obliki zapisa izključitve poti je mogoče uporabiti naslednje spremenljivke:

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

Uporabniške sistemske spremenljivke (npr. *%TEMP%* ali *%USERPROFILE%*) ali okoljske spremenljivke (npr. *%PATH%*) niso podprte.

Nadomestni znaki znotraj poti niso podprti

Uporaba nadomestnih znakov znotraj poti (na primer *C:\Tools*\Data\file.dat*) lahko deluje, vendar ni uradno podprta za izključitve delovanja.
Pri izključitvah zaznav ni omejitev glede uporabe nadomestnih znakov na sredini poti.

Vrstni red izključitev

- Za nastavitev prednostne ravni za izključitve možnosti razvrščanja z gumbi od vrha proti dnu niso na voljo (kot pri možnosti Pravila za požarni zid, kjer se pravila izvajajo od vrha proti dnu).
- Ko pregledovalnik najde prvo ujemajoče pravilo, drugo veljavno pravilo ne bo ovrednoteno.
- Manjše število pravil omogoča boljše delovanje pregledovalnika.
- Odsvetujemo ustvarjanje sočasnih pravil.

Oblika zapisa izključitve poti

Skupino datotek lahko izključite z nadomestnimi znaki. Vprašaj (*?*) predstavlja en znak, medtem ko zvezdica (***) predstavlja niz z nič ali več znaki.

Oblika zapisa izključitev

- Če želite izključiti vse datoteke in podmape v mapi, vnesite pot do nje in uporabite masko ***
- Če želite izključiti le datoteke doc, uporabite masko **.doc*
- Če ima ime izvedljive datoteke določeno število znakov (in se ti znaki razlikujejo), vi pa poznate le prvi znak (recimo »D«), uporabite to obliko zapisa:
D????.exe (vprašaji nadomestijo manjkajoče/neznane znake)

Primeri:

- *C:\Tools** – pot se mora končati s poševnico nazaj (\) in zvezdico (*), kar označuje, da je to mapa, vsa vsebina mape (datoteke in podmape) pa bo izključena.
- *C:\Tools*.** – enako vedenje kot *C:\Tools**
- *C:\Tools* – mapa *Tools* ne bo izključena. Za pregledovalnik je *Tools* lahko tudi kot ime datoteke.
- *C:\Tools*.dat* – s tem bodo izključene datoteke .dat v mapi *Tools*.
- *C:\Tools\sg.dat* – s tem bo izključena točno ta datoteka na točno tej poti.

Sistemske spremenljivke v izključitvah

S sistemskimi spremenljivkami, npr. %PROGRAMFILES%, lahko določite iz pregleda.

- Če želite mapo Programske datoteke izključiti s to sistemsko spremenljivko, uporabite pot *%PROGRAMFILES%** (na koncu poti je treba dodati poševnico nazaj in zvezdico), ko dodajate izključitve.
- Če želite izključiti vse datoteke in mape v podimeniku *%PROGRAMFILES%*, uporabite pot *%PROGRAMFILES%\Excluded_Directory**

Razširjen seznam podprtih sistemskih spremenljivk

V obliki zapisa izključitve poti je mogoče uporabiti naslednje spremenljivke:

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

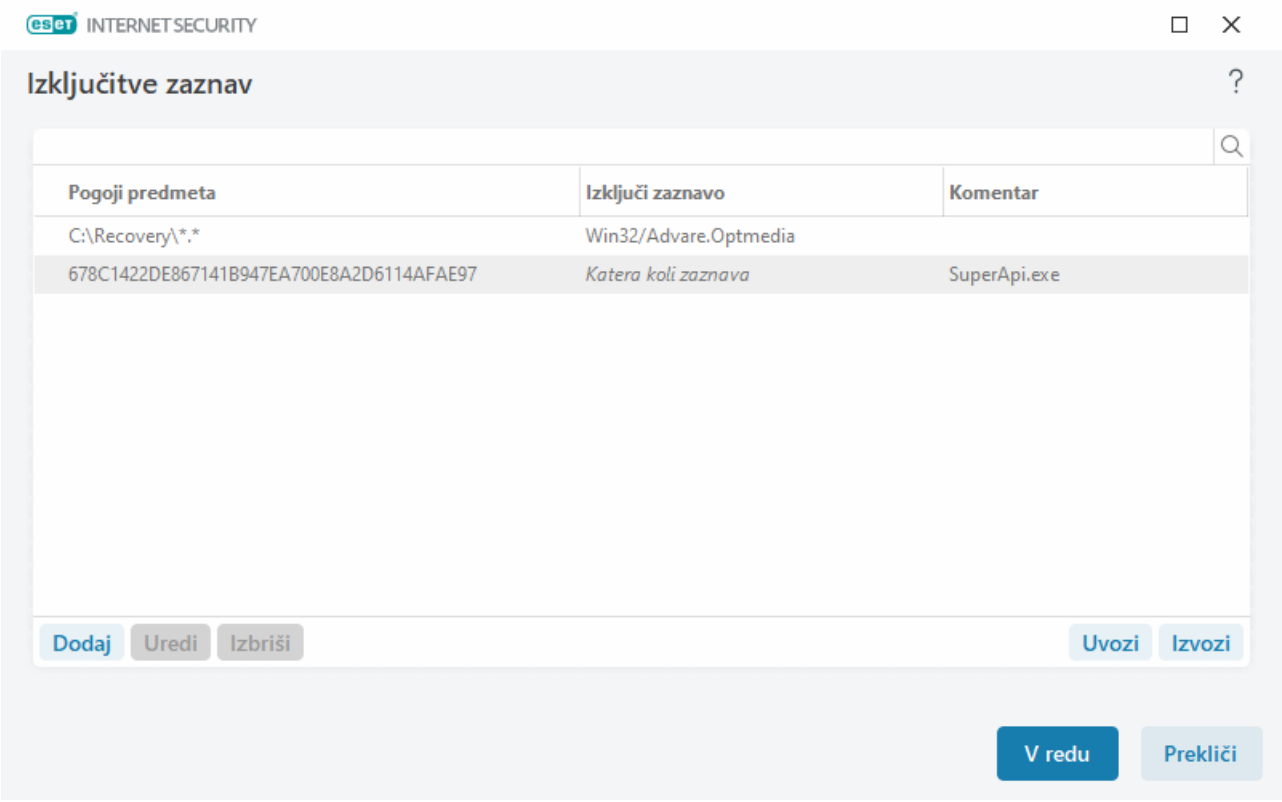
Uporabniške sistemske spremenljivke (npr. *%TEMP%* ali *%USERPROFILE%*) ali okoljske spremenljivke (npr. *%PATH%*) niso podprte.

Izključitve zaznav

Izključitve zaznav vam omogočajo izključitev predmetov iz nabora zaznanih elementov s pomočjo filtriranja zaznanega imena, poti predmeta ali njegove zgoščene vrednosti.

Delovanje izključitev zaznav

Izključitve zaznav ne izključijo datotek in map iz pregledovanja kot izključitve delovanja. Izključitve zaznav elemente izključijo le, če slednje zazna pogon za zaznavo in če je na seznamu za izključitev ustrezno pravilo. Na primer, če je predmet zaznan kot Win32/Adware.Optmedia in je zaznana datoteka *C:\Recovery\file.exe* (glejte prvo vrstico na spodnji sliki). Vsaka datoteka z ustrezno zgoščena vrednostjo SHA-1 bo vedno izključena ne glede na ime zaznave (glejte drugo vrstico).



Priporočamo, da ustvarite izključitve zaznavanja le, če je nujno potrebno, saj bodo le tako lahko zaznane vse grožnje.

Če želite dodati datoteke in mape na seznam izključitev, izberite Napredne nastavitve > **Pogon za zaznavo** > **Izključitve** > **Izključitve zaznav** > **Uredi**.

Ta funkcija ni enaka funkciji Izključitve delovanja, Pripone datotek, izključenih iz pregledovanja, Izključitve sistema HIPS ali Izključitve postopkov.

Če želite izključiti predmet (na podlagi imena zaznave ali zgoščene vrednosti) iz pogona za zaznavo, kliknite **Dodaj**.

Za morebitno neželene programe in morebitno nevarne programe je mogoče ustvariti tudi izključitev z imenom zaznenga elementa:

- V oknu opozorila, ki poroča o zaznavanju (kliknite **Pokaži dodatne možnosti** in nato izberite možnost **Izključi iz zaznave**).
- V priročnem meniju dnevniških datotek s funkcijo Čarovnik za ustvarjanje izključitev zaznav.
- V razdelku **Orodja** > **Karantena** z desno tipko miške kliknete datoteko, ki je v karanteni, in v priročnem meniju izberete možnost **Obnovi in izključi iz pregleda**.

Pogoji predmeta za izključitve zaznav

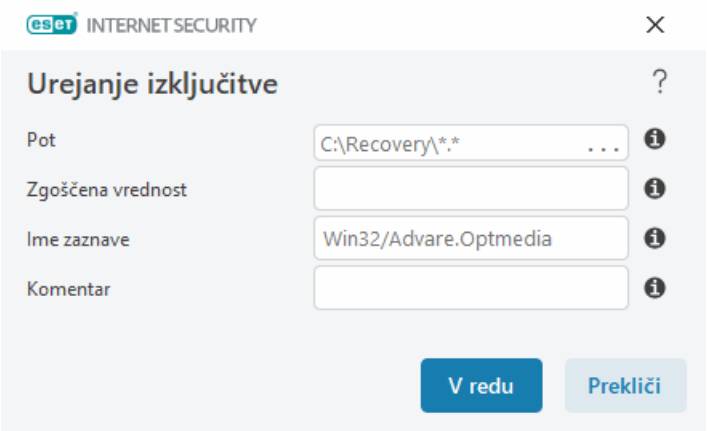
- **Pot** – omejite izključitev zaznave za določeno pot (ali poljubno pot).
- **Ime zaznave** – če je poleg izključene datoteke ime zaznanega elementa, to pomeni, da je datoteka izključena le za dano odkrivanje, ne pa v celoti. Če se ta datoteka kasneje okuži z drugo zlonamerno programsko opremo, bo zaznana.
- **Zgoščena vrednost** – izključi datoteko na podlagi določene zgoščene vrednosti SHA-1 ne glede na vrsto, lokacijo, ime ali pripono datoteke.

Dodajanje ali urejanje izključitve zaznav

Izključi zaznavo

Navedeno mora biti veljavno ime zaznave ESET. Če želite veljavno ime zaznave, glejte Dnevniške datoteke in nato na spustnem seznamu Dnevniške datoteke izberite **Zaznave**. To je koristno, če ESET Internet Security zazna napačno pozitiven vzorec. Izključitve pravih infiltracij s zelo nevarne, zato priporočamo izključevanje samo datotek/imenikov, datoteke, na katere je vplivala infiltracija, in s, da kliknete **...** v polju **Maska poti** in/ali le za določeno časovno obdobje. Izključitve veljajo tudi za morebitno neželene programe, morebitno nevarne programe in sumljive programe.

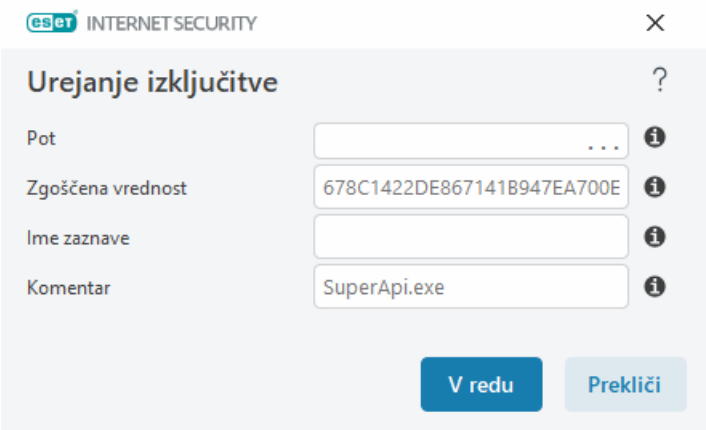
Glejte tudi razdelek Oblika zapisa izključitve poti.



Glejte razdelek Primer izključitev zaznave spodaj.

Izključi zgoščeno vrednost

Izključi datoteko na podlagi določene zgoščene vrednosti SHA-1 ne glede na vrsto, lokacijo, ime ali pripono datoteke.



Izključitve glede na ime zaznave

Če želite izključiti določeno zaznavo glede na njeno ime, vnesite veljavno ime zaznave:
Win32/Adware.Optmedia
Če želite zaznavo izključiti v oknu z opozorilom programa ESET Internet Security, lahko uporabite tudi naslednjo obliko zapisa:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Elementi kontrolnika

- **Dodaj** – izključi predmete iz zaznavanja.
- **Uredi** – omogoča urejanje izbranih vnosov.
- **Izbriši** – odstrani izbrane vnose (CTRL + kliknite za izbiro več vnosov).

Čarovnik za ustvarjanje izključitev zaznav

Izključitev zaznave lahko ustvarite tudi v priročnem meniju Dnevniške datoteke (ni na voljo za zaznave zlonamerne programske opreme):

1. V glavnem oknu programa kliknite **Orodja** > **Dnevniške datoteke**.
2. Z desno tipko miške kliknite zaznani element v **dnevniku zaznanih elementov**.
3. Kliknite **Ustvari izključitev**.

Če želite izključiti enega ali več zaznanih elementov na podlagi **pogojev za izključitev**, kliknite **Spremeni pogoje**:

- **Točne datoteke** – izključi vsako datoteko na podlagi zgoščene vrednosti SHA-1.
- **Zaznava** – izključi vsako datoteko glede na ime zaznave.
- **Pot + zaznava** – izključi vsako datoteko na podlagi imena in poti, vključno z imenom datoteke (npr. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Glede na vrsto zaznave je predhodno izbrana priporočena možnost.

Po želji lahko dodate **komentar** in nato kliknete **Ustvari izključitev**.

Napredne možnosti pogona za zaznavo

Omogoči napredno pregledovanje prek vmesnika AMSI je Microsoftovo orodje Antimalware Scan Interface ter omogoča pregledovanje skriptov PowerShell, skriptov, ki jih izvaja Windows Script Host, in podatkov, ki so pregledani prek SDK-ja AMSI.

Pregledovalnik omrežnega prometa

Pregledovalnik omrežnega prometa zagotavlja zaščito pred zlonamerno programsko opremo za protokole programov, ki integrira več naprednih tehnik pregledovanja zlonamerne programske opreme. Pregledovalnik omrežnega prometa samodejno pregleda protokole HTTP(S), POP3(S) in IMAP(S), ne glede na internetni brskalnik ali e-poštni odjemalec. Pregledovalnik omrežnega prometa lahko omogočite/onemogočite v razdelku Napredne nastavitve > **Pogon za zaznavo** > **Pregledovalnik omrežnega prometa**.

Omogoči pregledovalnik omrežnega prometa – če onemogočite to možnost, protokoli HTTP(S), POP3(S) in IMAP(S) ne bodo pregledani. Upoštevajte, da naslednje funkcije programa ESET Internet Security zahtevajo omogočen pregledovalnik omrežnega prometa:

- Zaščita spletnega dostopa
- Starševski nadzor
- Zasebnost in varnost brskalnika
- Varno bančništvo in brskanje
- SSL/TLS
- Preprečevanje lažnega predstavljanja
- Zaščita e-poštnega odjemalca

Zaščita v oblaku

ESET LiveGrid® temelji na naprednemu sistemu zgodnjega opozarjanja ThreatSense.Net in uporablja podatke, ki so jih poslali uporabniki izdelkov ESET po svetu, ter jih pošlje v raziskovalni laboratorij družbe ESET. ESET LiveGrid® Navaja sumljive vzorce metapodatkov in nam tako omogoča, da se nemudoma odzovemo na potrebe strank in stalno posodabljajmo programsko opremo ESET.

Na voljo so naslednje možnosti:

Omogočite sistem ugleda ESET LiveGrid®

Sistem ugleda ESET LiveGrid® zagotavlja seznam varnih pošiljateljev in seznam blokiranih pošiljateljev v oblaku.

Preverite ugled možnosti Izvajajoči se procesi in datotek neposredno iz vmesnika programa ali priročnega menija z dodatnimi informacijami, ki so na voljo v tehnologiji ESET LiveGrid®.

Omogočite sistem za povratne informacije ESET LiveGrid®

Poleg sistema ugleda ESET LiveGrid® sistem za povratne informacije ESET LiveGrid® zbira podatke o vašem računalniku, povezane z novo zaznanimi grožnjami. Ti podatki lahko vključujejo naslednje elemente:

- Vzorec ali kopija datoteke, v kateri se je pojavila grožnja
- Pot do datoteke
- Ime datoteke
- Datum in ura
- Način, na katerega se je grožnja pojavila v vašem računalniku
- Podatki o operacijskem sistemu vašega računalnika

Izdelek ESET Internet Security je privzeto konfiguriran tako, da pošlje sumljive datoteke v podrobno analizo v virusni laboratorij družbe ESET. Datoteke z določenimi priponami, kot sta *.doc* ali *.xls*, so vedno izključene. Dodate lahko tudi druge pripone, če vi oz. vaša organizacija ne želita poslati določenih datotek.

Več o pošiljanju ustreznih podatkov lahko preberete v pravilniku o zasebnosti.

Odločite se lahko tudi, da tehnologije ESET LiveGrid® ne želite omogočiti.

Funkcij v programski opremi ne boste izgubili, vendar se lahko ESET Internet Security v nekaterih primerih hitreje odzove na nove grožnje, če je tehnologija ESET LiveGrid® omogočena. Če ste tehnologijo ESET LiveGrid® že uporabljali in ste jo zdaj onemogočili, nekateri podatkovni paketi morda še vedno čakajo na pošiljanje. Paketi bodo, tudi če jih deaktivirate, poslani družbi ESET. Ko so vse trenutne informacije poslane, ne bo ustvarjen noben nov paket.

Več o tehnologiji ESET LiveGrid® preberite v slovarju izrazov.
Oglejte si ilustrirana navodila, ki so na voljo v angleščini ter v nekaterih drugih jezikih in vsebujejo informacije o tem, kako omogočiti ali onemogočiti tehnologijo ESET LiveGrid® v izdelku ESET Internet Security.

Konfiguracija zaščite v oblaku v naprednih nastavitvah

Če želite dostopati do nastavitev za funkcijo ESET LiveGrid®, odprite razdelek Napredne nastavitve > **Pogon za zaznavo** > **Zaščita v oblaku**.

- **Omogoči sistem ugleda ESET LiveGrid® (priporočeno)** – sistem ugleda ESET LiveGrid® izboljša učinkovitost rešitev za zaščito pred zlonamerno programsko opremo družbe ESET, tako da primerja pregledane datoteke z zbirko varnih in blokiranih elementov v oblaku.

- **Omogoči sistem za povratne informacije ESET LiveGrid®** – pošlje ustrezne podatke za predložitev (opisani v **razdelku o predložitvi vzorcev** spodaj) skupaj s poročili o zrušitvah in statistiko v raziskovalni laboratorij družbe ESET za nadaljnjo analizo.

• **Pošlji poročila o zrušitvah in diagnostične podatke** – pošlje diagnostične podatke sistema ESET LiveGrid®, kot so poročila o zrušitvah in izvozi pomnilnikov modulov. Priporočamo, da imate to možnost omogočeno, saj bo to družbi ESET pomagalo diagnosticirati težave, izboljšati izdelke in zagotoviti zaščito končnih uporabnikov.

• **Pošlji anonimne statistične podatke** – dovolite, da ESET zbira podatke o novih odkritih grožnjah, kot je ime grožnje, čas in datum odkritja, način odkritja in povezani metapodatki, različica in konfiguracija izdelka, vključno z informacijami o vašem sistemu.

• **E-poštni naslov za stik (neobvezno)** – e-poštni naslov za stik je lahko dodan vsem sumljivim datotekam, prek njega pa lahko vzpostavimo stik z vami, če potrebujemo dodatne podatke za analizo. Če od vas ne bomo potrebovali dodatnih informacij, vam ESET ne bo poslal odgovora.

Predložitev vzorcev

Ročno pošiljanje vzorcev – omogoča možnost ročnega pošiljanja vzorcev družbi ESET iz priročnega menija, karantene ali razdelka Orodja.

Samodejno pošiljanje zaznanih vzorcev

Izberite, kateri vzorci bodo poslani družbi ESET za analizo in prihodnje izboljšanje zaznavanja (privzeta največja velikost vzorca je 64 MB). Na voljo so naslednje možnosti:

• **Vsi zaznani vzorci** – vsi predmeti, ki jih zazna pogon za zaznavo (vključno z morebitno neželenimi programi, ko je možnost omogočena v nastavitvah pregledovalnika).

• **Vsi vzorci razen dokumentov** – vsi zaznani predmeti razen **dokumentov** (glejte spodaj).

• **Ne predloži** – zaznani predmeti ne bodo poslani družbi ESET.

Samodejno pošiljanje sumljivih vzorcev

Ti vzorci bodo družbi ESET poslani, tudi če jih pogon za zaznavo ne zazna. Gre za vzorce, ki so se na primer skorajda izognili zaznavanju, ali pa za to, da eden od modulov zaščite za izdelek ESET Internet Security te vzorce obravnava kot sumljive ali jim pripiše nejasno vedenje (največja privzeta velikost vzorca je 64 MB).

• **Izvedljive datoteke** – ta možnost vključuje izvedljive datoteke, kot so .exe, .dll, .sys.

• **Arhivi** – ta možnost vključuje vrste arhivskih datotek, kot so .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Skripti** – ta možnost vključuje vrste skriptnih datotek, kot so .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Drugo** – vključuje vrste datotek kot .jar, .reg, .msi, .sfw, .lnk.

• **Morebitno neželena e-pošta** – s tem bo omogočeno pošiljanje delov morebitno neželenih e-poštnih sporočil ali celotnih morebitno neželenih e-poštnih sporočil s priponkami družbi ESET za nadaljnjo analizo. Če omogočite to možnost, bo izboljšano globalno zaznavanje neželene e-pošte, kar vključuje izboljšave zaznavanja neželene e-pošte za vas v prihodnosti.

• **Dokumenti** – vključujejo dokumente zbirke Microsoft Office ali PDF-je z aktivno vsebino ali brez nje.

Razširitev za seznam vseh vključenih vrst datotek dokumentov

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

Izključitve

Filter za izključevanje vam omogoča, da iz pošiljanja izključite določene datoteke/mape (ta možnost je na primer uporabna za izključitev datotek, v katerih so zaupni podatki, na primer dokumentov ali razpredelnic). Navedene datoteke ne bodo nikoli poslane laboratorijem družbe ESET v analizo, tudi če je v njih sumljiva koda. Najpogosteje uporabljene vrste datotek so privzeto izključene (.doc itn.). Če želite, lahko seznam izključenih datotek dopolnjujete.

Če želite izključiti datoteke, prenesene s spletnega mesta `download.domain.com`, odprite razdelek Napredne nastavitve > **Pogon za zaznavo** > **Zaščita v oblaku** > **Predložitev vzorcev** in kliknite možnost **Uredi** poleg možnosti **Izključitve**. Dodajte izključitev `.download.domain.com`.

Največja velikost vzorcev (MB) – določa največjo velikost samodejno poslanih vzorcev (1–64 MB).

Filter za izključevanje za zaščito v oblaku

Filter za izključevanje omogoča izključitev nekaterih datotek ali map iz pošiljanja vzorcev. Navedene datoteke ne bodo nikoli poslane laboratorijem družbe ESET v analizo, tudi če je v njih sumljiva koda. Pogosto uporabljene vrste datotek so privzeto izključene (npr. .doc itd.).

Ta funkcija je uporabna za izključevanje datotek, v katerih so morda zaupni podatki, na primer dokumenti ali preglednice.

Če želite izključiti datoteke, prenesene s spletnega mesta download.domain.com kliknite možnost Napredne nastavitve > **Pogon za zaznavo** > **Zaščita v oblaku** > **Predložitev vzorcev** > **Izključitve** in dodajte izključitev *download.domain.com*.

Pregledi zlonamerne programske opreme

Do razdelka **Pregledi zlonamerne programske opreme** je mogoče dostopati prek razdelka Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** in vam omogoča, da konfigurirate parametre pregleda za profile pregleda.

Pregled na zahtevo

Izbrani profil – nabor parametrov, ki jih uporablja pregledovalnik na zahtevo. Če želite ustvariti novega, kliknite **Uredi** ob možnosti **Seznam profilov**. Več informacij je na voljo v razdelku Profili pregleda.

Ko izberete profil pregleda, lahko konfigurirate naslednje možnosti:

Cilji pregleda – če želite pregledati določen cilj ali skupino ciljev ob možnosti **Cilji pregleda** kliknite **Uredi** in izberite možnost v (drevesni) strukturi mape. Več informacij je na voljo v razdelku Cilji pregleda.

Zaščita na zahtevo s strojnim učenjem – za vsak profil pregleda lahko konfigurirate ravni poročanja in zaščite.

Profili pregleda privzeto uporabljajo enako nastavitev, kot je opredeljena v možnosti Sprotna zaščita datotečnega sistema. Onemogočite gumb za preklop ob možnosti **Uporaba nastavitev sprotne zaščite** za konfiguracijo ravni poročanja in zaščite po meri. Za podrobnejšo razlago ravni poročanja in zaščite glejte Zaščite.

ThreatSense – napredne možnosti nastavitev, kot so datotečne pripone, ki jih želite nadzorovati, in uporabljeni načini zaznavanja. Za več informacij glejte ThreatSense.

Profili pregleda

V programu ESET Internet Security so 4 vnaprej določeni profili pregleda:

- **Pametni pregled**: to je privzeti napredni profil pregleda. Profil pametnega pregleda uporablja tehnologijo pametne optimizacije, ki preskoči datoteke, ki so bile med prejšnjim pregledom neproblematične in od takrat niso bile spremenjene. To omogoča krajši čas pregleda z najmanjšim možnim vplivom na varnost sistema.

- **Pregled priročnega menija** – zahtevate lahko pregled katere koli datoteke iz priročnega menija. Profil pregleda priročnega menija omogoča, da določite konfiguracijo pregleda, ki se uporablja pri tovrstnem zagonu pregleda.

- **Poglobljen pregled** – profil poglobljenega preglede privzeto ne uporablja pametne optimizacije, zato pri uporabi tega profila niso izpuščene nobene datoteke.

- **Pregled računalnika** – to je privzeti profil, ki se uporablja pri standardnem pregledu računalnika.

Prednostne parametre pregleda lahko shranite za pregledovanje v prihodnje. Priporočamo, da za vsak pregled, ki ga redno uporabljate, ustvarite drugačen profil (z različnimi cilji in načini pregleda ter drugimi parametri).

Če želite ustvariti nov profil, odprite okno razdelek Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** > **Pregled na zahtevo** > **Seznam profilov** > **Uredi**. V oknu **Upravitelj profila** je spustni meni **Izbrani profil** z obstoječimi profili pregleda in možnost za ustvarjanje novega profila. Če želite ustvariti profil pregleda, ki bo ustrezal vašim potrebam, glejte razdelek ThreatSense, v katerem boste našli opis vseh parametrov nastavitev pregleda.

> Recimo, da želite ustvariti lasten profil pregleda in konfiguracija **Preglejte računalnik** deloma ustreza vašim potrebam, vendar ne želite pregledati samoustvarjenih arhivov ali morebitno nevarnih programov, poleg tega pa želite uporabiti še možnost **Vedno popravi zaznani element**. V okno **Upravitelj profila** vnesite ime svojega novega profila in kliknite **Dodaj**. Iz spustnega menija **Izbrani profil** izberite svoj novi profil in preostale parametre prilagodite tako, da ustrezajo vašim zahtevam, nato za shranjevanje kliknite možnost **V redu**.

Cilji pregleda

Spustni meni **Cilji pregleda** omogoča, da izberete vnaprej določene cilje pregleda.

- **Po nastavitvah profila** – izbere cilje, določene v izbranem profilu pregleda.
- **Izmenljivi nosilci podatkov** – izbere diskete, naprave za shranjevanje USB, CD-je/DVD-je.

- **Lokalni pogoni** – izbere vse trde diske sistema.

- **Omrežni pogoni** – izbere vse preslikane omrežne pogone.
- **Izbor po meri** – prekliče vse prejšnje izbire.

Struktura mape (drevesa) vsebuje tudi določene cilje pregleda.

- **Delovni pomnilnik** – pregleda vse procese in podatke, ki jih trenutno uporablja delovni pomnilnik.
- **Zagonski sektorji/UEFI** – pregleda zagonske sektorje in UEFI za prisotnost zlonamerne programske opreme. Preberite več o pregledovalniku za UEFI v slovarčku.
- **Zbirka podatkov WMI** – pregleda celotno zbirko podatkov Windows Management Instrumentation (WMI), vse imenske prostore, vse primerke razredov in vse lastnosti. Išče sklice na okuženo datoteko ali zlonamerno programsko opremo, vdelano kot podatke.
- **Sistemski register** – pregleda celoten sistemski register, vse ključe in podključe. Išče sklice na okuženo datoteko ali zlonamerno programsko opremo, vdelano kot podatke. Pri čiščenju zaznanih elementov ostane sklic v registru, da se zagotovi, da ne bodo izgubljeni nobeni pomembni podatki.

Če se želite hitro pomakniti na cilj pregleda (datoteka ali mapa), vnesite njegovo pot v besedilno polje pod drevesno strukturo. Pot razlikuje med malimi in veliki črkami. Če želite cilj vključiti v pregled, izberite njegovo potrditveno polje v drevesni strukturi.

Pregled v mirovanju

Pregledovanje v mirovanju lahko omogočite v razdelku Napredne nastavitve > **Orodje za zaznavanje** > **Pregledi zlonamerne programske opreme** > **Pregledovanje v mirovanju**.

Pregled v mirovanju

Omogočite gumb za preklop ob možnosti **Omogoči pregledovanje v mirovanju**, da omogočite to funkcijo. Ko je računalnik v mirovanju, se v njem na vseh lokalnih diskih izvede tiho pregledovanje.

Funkcija pregledovanja v mirovanju se privzeto ne zažene, če se računalnik (prenosnik) napaja iz akumulatorja. To nastavitev lahko preglasite tako, da v naprednih nastavitvah zraven možnosti **Zaženi, tudi če se računalnik napaja iz akumulatorja** omogočite gumb za preklop.

V naprednih nastavitvah omogočite gumb za preklop zraven možnosti **Omogoči pisanje dnevnika**, da zapišete rezultat pregleda računalnika v razdelku Dnevniške datoteke (v glavnem oknu programa kliknite **Orodja** > **Dnevniške datoteke** in v spustnem meniju **Dnevnik** izberite **Pregled računalnika**).

Zaznavanje stanja mirovanja

Seznam vseh pogojev, ki morajo biti izpolnjeni za sprožitev funkcije pregledovanja v mirovanju, najdete v razdelku Sprožilci zaznavanja stanja mirovanja.

ThreatSense – napredne možnosti nastavitev, kot so datotečne pripone, ki jih želite nadzorovati, in uporabljeni načini zaznavanja. Za več informacij glejte ThreatSense.

Zaznavanje stanja mirovanja

Nastavitve zaznavanja stanja mirovanja lahko konfigurirate v razdelku Napredne nastavitve > **Orodje za zaznavanje** > **Pregledi zlonamerne programske opreme** > **Pregledovanje v mirovanju** > **Zaznavanje stanja mirovanja**. Te nastavitve določajo sprožilec za pregledovanje v mirovanju:

- **Izklopljen zaslon ali ohranjevalnik zaslona**
- **Zaklep računalnika**
- **Odjava uporabnika**

Uporabite gumb za preklop za vsako posamezno stanje in omogočite ali onemogočite sprožilce za zaznavanje stanja mirovanja.

Zagonski pregled

Ob zagonu sistema in med posodobitvami orodja za zaznavanje je privzeto izveden samodejni zagon pregledovanja datotek. Ta pregled je odvisen od konfiguracije in opravil urnika opravil.

Možnosti pregleda ob zagonu so del opravila **Preverjanje datotek ob zagonu sistema** razporejevalnika opravil. Če želite prilagoditi njegove nastavitve, odprite **Orodja** > **Urnik opravil**, kliknite **Samodejni zagon pregledovanja datoteke** in nato **Uredi**. Pri zadnjem koraku se prikaže okno Samodejni zagon pregledovanja datotek. Če želite podrobnejša navodila o ustvarjanju in upravljanju opravil razporejevalnika, glejte Ustvarjanje novih opravil.

ThreatSense – napredne možnosti nastavitev, kot so datotečne pripone, ki jih želite nadzorovati, in uporabljeni načini zaznavanja. Za več informacij glejte ThreatSense.

Samodejni zagon pregledovanja datotek

Ko ustvarjate načrtovano opravilo preverjanja datotek ob zagonu sistema, lahko na več načinov prilagodite te parametre:

Spustni meni **Predmet pregleda** določi globino pregleda za datoteke, ki se zaženejo ob zagonu sistema, glede na skrivni napredni algoritem. Datoteke so razporejene v padajočem vrstnem redu skladno s temi kriteriji:

- **Vse registrirane datoteke** (pregledanih je največ datotek)
- **Redko uporabljene datoteke**
- **Običajno uporabljene datoteke**
- **Pogosto uporabljene datoteke**
- **Samo datoteke, ki so največkrat uporabljene** (pregledanih je najmanj datotek)

Vključeni sta tudi dve določeni skupini:

- **Datoteke, zagnane pred prijavo uporabnika** – v tej skupini so datoteke mest, do katerih lahko dostopate

brez prijave uporabnika (vključuje večino mest zagona, na primer storitve, predmete za pomoč brskalniku, obvestila o prijavi v sistem Windows, vnose razporejevalnika v sistemu Windows, poznane knjižnice DLL itd).

- **Datoteke, zagnane po prijavi uporabnika** – v tej skupini so datoteke mest, do katerih uporabnik lahko dostopa le po prijavi (vključuje datoteke, ki jih zažene le določeni uporabnik, običajno so to datoteke v *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Seznami datotek, ki jih je treba pregledati, so določeni za vsako zgornjo skupino. Če za datoteke, ki se zaženejo ob zagonu sistema, izberete manjšo globino pregledovanja, bodo nepreiskane datoteke pregledane ob odprtju ali izvajanju.

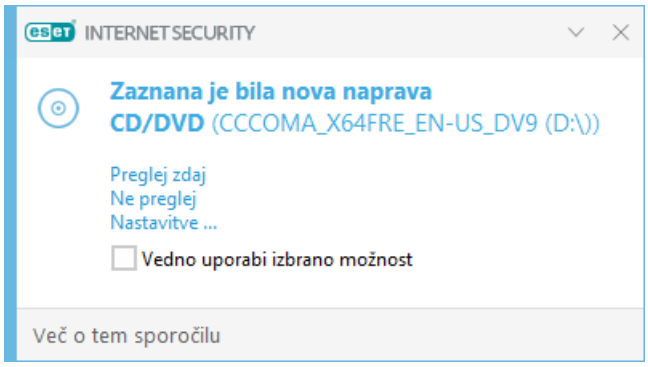
Prioriteta pregleda – raven prioritete, s katero določite začetek pregleda:

- **Pri nedejavnosti** – opravilo se izvede le, če je sistem nedejaven,
- **Najnižja** – ko je obremenitev sistema na najnižji možni ravni,
- **Nizka** – pri nizki obremenitvi sistema,
- **Navadna** – pri povprečni obremenitvi sistema.

Izmenljivi nosilci podatkov

Program ESET Internet Security omogoča samodejno pregledovanje izmenljivih nosilcev podatkov (CD/DVD/USB ...) po vstavljanju v računalnik. Ta funkcija je uporabna, če želi skrbnik računalnika uporabnikom preprečiti uporabo izmenljivih nosilcev podatkov z neželeno vsebino.

Ko je vstavljen izmenljivi nosilec podatkov in je v razdelku Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** > **Izmenljivi nosilci podatkov** nastavljena možnost **Prikaz možnosti pregleda**, se prikaže naslednje pogovorno okno:



Možnosti v tem pogovornem oknu:

- **Preglej zdaj** – s tem ukazom se sproži pregledovanje izmenljivih nosilcev.
- **Ne preglej** – izmenljivi nosilci podatkov ne bodo pregledani.
- **Nastavitev** – odpre napredne nastavitve.
- **Vedno uporabi izbrano možnost** – ko je izbrana ta možnost, se bo enako dejanje izvedlo tudi, ko bo izmenljivi nosilec naslednjič vstavljen.

Poleg tega program ESET Internet Security omogoča tudi funkcijo nadzora naprave, s katero lahko določate pravila za uporabo zunanjih naprav v danem računalniku. Podrobnejša navodila o nadzoru naprave najdete v razdelku Nadzor naprav.

Za dostop do nastavitev za pregled izmenljivih nosilcev podatkov odprite Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** > **Izmenljivi nosilci podatkov**.

Dejanje po vstavitvi izmenljivega nosilca podatkov – izberite privzeto dejanje, ki bo izvedeno, ko bo v računalnik vstavljen izmenljivi nosilec podatkov (CD/DVD/USB). Izberete želeno dejanje, ki se bo izvedlo po vstavitvi izmenljivega nosilca podatkov v računalnik:

- **Ne preglej** – nobeno dejanje ne bo izvedeno, okno **Zaznana je bila nova naprava** pa se ne odpre.
- **Samodejni pregled naprave** – vstavljeni izmenljivi nosilec podatkov bo pregledan s postopkom pregleda računalnika.
- **Prikaži možnosti pregledovanja** – odpre razdelek za nastavitev **izmenljivih nosilcev podatkov**.

Zaščita dokumentov

Funkcija zaščite dokumentov pregleda dokumente sistema Microsoft Office, preden jih odprete, in datoteke, ki jih Internet Explorer samodejno prenese, na primer elemente Microsoft ActiveX. Funkcija zaščite dokumentov poleg sprotne zaščite datotečnega sistema zagotavlja tudi dodatno zaščito, ki jo lahko onemogočite, če želite izboljšati učinkovitost delovanja sistemov, ki ne obravnavajo velikega števila dokumentov Microsoft Office.

Če želite aktivirati funkcijo Zaščita dokumentov, odprite razdelek Napredne nastavitve > **Pogon za zaznavo** > **Pregledi zlonamerne programske opreme** > **Zaščita dokumentov**, nato pa kliknite gumb za preklop ob možnosti **Omogoči zaščito dokumentov**.

ThreatSense – napredne možnosti nastavitev, kot so datotečne pripone, ki jih želite nadzorovati, in uporabljeni načini zaznavanja. Za več informacij glejte ThreatSense.

Funkcijo aktivirajo aplikacije, ki uporabljajo Microsoft Antivirus API (npr. Microsoft Office 2000 in novejše različice ali Microsoft Internet Explorer 5.0 in novejše različice).

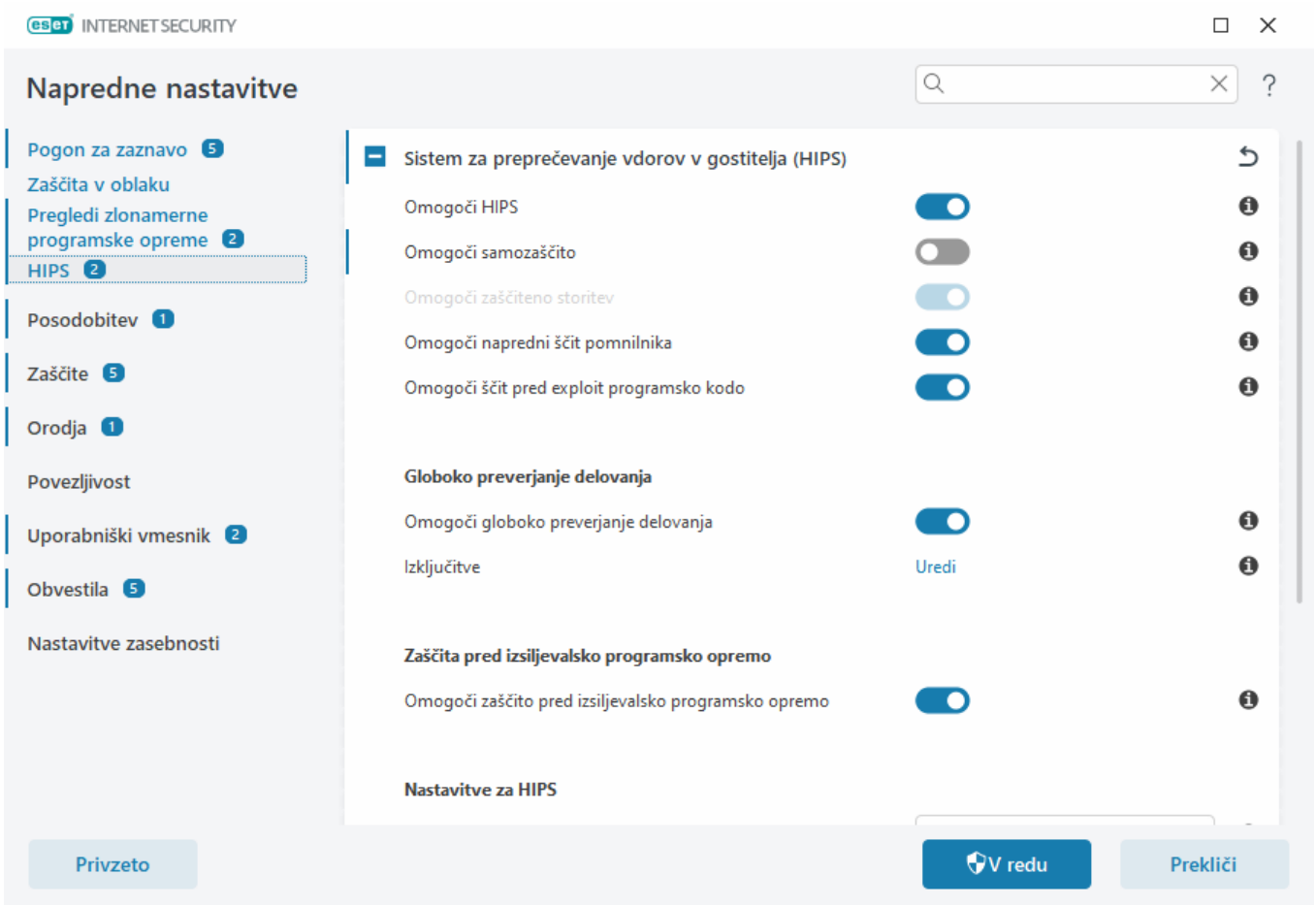
HIPS – Sistem za preprečevanje vdorov v gostitelja

Spremembe nastavitve sistema HIPS naj opravi le izkušen uporabnik. Nepravilna konfiguracija nastavitev HIPS lahko povzroči nestabilnost sistema.

Sistem preprečevanja vdora gostitelja (HIPS) ščiti vaš računalnik pred zlonamerno programsko opremo in neželenimi dejavnostmi, ki poskušajo negativno vplivati na vaš računalnik. HIPS uporablja napredno analizo vedenja skupaj z zmožnostmi zaznavanja omrežnega filtra za nadzor izvajajočih se procesov, datotek in registrskih ključev. Sistem HIPS je ločen od sprotne zaščite datotečnega sistema in ni požarni zid; nadzoruje le procese, ki se izvajajo v operacijskem sistemu.

Nastavitve za HIPS lahko konfigurirate v razdelku Napredne nastavitve > **Pogon za zaznavo** > **HIPS** > **Sistem za**

preprečevanje vdorov v gostitelja (HIPS). Stanje sistema HIPS (omogočeno/onemogočeno) je prikazano v glavnem oknu izdelka ESET Internet Security > **Nastavitve** > **Zaščita računalnika**.



Sistem za preprečevanje vdorov v gostitelja (HIPS)

Omogoči sistem HIPS – sistem HIPS je v izdelku ESET Internet Security p omogočen. Če sistem HIPS izklopite, s tem onemogočite funkcije sistema HIPS, kot je preprečevalnik izrabljanja.

Omogoči samozaščito – ESET Internet Security uporablja vgrajeno tehnologijo **samozaščite**, ki zlonamerni programski opremi prepreči, da bi poškodovala ali onemogočila zaščito pred virusi in vohunsko programsko opremo. Samozaščita varuje ključne sistemske procese in procese izdelkov ESET, registrske ključe in datoteke pred vdori.

Omogoči zaščiteno storitev – omogoči zaščito za storitev ESET (ekrn.exe). Ko je ta možnost omogočena, se storitev zažene kot zaščiten postopek sistema Windows, kar varuje pred napadi z zlonamerno programsko opremo.

Omogoči napredni pregledovalnik pomnilnika – skupaj s preprečevalnikom izrabljanja izboljša zaščito pred zlonamerno programsko opremo, ki je bila zasnovana tako, da je izdelki za preprečevanje zlonamerne programske opreme ne uspejo zaznati, in sicer z zameglitvijo ali šifriranjem. Napredni pregledovalnik pomnilnika je privzeto omogočen. Več o tej vrsti zaščite preberite v slovarju izrazov.

Omogoči preprečevalnik izkoriščanja – dodatno zaščiti vrste programov, ki so pogosto tarča napadov, npr. spletni brskalniki, bralniki PDF, e-poštni odjemalci in komponente sistema MS Office. Preprečevalnik izrabljanja je privzeto omogočen. Več o tej vrsti zaščite preberite v slovarčku.

Globoko preverjanje delovanja

Globoko preverjanje delovanja – druga plast zaščite znotraj funkcije HIPS. Ta plast funkcije HIPS analizira delovanje vseh programov, ki se izvajajo v računalniku, in vas opozori na zlonamerno delovanje procesov.

Izključitve iz globokega preverjanja delovanja sistema HIPS omogočajo izključitev postopkov iz analize. Če želite zagotoviti, da program pregleda vse procese in preveri, ali so v njih grožnje, vam priporočamo, da izključitve ustvarite samo v res nujnih primerih.

Zaščita pred programsko opremo z zahtevo po odkupnini

Omogoči zaščito pred izsiljevalsko programsko opremo – dodatna zaščita, ki deluje kot del funkcije HIPS. Če želite zagotoviti delovanje zaščite pred programsko opremo z zahtevo po odkupnini, morate imeti omogočen sistem za preverjanje ugleda ESET LiveGrid®. Več o tej vrsti zaščite preberite tukaj.

Omogoči Intel® Threat Detection Technology – pomaga odkrivati izsiljevalsko programsko opremo z uporabo edinstvene telemetrije CPE Intel za večjo učinkovitost zaznavanja, manj napačno pozitivnih opozoril in razširjeno vidljivost za odkrivanje naprednih tehnik izmikanja. Oglejte si podprte procesorje.

Nastavitve za HIPS

Način filtriranja lahko izvedete na enega od naslednjih načinov:

Način filtriranja	Opis
Samodejni način	Operacije so omogočene, razen tistih, ki jih blokirajo vnaprej določena pravila za zaščito vašega sistema.
Pametni način	Uporabnik bo obveščen samo o zelo sumljivih dogodkih.
Interaktivni način	Uporabnik bo moral potrditi operacije.
Način glede na pravilnik	blokira vse postopke, ki niso določeni s posebnim pravilom, ki jih dovoli.
Način za učenje	Po vsakem postopku so omogočeni postopki in ustvarjeno je pravilo. Pravila, ustvarjena v tem načinu, si lahko ogledate v urejevalniku **pravil HIPS**, vendar je njihova pomembnost manjša od pomembnosti pravil, ustvarjenih ročno, ali pravil, ustvarjenih v samodejnem načinu. Ko v spustnem meniju za **način filtriranja** izberete **način učenja**, bo na voljo tudi nastavitev **Način za učenje se zaključi ob**. Izberite časovno obdobje, v katerem naj bo omogočen način učenja; najdaljše trajanje je 14 dni. Ko določeno trajanje načina mine, boste pozvani, da uredite pravila, ki jih je v načinu učenja ustvaril HIPS. Izberete lahko tudi drugačen način filtriranja ali odločitev odložite in še naprej uporabljate način učenja.

Način, nastavljen po poteku načina za učenje – izberite način filtriranja po preteku načina za učenje. Po poteku možnost **Vprašaj uporabnika** za izvajanje sprememb načina filtriranja HIPS zahteva skrbniške pravice.

Sistem HIPS nadzira dogodke v operacijskem sistemu in se ustrezno odzove glede na pravila, ki so podobna tistim, ki jih uporablja požarni zid. Kliknite **Uredi** pri možnosti **Pravila**, če želite odpreti urejevalnik za **Pravila HIPS**. V oknu pravil HIPS lahko izberete, dodate, urejate ali odstranite pravila. Več informacij o ustvarjanju pravil in postopkih sistema HIPS najdete v razdelku Urejanje pravila HIPS.

Izključitve sistema HIPS

Z izključitvami lahko postopke izključite iz globokega preverjanja delovanja sistema HIPS.

Če želite urediti izključitve sistema HIPS, odprite razdelek Napredne nastavitve > **Pogon za zaznavo** > **HIPS** > **Sistem za preprečevanje vdorov v gostitelja (HIPS)** > **Izključitve** > **Uredi**.

Ta funkcija ni enaka funkciji Izključene datotečne pripone, Izključitve zaznav, Izključitve delovanja ali Izključitve postopkov.

Če želite predmet izključiti, kliknite**Dodaj** in vnesite pot do predmeta ali ga izberite v drevesni strukturi. Izbrane vnose lahko tudi urejate ali izbrišete.

Napredne nastavitve HIPS

Spodnje možnosti so koristne pri iskanju napak in analiziranju vedenja programa:

Gonilniki, ki se lahko vedno naložijo – Izbrani gonilniki se lahko vedno naložijo, ne glede na konfiguriran način filtriranja, razen če jih izrecno blokira pravilo uporabnika.

Zabeleži vse blokirane operacije – vse blokirane operacije bodo zapisane v dnevnik HIPS. To funkcijo uporabite samo takrat, ko odpravljate težave ali ko to zahteva tehnična podpora družbe ESET, saj lahko ustvari ogromno dnevniško datoteko in upočasni delovanje vašega računalnika.

Obvesti, ko pride do sprememb pri zagonskih programih – prikaže obvestilo na namizju, vsakič ko je program dodan ali odstranjen iz zagona sistema.

Gonilniki, ki se lahko vedno naložijo

Gonilniki, prikazani na tem seznamu, se lahko vedno naložijo, ne glede na način filtriranja HIPS, razen če jih izrecno blokira pravilo uporabnika.

Dodaj – doda nov gonilnik.

Uredi – uredi izbran gonilnik.

Odstrani – odstrani gonilnik s seznama.

Ponastavi – znova naloži niz sistemskih gonilnikov.

kliknite **Ponastavi**, če želite, da so vključeni tudi gonilniki, ki ste jih dodali ročno. Ta možnost je uporabna, če ste dodali več gonilnikov in jih ni mogoče ročno izbrisati s seznama.

Po namestitvi je seznam gonilnikov prazen. ESET Internet Security s časom samodejno dopolnjuje seznam.

Interaktivno okno HIPS

V pogovornem oknu HIPS lahko ustvarite pravilo glede na nova dejanja, ki jih zazna HIPS, in nato določite pogoje za dovoljenje ali zavrnitev teh dejanj.

Pravila, ustvarjena v pogovornem oknu obvestila, so enakovredna pravilom, ki so ustvarjena ročno. Zato je pravilo, ustvarjeno v pogovornem oknu, lahko manj specifično od pravila, ki je sprožilo pogovorno okno. To pomeni, da po tem, ko ustvarite takšno pravilo, lahko ista operacija sproži isto okno. Za več informacij glejte Prednost za pravila HIPS.

Če je privzeto dejanje za pravilo nastavljeno na možnost **Vedno vprašaj**, se prikaže pogovorno okno vsakič, ko se sproži to pravilo. Uporabite lahko možnost **Zavrni** ali **Dovoli** postopek. Če uporabnik v določenem času ne izbere dejanja, je izbrano novo dejanje glede na pravila.

Možnost **Zapomni si, dokler se program ne zapre** povzroči uporabo dejanja (**Dovoli/Zavrni**) do spremembe pravil ali načinov filtriranja, posodobitve modula HIPS ali vnovičnega zagona sistema. Začasna pravila so izbrisana, ko je katero koli od teh treh dejanj izvedeno.

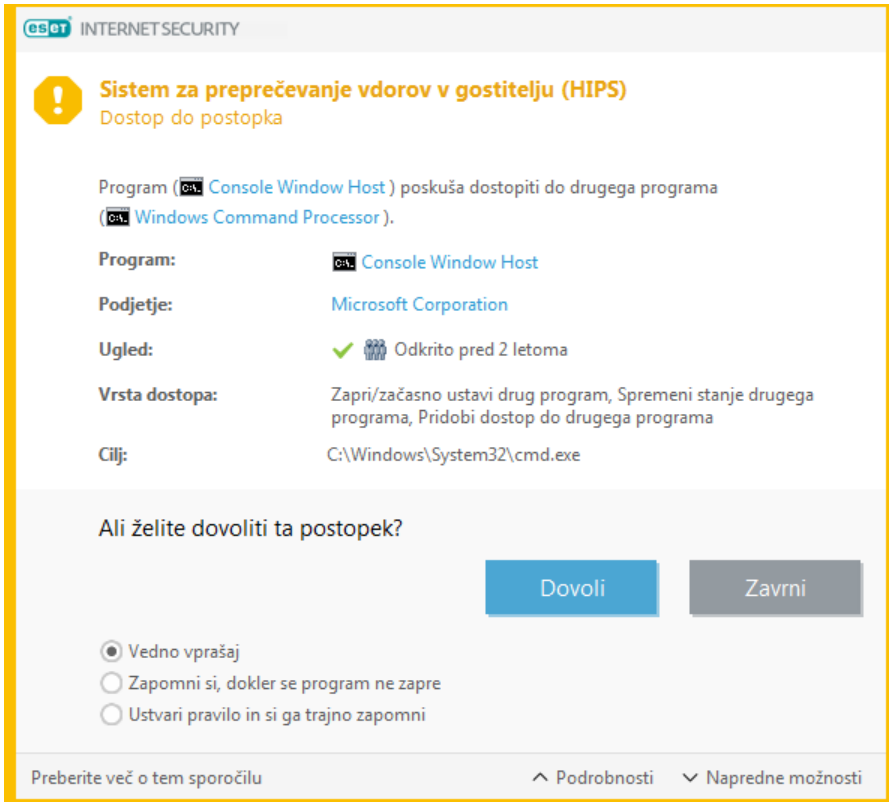
Možnost **Ustvari pravilo in si ga trajno zapomni** ustvari novo pravilo HIPS, ki ga je naknadno mogoče spremeniti v razdelku Upravljanje pravil HIPS (pri čemer potrebujete skrbniške pravice).

Na dnu kliknite možnost**Podrobnosti** in si oglejte, kateri program sproži dejanje, kakšen je ugled datoteke ali kakšno vrsto dejanja morate dovoliti ali zavrniti.

Nastavitve za natančnejše parametre pravil so na voljo tako, da kliknete **Napredne možnosti**. Če izberete možnost **Ustvari pravilo in si ga trajno zapomni**, so na voljo spodnje možnosti:

- **Ustvari pravilo, ki velja le za ta program** – če počistite to potrditveno polje, se pravilo ustvari za vse izvirne programe.
- **Samo za postopek** – izberite enega ali več postopkov datoteke/programa/registra za pravilo. Glejte opis vseh postopkov HIPS.
- **Samo za cilj** – izberite enega ali več ciljev datoteke/programa/registra za pravilo.

> **Prevej obvestil sistema HIPS?**
> Prikaz obvestil ustavite tako, da način filtriranja spremenite na **Samodejno** v razdelku Napredne nastavitve > **Pogon za zaznavo** > **HIPS** > **Sistem za preprečevanje vdorov v gostitelja (HIPS)**.



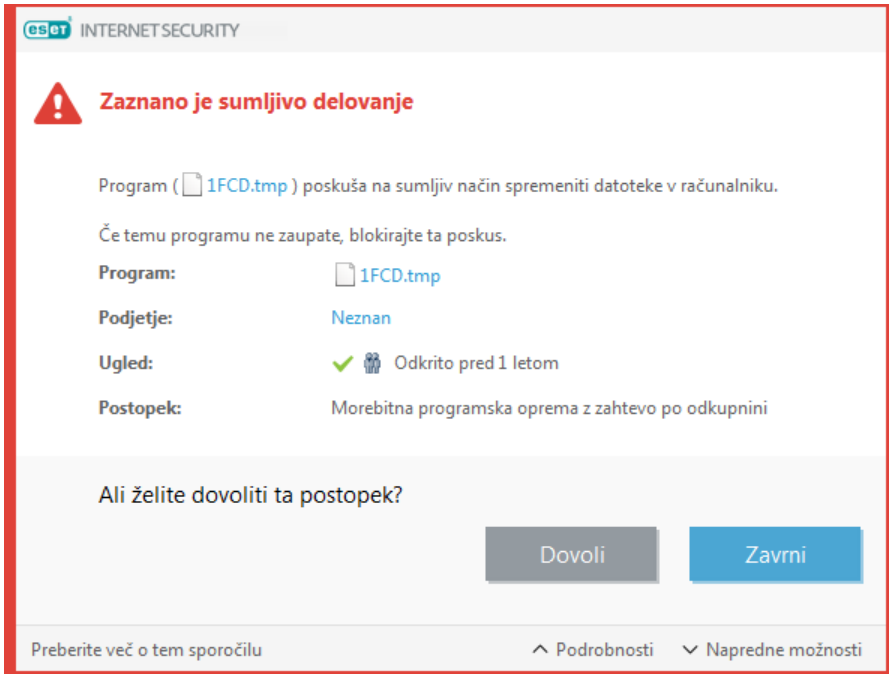
Način za učenje je končan

Način za učenje samodejno ustvari in shrani pravila. Vsa ustvarjena pravila lahko preverite v nastavitvah pravil HIPS. Ta način je najbolje uporabiti za začetno konfiguracijo sistema HIPS, vendar naj bo vklopljen le kratek čas. Posredovanje uporabnika ni potrebno, saj program ESET Internet Security shrani pravila v skladu z vnaprej določenimi parametri. Preklopite v **interaktivni** način ali **način na podlagi pravilnika**, ko so ustvarjena vsa pravila za zahtevane procese, ki se izvajajo v operacijskem sistemu, da se izognete varnostnim tveganjem.

To odločitev lahko odložite, če ne želite spremeniti nastavitev.

Zaznana morebitna programska oprema z zahtevo po odkupnini

To interaktivno okno se bo pojavilo, ko je zaznano obnašanje, značilno za programsko opremo z zahtevo po odkupnini. Uporabite lahko možnost **Zavrni** ali **Dovoli** postopek.



Če si želite ogledati določene parametre zaznavanja, kliknite **Podrobnosti**. V pogovornem oknu lahko izberete možnost **Pošlji v analizo** ali **Izključi iz zaznave**.

Za pravilno delovanje zaščite pred izsiljevalsko programsko opremo mora biti omogočena tehnologija ESET LiveGrid®.

Upravljanje pravil HIPS

Seznam uporabniško določenih in samodejno dodanih pravil iz sistema HIPS. Podrobnejše informacije o ustvarjanju pravil in delovanju sistema HIPS najdete v poglavju Nastavitve pravil HIPS. Glejte tudi Splošno načelo sistema HIPS.

Stolpci

Pravilo – ime pravila, ki ga določi uporabnik, ali samodejno izbrano ime.

Omogočeno – onemogočite gumb za preklop, če želite pravilo ohraniti na seznamu, vendar ga ne želite uporabiti.

Dejanje – pravilo določa dejanje **Dovoli**, **Blokiraj** ali **Vprašaj**, ki se izvede, če so izpolnjeni pogoji.

Viri – pravilo bo uporabljeno le, če dogodek sproži program ali programi.

Cilji – pravilo bo uporabljeno le, če je postopek povezan z določeno datoteko, programom ali vnosom registra.

Resnost zapisovanja v dnevnik – če potrdite to možnost, bodo informacije o tem pravilu zapisane v Dnevnik HIPS.

Obvesti – če je dogodek sprožen, se v spodnjem desnem kotu prikaže majhno okno z obvestilom.

Elementi kontrolnika

Dodaj – ustvari novo pravilo.

Uredi – omogoča urejanje izbranih vnosov.

Izbriši – odstrani izbrane vnose.

Prednost za pravila HIPS

Za nastavitev prednostne ravni za pravila HIPS možnosti razvrščanja z gumbi od vrha proti dnu niso na voljo (kot pri možnosti Pravila za požarni zid, kjer se pravila izvajajo od vrha proti dnu).

- Vsa ustvarjena pravila imajo enako prednost.
- Bolj kot je pravilo natančno, višja je prednost (npr. pravilo, ustvarjeno za določen program, ima višjo prednost od pravila, ki velja za vse programe).
- Sistem HIPS interno vsebuje pravila z višjo prednostjo, do katerih nimate dostopa (tako npr. ne morete preglasiti pravil, določenih za samozaščito)
- Če ustvarite pravilo, ki bi lahko povzročilo zamrznitev operacijskega sistema, se ne bo uporabilo (bo imelo najnižjo stopnjo prednosti).

Urejanje pravila HIPS

Najprej si oglejte Upravljanje pravil HIPS.

Ime pravila – ime pravila, ki ga določi uporabnik, ali samodejno izbrano ime.

Dejanje – določa dejanje **Dovoli**, **Blokiraj** ali **Vprašaj**, ki se izvede, če so izpolnjeni pogoji.

Postopki, za katere velja – izbrati morate vrsto postopka, za katero bo pravilo veljalo. Pravilo bo uporabljeno le za to vrsto postopkov in za izbrani cilj.

Omogočeno – onemogočite gumb za preklop, če želite pravilo ohraniti na seznamu, vendar ga ne želite uporabiti.

Resnost zapisovanja v dnevnik – če potrdite to možnost, bodo informacije o tem pravilu zapisane v Dnevnik HIPS.

Obvesti uporabnika – če je dogodek sprožen, se v spodnjem desnem kotu prikaže majhno okno z obvestilom.

Pravilo je sestavljeno iz delov, ki opisujejo pogoje za sprožanje tega pravila:

Izvirni programi – pravilo bo uporabljeno le, če dogodek sprožijo ti programi. V spustnem meniju izberite možnost **Določeni programi** in kliknite **Dodaj**, da dodate nove datoteke, ali pa v spustnem meniju izberite možnost **Vsi programi** in dodajte vse programe.

Ciljne datoteke – pravilo bo uporabljeno le, če je postopek povezan s tem ciljem. V spustnem meniju izberite možnost **Določene datoteke** in kliknite **Dodaj**, da dodate nove datoteke ali mape, ali pa v spustnem meniju izberite možnost **Vse datoteke** in dodajte vse datoteke.

Programi – pravilo bo uporabljeno le, če je postopek povezan s tem ciljem. V spustnem meniju izberite možnost **Določeni programi** in kliknite **Dodaj**, da dodate nove datoteke ali mape, ali pa v spustnem meniju izberite možnost **Vsi programi** in dodajte vse programe.

Vnosi v register – pravilo bo uporabljeno le, če je postopek povezan s tem ciljem. Izberite **Določeni vnosi** s spustnega menija in kliknite **Dodaj** za ročen vnos ali pa kliknite **Odpri urejevalnik registra** za izbiro ključa registra. Prav tako lahko izberete **Vsi vnosi** s spustnega menija, da dodate vse programe.

> Nekaterih postopkov za določena pravila, ki so vnaprej določena s sistemom HIPS, ni mogoče blokirati in so privzeto dovoljeni. Poleg tega sistem HIPS ne nadzira vseh sistemskih postopkov. HIPS nadzira postopke, ki so morda nevarni.

Opisi pomembnih postopkov:

Postopki datoteke

- **Izbriši datoteko** – program zahteva dovoljenje za brisanje ciljne datoteke.
- **Zapiši v datoteko** – program zahteva dovoljenje za pisanje v ciljno datoteko.
- **Neposredni dostop do diska** – program poskuša brati z diska ali pisati nanj na nestandarden način, s čimer se izogne pogostim postopkom v sistemu Windows. To lahko pomeni, da se datoteke spreminjajo brez uporabe ustreznih pravil. Ta postopek lahko sproži zlonamerna programska oprema, ki se poskuša izogniti zaznavanju, programska oprema za varnostno kopiranje, ki poskuša narediti natančno kopijo diska ali upravitelj particij, ki poskuša reorganizirati diske.
- **Namesti globalno ročico** – nanaša se na klicanje funkcije SetWindowsHookEx iz knjižnice MSDN.
- **Naloži gonilnik** – namestitev in nalaganje gonilnikov v sistem.

Postopki programa

- **Iskanje in odpravljanje napak v drugem programu** – prilaganje iskalnika napak v proces. Med iskanjem napak v programu je mogoče prikazati in spremeniti številne podrobnosti o njegovem delovanju in imeti dostop do podatkov v njem.
- **Prestrezi dogodke iz drugega programa** – izvirni program poskuša ujeti ciljne dogodke v določenem programu (zapisovalnik tipkanja na primer poskuša zajeti dogodke brskalnika).
- **Zapri/začasno prekini drug program** – začasna prekinitev, nadaljevanje ali prekinitev postopka (dostop je mogoč neposredno iz podokna »Raziskovalec postopkov« ali »Postopki«).
- **Zaženi nov program** – zagon novih programov ali procesov.
- **Spremeni stanje drugega programa** – izvirni program poskuša pisati v pomnilnik ciljnega programa ali zagnati kodo namesto njega. Ta funkcija je lahko uporabna pri zaščiti osnovnega programa s konfiguracijo tega kot ciljnega programa v pravilu, ki blokira uporabo te operacije.

Postopki registra

- **Spremeni nastavitve zagona** – vse spremembe nastavitev, ki določajo, kateri programi bodo zagnani ob zagonu sistema Windows. Najdete jih tako, da v registru sistema Windows poiščete ključ Run.
- **Izbriši iz registra** – brisanje ključa registra ali pripadajoče vrednosti.

- **Preimenuj ključ registra** – preimenovanje ključa registra.

- **Spremeni register** – ustvarjanje novih vrednosti registrskih ključev, spreminjanje obstoječih vrednosti, premikanje podatkov v drevesni strukturi zbirke podatkov ali nastavitev pravic uporabnika ali skupine za registrske ključe.

Pri vnašanju cilja lahko uporabite nadomestne znake z določenimi omejitvami. Namesto določenega ključa lahko v poteh do registra uporabite * (zvezdico). *HKEY_USERS*\software* lahko na primer pomeni *HKEY_USER\.default\software*, vendar ne *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** ni veljavna pot registrskega ključa. Pot do registra je pot, ki vsebuje znake »*«, določa »to pot ali katero koli pot na kateri koli ravni po tem simbolu«. Le na ta način lahko uporabljate nadomestne znake za ciljne datoteke. Najprej bo ocenjen določen del poti, nato pa pot, ki sledi simbolu s posebnim znakom (*).

Če ustvarite zelo splošno pravilo, se bo prikazalo opozorilo, da je pravilo preveč splošno.

V spodnjem primeru vam bomo pokazali, kako omejiti neželeno delovanje posameznih programov:

1. Poimenujte pravilo in v spustnem meniju **Dejanje** izberite **Blokiraj** (ali **Vprašaj**, če želite uporabiti to možnost).

2. Omogočite gumb za preklop ob možnosti **Obvesti uporabnika**, da se ob vsaki uporabi pravila prikaže obvestilo.

3. Izberite vsaj en postopek v razdelku**Postopki, za katere velja**, za katerega bo veljalo pravilo.

4. Kliknite **Naprej**.

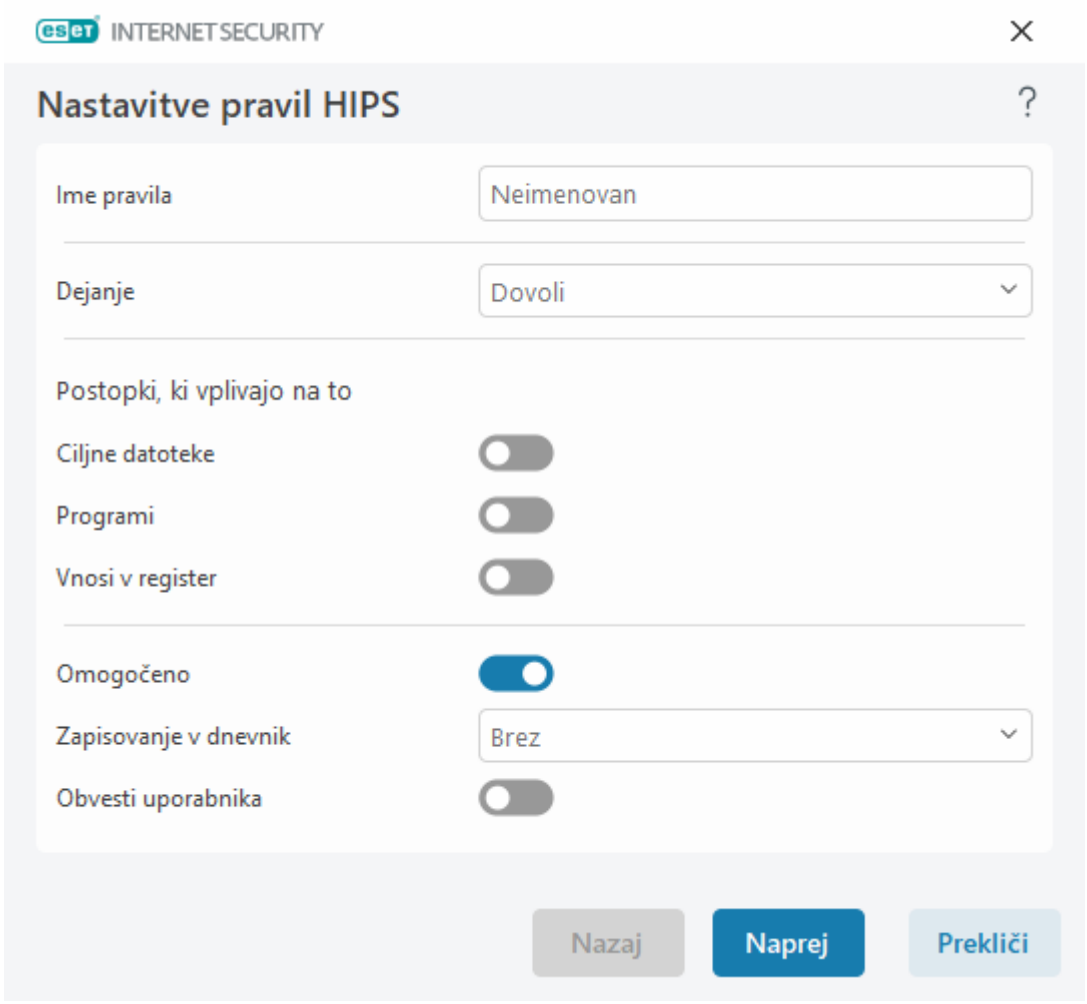
5. V oknu **Izvirni programi** v spustnem meniju izberite **Določeni programi**, da uporabite novo pravilo za vse programe, ki poskušajo izvesti katerega koli od izbranih postopkov v programih, ki ste jih določili.

6. Kliknite **Dodaj** in nato **...** za izbiro poti do določenega programa, nato pritisnite **V redu**. Če želite, lahko dodate več programov.
Primer: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Izberite postopek **Zapiši v datoteko**.

8. V spustnem meniju izberite **Vse datoteke**. Na ta način se blokirajo vsi poskusi zapisovanja v vse datoteke za izbrane programe iz prejšnjega koraka.

9. Kliknite **Dokončaj**, da shranite novo pravilo.



Dodajanje poti do programa/registra za HIPS

Izberite pot do programa, tako da kliknete **...**. Ko izberete mapo, bodo vključeni vsi programi na tem mestu.

Možnost **Odpri urejevalnik registra** bo zagnala urejevalnik registra sistema Windows (regedit). Ko dodate pot do registra, vnesite trenutno lokacijo v polje **Vrednost**.

Primeri poti do datoteke ali registra:

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

Posodabljanje

Možnosti nastavitev posodobitve so na voljo v razdelku Napredne nastavitve > **Posodobitev**. V tem razdelku so navedeni podatki o posodobitvi, kot so strežniki za posodabljanje in podatki za preverjanje pristnosti teh strežnikov.

Posodabljanje

Trenutno uporabljeni profil posodobitve je prikazan v spustnem meniju **Izberi privzeti profil posodobitve**.

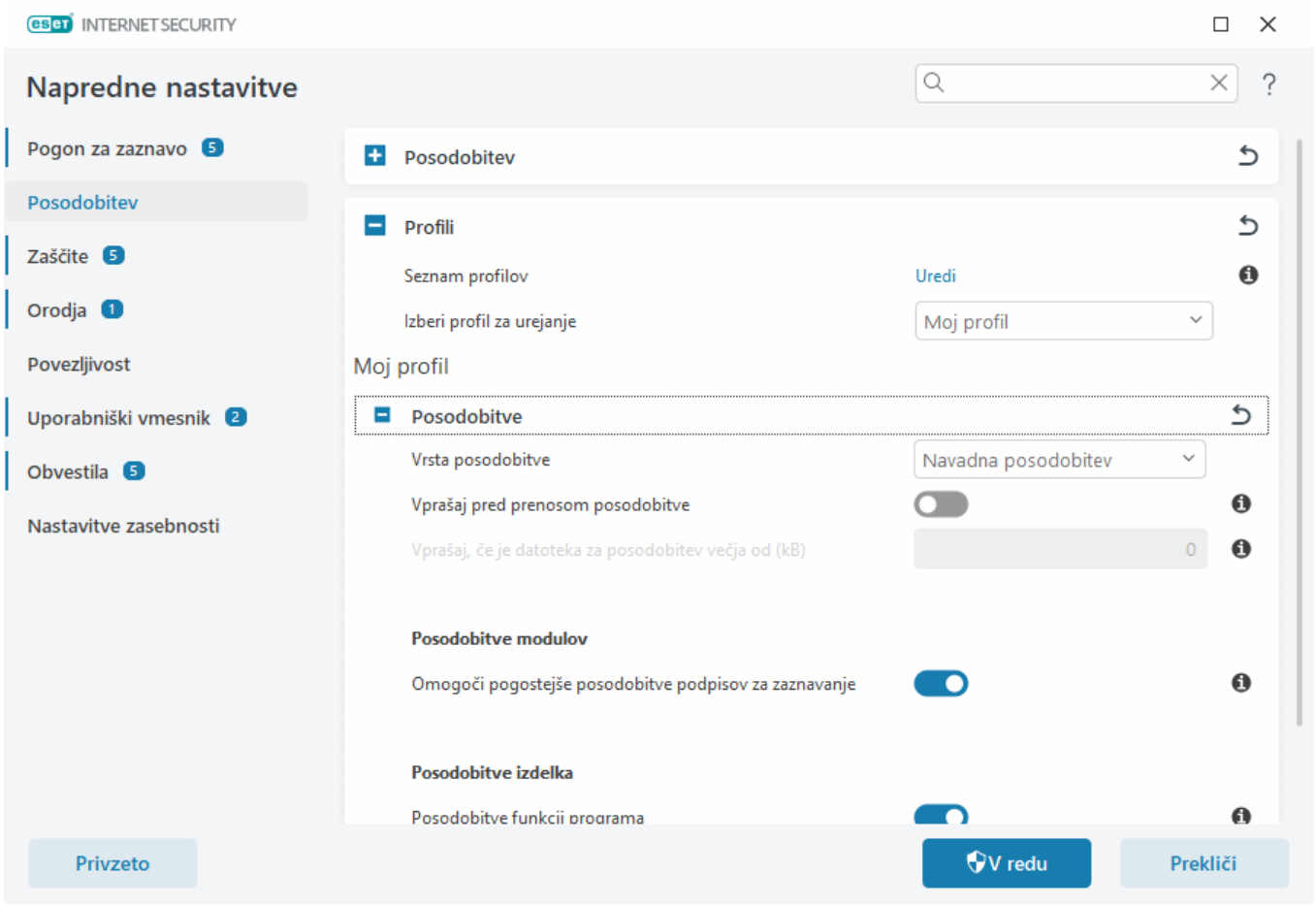
Če želite ustvariti nov profil, glejte razdelek Profili posodobitve.

Samodejno preklapljanje med profili – omogoča dodeljevanje profila določenemu profilu omrežnih povezav.

Če prihaja do težav pri poskusu prenosa pogona za zaznavo ali posodobitev modulov, kliknite **Počisti** ob možnosti **Počisti predpomnilnik za posodobitve**, da počistite začasne datoteke/predpomnilnik za posodobitev.

Module Povrnitev prejšnjega stanja

Če menite, da je novo orodje za zaznavanje ali modul programa morda nestabilen ali poškodovan, ga lahko povrnete na prejšnjo različico in za določen čas onemogočite posodobitve.



Za pravilen prenos posodobitev je bistvenega pomena, da pravilno izpolnite vse parametre. Če uporabljate požarni zid, se prepričajte, ali je omogočena komunikacija med programom ESET in internetom (npr. komunikacija HTTP).

Profili

Za različne konfiguracije posodobitev in opravila lahko ustvarite profile posodobitve. Različni profili posodobitve so še posebej uporabni za uporabnike mobilnih naprav, ki potrebujejo nadomestni profil za lastnosti internetne povezave, ki se redno spreminjajo.

V spustnem meniju **Izberi profil za urejanje** je prikazan trenutno izbrani profil, ki je privzeto nastavljen na vrednost **Moj profil**. Če želite urediti ustvarjeni profil, izberite ustvarjeni profil in kliknite **Uredi** poleg možnosti **Seznam profilov**, vnesite svoje **Ime profila** in kliknite **Dodaj**.

Posodobitve

Možnost v meniju **Vrsta posodobitve** je privzeto nastavljena na **Navadna posodobitev**, kar omogoča samodejni prenos posodobitvenih datotek iz strežnika ESET z najmanjšim omrežnim prometom. Predizdajna različica posodobitev (možnost **Predizdajna različica posodobitev**) so posodobitve, ki so bile vključene v notranje preskušanje in bodo kmalu na voljo za vse uporabnike. Če omogočite predizdajno različico posodobitev, si zagotovite dostop do najnovejših načinov zaznavanja in popravkov. Vendar pa predizdajna različica posodobitev morda ni vedno dovolj stabilna, zato JE NE UPORABITE v produkcijskih strežnikih in delovnih postajah, v katerih sta potrebna največja mogoča razpoložljivost in stabilnost.

Vprašaj pred prenosom posodobitve – program bo prikazal obvestilo, kjer lahko potrdite ali zavrnete prenose datotek za posodobitve.

Vprašaj, če je datoteka za posodobitev večja od (kB) – program bo prikazal pogovorno okno za potrditev, če je velikost datoteke za posodobitev večja od navedene vrednosti. Če je velikost datoteke za posodobitev nastavljena na 0 KB, bo program vedno prikazal potrditveno pogovorno okno.

Posodobitve modula

Omogoči pogostejše posodobitve definicij za zaznavanje – definicije za zaznavanje se bodo posodabljale v krajših intervalih. Če to možnost onemogočite, se lahko stopnja zaznavanja zmanjša.

Posodobitve izdelka

Posodobitve funkcij programa – samodejna namestitev nove različice programa ESET Internet Security.

Možnosti povezave

Za uporabo strežnika proxy za prenos posodobitev glejte razdelek Možnosti povezave.

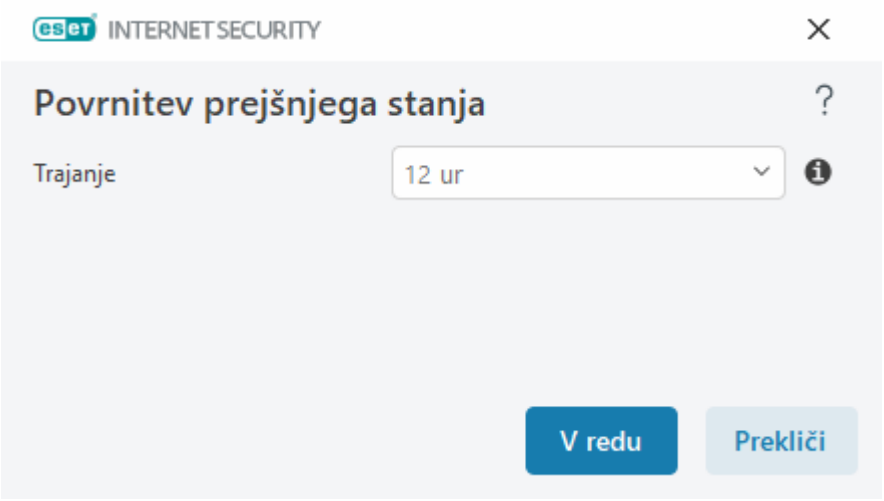
Povrnitev prejšnjega stanja posodobitve

Če menite, da je nov pogon za zaznavo ali posodobitev modula programa morda nestabilna ali poškodovana, jo lahko povrnete na prejšnjo različico in začasno onemogočite posodobitve. Predhodno onemogočene posodobitve lahko tudi omogočite, če ste jih odložili za nedoločen čas.

ESET Internet Security beleži posnetke pogona za zaznavo in modulov programa za uporabo s funkcijo povrnitev prejšnjega stanja. Če želite ustvariti zbirko virusnih definicij, omogočite **ustvarjanje posnetkov modulov**. Ko je **ustvarjanje posnetkov modulov** omogočeno, se prvi posnetek ustvari med prvo posodobitvijo. Naslednji se ustvari po 48 urah. Polje **Število lokalno shranjenih posnetkov** določa število shranjenih posnetkov pogona za zaznavo.

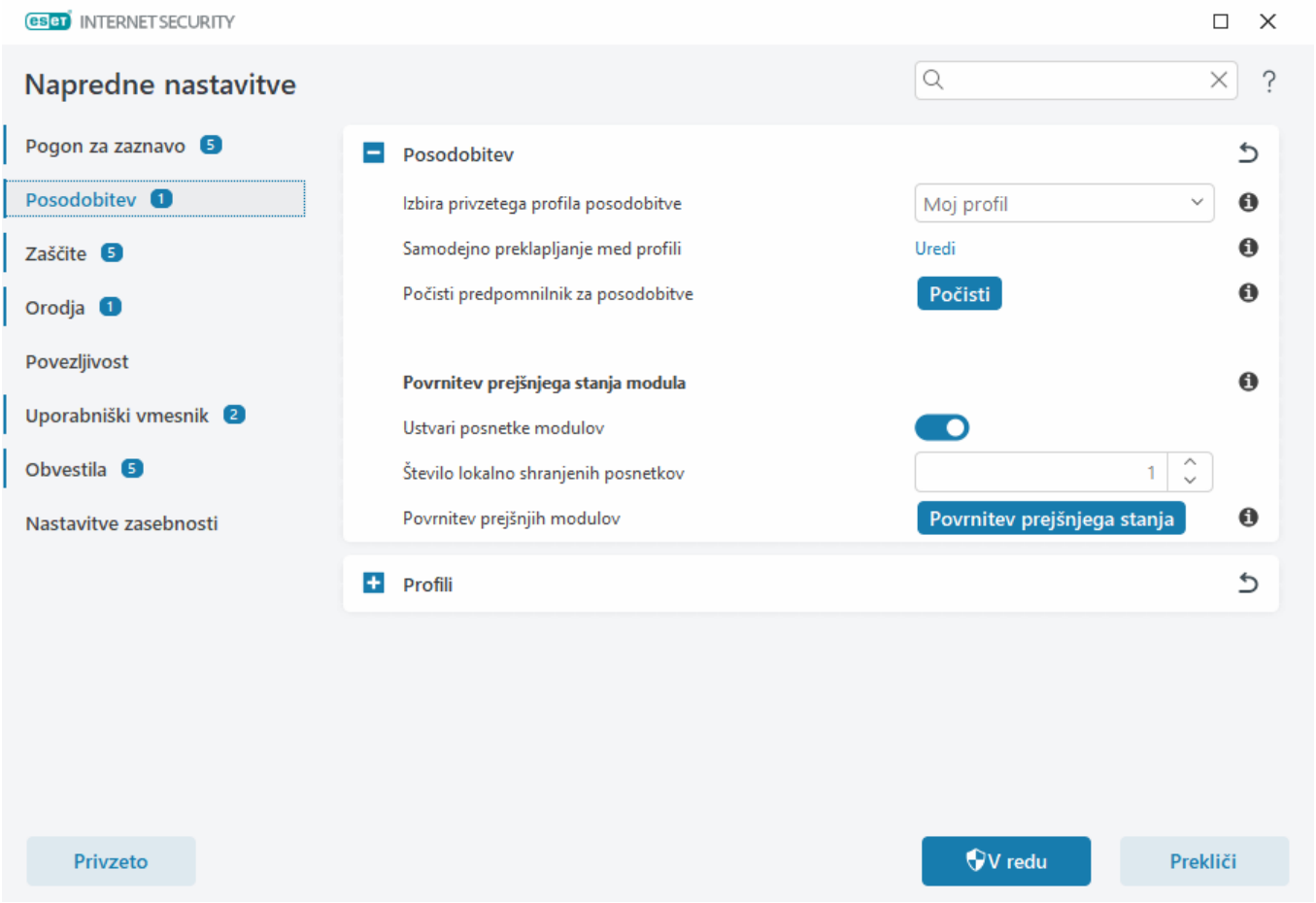
> Ko dosežete največjo količino posnetkov (na primer tri), se najstarejši posnetek nadomesti z novim posnetkom vsakih 48 ur. ESET Internet Security povrne različico pogona za zaznavo in posodobitev modula programa na najstarejšem posnetku.

Če kliknete **Povrnitev prejšnjega stanja** (v razdelku Napredne nastavitve > **Posodobitev** > **Posodobitev**), morate v spustnem meniju **Trajanje** izbrati časovno obdobje, ki predstavlja obdobje, med katerim bodo posodobitve pogona za zaznavo in modula programa začasno ustavljene.



Izberite **Do preklica**, če želite odložiti redne posodobitve za nedoločen čas, dokler ročno ne obnovite funkcije posodobitve. Ker ta možnost predstavlja morebitno varnostno tveganje, ESET priporoča, da je ne izberete.

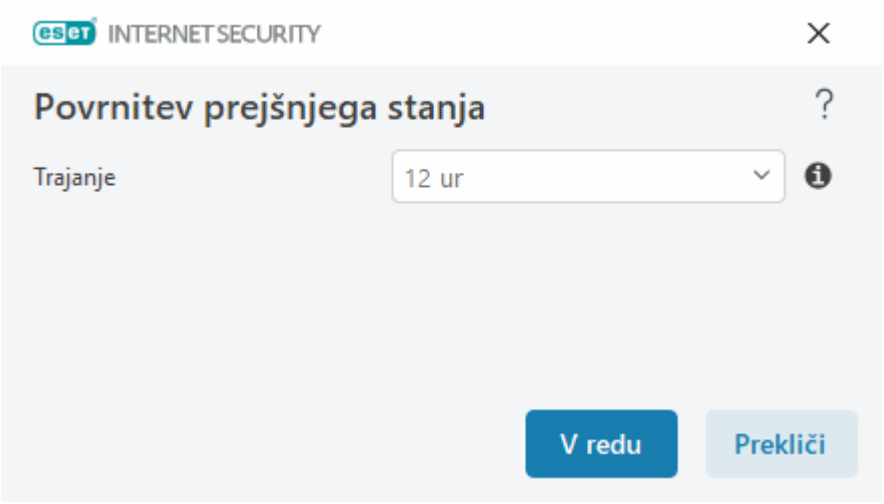
Če je možnost povrnitve prejšnjega stanja izvedena, se gumb **Povrni v prejšnje stanje** spremeni v **Dovoli posodobitve**. Za časovni interval, izbran v spustnem meniju **Začasno prekini posodobitve**, posodobitve niso dovoljene. Različica pogona za zaznavo bo zamenjana z najstarejšo različico, ki je na voljo, in shranjena kot posnetek v datotečnem sistemu lokalnega računalnika.



Število 22700 naj bo najnovejša različica orodja za zaznavanje. Števili 22698 in 22696 sta shranjeni kot posnetka pogona za zaznavo. Število 22697 ni na voljo. Ker ste na primer računalnik izklopili še preden je bila prenesena številka 22697 in je že na voljo novejša različica posodobitve. Če je polje **Število lokalno shranjenih posnetkov** nastavljeno na 2 in kliknete možnost **Povrni v prejšnje stanje**, se pogon za zaznavo (vključno z moduli programa) povrne v različico 22696. Ta postopek lahko traja nekaj časa. Na zaslonu Posodabljanje preverite, ali je bila različica orodja za zaznavanje zamenjana s starejšo različico.

Časovni interval prejšnjega stanja posodobitve

Če kliknete **Povrnitev prejšnjega stanja** (v razdelku Napredne nastavitve > **Posodobitev** > **Posodobitev**), morate v spustnem meniju **Trajanje** izbrati časovno obdobje, ki predstavlja obdobje, med katerim bodo posodobitve pogona za zaznavo in modula programa začasno ustavljene.



Izberite **Do preklica**, če želite odložiti redne posodobitve za nedoločen čas, dokler ročno ne obnovite funkcije posodobitve. Ker ta možnost predstavlja morebitno varnostno tveganje, ESET priporoča, da je ne izberete.

Posodobitve izdelka

V razdelku **Posodobitve izdelka** lahko samodejno namestite nove posodobitve funkcij, ko so na voljo.

Posodobitve funkcij programa uvajajo nove funkcije oziroma spreminjajo tiste, ki že obstajajo v prejšnjih različicah programov. To posodabljanje se lahko izvede samodejno brez posredovanja uporabnika ali pa izberete možnost, da ste o tem obveščeni. Ko je nameščena posodobitev funkcij programa, bo morda potreben ponovni zagon računalnika.

Posodobitve funkcij programa – ko je ta možnost omogočena, se posodobitve funkcij programa izvedejo samodejno.

Možnosti povezave

Če želite dostopati do možnosti za nastavitev strežnika proxy za določen profil posodobitve, odprite razdelek Napredne nastavitve > **Posodobitev** > **Profili** > **Posodobitve** > **Možnosti povezave**. Kliknite spustni meni **Način za strežnik proxy** in izberite eno od teh treh možnosti:

- Ne uporabi strežnika proxy
- Vzpostavi povezavo prek strežnika proxy
- Uporabi globalne nastavitve strežnika proxy

Če želite uporabiti konfiguracijo strežnika proxy, ki je že določena v razdelku Napredne nastavitve > **Povezljivost** > **Strežnik proxy**, izberite možnost **Uporabi globalne nastavitve strežnika proxy**.

Če želite določiti, da za posodobitev programa ESET Internet Security ne bo uporabljen strežnik proxy, izberite možnost **Ne uporabi strežnika proxy**.

Vzpostavi povezavo prek strežnika proxy izberite v teh primerih:

- Za posodobitev programa ESET Internet Security je izbran strežnik, ki ni opredeljen v možnosti Napredne nastavitve > **Povezljivost**. V tej konfiguraciji je treba podatke novega strežnika proxy določiti v možnostih za naslov **strežnika proxy**, komunikacijska **vrata** (privzeto 3128) ter po potrebi še **uporabniško ime** in **geslo** strežnika proxy.
- Nastavitve strežnika proxy niso nastavljene globalno, vendar bo program ESET Internet Security vzpostavil povezavo s strežnikom proxy in preveril, ali so na voljo posodobitve.
- Računalnik je z internetom povezan prek strežnika proxy. Med namestitvijo programa se uporabijo nastavitve brskalnika Internet Explorer, toda če so spremenjene (če na primer spremenite ISP), preverite, ali so nastavitve za proxy v tem oknu pravilne. Program v nasprotnem primeru ne bo mogel vzpostaviti povezave za posodobitev strežnikov.

Privzeta nastavitev strežnika proxy je **Uporabi globalne nastavitve strežnika proxy**.

Če posredniški strežnik ni na voljo, uporabi neposredno povezavo – če bo strežnik proxy nedosegljiv, bo med posodobitvijo preskočen.

Polji **Uporabniško ime** in **Geslo** v tem razdelku se nanašata na strežnik proxy. Polji izpolnite le, če sta za dostop do strežnika proxy obvezna uporabniško ime in geslo. Izpolnite ju le, če veste, da za dostop do spleta prek strežnika proxy potrebujete geslo.

Zaščite

Zaščita varuje pred zlonamernimi sistemskimi napadi tako, da nadzoruje komunikacijo med datotekami ter e-poštno in internetno komunikacijo. Če je na primer zaznan predmet, ki se uvršča med zlonamerno programsko opremo, se bo začel postopek popravljanja. Zaščita lahko predmet odstrani tako, da ga blokira in nato očisti, izbriše ali premakne v karanteno.

Če želite podrobno konfigurirati zaščito, odprite Napredne nastavitve > **Zaščite**.

Spremembe zaščit naj opravi le izkušen uporabnik. Nepravilna konfiguracija nastavitev lahko povzroči slabšo zaščito.

V tem razdelku:

- Odzivi na zaznane elemente

- Nastavitev poročanja
- Nastavitev zaščite

Odzivi na zaznane elemente

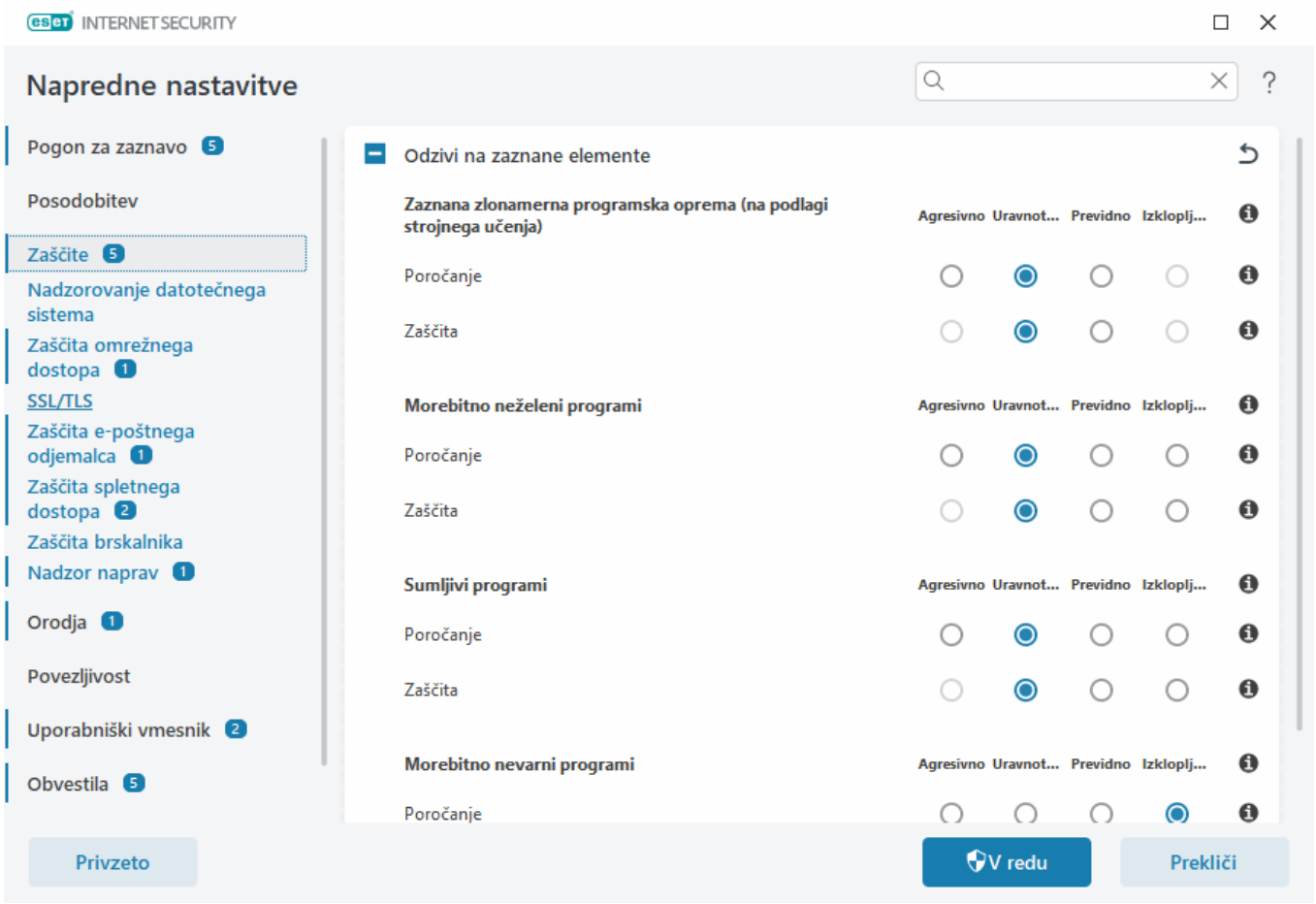
Odzivi na zaznane elemente omogočajo konfiguriranje ravni poročanja in zaščite za naslednje kategorije:

- **Zaznana zlonamerna programska oprema (na podlagi strojnega učenja)** – Računalniški virus predstavlja zlonamerno kodo, ki je vnaprej dodana v obstoječe datoteke v računalniku. Toda izraz »virus« se pogosto napačno uporablja. »Zlonamerna programska oprema« je ustreznejši izraz. Zaznavanje zlonamerne programske opreme izvaja modul pogona za zaznavo, ki vključuje komponento strojnega učenja. Več o teh vrstah programov preberite v slovarju izrazov.

- **Morebitno neželeni programi** – morebitna neželena programska oprema ali morebitno neželeni programi so široka kategorija programske opreme, ki ni jasno zlonamerna kot druge vrste zlonamerne programske opreme, na primer virusi ali trojanski konji. Vseeno lahko namesti dodatno neželeno programsko opremo, spremeni vedenje digitalne naprave ali izvaja dejavnosti, ki jih uporabnik ne dovoli ali pričakuje. Več o teh vrstah programov preberite v slovarju izrazov.

- **Sumljivi programi** – vključujejo programe, ki so stisnjeni z arhivi ali zaščitniki. Te vrste zaščitnikov pogosto izkoriščajo avtorji zlonamerne programske opreme, da se izognejo zaznavanju.

- **Morebitno nevarni programi** – nanašajo se na komercialno programsko opremo z dovoljeno uporabo, ki je lahko uporabljena zlonamerno. Morebitno nevarni programi vključujejo na primer orodja za oddaljeni dostop, programe za razbijanje gesel in zapisovalnike tipkanja (programi, ki beležijo posamezne uporabnikove pritiske tipk). Več o teh vrstah programov preberite v slovarju izrazov.



Izboljšana zaščita

Napredno strojno učenje je zdaj del zaščit kot napredna raven zaščite, ki izboljša zaznavanje na podlagi strojnega učenja. Več o tej vrsti zaščite preberite v slovarju izrazov.

Nastavitev poročanja

Ko je zaznan element (npr. je najdena grožnja, ki se uvršča med zlonamerno programsko opremo), se podatki zabeležijo v dnevnik zaznanih elementov, na namizju pa se prikažejo obvestila, če so konfigurirana v programu ESET Internet Security.

Meja poročanja je konfigurirana za vsako kategorijo (v nadaljevanju »KATEGORIJA«):

1. Zaznave zlonamerne programske opreme
2. Morebitno neželeni programi
3. Morebitno nevarno
4. Sumljivi programi

Poročanje izvaja pogon za zaznavo, ki vključuje komponento strojnega učenja. Nastavite lahko višjo mejo poročanja od trenutne meje zaščite. Nastavitve poročanja ne vplivajo na blokiranje, čiščenje ali brisanje predmetov.

Preden spremenite mejo (ali raven) poročanja za KATEGORIJE, preberite naslednje:

Meja	Pojasnilo
Agresivno	Poročanje o KATEGORIJAH je konfigurirano na najvišjo raven občutljivosti. Prijavljenih je več zaznanih elementov. **Agresivna** nastavitev lahko lažno prepozna predmete kot KATEGORIJO.
Uravnoteženo	Poročanje o KATEGORIJAH je konfigurirano kot uravnoteženo. Ta nastavitev je optimizirana za uravnoteženje učinkovitosti ter točnosti stopenj zaznavanja in števila lažno prepoznanih predmetov.
Previdno	Poročanje o KATEGORIJAH je konfigurirano tako, da kar najbolj zniža število lažno prepoznanih predmetov, hkrati pa ohranja zadostno raven zaščite. Predmeti so prijavljeni le, ko je verjetnost velika in se njihovo obnašanje ujema z obnašanjem KATEGORIJ.
Izklopljeno	Poročanje za KATEGORIJO ni aktivno in te vrste elementov ne bodo iskane, prijavljene ali očiščene. Zato nastavitev onemogoči zaščito pred to vrsto elementov. Poročanja o zlonamerni programski opremi ni mogoče izklopiti in je privzeta vrednost za morebitno nevarne programe.

Izbira modulov zaščite programa ESET Internet Security

Izbira (omogočeno ali onemogočeno) modula zaščite za izbrano mejo KATEGORIJE je naslednja:

	Agresivno	Uravnoteženo	Previdno	Izklopljeno*
Modul za napredno strojno učenje	✔ (agresivni način)	✔ (previdni način)	X	X
Modul pogona za zaznavo	✔	✔	✔	X
Drugi moduli zaščite	✔	✔	✔	X

* Ni priporočeno.

Ugotavljanje različice izdelka, različice modulov programa in datuma graditev

1. Kliknite **Pomoč in podpora** > **ESET Internet Security – vizitka**.
2. Številka različice izdelka ESET je prikazana v prvi vrstici besedila na zaslonu **Vizitka**.
3. Za informacije o posameznih modulih kliknite **Nameščene komponente**.

Ključni napotki

Ključni napotki za nastavitev ustrezne mejne ravni za svoje okolje:

- V večini primerov je priporočljivo izbrati **uravnoteženo** mejno raven.
- Višja ko je meja poročanja, višja je stopnja zaznavanja, s tem pa se poveča tudi verjetnost napačne pozitivne prepoznave predmetov.
- V praksi ni zagotovila za 100-% stopnjo zaznavanja niti za 0-% stopnjo napačnega prepoznavanja nenevarnih predmetov kot zlonamerne programske opreme.
- Redno posodabljajte program ESET Internet Security in njegove module, saj boste s tem dosegli kar najboljše razmerje med učinkovitostjo in točnostjo stopenj zaznavanja ter številom lažno prepoznanih predmetov.

Nastavitev zaščite

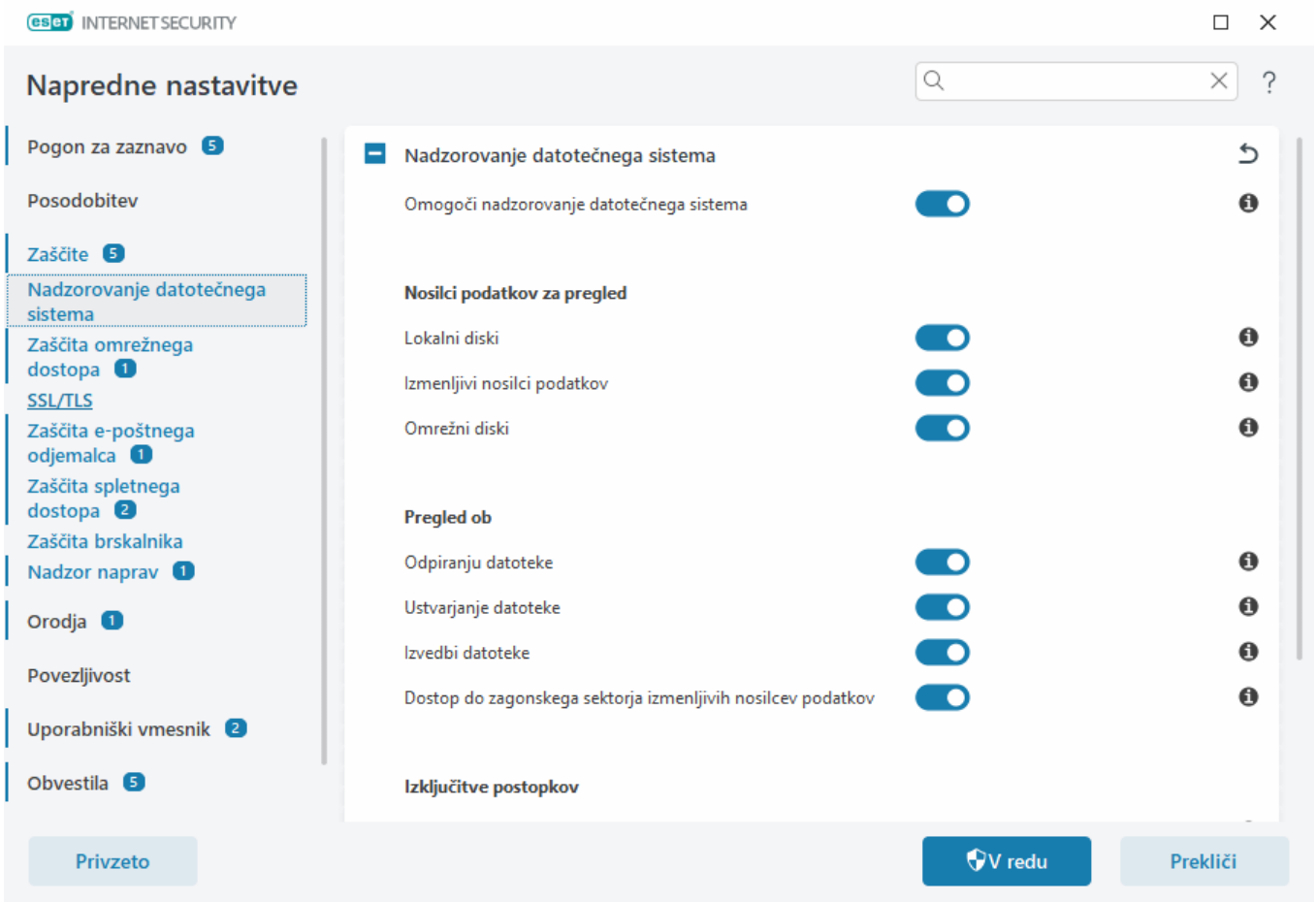
Če je prijavljen predmet, ki je prepoznan kot KATEGORIJA, ga program blokira in nato očisti, izbriše ali premakne v karanteno.

Preden spremenite mejo (ali raven) zaščite za KATEGORIJO, preberite naslednje:

Meja	Pojasnilo
Agresivno	Elementi, zaznani z agresivno (ali nižjo) ravnijo, so blokirani in začne se samodejno popravljanje (tj. čiščenje). Ta nastavitev je priporočljiva, ko so bile vse delovne postaje pregledane z agresivnimi nastavitvami, lažno pozitivno prepoznani predmeti pa so bili dodani med izključitve pri zaznavanju.
Uravnoteženo	Elementi, zaznani z uravnoteženo (ali nižjo) ravnijo, so blokirani in začne se samodejno popravljanje (tj. čiščenje).
Previdno	Elementi, zaznani s previdno (ali nižjo) ravnijo, so blokirani in začne se samodejno popravljanje (tj. čiščenje).
Izklopljeno	Uporabno za prepoznavanje in izključitev lažno prepoznanih predmetov. Zaščite pred zlonamerno programsko opremo ni mogoče izklopiti in je privzeta vrednost za morebitno nevarne programe.

Sprotna zaščita datotečnega sistema

Nadzorovanje datotečnega sistema preverja prisotnost zlonamerne kode pri odpiranju, ustvarjanju ali izvajanju vseh datotek v sistemu.



Privzeto se nadzorovanje datotečnega sistema zažene ob zagonu sistema in omogoča neprekinjeno pregledovanje. Priporočamo, da ne onemogočite možnosti **Omogoči sprotno zaščito datotečnega sistema** v naprednih nastavitvah > **Zaščite** > **Sprotna zaščita datotečnega sistema** > **Sprotna zaščita datotečnega sistema**.

Nosilci podatkov za pregled

Vsi nosilci podatkov so privzeto pregledani zaradi morebitnih groženj:

- **Lokalni diski** – pregleda vse sistemske in nespremenljive trde diske (na primer: *C:*\, *D:*\).
- **Izmenljivi nosilci podatkov** – pregleda CD-je/DVD-je, pogone USB, spominske kartice itd.
- **Omrežni diski** – pregleda vse preslikane omrežne diske (na primer: *H:*\ kot *store04*) ali omrežne diske z neposrednim dostopom (na primer: *store08*).

Priporočamo, da uporabite privzete nastavitve in jih spremenite le takrat, ko pregled določenih nosilcev podatkov znatno upočasni prenos podatkov.

Pregled

Privzeto so pregledane vse datoteke, ko jih odprete, ustvarite ali zaženete. Priporočamo vam, da ohranite privzete nastavitve, ki zagotavljajo največjo možno raven sprotne zaščite računalnika:

- **Odpiranju datoteke** – pregleda datoteko, ko jo odprete.
- **Ustvarjanje datoteke** – pregleda datoteko, ko jo ustvarite ali spremenite.
- **Izvedbi datoteke** – pregleda datoteko, ko jo zaženete ali izvajate.
- **Dostop do zagonskega sektorja na izmenljivih nosilcih podatkov** – ko v napravo vstavite izmenljivi nosilec podatkov, ki vsebuje zagonski sektor, se takoj izvede pregled zagonskega sektorja. Ta možnost ne omogoča pregledovanja datotek na izmenljivih nosilcih podatkov. Pregledovanje datotek na izmenljivih nosilcih podatkov je na voljo v razdelku **Nosilci podatkov za pregled** > **Izmenljivi nosilci podatkov**. Za pravilno delovanje funkcije **Dostop do zagonskega sektorja na izmenljivih nosilcih podatkov** ohranite možnost **Zagonski sektorji/UEFI** v orodju ThreatSense omogočeno.

Izključitve postopkov

Glejte Izključitve postopkov.

ThreatSense

Sprotna zaščita datotečnega sistema omogoča pregled vseh vrst nosilcev podatkov in se sproži z različnimi sistemskimi dogodki, kot je na primer dostop do datoteke. Z uporabo načinov zaznavanja, ki jih ponuja tehnologija **ThreatSense**, (kot so opisani v ThreatSense), je sprotno zaščito datotečnega sistema mogoče konfigurirati tako, da obravnava novo ustvarjene datoteke drugače kot obstoječe datoteke. Sprotno zaščito datotečnega sistema lahko na primer konfigurirate tako, da podrobneje nadzoruje novo ustvarjene datoteke.

Da bi pri uporabi sprotne zaščite zagotovili kar najmanjši odtis v sistemu, datotek, ki so že bile pregledane, zaščita ne pregleduje več (razen, če niso bile spremenjene). Datoteke se znova takoj pregledajo po vsaki posodobitvi orodja za zaznavanje. Takšno delovanje nadzorujete z uporabo možnosti **Pametna optimizacija**. Če je **Pametna**

optimizacija onemogočena, bodo vse datoteke pregledane ob vsakem dostopu do njih. Če želite spremeniti to nastavitev, odprite razdelek Napredne nastavitve > **Zaščite** > **Sprotna zaščita datotečnega sistema**. Kliknite **ThreatSense** > **Ostalo** in izberite ali prekličite izbiro možnosti **Omogoči pametno optimizacijo**.

Sprotna zaščita datotečnega sistema omogoča tudi konfiguriranje dodatnih parametrov orodja ThreatSense.

Izključitve postopkov

Funkcija izključitev postopkov omogoča, da postopke programov izključite iz sprotne zaščite datotečnega sistema. Za izboljšanje hitrosti varnostnega kopiranja, celovitosti postopkov in razpoložljivosti storitev se med varnostnim kopiranjem izvajajo nekateri procesi, ki so lahko v sporu z zaščito pred zlonamerno programsko opremo na ravni datotek. Edini učinkovit način za preprečevanje teh težav je deaktiviranje programa za zaščito pred zlonamerno programsko opremo. Z izključitvijo določenih postopkov (npr. postopkov rešitve za varnostno kopiranje) se vsi postopki datotek, povezani s temi izključenimi postopki, prezrejo in obravnavajo kot varni, zato prihaja do manjšega števila motenj postopka varnostnega kopiranja. Svetujemo previdnost pri uporabi funkcije izključitev postopkov, saj lahko orodje za varnostno kopiranje, ki ga izključite, dostopa do okuženih datotek in pri tem ne sproži opozorila. Iz tega razloga so razširjena dovoljenja dovoljena samo v modulu sprotne zaščite.

Ta funkcija ni enaka funkciji Izključene datotečne pripone, Izključitve sistema HIPS, Izključitve zaznav ali Izključitve delovanja.

Izključitve postopkov zmanjšajo tveganje za morebitne spore in izboljšajo delovanje izključenih programov, kar ima pozitiven učinek na splošno delovanje in stabilnost operacijskega sistema. Izključitev postopka/programa je izključitev njegove izvedljive datoteke (*.exe*).

Izvedljive datoteke lahko dodate na seznam izključenih postopkov v razdelku Napredne nastavitve > **Zaščite** > **Sprotna zaščita datotečnega sistema** > **Sprotna zaščita datotečnega sistema** > **Izključitve postopkov**.

Ta funkcija je izdelana za izključevanje orodij za varnostno kopiranje. Izključitev postopkov orodja za varnostno kopiranje zagotovi stabilnost sistema, obenem pa ne vpliva na delovanje varnostnega kopiranja, saj se varnostno kopiranje pri tem ne upočasni.

Kliknite **Uredi**, da se odpre okno za upravljanje funkcije **Izključitve postopkov**, v katerem lahko dodate izključitve in z brskanjem poiščete izvedljivo datoteko (npr. *Backup-tool.exe*), ki bo izključena iz pregledovanja.
Ko je datoteka *.exe* dodana med izključitve, ESET Internet Security tega postopka ne spremlja in za postopke datotek tega postopka se pregledovanje ne izvaja.

Če za izbiro izvedljive datoteke postopka ne uporabite funkcije brskanja, morate ročno vnesti celotno pot po izvedljive datoteke. V nasprotnem primeru izključitve ne bodo delovale pravilno in HIPS lahko sporoči napake.

Obstoječe postopke lahko tudi **urejate** ali jih **izbrišete** s seznama izključitev.

Zaščita spletnega dostopa izključitve ne upošteva. Če torej izključite izvedljivo datoteko spletnega brskalnika, se pregledovanje prenesenih datotek še vedno izvaja. Zato je infiltracijo še vedno mogoče zaznati. Omenjeni scenarij je zgolj primer in ustvarjanje izključitev za spletne brskalnike odsvetujemo.

Dodajanje ali urejanje izključitev procesov

V tem pogovornem oknu lahko **dodajate** postopke, izključene iz pogona za zaznavo. Izključitve postopkov zmanjšajo tveganje za morebitne spore in izboljšajo delovanje izključenih programov, kar ima pozitiven učinek na splošno delovanje in stabilnost operacijskega sistema. Izključitev postopka/programa je izključitev njegove izvedljive datoteke (*.exe*).

Izberite pot do datoteke izvzetega programa tako, da kliknete ... (npr. *C:\Program Files\Firefox\Firefox.exe*). NE vnesite imena programa.
Ko je datoteka *.exe* dodana med izključitve, ESET Internet Security tega postopka ne spremlja in za postopke datotek tega postopka se pregledovanje ne izvaja.

Če za izbiro izvedljive datoteke postopka ne uporabite funkcije brskanja, morate ročno vnesti celotno pot po izvedljive datoteke. V nasprotnem primeru izključitve ne bodo delovale pravilno in HIPS lahko sporoči napake.

Obstoječe postopke lahko tudi **urejate** ali jih **izbrišete** s seznama izključitev.

Kdaj spremeniti konfiguracijo sprotne zaščite

Sprotna zaščita je ključna pri vzdrževanju varnega sistema. Zato bodite previdni pri spreminjanju njenih parametrov. Priporočamo, da njene parametre spremenite le v posebnih primerih.

Po namestitvi programa ESET Internet Security so vse nastavitve optimizirane tako, da uporabnikom zagotavljajo največjo možno raven varnosti računalnika. Če želite obnoviti privzete nastavitve, kliknite ob razdelku Napredne nastavitve > **Zaščite** > **Odzivi na zaznane elemente**.

Preverjanje sprotne zaščite

Če želite preveriti, ali sprotna zaščita deluje in zaznava viruse, uporabite preskusno datoteko *www.eicar.com*. Omenjena preskusna datoteka je nenevarna datoteka, ki jo zaznajo vsi protivirusni programi. Datoteko so ustvarili v podjetju EICAR (European Institute for Computer Antivirus Research), da bi z njo preskusili funkcionalnost protivirusnih programov.

Datoteko lahko prenesete na naslednjem spletnem mestu: http://www.eicar.org/download/eicar.com
Ko vnesete ta URL v svoj brskalnik, bi moralo biti prikazano sporočilo, da je bila grožnja odstranjena.

Kaj storiti, če sprotna zaščita ne deluje

V tem poglavju najdete opis težav, do katerih lahko pride pri uporabi sprotne zaščite, in navodila za odpravo teh težav.

Sprotna zaščita je onemogočena

Če uporabnik pomotoma onemogoči sprotno zaščito, je treba funkcijo znova aktivirati. Če želite znova aktivirati sprotno zaščito, se v glavnem oknu programa pomaknite do razdelka **Nastavitve** in kliknite možnost **Zaščita računalnika** > **Nadzorovanje datotečnega sistema**.

Če se sprotna zaščita ne zažene ob zagonu sistema, je možnost **Omogoči sprotno zaščito datotečnega sistema** verjetno onemogočena. Če želite zagotoviti, da je ta možnost omogočena, odprite razdelek Napredne nastavitve > **Zaščite** > **Sprotna zaščita datotečnega sistema**.

Če sprotna zaščita ne zazna infiltracij in jih ne odstrani

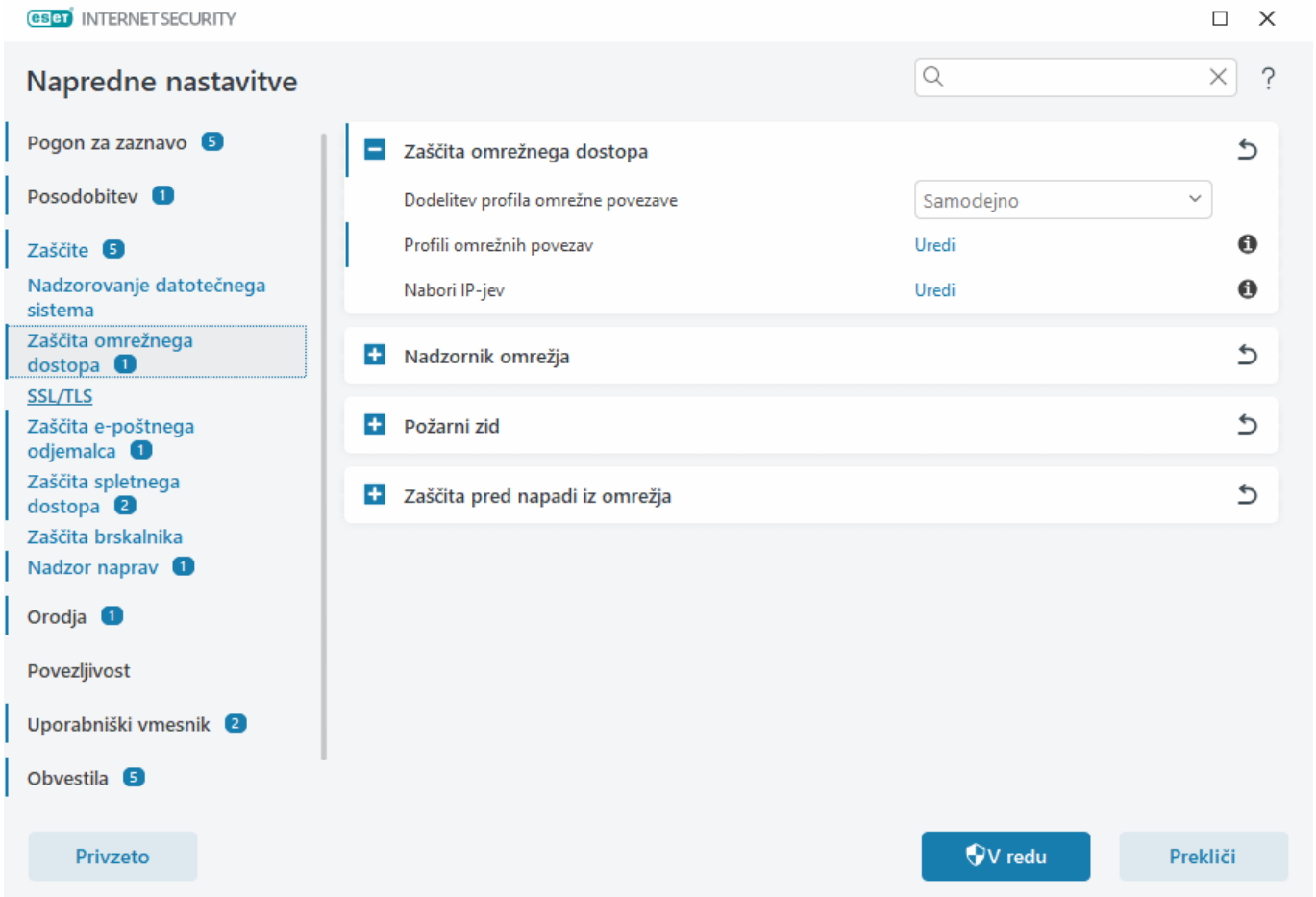
Prepričajte se, da v računalniku ni nameščen noben drug protivirusni program. Če imate hkrati nameščena dva protivirusna programa, lahko prideta v spor. Pred namestitvijo programa ESET vam priporočamo, da iz sistema odstranite vse druge protivirusne programe.

Sprotna zaščita se ne zažene

Če se sprotna zaščita ne zažene ob zagonu sistema (možnost **Omogoči nadzorovanje datotečnega sistema** pa je omogočena), je morda prišlo do sporov z drugimi programi. Za odpravljanje težave ustvarite dnevnik ESET SysInspector in ga posredujte tehnični podpori ESET v analizo.

Zaščita omrežnega dostopa

Zaščita omrežnega dostopa omogoča podrobno konfiguriranje vseh omrežnih povezav. Dovolite/zavrnite dostop do računalnika v določenih omrežjih, dovolite/zavrnite dostop do omrežnih naprav iz računalnika in več na podlagi konfiguracije. Program ESET Internet Security ima privzeto vnaprej konfigurirana pravila za požarni zid in zaščito omrežnega dostopa za največjo varnost. Vendar pa bodo določena okolja morda potrebovala konfiguracijo po meri. Spreminjanje privzetih nastavitev lahko opravi samo izkušen uporabnik.



Naslednje nastavitve lahko konfigurirate v razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa**

(za podroben opis vsake možnosti zaščite omrežnega dostopa kliknite spodnje povezave):

Zaščita omrežnega dostopa

Profili omrežnih povezav – profile lahko uporabite za nadzor delovanja požarnega zidu za določene omrežne povezave.

Nabori IP-jev – določite lahko zbirke naslovov IP, ki ustvarijo eno logično skupino naslovov IP, ki jih lahko uporabite za pravila za požarni zid.

Nadzornik omrežja

Požarni zid

Zaščita pred napadi iz omrežja

Profili omrežnih povezav

Profile lahko uporabljate za spremljanje delovanja zaščite omrežja programa ESET Internet Security za določene omrežne povezave. Pri ustvarjanju ali urejanju pravila za požarni zid, pravila ali varnostnega pravila za zaščito pred napadi z grobo silo ga lahko dodelite določenemu profilu ali ga uporabite za vse profile. Ko je profil aktiven v omrežni povezavi, zanj veljajo le globalna pravila (pravila brez določenega profila) in pravila, ki so bila dodeljena temu profilu. Ustvarite lahko več profilov z različnimi pravili, dodeljenimi omrežnim povezavam, tako da lahko preprosto spremenite delovanje požarnega zidu.

Profile in dodelitve omrežne povezave lahko konfigurirate v razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Zaščita omrežnega dostopa**.

Dodelitev profila omrežne povezave – omogoča, da izberete, ali je na novo odkritim omrežnim povezavam samodejno (v spustnem meniju izberite možnost **Samodejno**) dodeljen vnaprej določen profil ali profil po meri na podlagi aktivatorjev, konfiguriranih v profilih omrežnih povezav, ali če želite biti pozvani (v spustnem meniju izberite možnost **Vprašaj**), da konfigurirate zaščito omrežja in ročno dodelite profil vsakič, ko je zaznana nova omrežna povezava.

Prav tako lahko ročno dodelite določen profil omrežnih povezav v glavnem oknu programa > **Nastavitve** > **Zaščita omrežja** > **Omrežne povezave**. Pomaknite se na določeno omrežno povezavo in kliknite ikono menija ⋮ > **Uredi**, da odprete okno Konfiguriranje zaščite omrežja in izberete profil.

Profili omrežnih povezav – kliknite možnost **Uredi** da dodate ali uredite profile omrežnih povezav.

Naslednji profili so vnaprej določeni in jih ni mogoče urejati/izbrisati:

Zasebno – za zaupanja vredna omrežja (domače ali službeno omrežje). Računalnik in datoteke v skupni rabi, shranjene v računalniku, so vidne drugim uporabnikom omrežja, sistemski viri pa so dostopni drugim uporabnikom v omrežju (omogočen je dostop do datotek in tiskalnikov v skupni rabi, omogočena je dohodna komunikacija RPC in na voljo je skupna raba oddaljenega namizja). Priporočamo uporabo te nastavitve pri dostopu do varnega lokalnega omrežja. Ta profil je samodejno dodeljen omrežni povezavi, če je konfiguriran kot domena ali zasebno omrežje v sistemu Windows.

Javno – za omrežja, ki niso vredna zaupanja (javno omrežje). Datoteke in mape v vašem sistemu niso v skupni rabi ali vidne drugim uporabnikom v omrežju in deljenje sistemskih virov je deaktivirano. Pri dostopu do brezžičnih

omrežij priporočamo uporabo te nastavitve. Ta profil je samodejno dodeljen kateri koli omrežni povezavi, ki ni konfigurirana kot domena ali zasebno omrežje v sistemu Windows.

Ko omrežna povezava preklopi na drug profil, se v spodnjem desnem kotu zaslona prikaže obvestilo.

Dodajanje ali urejanje profilov omrežnih povezav

Profile omrežnih povezav lahko dodate ali uredite v razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Zaščita omrežnega dostopa** > **Profili omrežnih povezav** > **Uredi**. Če želite urediti profil, ga morate izbrati s seznama **profilov omrežnih povezav**.

Naslednji profili so vnaprej določeni in jih ni mogoče urejati/izbrisati:

Zasebno – za zaupanja vredna omrežja (domače ali službeno omrežje). Računalnik in datoteke v skupni rabi, shranjene v računalniku, so vidne drugim uporabnikom omrežja, sistemski viri pa so dostopni drugim uporabnikom v omrežju (omogočen je dostop do datotek in tiskalnikov v skupni rabi, omogočena je dohodna komunikacija RPC in na voljo je skupna raba oddaljenega namizja). Priporočamo uporabo te nastavitve pri dostopu do varnega lokalnega omrežja. Ta profil je samodejno dodeljen omrežni povezavi, če je konfiguriran kot domena ali zasebno omrežje v sistemu Windows.

Javno – za omrežja, ki niso vredna zaupanja (javno omrežje). Datoteke in mape v vašem sistemu niso v skupni rabi ali vidne drugim uporabnikom v omrežju in deljenje sistemskih virov je deaktivirano. Pri dostopu do brezžičnih omrežij priporočamo uporabo te nastavitve. Ta profil je samodejno dodeljen kateri koli omrežni povezavi, ki ni konfigurirana kot domena ali zasebno omrežje v sistemu Windows.

Vrh/gor/dol/dno  – omogoča prilagoditev prednostne ravni profilov omrežnih povezav (Profili omrežnih povezav se ocenjujejo in uporabljajo po prednosti. Vedno se uporablja prvi ujemajoči se profil).

Dodajanje ali urejanje profila

Profil omrežne povezave po meri omogoča uporabo pravil za požarni zid in določanje dodatnih nastavitev za določene omrežne povezave. Določili boste, katerim omrežnim povezavam bo profil po meri dodeljen v razdelku Aktivatorji.

Če želite odpreti urejevalnik profilov, v oknu **Profili omrežnih povezav**:

- Kliknite **Dodaj**.
- Izberite enega od obstoječih profilov in kliknite **Uredi**.
- Izberite enega od obstoječih profilov in kliknite **Kopiraj**.

Ime – ime po meri za vaš profil.

Opis – opis profila za lažje prepoznavanje profila.

Dodatni zaupanja vredni naslovi – naslovi, ki so določeni tukaj, so dodani zaupanja vrednem območju omrežne povezave, za katero se uporablja ta profil (ne glede na vrsto zaščite omrežja).

Zaupanja vredna povezava – računalnik in datoteke v skupni rabi, shranjene v računalniku, so vidne drugim uporabnikom omrežja, sistemski viri pa so dostopni drugim uporabnikom v omrežju (omogočen je dostop do

datotek in tiskalnikov v skupni rabi, omogočena je dohodna komunikacija RPC in na voljo je skupna raba oddaljenega namizja). Priporočamo uporabo te nastavitve pri ustvarjanju profila za varno lokalno omrežno povezavo. Vsa neposredna povezana podomrežja so prav tako obravnavana kot zaupanja vredna. Če je na primer omrežna kartica povezana s tem omrežjem z naslovom IP 192.168.1.5 in je maska podomrežja 255.255.255.0, je podomrežje 192.168.1.0/24 dodano v zaupanja vredno območje te omrežne povezave. Če ima kartica več naslovov/podomrežij, bodo vsi zaupanja vredni.

Prijava šibkega šifriranja omrežja Wi-Fi – ESET Internet Security prikaže obvestilo na namizju, ko je vzpostavljena povezava z nezaščitenim brezžičnim omrežjem ali s slabo zaščitenim omrežjem.

Aktivatorji – pogoji po meri, ki morajo biti izpolnjeni, da se ta profil omrežne povezave dodeli omrežni povezavi. Za podrobnejšo razlago glejte Aktivatorji.

Aktivatorji

Aktivatorji so pogoji po meri, ki morajo biti izpolnjeni, da se profil omrežnih povezav dodeli omrežni povezavi. Če ima povezano omrežje enake atribute, kot so določeni v aktivatorjih za povezan profil omrežja, bo profil uporabljen v omrežju. Profil omrežnih povezav ima lahko enega ali več aktivatorjev. Če je aktivatorjev več, velja logika OR (izpolnjen mora biti vsaj en pogoj). V urejevalniku profila omrežnih povezav lahko določite aktivatorje. Ustvarjanje profilov omrežnih povezav po meri mora opraviti izkušen uporabnik.

Na voljo so naslednji aktivatorji (če želite vedeti podrobnosti za trenutno omrežje, glejte Omrežne povezave):

Kartica

Vrsta kartice – uporabite profil, če je omrežna povezava vzpostavljena na izbrani vrsti kartice.
Ime kartice – uporabite profil, če se ime omrežne kartice ujema.
IP kartice – uporabite profil, če se naslov IP vaše omrežne kartice ujema.

DNS

Pripona DNS – uporabite profil, če se ime domene ujema.
IP strežnika DNS – uporabite profil, če se naslov IP strežnika DNS ujema.

WINS

Uporabite profil, če se preslikani naslov IP Windows Internet Name Service (WINS) ujema.

DHCP

IP strežnika DHCP – prilagodite IP naslova strežnika DHCP, da se ujema.

Privzeti prehod

IP – uporabite profil, če se naslov IP privzetega prehoda ujema.
Naslov MAC – uporabite profil, če se naslov privzetega prehoda MAC ujema.

Wi-Fi

SSID – uporabite profil, če se SSID (ime omrežja Wi-Fi) ujema.
Ime profila – uporabite profil, če se ime profila omrežja Wi-Fi ujema.
Vrsta zaščite – uporabite profil, če se vrsta zaščite ujema z vrsto zaščite, izbrano v spustnem meniju. (Če se želite zagotoviti ujemanje z več kot eno zaščito, ustvarite drug aktivator).
Vrsta šifriranja – uporabite profil, če se vrsta šifriranja ujema z vrsto šifriranja, izbrano v spustnem meniju. (Če se želite zagotoviti ujemanje z več kot eno zaščito, ustvarite drug aktivator).
Varnost omrežja – uporabite profil, če je omrežje **odprto/zavarovano**.

Profil sistema Windows

Uporabite profil, če je omrežje konfigurirano v sistemu Windows kot **domena/zasebno/javno**.

Preverjanje pristnosti

Preverjanje pristnosti omrežja poišče določen strežnik v omrežju in uporabi asimetrično šifriranje za preverjanje pristnosti tega strežnika. Preverjanje pristnosti imena omrežja se mora ujemati z imenom, nastavljenim v nastavitvah strežnika za preverjanje pristnosti. Ime razlikuje med malimi in veliki črkami. Ime strežnika lahko vnesete kot naslov IP, DNS ali ime NetBios.
Prenesite strežnik ESET Authentication Server.
Javni ključ lahko uvozite z eno od teh vrst datotek:
• Šifriran javni ključ PEM (.pem); ta ključ lahko ustvarite s strežnikom za preverjanje pristnosti ESET
• Šifriran javni ključ
• Potrdilo o javnem ključu (.crt)
Kliknite **Preskusi**, da preskusite nastavitve. Če je preverjanje pristnosti uspešno, se prikaže Preverjanje pristnosti strežnika je bilo uspešno. Če preverjanje pristnosti ni pravilno konfigurirano, se prikaže eno od navedenih sporočil o napaki:
Pristnosti strežnika ni bilo mogoče preveriti. Neveljaven ali neskladen podpis.
Podpis strežnika se ne ujema z vnesenim javnim ključem.
Pristnosti strežnika ni bilo mogoče preveriti. Ime omrežja se ne ujema.
Ime konfiguriranega omrežja se ne ujema z imenom omrežja strežnika za preverjanje pristnosti. Preglejte obe imeni in se prepričajte, da sta enaki.
Pristnosti strežnika ni bilo mogoče preveriti. Neveljaven ali manjkajoč odgovor iz strežnika.
Če se strežnik ne izvaja oz. ni dostopen, ni odgovora. Neveljaven odgovor je lahko prejet, če se na navedenem naslovu izvaja drug strežnik HTTP.
Vnesen neveljaven javni ključ.
Prepričajte se, da vnesen javni ključ ni poškodovan.

Nabori IP-jev

Nabor IP-jev je zbirka naslovov IP, ki ustvarijo eno logično skupino naslovov IP, uporabnih pri ponovni uporabi istega nabora naslovov v več pravilih za požarni zid ali varnostnih pravilih za zaščito pred napadi z grobo silo. ESET Internet Security vsebuje tudi vnaprej določene nabore IP-jev, za katere se uporabljajo notranja pravila. Primer take skupine je **Zaupanja vredno območje**. Zaupanja vredno območje predstavlja skupino omrežnih naslovov, kjer so računalnik in datoteke v skupni rabi, shranjene v računalniku, vidne drugim uporabnikom omrežja, sistemski viri pa so dostopni drugim uporabnikom v omrežju.

Za dodajanje nabora IP-jev:

1. Odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Nabori IP-jev** > **Uredi**.

2. Kliknite možnost **Dodaj**, vnesite **Ime** in **Opis** za območje in vnesite oddaljeni naslov IP v polje **Naslov oddaljenega računalnika (IPv4/IPv6, doseg, maska)**.

3. Kliknite **V redu**.

Za več informacij glejte Urejanje naborov IP-jev.

Urejanje naborov IP-jev

Za več informacij o naborih IP-jev glejte Nabori IP-jev.

Stolpci

Ime – ime skupine oddaljenih računalnikov.

Opis – splošen opis skupine.

Naslovi IP – oddaljeni naslovi IP, ki pripadajo naboru IP-jev.

Elementi kontrolnika

Ko **dodajate** ali **urejate** nabor IP-jev, so na voljo naslednja polja:

Ime – ime skupine oddaljenih računalnikov.

Opis – splošen opis skupine.

Naslov oddaljenega računalnika (IPv4, IPv6, obseg, maska) – omogoča, da dodate oddaljeni naslov, obseg naslovov ali podomrežje.

Izbriši – odstrani območje s seznama.

Vnaprej opredeljenih naborov IP-jev ni mogoče odstraniti.

Primeri naslovov IP

Dodaj naslov IPv4:
Enotni naslov – doda naslov IP posameznega računalnika (na primer *192.168.0.10*).
Obseg naslovov – vnesite začetni in končni naslov IP naslova, da določite obseg IP več računalnikov (na primer *od 192.168.0.1 do 192.168.0.99*).
Podomrežje – podomrežje (skupina računalnikov) je določeno z naslovom IP in masko. 255.255.255.0 je na primer maska omrežja za podomrežje 192.168.1.0. Za izključitev celotne vrste podomrežja v *192.168.1.0/24*.
Dodaj naslov IPv6:
Enotni naslov – doda naslov IP posameznega računalnika (na primer *2001:718:1c01:16:214:22ff:fec9:ca5*).
Podomrežje – podomrežje (skupina računalnikov) je določeno z naslovom IP in masko (na primer: *2002:c0a8:6301:1::1/64*).

Nadzornik omrežja

Nadzornik omrežja pomaga odkriti ranljivosti v vašem zaupanja vrednem (domačem ali službenem) omrežju (npr. odprta vrata ali šibko geslo usmerjevalnika). Zagotavlja tudi seznam povezanih naprav, razvrščenih glede na vrsto (npr. tiskalnik, usmerjevalnik, mobilna naprava), ter vam tako omogoča, da imate pregled nad napravami, ki so

povezane z vašim domačim omrežjem (npr. igralna konzola, naprave IoT ali druge domače pametne naprave). Nadzornika omrežja lahko konfigurirate v razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Nadzornik omrežja**.

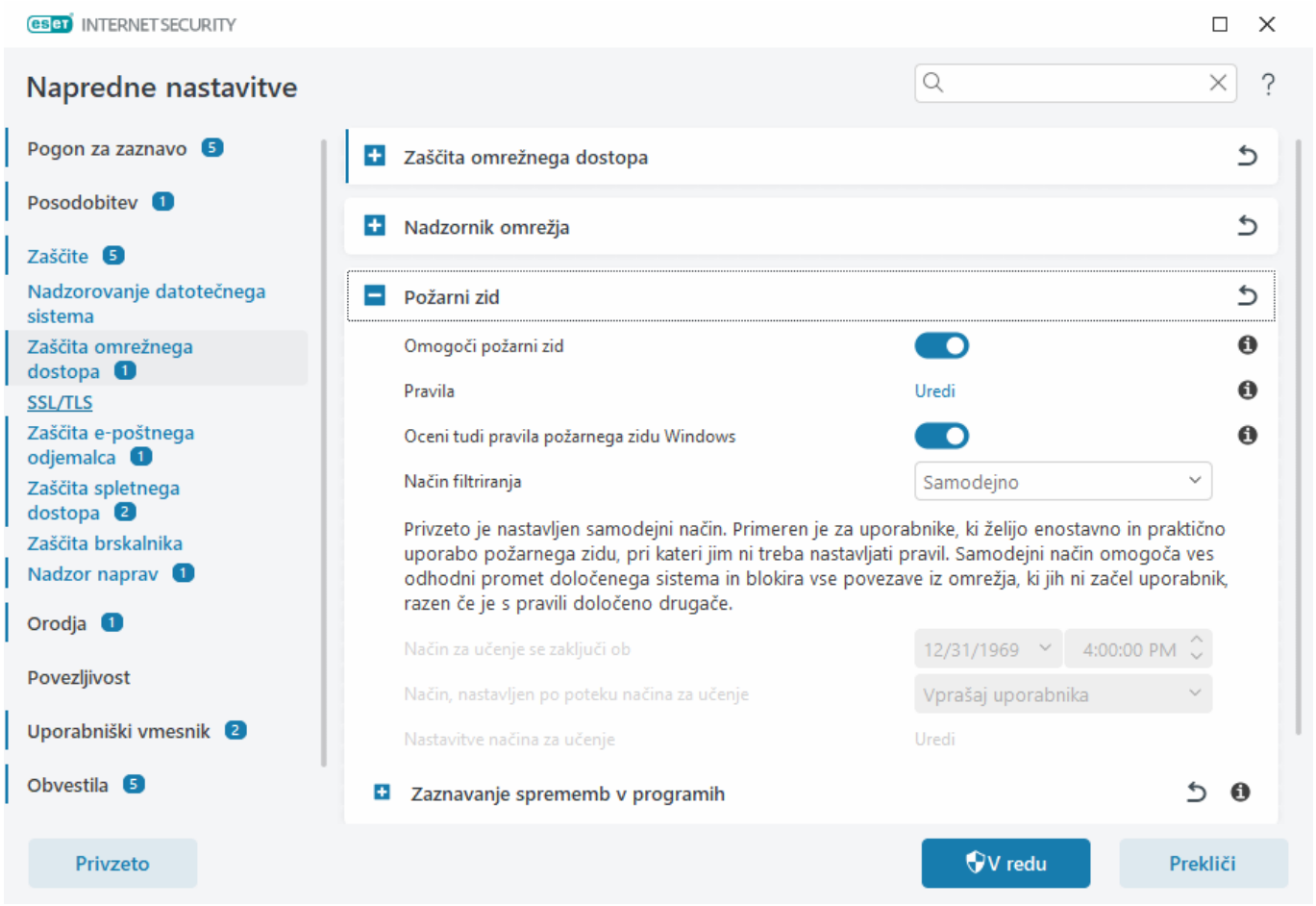
Omogoči nadzornika omrežja – Nadzornik omrežjapomaga odkriti ranljivosti v domačem omrežju, npr. odprta vrata ali šibko geslo usmerjevalnika. Zagotavlja tudi seznam povezanih naprav, razvrščenih glede na vrsto.

Obvesti me o novo zaznanih omrežnih napravah – obvesti vas, ko je v vašem omrežju zaznana nova naprava.

Požarni zid

Požarni zid nadzira ves dohodni in odhodni omrežni promet v računalniku na podlagi notranjih pravil in pravil, ki jih določite vi. To izvedete tako, da omogočite ali zavrnete posamezne omrežne povezave. Požarni zid zagotavlja zaščito pred napadi iz oddaljenih naprav in lahko blokira storitve, ki predstavljajo morebitno grožnjo.

Če želite konfigurirati požarni zid, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Požarni zid**.



Požarni zid

Omogoči požarni zid

Priporočamo, da to funkcijo pustite omogočeno, da zagotovite varnost sistema. Če je požarni zid omogočen, omrežni promet pregledan v obeh smereh.

Pravila

Nastavitev pravil omogoča ogled in urejanje vseh pravil za požarni zid, ki veljajo za promet posameznih programov v zaupanja vrednih območjih in v internetu.

> Ko Botnet napade vaš računalnik, lahko ustvarite pravilo IDS. Pravilo lahko spremenite v razdelku Napredne nastavitve > **Zaščite** > **Zaščita dostopa do omrežja** > **Zaščita pred napadi iz omrežja** > **Pravila IDS** tako, da kliknete možnost **Uredi**.

Oceni tudi pravila požarnega zidu Windows

V samodejnem načinu filtriranja dovoli tudi promet, ki ga dovoljujejo pravila požarnega zidu Windows, razen če to izrecno blokirajo pravila programa ESET.

Način filtriranja

Način delovanja požarnega zidu se spremeni glede na način filtriranja. Načini filtriranja vplivajo tudi na raven potrebnega posredovanja uporabnika.

Za požarni zid ESET Internet Security so na voljo naslednji načini filtriranja:

Način filtriranja	Opis
Samodejni način	Privzeti način. Ta način je primeren za uporabnike, ki si želijo preproste in priročne uporabe požarnega zidu, ne da bi morali določiti pravila. Ustvarite lahko uporabniško določena pravila po meri, vendar pa v **samodejnem načinu** niso obvezna. Samodejni način dovoli ves odhodni promet za navedeni sistem in blokira večino dohodnega prometa, razen dela prometa iz zaupanja vrednega območja (kot je navedeno v možnosti IDS in napredne možnosti/Dovoljene storitve) in odgovorov na nedavno odhodno komunikacijo.
Interaktivni način	Omogoča ustvarjanje konfiguracije po meri za požarni zid. Ko je zaznana komunikacija, na katero se ne nanaša nobeno pravilo, se prikaže pogovorno okno s sporočilom o neznani povezavi. V pogovornem oknu je na voljo možnost za omogočanje ali zavrnitev komunikacije, izbrano odločitev pa lahko shranite kot novo pravilo za požarni zid. Če želite ustvariti novo pravilo, bodo vse prihodnje komunikacije te vrste omogočene ali zavrnjene v skladu s tem pravilom.
Način glede na pravilnik	Blokira vse povezave, ki niso določene s pravilom, ki jih omogoča. V tem načinu lahko izkušeni uporabniki določijo pravila, ki omogočajo le želene in varne povezave. Vse druge nedoločene povezave bo blokiral požarni zid.
Način za učenje	Samodejno ustvari in shrani pravila; ta način je najbolje uporabiti pri začetni konfiguraciji osebnega požarnega zidu, vendar ni namenjen uporabi v daljšem obdobju. Posredovanje uporabnika ni potrebno, saj program ESET Internet Security shrani pravila v skladu z vnaprej določenimi parametri. Način za učenje naj bi se uporabljal le, dokler niso ustvarjena vsa pravila za zahtevano komunikacijo, da se prepreči varnostno tveganje.

Način za učenje se zaključi ob – nastavite datum in čas, ko se način za učenje samodejno zaključi. Način za učenje lahko kadar koli izklopite tudi ročno.

Način, nastavljen po poteku načina za učenje – določa, na kateri način filtriranja bo požarni zid preklopil po poteku časovnega obdobja za način za učenje. Preberite več o načinih filtriranja v zgornji tabeli. Po poteku možnost **Vprašaj uporabnika** za izvajanje sprememb načina filtriranja požarnega zidu zahteva skrbniške pravice.

Nastavitve načina za učenje – kliknite možnost **Uredi**, če želite konfigurirati parametre za shranjevanje pravil, ustvarjenih v načinu za učenje.

Zaznavanje sprememb v programih

Če spremenjeni programi, za katere obstaja pravilo požarnega zidu, poskušajo vzpostaviti povezave, funkcija zaznavanja sprememb programa prikaže obvestila.

Nastavitve načina za učenje

Način za učenje samodejno ustvari in shrani pravilo za vsako komunikacijo, ki je bila vzpostavljena v sistemu. Interakcija uporabnika ni potrebna, saj program ESET Internet Security pravila shrani v skladu z vnaprej določenimi parametri.

V tem načinu je sistem lahko izpostavljen tveganju, zato se priporoča le za začetno konfiguracijo požarnega zidu.

S spustnega seznama v razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Požarni zid** > **Požarni zid** > **Način filtriranja** izberite možnost **Učenje**, da aktivirate možnosti načina za učenje. Kliknite možnost **Uredi** ob možnosti **Nastavitve načina za učenje**, da konfigurirate naslednje možnosti:

V načinu učenja požarni zid ne filtrira komunikacije. Vsa odhodna in dohodna komunikacija je omogočena. V tem načinu požarni zid računalnika ne zaščiti v celoti.

Dohodni promet iz zaupanja vrednega območja – primer dohodne povezave znotraj zaupanja vrednega območja je oddaljena naprava v zaupanja vrednem območju, ki poskuša vzpostaviti komunikacijo z lokalnim programom, ki se izvaja v računalniku.

Odhodni promet v zaupanja vredno območje – lokalni program poskuša vzpostaviti povezavo z drugo napravo v lokalnem omrežju ali v omrežju v zaupanja vrednem območju.

Dohodni internetni promet – oddaljena naprava poskuša komunicirati s programom, ki se izvaja v računalniku.

Odhodni internetni promet – lokalni program poskuša vzpostaviti povezavo z drugo napravo.

Vsak razdelek omogoča, da določite parametre, ki bodo dodani v novoustvarjena pravila:

Dodaj lokalna vrata – vključuje številko lokalnih vrat omrežne komunikacije. Za odhodne komunikacije so navadno ustvarjene naključne številke. Zato priporočamo, da to možnost omogočite samo za dohodne komunikacije.

Dodaj program – vključuje ime lokalnega programa. Ta možnost je primerna za prihodnja pravila na ravni programa (pravila, ki določajo komunikacijo za celoten program). Na primer, komunikacijo lahko omogočite samo za spletni brskalnik ali e-poštnega odjemalca.

Dodaj oddaljena vrata – vključuje številko oddaljenih vrat omrežne komunikacije. Dovolite ali zavrnete lahko na primer določeno storitev, ki je povezana s številko standardnih vrat (HTTP - 80, POP3 - 110 itn.).

Dodaj oddaljeni naslov IP/zaupanja vredno območje – oddaljeni naslov IP ali območje se lahko uporablja kot parameter za nova pravila, ki določajo vse omrežne povezave med lokalnim sistemom in tem oddaljenim naslovom/območjem. Ta možnost je primerna, če želite določiti dejanja za posamezno napravo ali skupino naprav v omrežju.

Največje dovoljeno število različnih pravil za program – če program komunicira prek različnih vrat z različnimi naslovi IP itn., požarni zid v načinu učenja ustvari primerno število pravil za ta program. Ta možnost vam

omogoča, da omejite število pravil, ki jih je mogoče ustvariti za posamezni program.

Pravila za požarni zid

Pravila za požarni zid so nabor pogojev, s katerimi je mogoče pomembno preskusiti vse omrežne povezave in vsa dejanja, dodeljena tem pogojem. S pravili požarnega zidu lahko določite dejanje, ki se izvede ob vzpostavitvi različnih vrst omrežnih povezav.

Pravila so ovrednotena od zgoraj navzdol in njihovo prednost lahko vidite v prvem stolpcu. Dejanje prvega ujemajočega se pravila se uporabi za vsako ovrednoteno omrežno povezavo.

Povezave lahko razdelite v dohodne in odhodne povezave. Dohodne povezave zažene oddaljena naprava, ki poskuša vzpostaviti povezavo z lokalnim sistemom. Odhodne povezave delujejo v nasprotni smeri – lokalni sistem poskuša vzpostaviti povezavo z oddaljeno napravo.

Če je zaznana nova neznana komunikacija, morate skrbno premisliti, ali jo želite omogočiti ali zavrniti. Vsiljene, nevarne ali povsem neznane povezave predstavljajo varnostno tveganje za računalnik. Če vzpostavite tako povezavo, priporočamo, da ste pozorni na oddaljeno napravo in program, ki poskušata vzpostaviti povezavo z vašim računalnikom. Mnogo infiltracij poskuša pridobiti in poslati zasebne podatke ali v gostiteljske delovne postaje prenesti druge zlonamerne programe. S požarnim zidom lahko take povezave zaznate in jih prekinete.

Pravila za požarni zid si lahko ogledate in jih urejate v razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Požarni zid** > **Pravila** > **Uredi**.

Če imate veliko pravil za požarni zid, lahko s filtrom prikažete samo določena pravila. Če želite filtrirati pravila za požarni zid, kliknite možnost **Več filtrov** nad seznamom pravil za požarni zid. Pravila lahko filtrirate na podlagi naslednjih meril:

- Poreklo
- Smer
- Dejanje
- Razpoložljivost

Privzeto so vnaprej določena pravila za požarni zid skrita. Če želite prikazati vsa vnaprej določena pravila, onemogočite gumb za preklop ob možnosti **Skrij vgrajena (vnaprej določena) pravila**. Pravila lahko onemogočite, vendar vnaprej določenih pravil ni mogoče izbrisati.

Za iskanje pravil zgoraj desno kliknite ikono za iskanje .

Stolpci

Prednost – pravila so ovrednotena od zgoraj navzdol in njihovo prednost si lahko ogledate v prvem stolpcu.

Omogočeno – pokaže, ali so pravila omogočena ali onemogočena; če želite aktivirati pravilo, mora biti izbrano ustrezno potrditveno polje.

Program – označuje program, za katerega velja pravilo.

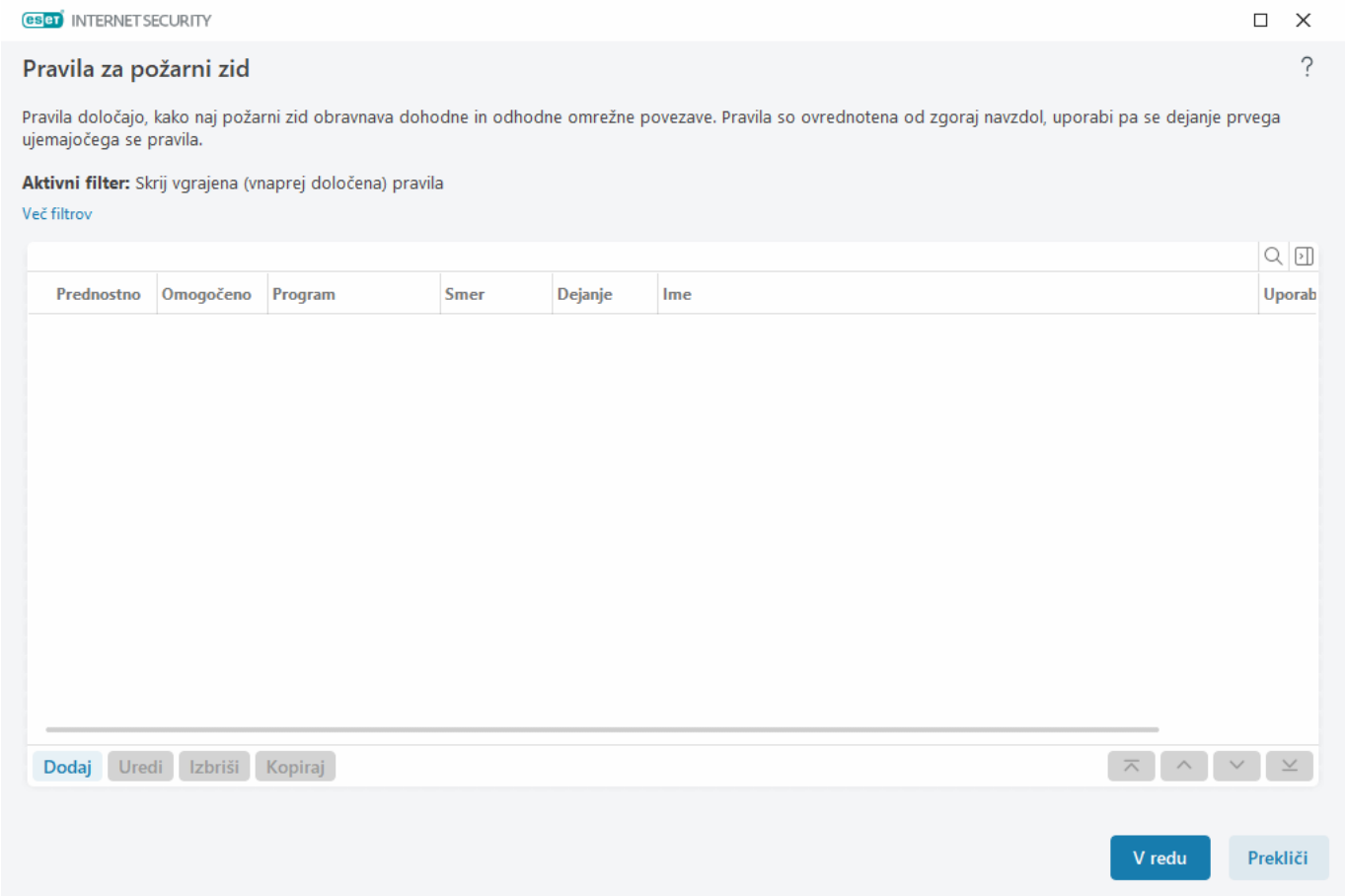
Smer – smer komunikacije (dohodno/odhodno/oboje).

Dejanje – pokaže stanje komunikacije (blokiraj/dovoli/vprašaj).

Ime – ime pravila. Ikona ESET predstavlja vnaprej določeno pravilo.

Uporabljeni časi – skupno število primerov uporabe pravila.

Kliknite ikono za razširitev, da prikažete podrobnosti pravila.



Elementi kontrolnika

Dodaj – ustvari novo pravilo.

Uredi – uredi obstoječe pravilo.

Izbriši – odstrani obstoječe pravilo.

Kopiraj – ustvari kopijo izbranega pravila.

Vrh/gor/dol/dno – s temi gumbi lahko prilagodite raven prednosti pravil (pravila se izvajajo od vrha proti dnu).

Dodajanje ali urejanje pravil za požarni zid

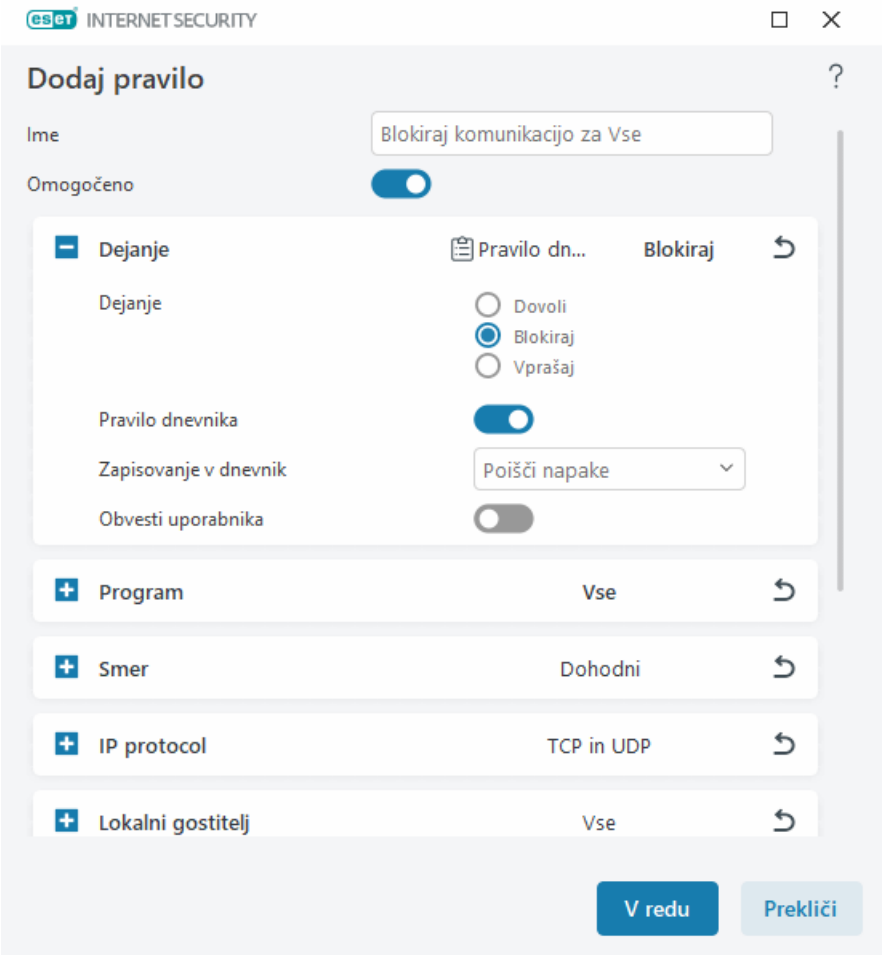
Pravila za požarni zid predstavljajo pogoje, s katerimi je mogoče pomembno preskusiti vse omrežne povezave in vsa dejanja, dodeljena tem pogojem. Urejanje ali dodajanje pravil požarnega zidu je morda potrebno v primeru spremembe nastavitev omrežja (ko se na primer spremeni omrežni naslov ali številka vrat za oddaljeno stran), da se zagotovi pravilno delovanje programa, na katerega vpliva pravilo. Pravil za požarni zid po meri naj ustvari izkušeni uporabnik.

Ilustrirana navodila

Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:

- Odpiranje ali zapiranje (odobritev ali zavrnitev) posameznih vrat s požarnim zidom
- Ustvarjanje pravila požarnega zidu iz dnevniških datotek v izdelku ESET Internet Security

Če želite dodati ali urediti pravilo za požarni zid, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Požarni zid** > **Pravila** > **Uredi**. V oknu Pravila za požarni zid kliknite možnost **Dodaj** ali **Uredi**.



Ime – vnesite ime pravila.

Omogočeno – kliknite gumb za preklop, da aktivirate pravilo.

Dodajte dejanja in pogoje za pravilo za požarni zid:

Dejanje

Dejanje – izberite, če želite **dovoliti/blokirati** komunikacijo, ki ustreza pogojem, določenim v tem pravilu, ali če želite, da vas ESET Internet Security **vpraša** vsakič, ko se vzpostavi komunikacija.
Pravilo dnevnika – če je pravilo uporabljeno, bo zabeleženo v dnevniške datoteke.
Resnost zapisovanja v dnevnik – izberite resnost zapisa v dnevnik za to pravilo.
Možnost **Obvesti uporabnika** prikaže obvestilo, ko je uporabljeno pravilo.

Program

Navedite program, v katerem bo uporabljeno to pravilo.
Pot do programa – kliknite **...** in se pomaknite do programa ali vnesite polno pot do programa (na primer C:\Program Files\Firefox\Firefox.exe). NE vnesite samo imena programa.
Podpis programa – pravilo lahko uporabite za programe na podlagi podpisov (ime založnika). V spustnem meniju izberite, če želite pravilo uporabiti za programe z **vsakim veljavnim podpisom** ali za programe, **ki jih podpiše določen podpisnik**. Če izberete programe, **ki jih podpiše določen podpisnik**, morate določiti podpisnika v polju **Ime podpisnika**.
Program trgovine Microsoft Store – izberite program, ki je nameščen iz trgovine Microsoft Store v spustnem meniju.
Storitev – namesto programa lahko izberete sistemsko storitev. Če želite izbrati storitev, odprite spustni meni.
Uporabi za podrejene postopke – nekateri programi lahko zaženejo več postopkov, medtem ko vidite samo eno okno programa. Kliknite gumb za preklop, da omogočite pravilo za vsak postopek v določenem programu.

Smer

Izberite **smer** komunikacije za to pravilo:
- **Oboje** – dohodna in odhodna komunikacija
- **Dohodna** – samo dohodna komunikacija
- **Odhodna** – samo odhodna komunikacija

Protokol IP

V spustnem meniju izberite **Protokol**, če želite, da se to pravilo uporabi samo za določen protokol.

Lokalni gostitelj

Lokalni naslovi, obseg naslovov ali podomrežje, kjer se uporablja to pravilo. Če naslov ni določen, bo pravilo veljalo za vso komunikacijo z lokalnimi gostitelji. Naslove IP, obsege naslovov ali podomrežja lahko dodate neposredno v besedilno polje **IP** ali izberete med obstoječimi nabori IP-jev tako, da kliknete možnost **Uredi** ob možnosti **Nabori IP-jev**.

Lokalna vrata

Številke lokalnih **vrat**. Če številke niso na voljo, bo pravilo veljalo za vsa vrata. Dodajte ena komunikacijska vrata ali več komunikacijskih vrat.

Oddaljeni gostitelj

Oddaljeni naslov, obseg naslovov ali podomrežje, kjer je uporabljeno to pravilo. Če naslov ni določen, bo pravilo veljalo za vso komunikacijo z oddaljenimi gostitelji. Naslove IP, obsege naslovov ali podomrežja lahko dodate neposredno v besedilno polje **IP** ali izberete med obstoječimi nabori IP-jev tako, da kliknete možnost **Uredi** ob možnosti **Nabori IP-jev**.

Oddaljena vrata

Številke oddaljenih **vrat**. Če številke niso na voljo, bo pravilo veljalo za vsa vrata. Dodajte ena komunikacijska vrata ali več komunikacijskih vrat.

Profil

Pravilo za požarni zid je mogoče uporabiti za določene profile omrežnih povezav.
Vse – pravilo bo uporabljeno za vsako omrežno povezavo kljub uporabljenemu profilu.
Izbrano – pravilo bo uporabljeno za določeno omrežno povezavo na podlagi izbranega profila. Izberite potrditveno polje zraven profilov, ki jih želite izbrati.

Ustvarimo novo pravilo, ki bo spletnemu brskalniku Firefox dovolilo dostop do naslednjih lokacij: Internet/spletna mesta lokalnega omrežja.
1.V razdelku **Dejanje** izberite možnost **Dejanje** > **Dovoli**.
2.V razdelku **Program** določite **pot do programa** spletnega brskalnika (na primer C:\Program Files\Firefox\Firefox.exe). NE vnesite samo imena programa.
3.V razdelku **Smer** izberite **Smer** > **Odhodna**.
4.V razdelku **Protokol IP** v spustnem meniju **Protokol** izberite **TCP & UDP**.
5.V razdelku **Oddaljena vrata** dodajte številke **vrat**: *80,443* omogoča standardno brskanje.

Zaznavanje sprememb v programih

Če spremenjeni programi, za katere obstaja pravilo požarnega zidu, poskušajo vzpostaviti povezave, funkcija zaznavanja sprememb programa prikaže obvestila. Spremembe v programih so mehanizem začasne ali trajne zamenjave izvirnega programa z drugim programom z drugo izvedljivo datoteko (funkcija ščiti pred zlorabo pravil za požarni zid).

Ta funkcija ni namenjena splošnemu zaznavanju sprememb v programih. Cilj se je izogniti zlorabljanju obstoječih pravil požarnega zida, zato se nadzorujejo samo programi, za katere obstajajo določena pravila požarnega zida.

Če želite urediti **zaznavanje sprememb v programih**, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Požarni zid** > **Zaznavanje sprememb v programih**.

Omogoči zaznavanje sprememb v programu – če je ta možnost izbrana, program nadzira spremembe v programu (posodobitve, okužbe, druge spremembe). Ko spremenjen program poskuša vzpostaviti povezavo, prejmete obvestilo od požarnega zidu.

Omogoči spreminjanje podpisanih (zaupanja vrednih) programov – ne obvesti me, če ima program enak veljaven elektronski podpis pred spremembo in po njej.

Seznam programov, izključenih iz zaznavanja – v tem oknu lahko dodate ali odstranite posamezne programe, za katere je dovoljeno spreminjanje brez obvestila.

Seznam programov, izključenih iz zaznavanja

Osebni požarni zid v programu ESET Internet Security zazna spremembe v programih, za katere obstajajo pravila (glejte Zaznavanje sprememb v programih).

V nekaterih primerih morda ne želite uporabiti te funkcije za določene programe, saj jih želite izključiti iz pregleda, ki ga opravi požarni zid.

Dodaj – odpre okno, v katerem lahko izberete program, ki ga želite dodati na seznam programov, ki so izključeni iz

zaznavanja sprememb. Izbirate lahko s seznama aplikacij, ki se izvajajo, z odprto komunikacijo z omrežjem, za katere obstaja pravilo požarnega zidu, ali dodate posameni program.

Uredi – odpre okno, v katerem lahko spremenite lokacijo programov s seznama, ki so izključeni iz zaznavanja sprememb. Izbirate lahko s seznama aplikacij, ki se izvajajo, z odprto komunikacijo z omrežjem, za katere obstaja pravilo požarnega zidu, ali ročno spremenite lokacijo.

Odstrani – odstrani vnose s seznama programov, ki so izključeni iz zaznavanja sprememb.

Zaščita pred napadi iz omrežja (IDS)

Funkcija zaščite pred napadi iz omrežja (IDS) izboljša zaznavanje napadov na znane ranljivosti. Več o zaščiti pred napadi iz omrežja lahko preberete v slovarčku. Če želite konfigurirati zaščito pred napadi iz omrežja, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Zaščita pred napadi iz omrežja**.

Omogoči zaščito pred napadi iz omrežja (IDS) – analizira vsebino omrežnega prometa in ščiti pred napadi iz omrežja. Ves promet, ki bi lahko bil škodljiv, se blokira.

Omogoči zaščito pred omrežjem robotskih računalnikov – zazna in blokira komunikacijo z zlonamernimi strežniki za ukaze in nadzor na podlagi značilnih vzorcev, ko je računalnik okužen in robotski računalnik poskuša komunicirati. Več o zaščiti pred preprečevanje napadov iz omrežja lahko preberete v slovarčku.

Pravila IDS – Ta možnost omogoča, da konfigurirate napredne možnosti filtriranja in zaznate več vrst napadov in izkoriščanj, ki lahko škodujejo vašemu računalniku.

> **Ilustrirana navodila**
> Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:
> - Izključitev naslova IP iz IDS v izdelku ESET Internet Security

Vsi pomembni dogodki, ki jih zazna zaščita omrežja, so zabeleženi v dnevniški datoteki. Za več informacij glejte dnevnik zaščite omrežja.

IDS pravila

V nekaterih okoliščinah lahko storitev zaznavanja vdorov (IDS) kot morebiten napad zazna komunikacijo med usmerjevalniki ali drugimi notranjimi omrežnimi napravami. Če želite zaobiti IDS, lahko na primer dodate znane varne naslove na območje »Naslovi, izključeni iz IDS«.

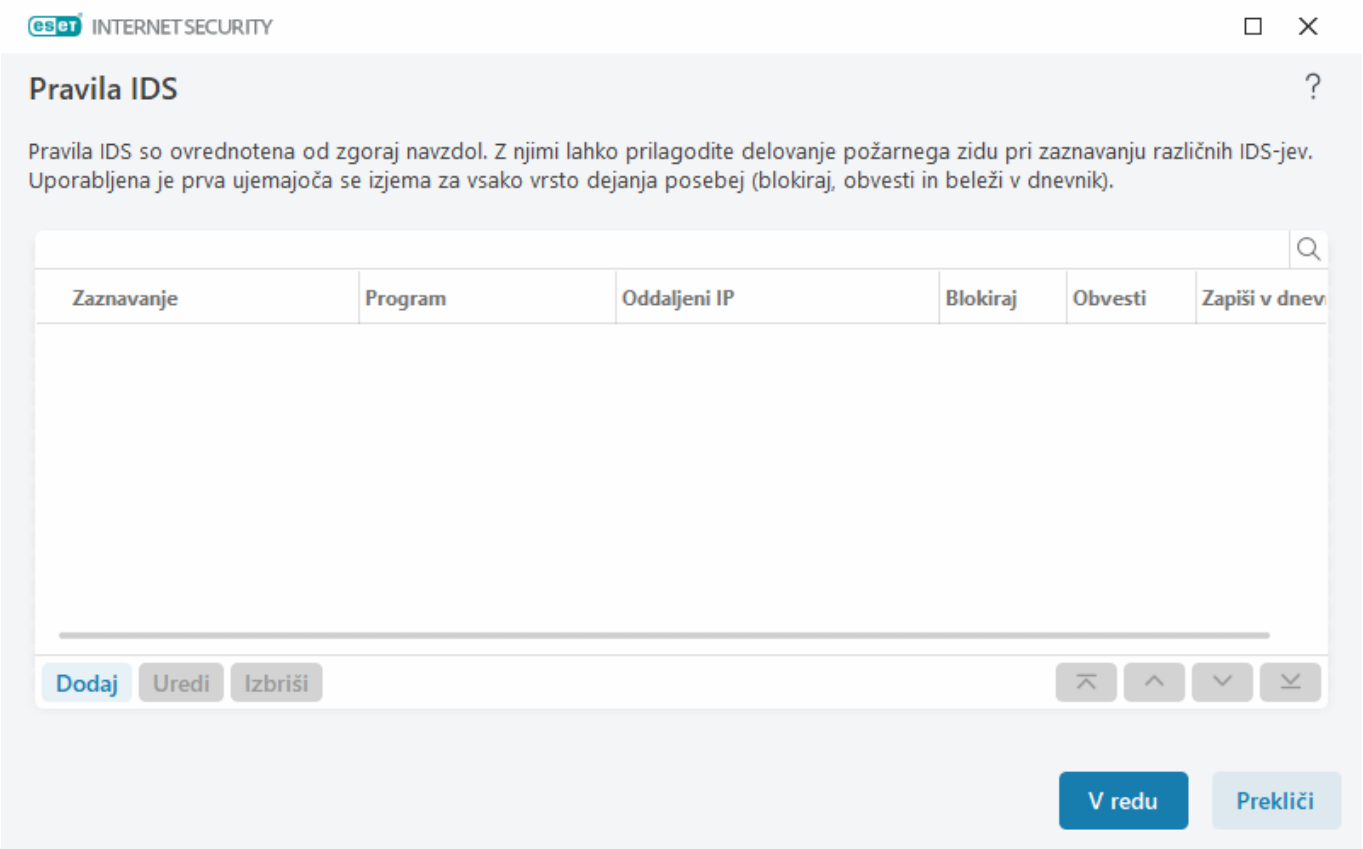
> **Ilustrirana navodila**
> Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:
> - Izključitev naslova IP iz IDS v izdelku ESET Internet Security

Upravljanje pravil IDS

- **Dodaj** – kliknite, če želite ustvariti novo pravilo IDS.
- **Uredi** – kliknite, če želite urediti obstoječo pravilo IDS.

- **Odstrani** – izberite in kliknite, če želite odstraniti obstoječe pravilo s seznama pravil IDS.

• **Vrh/gor/dol/dno** – omogoča prilagajanje ravni prednosti pravil (izjeme so ovrednotene od zgoraj navzdol).



Urejevalnik pravil

Zaznani element – vrsta zaznanega elementa.

Ime grožnje – določite lahko ime grožnje za nekatera od razpoložljivih zaznav.

Program – izberite pot do datoteke izvzetega programa tako, da kliknete ... (npr. *C:\Program Files\Firefox\Firefox.exe*). NE vnesite imena programa.

Oddaljen naslov IP – seznam oddaljenih naslovov IPv4 ali IPv6/obsegov/podomrežij. Več naslovov je treba ločiti z vejico.

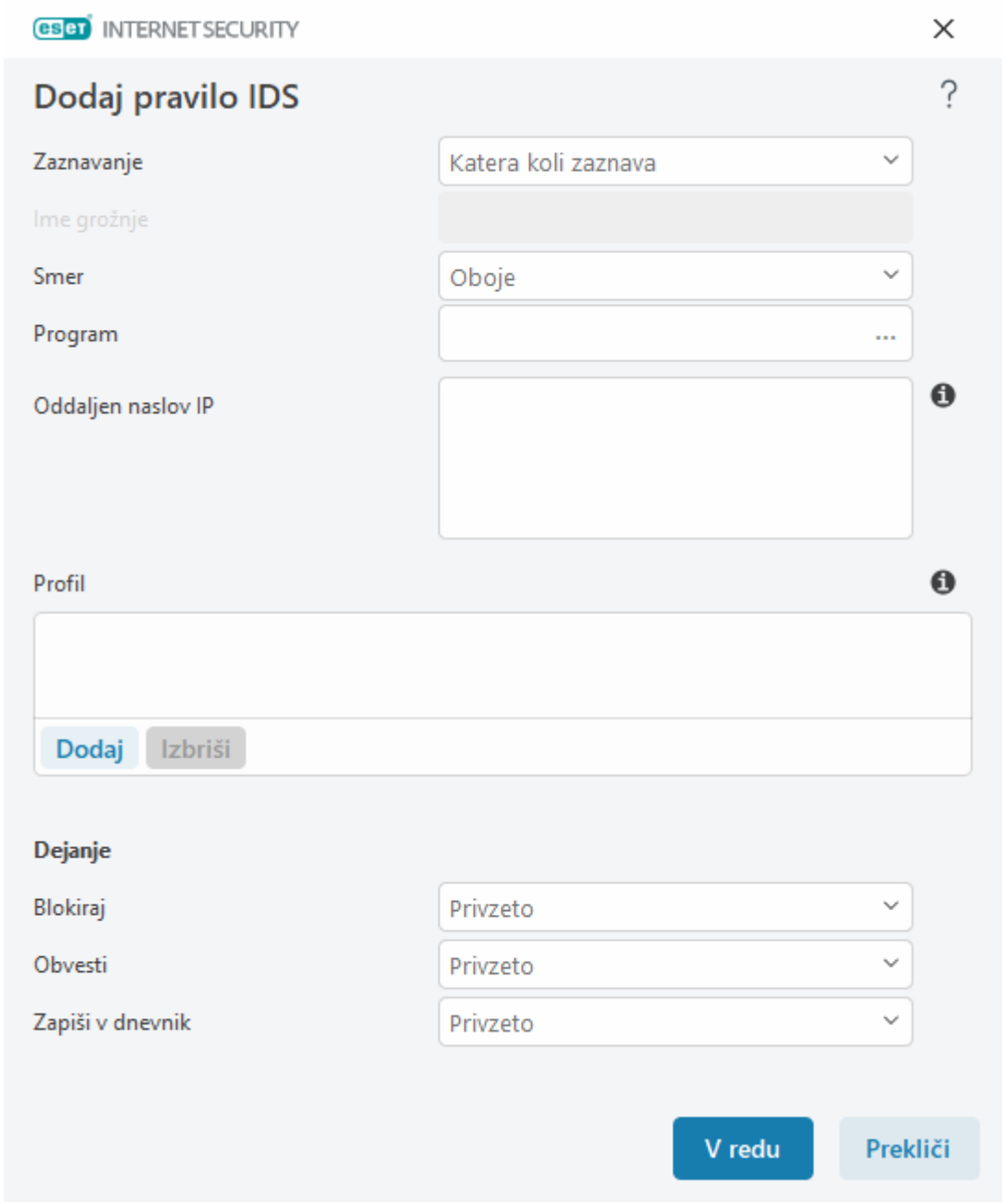
Profil – izberete lahko profil omrežnih povezav, za katerega bo veljalo to pravilo.

Dejanje

Blokiraj – vsak sistemski proces ima svoje privzeto delovanje in dodeljeno dejanje (blokiraj ali dovoli). Če želite preglasiti privzeto delovanje za ESET Internet Security, lahko na spustnem meniju izberete, da ga želite blokirati ali dovoliti.

Obvesti – izberite Da, če želite, da vam računalnik prikaže obvestila na namizju. Izberite Ne, če obvestil na namizju ne želite. Razpoložljive vrednosti so Privzeto/Da/Ne.

Zapiši v dnevnik – izberite **Da**, če želite, da se dogodki zapišejo v dnevniške datoteke programa. Izberite **Ne**, če zapisovanja dogodkov ne želite. Razpoložljive vrednosti so **Privzeto**/**Da**/**Ne**.



Če želite, da se prikaže obvestilo in v dnevniku ustvari zapis, kadar koli pride do dogodka:
1.Kliknite **Dodaj** za dodajanje novega pravila IDS.
2.Izberite posamezni zaznani element v spustnem meniju **Zaznani element**.
3.Izberite pot do programa tako, da kliknete možnost **...**, za katero želite uporabiti to obvestilo.
4.V spustnem meniju **Blokiraj** pustite vrednost **Privzeto**. S tem se podeduje privzeto dejanje, ki ga uporabi ESET Internet Security.
5.V spustnih menijih **Obvesti** in **Zapiši v dnevnik** nastavite vrednost **Da**.
6.Kliknite **V redu**, da se to obvestilo shrani.

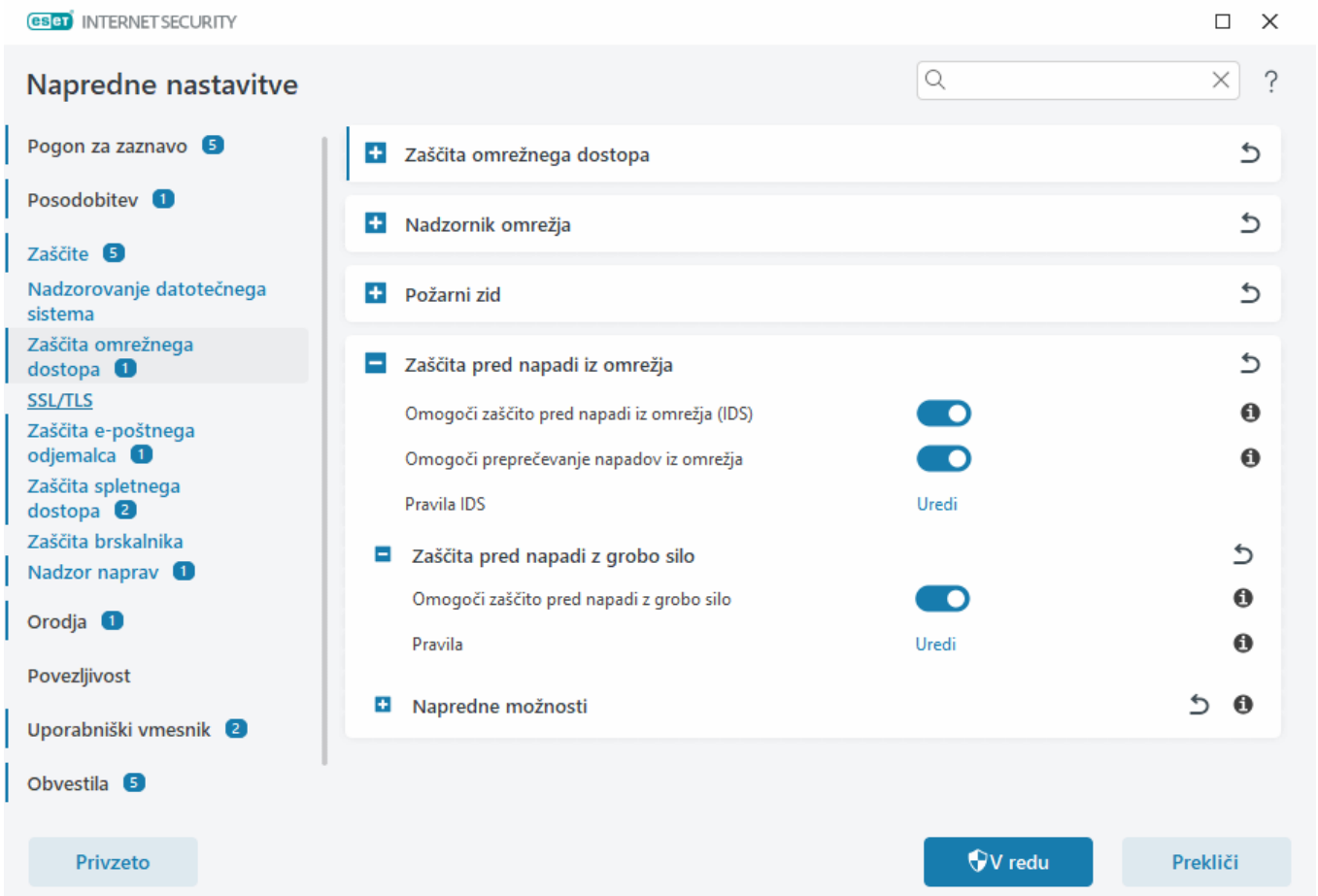
Če želite, da se prenehajo prikazovati obvestila za posamezno vrsto **zaznanega elementa**, ki po vašem mnenju ne predstavlja grožnje:
1.Kliknite **Dodaj** za dodajanje novega pravila IDS.
2.Izberite posamezni zaznani element s spustnega menija **Zaznani element**, npr. **Seja SMB brez varnostnih razširitev** ali **Napad na pregled vrat TCP**.
3.V spustnem meniju za smer izberite **Dohodni** za primer, da gre za dohodno komunikacijo.
4.V spustnem meniju **Obvesti** nastavite vrednost **Ne**.
5.V spustnem meniju **Zapiši v dnevnik** nastavite vrednost **Da**.
6.Polje **Program** pustite prazno.
7.Le komunikacija ne izvira z določenega naslova IP, pustite polje **Oddaljeni naslovi IP** prazno.
8.Kliknite **V redu**, da se to obvestilo shrani.

Zaščita pred napadi z grobo silo

Zaščita pred napadi z grobo silo blokira napade z ugibanjem gesla za storitve RDP in SMB. Napad z grobo silo je način odkrivanja ciljanega gesla s sistematičnim preizkušanjem vseh kombinacij črk, številk in simbolov. Če želite konfigurirati zaščito pred napadi z grobo silo, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Zaščita pred napadi iz omrežja** > **Zaščita pred napadi z grobo silo**.

Omogočanje zaščite pred napadi z grobo silo – ESET Internet Security pregleda vsebino omrežnega prometa in blokira poskuse napadov za ugibanje gesla.

Pravila – omogoča ustvarjanje, urejanje in ogled pravil za dohodne in odhodne omrežne povezave. Za več informacij glejte poglavje Pravila.



Pravila

Pravila za zaščito pred napadi z grobo silo omogočajo ustvarjanje, urejanje in ogled pravil za dohodne in odhodne omrežne povezave. Vnaprej določenih pravil ni mogoče urejati ali izbrisati.

Upravljanje varnostnih pravil za zaščito pred napadi z grobo silo

Dodaj – ustvari novo pravilo.

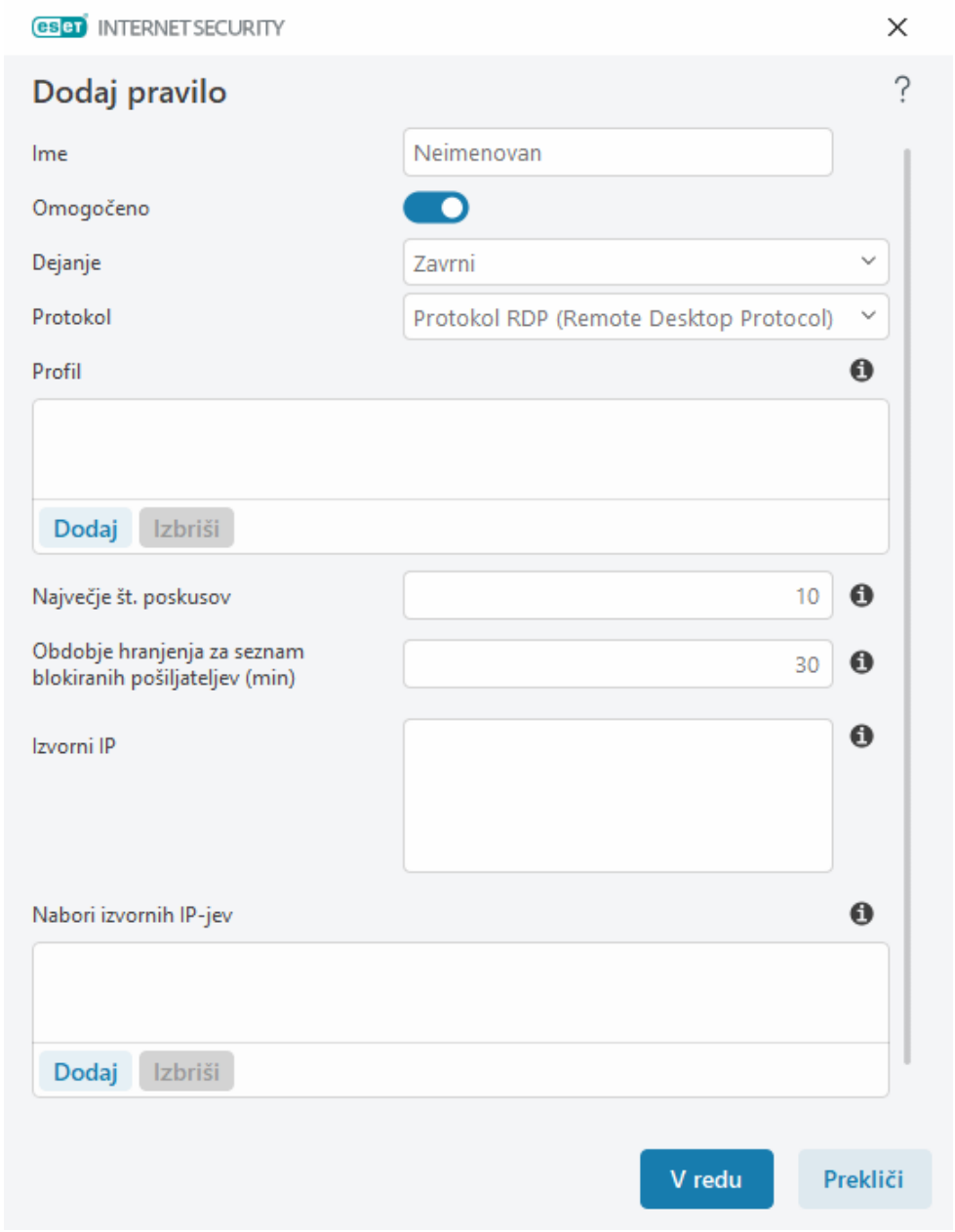
Uredi – uredi obstoječe pravilo.

Izbriši – odstrani obstoječe pravilo s seznama pravil.

 **Vrh/gor/dol/dno** – prilagodite raven prednosti pravil.

> Če želite zagotoviti najboljšo možno zaščito, se uporabi pravilo blokiranja z najnižjo vrednostjo za **Največje št. poskusov**, tudi če je pravilo postavljeno nižje na seznamu Pravil, ko se več pravil za blokiranje ujema s pogoji zaznavanja.

Urejevalnik pravil



Ime – ime pravila.

Omogočeno – onemogočite gumb za preklop, če želite pravilo ohraniti na seznamu, a ga ne želite uporabiti.

Dejanje – izberite, ali želite **zavrniti** ali **dovoliti** povezavo, če so nastavitve pravila izpolnjene.

Protokol – pokaže protokol komunikacije, ki ga bo to pravilo pregledalo.

Profil – za določene profile se lahko nastavijo in uporabijo pravila po meri.

Največje št. poskusov – Največje število dovoljenih poskusov ponovitve napada, dokler naslov IP ni blokiran in dodan na seznam blokiranih pošiljateljev.

Obdobje hranjenja za seznam blokiranih pošiljateljev (min) – določa čas, ko hranjenje naslova na seznamu blokiranih pošiljateljev poteče.

Izvorni IP – seznam naslovov IP, obsegov ali podomrežij. Več naslovov je treba ločiti z vejico.

Nabori izvornih IP-jev – nabor naslovov IP, ki ste jih že določili v naborih IP-jev.

Napredne možnosti

V razdelku Napredne nastavitve > **Zaščite** > **Zaščita omrežnega dostopa** > **Zaščita pred napadi iz omrežja** > **Napredne možnosti** lahko omogočite ali onemogočite zaznavanje več vrst napadov in izkoriščanj, ki lahko škodujejo vašemu računalniku.

V nekaterih primerih ne boste prejeli obvestila o grožnji o blokirani komunikaciji. Navodila za ogled vseh blokiranih komunikacij v dnevniku požarnega zidu najdete v razdelku Pisanje dnevnika in ustvarjanje pravil ali izjem iz dnevnika.

Razpoložljivost posameznih možnosti v tem oknu je odvisna od vrste ali različice vašega izdelka ESET, modula požarnega zidu in različice vašega operacijskega sistema.

Zaznavanje vdorov

Zaznavanje vdora spremlja omrežno komunikacijo naprave in išče v njej zlonamerno dejavnost.

- **Protokol SMB** – zazna in blokira različne varnostne težave v protokolu SMB.
- **Protokol RPC** – zazna in blokira različne splošne ranljivosti in nevarnosti v sistemu klica oddaljene procedure, zasnovanega za DCE (Distributed Computing Environment).
- **Protokol RDP** – zazna in blokira različne splošne ranljivosti in nevarnosti v protokolu RDP (glejte zgoraj).
- **Zaznavanje napadov zastrupljanja ARP**-ja – zaznavanje napada zastrupljanja ARP-ja, ki ga sprožijo napadi vmesnega člena, ali zaznavanje iskanja omrežnega preklopnika. Omrežni program ali naprava uporabljata ARP (Address Resolution Protocol) za določanje ethernetnega naslova.
- Zaznavanje napadov na pregled vrat **TCP/UDP** – zazna napade programske opreme za pregledovanje vrat – program, ki je zasnovan tako, da preverja, ali ima gostitelj odprta vrata, in sicer tako, da pošilja zahteve odjemalca na različne naslove vrat, da bi našel aktivna vrata in izkoristil ranljivost storitve. Več o tej vrsti napadov preberite v slovarju izrazov.
- **Blokiraj nevaren naslov po zaznanem napadu** – naslovi IP, ki so bili zaznani kot vir napadov, so dodani na seznam blokiranih pošiljateljev in povezava je nekaj časa onemogočena. Določite lahko **obdobje hranjenja za seznam blokiranih pošiljateljev**, ki določa čas, kako dolgo po zaznanem napadu bo naslov blokiran.
- **Prikaži obvestilo, ko je zaznan napad** – vklopi obvestilo v območju za obvestila sistema Windows v spodnjem desnem kotu zaslona.
- **Prikaži obvestila tudi za dohodne napade varnostnih lukenj** – opozori, če so zaznani napadi varnostnih lukenj ali če grožnja na ta način poskuša vstopiti v sistem.

Preverjanje paketov

Vrsta analize paketov, ki filtrira podatke, prenesene prek omrežja.

- **Dovoli dohodno povezavo s skrbniškimi omrežnimi pogoni v protokolu SMB** – skrbniški omrežni pogoni so privzeti omrežni pogoni, ki omogočajo skupno rabo particij trdega diska (*C$*, *D$*, ...) v sistemu in sistemske mape (*ADMIN$*). Če onemogočite povezavo s skrbniškimi omrežnimi pogoni, zmanjšate številna varnostna tveganja. Črv Conficker na primer izvaja napade s slovarjem, da se poveže s skrbniškimi omrežnimi pogoni.

- **Zavrni stare (nepodprte) dialekte SMB** – zavrnite seje SMB s starim dialektom SMB, ki ga IDS ne podpira. Moderni operacijski sistemi Windows podpirajo stare dialekte SMB zaradi vzvratne združljivosti s starejšimi operacijskimi sistemi, kot je Windows 95. Napadalec lahko v seji SMB uporabi star dialekt, da se izogne preverjanju prometa. Zavrnite stare dialekte SMB, če vam ni treba omogočiti skupne rabe datotek (ali uporabiti komunikacije SMB) z računalnikom s starejšo različico sistema Windows.

- **Zavrni seje SMB brez razširjene varnosti** – razširjeno varnost lahko uporabite med pogajanji o seji SMB, da bi zagotovili varnejši mehanizem preverjanja pristnosti od protokola preverjanja pristnosti izziv–odgovor za LAN Manager (LM). Shema LM se smatra za šibko in je ni priporočljivo uporabljati.

- **Zavrni odpiranje izvedljivih datotek v protokolu SMB v strežniku, ki je zunaj zaupanja vrednega območja** – prekine povezavo, ko poskušate odpreti izvedljivo datoteko (.exe, .dll ...) iz mape v skupni rabi v strežniku, ki ni v zaupanja vrednem območju požarnega zida. Upoštevajte, da je kopiranje izvedljivih datotek iz zaupanja vrednih virov lahko legitimno. Kopiranje izvedljivih datotek iz zaupanja vrednih virov je lahko zakonito, vendar pa to zaznavanje poskuša zmanjšati tveganje neželenega odpiranja datotek v zlonamernih strežnikih (če datoteko na primer odprete tako, da kliknete hiperpovezavo do zlonamerne izvedljive datoteke v skupni rabi).

- **Zavrni preverjanje pristnosti NTLM** v protokolu **SMB za vzpostavljanje povezave s strežnikom v zaupanja vrednem območju ali zunaj njega** – protokoli, ki uporabljajo sheme preverjanja pristnosti NTLM (obe različici), so predmet napada na posredovanje poverilnic (znanega kot napad na rele SMB v primeru protokola SMB). Zavrnitev preverjanja pristnosti NTLM v strežniku zunaj zaupanja vrednega območja zmanjša tveganje posredovanja poverilnic zlonamernega strežnika zunaj zaupanja vrednega območja. Preverjanje pristnosti NTLM lahko zavrnete tudi v strežnikih v zaupanja vrednem območju.

- **Dovoli komunikacijo s storitvijo upravitelja varnostnih računov** – če želite več informacij o tej storitvi, glejte [MS–SAMR].

- **Dovoli komunikacijo s storitvijo lokalnega varnostnega urada** – če želite več informacij o tej storitvi, glejte [MS-LSAD] in [MS-LSAT].

- **Dovoli komunikacijo s storitvijo oddaljenega registra** – če želite več informacij o tej storitvi, glejte [MS–RRP].

- **Dovoli komunikacijo s storitvijo upravitelja varnostnih računov** – če želite več informacij o tej storitvi, glejte [MS–SCMR].

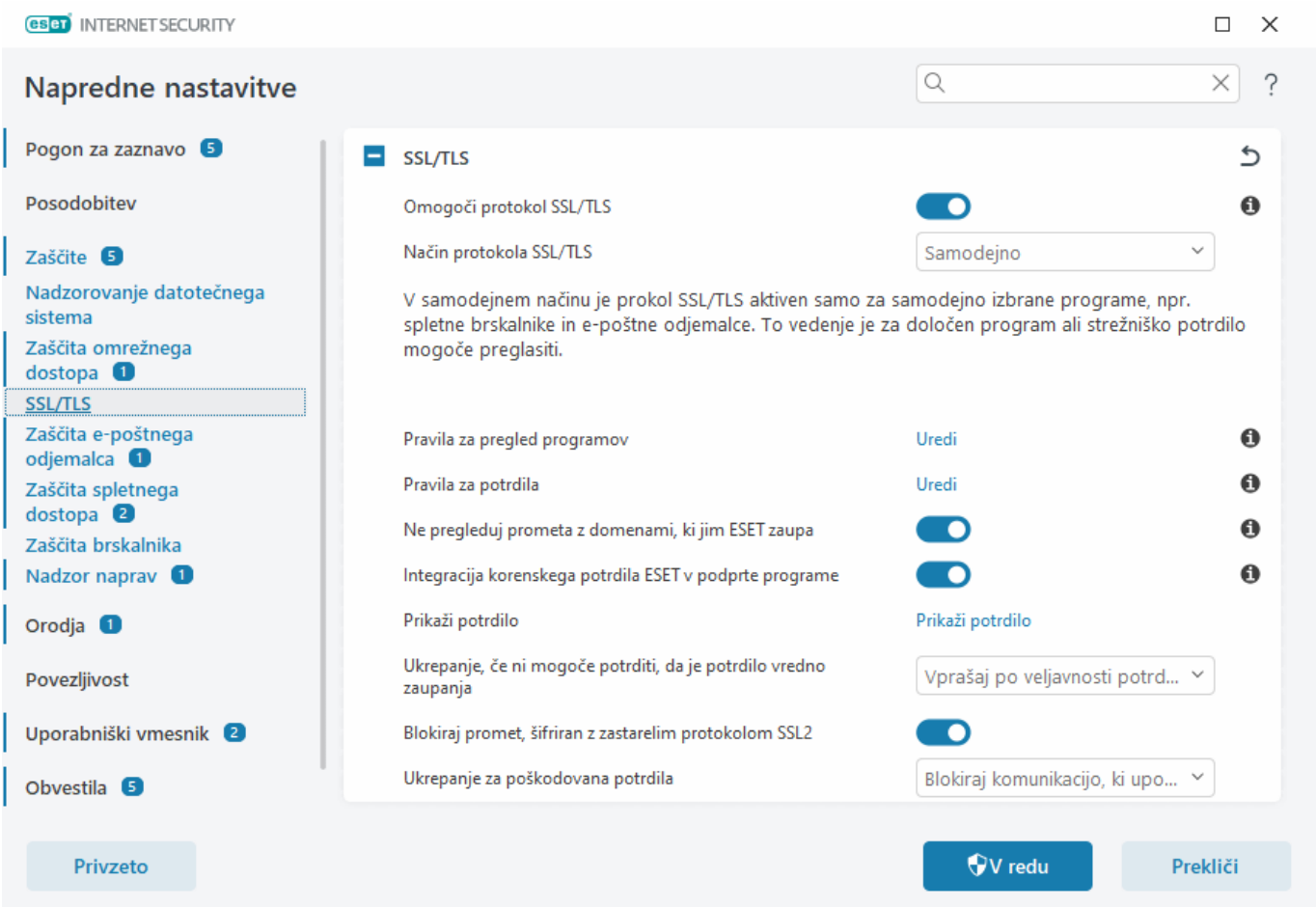
- **Dovoli komunikacijo s strežniško storitvijo** – če želite več informacij o tej storitvi, glejte [MS–SRVS].

- **Dovoli komunikacijo z drugimi storitvami** – druge storitve MSRPC. MSRPC je Microsoftova izvedba mehanizma DCE RPC. Poleg tega lahko MSRPC uporablja tudi poimenovane cevi, ki jih vnese v protokol SMB (skupna raba omrežnih datotek) za prenos (prenos ncacn_np). Storitve MSRPC zagotavljajo vmesnike za oddaljeni dostop in oddaljeno upravljanje sistemov Windows. V sistemu Windows MSRPC je bilo odkritih in izkoriščenih več varnostnih ranljivosti (črv Conficker, črv Sasser ...). Če onemogočite komunikacijo s storitvami MSRPC, ki jih ne potrebujete, zmanjšate številna varnostna tveganja (na primer izvajanje oddaljene kode ali napadi zavrnitve storitve).

SSL/TLS

ESET Internet Security lahko preveri komunikacijske grožnje, ki uporabljajo protokol SSL. Za komunikacije, zaščitene s protokolom SSL, lahko uporabite različne načine filtriranja na primer zaupanja vredna potrdila, neznana potrdila ali potrdila, ki so izključena iz preverjanja komunikacije, zaščitene s protokolom SSL. Če želite

urediti nastavitve protokola SSL/TLS, odprite razdelek Napredne nastavitve > **Zaščite** > **SSL/TLS**.



Omogoči SSL/TLS – če je možnost onemogočena, program ESET Internet Security ne bo pregledal komunikacije prek protokola SSL/TLS.

Način SSL/TLS je na voljo v naslednjih možnostih:

Način filtriranja	Opis
Samodejno	Privzeti način, ki pregleda le primerne programe, kot so spletni brskalniki in e-poštni odjemalci. Preglasite ga lahko tako, da izberete programe, kjer se izvaja pregledovanje komunikacije.
Interaktivno	Če vnesete novo spletno mesto, zaščiteno s protokolom SSL (z neznanim potrdilom), se prikaže pogovorno okno, v katerem lahko izberete dejanje. Ta način omogoča, da ustvarite seznam potrdil SSL/programov, overjenih s potrdilom SSL, ki bodo izključeni iz pregledovanja.
Na podlagi pravilnika	Če želite pregledati vse komunikacije, zaščitene s protokolom SSL, razen komunikacij, zaščitenih s potrdili, ki so izključena iz preverjanja, izberite to možnost. Če je vzpostavljena nova komunikacija z neznanim, podpisanim potrdilom, o tem ne boste obveščeni, komunikacija pa bo filtrirana samodejno. Ko dostopate do strežnika s potrdilom brez zaupanja, ki je označeno kot zaupanja vredno (je na seznamu zaupanja vrednih potrdil), je komunikacija s strežnikom dovoljena, vsebina komunikacijskega kanala pa je filtrirana.

Pravila za pregled programov – omogoča prilagajanje delovanja programa ESET Internet Security za določene programe.

Pravila za potrdila – omogoča prilagajanje delovanja programa ESET Internet Security za določena potrdila SSL.

Ne pregleduj prometa z domenami, ki jim ESET zaupa – ko je možnost omogočena, bo komunikacija z zaupanja vrednim domenam izključena iz pregleda. Vgrajen seznam varnih pošiljateljev, ki ga upravlja ESET, določa zanesljivost domene.

Integracija korenskega potrdila ESET v podprte programe – komunikacija SSL v odjemalcih brskalnikov ali e-pošte bo delovala pravilno le, če je korensko potrdilo za ESET dodano na seznam znanih korenskih potrdil (založnikov). Ko je izbrana ta možnost, program ESET Internet Security potrdilo ESET SSL Filter CA samodejno doda znanim brskalnikom (na primer brskalniku Opera). Pri brskalnikih, ki uporabljajo sistemsko shrambo potrdil, je potrdilo dodano samodejno. Brskalnik Firefox je na primer samodejno konfiguriran tako, da zaupa korenskim potrdilom v sistemski shrambi potrdil.

Če želite potrdilo uporabiti v nepodprtih brskalnikih, kliknite **Ogled potrdila** > **Podrobnosti** > **Kopiraj v datoteko** ter ga nato ročno uvozite v brskalnik.

Ukrepanje, če ni mogoče potrditi, da je potrdilo vredno zaupanja – v nekaterih primerih potrdila spletnega mesta ni mogoče preveriti s shrambo zaupanja vrednih overiteljev korenskih potrdil (TRCA) (na primer poteklo potrdilo, potrdilo, ki ni vredno zaupanja, potrdilo, ki ni veljavno za določeno domeno, ali podpis, ki ga je mogoče razčleniti, vendar potrdila ne podpiše pravilno). Zakonita spletna mesta vedno uporabljajo zaupanja vredna potrdila. Če ga ne zagotavljajo, bi to lahko pomenilo, da napadalec dešifrira vašo komunikacijo ali pa ima spletno mesto tehnične težave.

Če je izbrana možnost **Vprašaj po veljavnosti potrdila** (privzeto izbrana), boste pozvani, da izberete dejanje, ko je vzpostavljena šifrirana komunikacija. Prikazano bo pogovorno okno za izbor dejanja, v katerem lahko potrdilo označite kot zaupanja vredno ali izključeno. Če potrdila ni na seznamu zaupanja vrednih overiteljev korenskih potrdil, je okno rdeče. Če je potrdilo na seznamu, bo okno zeleno.

Izberete lahko možnost **Blokiraj komunikacijo, ki uporablja potrdilo**, s katero boste vedno prekinili šifrirano komunikacijo s spletnim mestom, ki uporablja potrdilo, ki ni vredno zaupanja.

Blokiraj promet, šifriran z zastarelim protokolom SSL2 – komunikacija, ki uporablja starejšo različico protokola SSL, bo samodejno blokirana.

Ukrepanje za poškodovana potrdila – poškodovano potrdilo pomeni, da potrdilo uporablja obliko zapisa, ki je program ESET Internet Security ni prepoznal, ali pa je že bilo poškodovano ob prejemu (na primer prepisan z naključnimi podatki). V tem primeru priporočamo, da možnost **Blokiraj komunikacijo, ki uporablja potrdilo** ostane izbrana. Če je izbrana možnost **Vprašaj po veljavnosti potrdila**, je uporabnik pozvan, da izbere dejanje, ki se izvede, ko je vzpostavljena šifrirana komunikacija.

> **Ilustrirani primeri**
>
> Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:
> - Obvestila o potrdilih v izdelkih ESET za domačo uporabo za sistem Windows
> - »Šifriran omrežni promet: potrdilo brez zaupanja« ob obisku spletnih strani se prikaže obvestilo

Pravila za pregled programov

Pravila za pregled programov lahko uporabite, da prilagodite delovanje programa ESET Internet Security za določene programe in shranite izbrana dejanja, ko je **način SSL/TLS** v **interaktivnem načinu**. Seznam si je mogoče ogledati in ga urediti v razdelku Napredne nastavitve > **Zaščite** > **SSL/TLS** > **Pravila za pregled programov** > **Uredi**.

Okno **Pravila za pregled programov** vsebuje naslednje:

Stolpci

Program – izberite izvedljivo datoteko iz drevesa imenika, kliknite možnost **...** ali ročno vnesite pot.

Dejanje pregleda – izberite **Preglej** ali **Prezri**, da pregledate ali prezrete komunikacijo. Izberite **Samodejno** za pregled v samodejnem načinu in potrditev v interaktivnem načinu. Izberite **Vprašaj**, da lahko uporabnik vedno izbere, kaj želi narediti.

Elementi kontrolnika

Dodaj – dodajte program za filtriranje.

Uredi – izberite aplikacijo, ki jo želite konfigurirati, in kliknite **Uredi**.

Odstrani – izberite aplikacijo, ki jo želite izbrisati, in kliknite **Odstrani**.

Uvoz/izvoz – uvozite aplikacije iz datoteke ali shranite trenutni seznam aplikacij v datoteko.

V redu/**Prekliči** – kliknite **V redu**, če želite shraniti spremembe, ali **Prekliči**, če želite zapreti okno brez shranjevanja.

Pravila za potrdila

Pravila za potrdila se lahko uporabijo za prilagajanje delovanja programa ESET Internet Security za določena potrdila SSL in shranjevanje izbranih dejanj, ko je **način SSL/TLS** v **interaktivnem načinu**. Seznam si lahko ogledate in ga uredite v razdelku Napredne nastavitve > **Zaščite** > **SSL/TLS** > **Pravila za potrdila** > **Uredite**.

Okno **Pravila za potrdila** vsebuje naslednje:

Stolpci

Ime – ime potrdila.

Izdajatelj potrdila – ime avtorja potrdila.

Zadeva potrdila – polje za zadevo označuje entiteto, povezano z javnim ključem, ki je shranjen v polju za javni ključ.

Dostop – izberite **Dovoli** ali **Blokiraj** kot **Dejanje dostopa** in dovolite/blokirajte komunikacijo, ki je zaščitena s tem potrdilom, ne glede na njegovo zanesljivost. Izberite **Samodejno**, da dovolite zaupanja vredna potrdila in preverite tista, ki niso vredna zaupanja. Izberite **Vprašaj**, da lahko uporabnik vedno izbere, kaj želi narediti.

Pregled – Izberite **Preglej** ali **Prezri** kot **Dejanje pregleda** in preglejte ali prezrite komunikacijo, ki je zaščitena s tem potrdilom. Izberite **Samodejno** za pregled v samodejnem načinu in potrditev v interaktivnem načinu. Izberite **Vprašaj**, da lahko uporabnik vedno izbere, kaj želi narediti.

Elementi kontrolnika

Dodaj – dodajte novo potrdilo in prilagodite njegove nastavitve, povezane z dostopom in možnostjo pregleda.

Uredi – izberite potrdilo, ki ga želite konfigurirati, in kliknite **Uredi**.

Izbriši – izberite potrdilo, ki ga želite izbrisati, in kliknite **Odstrani**.

V redu/Prekliči – kliknite **V redu**, če želite shraniti spremembe, ali **Prekliči**, če želite zapreti okno brez shranjevanja.

Šifriran omrežni promet

Če je sistem konfiguriran tako, da uporablja pregledovanje s protokolom SSL/TLS, se v dveh primerih prikaže pogovorno okno, ki vas poziva, da izberete dejanje:

Prvi primer: če spletno mesto uporablja neveljavno potrdilo ali potrdilo, ki ga ni mogoče preveriti, program ESET Internet Security pa je konfiguriran tako, da v takem primeru pozove uporabnika (privzeto je odgovor »da« za potrdila, ki jih ni mogoče preveriti, in »ne« za neveljavna potrdila), vas bo pogovorno okno pozvalo, ali želite **dovoliti** ali **blokirati** povezavo. Če potrdila ni na lokaciji Trusted Root Certification Authorities store (TRCA), se šteje, da ni zaupanja vredno.

Drugi primer: če je način **SSL/TLS** nastavljen na **interaktivni način**, vas bo pogovorno okno za vsako spletno mesto pozvalo, ali želite **pregledati** ali **prezreti** promet. Nekateri programi potrjujejo, da prometa SSL nihče ne spreminja ali pregleduje. V teh primerih mora program ESET Internet Security ta promet **prezreti**, da program lahko deluje.

> **Ilustrirani primeri**
>
> Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:
> - Obvestila o potrdilih v izdelkih ESET za domačo uporabo za sistem Windows
> - »Šifriran omrežni promet: potrdilo brez zaupanja« ob obisku spletnih strani se prikaže obvestilo

V obeh primerih lahko uporabnik izbere možnost, da si program zapomni izbrano dejanje. Shranjena dejanja so shranjena v pravilih za potrdila.

Zaščita e-poštnega odjemalca

Če želite konfigurirati zaščito e-poštnega odjemalca, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita e-poštnega odjemalca** in izberite med naslednjimi možnostmi konfiguracije:

- Zaščita prenosa e-pošte
- Zaščita e-poštnega nabiralnika
- Upravljanje seznamov naslovov
- ThreatSense

Zaščita prenosa e-pošte

Protokola IMAP(S) in POP3(S) sta najbolj razširjena protokola, ki se uporabljata za sprejemanje e-poštne komunikacije v programu e-poštnega odjemalca. Standard za sprejemanje e-pošte IMAP je drug internetni protokol za sprejemanje e-pošte. Protokol IMAP ima nekaj prednosti pred protokolom POP3: z istim e-poštnim

nabiralnikom se lahko na primer poveže več e-poštnih odjemalcev, ki nato vzdržujejo informacije o stanju sporočil (ali je bilo na primer sporočilo prebrano, ali je bilo nanj odgovorjeno ali pa je bilo sporočilo izbrisano). Modul zaščite, ki zagotavlja ta nadzor, se samodejno inicializira ob zagonu sistema in je potem aktiven v pomnilniku.

ESET Internet Security zagotavlja zaščito za ta protokola, ne glede na uporabljen e-poštni odjemalec in brez vnovične konfiguracije e-poštnega odjemalca. Privzeto je pregledana vsa komunikacija prek protokolov POP3 and IMAP, ne glede na privzeto številko vrat za POP3/IMAP.
Protokol MAPI ni vključen v pergled. Vendar je komunikacijo s strežnikom Microsoft Exchange mogoče pregledovati z integracijskim modulom v e-poštnih odjemalcih, kot je Microsoft Outlook.

ESET Internet Security podpira tudi preverjanje protokolov IMAPS (585, 993) in POP3S (995), ki uporabljata šifrirani kanal za prenos informacij med strežnikom in odjemalcem. ESET Internet Security preverja komunikacijo s protokoloma SSL (sloj varnih vtičnic) in TLS (varnost transportnega sloja).
Šifrirana komunikacija bo privzeto pregledana. Če si želite ogledati nastavitev pregledovalnika, odprite razdelek Napredne nastavitve > **Zaščite** > SSL/TLS.

Če želite konfigurirati zaščito prenosa e-pošte, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita e-poštnega odjemalca** > **Zaščita prenosa e-pošte**.

Omogoči zaščito prenosa e-pošte – ko je možnost omogočena, bo komunikacijo o prenosu e-pošte pregledal program ESET Internet Security.

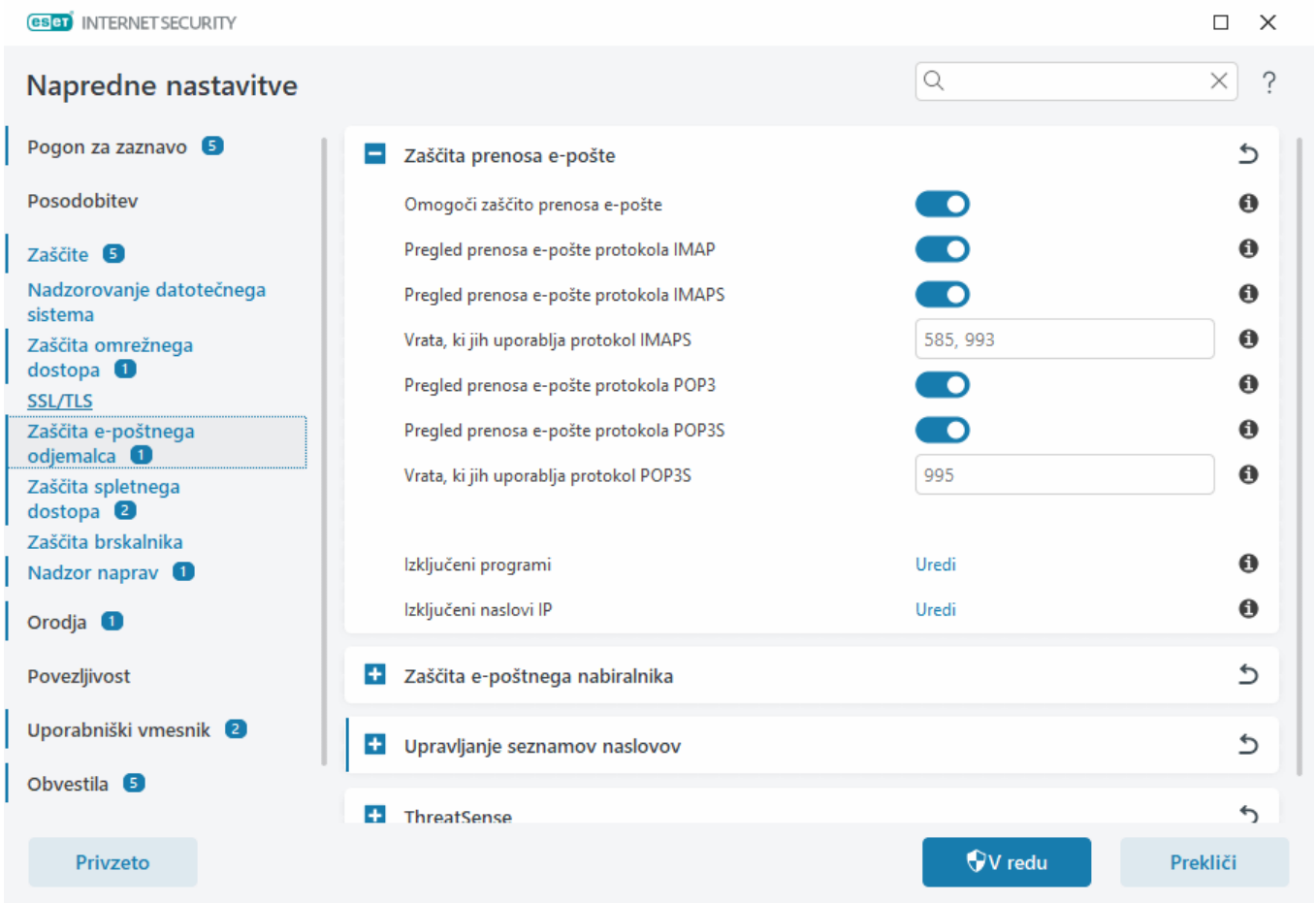
Izberete lahko, kateri protokoli prenosa naj bodo pregledani, tako, da kliknete gumb za preklop ob naslednjih možnostih (privzeto je omogočen pregled vseh protokolov):

- **Pregled prenosa e-pošte protokola IMAP**
- **Pregled prenosa e-pošte protokola IMAPS**
- **Pregled prenosa e-pošte protokola POP3**
- **Pregled prenosa e-pošte protokola POP3S**

Program ESET Internet Security bo privzeto pregledal komunikacijo IMAPS in POP3S v standardnih vratih. Če želite dodati vrata po meri za protokola IMAPS in POP3S, jih dodajte v besedilno polje zraven **vrat, ki jih uporablja protokol IMAPS** ali **vrat, ki jih uporablja protokol POP3S**. Številke več vrat morajo biti ločene z vejico.

Izključeni programi – omogoča izključitev določenih programov iz pregleda zaščite prenosa e-pošte. To je uporabno, če zaščita spletnega dostopa povzroča težave z združljivostjo.

Izključeni naslovi IP – omogoča izključitev določenih oddaljenih naslovov iz pregleda zaščite prenosa e-pošte. To je uporabno, če zaščita spletnega dostopa povzroča težave z združljivostjo.



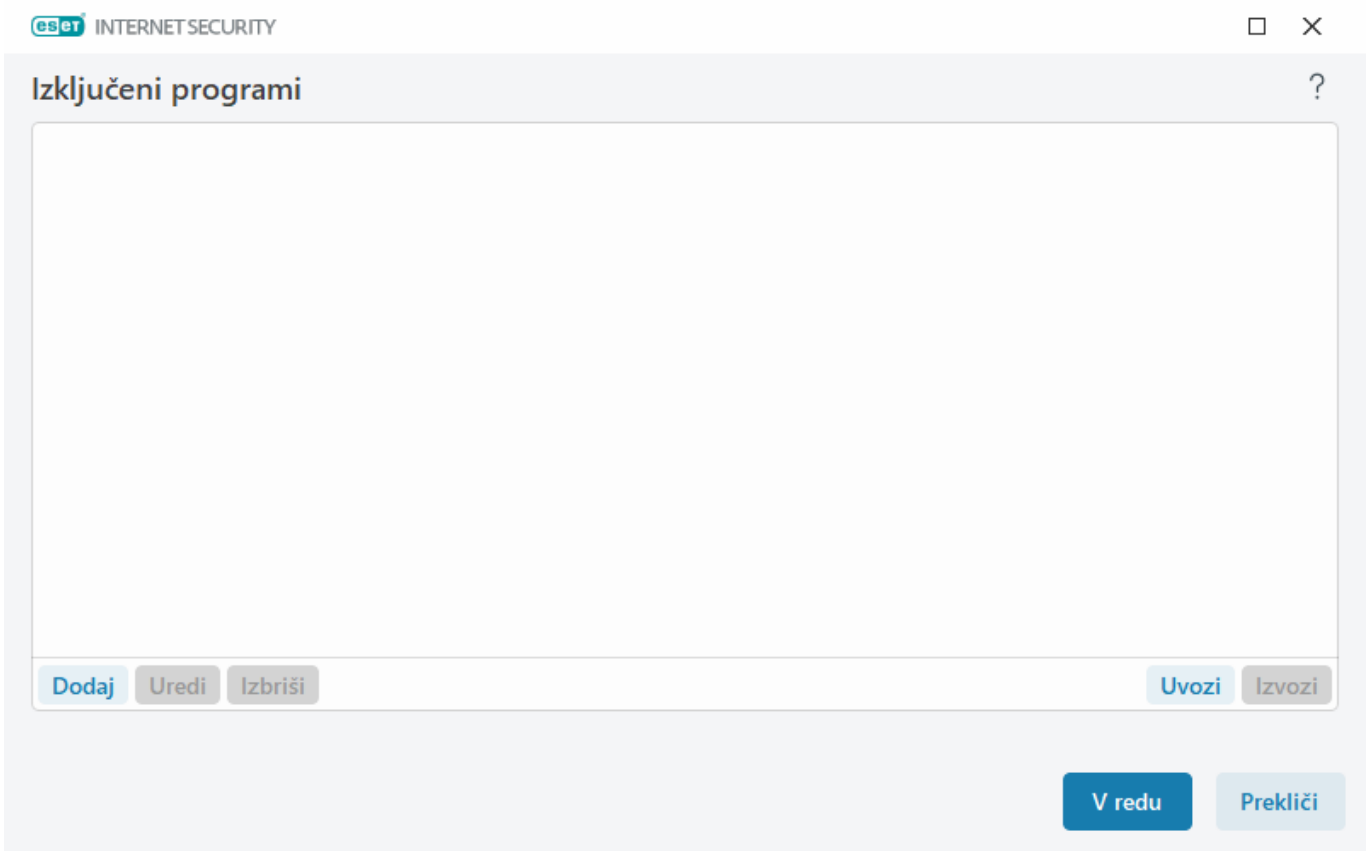
Izključeni programi

Če želite izključiti pregled komunikacije za določene programe, jih dodajte na seznam. V komunikaciji HTTP(S)/POP3(S)/IMAP(S) izbranih programov ne bo preverjeno, ali so v njej grožnje. Priporočamo, da to uporabite le za programe, ki ne delujejo pravilno pri pregledu komunikacije.

Ko kliknete možnost **Dodaj**, bodo tu samodejno na voljo programi in storitve, ki ste izvajajo. Kliknite **...** in se pomaknite v program, če želite ročno dodati izključitev.

Uredi – uredite izbrane vnose na seznamu.

Odstrani – odstranite izbrane vnose s seznama.



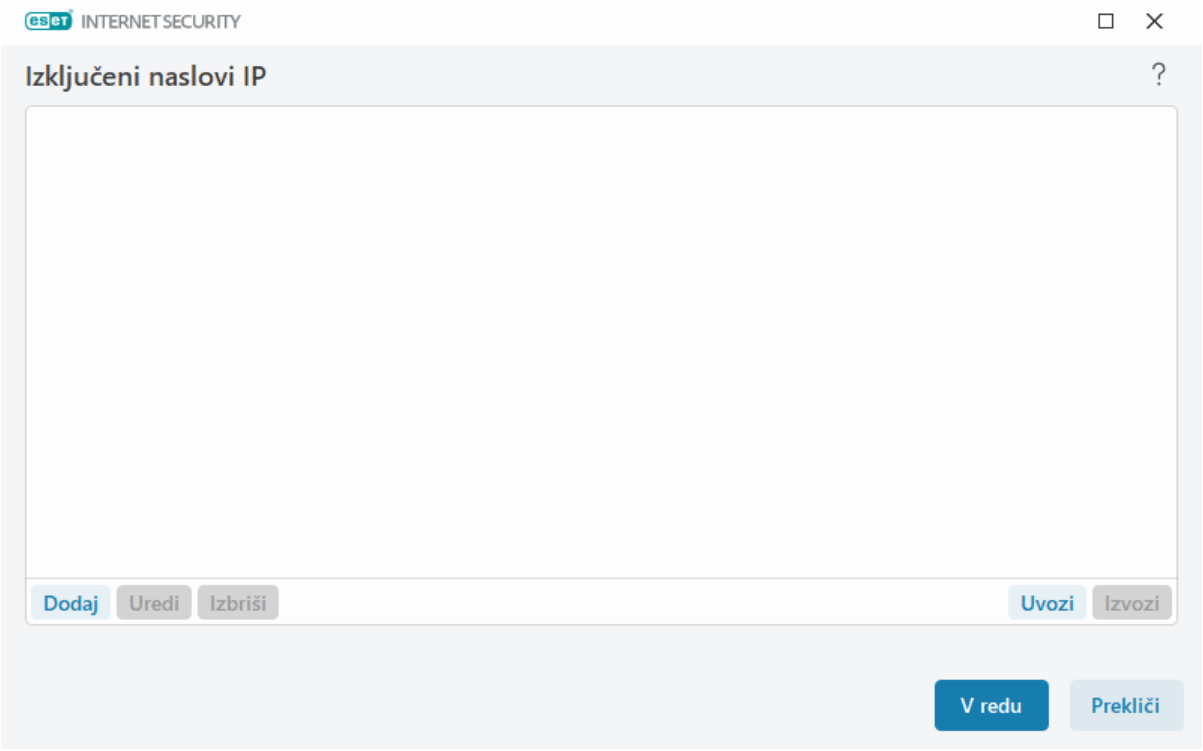
Izključeni naslovi IP

Vnosi na seznamu bodo izključeni iz pregleda. V komunikaciji HTTP(S)/POP3(S)/IMAP(S) iz izbranih naslovov in na njih ne bo preverjeno, ali so njej grožnje. Priporočamo, da to možnost uporabite le za zaupanja vredne naslove.

Kliknite **Dodaj**, če želite izključiti naslov IP/obseg naslovov/podomrežje oddaljene točke.

Kliknite možnost **Uredi**, če želite spremeniti izbrani naslov IP.

Kliknite **Izbriši**, če želite odstraniti izbrane vnose s seznama.



Primeri naslovov IP

Dodaj naslov IPv4:
Enotni naslov – doda naslov IP posameznega računalnika (na primer *192.168.0.10*).
Obseg naslovov – vnesite začetni in končni naslov IP naslova, da določite obseg IP več računalnikov (na primer *od 192.168.0.1 do 192.168.0.99*).
Podomrežje – podomrežje (skupina računalnikov) je določeno z naslovom IP in masko. 255.255.255.0 je na primer maska omrežja za podomrežje 192.168.1.0. Za izključitev celotne vrste podomrežja v *192.168.1.0/24*.
Dodaj naslov IPv6:
Enotni naslov – doda naslov IP posameznega računalnika (na primer *2001:718:1c01:16:214:22ff:fec9:ca5*).
Podomrežje – podomrežje (skupina računalnikov) je določeno z naslovom IP in masko (na primer: *2002:c0a8:6301:1::1/64*).

Zaščita e-poštnega nabiralnika

Z integracijo programa ESET Internet Security z e-poštnim nabiralnikom se poveča raven aktivne zaščite pred zlonamerno kodo v e-poštnih sporočilih.

Če želite konfigurirati zaščito e-poštnega nabiralnika, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita e-poštnega odjemalca** > **Zaščita e-poštnega nabiralnika**.

Omogoči zaščito e-pošte z vtičniki odjemalca – če je možnost onemogočena, je zaščita e-pošte z vtičniki izklopljena.

Izberite e-poštna sporočila, ki jih želite pregledati:

- **Prejeta e-pošta**
- **Poslana e-pošta**
- **Prebrana e-pošta**

- **Spremenjeno e-poštno sporočilo**

Priporočamo, da imate možnost **Omogoči zaščito e-pošte z vtičniki odjemalca** omogočeno. Tudi če integracija ni omogočena, je e-poštna komunikacija zaščitena z zaščito prenosa e-pošte (IMAP/IMAPS in POP3/POP3S).

Pregled neželene pošte

Neželena pošta predstavlja eno največjih težav v današnji elektronski komunikaciji. Predstavlja kar 30 odstotkov vse e-poštne komunikacije. Zaščita pred neželeno pošto v e-poštnem odjemalcu služi kot zaščita pred to težavo. Zaščita pred neželeno pošto v e-poštnem odjemalcu, ki združuje več e-poštnih varnostnih načel, zagotavlja vrhunsko filtriranje, s katerim očisti vaš nabiralnik. Za zaznavanje neželene pošte je pomembno načelo prepoznavanja vsiljene e-pošte na podlagi vnaprej določenih zaupanja vrednih naslovov (dovoljeno) in naslovov neželene pošte (blokirano).

Primarni način zaznavanja neželene pošte je pregledovanje lastnosti e-poštnega sporočila. Prejeta sporočila so pregledana v skladu z osnovnimi kriteriji za preprečevanje neželene pošte (definicije sporočil, statistična hevristika, algoritmi prepoznavanja in drugi enolični načini); rezultat vrednosti indeksa določa, ali je sporočilo neželeno ali želeno.

Omogočanje zaščite pred neželeno pošto v e-poštnem odjemalcu – ko je možnost omogočena, bodo prejeta sporočila pregledana kot neželena pošta.

Uporabi napredni pregledovalnik neželene pošte – občasno se bodo prenesli dodatni podatki za preprečevanje neželene pošte, ki bodo izboljšali funkcije preprečevanja neželene pošte in zagotovili boljše rezultate.

Pisanje dnevnika ocen neželene pošte – mehanizem za preprečevanje neželene pošte programa ESET Internet Security vsakemu pregledanemu sporočilu dodeli oceno neželene pošte. Sporočilo bo zabeleženo v dnevniku zaščite pred neželeno pošto (glavno okno programa > **Orodja** > **Dnevniške datoteke** > **Zaščita pred neželeno pošto v e-poštnem odjemalcu**).

- **Brez** – ocena neželene pošte pri pregledovanju ne bo zapisana v dnevnik.
- **Prerazvrščeno in označeno kot neželena pošta** – izberite to možnost, če želite zapisati oceno neželene pošte za sporočila, ki so označena kot SPAM.
- **Vse** – vsa sporočila bodo zapisana v dnevnik z oceno neželene pošte.

Ko kliknete sporočilo v mapi z neželeno pošto, lahko izberete možnost **Prerazvrsti izbrana sporočila kot ŽELENO pošto** in sporočilo bo premaknjeno v mapo »Prejeto«. Ko v mapi »Prejeto« kliknete neželeno sporočilo, lahko izberete možnost **Prerazvrsti izbrana sporočila kot neželeno pošto** in sporočilo bo premaknjeno v mapo z neželeno pošto. Izberete lahko več sporočil in to dejanje izvedete na vseh hkrati.

Optimizacija obravnave prilog – Če je optimizacija onemogočena, bodo vse priloge takoj optično pregledane. Morda se bo hitrost delovanja odjemalca e-pošte upočasnila.

Integracije – omogoča integracijo zaščite e-poštnega nabiralnika v e-poštni odjemalec. Za več informacij glejte Integracije.

Odgovor – omogoča prilagajanje obravnavanja neželenih sporočil. Za več informacij glejte Odgovor.

Integracije

Z integracijo programa ESET Internet Security z e-poštnimi odjemalci se poveča raven aktivne zaščite pred zlonamerno kodo v e-poštnih sporočilih. Če je vaš e-poštni odjemalec podprt, lahko omogočite integracijo v programu ESET Internet Security. Če je program integriran v vaš e-poštni odjemalec, je orodna vrstica programa ESET Internet Security vstavljena neposredno v e-poštni odjemalec za večjo učinkovitost zaščite e-pošte. Če želite urediti nastavitve integracije, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita e-poštnega odjemalca** > **Zaščita e-poštnega nabiralnika** > **Integracija**.

Integriraj s programom Microsoft Outlook – Microsoft Outlook je trenutno edini podprti e-poštni odjemalec. Zaščite e-pošte deluje kot vtičnik. Glavna prednost vtičnika je, da je neodvisen od uporabljenega protokola. Ko e-poštni odjemalec prejme šifrirano sporočilo, se to dešifrira in pošlje v pregledovalnik virusov. Za celotni seznam podprtih različic programa Microsoft Outlook glejte ta članek v zbirki znanja družbe ESET.

Napredna obdelava e-poštnega odjemalca – obdela dodatne dogodke Outlook Messaging API (MAPI)***: Predmet je spremenjen (`fnevObjectModified`) in predmet je ustvarjen (`fnevObjectCreated`). Če se vaš sistem pri delu z e-poštnim odjemalcem upočasni, to možnost onemogočite.

Orodna vrstica programa Microsoft Outlook

Zaščita programa Microsoft Outlook deluje kot modul za uporabo vtičnikov. Po namestitvi programa ESET Internet Security se ta orodna vrstica, ki vsebuje možnosti protivirusne zaščite in zaščite pred neželeno pošto v e-poštnem odjemalcu, doda v Microsoft Outlook:

Neželena pošta – označi izbrana sporočila kot neželeno pošto. Ko je sporočilo označeno, je njegov odtis poslan v osrednji strežnik, ki shranjuje podpise neželene pošte. Če strežnik prejme več podobnih odtisov od različnih uporabnikov, bo sporočilo v prihodnosti razvrščeno med neželeno pošto.

Ni neželena pošta – označi izbrana sporočila kot pošto, ki ni neželena.

Neželen naslov (blokirano, seznam neželenih naslovov) – doda nov naslov pošiljatelja na seznam naslovov kot blokiran. Vsa sporočila, prejeta z naslovov na seznamu, bodo samodejno razvrščena med neželeno pošto.

> Bodite pozorni na lažno predstavljanje – ponarejanje pošiljateljevega naslova v e–poštnih sporočilih z namenom zavajanja prejemnika, da sporočilo prebere in nanj odgovori.

Zaupanja vreden naslov (dovoljeno, seznam zaupanja vrednih naslovov) – doda nov naslov pošiljatelja na seznam naslovov kot dovoljen. Sporočila, prejeta z dovoljenih naslovov, nikoli ne bodo samodejno razvrščena kot neželena pošta.

ESET Internet Security – dvakrat kliknite ikono, da se odpre glavno okno izdelka ESET Internet Security.

Vnovični pregled sporočil – omogoča, da ročno zaženete pregledovanje e–pošte. Določite lahko sporočila, ki bodo preverjena, in aktivirate vnovični pregled prejete e-pošte. Za več informacij glejte Zaščita e-poštnega nabiralnika.

Nastavitev pregledovalnika – prikaže možnosti nastavitve zaščite e-poštnega nabiralnika.

Nastavitve neželene pošte – prikaže možnosti nastavitve zaščite e-poštnega nabiralnika.

Imeniki – odpre okno Upravljanje seznamov naslovov, v katerem imate dostop do seznamov izključenih in zaupanja vrednih naslovov ter naslovov neželene pošte.

Pogovorno okno za potrditev

Namen tega obvestila je preveriti, ali uporabnik res želi izvesti izbrano dejanje, s čimer naj bi bile odpravljene morebitne napake.

Vendar pa je v pogovornem oknu na voljo tudi možnost za onemogočanje potrditev.

Vnovični pregled sporočil

Orodna vrstica programa ESET Internet Security je vgrajena v odjemalce e-pošte in omogoča uporabniku več možnosti pregledovanja e-pošte. Možnost **Vnovični pregled sporočil** omogoča dva načina pregledovanja:

Vsa sporočila v trenutni mapi – pregleda sporočila v trenutno prikazani mapi.

Samo izbrana sporočila – pregleda le sporočila, ki jih označi uporabnik.

Potrditveno polje **Znova preglej že pregledana sporočila** omogoča uporabniku vnovični pregled sporočil, ki so že bila pregledana.

Odziv

Na podlagi rezultatov pregledovanja sporočil lahko program ESET Internet Security pregledana sporočila premakne ali pa v zadevo doda besedilo po meri. Te nastavitve lahko konfigurirate v razdelku Napredne nastavitve > **Zaščite** > **Zaščita e-poštnega odjemalca** > **Zaščita e-poštnega nabiralnika** > **Odziv**.

Zaščita pred neželeno pošto v e-poštnem odjemalcu v ESET Internet Security vam omogoča, da konfigurirate naslednje parametre za sporočila:

Dodaj besedilo v zadevo e–pošte – omogoči dodajanje niza predpone po meri v vrstico za zadevo v sporočilih, ki so razvrščena kot neželena pošta. Privzeto **besedilo** je »[SPAM]«.

Premakni v mapo z neželeno pošto – ko je možnost omogočena, bodo neželena e–poštna sporočila premaknjena v privzeto mapo za neželeno pošto in izbrana nezaželena sporočila, prerazvrščena kot želena pošta, premaknjena v mapo s prejeto pošto. Ko z desno tipko miške kliknete e-poštno sporočilo in v priročnem meniju izberete ESET Internet Security, lahko izbirate med veljavnimi možnostmi.

Premakni v mapo po meri – ko je možnost omogočena, se neželena sporočila premaknejo v spodnjo mapo.

Mapa – določite mapo po meri, v katero želite premakniti zaznano okuženo e–pošto.

Če obstaja sporočilo, ki vsebuje zaznani element, ESET Internet Security privzeto poskuša počistiti sporočilo. Če sporočila ni mogoče počistiti, lahko izberete možnost **Ukrepanje, če čiščenje ni mogoče**:

- **Ne naredi ničesar** – če je omogočeno, bo program prepoznal okužene priloge, vendar ne bo v e–pošti naredil ničesar.

- **Izbriši e-pošto** – program bo obvestil uporabnika o infiltraciji/-ah in izbrisal sporočilo.

- **Premakni e-pošto v mapo »Izbrisano«** – okužena e-pošta bo samodejno premaknjena v mapo »Izbrisano«.

- **Premakni e-pošto v mapo** (privzeto dejanje) – okužena e-pošta bo samodejno premaknjena v izbrano mapo.

Mapa – določite mapo po meri, v katero želite premakniti zaznano okuženo e–pošto.

Označi neželena sporočila kot prebrana – izberite to možnost, če želite neželeno pošto samodejno označiti kot prebrano. Tako se boste laže osredotočili na »čista« sporočila.

Označi prerazvrščena sporočila kot neprebrana – sporočila, ki so bila prvotno razvrščena kot neželena pošta, pozneje pa označena kot »čista«, bodo prikazana kot neprebrana.

Ko je e-pošta preverjena, je sporočilu mogoče dodati obvestilo z rezultati pregledovanja. Izberete lahko možnost **Prejeti in prebrani e-pošti dodaj označevalna sporočila** ali **Poslani e-pošti dodaj označevalna sporočila**. V redkih primerih se lahko zgodi, da so sporočila z oznakami v spornih sporočilih HTML izpuščena ali pa jih ponaredi zlonamerna programska oprema. Sporočila z oznakami je mogoče dodati prejeti in prebrani e-pošti ter poslani e-pošti (ali obema). Na voljo so naslednje možnosti:

- **Nikoli** – dodano ne bo nobeno sporočilo z oznako.

- **Ko pride do zaznave** – kot preverjena bodo označena le sporočila z zlonamerno programsko opremo (privzeta nastavitev).

- **Za vso e-pošto, ko je pregledana** – program bo sporočila dodal vsem pregledanim e-poštnim sporočilom.

Posodobitev zadeve prejete in prebrane e-pošte/Posodobitev zadeve poslane e-pošte – omogočite to možnost za dodajanje besedila po meri, ki je navedeno spodaj, v sporočilo.

Besedilo, ki ga želite dodati v zadevo zaznane e-pošte – če želite spremeniti obliko zapisa niza v vrstici z zadevo okuženega e-poštnega sporočila, uredite to predlogo. Funkcija bo sporočilo v vrstici z zadevo »Pozdravljeni« spremenila v to obliko zapisa: »[zaznani element %DETECTIONNAME%] Pozdravljeni«. Spremenljivka %DETECTIONNAME% predstavlja zaznano grožnjo.

Upravljanje seznamov naslovov

Funkcija za zaščito pred neželeno pošto v e-poštnem odjemalcu v ESET Internet Security omogoča, da konfigurirate različne parametre za sezname naslovov. Če želite konfigurirati sezname naslovov, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita e-poštnega odjemalca** > **Upravljanje seznamov naslovov**.

Omogoči seznam naslovov uporabnika – omogočite to možnost, če želite aktivirati seznam naslovov uporabnika.

Seznam naslovov uporabnika – seznam e-poštnih naslovov, na katerega lahko dodate, uredite ali izbrišete naslove, da določite pravila za preprečevanje neželene pošte. Pravila na tem seznamu bodo veljala za trenutnega uporabnika.

Omogoči globalni seznam naslovov – omogočite to možnost, če želite aktivirati globalni seznam naslovov, ki ga uporabljajo vsi uporabniki v tej napravi.

Globalni seznam naslovov – seznam e-poštnih naslovov, na katerega lahko dodate, uredite ali izbrišete naslove, da določite pravila za preprečevanje neželene pošte. Pravila na tem seznamu bodo veljala za vse uporabnike.

Samodejno dovoli in dodaj na seznam naslovov uporabnika

Naslove iz imenika obravnavaj kot zaupanja vredne – Naslovi na vašem seznamu stikov bodo obravnavani kot zaupanja vredni, ne da bi jih dodali na seznam naslovov uporabnika.

Dodaj naslove prejemnikov iz odhodnih sporočil – na seznam naslovov uporabnika dodajte naslove prejemnikov iz poslanih sporočil kot dovoljeno.

Dodaj naslove iz sporočil, ki so prerazvrščena kot ŽELENA pošta – na seznam naslovov uporabnika dodajte naslove pošiljateljev iz sporočil, ki so razvrščena kot ŽELENA, kot dovoljeno.

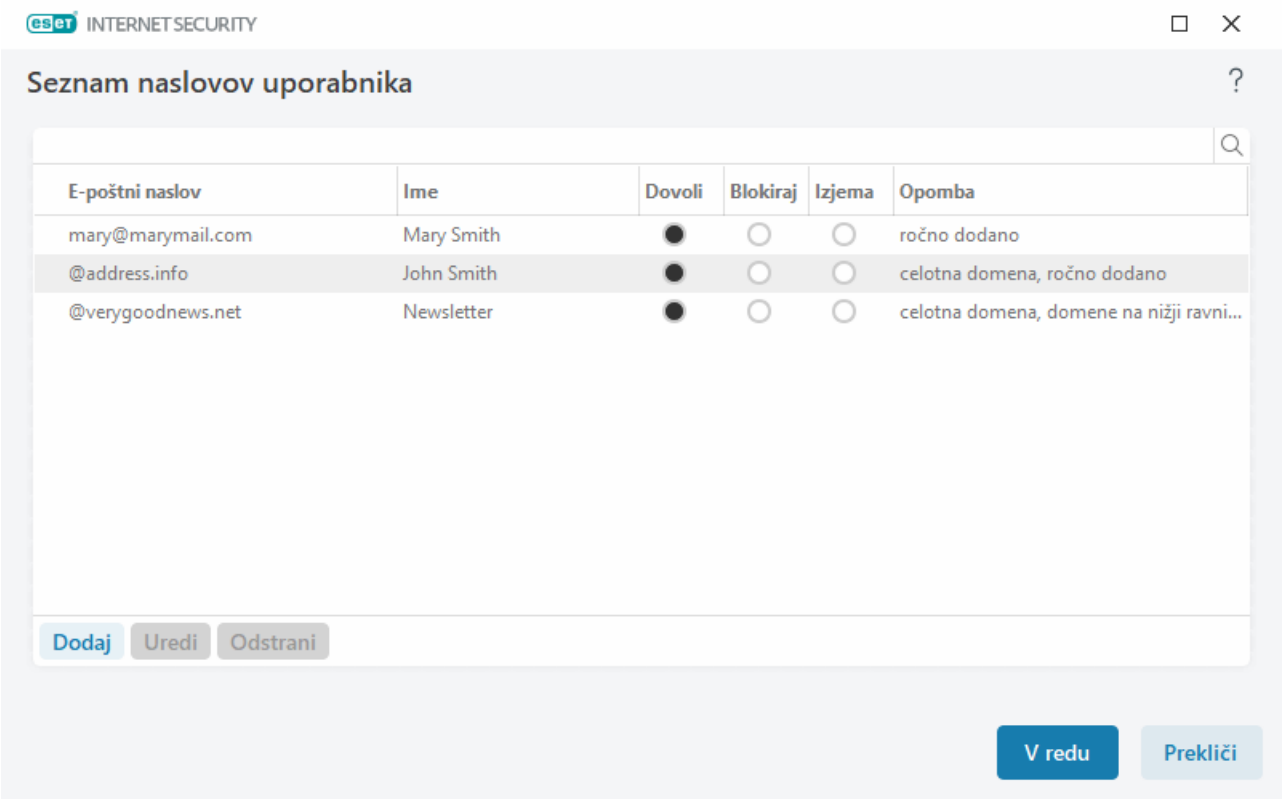
Samodejno dodaj na seznam naslovov uporabnika kot izjemo

Dodaj naslove iz lastnih računov – na seznam naslovov uporabnika dodajte naslove iz obstoječih računov e-poštnega odjemalca kot izjemo.

Seznami naslovov

Za zaščito pred vsiljeno e-pošto vam program ESET Internet Security omogoča, da e-poštne naslove razvrstite na sezname naslovov.

Če želite urediti sezname naslovov, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita e-poštnega odjemalca** > **Upravljanje seznamov naslovov** in kliknite možnost **Uredi** zraven **seznama naslovov uporabnika** ali **globalnega seznama naslovov**.



Stolpci

E-poštni naslov – naslov, za katerega velja pravilo. Nadomestni znaki niso podprti.

Ime – ime pravila po meri.

Dovoli/blokiraj/izjema – radijski gumbi, s katerimi določite, katero dejanje naj se izvede za e-poštni naslov (če želite hitro spremeniti dejanje, kliknite radijski gumb v želenem stolpcu):

- **Dovoli** – naslove, ki veljajo za varne in od katerih želite prejemati sporočila.
- **Blokiraj** – naslove, ki veljajo za nevarne/neželene in od katerih ne želite prejemati sporočil.
- **Izjema** – naslovi, ki se vedno preverjajo, ali pošiljajo neželeno pošto, in pri katerih gre morda za lažno predstavljanje ter se uporabljajo za pošiljanje neželene pošte.

Opomba – podatki o tem, kako je bilo pravilo ustvarjeno in ali velja za celotno domeno/domene nižje ravni.

Upravljanje naslovov

- **Dodaj** – kliknite to možnost, če želite dodati pravilo za nov naslov.
- **Uredi** – izberite in kliknite to možnost, če želite urediti obstoječe pravilo.
- **Odstrani** – izberite in kliknite to možnost, če želite izbrisati pravilo s seznama naslovov.

Dodaj/uredi naslov

V tem oknu lahko dodate ali uredite naslov v možnosti Upravljanje seznamov naslovov in konfigurirate izvedeno dejanje:

E-poštni naslov – naslov, za katerega velja pravilo.

Ime – ime pravila po meri.

Dejanje – dejanje, ki ga je treba izvesti, če se e-poštni naslov stika ujema z naslovom, določenim v polju **E-poštni naslov**:

- **Dovoli** – naslove, ki veljajo za varne in od katerih želite prejemati sporočila.
- **Blokiraj** – naslove, ki veljajo za nevarne/neželene in od katerih ne želite prejemati sporočil.
- **Izjema** – naslovi, ki se vedno preverjajo, ali pošiljajo neželeno pošto, in pri katerih gre morda za lažno predstavljanje ter se uporabljajo za pošiljanje neželene pošte.

Celotna domena – to možnost izberite za pravilo, ki bo veljalo za celotno domeno stika (ne le za naslov, določen v polju **E-poštni naslov**, ampak za vse e-poštne naslove v domeni *address.info* domain).

Domene na nižji ravni – izberite to možnost, če želite pravilo uporabiti za domene na nižji ravni stika (*address.info* predstavlja domeno, *my.address.info* pa poddomeno).

Rezultat obdelave naslova

Ko dodate nove naslove ali spremenite dejanje, ki ste ga izvedli za e-poštni naslov, program ESET Internet Security prikaže sporočila z obvestili. Vsebina sporočil z obvestili je odvisna od dejanja, ki ga poskušate izvesti.

Izberite potrditveno polje **Ne vprašaj več**, če želite, da se dejanje naslednjič izvede samodejno, ne da bi se prikazalo sporočilo.

ThreatSense

ThreatSense je sestavljen iz veliko zapletenih načinov zaznavanja groženj. Ta tehnologija je proaktivna, kar pomeni, da ponuja zaščito tudi med začetno fazo širitve nove grožnje. Uporablja kombinacijo analize kode, posnemanja kode, splošnih definicij in definicij virusov, ki s skupnim delovanjem znatno izboljšajo varnost računalnika. Orodje za pregledovanje lahko nadzira več podatkovnih tokov hkrati in tako poveča učinkovitost ter stopnjo zaznavanja na najvišjo možno raven. ThreatSense tehnologija tudi uspešno odstrani korenske komplete.

Z možnostmi za nastavitev mehanizma tehnologije ThreatSense lahko določite več parametrov pregledovanja:

- vrste datotek in datotečnih pripon, ki jih želite pregledati
- kombinacijo različnih načinov zaznavanja
- ravni čiščenja itd.

Če želite odpreti okno z nastavitvami kliknite **ThreatSense** v naprednih nastavitvah za vsak modul, ki uporablja tehnologijo ThreatSense (glejte spodaj). Za različne primere varnosti boste morda potrebovali različne konfiguracije. Orodje ThreatSense je zato mogoče posamezno konfigurirati za naslednje module zaščite:

- Sprotna zaščita datotečnega sistema
- Pregledovanje v mirovanju
- Zagonski pregled
- Zaščita dokumentov
- Zaščita e-poštnega odjemalca
- Zaščita spletnega dostopa
- Pregled računalnika

Parametri za ThreatSense so optimizirani za vsak modul. Če spremenite te parametre, lahko močno vplivate na delovanje računalnika. Če parametre na primer spremenite tako, da vedno pregledajo samoustvarjalne arhive, ali omogočite napredno hevristiko v modulu za sprotno zaščito datotečnega sistema, lahko računalnik začne delovati počasneje (običajno so s temi načini pregledane samo nove datoteke). Zato priporočamo, da za noben modul, razen za pregled računalnika, ne spreminjate privzetih parametrov orodja ThreatSense.

Predmeti za pregled

V tem razdelku lahko določite, v katerih komponentah računalnika in datotekah bo izveden pregled za morebitne infiltracije.

Delovni pomnilnik – s pregledom je ugotovljeno, ali so v računalniku grožnje, ki napadejo delovni pomnilnik sistema.

Zagonski sektorji/UEFI – S pregledom se ugotovi, ali je zlonamerna programska oprema v glavnih zagonskih zapisih. Več o vmesniku UEFI lahko preberete v slovarju izrazov.

E–poštne datoteke – program podpira te pripone: DBX (Outlook Express) in EML.

Arhivi – program podpira naslednje pripone: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE in mnoge druge.

Samoraztezni arhivi – samoraztezni arhivi (SFX) so arhivi, ki se lahko raztezajo sami.

Samoustvarjalni arhivi – po izvajanju se samoustvarjalni arhivi (v nasprotju s standardnimi vrstami arhivov) v pomnilniku raztegnejo. Poleg standardnih statičnih arhivov (UPX, yoda, ASPack, FSG itn.) lahko pregledovalnik s posnemanjem kode prepozna še številne druge vrste arhivov.

Možnosti pregleda

Izberite načine, ki jih želite uporabiti pri preverjanju morebitnih infiltracij. Na voljo so naslednje možnosti:

Hevristika – hevristika je algoritem, ki analizira (zlonamerno) dejavnost programov. Njena glavna prednost je ta, da zna prepoznati zlonamerno programsko opremo, ki prej ni obstajala ali je prejšnja različica orodja za zaznavanje ni poznala. Njena pomanjkljivost pa je (zelo majhna) možnost lažnega preplaha.

Napredna hevristika/definicije DNA – napredna hevristika je enolični hevristični algoritem, ki ga je razvilo podjetje ESET in je optimiziran za zaznavanje računalniških črvov in trojanskih konjev ter napisan z visoko razvitimi programskimi jeziki. Uporaba napredne hevristike izdelkom ESET močno poveča zmogljivost zaznavanja groženj. Z definicijami je mogoče zanesljivo zaznati in prepoznati viruse. Nov samodejni sistem posodabljanja omogoča, da so nove definicije na voljo že v nekaj urah po odkritju grožnje. Pomanjkljivost definicij je, da zaznajo le viruse, ki jih poznajo (oziroma rahlo spremenjene različice teh virusov).

Čiščenje

Z nastavitvami čiščenja je določeno delovanje programa ESET Internet Security med čiščenjem predmetov. Na voljo so 4 ravni čiščenja:

ThreatSense ima naslednje ravni popravljanja (tj. čiščenja).

Popravljanje s programom ESET Internet Security

Raven čiščenja	Opis
Vedno popravi zaznani element	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih redkih primerih (na primer pri sistemskih datotekah) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.

Raven čiščenja	Opis
Popravi zaznani element, če je varno, sicer ohrani	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih primerih (na primer pri sistemskih datotekah ali arhivih z neokuženimi in okuženimi datotekami) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.
Popravi zaznani element, če je varno, sicer vprašaj	Poskuša popraviti zaznani element med čiščenjem predmetov. V nekaterih primerih, če ni mogoče izvesti nobenega dejanja, se končnemu uporabniku prikaže interaktivno opozorilo in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta nastavitev je priporočljiva v večini primerov.
Vedno vprašaj končnega uporabnika	Končnemu uporabniku se med čiščenjem predmetov prikaže interaktivno okno in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta raven je namenjena bolj izkušenim uporabnikom, ki vedo, kako ukrepati v primeru zaznanega elementa.

Izključitve

Pripona je del imena datoteke, ki je od drugega dela imena ločena s piko. S pripono je označena vrsta in vsebina datoteke. V tem razdelku z nastavitvami orodja ThreatSense je mogoče določiti vrste datotek za pregledovanje.

Ostalo

Pri konfiguriranju parametrov orodja ThreatSense za pregled računalnika na zahtevo so na voljo tudi naslednje možnosti v razdelku **Ostalo**:

Preglej nadomestne podatkovne tokove (ADS) – nadomestni podatkovni tokovi, ki jih uporablja datotečni sistem NTFS, so povezave z datotekami in mapami, ki jih navadne tehnike pregledovanja ne zaznajo. Mnoge infiltracije se poskušajo izogniti zaznavanju tako, da se predstavijo kot nadomestni podatkovni tokovi.

Zaženi preglede v ozadju z nizko pomembnostjo – vsak pregled porabi določeno količino sistemskih sredstev. Če delate s programi, ki porabijo veliko sistemskih sredstev, lahko aktivirate pregledovanje v ozadju z nizko prioriteto in prihranite sredstva za svoje programe.

Zapiši v dnevnik vse predmete – dnevnik pregledovanja prikaže vse pregledane datoteke v samorazteznih arhivih, tudi tiste, ki niso okužene (to lahko ustvari veliko podatkov v dnevniku pregledovanja in poveča velikost datoteke dnevnika pregledovanja).

Omogoči pametno optimizacijo – če je pametna optimizacija omogočena, so uporabljene najbolj optimalne nastavitve, ki zagotavljajo najbolj učinkovito pregledovanje pri najvišjih hitrostih pregledovanja. Različni moduli zaščite pregledujejo na pameten način, kar pomeni, da uporabljajo različne načine pregledovanja, ki jih uporabijo za določene vrste datotek. Če je pametna optimizacija onemogočena, so pri pregledu uporabljene le uporabniško določene nastavitve v jedru ThreatSense posameznih modulov.

Ohrani časovni žig zadnjega dostopa – izberite to možnost, če želite ohraniti originalni čas dostopa do pregledane datoteke, namesto da bi se ta posodobil (na primer za uporabo s sistemi za varnostno kopiranje podatkov).

Omejitve

V razdelku »Omejitve« lahko določite največjo velikost predmetov in ravni gnezdenja arhivov, ki bodo pregledani:

Nastavitve predmeta

Največja velikost predmeta – določa največjo velikost predmetov, ki bodo pregledani. Protivirusni modul bo pregledoval samo predmete, ki so manjši od določene velikosti. To možnost naj spreminjajo le napredni uporabniki, ki imajo morda določene razloge, da iz pregledovanja izključijo večje predmete. Privzeta vrednost: neomejeno.

Najdaljši čas pregledovanja predmeta (s) – določi največjo časovno vrednost za pregled datotek v vsebniškem predmetu (na primer arhivski datoteki RAR/ZIP ali e-poštnem sporočilu z več prilogami. Ta nastavitev ne velja za samostojne datoteke. Če je bila vnesena uporabniško določena vrednost in je čas potekel, se pregled konča takoj, ko je mogoče, ne glede na to, ali je pregled vseh datotek v vsebniškem predmetu zaključen.
V primeru arhiva z velikimi datotekami se pregled ustavi šele, ko je datoteka iz arhiva ekstrahirana (na primer: uporabniško določena spremenljivka je 3 sekunde, ekstrakcija datoteke pa traja 5 sekund). Preostale datoteke v arhivu po poteku določenega časa ne bodo pregledane.
Za omejitev časa pregledovanja, vključno z velikimi arhivi, uporabite možnosti **Največja velikost predmeta** in **Največja velikost datoteke v arhivu** (ni priporočeno zaradi morebitnih varnostnih tveganj).
Privzeta vrednost: neomejeno.

Nastavitev pregledovanja arhiva

Raven gnezdenja arhiva – določa največjo globino pregledovanja arhivov. Privzeta vrednost: 10.

Največja velikost datoteke v arhivu – ta možnost omogoča, da določite največjo velikost datotek v arhivu (ko so ekstrahirane), ki bodo pregledane. Privzeta vrednost je: **3 GB**.

priporočamo, da ne spreminjate privzetih vrednosti, v normalnih okoliščinah to običajno ni potrebno.

Zaščita spletnega dostopa

Zaščita spletnega dostopa omogoča konfiguriranje naprednih nastavitev modula Zaščita na spletu. Te možnosti so na voljo v razdelku Napredne nastavitve > **Zaščite** > **Zaščita spletnega dostopa** > **Zaščita spletnega dostopa**:

Omogoči zaščito spletnega dostopa – ko je ta možnost onemogočena, se zaščita spletnega dostopa in preprečevanje lažnega predstavljanja ne izvajata.

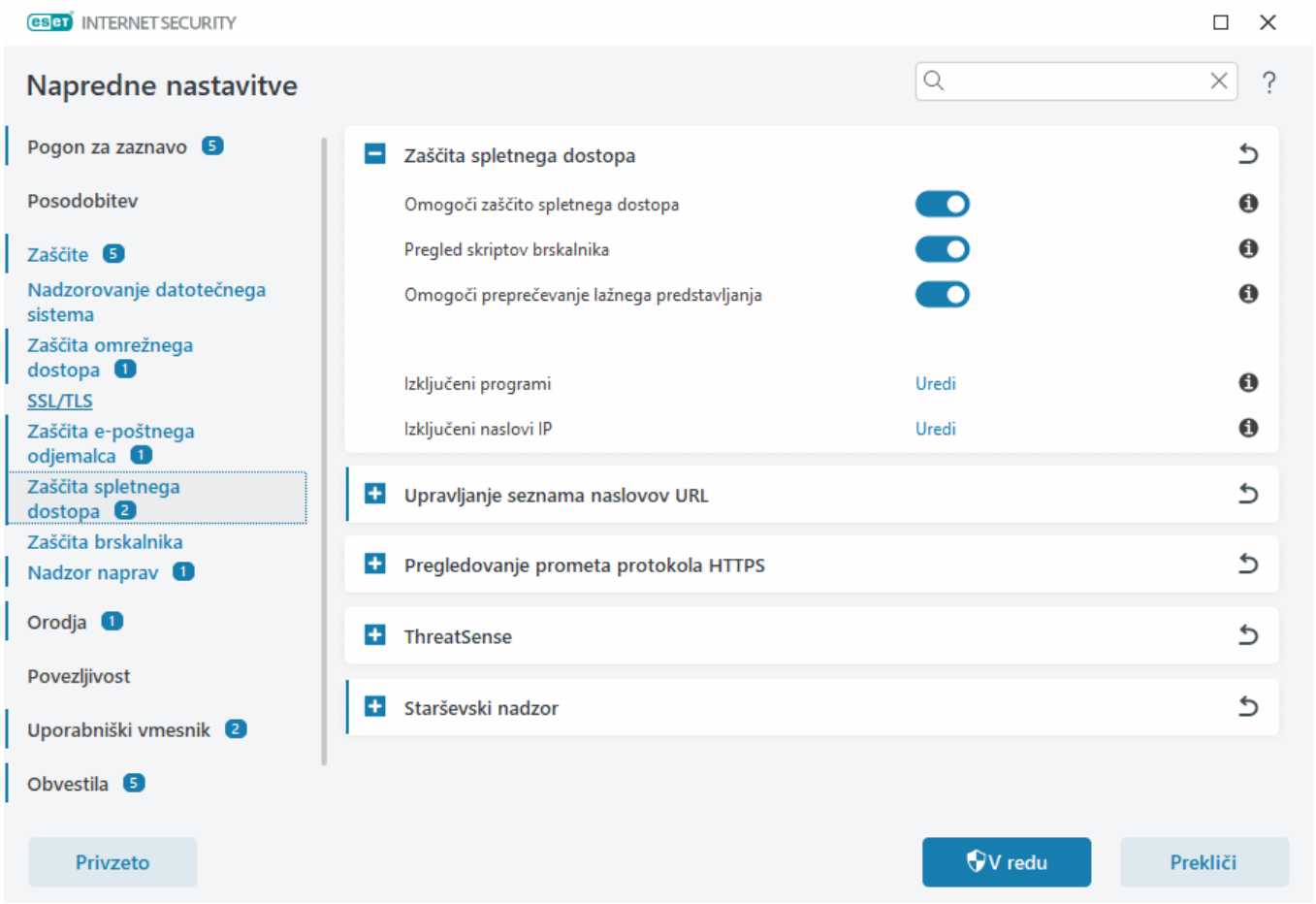
Priporočamo, da privzeto pustite omogočeno zaščito spletnega dostopa in ne izključujte nobenih programov ali naslovov IP.

Pregled skriptov brskalnika – ko je možnost omogočena, pogon za zaznavo preveri se programe JavaScript, ki se izvajajo v spletnih brskalnikih.

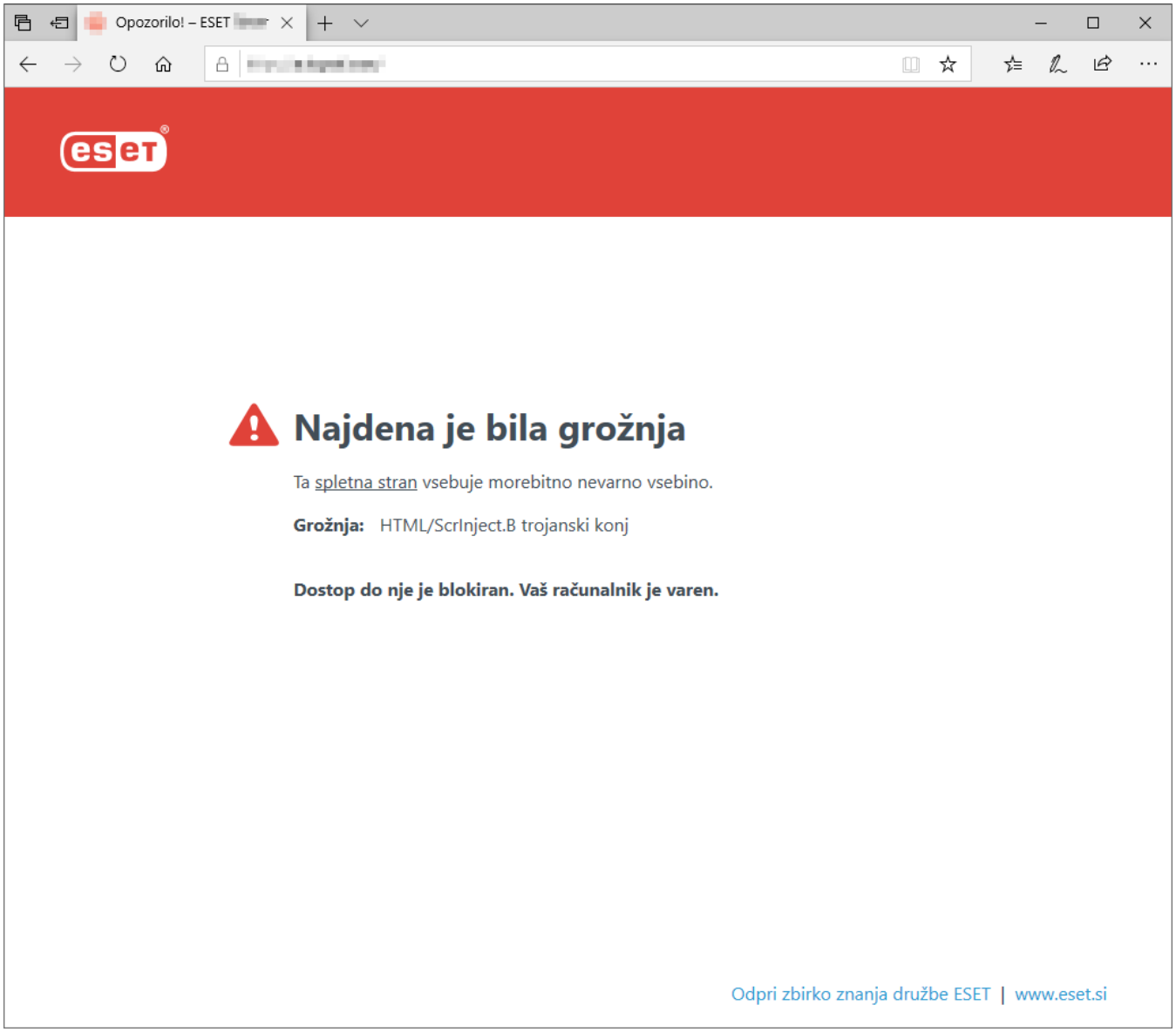
Omogoči preprečevanje lažnega predstavljanja – ko je možnost omogočena, so spletne strani z lažnim predstavljanjem blokirane. Za več informacij glejte razdelek Preprečevanje lažnega predstavljanja.

Izključeni programi – omogoča izključitev določenih programov iz pregleda zaščite spletnega dostopa. To je uporabno, če zaščita spletnega dostopa povzroča težave z združljivostjo.

Izključeni naslovi IP – omogoča izključitev določenih oddaljenih naslovov iz pregleda zaščite spletnega dostopa. To je uporabno, če zaščita spletnega dostopa povzroča težave z združljivostjo.



Zaščita spletnega dostopa bo ob blokiranju spletnega mesta v brskalniku prikazala naslednje sporočilo:



Ilustrirana navodila

Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:

- Izključevanje varnega spletnega mesta iz blokade funkcije zaščite spletnega dostopa
- Blokiranje spletnega mesta s programom ESET Internet Security

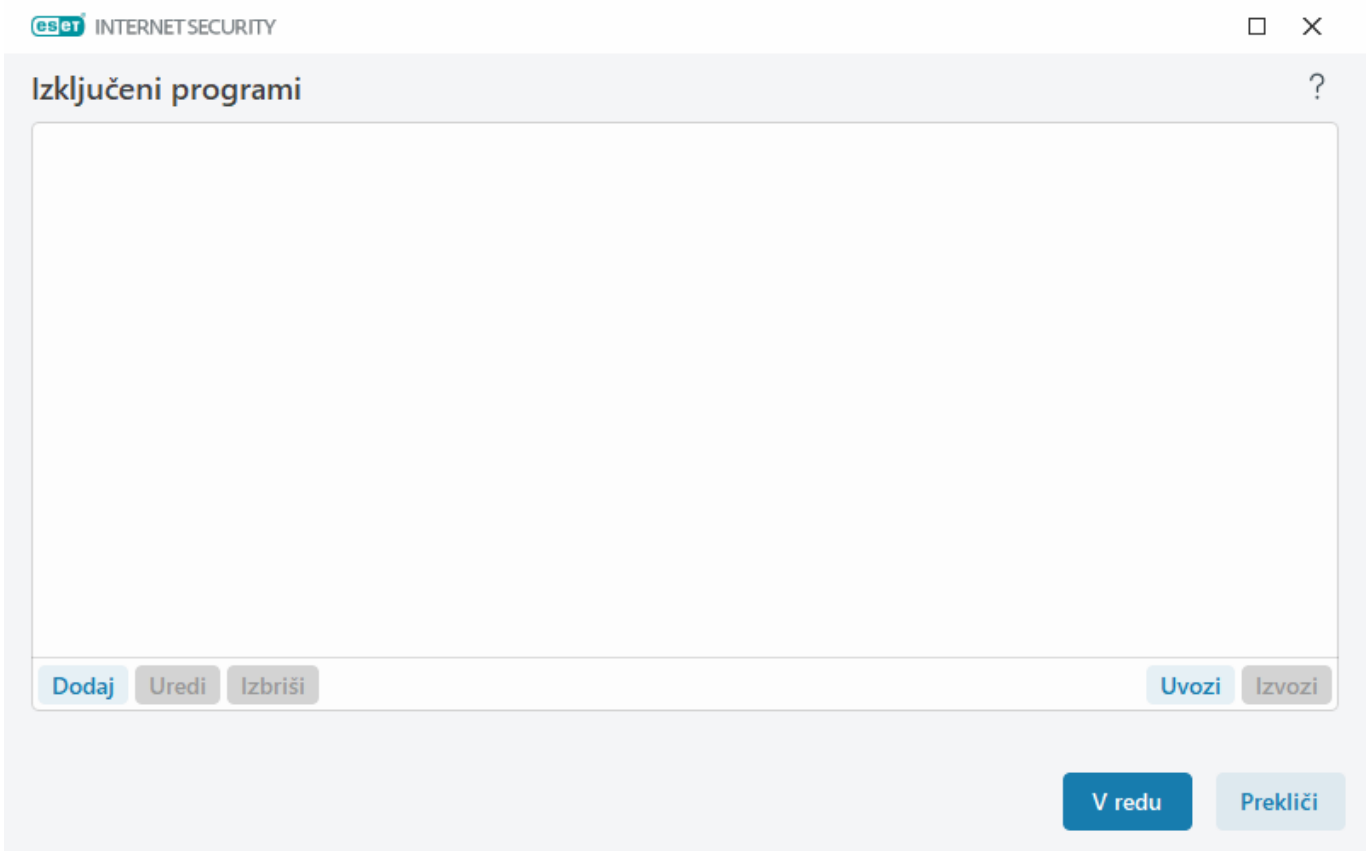
Izključeni programi

Če želite izključiti pregled komunikacije za določene programe, jih dodajte na seznam. V komunikaciji HTTP(S)/POP3(S)/IMAP(S) izbranih programov ne bo preverjeno, ali so v njej grožnje. Priporočamo, da to uporabite le za programe, ki ne delujejo pravilno pri pregledu komunikacije.

Ko kliknete možnost **Dodaj**, bodo tu samodejno na voljo programi in storitve, ki ste izvajajo. Kliknite **...** in se pomaknite v program, če želite ročno dodati izključitev.

Uredi – uredite izbrane vnose na seznamu.

Odstrani – odstranite izbrane vnose s seznama.



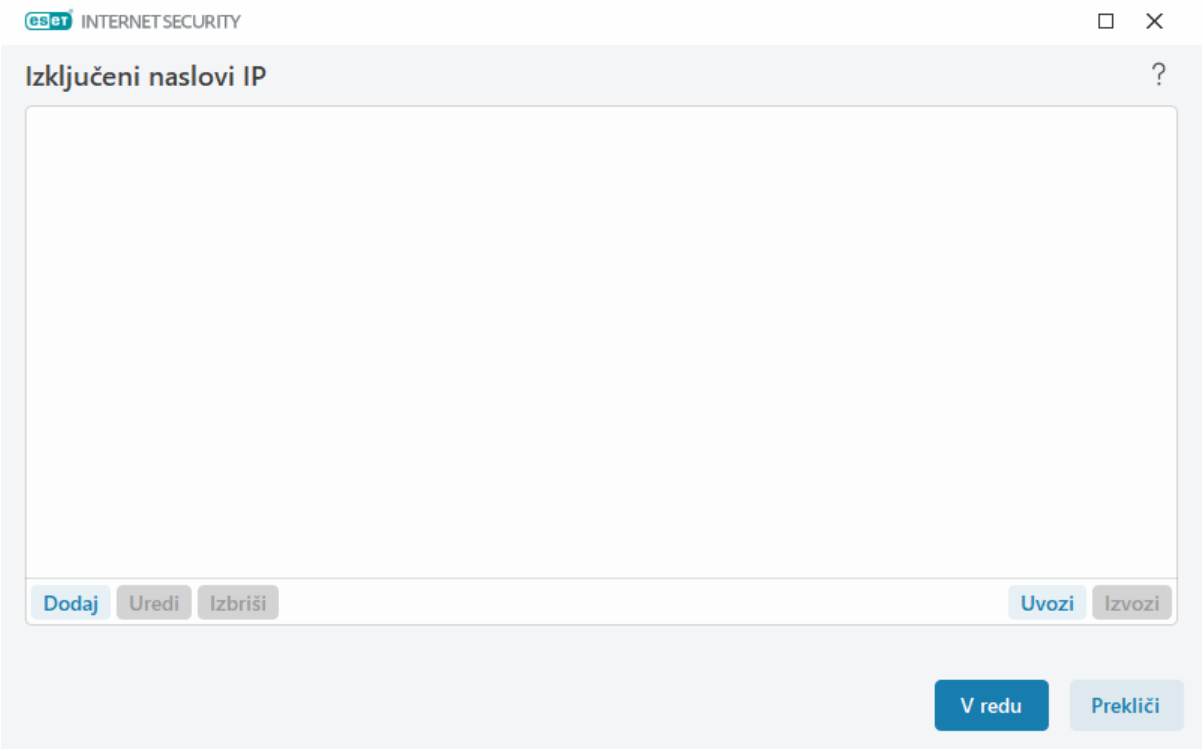
Izključeni naslovi IP

Vnosi na seznamu bodo izključeni iz pregleda. V komunikaciji HTTP(S)/POP3(S)/IMAP(S) iz izbranih naslovov in na njih ne bo preverjeno, ali so njej grožnje. Priporočamo, da to možnost uporabite le za zaupanja vredne naslove.

Kliknite **Dodaj**, če želite izključiti naslov IP/obseg naslovov/podomrežje oddaljene točke.

Kliknite možnost **Uredi**, če želite spremeniti izbrani naslov IP.

Kliknite **Izbriši**, če želite odstraniti izbrane vnose s seznama.



Primeri naslovov IP

Dodaj naslov IPv4:
Enotni naslov – doda naslov IP posameznega računalnika (na primer *192.168.0.10*).
Obseg naslovov – vnesite začetni in končni naslov IP naslova, da določite obseg IP več računalnikov (na primer *od 192.168.0.1 do 192.168.0.99*).
Podomrežje – podomrežje (skupina računalnikov) je določeno z naslovom IP in masko. 255.255.255.0 je na primer maska omrežja za podomrežje 192.168.1.0. Za izključitev celotne vrste podomrežja v *192.168.1.0/24*.
Dodaj naslov IPv6:
Enotni naslov – doda naslov IP posameznega računalnika (na primer *2001:718:1c01:16:214:22ff:fec9:ca5*).
Podomrežje – podomrežje (skupina računalnikov) je določeno z naslovom IP in masko (na primer: *2002:c0a8:6301:1::1/64*).

Upravljanje seznama naslovov URL

Upravljanje seznama naslovov URL v razdelku Napredne nastavitve > **Zaščite** > **Zaščita spletnega dostopa** vam omogoča določanje naslovov HTTP, ki jih želite blokirati, dovoliti ali izključiti iz pregledovanja vsebine.

Protokol SSL/TLS mora biti omogočen, če želite poleg naslovov HTTP filtrirati tudi naslove HTTPS. V nasprotnem primeru so dodane samo domene obiskanih spletnih mest HTTPS, ne pa celoten URL.

Spletna mesta na **seznamu blokiranih naslovov** ne bodo dostopna, razen če so vključena tudi na **seznam dovoljenih naslovov**. Spletna mesta na **seznamu naslovov, izključenih iz pregledovanja vsebine**, pri odpiranju niso pregledana za prisotnost zlonamerne kode.

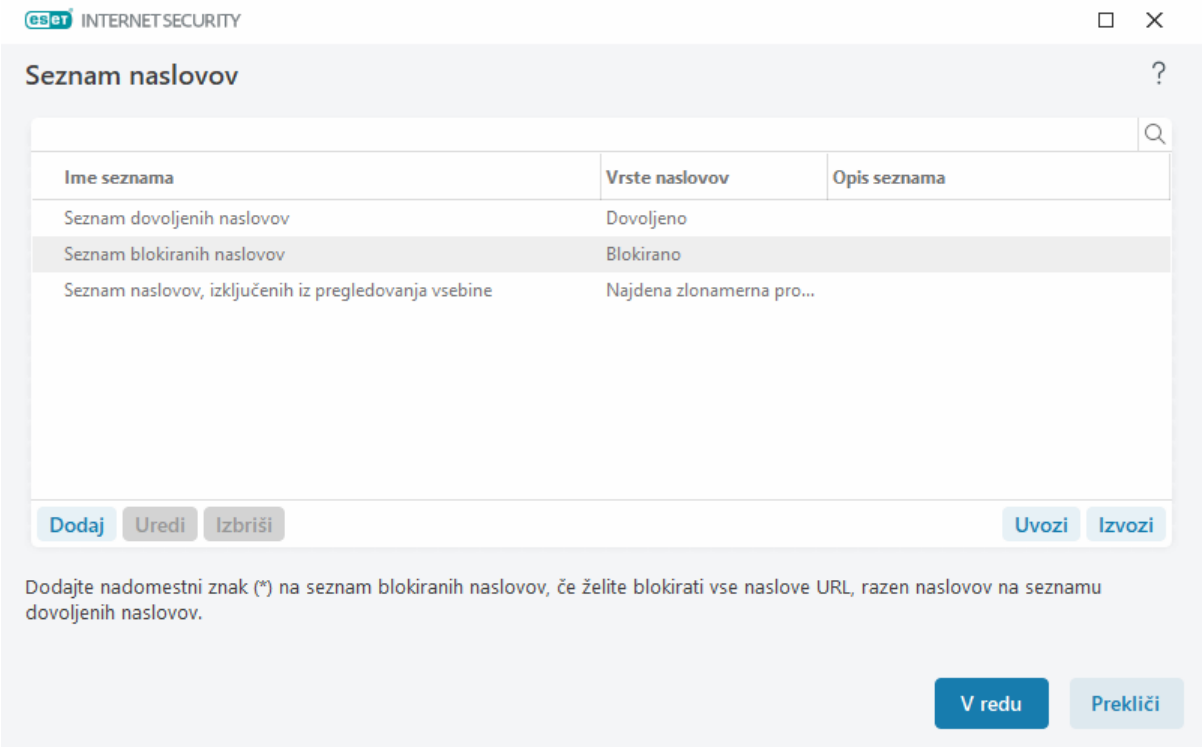
Če želite blokirati vse naslove HTTP, razen naslovov na aktivnem **seznamu dovoljenih naslovov**, dodajte »*« na aktiven **seznam blokiranih naslovov**.

Uporabite lahko posebna simbola »*« (zvezdica) in »?« (vprašaj). Z zvezdico nadomestite poljuben niz znakov, z vprašajem pa poljuben simbol. Pazljivi bodite, ko določate izključene naslove, saj lahko seznam vsebuje le zaupanja vredne in varne naslove. Poleg tega se prepričajte, da ste na tem seznamu pravilno uporabili simbola

»*« in »?«. V razdelku Dodajanje maske naslova/domene HTTP preberite, kako je mogoče varno ujemanje celotne domene, vključno z vsemi poddomenami. Če želite aktivirati seznam, izberite možnost **Aktivni seznam**. Če želite biti obveščeni, kadar vnašate naslov s trenutnega seznama, izberite možnost **Obvesti ob uporabi**.

Naslovi, ki jim ESET zaupa

Če je omogočena možnost **Ne pregleduj prometa z domenami, ki jim ESET zaupa**, je SSL/TLS, konfiguracija upravljanja seznama naslovov URL ne bo vplivala na domene na seznamu varnih pošiljateljev, ki ga upravlja ESET.



Elementi kontrolnika

Dodaj – ustvari nov seznam poleg že določenih. To je uporabno, če želite logično razdeliti različne skupine naslovov. Na enem seznamu blokiranih naslovov so na primer naslovi iz zunanjega javnega seznama blokiranih naslovov, na drugem pa naslovi iz osebnega seznama blokiranih naslovov. V tem primeru zlahka posodobite zunanji seznam, ne da bi spreminjali svojega.

Uredi – spremeni obstoječe sezname. To možnost uporabite za dodajanje ali odstranjevanje naslovov.

Izbriši – izbriše obstoječe sezname. Ta možnost ni na voljo za privzete sezname, ampak samo za sezname, ustvarjene z možnostjo **Dodaj**.

Seznam naslovov

V tem razdelku lahko določite sezname naslovov HTTP(S), ki bodo blokirani, dovoljeni ali izključeni iz preverjanja.

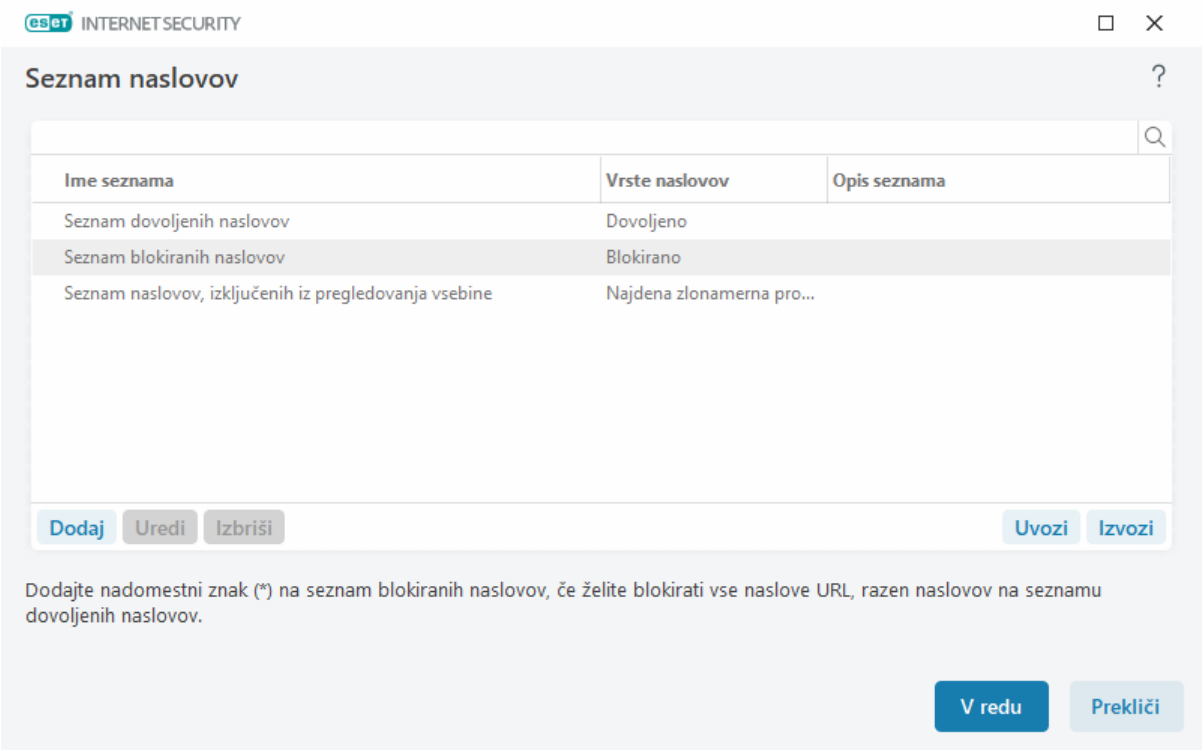
Privzeto so na voljo ti trije seznami:

- **Seznam naslovov, izključenih iz pregledovanja vsebine** – brez iskanja zlonamerne kode za kateri koli naslov, ki je dodan na ta seznam.

• **Seznam dovoljenih naslovov** – če je omogočena možnost Dostop dovoli le za naslove HTTP, ki so na seznamu dovoljenih naslovov in seznam blokiranih naslovov vsebuje simbol »*« (ujemanje z vsem), bo uporabniku dovoljen le dostop do naslovov, določenih na tem seznamu. Naslovi na tem seznamu so dovoljeni, tudi če so navedeni na seznamu blokiranih naslovov.

• **Seznam blokiranih naslovov** – uporabnik ne bo smel dostopati do naslovov, navedenih na tem seznamu, razen če so navedeni tudi na seznamu dovoljenih naslovov.

Če želite ustvariti nov seznam, kliknite **Dodaj**. Če želite izbrane sezname izbrisati, kliknite **Izbriši**.



Ilustrirana navodila

Naslednji članki zbirke znanja družbe ESET so morda na voljo le v angleščini:
- Izključevanje varnega spletnega mesta iz blokade funkcije zaščite spletnega dostopa
- Blokiranje spletnega mesta z izdelki za domačo uporabo ESET za Windows

Za več informacij glejte Upravljanje seznama naslovov URL.

Ustvarjanje novega seznama naslovov

To pogovorno okno omogoča, da konfigurirate nov seznam naslovov/mask URL, ki bodo blokirani, dovoljeni ali izključeni iz preverjanja.

Konfigurirate lahko naslednje možnosti:

Vrsta seznama naslovov – na voljo so tri vrste seznama:

• **Najdena zlonamerna programska oprema je prezrta** – brez preverjanja zlonamerne kode za kateri koli naslov, ki je dodan na ta seznam.

• **Blokirano** – dostop do naslovov, navedenih na tem seznamu, bo blokiran.

- **Dovoljeno** – dostop do naslovov, navedenih na tem seznamu, bo dovoljen. Naslovi na tem seznamu so dovoljeni, tudi če so navedeni na seznamu blokiranih naslovov.

Ime seznama – določite ime seznama. To polje ne bo na voljo, kadar urejate enega od vnaprej določenih seznamov.

Opis seznama – vnesite kratek opis seznama (izbirno). Ni na voljo, kadar urejate enega od vnaprej določenih seznamov.

Če želite aktivirati seznam, izberite možnost **Aktivni seznam** ob seznamu. Če želite biti obveščeni, ko je določen seznam uporabljen pri dostopu do spletnih mest, izberite možnost **Obvesti ob prijavi**. Obvestilo boste na primer prejeli, ko je spletno mesto blokirano ali dovoljeno, ker je na seznamu blokiranih ali dovoljenih naslovov. V obvestilu bo ime seznama.

Resnost zapisovanja v dnevnik – podatke o seznamu, ki se uporablja pri dostopu do spletnih mest, lahko zapišete v dnevniške datoteke.

Elementi kontrolnika

Dodaj – dodajte nov naslov URL na seznam (več vrednosti vnesite z ločilom).

Uredi – spremeni obstoječ naslov na seznamu. Na voljo samo za naslove, ki ste jih ustvarili prek možnosti **Dodaj**.

Odstrani – odstrani obstoječ naslov na seznamu. Na voljo samo za naslove, ki ste jih ustvarili prek možnosti **Dodaj**.

Uvozi – uvozi datoteko z naslovi URL (vrednosti ločite s prelomom vrstice, na primer *.txt s kodiranjem UTF-8).

Kako dodati masko URL-ja

Pred vnosom želene maske naslova/domene preberite navodila v tem pogovornem oknu.

ESET Internet Security omogoča uporabnikom, da blokirajo dostop do navedenih spletnih mest in internetnim brskalnikom preprečijo prikaz vsebine na teh mestih. Poleg tega lahko uporabniki določijo naslove, ki jih želijo izključiti iz pregleda. Če je celotno ime oddaljenega strežnika neznano ali če uporabnik želi določiti celotno skupino oddaljenih strežnikov, je tako skupino mogoče prepoznati s tako imenovanimi maskami. V maske sta vključena simbola »?« in »*«.

- Če želite nadomestiti simbol, uporabite »?«.
- Če želite nadomestiti besedilni niz, uporabite »*«.

*.c?m velja na primer za vse naslove, v katerih se zadnji del začne s črko c, se konča s črko m, med tema črkama pa je neznani simbol (.com, .cam, itd.).

Začetni zapis »*.« se obravnava na poseben način, če je uporabljen na začetku imena domene. Nadomestni znak »*« se v tem primeru ne ujema z znakom »/«. To prepreči, da se maska zaobide, npr. maska **.domain.com* se ne bo ujemala z naslovom *http://anydomain.com/anypath#.domain.com* (to pripono je mogoče dodati kateremu koli naslovu URL brez vpliva na prenos). Poleg tega se »*« v tem posebnem primeru ujema s praznim nizom. To omogoči ujemanje celotne domene, vključno z vsemi poddomenami, z uporabo ene maske. Maska **.domain.com* se na primer ujema tudi z domeno *http://domain.com*. Uporaba zapisa **domain.com* ni pravilna, ker bi to pomenilo ujemanje z drugo domeno *http://anotherdomain.com*.

Pregledovanje prometa protokola HTTPS

Program ESET Internet Security je privzeto konfiguriran za pregled prometa protokolov HTTP in HTTPS, ki ga uporabljajo internetni brskalniki in drugi programi. Pregledovanje prometa onemogočite samo, če imate težave s programsko opremo drugih proizvajalcev in želite izvedeti, če težavo povzroča ESET Internet Security.

Omogoči pregledovanje prometa protokola HTTP – Promet HTTP se vedno nadzoruje na vseh vratih za vse programe.

Omogoči pregledovanje prometa protokola HTTP – promet protokola HTTPS uporablja šifrirani kanal za prenos informacij med strežnikom in odjemalcem. ESET Internet Security preverja komunikacije, ki uporabljajo protokola SSL (sloj varnih vtičnic) in TLS (varnost transportnega sloja). Program bo pregledal promet samo za vrata, določena v možnosti **Vrata, ki jih uporablja protokol HTTPS**, ne glede na različico operacijskega sistema (vrata lahko dodate vnaprej določenima 443 in 0-65535).

ThreatSense

ThreatSense je sestavljen iz veliko zapletenih načinov zaznavanja groženj. Ta tehnologija je proaktivna, kar pomeni, da ponuja zaščito tudi med začetno fazo širitve nove grožnje. Uporablja kombinacijo analize kode, posnemanja kode, splošnih definicij in definicij virusov, ki s skupnim delovanjem znatno izboljšajo varnost računalnika. Orodje za pregledovanje lahko nadzira več podatkovnih tokov hkrati in tako poveča učinkovitost ter stopnjo zaznavanja na najvišjo možno raven. ThreatSense tehnologija tudi uspešno odstrani korenske komplete.

Z možnostmi za nastavitev mehanizma tehnologije ThreatSense lahko določite več parametrov pregledovanja:

- vrste datotek in datotečnih pripon, ki jih želite pregledati
- kombinacijo različnih načinov zaznavanja
- ravni čiščenja itd.

Če želite odpreti okno z nastavitvami kliknite **ThreatSense** v naprednih nastavitvah za vsak modul, ki uporablja tehnologijo ThreatSense (glejte spodaj). Za različne primere varnosti boste morda potrebovali različne konfiguracije. Orodje ThreatSense je zato mogoče posamezno konfigurirati za naslednje module zaščite:

- Sprotna zaščita datotečnega sistema
- Pregledovanje v mirovanju
- Zagonski pregled
- Zaščita dokumentov
- Zaščita e-poštnega odjemalca
- Zaščita spletnega dostopa
- Pregled računalnika

Parametri za ThreatSense so optimizirani za vsak modul. Če spremenite te parametre, lahko močno vplivate na delovanje računalnika. Če parametre na primer spremenite tako, da vedno pregledajo samoustvarjalne arhive, ali

omogočite napredno hevristiko v modulu za sprotno zaščito datotečnega sistema, lahko računalnik začne delovati počasneje (običajno so s temi načini pregledane samo nove datoteke). Zato priporočamo, da za noben modul, razen za pregled računalnika, ne spreminjate privzetih parametrov orodja ThreatSense.

Predmeti za pregled

V tem razdelku lahko določite, v katerih komponentah računalnika in datotekah bo izveden pregled za morebitne infiltracije.

Delovni pomnilnik – s pregledom je ugotovljeno, ali so v računalniku grožnje, ki napadejo delovni pomnilnik sistema.

Zagonski sektorji/UEFI – S pregledom se ugotovi, ali je zlonamerna programska oprema v glavnih zagonskih zapisih. Več o vmesniku UEFI lahko preberete v slovarju izrazov.

E–poštne datoteke – program podpira te pripone: DBX (Outlook Express) in EML.

Arhivi – program podpira naslednje pripone: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE in mnoge druge.

Samoraztezni arhivi – samoraztezni arhivi (SFX) so arhivi, ki se lahko raztezajo sami.

Samoustvarjalni arhivi – po izvajanju se samoustvarjalni arhivi (v nasprotju s standardnimi vrstami arhivov) v pomnilniku raztegnejo. Poleg standardnih statičnih arhivov (UPX, yoda, ASPack, FSG itn.) lahko pregledovalnik s posnemanjem kode prepozna še številne druge vrste arhivov.

Možnosti pregleda

Izberite načine, ki jih želite uporabiti pri preverjanju morebitnih infiltracij. Na voljo so naslednje možnosti:

Hevristika – hevristika je algoritem, ki analizira (zlonamerno) dejavnost programov. Njena glavna prednost je ta, da zna prepoznati zlonamerno programsko opremo, ki prej ni obstajala ali je prejšnja različica orodja za zaznavanje ni poznala. Njena pomanjkljivost pa je (zelo majhna) možnost lažnega preplaha.

Napredna hevristika/definicije DNA – napredna hevristika je enolični hevristični algoritem, ki ga je razvilo podjetje ESET in je optimiziran za zaznavanje računalniških črvov in trojanskih konjev ter napisan z visoko razvitimi programskimi jeziki. Uporaba napredne hevristike izdelkom ESET močno poveča zmogljivost zaznavanja groženj. Z definicijami je mogoče zanesljivo zaznati in prepoznati viruse. Nov samodejni sistem posodabljanja omogoča, da so nove definicije na voljo že v nekaj urah po odkritju grožnje. Pomanjkljivost definicij je, da zaznajo le viruse, ki jih poznajo (oziroma rahlo spremenjene različice teh virusov).

Čiščenje

Z nastavitvami čiščenja je določeno delovanje programa ESET Internet Security med čiščenjem predmetov. Na voljo so 4 ravni čiščenja:

ThreatSense ima naslednje ravni popravljanja (tj. čiščenja).

Popravljanje s programom ESET Internet Security

Raven čiščenja	Opis
Vedno popravi zaznani element	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih redkih primerih (na primer pri sistemskih datotekah) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.
Popravi zaznani element, če je varno, sicer ohrani	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih primerih (na primer pri sistemskih datotekah ali arhivih z neokuženimi in okuženimi datotekami) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.
Popravi zaznani element, če je varno, sicer vprašaj	Poskuša popraviti zaznani element med čiščenjem predmetov. V nekaterih primerih, če ni mogoče izvesti nobenega dejanja, se končnemu uporabniku prikaže interaktivno opozorilo in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta nastavitev je priporočljiva v večini primerov.
Vedno vprašaj končnega uporabnika	Končnemu uporabniku se med čiščenjem predmetov prikaže interaktivno okno in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta raven je namenjena bolj izkušenim uporabnikom, ki vedo, kako ukrepati v primeru zaznanega elementa.

Izključitve

Pripona je del imena datoteke, ki je od drugega dela imena ločena s piko. S pripono je označena vrsta in vsebina datoteke. V tem razdelku z nastavitvami orodja ThreatSense je mogoče določiti vrste datotek za pregledovanje.

Ostalo

Pri konfiguriranju parametrov orodja ThreatSense za pregled računalnika na zahtevo so na voljo tudi naslednje možnosti v razdelku **Ostalo**:

Preglej nadomestne podatkovne tokove (ADS) – nadomestni podatkovni tokovi, ki jih uporablja datotečni sistem NTFS, so povezave z datotekami in mapami, ki jih navadne tehnike pregledovanja ne zaznajo. Mnoge infiltracije se poskušajo izogniti zaznavanju tako, da se predstavijo kot nadomestni podatkovni tokovi.

Zaženi preglede v ozadju z nizko pomembnostjo – vsak pregled porabi določeno količino sistemskih sredstev. Če delate s programi, ki porabijo veliko sistemskih sredstev, lahko aktivirate pregledovanje v ozadju z nizko prioriteto in prihranite sredstva za svoje programe.

Zapiši v dnevnik vse predmete – dnevnik pregledovanja prikaže vse pregledane datoteke v samorazteznih arhivih, tudi tiste, ki niso okužene (to lahko ustvari veliko podatkov v dnevniku pregledovanja in poveča velikost datoteke dnevnika pregledovanja).

Omogoči pametno optimizacijo – če je pametna optimizacija omogočena, so uporabljene najbolj optimalne nastavitve, ki zagotavljajo najbolj učinkovito pregledovanje pri najvišjih hitrostih pregledovanja. Različni moduli zaščite pregledujejo na pameten način, kar pomeni, da uporabljajo različne načine pregledovanja, ki jih uporabijo za določene vrste datotek. Če je pametna optimizacija onemogočena, so pri pregledu uporabljene le uporabniško določene nastavitve v jedru ThreatSense posameznih modulov.

Ohrani časovni žig zadnjega dostopa – izberite to možnost, če želite ohraniti originalni čas dostopa do pregledane datoteke, namesto da bi se ta posodobil (na primer za uporabo s sistemi za varnostno kopiranje podatkov).

Omejitve

V razdelku »Omejitve« lahko določite največjo velikost predmetov in ravni gnezdenja arhivov, ki bodo pregledani:

Nastavitve predmeta

Največja velikost predmeta – določa največjo velikost predmetov, ki bodo pregledani. Protivirusni modul bo pregledoval samo predmete, ki so manjši od določene velikosti. To možnost naj spreminjajo le napredni uporabniki, ki imajo morda določene razloge, da iz pregledovanja izključijo večje predmete. Privzeta vrednost: neomejeno.

Najdaljši čas pregledovanja predmeta (s) – določi največjo časovno vrednost za pregled datotek v vsebniškem predmetu (na primer arhivski datoteki RAR/ZIP ali e-poštnem sporočilu z več prilogami. Ta nastavitev ne velja za samostojne datoteke. Če je bila vnesena uporabniško določena vrednost in je čas potekel, se pregled konča takoj, ko je mogoče, ne glede na to, ali je pregled vseh datotek v vsebniškem predmetu zaključen.
V primeru arhiva z velikimi datotekami se pregled ustavi šele, ko je datoteka iz arhiva ekstrahirana (na primer: uporabniško določena spremenljivka je 3 sekunde, ekstrakcija datoteke pa traja 5 sekund). Preostale datoteke v arhivu po poteku določenega časa ne bodo pregledane.
Za omejitev časa pregledovanja, vključno z velikimi arhivi, uporabite možnosti **Največja velikost predmeta** in **Največja velikost datoteke v arhivu** (ni priporočeno zaradi morebitnih varnostnih tveganj).
Privzeta vrednost: neomejeno.

Nastavitev pregledovanja arhiva

Raven gnezdenja arhiva – določa največjo globino pregledovanja arhivov. Privzeta vrednost: 10.

Največja velikost datoteke v arhivu – ta možnost omogoča, da določite največjo velikost datotek v arhivu (ko so ekstrahirane), ki bodo pregledane. Privzeta vrednost je: **3 GB**.

priporočamo, da ne spreminjate privzetih vrednosti, v normalnih okoliščinah to običajno ni potrebno.

Starševski nadzor

Možnost **Omogoči starševski nadzor** vključuje starševski nadzor v programu ESET Internet Security. Kliknite možnost **Uredi** ob možnosti Uporabniški računi, da povežete uporabniške račune sistema Windows, ki jih uporablja starševski nadzor, z določenimi uporabniki za omejitev njihovega dostopa do neprimerne ali škodljive vsebine v internetu.

Uporabniški računi

V razdelku Napredne nastavitve > **Zaščite** > **Zaščita spletnega dostopa** > **Starševski nadzor** > **Uporabniški računi** > **Uredi** lahko povežete uporabniške račune sistema Windows, ki jih uporablja starševski nadzor, z določenimi uporabniki za omejitev njihovega dostopa do neprimerne ali škodljive vsebine v internetu.

Stolpci

Račun sistema Windows – ime uporabnika.

Omogočeno – ko je možnost omogočena, je starševski nadzor za navedeni uporabniški račun aktiven.

Domena – ime domene, ki ji pripada uporabnik.

Rojstni datum – starost uporabnika tega računa.

Elementi kontrolnika

Dodaj – odpre se pogovorno okno Delo z uporabniškimi računi.

Uredi – ta možnost omogoča urejanje izbranih računov.

Izbriši – izbriše izbrani račun.

Osveži – če ste dodali uporabniški račun, lahko program ESET Internet Security osveži seznam uporabniških računov brez ponovnega odpiranja tega okna.

Nastavitve uporabniškega računa

To okno ima tri zavihke:

Splošno

Omogočite gumb za preklop ob možnosti **Omogočeno**, da vklopite starševski nadzor za spodaj izbrani račun Windows.

Najprej **izberite** Windows račun v računalniku. Omejitve, nastavljene v starševskem nadzoru, vplivajo le na standardne račune sistema Windows. Skrbniški računi lahko preglasijo omejitve.

Če račun uporablja starš, izberite **Starševski račun**.

Nastavite **Rojstni datum otroka** za račun, da določite raven dostopa in nastavite pravila za dostop do spletnih strani, ki so primerne za to starost.

Zapisovanje v dnevnik

Program ESET Internet Security shrani vse pomembne dogodke v dnevniško datoteko, ogledate pa si jih lahko neposredno iz glavnega menija. Kliknite **Orodja** > **Dnevniške datoteke** in nato v spustnem meniju **Dnevnik** izberite možnost **Starševski nadzor**.

- **Diagnostika** – zabeleži podatke, ki so potrebni za natančno prilagajanje programa.
- **Informacije** – zabeleži informativna sporočila, vključno z dovoljenimi ter blokiranimi izjemami in vsemi zgornjimi zapisi.
- **Opozorilo** – zabeleži kritične napake in opozorilna sporočila.
- **Brez** – dnevniki se ne ustvarijo.

Izjeme

Če ustvarite izjemo, lahko uporabniku dovolite ali preprečite dostop do spletnih mest, ki niso na seznamu izjem. To je uporabno, če želite nadzorovati dostop do določenih spletnih mest, ne da bi uporabljali kategorije. Izjeme, ustvarjene za en račun, lahko kopirate in uporabite za drug račun. To je uporabno, ko želite ustvariti identična pravila za otroke podobne starosti.

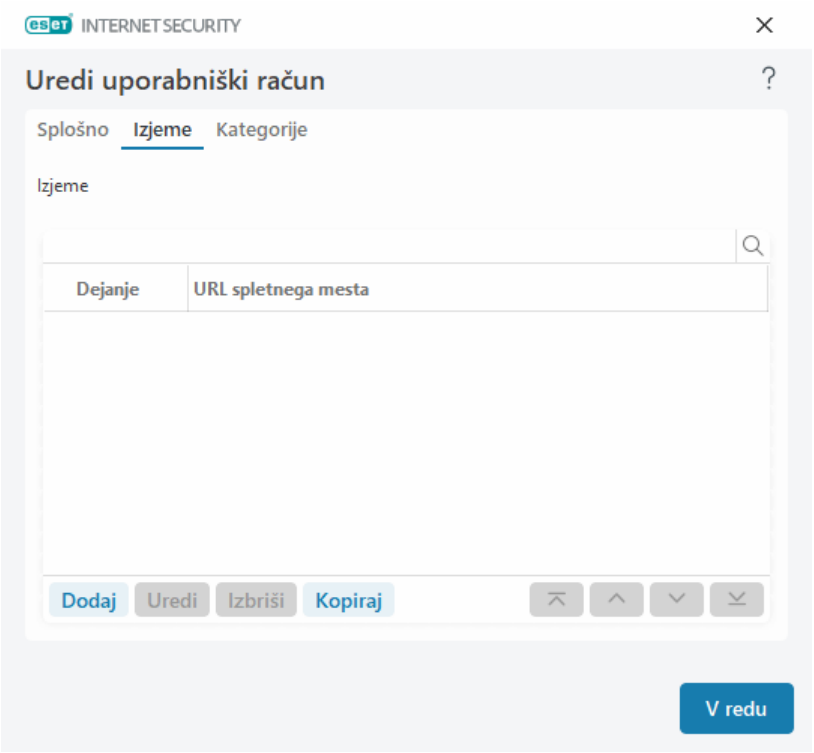
Če želite ustvariti novo izjemo, kliknite **Dodaj**. V spustnem meniju določite **Dejanje** (npr. **Blokiraj**), vnesite **URL spletnega mesta**, za katerega velja ta izjema in kliknite **V redu**. Izjema bo dodana na seznam obstoječih izjem, pri čemer bo prikazano njeno stanje.

Dodaj – ustvari novo izjemo.

Uredi – uredite lahko naslov **URL spletnega mesta** ali **Dejanje izbrane izjeme**.

Izbriši – odstrani izbrano izjemo.

Kopiraj – izbere uporabnika s spustnega menija, s katerega želite kopirati ustvarjeno izjemo.

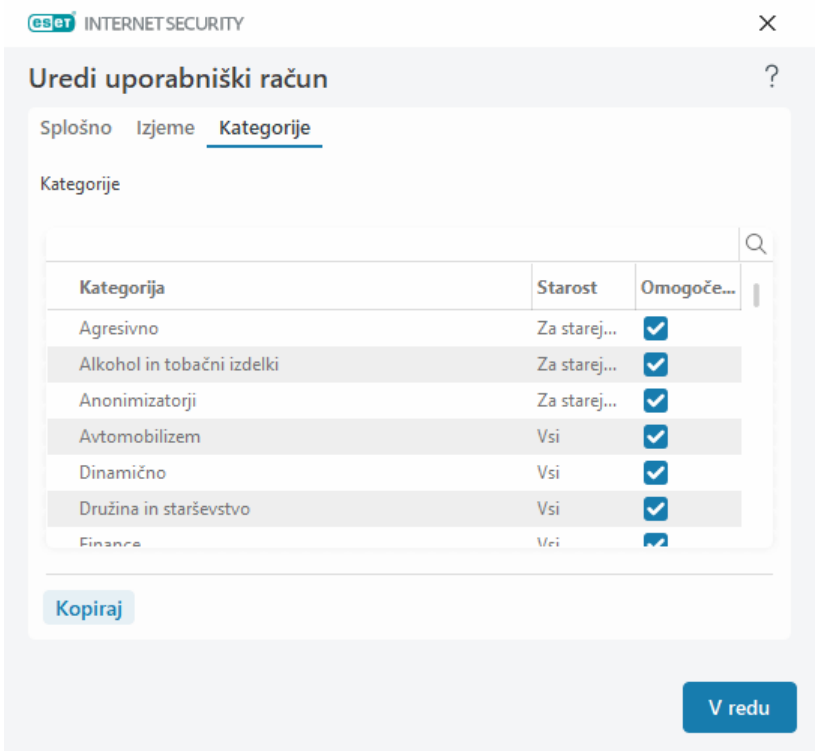


Izjeme, ki jih določite, imajo prednost pred kategorijami, določenimi za izbrane račune. Če je za račun na primer blokirana kategorija **Novice**, vendar določite neko spletno stran z novicami kot dovoljeno izjemo, lahko račun dostopa do dovoljene spletne strani. Vse spremembe si lahko ogledate v razdelku Izjeme.

Kategorije

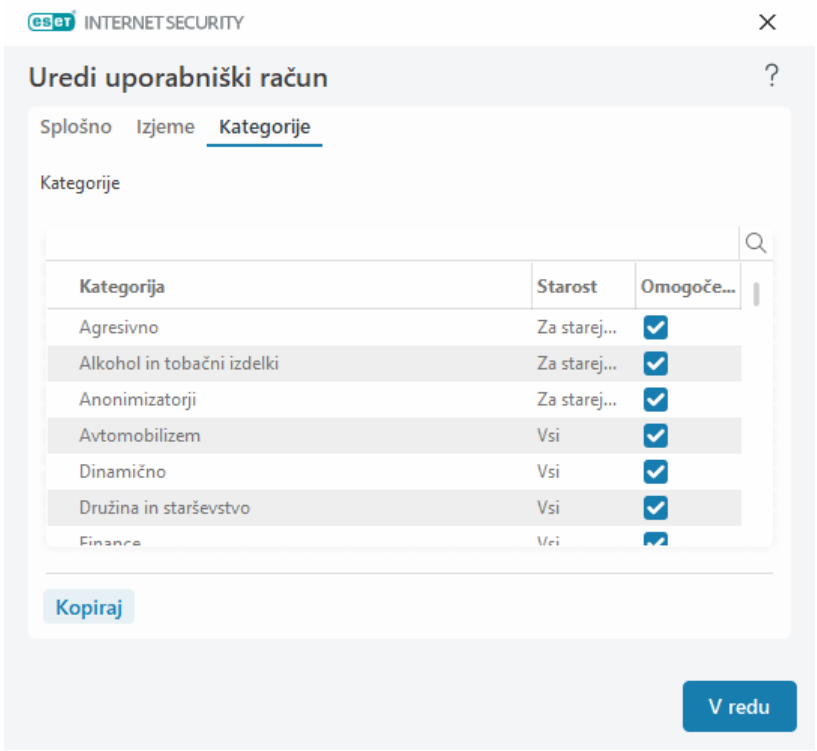
Na zavihku **Kategorije** lahko določite splošne kategorije spletnih mest, ki jih želite blokirati ali dovoliti za posamezni račun. Če želite dovoliti kategorijo, izberite potrditveno polje zraven nje. Če potrditveno polje pustite prazno, kategorija za ta račun ne bo dovoljena.

Kopiraj – omogoča kopiranje seznama blokiranih ali dovoljenih kategorij iz obstoječega spremenjenega računa.



Kategorije

Označite potrditvena polja na stolpcu **Omogočeno** ob posamezni kategoriji, da ji dovolite delovanje. Če polje ni označeno, kategorija ne bo dovoljena za ta račun.



Tukaj je nekaj primerov kategorij (skupin), ki jih uporabniki morda ne poznajo:

- **Razno** – običajno zasebni (lokalni) naslovi IP, kot je internet 127.0.0.0/8, 192.168.0.0/16 itd. Ko prejmete kodo napake 403 ali 404, se spletno mesto prav tako ujema s to kategorijo.

- **Nerešeno** – v tej kategoriji so spletne strani, ki so nerešene zaradi napake pri vzpostavljanju povezave z mehanizmom zbirke podatkov starševskega nadzora.
- **Nerazvrščeno** – neznane spletne strani, ki še niso v zbirki podatkov starševskega nadzora.
- **Dinamično** – spletne strani, ki preusmerjajo na druge strani na drugih spletnih mestih.

Zaščita brskalnika

Zaščita brskalnika je dodatna plast zaščite za vašo varnost in zasebnost, ki ščiti pomnilnik brskalnika pred vpogledom drugih procesov, povečuje zaščito pred zapisovalniki tipkanja in preprečuje lepljenje vseh podatkov, povezanih s spletnimi plačili, ki jih je spremenila zlonamerna programska oprema, iz odložišča v zaščiten brskalnik. Če želite konfigurirati zaščito brskalnika, odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita brskalnika** in izberite med naslednjimi možnostmi konfiguracije:

- Varno bančništvo in brskanje
- Seznam dovoljenih datotek za zaščito brskalnika
- Okvir brskalnika

Varno bančništvo in brskanje

Varno bančništvo in brskanje lahko konfigurirate v razdelku Napredne nastavitve > **Zaščite** > **Zaščita brskalnika** > **Varno bančništvo in brskanje**.

Varno bančništvo in brskanje

Omogočanje funkcije Varno bančništvo in brskanje – ko je omogočena funkcija Varno bančništvo in brskanje, se vsi podprti spletni brskalniki privzeto zaženejo v varnem načinu.

Zaščita brskalnika

Omogočite funkcijo **Zaščiti vse brskalnike**, da se vsi podprti spletni brskalniki zaženejo v varnem načinu.

Način za nameščanje razširitev – s spustnega menija lahko izberete razširitve, katerim je dovoljena namestitev v brskalniku, ki ga ščiti ESET:

- **Bistvene razširitve** – le najpomembnejše razširitve, ki jih je razvil posamezni razvijalec brskalnika.
- **Vse razširitve** – vse razširitve, ki jih podpira posamezni brskalnik.

> Spreminjanje načina namestitve razširitve ne vpliva na predhodno nameščene razširitve brskalnika:

Zaščiten brskalnik

Izboljšana zaščita pomnilnika – če je možnost omogočena, bo pomnilnik zaščitenega brskalnika zaščiten pred pregledovanjem v okviru drugih procesov.

Zaščita tipkovnice – če je možnost omogočena, bodo informacije, vnesene v zaščiten brskalnik prek tipkovnice, skrite pred drugimi programi. To izboljša zaščito pred zapisovalniki tipkanja.

Zaščita odložišča – če je ta možnost omogočena, ESET Internet Security prepreči lepljenje vseh podatkov, povezanih s spletnimi plačili, ki jih je spremenila zlonamerna programska oprema, iz odložišča v zaščiten brskalnik. To zagotavlja zaščito pred morebitnimi spremembami, ki jih je ustvarila zlonamerna programska oprema.

Okvir brskalnika – Prilagodite nastavitve prikaza za okvir brskalnika v zaščitenih brskalnikih.

Seznam dovoljenih datotek za zaščito brskalnika – Upravljajte datoteke, dodane na seznam dovoljenih datotek za zaščito brskalnika.

Zasebnost in varnost brskalnika

Omogočanje funkcije Zasebnost in varnost brskalnika – če onemogočite to funkcijo, bo razširitev Zasebnost in varnost brskalnika odstranjena iz vseh podprtih brskalnikov v vseh računih Windows.

Prikaz obvestil funkcije Zasebnost in varnost brskalnika – če je ta možnost omogočena, bo izdelek ESET Internet Security prikazal obvestila funkcije Zasebnost in varnost brskalnika.

Pregledovalnik skriptov brskalnikov

Omogočanje naprednega pregledovanja skriptov brskalnika – če je ta možnost omogočena, protivirusni pregledovalnik preveri vse programe JavaScript, ki jih izvajajo spletni brskalniki.

00

Nadzor naprave

ESET Internet Security omogoča samodejni nadzor naprav (CD/DVD/USB/itd.). S tem modulom lahko blokirate ali prilagodite razširjene filtre in dovoljenja ter izberete način, kako bo uporabnik dostopal do naprave in jo uporabljal. To pride prav, če želi skrbnik računalnika preprečiti uporabo naprav z neželeno vsebino.

Podprte zunanje naprave:

- Shramba diska (HDD, izmenljivi disk USB)
- CD/DVD
- Tiskalnik USB
- Shramba FireWire
- Bluetooth Naprava
- Bralnik pametnih kartic
- Naprava za zajem slik
- Modem

- LPT/COM vrata
- Prenosna naprava (naprave, ki se napajajo iz baterije, kot so predvajalniki predstavnosti, pametni telefoni, naprave plug-and-play itd.)
- Vse vrste naprav

Možnosti nastavitev za nadzor naprav lahko spreminjate v razdelku Napredne nastavitve > **Zaščite** > **Nadzor naprav**.

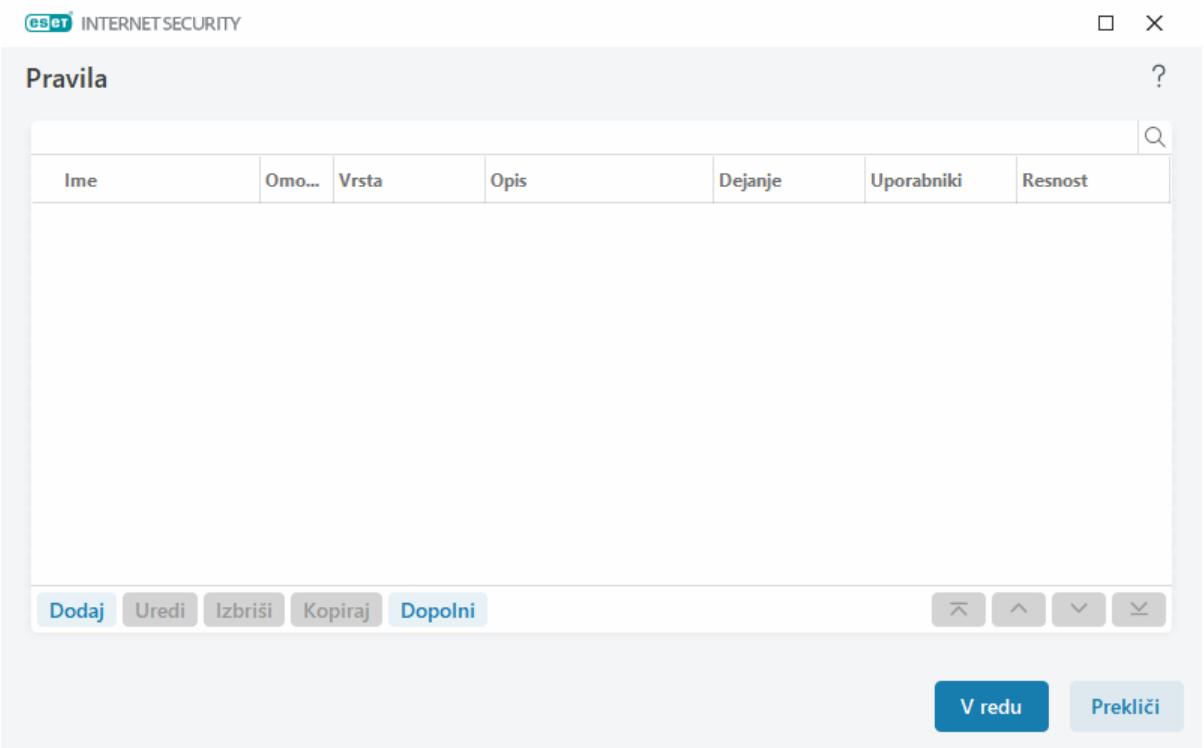
Če želite omogočiti funkcijo nadzora naprav v ESET Internet Security, kliknite gumb za preklop **Omogoči nadzor naprav**; spremembo uveljavite tako, da znova zaženete računalnik. Ko je funkcija nadzora naprav omogočena, lahko v oknu Urejevalnik pravil določite **pravila**.

> Ustvarite lahko različne skupine naprav, za katere bodo uporabljena različna pravila. Ustvarite lahko tudi samo eno skupino naprav, za katero bo uporabljeno pravilo z dejanjem **Dovoli** ali **Blokiraj pisanje**. Tako zagotovite, da bo nadzor naprav blokiral neprepoznane naprave, ki so priključene v računalnik.

Če vstavite napravo, ki je blokirana z obstoječim pravilom, se prikaže okno z obvestilom in dostop do naprave ni mogoč.

Urejevalnik pravil za nadzor naprave

V oknu **Urejevalnik pravil za nadzor naprave** so prikazana obstoječa pravila, kjer lahko natančno nadzirate zunanje naprave, ki jih uporabniki priključijo na računalnik.

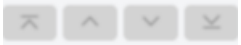


Določene naprave lahko omogočite ali blokirate za uporabnika ali skupino uporabnikov glede na dodatne parametre naprave, ki jih je mogoče določiti v konfiguraciji pravila. Na seznamu pravil je več opisov pravila, kot so ime, vrsta zunanje naprave, dejanje, ki se izvede ob priključitvi zunanje naprave na računalnik, in resnost beleženja v dnevnik. Glejte tudi Dodajanje pravil za nadzor naprave.

Če želite upravljati pravilo, kliknite **Dodaj** ali **Uredi**. Če želite ustvariti novo pravilo z vnaprej določenimi možnostmi, ki se uporabljajo za drugo izbrano pravilo, kliknite **Kopiraj**. Nize XML, ki se prikažejo, ko kliknete pravilo, lahko kopirate v odložišče. Skrbniki sistema lahko s temi nizi XML izvozijo ali uvozijo te podatke in jih uporabijo.

Če pritisnete tipko **CTRL** in kliknete, lahko izberete več pravil in uporabite dejanja, kot je brisanje ali premikanje na seznamu navzgor ali navzdol, za vsa izbrana pravila. S potrditvenim poljem **Omogočeno** onemogočite ali omogočite pravilo; to je lahko koristno, če želite pravilo obdržati.

Če želite samodejno dopolniti parametre izmenljivega nosilca podatkov za naprave, priključene v računalnik, kliknite **Dopolni**.

Pravila so navedena po prednosti, in sicer so pravila z višjo prednostjo bližje vrhu. Pravila lahko premaknete tako, da kliknete  **Vrh/gor/dol/dno**. Premikate lahko posamezna pravila ali skupine pravil.

Vnose v dnevniku si lahko ogledate v glavnem oknu programa > **Orodja** > Dnevniške datoteke.

Dnevnik nadzora naprave zabeleži vse sprožitve nadzora naprave.

Zaznane naprave

Gumb **Dopolni** omogoča pregled vseh trenutno povezanih naprav s temi podatki: vrsta naprave, dobavitelj naprave, model in serijska številka (če je na voljo). Če si želite ogledati vse skrite naprave, izberite **Prikaži skrite naprave**.

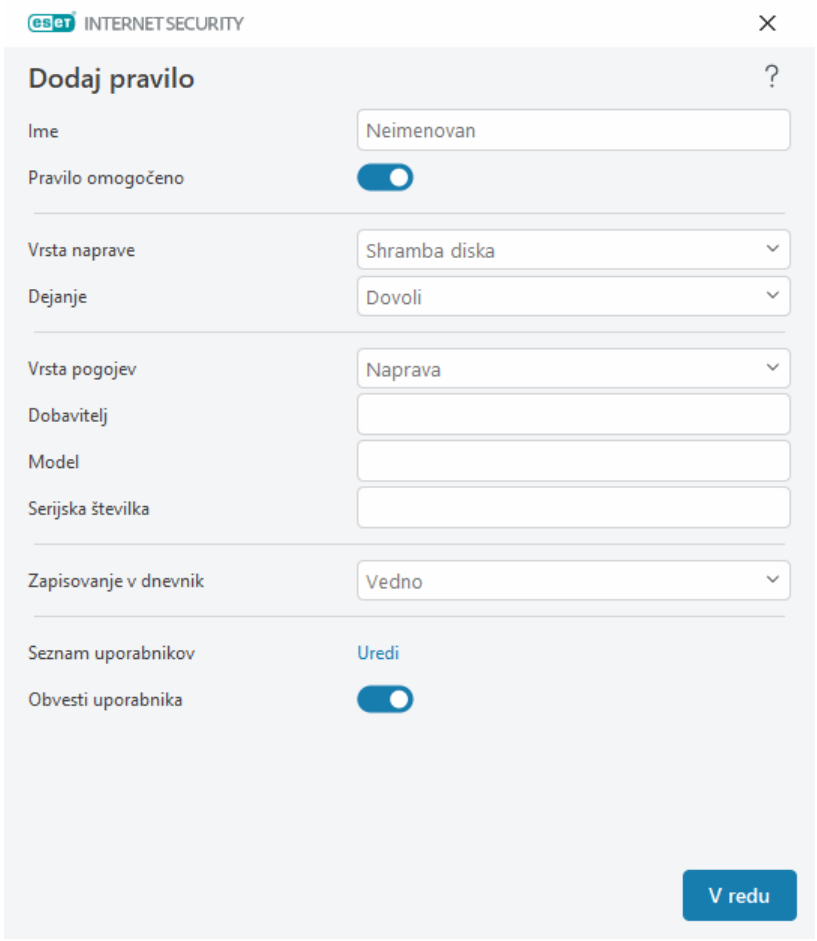
Na seznamu zaznanih naprav izberite napravo in kliknite **V redu**, če želite dodati pravilo za nadzor naprav z vnaprej določenimi podatki (vse nastavitve lahko prilagodite).

Naprave v načinu nizke porabe energije (stanje pripravljenosti) so označene z opozorilno ikono . Če želite omogočiti gumb **V redu** in dodati pravilo za to napravo:

- ponovno povežite napravo
- uporabite napravo (zaženite na primer aplikacijo Kamera v sistemu Windows, da zbudite spletno kamero)

Dodajanje pravil za nadzor naprav

S pravilom za nadzor naprav določite dejanje, ki se izvede, ko napravo, ki izpolnjuje pogoje pravila, priključite v računalnik.



V polje **Ime** vnesite opis pravila, da ga boste lažje prepoznali. Kliknite gumb za preklop ob možnosti **Pravilo omogočeno**, da onemogočite ali omogočite to pravilo; to je lahko uporabno, če ne želite trajno izbrisati pravila.

Vrsta naprave

V spustnem meniju izberite vrsto zunanje naprave (shramba diska/prenosna naprava/Bluetooth/FireWire/...). Podatki o vrsti naprave so zbrani iz operacijskega sistema in so prikazani v upravitelju naprav sistema, če je naprava priključena v računalnik. Naprave za shranjevanje vključujejo zunanje diske ali bralnike pomnilniških kartic, ki so povezani prek vrat USB ali FireWire. Med bralnike pametnih kartic spadajo vsi bralniki pametnih kartic z vdelanim integriranim vezjem, na primer kartice SIM ali kartice za preverjanje pristnosti. Primeri naprav za zajem slik so optični bralniki in kamere. Ker te naprave vsebujejo samo informacije o dejanjih, informacij o uporabnikih pa ne, jih lahko blokirate samo globalno.

Dejanje

Dostop do naprav, ki niso namenjene shranjevanju, je lahko dovoljen ali blokiran. Pravila za naprave za shranjevanje pa omogočajo izbiro ene od teh nastavitev pravic:

- **Dovoli** – omogočen je poln dostop do naprave.
- **Blokiraj** – dostop do naprave je blokiran.
- **Zapiši blokiranje** – omogočeno je le branje v napravi.
- **Opozori** – vsakič ko priključite napravo, boste obveščeni, ali je dostop dovoljen/blokiran, poleg tega bo ustvarjen vnos v dnevnik. Računalnik si naprav ne zapomni, zato bo obvestilo prikazano vsakič, ko priključite isto napravo.

Ne pozabite, da niso vsa dejanja (dovoljenja) na voljo za vse vrste naprav. Če je naprava namenjena za

shranjevanje, so na voljo vsa štiri dejanja. Pri napravah, ki niso namenjene za shranjevanje, so na voljo le tri dejanja (dejanje **Zapiši blokiranje** na primer ni na voljo za naprave Bluetooth, kar pomeni, da je naprave Bluetooth mogoče le omogočiti, blokirati ali opozoriti).

Vrsta pogojev

Izberite možnost **Skupina naprav** ali **Naprava**.

Spodaj prikazane dodatne parametre lahko uporabimo za podrobno prilagajanje pravil za posamezne naprave. Vsi parametri omogočajo razlikovanje med velikimi in malimi črkam in podpirajo nadomestne znake (*, ?):

- **Dobavitelj** – filtriranje po imenu ali ID-ju dobavitelja.
- **Model** – dano ime naprave.
- **Serijska številka** – zunanje naprave imajo običajno svoje serijske številke. Če je nosilec podatkov CD/DVD, je to serijska številka nosilca podatkov in ne pogona CD.

i če ne določite teh treh parametrov, bo pravilo med ujemanjem ta polja prezrlo. Parametri za filtriranje v vseh besedilnih poljih razlikujejo med velikimi in malimi črkami in podpirajo nadomestne znake (vprašaj (?) predstavlja en znak, medtem ko zvezdica (*) predstavlja niz z nič ali več znaki).

i če si želite ogledati podatke o napravi, ustvarite pravilo za to vrsto naprav, priključite napravi v računalnik in nato preverite podrobnosti naprave v dnevniku nadzora naprave.

Zapisovanje v dnevnik

Program ESET Internet Security shrani vse pomembne dogodke v dnevniško datoteko, ogledate pa si jih lahko neposredno iz glavnega menija. Kliknite **Orodja** > **Dnevniške datoteke** in nato v spustnem meniju **Dnevnik** izberite možnost **Nadzor naprav**.

- **Vedno** – v dnevnik zapiše vse dogodke.
- **Diagnostika** – zabeleži podatke, ki so potrebni za natančno prilagajanje programa.
- **Informacije** – zabeleži informativna sporočila, vključno s sporočili o uspešnem posodabljanju in vsemi zgornjimi zapisi.
- **Opozorilo** – zabeleži kritične napake in opozorilna sporočila.
- **Brez** – dnevniki se ne ustvarijo.

Seznam uporabnikov

Pravila lahko omejite na določene uporabnike ali skupine uporabnikov tako, da jih dodate na Seznam uporabnikov s klikom možnosti **Uredi** zraven možnosti **Seznam uporabnikov**.

- **Dodaj** – odpre razdelek **Vrste predmeta: Uporabniki ali skupine** – pogovorno okno, kjer lahko izberete želene uporabnike.
- **Odstrani** – odstrani izbranega uporabnika iz filtra.

Omejitve seznama uporabnikov

Seznama uporabnikov ni mogoče določiti za pravila posameznih vrst naprav:

- Tiskalnik USB
- Naprava Bluetooth
- Bralnik pametnih kartic
- Naprava za zajem slik
- Modem
- Vrata LPT/COM

Obvesti uporabnika – če vstavite napravo, ki je blokirana z obstoječim pravilom, se prikaže okno z obvestilom.

Skupine naprav

Naprava, ki je priključena v računalnik, morda predstavlja varnostno tveganje.

Okno s skupinami naprav je razdeljeno na dva dela. V desnem delu okna je seznam naprav, ki spadajo v posamezno skupino, v levem delu okna pa so ustvarjene skupine. Izberite skupino za prikaz naprav v desnem podoknu.

Ko odprete okno s skupinami naprav in izberete skupino, lahko dodajate naprave na seznam ali jih z njega odstranite. Naprave lahko dodate v skupino tudi tako, da jih uvozite iz datoteke. Druga možnost je, da kliknete gumb **Dopolni** in vse naprave, ki so priključene v računalnik, bodo prikazane v oknu **Zaznane naprave**. Če želite naprave dodati v skupino, jih izberite na seznamu in kliknite **V redu**.

Elementi kontrolnika

Dodaj – Dodate lahko skupino, tako da vnesete njeno ime, ali napravo v obstoječo skupino, odvisno od tega, v katerem delu okna kliknete gumb.

Uredi – omogoča urejanje imena izbrane skupine ali parametrov naprave (dobavitelja, modela, serijske številke).

Izbriši – izbriše izbrano skupino ali napravo, odvisno od tega, v katerem delu okna ste kliknili gumb.

Uvoz – uvozi seznam naprav iz besedilne datoteke. Za uvoz naprav iz besedilne datoteke je potrebno pravilno oblikovanje:

- Vsaka naprava se začne v novi vrstici.
- Vrednosti za **Dobavitelj**, **Model** in **Serijska številka** morajo biti prisotne za vsako napravo ter ločene z vejico.

Tukaj je primer vsebine besedilne datoteke:

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

Izvoz – izvozi seznam naprav v datoteko.

Gumb **Dopolni** omogoča pregled vseh trenutno povezanih naprav s temi podatki: vrsta naprave, dobavitelj naprave, model in serijska številka (če je na voljo).

Dodaj napravo

Če želite dodati napravo v obstoječo skupino, v desnem oknu kliknite **Dodaj**. Spodaj prikazane dodatne parametre lahko uporabimo za podrobno prilagajanje pravil za posamezne naprave. Vsi parametri omogočajo razlikovanje med velikimi in malimi črkam in podpirajo nadomestne znake (*, ?):

- **Dobavitelj** – filtriranje po imenu ali ID-ju dobavitelja.
- **Model** – dano ime naprave.
- **Serijska številka** – zunanje naprave imajo običajno svoje serijske številke. Če je nosilec podatkov CD/DVD, je to serijska številka nosilca podatkov in ne pogona CD.
- **Opis** – vaš opis naprave za boljšo organizacijo.

> Če ne določite teh treh parametrov, bo pravilo med ujemanjem ta polja prezrlo. Parametri filtriranja v vseh besedilnih poljih razlikujejo med velikimi in malimi črkami ter podpirajo nadomestne znake (vprašaj [?] predstavlja en znak, zvezdica [*] pa niz ničel ali več znakov).

Če želite spremembe shraniti, kliknite **V redu**. Če želite zapreti okno **Skupine naprav** brez shranjevanja sprememb, kliknite **Prekliči**.

> Ko ustvarite skupino naprav, morate dodati novo pravilo za nadzor naprav za ustvarjeno skupino naprav in izbrati želeno dejanje.

Ne pozabite, da niso vsa dejanja (dovoljenja) na voljo za vse vrste naprav. Če gre za napravo za shranjevanje, so na voljo vsa štiri dejanja. Pri napravah, ki niso namenjene za shranjevanje, so na voljo le tri dejanja (dejanje **Blokiraj pisanje** na primer ni na voljo za naprave Bluetooth, kar pomeni, da je naprave Bluetooth mogoče le omogočiti, blokirati ali opozoriti).

Zaščita spletne kamere

Zaščita spletne kamere vas obvešča o procesih in programih, ki dostopajo do spletne kamere računalnika. Če program poskuša pridobiti dostop do kamere, prejmete obvestilo, v katerem lahko **dovolite** ali **blokirate** dostop. Barva okna z opozorilom je odvisna od ugleda programa.

Možnosti nastavitev za zaščito spletne kamere je mogoče urejati v razdelku Napredne nastavitve > **Zaščite** > **Nadzor naprav** > **Zaščita spletne kamere**.

Če želite aktivirati funkcijo zaščite spletne kamere v programu ESET Internet Security, omogočite gumb za preklop ob možnosti **Omogoči zaščito spletne kamere**.

Ko je zaščita spletne kamere omogočena, se aktivirajo **Pravila**, kar omogoča odpiranje okna za Urejevalnik pravil.

Če želite s pravilom izklopiti opozorila za programe, ki so bili spremenjeni, vendar imajo še vedno veljaven digitalni podpis (npr. za posodobitev programa), omogočite gumb za preklop ob možnosti **Onemogoči opozorila o dostopu do spletne kamere za spremenjene programe**.

Urejevalnik pravil zaščite spletne kamere

V tem oknu so navedena obstoječa pravila, v njem pa lahko nadzirate programe in postopke, ki dostopajo do spletne kamere računalnika glede na dejanje, ki ste ga izvedli.

Na voljo so naslednja dejanja:

- **Dovoli dostop**
- **Blokiraj dostop**

- **Vprašaj** (Če želi program dostop do kamere, vedno vprašaj uporabnika)

V razdelku **Obvesti** prekličite izbor potrditvenega polja, da prenehate prejemati obvestila, ko programi dostopajo do spletne kamere.

> Ilustrirana navodila
> Kako ustvariti in urejati pravila za spletne kamere v izdelku ESET Internet Security.

ThreatSense

ThreatSense je sestavljen iz veliko zapletenih načinov zaznavanja groženj. Ta tehnologija je proaktivna, kar pomeni, da ponuja zaščito tudi med začetno fazo širitve nove grožnje. Uporablja kombinacijo analize kode, posnemanja kode, splošnih definicij in definicij virusov, ki s skupnim delovanjem znatno izboljšajo varnost računalnika. Orodje za pregledovanje lahko nadzira več podatkovnih tokov hkrati in tako poveča učinkovitost ter stopnjo zaznavanja na najvišjo možno raven. ThreatSense tehnologija tudi uspešno odstrani korenske komplete.

Z možnostmi za nastavitev mehanizma tehnologije ThreatSense lahko določite več parametrov pregledovanja:

- vrste datotek in datotečnih pripon, ki jih želite pregledati
- kombinacijo različnih načinov zaznavanja
- ravni čiščenja itd.

Če želite odpreti okno z nastavitvami kliknite **ThreatSense** v naprednih nastavitvah za vsak modul, ki uporablja tehnologijo ThreatSense (glejte spodaj). Za različne primere varnosti boste morda potrebovali različne konfiguracije. Orodje ThreatSense je zato mogoče posamezno konfigurirati za naslednje module zaščite:

- Sprotna zaščita datotečnega sistema
- Pregledovanje v mirovanju
- Zagonski pregled
- Zaščita dokumentov
- Zaščita e-poštnega odjemalca
- Zaščita spletnega dostopa
- Pregled računalnika

Parametri za ThreatSense so optimizirani za vsak modul. Če spremenite te parametre, lahko močno vplivate na delovanje računalnika. Če parametre na primer spremenite tako, da vedno pregledajo samoustvarjalne arhive, ali omogočite napredno hevristiko v modulu za sprotno zaščito datotečnega sistema, lahko računalnik začne delovati počasneje (običajno so s temi načini pregledane samo nove datoteke). Zato priporočamo, da za noben modul, razen za pregled računalnika, ne spreminjate privzetih parametrov orodja ThreatSense.

Predmeti za pregled

V tem razdelku lahko določite, v katerih komponentah računalnika in datotekah bo izveden pregled za morebitne infiltracije.

Delovni pomnilnik – s pregledom je ugotovljeno, ali so v računalniku grožnje, ki napadejo delovni pomnilnik sistema.

Zagonski sektorji/UEFI – S pregledom se ugotovi, ali je zlonamerna programska oprema v glavnih zagonskih zapisih. Več o vmesniku UEFI lahko preberete v slovarju izrazov.

E–poštne datoteke – program podpira te pripone: DBX (Outlook Express) in EML.

Arhivi – program podpira naslednje pripone: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE in mnoge druge.

Samoraztezni arhivi – samoraztezni arhivi (SFX) so arhivi, ki se lahko raztezajo sami.

Samoustvarjalni arhivi – po izvajanju se samoustvarjalni arhivi (v nasprotju s standardnimi vrstami arhivov) v pomnilniku raztegnejo. Poleg standardnih statičnih arhivov (UPX, yoda, ASPack, FSG itn.) lahko pregledovalnik s posnemanjem kode prepozna še številne druge vrste arhivov.

Možnosti pregleda

Izberite načine, ki jih želite uporabiti pri preverjanju morebitnih infiltracij. Na voljo so naslednje možnosti:

Hevristika – hevristika je algoritem, ki analizira (zlonamerno) dejavnost programov. Njena glavna prednost je ta, da zna prepoznati zlonamerno programsko opremo, ki prej ni obstajala ali je prejšnja različica orodja za zaznavanje ni poznala. Njena pomanjkljivost pa je (zelo majhna) možnost lažnega preplaha.

Napredna hevristika/definicije DNA – napredna hevristika je enolični hevristični algoritem, ki ga je razvilo podjetje ESET in je optimiziran za zaznavanje računalniških črvov in trojanskih konjev ter napisan z visoko razvitimi programskimi jeziki. Uporaba napredne hevristike izdelkom ESET močno poveča zmogljivost zaznavanja groženj. Z definicijami je mogoče zanesljivo zaznati in prepoznati viruse. Nov samodejni sistem posodabljanja omogoča, da so nove definicije na voljo že v nekaj urah po odkritju grožnje. Pomanjkljivost definicij je, da zaznajo le viruse, ki jih poznajo (oziroma rahlo spremenjene različice teh virusov).

Čiščenje

Z nastavitvami čiščenja je določeno delovanje programa ESET Internet Security med čiščenjem predmetov. Na voljo so 4 ravni čiščenja:

ThreatSense ima naslednje ravni popravljanja (tj. čiščenja).

Popravljanje s programom ESET Internet Security

Raven čiščenja	Opis
Vedno popravi zaznani element	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih redkih primerih (na primer pri sistemskih datotekah) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.
Popravi zaznani element, če je varno, sicer ohrani	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih primerih (na primer pri sistemskih datotekah ali arhivih z neokuženimi in okuženimi datotekami) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.
Popravi zaznani element, če je varno, sicer vprašaj	Poskuša popraviti zaznani element med čiščenjem predmetov. V nekaterih primerih, če ni mogoče izvesti nobenega dejanja, se končnemu uporabniku prikaže interaktivno opozorilo in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta nastavitev je priporočljiva v večini primerov.
Vedno vprašaj končnega uporabnika	Končnemu uporabniku se med čiščenjem predmetov prikaže interaktivno okno in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta raven je namenjena bolj izkušenim uporabnikom, ki vedo, kako ukrepati v primeru zaznanega elementa.

Izključitve

Pripona je del imena datoteke, ki je od drugega dela imena ločena s piko. S pripono je označena vrsta in vsebina datoteke. V tem razdelku z nastavitvami orodja ThreatSense je mogoče določiti vrste datotek za pregledovanje.

Ostalo

Pri konfiguriranju parametrov orodja ThreatSense za pregled računalnika na zahtevo so na voljo tudi naslednje možnosti v razdelku **Ostalo**:

Preglej nadomestne podatkovne tokove (ADS) – nadomestni podatkovni tokovi, ki jih uporablja datotečni sistem NTFS, so povezave z datotekami in mapami, ki jih navadne tehnike pregledovanja ne zaznajo. Mnoge infiltracije se poskušajo izogniti zaznavanju tako, da se predstavijo kot nadomestni podatkovni tokovi.

Zaženi preglede v ozadju z nizko pomembnostjo – vsak pregled porabi določeno količino sistemskih sredstev. Če delate s programi, ki porabijo veliko sistemskih sredstev, lahko aktivirate pregledovanje v ozadju z nizko prioriteto in prihranite sredstva za svoje programe.

Zapiši v dnevnik vse predmete – dnevnik pregledovanja prikaže vse pregledane datoteke v samorazteznih arhivih, tudi tiste, ki niso okužene (to lahko ustvari veliko podatkov v dnevniku pregledovanja in poveča velikost datoteke dnevnika pregledovanja).

Omogoči pametno optimizacijo – če je pametna optimizacija omogočena, so uporabljene najbolj optimalne nastavitve, ki zagotavljajo najbolj učinkovito pregledovanje pri najvišjih hitrostih pregledovanja. Različni moduli zaščite pregledujejo na pameten način, kar pomeni, da uporabljajo različne načine pregledovanja, ki jih uporabijo za določene vrste datotek. Če je pametna optimizacija onemogočena, so pri pregledu uporabljene le uporabniško določene nastavitve v jedru ThreatSense posameznih modulov.

Ohrani časovni žig zadnjega dostopa – izberite to možnost, če želite ohraniti originalni čas dostopa do pregledane datoteke, namesto da bi se ta posodobil (na primer za uporabo s sistemi za varnostno kopiranje podatkov).

Omejitve

V razdelku »Omejitve« lahko določite največjo velikost predmetov in ravni gnezdenja arhivov, ki bodo pregledani:

Nastavitve predmeta

Največja velikost predmeta – določa največjo velikost predmetov, ki bodo pregledani. Protivirusni modul bo pregledoval samo predmete, ki so manjši od določene velikosti. To možnost naj spreminjajo le napredni uporabniki, ki imajo morda določene razloge, da iz pregledovanja izključijo večje predmete. Privzeta vrednost: neomejeno.

Najdaljši čas pregledovanja predmeta (s) – določi največjo časovno vrednost za pregled datotek v vsebniškem predmetu (na primer arhivski datoteki RAR/ZIP ali e-poštnem sporočilu z več prilogami. Ta nastavitev ne velja za samostojne datoteke. Če je bila vnesena uporabniško določena vrednost in je čas potekel, se pregled konča takoj, ko je mogoče, ne glede na to, ali je pregled vseh datotek v vsebniškem predmetu zaključen.
V primeru arhiva z velikimi datotekami se pregled ustavi šele, ko je datoteka iz arhiva ekstrahirana (na primer: uporabniško določena spremenljivka je 3 sekunde, ekstrakcija datoteke pa traja 5 sekund). Preostale datoteke v arhivu po poteku določenega časa ne bodo pregledane.
Za omejitev časa pregledovanja, vključno z velikimi arhivi, uporabite možnosti **Največja velikost predmeta** in **Največja velikost datoteke v arhivu** (ni priporočeno zaradi morebitnih varnostnih tveganj).
Privzeta vrednost: neomejeno.

Nastavitev pregledovanja arhiva

Raven gnezdenja arhiva – določa največjo globino pregledovanja arhivov. Privzeta vrednost: 10.

Največja velikost datoteke v arhivu – ta možnost omogoča, da določite največjo velikost datotek v arhivu (ko so ekstrahirane), ki bodo pregledane. Privzeta vrednost je: **3 GB**.

priporočamo, da ne spreminjate privzetih vrednosti, v normalnih okoliščinah to običajno ni potrebno.

Ravni čiščenja

Če želite spremeniti nastavitve ravni čiščenja za želeni modul zaščite, razširite **ThreatSense** (na primer **Sprotna zaščita datotečnega sistema**) in v spustnem meniju izberite **Raven čiščenja**.

ThreatSense ima naslednje ravni popravljanja (tj. čiščenja).

Popravljanje s programom ESET Internet Security

Raven čiščenja	Opis
Vedno popravi zaznani element	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih redkih primerih (na primer pri sistemskih datotekah) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.

Raven čiščenja	Opis
Popravi zaznani element, če je varno, sicer ohrani	Poskuša popraviti zaznani element med čiščenjem predmetov brez ukrepanja končnega uporabnika. V nekaterih primerih (na primer pri sistemskih datotekah ali arhivih z neokuženimi in okuženimi datotekami) prijavljeni predmet ostane na prvotni lokaciji, če zaznanega elementa ni mogoče popraviti.
Popravi zaznani element, če je varno, sicer vprašaj	Poskuša popraviti zaznani element med čiščenjem predmetov. V nekaterih primerih, če ni mogoče izvesti nobenega dejanja, se končnemu uporabniku prikaže interaktivno opozorilo in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta nastavitev je priporočljiva v večini primerov.
Vedno vprašaj končnega uporabnika	Končnemu uporabniku se med čiščenjem predmetov prikaže interaktivno okno in izbrati mora popravljalni ukrep (na primer izbris ali prezrtje). Ta raven je namenjena bolj izkušenim uporabnikom, ki vedo, kako ukrepati v primeru zaznanega elementa.

Pripone datotek, izključenih iz pregledovanja

Izključene pripone datotek so del ThreatSense. Če želite konfigurirati izključene pripone datotek, kliknite **ThreatSense** v možnosti Napredne nastavitve za vsak modul, ki uporablja tehnologijo ThreatSense.

Pripona je del imena datoteke, ki je od drugega dela imena ločena s piko. S pripono je označena vrsta in vsebina datoteke. V tem razdelku z nastavitvami orodja ThreatSense je mogoče določiti vrste datotek za pregledovanje.

Ta funkcija ni enaka funkciji Izključitve postopkov, Izključitve sistema HIPS ali Izključitve datotek/map.

Privzeto se pregledajo vse datoteke. Na seznam datotek, ki so izključene iz pregledovanja, je mogoče dodati katero koli pripono.

Včasih je treba nekatere datoteke izključiti iz pregleda, če zaradi pregleda določenih vrst datotek program, ki te pripone uporablja, ne deluje pravilno. Pri uporabi strežnikov Microsoft Exchange bi bilo morda smiselno izključiti pripone `.edb`, `.eml` in `.tmp`.

Če želite na seznam dodati novo pripono, kliknite **Dodaj**. Vnesite pripono v prazno polje (na primer tmp) in kliknite **V redu**. Če izberete možnost **Vnesite več vrednosti**, lahko dodate več datotečnih pripon, ki jih ločite z vrsticami, vejicami ali podpičji (kot ločilo v spustnem seznamu izberite npr. pripono **Podpičje** in vnesite `edb;eml;tmp`).
Uporabite lahko posebni znak ? (vprašaj). Vprašaj predstavlja kateri koli simbol (npr. `?db`).

Če želite videti pripone datotek v operacijskem sistemu Windows, potrdite potrditveno polje **Pripone imen datotek** v **raziskovalcu za Windows** > zavihek **Pogled**.

Dodatni ThreatSense parametri

Če želite urediti te nastavitve, odprite razdelek Napredne nastavitve > **Zaščite** > **Sprotna zaščita datotečnega sistema** > **Dodatni parametri orodja ThreatSense**.

Dodatni parametri orodja ThreatSense za nove in spremenjene datoteke

Verjetnost okužbe novih in spremenjenih datotek je precej višja od verjetnosti okužbe obstoječih datotek. Zato program preveri te datoteke z dodatnimi parametri pregleda. ESET Internet Security uporablja napredno

hevristiko, ki lahko zazna nove grožnje, še preden je izdana posodobitev pogona za zaznavanje skupaj s pregledovanjem na podlagi definicij.

Poleg novo ustvarjenih datotek se pregled izvede tudi na **samodejno raztegljivih arhivih** (.sfx) in **samoustvarjalnih arhivih** (notranje stisnjenih izvedljivih datotekah). Privzeto se arhivi pregledujejo do desete ravni gnezdenja in se preverjajo, ne glede na njihovo dejansko velikost. Če želite spremeniti nastavitve pregleda arhiva, prekličite izbor možnosti **Privzete nastavitve pregledovanja arhiva**.

Dodatni parametri orodja ThreatSense za izvedljive datoteke

Dodatna hevristika pri izvedbi datotek – pri izvajanju datotek se privzeto uporablja napredna hevristika. Priporočamo, da funkciji Pametna optimizacija in ESET LiveGrid® ostaneta omogočeni, saj zmanjšata vpliv na učinkovitost delovanja sistema.

Napredna hevristika pri izvedbi datotek iz izmenljivih nosilcev podatkov – napredna hevristika emulira kodo v navideznem okolju in ovrednoti njeno vedenje, preden se lahko koda zažene iz izmenljivega nosilca podatkov.

Orodja

Napredne nastavitve lahko konfigurirate za funkcije, ki ponujajo dodatno varnost in pomagajo poenostaviti upravljanje programa ESET Internet Security v razdelku Napredne nastavitve > **Orodja**.

- Storitev Microsoft Windows® Update
- ESET CMD
- Dnevniške datoteke
- Način za igranje
- Diagnostika

Storitev Microsoft Windows® Update

Funkcija Windows posodobitev je pomembna komponenta zaščite uporabnikov pred zlonamerno programsko opremo. Zato je ključnega pomena, da namestite posodobitve sistema Microsoft Windows, takoj ko so na voljo. Program ESET Internet Security vas obvesti o manjkajočih posodobitvah glede na raven, ki jo določite v razdelku Napredne nastavitve > **Orodja**. Na voljo so te ravni:

- **Ne opozarjaj** – sistemske posodobitve niso na voljo za prenos.
- **Izbirne posodobitve**– za prenos bodo na voljo posodobitve z oznako »nizka prednost« in posodobitve z oznako večje pomembnosti.
- **Priporočene posodobitve** – za prenos bodo na voljo posodobitve z oznako »pogosto« in posodobitve z oznako večje pomembnosti.
- **Pomembne posodobitve** – za prenos bodo na voljo posodobitve z oznako »pomembne« in posodobitve z oznako večje pomembnosti.

- **Nujne posodobitve** – za prenos bodo na voljo samo kritične posodobitve.

Pogovorno okno – posodobitve sistema

Če so na voljo posodobitve za operacijski sistem, ESET Internet Security prikaže obvestilo v glavnem oknu programa > **Pregled**. Okno s sistemskimi posodobitvami odprete tako, da kliknete **Več informacij**.

V oknu s sistemskimi posodobitvami je prikazan seznam razpoložljivih posodobitev, ki so pripravljene za prenos in namestitev. Vrsta posodobitve je prikazana poleg imena posodobitve.

Če želite prikazati okno z informacijami o posodobitvi, dvokliknite poljubno vrstico s posodobitvijo.

Če želite prenesti in namestiti vse posodobitve operacijskega sistema na seznamu, kliknite **Zaženi posodobitev sistema**.

Informacije o posodobitvi

V oknu s sistemskimi posodobitvami je prikazan seznam razpoložljivih posodobitev, ki so pripravljene za prenos in namestitev. Raven prioritete posodobitve je prikazana ob imenu posodobitve.

Kliknite **Zaženi posodobitev operacijskega sistema**, če želite začeti nalagati in nameščati posodobitve operacijskega sistema.

Če želite prikazati novo okno z dodatnimi informacijami, kliknite poljubno vrstico s posodobitvijo z desno tipko miške in kliknite **Pokaži informacije**.

ESET CMD

To je funkcija, ki omogoča napredne ukaze ecmd. Omogoča izvažanje in uvažanje nastavitev prek ukazne vrstice (ecmd.exe). Do zdaj je bilo nastavitve mogoče uvoziti le prek grafičnega uporabniškega vmesnika (GUI). ESET Internet Security konfiguracijo je mogoče izvoziti v datoteko *.xml*.

Ko omogočite ESET CMD, sta na voljo dva načina za preverjanje pristnosti:

- **Brez** – brez preverjanja pristnosti. Ta način ni priporočljiv, saj omogoča uvoz nepodpisane konfiguracije in zato predstavlja morebitno tveganje.

- **Geslo za dodatne nastavitve** – geslo je potrebno za uvoz konfiguracije iz datoteke .xml, datoteka pa mora biti podpisana (glejte podpisovanje konfiguracijske datoteke .xml spodaj). Pred uvozom nove konfiguracije mora biti zagotovljeno geslo, določeno v razdelku Nastavitve dostopa. Če nastavitve dostopa niso omogočene, če se geslo ne ujema ali če konfiguracijska datoteka .xml ni podpisana, konfiguracija ne bo uvožena.

Ko je funkcija ESET CMD omogočena, lahko uvažate ali izvažate konfiguracije za ESET Internet Security prek ukazne vrstice. To lahko storite ročno ali ustvarite skript, če želite postopek avtomatizirati.

Če želite uporabiti napredne ukaze ecmd, jih morate zagnati s skrbniškimi pravicami ali odpreti ukazni poziv v sistemu Windows (cmd) tako, da uporabite možnost **Zaženi kot skrbnik**. Sicer se prikaže sporočilo **Error executing command**. Pri izvažanju konfiguracije mora obstajati ciljna mapa. Ukaz za izvoz deluje tudi, ko je funkcija ESET CMD izklopljena.

Izvoz ukaza za nastavitev:
`ecmd /getcfg c:\config\settings.xml`

Uvoz ukaza za nastavitev:
`ecmd /setcfg c:\config\settings.xml`

Napredne ukaze ecmd je mogoče zagnati le lokalno.

Podpisovanje konfiguracijske datoteke *.xml*:

1. Prenesite izvedljivo datoteko XmlSignTool.

2. Odprite ukazni poziv v sistemu Windows (cmd) tako, da uporabite možnost **Zaženi kot skrbnik**.

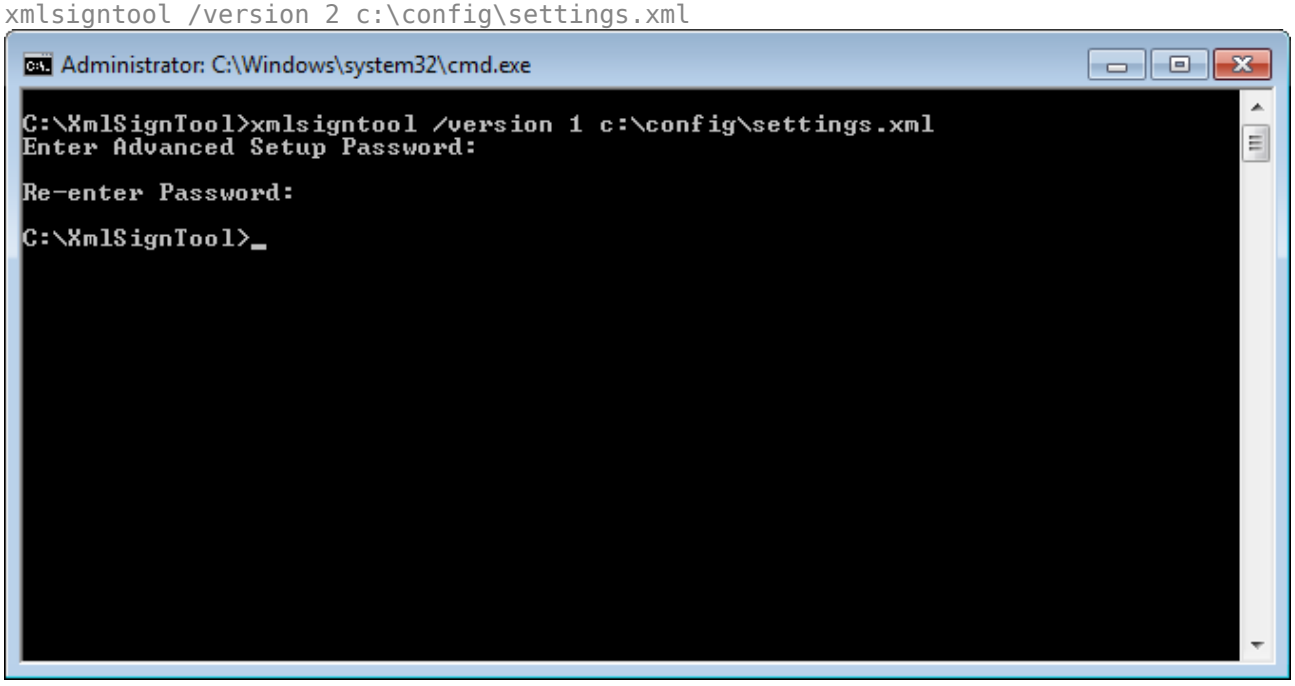
3. Pomaknite se do mesta z orodjem `xmlsigntool.exe`

4. Izvedite ukaz za podpis konfiguracijske datoteke *.xml*, pri čemer uporabite:`xmlsigntool /version 1|2 <xml_file_path>`

Vrednost parametra `/version` je odvisna od vaše različice izdelka ESET Internet Security. Uporabite `/version 1` za različice izdelka ESET Internet Security, starejše od 11.1. Uporabite `/version 2` za najnovejšo različico izdelka ESET Internet Security.

5. Vnesite in znova vnesite geslo za napredne nastavitve, ko to zahteva orodje XmlSignTool. Konfiguracijska datoteka *.xml* je zdaj podpisana in pripravljena za uvoz v drugem primerku izdelka ESET Internet Security prek funkcije ESET CMD z uporabo preverjanja pristnosti gesla.

Ukaz za podpis izvožene konfiguracijske datoteke:
`xmlsigntool /version 2 c:\config\settings.xml`



Če se vaše geslo za nastavitve dostopa spremeni in želite uvoziti konfiguracijo, ki je bila podpisana predhodno s starejšim geslom, morate znova podpisati konfiguracijsko datoteko *.xml* s trenutnim geslom. Tako lahko uporabite starejšo konfiguracijsko datoteko in vam je pred uvozom ni treba izvoziti v drugo napravo z nameščenim izdelkom ESET Internet Security.

Omogočanje ESET CMD brez preverjanja pristnosti ni priporočljivo, saj omogoča uvoz nepodpisane konfiguracije. Da uporabnikom preprečite nedovoljeno spreminjanje, nastavitve geslo v možnosti Napredne nastavitve > **Uporabniški vmesnik** > **Nastavitve dostopa**.

Dnevniške datoteke

Konfiguracijo pisanja dnevnika programa ESET Internet Security lahko najdete v razdelku Napredne nastavitve > **orodja** > **Dnevniške datoteke**. V razdelku z dnevniki lahko določite način upravljanja dnevnikov. Program samodejno izbriše starejše dnevnike, da bi prihranil prostor na trdem disku. Za dnevniške datoteke lahko izberete te možnosti:

Najmanjša dovoljena raven podrobnosti pri pisanju v dnevnik – določi najmanjšo dovoljeno raven podrobnosti za dogodke, ki se zabeležijo v dnevnik:

- **Diagnostika** – zabeleži podatke, ki so potrebni za natančno prilagajanje programa in vseh zgornjih zapisov.
- **Informativno** – zabeleži informativna sporočila, vključno s sporočili o uspešnem posodabljanju in vsemi zgornjimi zapisi.
- **Opozorila** – zabeleži kritične napake in opozorilna sporočila o grožnjah.
- **Napake** – zabeleži napake, kot je »Napaka pri prenosu datoteke«, in kritične napake.
- **Kritično** – v dnevnik zabeleži le kritične napake (napake pri zagonu protivirusne zaščite, požarnega zidu itd.).

Ko izberete raven podrobnosti diagnostike, bodo zabeležene vse blokirane povezave.

Vnosi v dnevnik, ki so starejši od števila dni, navedenega v polju **Samodejno izbriši zapise, ki so starejši od (dni)**, bodo samodejno izbrisani.

Samodejno optimiziraj dnevniške datoteke – če je ta možnost izbrana, bodo dnevniške datoteke samodejno defragmentirane, če je odstotek večji od vrednosti, navedene v polju **Če število neuporabljenih zapisov preseže (%)**.

Če želite začeti defragmentacijo dnevniških datotek, kliknite **Optimiziraj**. Med tem postopkom so odstranjeni vsi prazni vnosi v dnevnik, s čimer se izboljša učinkovitost delovanja in hitrost obdelave dnevnikov. Izboljšava bo posebej opazna, če je bilo v dnevniku veliko vnosov.

Vklopite možnost **Omogoči protokol besedila**, da omogočite shranjevanje dnevnikov v drugi obliki zapisa datoteke, ločeno od Dnevniških datotek:

- **Ciljni imenik** – imenik, v katerega se bodo shranjevale dnevniške datoteke (velja le za obliki zapisa besedilo/CSV). Vsak razdelek dnevnika ima svojo datoteko z vnaprej določenim imenom (na primer: virlog.txt za razdelek **Zaznave** dnevniških datotek, če uporabljate navadno obliko zapisa besedilne datoteke za shranjevanje dnevnikov).

• **Vrsta** – če izberete obliko zapisa datoteke **besedilo**, bodo dnevniki shranjeni v besedilni datoteki in podatki bodo ločeni po zavihkih. Enako velja za obliko zapisa datoteke **CSV**, v kateri podatke ločujejo vejice. Če izberete možnost **Dogodek**, bodo dnevniki shranjeni v dnevnik dogodkov sistema Windows (ogledate si ga lahko v pregledovalniku dogodkov na nadzorni plošči) in ne v datoteko.

• **Izbriši vse dnevniške datoteke** – izbriše vse shranjene dnevnike, ki so trenutno izbrani v spustnem meniju **Vrsta**. Prikaže se obvestilo, da so dnevniki uspešno izbrisani.

Za hitrejše odpravljanje težav boste morda morali družbi ESET posredovati dnevnike iz svojega računalnika. Orodje ESET Log Collector omogoča preprosto zbiranje potrebnih podatkov. Za več informacij o orodju ESET Log Collector preberite članek v zbirki znanja ESET.

Način za igranje

Način za igranje je funkcija za uporabnike, ki zahtevajo nemoteno uporabo programske opreme, ki ne želijo, da jih med uporabo motijo okna z obvestili/opozorili, in ki želijo zmanjšati obremenitev za CPU. Način za igranje lahko uporabite tudi med predstavitvami, ki jih ni mogoče prekiniti z delovanjem protivirusnih programov. Če omogočite to funkcijo, so onemogočena vsa pojavna okna, dejavnosti razporejevalnika pa so popolnoma zaustavljene. Zaščita sistema se še vedno izvaja v ozadju, vendar ne zahteva nobenega dejanja uporabnika.

Način za igranje lahko omogočite ali onemogočite v glavnem oknu programa v razdelku **Nastavitve** > **Zaščita računalnika**, tako da kliknete  ali  poleg možnosti **Način za igranje**. Če omogočite način za igranje, to predstavlja morebitno varnostno tveganje, zato se bo ikona stanja zaščite obarvala oranžno in prikazala opozorilo. To opozorilo bo prikazano tudi v glavnem oknu programa, kjer boste videli sporočilo **Način za igranje je aktiven** v oranžni barvi.

V razdelku **Napredne nastavitve** > Orodja > **Način za igranje** aktivirajte možnost **Pri uporabi programov v celozaslonskem načinu samodejno omogoči način za igranje**, če želite, da se način za igranje zažene ob vsakem zagonu celozaslonskega programa, in se samodejno ustavi, ko zaprete program.

Aktivirajte možnost **Samodejno onemogoči način za igranje po**, da določite časovno obdobje, po katerem bo način za igranje samodejno onemogočen.

Če je požarni zid v interaktivnem načinu, način za igranje pa je omogočen, boste imeli morda težave s povezovanjem z internetom. To lahko predstavlja težavo, če zaženete igro, ki potrebuje povezavo z internetom. Po navadi bi bili pozvani, da tovrstno dejanje potrdite (če ni bilo določenih pravil za komunikacijo ali izjem), vendar je uporabniški vmesnik v načinu za igranje onemogočen. Če želite dovoliti komunikacijo, določite pravilo za komunikacijo za vsak program, ki bi lahko naletel na to težavo, ali uporabite drug Način filtriranja v požarnem zidu. Ne pozabite: če je način za igranje omogočen, vi pa obiščete spletno stran ali zaženete program, ki bi bil lahko varnostno tveganje, bo ta morda blokiran brez razlage ali opozorila, ker je interakcija uporabnika onemogočena.

Diagnostika

Diagnostika zagotavlja izvoze ob zrušitvi procesov programa ESET (npr. ekrn). Če se program zruši, se ustvari izvoz. To lahko razvijalcem pomaga odpraviti in popraviti različne ESET Internet Security napake.

Kliknite spustni meni poleg možnosti **Vrsta izvoza** in izberite eno od treh možnosti, ki so na voljo:

- Izberite**Onemogoči**, da onemogočite to funkcijo.

- **Mini** (privzeto) – zabeleži najmanjši niz uporabnih podatkov, s pomočjo katerih bo morda mogoče ugotoviti, zakaj se je program nepričakovano zrušil. Tovrsten izvoz datotek je lahko uporaben, kadar imate na voljo omejeno količino prostora. Vendar zaradi omejene vključitve podatkov, morda napake, ki jih ni neposredno povzročila nit, ki se je izvajala v času nastanka težave, ne bodo odkrite pri analizi te datoteke.

- **Celotno** – zabeleži vso vsebino sistemskega pomnilnika, če se program nepričakovano ustavi. Celoten izvoz pomnilnika lahko vsebuje podatke iz procesov, ki so se izvajali, ko je bil izvoz pomnilnika ustvarjen.

Ciljni imenik – imenik, v katerem bo med zrušitvijo ustvarjen izvoz.

Odpri mapo z diagnostiko – če želite odpreti ta imenik v novem oknu *raziskovalca*, kliknite **Odpri**.

Ustvari diagnostični izvoz – kliknite **Ustvari**, če želite na lokaciji **Ciljni imenik** ustvariti datoteke diagnostičnega izvoza.

Napredno beleženje

Omogoči napredno beleženje v trženjskih sporočilih – beleženje vseh dogodkov, povezanih s tržnimi sporočili v izdelku.

Omogoči zapisovanje dnevnika zaščite pred neželeno pošto – zabeleži vse dogodke med pregledovanjem neželene pošte. Tako lahko razvijalci lažje diagnosticirajo in odpravijo težave, povezane z mehanizmom za preprečevanje neželene pošte ESET.

Omogoči napredno beleženje mehanizma za zaščito pred krajo – beležite vse dogodke zaščite pred krajo, da omogočite diagnosticiranje in odpravljanje težav.

Omogoči napredno beleženje zaščite brskalnika – beležite vse dogodke, do katerih pride med brskanjem v načinu Varno bančništvo in brskanje.

Omogoči napredno beleženje pregledovalnika računalnika – beleženje vseh dogodkov, do katerih pride pri pregledovanju datotek in map med pregledi računalnika.

Omogoči napredno beleženje pri nadzoru naprav – beleženje vseh dogodkov, do katerih pride v načinu nadzora naprav. Tako lahko razvijalci lažje diagnosticirajo in odpravijo težave, povezane z nadzorom naprav.

Omogoči napredno beleženje za neposredno povezljivost v oblaku – beleženje vseh dogodkov v tehnologiji ESET LiveGrid®. Tako lahko razvijalci lažje diagnosticirajo in odpravijo težave, povezane s tehnologijo ESET LiveGrid®.

Omogoči napredno beleženje Zaščite dokumentov – beleženje vseh dogodkov, do katerih pride v funkciji Zaščita dokumentov, s čimer se omogoči diagnosticiranje in reševanje težav.

Omogoči napredno beleženje zaščite e-poštnega odjemalca – beleženje vseh dogodkov, ki se pojavijo v zaščiti e-poštnega odjemalca in vtičniku e-poštnega odjemalca za omogočanje diagnosticiranja in reševanja težav.

Omogoči napredno beleženje jedra – beleženje vseh dogodkov, ki se pojavijo v jedru ESET (ekrn).

Omogoči napredno zapisovanje dnevnika licenc – beležite vso komunikacijo izdelka z ESET-ovimi strežniki za aktivacijo ali s portalom ESET License Manager.

Omogoči sledenje pomnilniku – beleženje vseh dogodkov, ki bodo razvijalcem pomagali diagnosticirati odtekanja

pomnilnika.

Omogoči napredno beleženje zaščite omrežja – zabeleži vse omrežne podatke, ki prehajajo skozi požarni zid v obliki PCAP, da lahko razvijalcem pomaga diagnosticirati težave, povezane s požarnim zidom, in jih odpraviti.

Omogoči napredno beleženje pregledovalnika omrežnega prometa – zabeleži vse podatke, ki gredo skozi pregledovalnik omrežnega prometa v obliki zapisa PCAP, da razvijalcem pomaga diagnosticirati in odpraviti težave v zvezi s pregledovalnikom omrežnega prometa.

Omogoči napredno beleženje operacijskega sistema – beleženje dodatnih podatkov o operacijskem sistemu, kot so izvajajoči se procesi, dejavnost CPE-ja in operacije diska. Tako lahko razvijalci lažje diagnosticirajo in odpravijo težave, povezane z izdelki ESET, ki se izvajajo v vašem operacijskem sistemu.

Omogoči napredno beleženje pri starševskem nadzoru – beleženje vseh dogodkov, do katerih pride v načinu starševskega nadzora. Tako lahko razvijalci lažje diagnosticirajo in odpravijo težave, povezane z s starševskim nadzorom.

Omogoči napredno beleženje potisnega sporočanja – beleženje vseh dogodkov, do katerih pride med potisnim sporočanjem.

Omogoči napredno beleženje nadzorovanja datotečnega sistema – beleženje vseh dogodkov, do katerih pride pri pregledovanju datotek in map med nadzorovanjem datotečnega sistema.

Omogoči napredno beleženje mehanizma za posodabljanje – zabeleži vse dogodke med posodobitvijo. Tako lahko razvijalci lažje diagnosticirajo in odpravijo težave, povezane z mehanizmom za posodabljanje.

Dnevniške datoteke najdete tukaj: *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Tehnična podpora

Če se na tehnično podporo ESET obrnete prek izdelka ESET Internet Security lahko pošljete podatke o konfiguraciji sistema. Za samodejno pošiljanje podatkov v spustnem meniju **Pošlji podatke o konfiguraciji sistema** izberite **Vedno pošlji** ali izberite **Vprašaj pred pošiljanjem**, če želite, da vas sistem pred pošiljanjem podatkov vpraša.

Povezljivost

V določenih omrežjih lahko pri povezavi med računalnikom in internetom posreduje strežnik proxy. Če uporabljate strežnik proxy, morate določiti naslednje nastavitve. Sicer se program ESET Internet Security in njegovi moduli ne morejo samodejno posodobiti. V programu ESET Internet Security je nastavitev strežnika proxy na voljo v dveh različnih razdelkih naprednih nastavitev.

Globalne nastavitve strežnika proxy lahko konfigurirate v razdelku Napredne nastavitve > **Povezljivost** > **Strežnik proxy**. Če navedete strežnik proxy na tej ravni, določite tudi globalne nastavitve strežnika proxy za celotnem program ESET Internet Security. Te parametre bodo uporabili vsi moduli, pri katerih je potrebna povezava z internetom.

Če želite določiti globalne nastavitve strežnika proxy, omogočite možnost **Uporabi strežnik proxy** ter vnesite naslov **strežnika proxy** in številko **vrat** strežnika proxy.

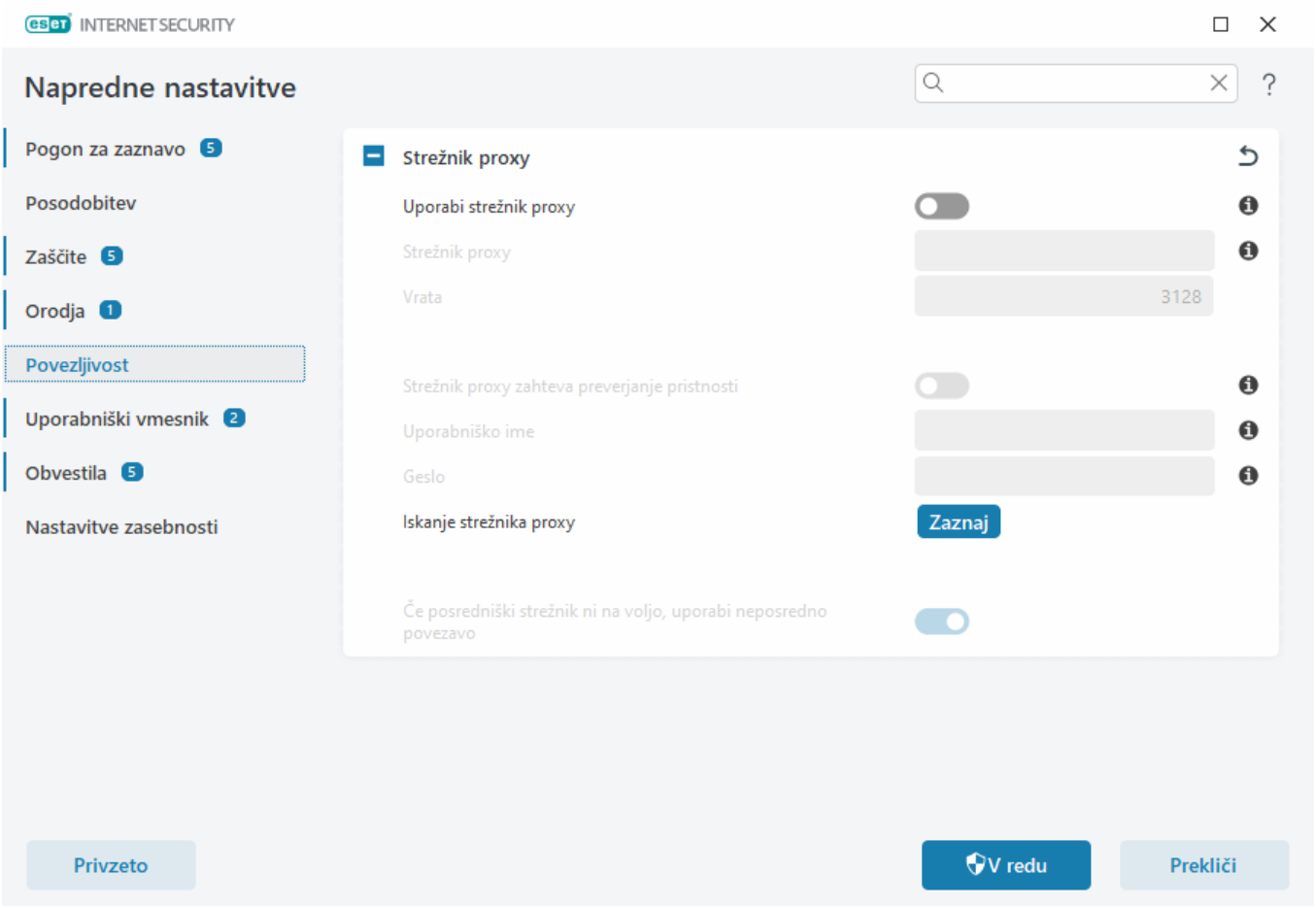
Če komunikacija s strežnikom proxy zahteva preverjanje pristnosti, izberite **Strežnik proxy zahteva preverjanje**

pristnosti in v ustrezni polji vnesite veljavno **uporabniško ime** in **geslo**. Kliknite **Iskanje strežnika proxy**, če želite samodejno zaznati in dopolniti nastavitve strežnika proxy. Program ESET Internet Security bo kopiral parametre, določene v internetnih možnostih za Internet Explorer ali Google Chrome.

V nastavitvah **strežnika proxy** morate ročno vnesti uporabniško ime in geslo.

Če posredniški strežnik ni na voljo, uporabi neposredno povezavo – če je izdelek ESET Internet Security konfiguriran za povezavo prek strežnika proxy, strežnik proxy pa je nedosegljiv, bo izdelek ESET Internet Security preskočil strežnik proxy in komuniciral neposredno s strežniki ESET.

Nastavitve strežnika proxy lahko konfigurirate tudi tako, da v razdelku Napredne nastavitve > **Posodobitev** > **Profili** > **Posodobitve** > **Možnosti povezave** izberete možnost **Vzpostavi povezavo prek strežnika proxy** v spustnem meniju **Način za strežnik proxy**. Ta konfiguracija se uporablja samo za posodobitve in je priporočljiva za prenosne računalnike, ki prejemajo posodobitve modulov iz oddaljenih lokacij. Za več informacij glejte Dodatne nastavitve posodabljanja.



Uporabniški vmesnik

Če želite konfigurirati delovanje grafičnega uporabniškega vmesnika programa (GUI), odprite razdelek Napredne nastavitve > **Uporabniški vmesnik**.

Na zaslonu z naprednimi nastavitvami za orodje Elementi uporabniškega vmesnika lahko prilagodite videz programa in učinke.

Če želite z varnostno programsko opremo zagotoviti najvišjo raven varnosti, lahko odstranjevanje programa ali

nepooblaščene spremembe preprečite tako, da nastavitve zaščitite z geslom. Za to uporabite orodje Nastavitve dostopa.

Če želite konfigurirati delovanje sistemskih obvestil, opozoril za zaznavanje in stanje aplikacij, glejte razdelek Obvestila.

Elementi uporabniškega vmesnika

Delovno okolje programa ESET Internet Security (GUI) lahko svojim potrebam prilagodite v razdelku Napredne nastavitve > **Uporabniški vmesnik** > **Elementi uporabniškega vmesnika**.

Barvni način – v spustnem meniju izberite barvno shemo grafičnega uporabniškega vmesnika aplikacije ESET Internet Security:

- **Enako kot sistemska barva** – nastavi barvno shemo programa ESET Internet Security na podlagi nastavitev operacijskega sistema.
- **Temno** – program ESET Internet Security bo imel temno barvno shemo (temni način).
- **Svetlo** – program ESET Internet Security bo imel standardno, svetlo barvno shemo.

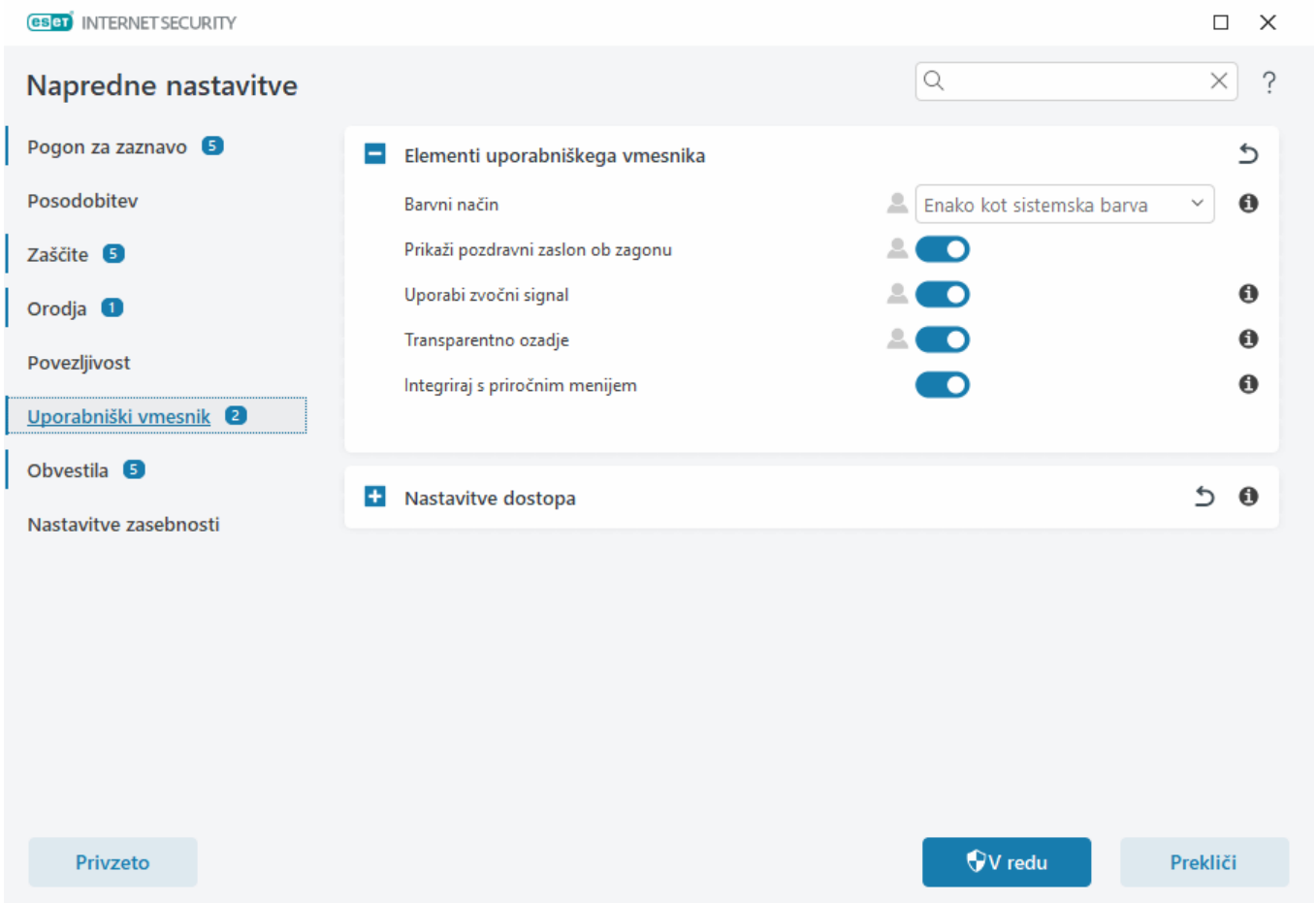
Barvno shemo grafičnega uporabniškega vmesnika programa ESET Internet Security lahko izberete tudi v zgornjem desnem kotu glavnega okna programa.

Prikaži pozdravni zaslon ob zagonu – ob zagonu prikaže pozdravni zaslon aplikacije ESET Internet Security.

Uporaba zvočnega signala – predvaja zvok ob pomembnih dogodkih med pregledovanjem (na primer ob zaznani grožnji ali koncu pregleda).

Transparentno ozadje – omogoča učinek transparentnega ozadja za glavno okno programa. Transparentno ozadje je na voljo le za najnovejše različice sistema Windows (RS4 in novejše).

Integriraj s priročnim menijem – v priročni meni lahko dodate tudi elemente kontrolnika programa ESET Internet Security.



Nastavitve dostopa

Nastavitve programa ESET Internet Security so bistven del vašega varnostnega pravilnika. Nepooblaščene spremembe lahko ogrozijo stabilnost in zaščito sistema. Če se želite izogniti takšnemu nepooblaščenemu spreminjanju, lahko parametre nastavitve za program ESET Internet Security zaščitite z geslom. Nastavitve dostopa je mogoče konfigurirati v razdelku Napredne nastavitve > **Uporabniški vmesnik** > **Nastavitve dostopa**.

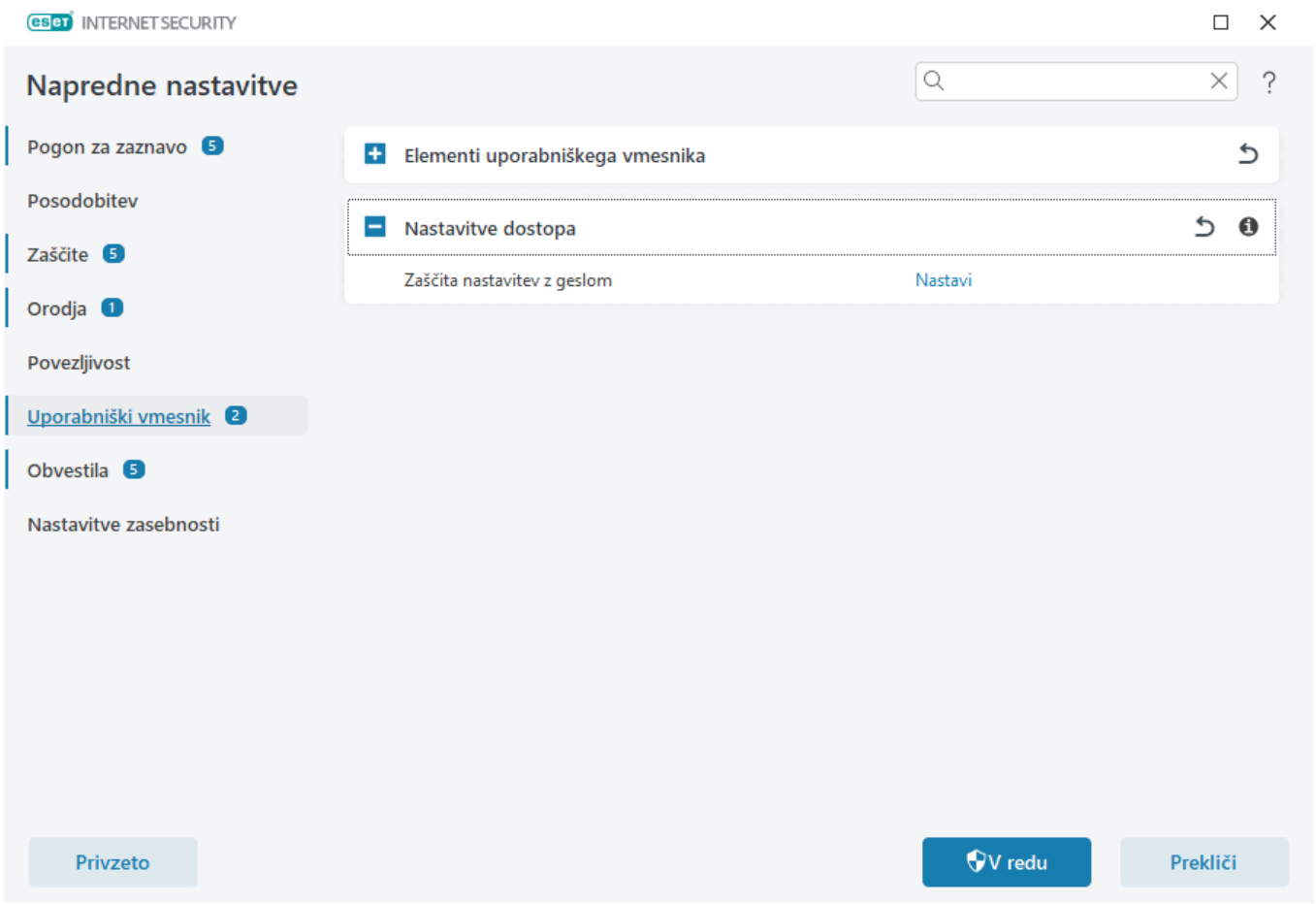
Če želite nastaviti geslo za zaščito parametrov nastavitve in odstranjevanja programa ESET Internet Security, kliknite možnost **Nastavi** ob možnosti **Zaščita nastavitev z geslom**.

Pri poskusu dostopa do napredne nastavitve se prikaže okno za vnos gesla. Če ste pozabili ali izgubili geslo, spodaj kliknite možnost **Ponastavi geslo** in vnesite e-poštni naslov, ki ste ga uporabili za registracijo naročnine. Družba ESET vam bo prek e-pošte poslala kodo za preverjanje in navodila za ponastavitev gesla.

- Odklepanje naprednih nastavitev

Za spremembo gesla kliknite možnost **Spremeni geslo** ob možnosti **Zaščita nastavitev z geslom**.

Za odstranitev gesla kliknite možnost **Odstrani** ob možnosti **Zaščita nastavitev z geslom**.



Geslo za napredne nastavitve

Če želite zaščititi napredne nastavitve za ESET Internet Security in preprečiti nepooblaščeno spreminjanje, vnesite novo geslo v polji **Novo geslo** in **Potrditev gesla**. Kliknite **V redu**.

Za spreminjanje obstoječega gesla:

1. V polje **Staro geslo** vnesite svoje staro geslo.
2. V polji **Novo geslo** in **Potrditev gesla** vnesite novo geslo.
3. Kliknite **V redu**.

To geslo bo potrebno za dostop do naprednih nastavitev.

Če pozabite geslo, glejte Odklepanje gesla za nastavitve v izdelkih ESET za domačo uporabo.

Če želite obnoviti izgubljeno aktivacijsko kodo ESET, datum poteka naročnine ali druge informacije o naročnini za izdelek ESET Internet Security, glejte razdelek Izgubil sem aktivacijsko kodo.

Podpora za bralnike zaslona

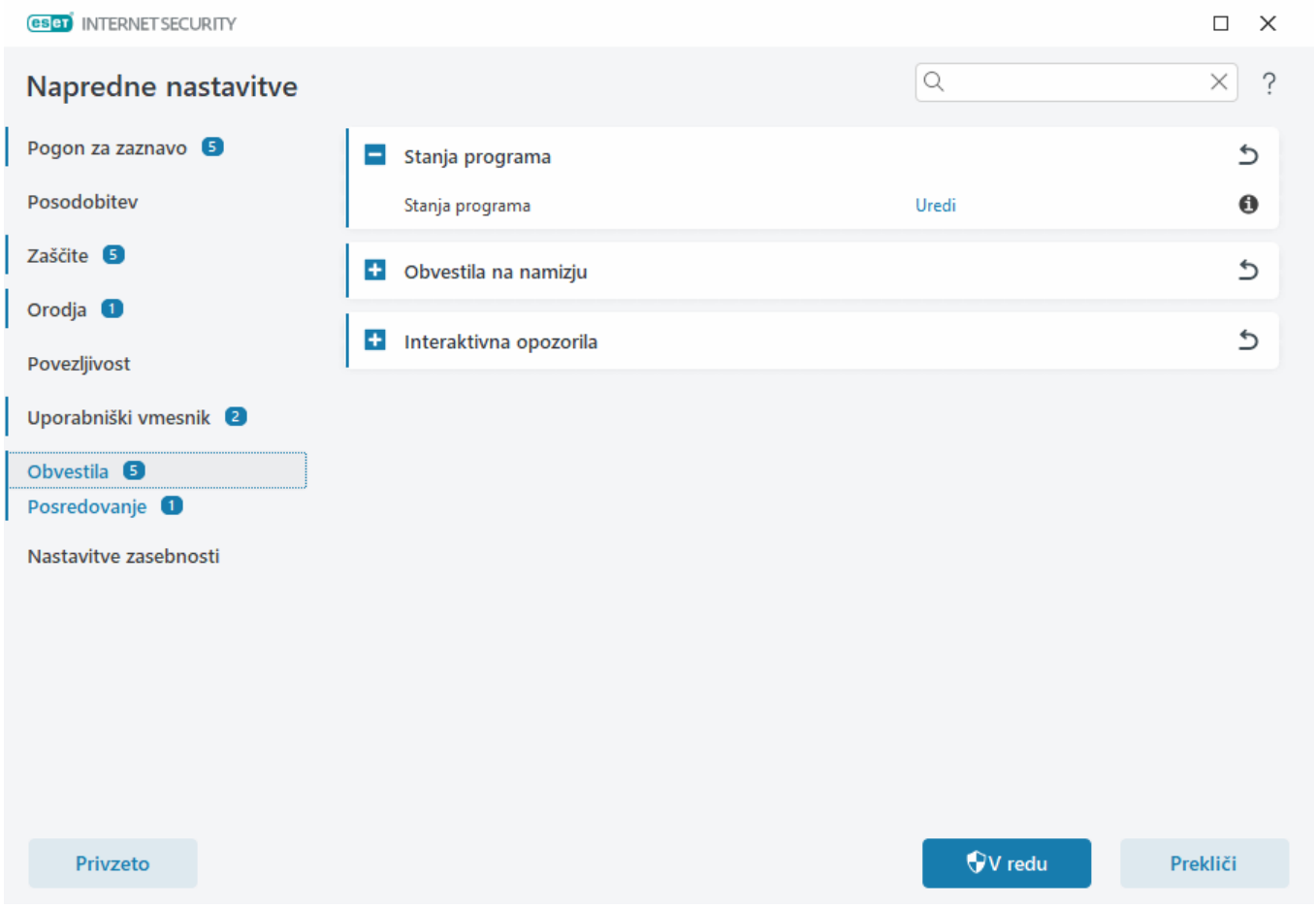
Program ESET Internet Security se lahko uporablja z bralniki zaslona, kar uporabnikom izdelkov ESET s poškodovanim vidom omogoča krmarjenje po programu ali konfiguracijo nastavitev. Podprti so naslednji bralniki (JAWS, NVDA, Narrator).

Upoštevajte navodila v članku iz zbirke znanja družbe, da programski opremi bralnika zagotovite pravilen dostop do grafičnega uporabniškega vmesnika programa ESET Internet Security.

Obvestila

Če želite upravljati obvestila programa ESET Internet Security, odprite razdelek Napredne nastavitve > **Obvestila**. Konfigurirate lahko naslednje vrste obvestil:

- Stanja programa – obvestila, prikazana v glavnem oknu programa > **Pregled**.
- Obvestila na namizju – majhna obvestila zraven opravilne vrstice sistema.
- Interaktivna opozorila – okna z opozorili in polja s sporočili, ki zahtevajo interakcijo uporabnikov.
- Posredovanje (E-poštna obvestila) – e-poštna obvestila se pošljejo na navedeni e-poštni naslov.



Stanja programa

Stanja programa – kliknite **Uredi**, da izberete, katera stanja programa bodo prikazana v začetnem razdelku v glavnem oknu programa > **Pregled**.

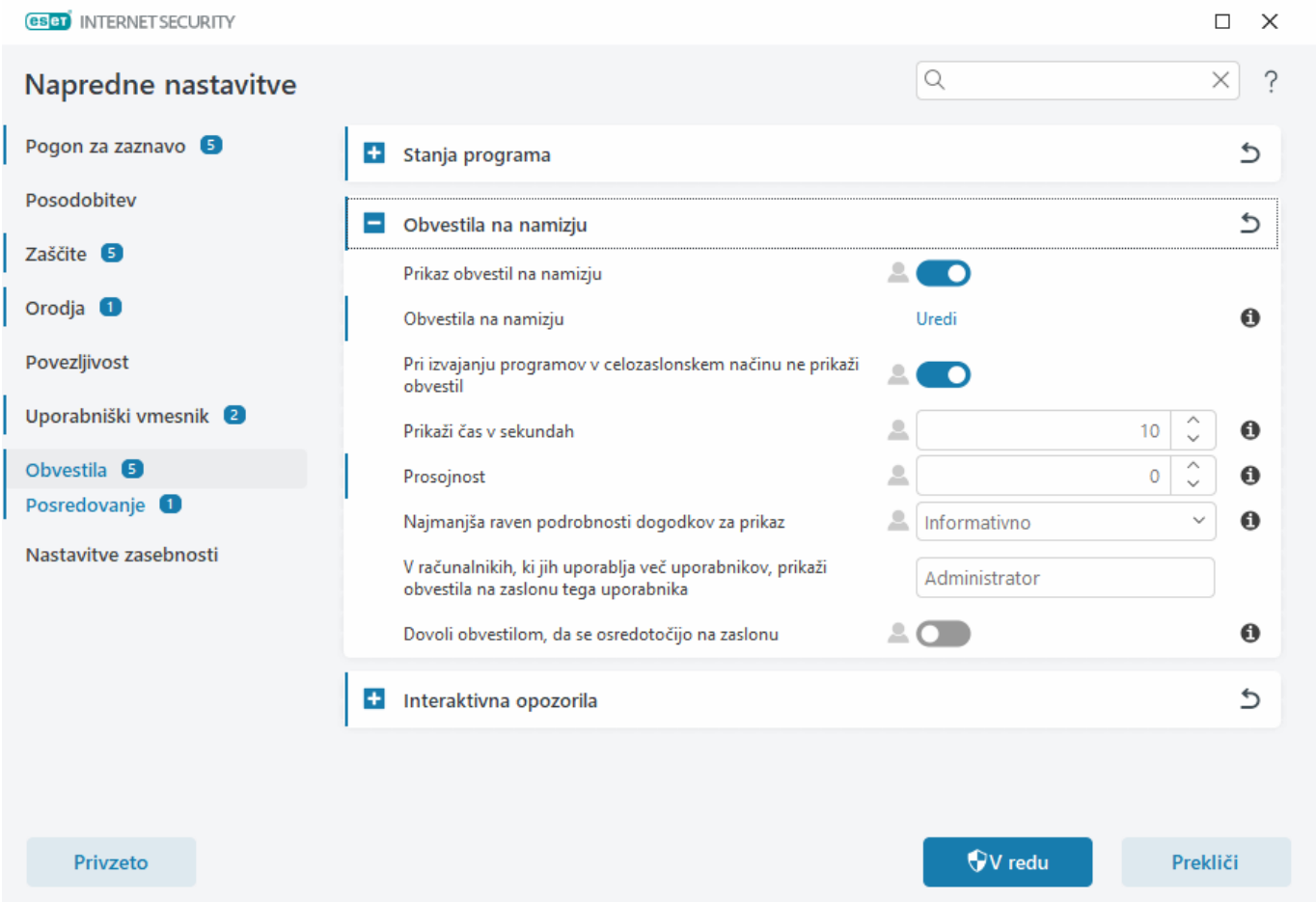
Pogovorno okno – stanja programa

V tem pogovornem oknu lahko izberete, katera stanja programa so prikazana. Ko na primer začasno onemogočite protivirusno in protivohunsko zaščito ali omogočite način za igranje.

Stanje programa se prikaže tudi, če izdelek ni aktiviran ali če je naročnina potekla.

Obvestila na namizju

Obvestila na namizju so majhna okna z obvestili zraven opravilne vrstice sistema. Privzeto je nastavljeno, da se prikažejo za 10 sekund, nato pa počasi izginejo. Obveščajo o uspešnih posodobitvah izdelka, novih povezanih napravah, dokončanih opravilih pregledov virusov ali novih zaznanih grožnjah.



Prikaži obvestila na namizju – priporočamo, da je ta možnost omogočena, tako da vas lahko izdelek obvešča o novih dogodkih.

Obvestila na namizju – kliknite **Uredi**, da omogočite ali onemogočite nekatera obvestila na namizju.

Pri izvajanju programov v celozaslonskem načinu ne prikaži obvestil – pri izvajanju programov v celozaslonskem načinu onemogočite vsa obvestila, ki niso interaktivna.

Čas prikaza v sekundah – omogoča nastavitev trajanja prikaza obvestila. Obvestila so lahko prikazana 3–30 sekund.

Prosojnost – v odstotkih nastavi prosojnost obvestil. Prosojnost lahko določite na lestvici od 0 (nična prosojnost)

do 80 (zelo visoka prosojnost).

Najmanjša raven podrobnosti dogodkov za prikaz – omogoča nastavitev ravni resnosti prikazanega obvestila. Na spustnem meniju izberite eno izmed naslednjih možnosti:

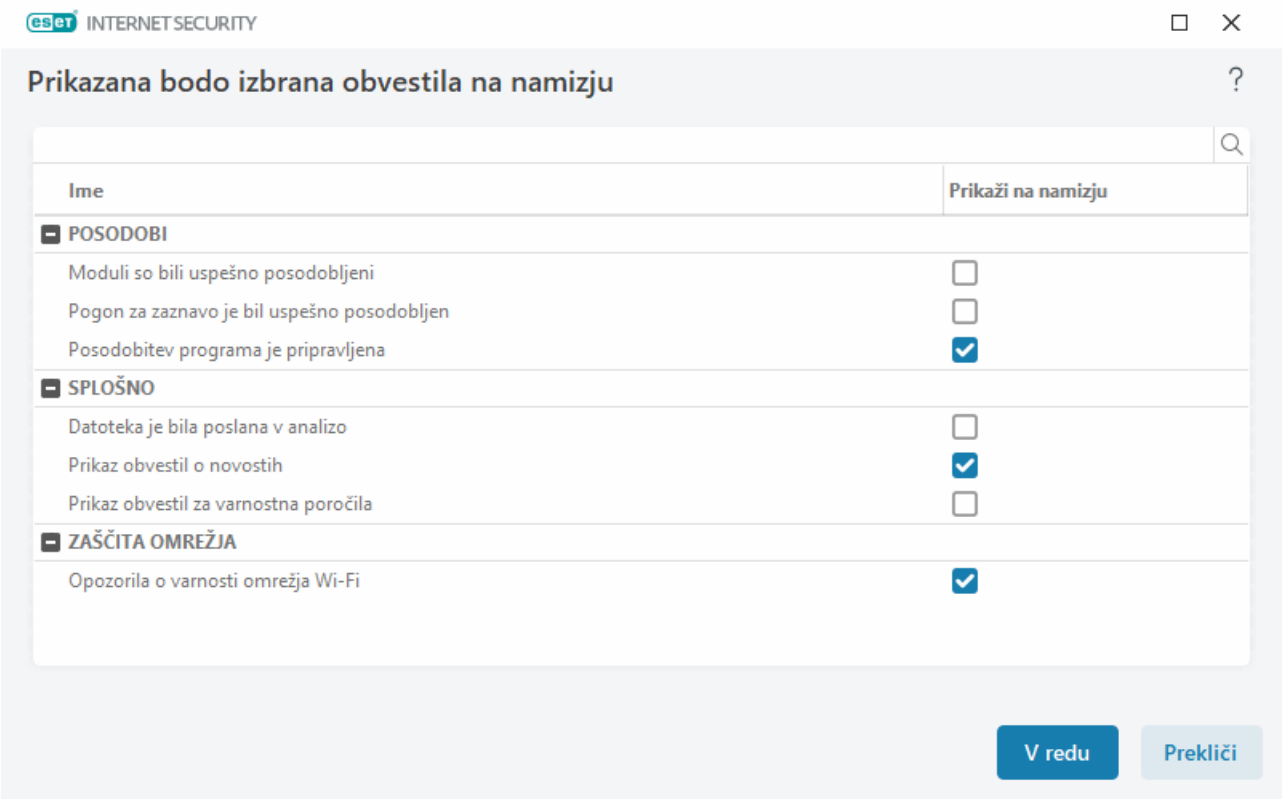
- **Diagnostika** – zabeleži podatke, ki so potrebni za natančno prilagajanje programa in vseh zgornjih zapisov.
- **Informacije** – zabeleži informativna sporočila, kot so na primer nestandardni dogodki v omrežju, vključno s sporočili o uspešnem posodabljanju in vsemi zgornjimi zapisi.
- **Opozorila** – prikaže opozorilna sporočila, napake in kritične napake (npr. da posodobitev ni uspela).
- **Napake** – prikaže napake (npr. da zaščite dokumentov ni bilo mogoče zagnati) in kritične napake.
- **Kritično** – prikaže samo kritične napake (napake pri zagonu protivirusne zaščite ali okužbi sistema itd.).

V računalnikih, ki jih uporablja več uporabnikov, prikaži obvestila na zaslonu vsakega uporabnika – omogoča, da izbrani račun prejme obvestila na namizju. Če na primer ne uporabljate skrbniškega računa, vnesite celotno ime računa in obvestila na namizju bodo prikazana za ta račun. Obvestila na namizju lahko prejema le uporabniški račun.

Obvestilom dovoli, da se osredotočijo na zaslonu – obvestilom omogoča, da se osredotočijo na zaslonu in da so na voljo v meniju **ALT + Tab**.

Seznam obvestil na namizju

Če želite prilagoditi vidljivost obvestil na namizju (prikazana so na dnu na desni strani zaslona), odprite razdelek Napredne nastavitve > **Obvestila** > **Obvestila na namizju**. Kliknite **Uredi** zraven možnosti **Obvestila na namizju** in izberite ustrezno potrditveno polje za možnost **Prikaži**.



Splošno

Prikaz obvestil za varnostna poročila – prejmite obvestilo, ko je ustvarjeno novo varnostno poročilo.

Prikaz obvestil o novostih – obvestila o vseh novih in izboljšanih funkcijah najnovejših različic izdelka.

Datoteka je poslana v analizo – prejmite obvestilo vedno, ko program ESET Internet Security pošlje datoteko v analizo.

Nadzornik omrežja

Obveščanje o novo odkritih omrežnih napravah– prejmite obvestilo, ko nova naprava vzpostavi povezavo z omrežjem.

Zaščita omrežja

Spremenjen profil omrežja – prejmite obvestilo, ko je profil omrežja spremenjen.

Opozorila o varnosti omrežja Wi-Fi – prejmite obvestilo, ko poskušate vzpostaviti povezavo z omrežjem Wi-Fi s šibkim geslom ali brez gesla.

Posodabljanje

Posodobitev programa je pripravljena – prejmite obvestilo, ko je pripravljena posodobitev izdelka ESET Internet Security na novo različico.

Pogon za zaznavo je uspešno posodobljen – prejmite obvestilo, ko izdelek posodobi module pogona za zaznavo.

Moduli so uspešno posodobljeni – prejmite obvestilo, ko izdelek posodobi komponente programa.

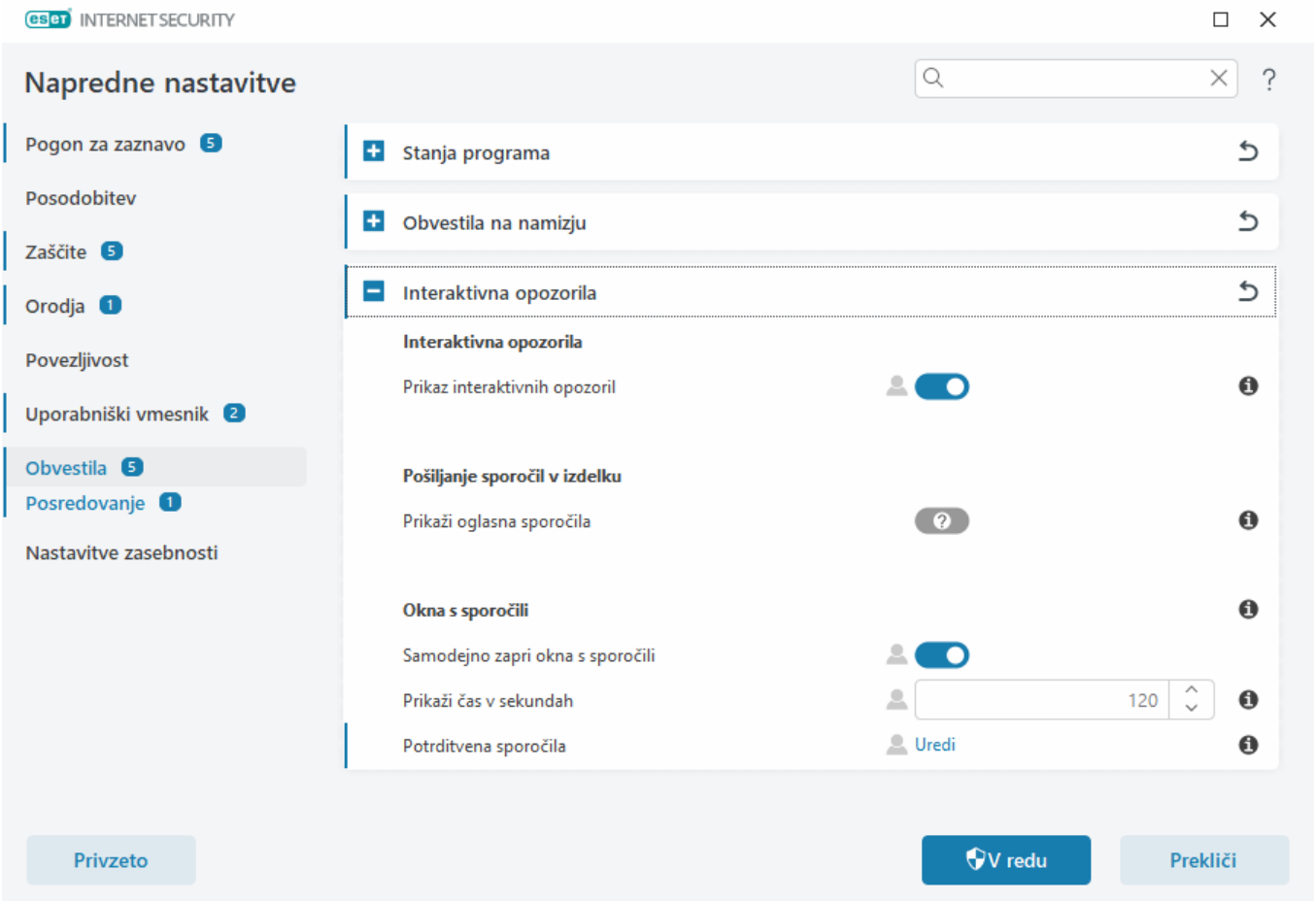
Če želite nastaviti splošne nastavitve za obvestila na namizju (na primer kako dolgo bo sporočilo prikazano ali najnižja raven podrobnosti dogodkov za prikaz), v razdelku Napredne nastavitve > **Obvestila** preglejte možnost Obvestila na namizju.

Interaktivna opozorila

Iščete informacije o pogostih opozorilih in obvestilih?

- Najdena je bila grožnja
- Naslov je blokiran
- Izdelek ni aktiviran
- Sprememba na izdelek z več funkcijami
- Sprememba na izdelek z manj funkcijami
- Na voljo je posodobitev
- Podatki o posodobitvi niso dosledni
- Odpravljanje težav za sporočilo »Posodobitev modulov ni uspela«
- Odpravljanje napak pri posodabljanju modulov
- Omrežna grožnja blokirana
- Potrdilo spletnega mesta preklicano

V razdelku **Interaktivna opozorila** v možnosti Napredne nastavitve > **Obvestila** lahko konfigurirate, kako naj program ESET Internet Security obravnava okna s sporočili in interaktivna opozorila za zaznane elemente, pri katerih mora uporabnik sprejeti odločitev (na primer pri morebitnih spletnih mestih z lažnim predstavljanjem).



Interaktivna opozorila

Če onemogočite možnost **Prikaz interaktivnih opozoril**, so vsa okna z opozorili in pogovorna okna v brskalniku skrita. Onemogočena možnost je primerna le za omejeno število posebnih primerov. Priporočamo, da je ta možnost omogočena.

Pošiljanje sporočil v izdelku

Pošiljanje sporočil v izdelku je namenjeno obveščanju uporabnikov o novicah družbe ESET in drugim sporočilom. Za pošiljanje oglaševalskih sporočil je potrebno soglasje uporabnika. Oglaševalska sporočila se zato privzeto ne pošiljajo uporabnikom (označeno z vprašajem). Če omogočite to možnost, soglašate s prejemanjem oglaševalskih sporočil družbe ESET. Če ne želite prejemati oglaševalskih vsebin družbe ESET, onemogočite možnost **Prikaži oglasna sporočila**.

Okna s sporočili

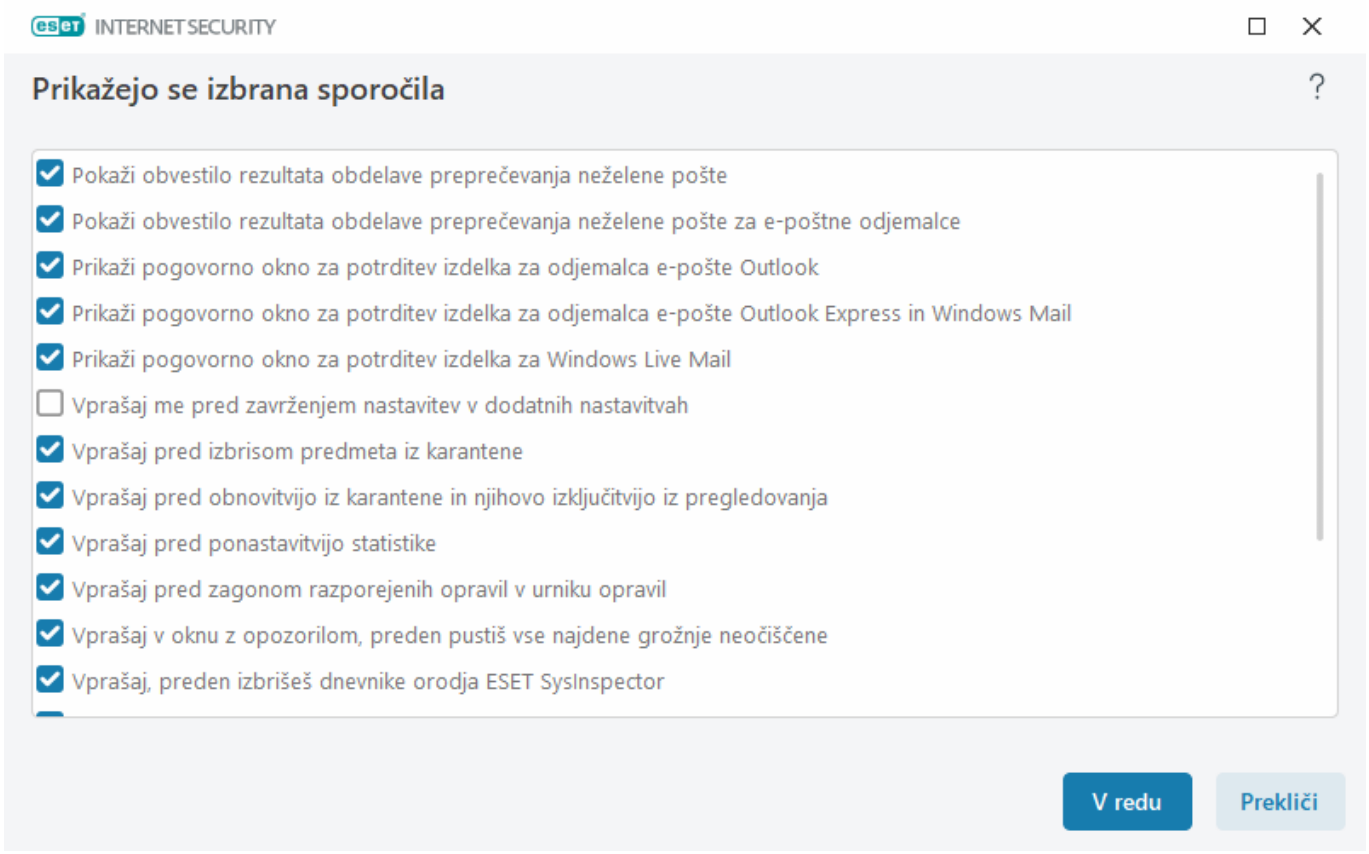
Če želite, da se okna s sporočili po določenem času samodejno zaprejo, izberite možnost **Samodejno zapri okna s sporočili**. Če uporabnik ne zapre oken z opozorili ročno, se ta po določenem času samodejno zaprejo.

Čas prikaza v sekundah – omogoča nastavitev trajanja prikaza opozorila. Obvestila so lahko prikazana 10–999 sekund.

Potrditvena sporočila – Kliknite **Uredi**, da se prikaže seznam potrditvenih sporočil, za katera lahko izberete, ali naj se prikazujejo.

Potrditvena sporočila

Če želite prilagoditi nastavitve potrditvenih sporočil, odprite razdelek Napredne nastavitve > **Obvestila** > **Interaktivna opozorila** in kliknite **Uredi** zraven možnosti **Potrditvena sporočila**.



V tem pogovornem oknu so prikazana potrditvena sporočila programa ESET Internet Security pred izvajanjem dejanj. Izberite ali počistite potrditveno polje poleg posameznega potrditvenega sporočila, da dovolite ali onemogočite dejanje.

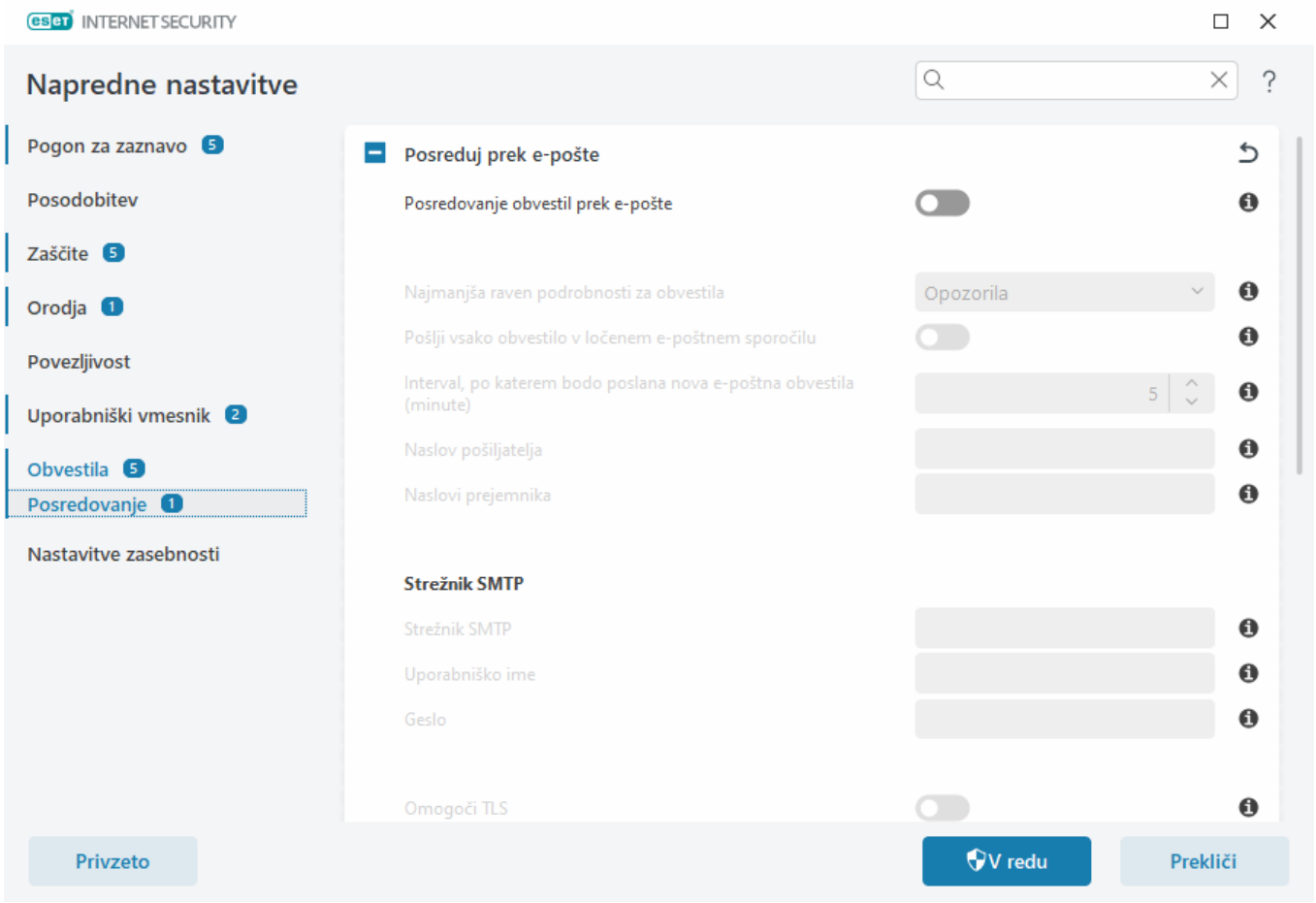
Preberite več o določeni funkciji, povezani s potrditvenimi sporočili:

- Vprašaj, preden izbrišeš dnevnike ESET SysInspector
- Vprašaj, preden izbrišeš vse dnevnike ESET SysInspector
- Vprašaj pred izbrisom predmeta iz karantene
- Vprašaj me pred zavrženjem nastavitev v dodatnih nastavitvah
- Vprašaj v oknu z opozorilom, preden pustiš vse najdene grožnje neočiščene
- Vprašaj, preden zapis odstraniš iz dnevnika
- Vprašaj, preden odstraniš razporejeno opravilo v urniku opravil
- Vprašaj, preden odstraniš vse beleži v dnevniku
- Vprašaj pred ponastavitvijo statistike
- Vprašaj, preden obnoviš predmet iz karantene
- Vprašaj pred obnovitvijo iz karantene in njihovo izključitvijo iz pregledovanja
- Vprašaj, preden zaženeš razporejeno opravilo v urniku opravil

- Pokaži obvestilo rezultata obdelave preprečevanja neželene pošte
- Pokaži obvestilo rezultata obdelave preprečevanja neželene pošte za e-poštne odjemalce
- Prikaži pogovorno okno za potrditev izdelka za odjemalca e-pošte Outlook Express in Windows Mail
- Prikaži pogovorno okno za potrditev izdelka za Windows Live Mail
- Prikaži pogovorno okno za potrditev izdelka za odjemalca e-pošte Outlook

Posredovanje

ESET Internet Security lahko samodejno pošlje e-poštna obvestila, če pride do dogodka z izbrano ravnjo podrobnosti. Odprite razdelek Napredne nastavitve > **Obvestila** > **Posredovanje** in omogočite možnost **Posreduj obvestila na e-poštni naslov**, če želite aktivirati e-poštna obvestila.



V spustnem meniju **Najmanjša raven podrobnosti za obvestila** lahko izberete začetno stopnjo resnosti obvestil za prikaz.

- **Diagnostika** – zabeleži podatke, ki so potrebni za natančno prilagajanje programa in vseh zgornjih zapisov.
- **Informacije** – zabeleži informativna sporočila, kot so na primer nestandardni dogodki v omrežju, vključno s sporočili o uspešnem posodabljanju in vsemi zgornjimi zapisi.
- **Opozorila** – zabeleži kritične napake in opozorilna sporočila (npr. da posodobitev ni uspela).

- **Napake** – zabeleži napake (zaščite dokumentov ni bilo mogoče zagnati) in kritične napake.
- **Kritično** – v dnevnik beleži samo kritične napake (napake pri zagonu protivirusne zaščite ali odkrita grožnja itd.).

Pošlji vsako obvestilo v ločenem e-poštnem sporočilu – ko je ta možnost omogočena, bo prejemnik za vsako obvestilo prejel novo e-poštno sporočilo. Zaradi tega se lahko zgodi, da v kratkem času prejme zelo veliko e-pošte.

Interval, po katerem bodo poslana nova e-poštna obvestila (minute) – interval v minutah, po preteku katerega bo poslano novo e-poštno obvestilo. Če to vrednost nastavite na 0, bodo obvestila poslana takoj.

Naslov pošiljatelja – določite naslov pošiljatelja, ki bo prikazan v glavi e–poštnih obvestil.

Naslovi prejemnikov – določite naslove prejemnikov, ki bodo prikazani v glavi e–poštnih obvestil. Podprtih je več vrednosti. Ločite jih s podpičjem.

SMTP strežnik

Strežnik **SMTP** – strežnik SMTP za pošiljanje obvestil (na primer smtp.provider.com:587, vnaprej določena številka vrat je 25).

> Program ESET Internet Security podpira strežnike SMTP s šifriranjem TLS.

Uporabniško ime in **geslo** – če strežnik SMTP zahteva preverjanje pristnosti, v ta polja vnesite veljavno uporabniško ime in geslo, s katerima je mogoč dostop do strežnika SMTP.

Omogoči TLS – Secure Alert in obvestila z uporabo šifriranja TLS.

Preizkusi povezavo SMTP – na prejemnikov e-poštni naslov bo poslano preizkusno e-poštno sporočilo. Strežnik SMTP, Uporabniško ime, Geslo, Naslov pošiljatelja in Naslovi prejemnikov.

Oblika zapisa sporočila

Komunikacija med programom in oddaljenim uporabnikom ali skrbnikom sistema se izvaja prek e-poštnih sporočil ali sporočil lokalnega omrežja (s storitvijo za pošiljanje sporočil v sistemu Windows). **Privzeta oblika zapisa** sporočil z opozorili in obvestil je v večini primerov optimalna. V nekaterih primerih boste morda morali spremeniti obliko zapisa sporočil o dogodkih.

Oblika zapisa sporočil o dogodkih – oblika zapisa sporočil o dogodkih, ki so prikazana v oddaljenih računalnikih.

Oblika zapisa opozorilnih sporočil o grožnjah – opozorila o grožnjah in sporočila z obvestili imajo vnaprej določeno privzeto obliko zapisa. Priporočamo, da obdržite vnaprej določeno obliko zapisa. Vendar boste v nekaterih primerih (če imate na primer samodejni sistem za obdelavo e-pošte) morda morali spremeniti obliko zapisa sporočil.

Nabor znakov – pretvori e-poštno sporočilo v lokalno kodiranje znakov ANSI glede na območne nastavitve sistema Windows (na primer windows-1250, Unicode (UTF-8), ACSII 7-bit ali japonščina (ISO-2022-JP)). Tako bo znak "á" spremenjen v "a" in neznan simbol "?".

Uporabi kodiranje »Navedba za tiskanje« – vir e-poštnega sporočila bo šifriran v obliko zapisa »Navedba za tiskanje« (QP), ki uporablja znake ASCII in prek e-pošte lahko pravilno prenese posebne znake v 8-bitni obliki

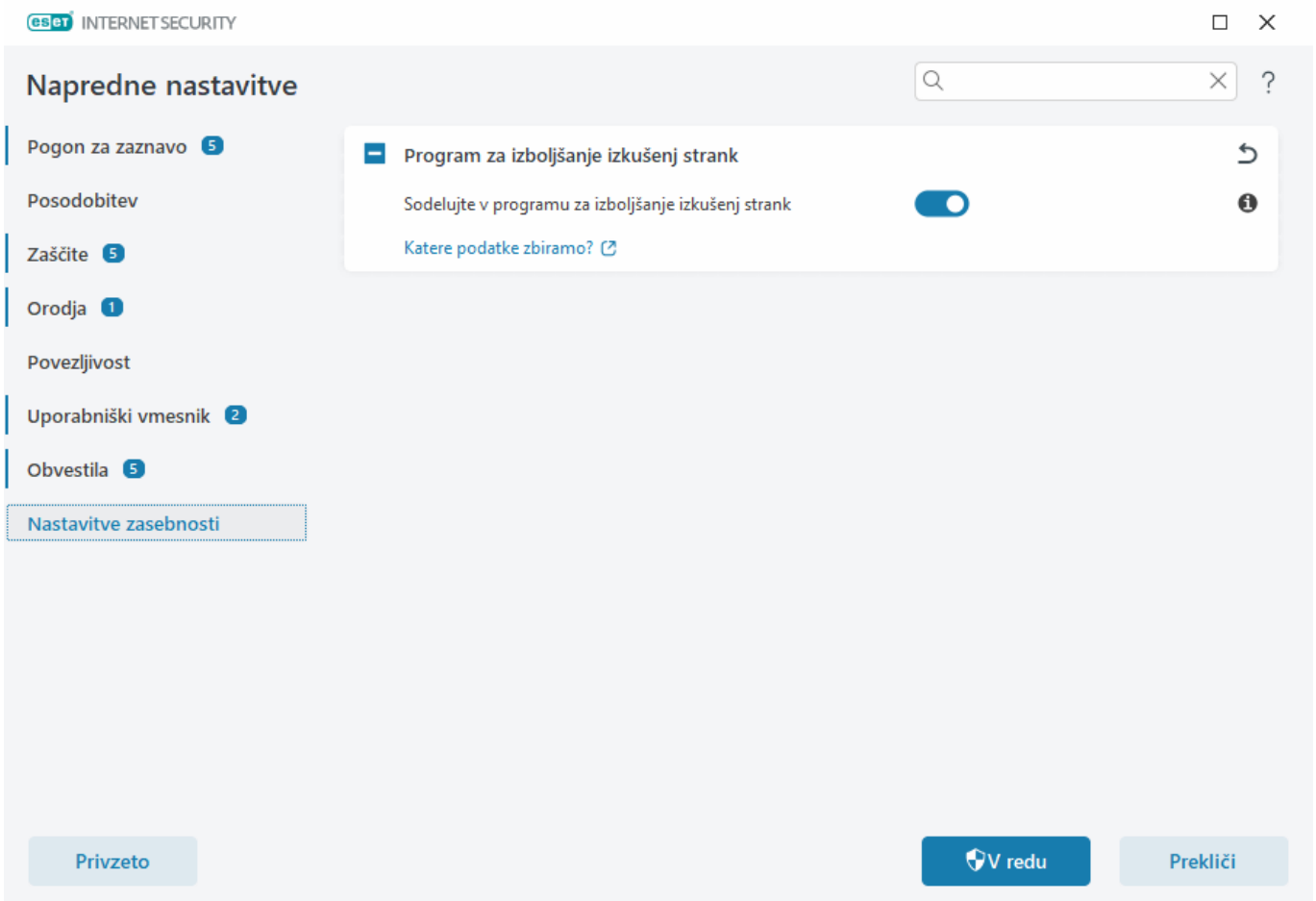
zapisa (áéíóú).

- **%TimeStamp%**– datum in čas dogodka
- **%Scanner%**– modul, na katerega se nanaša
- **%ComputerName%**– ime računalnika, v katerem se je prikazalo opozorilo
- **%ProgramName%**– program, ki je ustvaril opozorilo.
- **%InfectedObject%**– ime okužene datoteke, sporočila itd.
- **%VirusName%**– prepoznavanje okužbe
- **%Action%** – izvedeno dejanje za ukrepanje v zvezi z infiltracijo
- **%ErrorDescription%** – opis dogodka, ki ni povezan z virusom

Ključni besedi **%InfectedObject%** in **%VirusName%** se uporabljata le v opozorilnih sporočilih groženj, **%ErrorDescription%** pa se uporablja samo v sporočilih dogodka.

Nastavitve zasebnosti

Odprite Napredne nastavitve > **Nastavitve zasebnosti**.



Program za izboljšanje izkušenj strank

Omogočite gumb za preklop ob možnosti **Sodelovanje v programu za izboljšanje izkušenj strank**, da se pridružite programu za izboljšanje izkušenj strank. S pristopom družbi ESET zagotovite anonimne podatke u uporabi izdelkov ESET. Zbrani podatki nam bodo pomagali izboljšati vašo izkušnjo in nikoli ne bodo posredovani tretjim osebam. Katere podatke zbiramo?

Povrnitev privzetih nastavitev

Če želite ponastaviti vse programske nastavitve za vse module, v **naprednih nastavitvah** kliknite Privzeto. S tem bodo nastavitve ponastavljene na stanje nastavitev ob namestitvi.

Glejte tudi razdelek Uvoz in izvoz nastavitev.

Povrnitev vseh nastavitev v trenutnem razdelku

Če želite ponastaviti vse nastavitve v trenutnem razdelku na privzete nastavitve, ki jih je določil ESET, kliknite zavito puščico .

Potem ko kliknete **Povrni na privzeto**, bodo vse izvedene spremembe izgubljene.

Povrni vsebino tabel – če izberete ta ukaz, bodo pravila, opravila in profili, ki so bili dodani ročno ali samodejno, izgubljeni.

Glejte tudi razdelek Uvoz in izvoz nastavitev.

Napaka pri shranjevanju konfiguracije

Ta napaka označuje, da nastavitve zaradi napake niso bile pravilno shranjene.

To običajno pomeni: uporabnik, ki je poskušal spremeniti parametre programa:

- nima ustreznih pravic za dostop ali nima potrebnih pravic v operacijskem sistemu za spreminjanje konfiguracijskih datotek in sistemskega registra.
  > Če želite izvesti želene spremembe, se mora prijaviti skrbnik sistema.

- je pred kratkim v sistemu HIPS omogočil možnost »Način za učenje» ali »Požarni zid« in poskušal spreminjati napredne nastavitve.
  > Če želite shraniti konfiguracijo in preprečiti spor konfiguracij, zaprite napredne nastavitve ne da bi shranili spremembe in znova poskusite izvesti želene spremembe.

Drugi najpogostejši vzrok je, da program morda ne deluje več pravilno ali je poškodovan in ga morate zato znova namestiti.

Pregledovalnik v ukazni vrstici

ESET Internet SecurityProtivirusni modul programa lahko zaženete v ukazni vrstici – ročno (z ukazom »ecls«) ali s paketno datoteko (»bat«).

Uporaba pregledovalnika ukazne vrstice ESET:

```
ecls [OPTIONS..] FILES..
```

Kadar v ukazni vrstici zaženete pregledovalnik na zahtevo, uporabite te parametre in stikala:

Možnosti

/base-dir=MAPA	naloži module iz MAPE
/quar-dir=MAPA	dodaj MAPO v karanteno
/exclude=MASKA	iz pregleda izključi datoteke, ki se ujemajo z MASKO
/subdir	preglej podmape (privzeto)
/no-subdir	ne preglej podmap
/max-subdir-level=RAVEN	najgloblja raven map v mapah za pregled
/symlink	odpri simbolične povezave (privzeto)
/no-symlink	preskoči simbolične povezave
/ads	preglej ADS (privzeto)
/no-ads	ne preglej ADS-a
/log-file=DATOTEKA	izhod dnevnika v DATOTEKO
/log-rewrite	prepiši datoteko izhoda (privzeto – priloži)
/log-console	beleži izhod v konzolo (privzeto)
/no-log-console	ne beleži izhoda v konzolo
/log-all	beleži tudi čiste datoteke
/no-log-all	ne beleži čistih datotek v dnevnik (privzeto)
/aind	pokaži indikator dejavnosti
/auto	preglej in samodejno očisti vse lokalne diske

Možnosti pregledovalnika

/files	preglej datoteke (privzeto)
/no-files	ne preglej datotek
/memory	preglej pomnilnik
/boots	preglej zagonske sektorje
/no-boots	ne preglej zagonskih sektorjev (privzeto)
/arch	preglej arhive (privzeto)
/no-arch	ne preglej arhivov
/max-obj-size=VELIKOST	preglej samo datoteke, ki so manjše od VELIKOST megabajtov (privzeto 0 = neomejeno)

/max-arch-level=RAVEN	najgloblja raven arhivov v arhivu (ugnezdeni arhivi) za pregled
/scan-timeout=OMEJITEV	pregleduj arhive največ OMEJITEV s
/max-arch-size=VELIKOST	datoteke v arhivu preglej le, če so manjše od VELIKOST (privzeto 0 = neomejeno)
/max-sfx-size=VELIKOST	datoteke v samodejno raztegljivem arhivu preglej samo, če so manjše od VELIKOST megabajtov (privzeto 0 = neomejeno)
/mail	preglej e-poštne datoteke (privzeto)
/no-mail	ne preglej e-poštnih datotek
/mailbox	preglej poštne predale (privzeto)
/no-mailbox	ne preglej poštnih predalov
/sfx	preglej samodejno raztegljive arhive (privzeto)
/no-sfx	ne preglej samodejno raztegljivih arhivov
/rtp	preglej samoustvarjalne arhive (privzeto)
/no-rtp	ne preglej samoustvarjalnih arhivov
/unsafe	poišči morebitno nevarne programe
/no-unsafe	ne poišči morebitno nevarnih programov (privzeto)
/unwanted	poišči morebitno neželene programe
/no-unwanted	ne poišči morebitno neželenih programov (privzeto)
/suspicious	poišči sumljive programe (privzeto)
/no-suspicious	ne poišči sumljivih programov
/pattern	uporabi definicije (privzeto)
/no-pattern	ne uporabi definicij
/heur	omogoči hevristiko (privzeto)
/no-heur	onemogoči hevristiko
/adv-heur	omogoči napredno hevristiko (privzeto)
/no-adv-heur	onemogoči napredno hevristiko
/ext-exclude=PRIPONE	iz pregleda izključi datotečne PRIPONE, ločene z dvopičjem
/clean-mode=NAČIN	uporabi NAČIN čiščenja za okužene predmete Na voljo so naslednje možnosti: • `none` (privzeto) – samodejno čiščenje se ne bo izvedlo. • `standard` – program ecls.exe bo poskusil samodejno očistiti ali izbrisati okužene datoteke. • `strogo` – program ecls.exe bo poskusil samodejno očistiti ali izbrisati okužene datoteke brez posredovanja uporabnika (uporabnik ne bo pozvan pred brisanjem datotek). • `skrajno` – program ecls.exe bo izbrisal datoteke, ne da bi jih poskusil očistiti, in sicer ne glede na vrsto datoteke. • `brisanje` – program ecls.exe bo izbrisal datoteke, ne da bi jih poskusil očistiti, vendar pa ne bo izbrisal občutljivih datotek, kot so sistemske datoteke sistema Windows.
/quarantine	kopiraj okužene datoteke (če so očiščene) v karanteno (dodano dejanju pri čiščenju)
/no-quarantine	ne kopiraj okuženih datotek v karanteno

Splošne možnosti

/help	pokaži pomoč in zapri
/version	pokaži informacije o različici in zapri
/preserve-time	ohrani časovni žig zadnjega dostopa

Izhodne kode

0	ni najdenih groženj
1	najdena grožnja je počiščena
10	nekaterih datotek ni bilo mogoče pregledati (morda so grožnje)
50	najdena je bila grožnja
100	napaka

Izhodne kode, ki so večje od 100, pomenijo, da datoteka ni bila pregledana in je zato lahko okužena.

Pogosta vprašanja

Nekaj najpogosteje zastavljenih vprašanj in težav, s katerimi se srečujete, najdete spodaj. Če želite poiskati rešitev svoje težave, kliknite naslov teme:

- Kako posodobiti program ESET Internet Security
- Program ESET Internet Security je zaznal grožnjo
- Odstranjevanje virusa iz računalnika
- Kako dovoliti komunikacijo določenemu programu
- Kako omogočiti starševski nadzor računa
- Ustvarjanje novega opravila v razporejevalniku
- Kako razporediti opravilo pregledovanja (tedensko)
- Odklepanje naprednih nastavitev
- Kako razrešiti deaktivacijo izdelka s portala ESET HOME

Če svoje težave ne najdete na zgornjem seznamu, preiščite spletno pomoč ESET Internet Security.

Če rešitve za svojo težavo/vprašanje ne najdete v spletni pomoči ESET Internet Security, obiščite našo spletno zbirko znanja družbe ESET, ki jo redno posodabljamo. Spodaj so navedene povezave do najbolj branih člankov zbirke znanja:

- Kako lahko obnovim naročnino?
- Med nameščanjem izdelka ESET je prišlo do napake pri aktivaciji. Kaj to pomeni?

- Aktiviranje izdelka za domačo uporabo ESET za Windows z aktivacijsko kodo
- Odstranitev ali ponovna namestitev izdelka ESET za domačo uporabo
- Prejel sem sporočilo, da se je namestitev izdelka ESET predčasno končala.
- Kaj moram storiti, ko obnovim naročnino? (uporabniki domače različice)
- Kaj se zgodi, če spremenim svoj e-poštni naslov?
- Prenos ESET-ovega izdelka v nov računalnik ali napravo
- Kako zagnati Windows v varnem načinu ali varni način z omrežjem
- Izključevanje varnega spletnega mesta iz blokiranja
- Omogočanje dostopa programski opremi bralnikov zaslona v grafični vmesnik ESET

Če imate vprašanja ali težave, se lahko obrnete na našo tehnično podporo.

Posodobitev izdelka ESET Internet Security

Izdelek ESET Internet Security lahko posodobite ročno ali pa omogočite samodejno posodobitev. Če želite sprožiti posodobitev, v glavnem oknu programa kliknite **Posodobitev** in nato **Poišči posodobitve**.

Pri nastavitvi s privzeto namestitvijo se ustvari opravilo samodejnega posodabljanja, ki se izvaja vsako uro. Če želite spremeniti ta interval, se pomaknite do **Orodja** > Razporejevalnik.

Odstranjevanje virusa iz računalnika

Če menite, da je v vašem računalniku prišlo do okužbe z zlonamerno programsko opremo, če na primer računalnik deluje počasneje ali pogosto zamrzne, priporočamo, da naredite to:

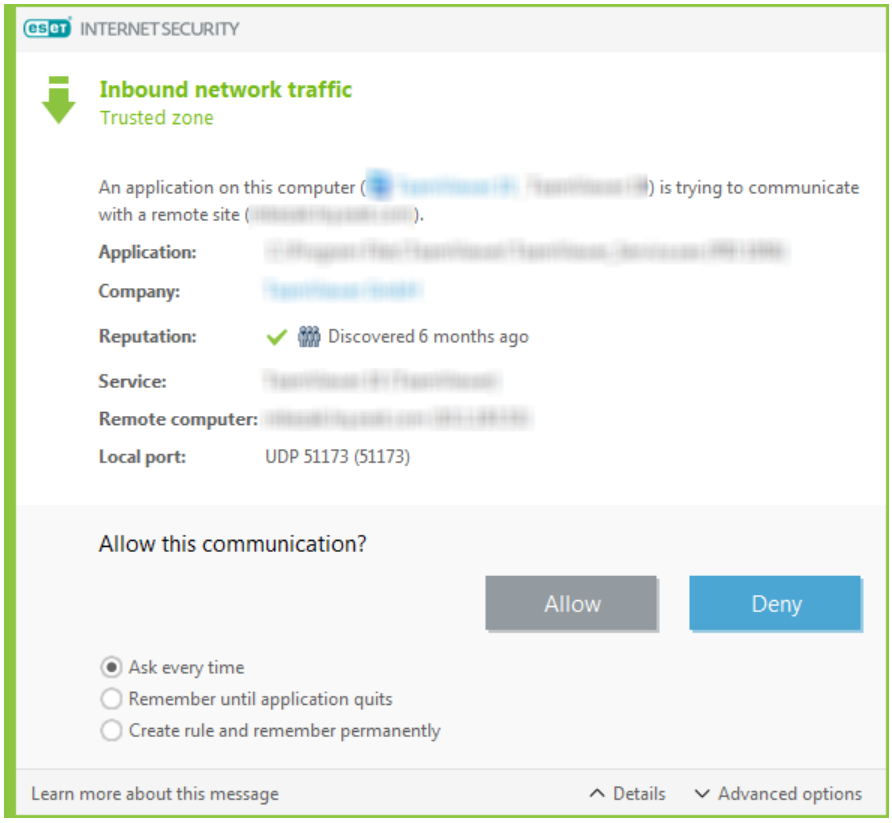
1. V glavnem oknu programa kliknite **Pregled računalnika**.
2. Kliknite **Preglejte računalnik**, da zaženete pregled sistema.
3. Ko je pregled dokončan, v dnevniku preverite, koliko datotek je pregledanih, okuženih in očiščenih.
4. Če želite pregledati le izbrani del diska, izberite možnost **Pregled po meri** in izberite cilje, za katere želite preveriti, ali vsebujejo viruse.

Za dodatne informacije glejte:

- Članek zbirke znanja družbe ESET
- Karantena

Kako dovoliti komunikacijo določenemu programu

Če je v interaktivnem načinu zaznana nova povezava in se z njo ne ujema nobeno pravilo, boste pozvani, da jo **dovolite** ali **zavrnete**. Če želite, da ESET Internet Security izvede isto dejanje vsakič, ko program poskuša vzpostaviti povezavo, potrdite potrditveno polje **Ustvari pravilo in si ga trajno zapomni**.



V nastavitvah požarnega zidu lahko ustvarite nova pravila požarnega zidu za aplikacije, preden jih zazna ESET Internet Security. Odprite glavno okno programa > **Nastavitve** > **Zaščita omrežja** > kliknite ⚙ zraven možnosti **Požarni zid** > **Konfiguriranje** > **Napredno** > **Pravila** > **Uredi**.

Kliknite gumb **Dodaj** in na zavihku **Splošno** vnesite ime, smer in protokol komunikacije za pravilo. V tem oknu lahko določite dejanje, ki naj se izvede, ko je uporabljeno pravilo.

Na zavihku **Lokalno** vnesite pot do izvedljive datoteke programa in lokalnih komunikacijskih vrat. Kliknite zavihek **Oddaljeno** in vnesite oddaljeni naslov in vrata (če obstajata). Na novo ustvarjeno pravilo bo uporabljeno takoj, ko bo program znova poskušal komunicirati.

Kako omogočiti starševski nadzor računa

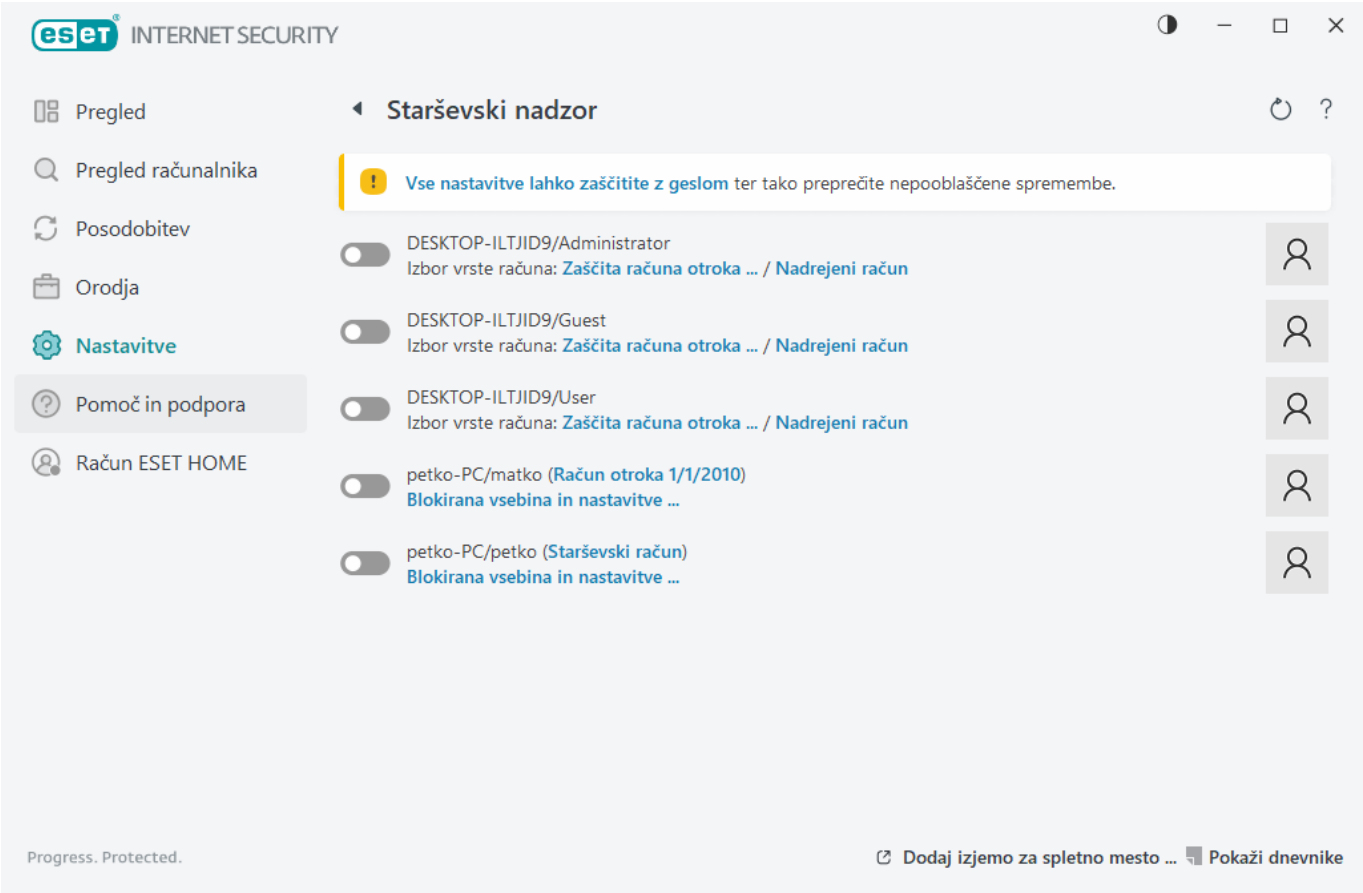
Če želite aktivirati starševski nadzor določenega uporabniškega računa, sledite spodnjim navodilom:

1. Starševski nadzor je privzeto onemogočen v programu ESET Internet Security. Starševski nadzor lahko aktivirate na dva načina:

   • V glavnem oknu programa kliknite ikono gumba za preklop v razdelku **Nastavitve** > **Zaščita na spletu** > **Starševski nadzor** in spremenite stanje starševskega nadzora na omogočeno.

• Odprite razdelek Napredne nastavitve > **Zaščite** > **Zaščita spletnega dostopa** > **Starševski nadzor** in nato omogočite gumb za preklop zraven možnosti **Omogoči starševski nadzor**.

2. V glavnem oknu programa kliknite **Nastavitve** > **Zaščita na spletu** > **Starševski nadzor**. Čeprav je ob možnosti **Starševski nadzor** prikazano **Omogočeno**, morate konfigurirati starševski nadzor za želeni račun tako, da kliknete simbol puščice in nato v naslednjem oknu izberete **Zaščita računa otroka** ali **Nadrejeni račun**. V naslednjem oknu izberite rojstni datum, da določite raven dostopa in priporočene spletne strani, primerne za določeno starost. Starševski nadzor je omogočen za navedeni uporabniški račun. Pod imenom računa kliknite **Blokirana vsebina in nastavitve**, da prilagodite kategorije, ki jih želite dovoliti ali blokirati na zavihku Kategorije. Če želite dovoliti ali blokirati spletne strani po meri, ki se ne ujemajo s kategorijo, kliknite zavihek Izjeme.



Ustvarjanje novega opravila v razporejevalniku

Če želite ustvariti novo opravilo v razdelku **Orodja** > **Razporejevalnik**, kliknite **Dodaj opravilo** ali pa kliknite z desno tipko miške in v priročnem meniju izberite možnost **Dodaj**. Na voljo je pet vrst razporejenih opravil:

• **Zaženi zunanji program** – razporedi izvajanje zunanjega programa.

• **Vzdrževanje dnevnika** – v dnevniških datotekah so tudi ostanki iz izbrisanih zapisov. S tem opravilom redno optimizirate zapise v dnevniških datotekah in tako omogočite učinkovito delovanje.

• **Preverjanje datotek ob zagonu sistema** – preveri datoteke, ki se lahko zaženejo ob zagonu sistema ali prijavi.

• **Ustvari posnetek stanja računalnika** – ustvari posnetek računalnika s programom ESET SysInspector;

zbere podrobne informacije o sistemskih komponentah (na primer gonilnikih, programih) in oceni raven tveganja za vsako posamezno komponento.

- **Pregled računalnika na zahtevo** – izvede pregled datotek in map v računalniku.
- **Posodobi** – razporedi opravilo posodabljanja tako, da posodobi module.

Posodobi je eno od najpogosteje uporabljenih razporejenih opravil; v nadaljevanju najdete navodila za dodajanje novega opravila posodabljanja:

V spustnem meniju **Razporejeno opravilo** potrdite **Posodobi**. V polje **Ime opravila** vnesite ime opravila in kliknite **Naprej**. Izberite pogostost opravila. Na voljo so naslednje možnosti: **Enkrat**, **Večkrat**, **Vsak dan**, **Tedensko** in **Ob dogodkih**. Izberite **Preskoči opravilo, ko se naprava napaja iz akumulatorja**, da zmanjšate sistemske vire, kadar se prenosnik napaja iz akumulatorja. Opravilo bo zagnano ob datumu in uri, ki sta določena v poljih **Izvedba opravil**. Nato določite dejanje, ki naj se izvede, če opravila ni mogoče izvesti ali dokončati ob izbranem času. Na voljo so naslednje možnosti:

- **Ob naslednjem razporejenem času**
- **Takoj, ko je mogoče**
- **Takoj, če čas od zadnjega zagona presega določeno vrednost** (interval je mogoče določiti z drsnim trakom **Čas od zadnjega zagona (ure)**)

V naslednjem koraku se prikaže okno s povzetkom podatkov o trenutnem razporejenem opravilu. Ko ste s spreminjanjem končali, kliknite možnost **Končaj**.

Prikaže se pogovorno okno, v katerem si lahko izberete profile, ki jih želite uporabiti za razporejeno opravilo. Tukaj lahko določite primarni in nadomestni profil. Nadomestni profil bo uporabljen, če opravila ni mogoče dokončati s primarnim profilom. Potrdite tako, da kliknete možnost **Končaj** , in novo razporejeno opravilo bo dodano na seznam trenutno razporejenih opravil.

Kako razporediti tedensko pregledovanje računalnika

Če želite razporediti redno opravilo, odprite glavno okno programa in kliknite **Orodja** > **Razporejevalnik**. Spodaj so kratka navodila za razporejanje opravila, s katerim se vsak teden izvede pregled lokalnih diskov. Podrobnejša navodila najdete v našem članku zbirke znanja družbe.

Opravilo pregledovanja razporedite tako:

1. V glavnem oknu razporejevalnika kliknite **Dodaj**.
2. Izberite ime opravila in izberite v spustnem meniju **Vrsta opravila** izberite **Pregled računalnika na zahtevo**.
3. Izberite **Tedensko** za pogostost opravila.
4. Nastavite datum in čas izvedbe opravila.
5. Izberite **Zaženi opravilo, takoj ko bo mogoče**, da se opravilo izvede pozneje, če se razporejeno opravilo ni moglo izvesti zaradi določenih razlogov (npr. računalnik je bil izklopljen).
6. Oglejte si povzetek razporejenega opravila in kliknite **Dokončaj**.

7. V spustnem meniju **Cilji** izberite **Lokalni pogoni**.

8. Če želite uporabiti opravilo, kliknite **Dokončaj**.

Odklepanje napredne nastavitve, zaščitene z geslom

Pri poskusu dostopa do zaščitene napredne nastavitve se prikaže okno za vnos gesla. Če ste geslo pozabili ali izgubili, kliknite **Ponastavi geslo** in vnesite e-poštni naslov, ki ste ga uporabili za registracijo naročnine. Družba ESET vam bo po e-pošti poslala kodo za preverjanje. Vnesite kodo za preverjanje, nato pa vnesite geslo in ga potrdite. Koda za preverjanje je veljavna sedem dni.

Obnova gesla v računu ESET HOME – to možnost uporabite, če je naročnina, uporabljena za aktivacijo, povezana z vašim računom ESET HOME. Vnesite e-poštni naslov, ki ga uporabljate za prijavo v račun ESET HOME.

Če ste pozabili svoj e-poštni naslov ali imate težave pri obnavljanju gesla, kliknite možnost **Stopi v stik s tehnično podporo**. Preusmerjeni boste na spletno mesto družbe ESET, na kateri lahko stopite v stik z oddelkom za tehnično podporo.

Ustvari kodo za tehnično podporo – s to možnostjo ustvarite kodo za tehnično podporo. Kopirajte kodo, ki vam jo je posredoval oddelek za tehnično podporo, in kliknite možnost **Imam kodo za preverjanje**. Vnesite kodo za preverjanje, nato pa vnesite in potrdite novo geslo. Koda za preverjanje je veljavna sedem dni.

Za več informacij si oglejte Odklepanje nastavitev gesla v izdelkih ESET za domačo uporabo za sistem Windows.

Kako razrešiti deaktivacijo izdelka s portala ESET HOME

Izdelek ni aktiviran

To sporočilo o napaki se prikaže, ko lastnik naročnine deaktivira vaš izdelek ESET Internet Security s portala ESET HOME ali če naročnina v skupni rabi z računom ESET HOME ni več v skupni rabi. Če želite odpraviti to težavo:

- Kliknite možnost **Aktiviraj** in uporabite enega od načinov aktivacije za aktiviranje izdelka ESET Internet Security.

- Lastniku naročnine posredujte informacije, da je lastnik naročnine deaktiviral vaš izdelek ESET Internet Security ali da naročnina ni več v skupni rabi z vami. Lastnik lahko težavo odpravi na ESET HOME.

Izdelek je deaktiviran, povezava z napravo je prekinjena

To sporočilo o napaki se prikaže po odstranitvi naprave s ESET HOME. Če želite odpraviti to težavo:

- Kliknite možnost **Aktiviraj** in uporabite enega od načinov aktivacije za aktiviranje izdelka ESET Internet Security.

- Lastniku naročnine posredujte informacije, da je bil vaš izdelek ESET Internet Security deaktiviran, naprava pa ni več povezana s portalom ESET HOME.

- Če ste lastnik naročnine in niste seznanjeni s temi spremembami, preglejte vir dejavnosti ESET HOME. Če opazite sumljivo dejavnost, spremenite geslo za računESET HOME in se obrnite na tehnično podporo družbe

ESET.

Izdelek je deaktiviran, povezava z napravo je prekinjena

To sporočilo o napaki se prikaže po odstranitvi naprave s ESET HOME. Če želite odpraviti to težavo:

- Kliknite možnost **Aktiviraj** in uporabite enega od načinov aktivacije za aktiviranje izdelka ESET Internet Security.
- Lastniku naročnine posredujte informacije, da je bil vaš izdelek ESET Internet Security deaktiviran, naprava pa ni več povezana s portalom ESET HOME.
- Če ste lastnik naročnine in niste seznanjeni s temi spremembami, preglejte vir dejavnosti ESET HOME. Če opazite sumljivo dejavnost, spremenite geslo za računESET HOME in se obrnite na tehnično podporo družbe ESET.

Izdelek ni aktiviran

To sporočilo o napaki se prikaže, ko lastnik naročnine deaktivira vaš izdelek ESET Internet Security s portala ESET HOME ali če naročnina v skupni rabi z računom ESET HOME ni več v skupni rabi. Če želite odpraviti to težavo:

- Kliknite možnost **Aktiviraj** in uporabite enega od načinov aktivacije za aktiviranje izdelka ESET Internet Security.
- Lastniku naročnine posredujte informacije, da je lastnik naročnine deaktiviral vaš izdelek ESET Internet Security ali da naročnina ni več v skupni rabi z vami. Lastnik lahko težavo odpravi na ESET HOME.

0

Program za izboljšanje izkušenj strank

S pridružitvijo programu za izboljšanje izkušenj strank boste družbi ESET zagotovili anonimne podatke o uporabi naših izdelkov. Več o obdelavi podatkov lahko preberete v našem pravilniku o zasebnosti.

Vaša privolitev

Sodelovanje v programu je prostovoljno in na podlagi privolitve. Po pridružitvi je sodelovanje pasivno, kar pomeni, da vam ni treba več storiti ničesar. S spremembo nastavitev izdelkov lahko kadar koli prekličete svojo privolitev. S tem nam boste preprečili nadaljnjo obdelavo vaših anonimnih podatkov.

S spremembo nastavitev izdelkov lahko kadar koli prekličete svojo privolitev:

- Spreminjanje nastavitev programa za izboljšanje izkušenj strank v izdelkih ESET za domačo uporabo za sistem Windows

Katere vrste podatkov zbiramo?

Podatki o interakciji z izdelkom

Ti podatki nam povedo več o tem, kako se naši izdelki uporabljajo. Na podlagi podatkov na primer izvemo, katere funkcije se pogosto uporabljajo, katere nastavitve uporabniki spremenijo ali koliko časa porabijo za uporabo izdelka.

Podatki o napravah

Te podatke zbiramo, da izvemo, kje in v katerih napravah se uporabljajo naši izdelki. Običajno so to model naprave, država, različica in ime operacijskega sistema.

Podatki o diagnostiki napak

Zbirajo se tudi podatki o napakah in zrušitvah. To vključuje na primer podatke o tem, do katere napake je prišlo in katera dejanja so bila izvedena pred tem.

Zakaj zbiramo te podatke?

Na podlagi teh anonimnih podatkov lahko izboljšamo svoje izdelke za vas, uporabnike. Pomagajo nam, da so naši izdelki kar najbolj prilagojeni, enostavni za uporabo in brez motenj v delovanju.

Kdo upravlja te podatke?

Družba ESET, spol. s r.o. je edini upravljavec podatkov, ki se zbirajo v okviru programa. Podatkov ne razkrivamo tretjim osebam.

Licenčna pogodba za končnega uporabnika

Velja od 19. oktobra 2021.

POMEMBNO: Pred prenosom, namestitvijo, kopiranjem ali uporabo pazljivo preberite spodnje pogoje in določila za uporabo izdelka. **S PRENOSOM, NAMESTITVIJO, KOPIRANJEM ALI UPORABO PROGRAMSKE OPREME SOGLAŠATE S TEMI POGOJI IN DOLOČILI TER SE STRINJATE Z PRAVILNIK O ZASEBNOSTI.**

Licenčno pogodbo za končnega uporabnika

Na podlagi pogojev te licenčne pogodbe za končnega uporabnika (»pogodba«), sklenjene med družbo ESET, spol. s r. o., s sedežem na naslovu Einsteinova 24, 85101 Bratislava, Slovak Republic, registrirano v trgovinskem registru okrožnega sodišča v Bratislavi, I, razdelek Sro, vnos št. 3586/B, identifikacijska številka podjetja: 31333532 (»ESET« ali »ponudnik«) in vami, fizično ali pravno osebo (»vi« ali »končni uporabnik«), imate pravico do uporabe programske opreme, navedene v 1. členu te pogodbe. Programsko opremo, navedeno v 1. členu te pogodbe, lahko shranite na nosilec podatkov, pošljete po elektronski pošti, prenesete iz interneta, prenesete iz strežnikov ponudnika ali jo pridobite od drugih virov v skladu s spodaj navedenimi pogoji in določili.

TO JE POGODBA O PRAVICAH KONČNEGA UPORABNIKA IN NE POGODBA ZA PRODAJO. Ponudnik ostaja lastnik izvoda programske opreme in fizičnih nosilcev podatkov, ki so vključeni v prodajni paket, ter drugih izvodov, za izdelavo katerih je v skladu s to pogodbo pooblaščen končni uporabnik.

S klikom možnosti »Sprejemam« ali »Sprejemam ...« med nameščanjem, prenašanjem, kopiranjem ali uporabo programske opreme soglašate s pogoji in določili te pogodbe ter potrjujete pravilnik o zasebnosti. Če ne soglašate

z vsemi pogoji in določili iz te pogodbe in/ali s pravilnikom o zasebnosti, takoj kliknite možnost za preklic, prekličite postopek namestitve ali prenosa oz. uničite ali vrnite programsko opremo, namestitvene nosilce podatkov, priloženo dokumentacijo in račun ponudniku, pri katerem ste kupili programsko opremo.

SOGLAŠATE, DA VAŠA UPORABA PROGRAMSKE OPREME POMENI, DA STE PREBRALI TO POGODBO, JO RAZUMETE IN BOSTE RAVNALI V SKLADU S POGOJI IN DOLOČILI V NJEJ.

1. **Programska oprema.** Izraz »programska oprema«, kot je uporabljen v tej pogodbi, pomeni: (i) računalniški program, ki ga spremlja ta pogodba, in vse pripadajoče komponente; (ii) vso vsebino na diskih, CD-ROM-ih, DVD-jih, v e-poštnih sporočilih in v vseh prilogah ali na drugih nosilcih podatkov, ki jim je priložena ta pogodba, vključno s programsko opremo v obliki predmetne kode, dobavljene na nosilcu podatkov, prek elektronske pošte ali s prenosom prek interneta; (iii) vso pisno gradivo z navodili in vse druge morebitne dokumente, povezane s programsko opremo, predvsem kakršne koli opise programske opreme, specifikacije programske opreme, kakršne koli opise lastnosti ali delovanja programske opreme, kakršne koli opise delovnega okolja za uporabo programske opreme, navodila za uporabo ali namestitev programske opreme ali kakršen koli opis načina uporabe programske opreme (»dokumentacija«); (iv) izvode programske opreme, popravke za morebitne napake v programski opremi, dodatke programske opreme, razširitve programske opreme, spremenjene različice programske opreme in posodobitve komponent programske opreme, če so na voljo, za katere vam ponudnik podeljuje licenco v skladu s 3. členom te pogodbe. Programska oprema bo zagotovljena izključno v obliki izvedljive predmetne kode.

2. **Namestitev, računalnik in licenčni ključ**. Programsko opremo, dobavljeno na nosilcu podatkov, poslano prek elektronske pošte, preneseno iz interneta, preneseno iz ponudnikovih strežnikov ali pridobljeno od drugih virov, je treba namestiti. Programsko opremo morate namestiti v pravilno konfiguriran računalnik, ki izpolnjuje vsaj tiste zahteve, ki so navedene v dokumentaciji. Postopek namestitve je opisan v dokumentaciji. V računalnik, v katerega namestite programsko opremo, ne smete namestiti nobenih računalniških programov ali strojne opreme, ki bi neugodno vplivali na programsko opremo. Računalnik pomeni strojno opremo, med drugim osebne računalnike, prenosne računalnike, delovne postaje, dlančnike, pametne telefone, ročne elektronske naprave ali druge elektronske naprave, za katere je programska oprema zasnovana in v katerih bo nameščena in/ali uporabljana. Licenčni ključ pomeni enolično zaporedje simbolov, črk, številk ali posebnih znakov, posredovano končnemu uporabniku za zakonito uporabo programske opreme in njene posamezne različice ali podaljšanje veljavnosti licence v skladu s to pogodbo.

3. **Licenca**. Pod pogojem, da soglašate z določili te pogodbe, plačate licenčnino do datuma zapadlosti in ravnate v skladu z vsemi določili ter pogoji, določenimi tukaj, vam ponudnik podeli te pravice (»licenco«):

a) **Namestitev in uporaba.** Imate neizključno in neprenosljivo pravico, da namestite programsko opremo na trdi disk računalnika ali drug nosilec podatkov za trajno shranjevanje podatkov, da namestite in shranite programsko opremo v pomnilnik računalniškega sistema ter da uporabljate, shranite in prikazujete programsko opremo.

b) **Določba o številu licenc.** Pravica do uporabe programske opreme je vezana na število končnih uporabnikov. En končni uporabnik pomeni spodaj navedeno: (i) namestitev programske opreme v en računalniški sistem oziroma, (ii) če je obseg licence vezan na število poštnih predalov, potem en končni uporabnik pomeni uporabnika računalnika, ki sprejme elektronsko sporočilo prek poštnega uporabniškega agenta (»MUA«). Če agent MUA sprejme elektronsko sporočilo in ga samodejno posreduje več uporabnikom, je število končnih uporabnikov določeno skladno z dejanskim številom uporabnikov, ki jim je posredovano elektronsko sporočilo. Če ima poštni strežnik funkcijo poštnih vrat, je število končnih uporabnikov enako številu uporabnikov poštnih strežnikov, za katere ta vrata ponujajo storitve. Če je poljubno število elektronskih naslovov usmerjeno na enega uporabnika (npr. vključno z vzdevki), in jih ta sprejme, ter odjemalec teh sporočil ne posreduje samodejno več uporabnikom, je zahtevana licenca za en računalnik. Iste licence ne smete hkrati uporabljati v več kot enem računalniku. Končni uporabnik je upravičen do vnosa licenčnega ključa v programsko opremo le v obsegu, v katerem ima končni uporabnik pravico do uporabe programske opreme v skladu z omejitvami števila licenc, ki jih je podelil ponudnik. Licenčni ključ je zaupen, zato licence ne smete deliti s tretjimi osebami ali tretjim osebam dovoliti uporabe

licenčnega ključa, razen če to dovoljuje pogodba ali ponudnik. Če pride do zlorabe licenčnega ključa, takoj obvestite ponudnika.

c) **Home/Business Edition.** Različica Home Edition programske opreme je lahko uporabljena izključno v zasebnih in/ali nekomercialnih okoljih, samo za domačo in družinsko uporabo. Različica Business Edition programske opreme je treba pridobiti za uporabo v komercialnem okolju in za uporabo programske opreme v poštnih strežnikih, poštnih posredovalnikih, poštnih ali internetnih prehodih.

d) **Veljavnost licence.** Vaša pravica do uporabe programske opreme je časovno omejena.

e) **Programska oprema izvirnega izdelovalca računalniške opreme (OEM).** Programska oprema, označena kot »OEM«, bo omejena na računalnik, s katerim ste jo pridobili. Programske opreme ni dovoljeno prenesti v drug računalnik.

f) **PRESKUSNA RAZLIČICA programske opreme (NFR).** Programske opreme, ki je označena kot »Ni za nadaljnjo prodajo«, »NFR« ali »PRESKUSNA RAZLIČICA«, ni mogoče zaračunati in se mora uporabljati le za predstavitev ali preskušanje funkcij programske opreme.

g) **Prenehanje veljavnosti licence.** Licenca preneha veljati samodejno, ko se konča obdobje, za katero je bila dodeljena. Če kršite katero koli določilo te pogodbe, lahko ponudnik odpove to pogodbo, ne da bi to vplivalo na katero koli pravico ali pravno sredstvo, ki je na voljo ponudniku v takšnih primerih. V primeru preklica licence morate programsko opremo in vse varnostne kopije na svoje stroške takoj izbrisati ali uničiti oziroma jo vrniti družbi ESET ali trgovini, kjer ste kupili programsko opremo. Po prekinitvi licenčne pogodbe ima ponudnik pravico preklicati pravico končnega uporabnika za uporabo funkcij programske opreme, ki zahtevajo povezavo s strežniki ponudnika ali tretjih oseb.

4. **Funkcije z zbiranjem podatkov in zahteve za internetno povezavo**. Za pravilno delovanje programske opreme je potrebna povezava z internetom in redno vzpostavljanje povezave s ponudnikovimi strežniki ali strežniki tretjih oseb ter ustrezno zbiranje podatkov v skladu s pravilnikom o zasebnosti. Povezava z internetom in ustrezno zbiranje podatkov je potrebno za spodaj navedene funkcije programske opreme:

a) **Posodobitve programske opreme.** Ponudnik lahko občasno izda posodobitve ali nadgradnje programske opreme (»posodobitve«), vendar jih ni dolžan zagotoviti. Ta funkcija je omogočena v okviru standardnih nastavitev programske opreme in posodobitve so zato nameščene samodejno, razen če ni končni uporabnik onemogočil samodejne namestitve posodobitev. Za zagotavljanje posodobitev je potrebno preverjanje pristnosti licence, vključno s podatki o računalniku in/ali platformi, v kateri je nameščena programska oprema, v skladu s pravilnikom o zasebnosti.

Za zagotavljanje posodobitev lahko velja pravilnik o koncu življenjske dobe (»pravilnik EOL«), ki je na voljo na spletnem mestu https://go.eset.com/eol_home. Ko programska oprema ali katera koli od njenih funkcij doseže datum konca življenjske dobe, kot je določeno v pravilniku EOL, posodobitve ne bodo zagotovljene.

b) **Posredovanje infiltracij in podatkov ponudniku.** Programska oprema vključuje funkcije, ki zbirajo vzorce računalniških virusov, drugih podobnih zlonamernih računalniških programov in sumljivih ali spornih datotek, morebitno neželenih ali morebitno nevarnih predmetov, kot so datoteke, URL-ji, paketi IP in ethernetni okvirji (»infiltracije«), ki jih nato pošlje ponudniku, vključno s podatki o namestitvi, računalniku in/ali platformi, na kateri je nameščena programska oprema, vendar ne omejeno nanje, ter vključno s podatki o postopkih in funkcijah programske opreme (»podatki«). Podatki in infiltracije lahko vsebujejo podatke (vključno z naključno ali nenamerno pridobljenimi osebnimi podatki) o končnem uporabniku ali drugih uporabnikih računalnika, v katerem je nameščena programska oprema, in datoteke, na katere je vplivala infiltracija, ter povezane metapodatke.

Podatke in infiltracije lahko zbirata naslednji funkciji programske opreme:

i. funkcija sistema za preverjanje ugleda LiveGrid zbiranje in pošiljanje enosmernih razpršitev, povezanih z infiltracijami, ponudniku. To funkcijo je mogoče omogočiti v standardnih nastavitvah programske opreme;

ii. Funkcija sistema za povratne informacije LiveGrid vključuje zbiranje in pošiljanje infiltracij s povezanimi metapodatki in podatkov ponudniku. To funkcijo lahko aktivira končni uporabnik med postopkom nameščanja programske opreme.

Ponudnik bo prejete podatke in infiltracije uporabil za analizo in raziskave o infiltracijah, izboljšanje programske opreme in preverjanje pristnosti licenc ter bo izvajal ustrezne ukrepe, da zagotovi varnost prejetih infiltracij in podatkov. Po aktivaciji te funkcije programske opreme lahko ponudnik zbira in obdeluje infiltracije in podatke, kot je navedeno v pravilniku o zasebnosti in v skladu z ustreznimi pravnimi uredbami. Te funkcije lahko kadar koli deaktivirate.

Za namene te pogodbe mora ponudnik zbirati, obdelovati in hraniti podatke, ki mu omogočajo vašo prepoznavo, v skladu s pravilnikom o zasebnosti. Potrjujete, da ponudnik prek lastnih sredstev preverja, ali uporabljate programsko opremo v skladu z določili te pogodbe. Potrjujete, da je za namene te pogodbe potreben prenos vaših podatkov med komunikacijo med programsko opremo in računalniškimi sistemi ponudnika ali računalniškimi sistemi njegovih poslovnih partnerjev znotraj ponudnikove mreže za distribucijo in podporo, da lahko ponudnik zagotovi delovanje programske opreme in dovoljenje za uporabo programske opreme ter zaradi zaščite ponudnikovih pravic.

Soglasno s sklepom iz te pogodbe imajo ponudnik in njegovi poslovni partnerji znotraj ponudnikove mreže za distribucijo in podporo pravico do prenosa, obdelave in hranjenja pomembnih podatkov, ki omogočajo vašo prepoznavo, za namene zaračunavanja, izvajanja te pogodbe ter pošiljanja obvestil v vaš računalnik.

Podrobnosti o zasebnosti, varovanju osebnih podatkov in vaših pravicah kot posameznik, na katerega se podatki nanašajo, najdete v pravilniku o zasebnosti, do katerega lahko dostopate na ponudnikovem spletnem mestu ali neposredno med postopkom namestitve. Do njega lahko dostopate tudi iz razdelka za pomoč za programsko opremo.

5. **Uporaba pravic končnega uporabnika.** Pravice končnega uporabnika morate uporabiti vi osebno ali vaši zaposleni. Programsko opremo lahko uporabite izključno za to, da zavarujete svoje operacije in zaščitite tiste računalnike ali računalniške sisteme, za katere ste pridobili licenco.

6. **Omejitev pravic.** Ne smete kopirati, posredovati, ekstrahirati komponent ali ustvariti izpeljanih del iz programske opreme. Pri uporabi programske opreme morate upoštevati spodaj navedene omejitve:

a) Lahko ustvarite eno kopijo programske opreme na nosilcu za trajno shranjevanje podatkov kot arhivsko varnostno kopijo pod pogojem, da arhivske varnostne kopije ne boste namestili v noben računalnik ali je v njem uporabili. S kakršno koli drugo kopijo programske opreme, ki jo naredite, kršite to pogodbo.

b) Pravic za uporabo programske opreme ali kopij programske opreme ne smete uporabljati, spreminjati, prevajati, reproducirati na kakršen koli način, razen kot je izrecno navedeno v tej pogodbi.

c) Programske opreme ne smete prodajati, podlicencirati, dajati v zakup ali najem, je posoditi oziroma uporabiti za omogočanje komercialnih storitev.

d) Ne smete izvajati obratnega inženiringa, povratnega prevajanja ali razstavljati programske opreme ali kakor koli drugače poskušati odkriti izvorno kodo programske opreme, razen do mere, za katero je navedena omejitev izrecno zakonsko prepovedana.

e) Soglašate, da boste programsko opremo uporabljali na način, ki je v skladu z vsemi veljavnimi zakoni v pristojnosti, kjer jo uporabljate, vključno, vendar ne omejeno na, z veljavnimi omejitvami glede avtorskih pravic in

drugih pravic intelektualne lastnine.

f) Strinjate se, da boste programsko opremo in njene funkcije uporabljali samo tako, da drugim končnim uporabnikom ne boste omejili možnosti dostopa do teh storitev. Ponudnik si pridržuje pravico, da omeji obseg storitev, ki so na voljo posameznim končnim uporabnikom da bi tako lahko omogočil uporabo storitev največjemu možnemu številu končnih uporabnikov. Če ponudnik omeji obseg storitev, tudi povsem onemogoči uporabo katere koli funkcije programske opreme ter izbriše podatke in informacije iz strežnikov ponudnika ali strežnikov tretjih oseb, ki so povezani z določeno funkcijo programske opreme.

g) Soglašate, da ne boste izvajali nobenih dejavnosti v zvezi z uporabo licenčnega ključa, ki so v nasprotju z določili te pogodbe ali lahko vodijo do zagotovitve licenčnega ključa osebi, ki ni pooblaščena za uporabo programske opreme, kot je prenos uporabljenega ali neuporabljenega licenčnega ključa v kateri koli obliki ter nepooblaščena reprodukcija ali distribucija podvojenih ali generiranih licenčnih ključev ali uporaba programske opreme z licenčnim ključem, pridobljenim od drugega vira kot ponudnika.

7. **Avtorske pravice**. Programska oprema in vse pravice, vključno z lastninskimi pravicami in pravicami intelektualne lastnine v programski opremi, vendar ne omejeno nanje, so last družbe ESET in/ali njenih izdajateljev licenc. ESET in njegovi izdajatelji licenc so zaščiteni z določili mednarodnih sporazumov in vsemi veljavnimi zakoni države, v kateri se uporablja programska oprema. Struktura, organizacija in koda programske opreme so pomembne poslovne skrivnosti in zaupni podatki družbe ESET in/ali njenih ponudnikov licenc. Programske opreme ne smete kopirati, razen kot je navedeno v členu 6 (a). Vse kopije, ki jih ustvarite skladno s to pogodbo, morajo vsebovati enaka obvestila o avtorskih pravicah, kot so navedena v programski opremi. Če izvajate obratni inženiring za potrebe odkrivanja izvorne kode programske opreme, jo obratno prevajate, razstavljate ali jo poskušate kako drugače odkriti, na način, ki krši določila te pogodbe, soglašate, da bodo vse tako pridobljene informacije samodejno in nepreklicno prenesene na ponudnika in bo ponudnik v celoti postal njihov lastnik, od trenutka nastanka takšnih informacij, kljub pravicam ponudnika v povezavi s kršitvijo te pogodbe.

8. **Pridržanje pravic**. Ponudnik si s tem pridržuje vse pravice do programske opreme, razen pravic, ki so vam kot končnemu uporabniku programske opreme izrecno dodeljene pod pogoji iz te pogodbe.

9. **Več jezikovnih različic, programski izdelek na dveh različnih nosilcih podatkov, več izvodov**. Če programska oprema podpira več platform ali jezikov ali če prejmete več izvodov programske opreme, lahko uporabljate le programsko opremo za tisto število računalniških sistemov in tiste različice, za katere ste pridobili licenco. Različic ali izvodov programske opreme, ki jih vi sami ne uporabljate, ne smete prodajati, dajati v najem, dajati v zakup, podlicencirati, posojati ali prenašati na druge osebe.

10. **Začetek in prekinitev veljavnosti pogodbe.** Ta pogodba velja od datuma, ko ste potrdili, da soglašate s pogoji te pogodbe. To pogodbo lahko kadar koli prekinete, tako da na svoje stroške trajno odstranite, uničite ali vrnete programsko opremo, vse varnostne kopije in vsa pripadajoča gradiva, ki vam jih je posredoval ponudnik ali njegovi poslovni partnerji. Za vašo pravico do uporabe programske opreme in njenih funkcij lahko velja pravilnik EOL. Ko programska oprema ali katera koli od njenih funkcij doseže datum konca življenjske dobe, opredeljen v pravilniku EOL, bo vaša pravica do uporabe programske opreme prekinjena. Ne glede na način prekinitve te pogodbe, bodo določila iz 7., 8., 11., 13., 19. in 21. člena še naprej veljali za neomejeno obdobje.

11. **IZJAVE KONČNEGA UPORABNIKA**. KOT KONČNI UPORABNIK SOGLAŠATE, DA JE PROGRAMSKA OPREMA ZAGOTOVLJENA »V TAKŠNEM STANJU, KOT JE«, BREZ KAKRŠNEGA KOLI JAMSTVA, IZRECNEGA ALI NAZNAČENEGA, IN V NAJVEČJI MOGOČI MERI, KI JO DOVOLJUJE VELJAVNA ZAKONODAJA. NITI PONUDNIK, NJEGOVI PONUDNIKI LICENC ALI LASTNIŠKO POVEZANA PODJETJA, NITI LASTNIKI AVTORSKIH PRAVIC NE DAJEJO NIKAKRŠNIH ZAGOTOVIL ALI JAMSTEV, IZRECNIH ALI NAZNAČENIH, VKLJUČNO Z, A NE OMEJENO NA JAMSTVA GLEDE PRIMERNOSTI ZA PRODAJO, PRIMERNOSTI ZA DOLOČEN NAMEN ALI JAMSTVA, DA PROGRAMSKA OPREMA NE KRŠI NOBENIH PATENTOV, AVTORSKIH PRAVIC, BLAGOVNIH ZNAMK ALI DRUGIH PRAVIC TRETJIH OSEB. PONUDNIK ALI KATERA KOLI DRUGA STRANKA NE DAJE NOBENEGA JAMSTVA, DA BODO FUNKCIJE, KI SO

VKLJUČENE V PROGRAMSKO OPREMO, IZPOLNJEVALE VAŠE ZAHTEVE ALI DA BO PROGRAMSKA OPREMA DELOVALA NEPREKINJENO ALI BREZ NAPAK. NASE PREVZAMETE VSO ODGOVORNOST IN TVEGANJE PRI IZBIRI PROGRAMSKE OPREME ZA DOSEGANJE ŽELENIH REZULTATOV TER ZA NAMESTITEV, UPORABO IN REZULTATE, KI JIH BOSTE DOSEGLI S PROGRAMSKO OPREMO.

12. **Brez drugih obveznosti**. S to pogodbo ponudnik in njegovi izdajatelji licenc nimajo nobenih obveznosti, razen tistih, ki so izrecno navedene tukaj.

13. **OMEJITEV ODGOVORNOSTI**. V NAJVEČJI MOGOČI MERI, KI JO DOVOLJUJE VELJAVNA ZAKONODAJA, PONUDNIK, NJEGOVI ZAPOSLENI ALI PONUDNIKI LICENC V NOBENEM PRIMERU NISO ODGOVORNI ZA KAKRŠNO KOLI IZGUBO DOBIČKA, PRIHODKA, PRODAJE, PODATKOV ALI ZA STROŠKE, KI SO POSLEDICA NABAVE DODATNIH IZDELKOV ALI STORITEV, ZA POŠKODBO LASTNINE, OSEBNO POŠKODBO, PREKINITEV POSLOVANJA, IZGUBO POSLOVNIH PODATKOV ALI ZA KAKRŠNO KOLI POSEBNO, NEPOSREDNO, POSREDNO, NENAMERNO, GOSPODARSKO, KAZENSKO, POSEBNO ALI POSLEDIČNO ŠKODO, KI JE POVZROČENA NA KATERI KOLI NAČIN, NE GLEDE NA TO, ALI IZHAJA IZ POGODBE, POMANJKLJIVOSTI, MALOMARNOSTI ALI DRUGEGA DEJSTVA, KI JE POVZROČILO NASTANEK ODGOVORNOSTI IN JE POSLEDICA NAMESTITVE, UPORABE ALI NEZMOŽNOSTI UPORABE RAČUNA, TUDI ČE SO BILI PONUDNIK ALI NJEGOVI PONUDNIKI LICENC ALI LASTNIŠKO POVEZANA PODJETJA OBVEŠČENI O MOŽNOSTI TAKŠNE ŠKODE. NEKATERE DRŽAVE IN PRISTOJNOSTI NE DOVOLJUJEJO IZKLJUČITVE ODGOVORNOSTI PONUDNIKA, VENDAR LAHKO DOVOLJUJEJO OMEJITEV ODGOVORNOSTI, ZATO JE V TAKŠNIH PRIMERIH ODGOVORNOST PONUDNIKA, NJEGOVIH ZAPOSLENIH ALI IZDAJATELJEV LICENC ALI LASTNIŠKO POVEZANIH PODJETIJ OMEJENA NA SKUPNI ZNESEK, KI STE GA PLAČALI ZA LICENCO.

14. Nič iz te pogodbe ne vpliva na zakonite pravice katere koli pogodbene stranke, obravnavane kot potrošnik, če bi ta stranka ravnala v nasprotju s to pogodbo.

15. **Tehnična podpora**. ESET ali tretje osebe, ki jih pooblasti ESET, bodo zagotovile tehnično podporo po lastni presoji, brez kakršnih koli jamstev ali izjav. Ko programska oprema ali katera koli od njenih funkcij doseže datum konca življenjske dobe, kot je določeno v pravilniku EOL, ne bo zagotovljena tehnična podpora. Pred zagotovitvijo tehnične podpore mora končni uporabnik varnostno kopirati vse obstoječe podatke, programsko opremo in programske pripomočke. ESET in/ali tretje osebe, ki jih pooblasti ESET, ne morejo sprejeti odgovornosti za škodo ali izgubo podatkov, lastnine, programske ali strojne opreme ali izgubo dobička zaradi zagotavljanja tehnične podpore. ESET in/ali tretje osebe, ki jih pooblasti ESET, si pridržujejo pravico do odločitve, da reševanje težave presega obseg tehnične podpore. ESET si pridržuje pravico do zavrnitve, opustitve ali prekinitve zagotavljanja tehnične podpore po lastni presoji. Za namene zagotavljanja tehnične podpore so lahko potrebni licenčni podatki, podatki in drugi podatki v skladu s pravilnikom o zasebnosti.

16. **Prenos licence**. Programsko opremo lahko prenesete iz enega računalniškega sistema v drugega, razen če je to v nasprotju s pogoji te pogodbe. Če ni v nasprotju s pogoji te pogodbe, lahko končni uporabnik trajno prenese licenco in vse pravice, ki izhajajo iz te pogodbe, na drugega končnega uporabnika le s privolitvijo ponudnika, pod pogojem, da (i) prvi končni uporabnik ne obdrži nobenega izvoda programske opreme; (ii) je prenos pravic neposreden, kar pomeni od prvega končnega uporabnika na novega končnega uporabnika; (iii) novi končni uporabnik prevzame vse pravice in obveznosti, ki so naložene prvemu končnemu uporabniku v skladu s pogoji te pogodbe; (iv) da prvi končni uporabnik novemu končnemu uporabniku posreduje dokumentacijo, s čimer omogoči preverjanje pristnosti programske opreme, kot je določeno v 17. členu.

17. **Preverjanje pristnosti programske opreme.** Končni uporabnik lahko dokazuje pravico do uporabe programske opreme na enega od spodaj navedenih načinov: (i) s potrdilom o licenci, ki ga je izdal ponudnik ali tretja oseba, ki jo je imenoval ponudnik; (ii) s pisno licenčno pogodbo, če je bila taka pogodba sklenjena; (iii) s predložitvijo e-poštnega sporočila ponudnika, v katerem so navedeni podatki o licenci (uporabniško ime in geslo). Za namene preverjanja pristnosti programske opreme so lahko potrebni licenčni podatki in podatki za prepoznavo končnega uporabnika v skladu s pravilnikom o zasebnosti.

18. **Licenciranje za državne organe in Vlado Združenih držav Amerike**. Programska oprema bo državnim organom, vključno z Vlado Združenih držav Amerike, posredovana z licenčnimi pravicami in omejitvami, ki so opisane v tej pogodbi.

19. **Skladnost z zakonodajo o nadzoru trgovine**.

a) Programske opreme ne smete neposredno ali posredno izvoziti, ponovno izvoziti, prenesti oz. komur koli omogočiti dostop do nje ter je ne smete uporabiti na kateri koli način oz. biti vpleteni v kateri koli postopek, zaradi česar bi družba ESET, njene holdinške družbe ali hčerinske družbe, hčerinske družbe katere koli od njenih holdinških družb ter entitete pod nadzorom njenih holdinških družb (»hčerinske družbe«) kršile ali imele negativne posledice na podlagi zakonodaje o nadzoru trgovine, kar vključuje

i. katere koli zakone, ki urejajo, omejujejo ali uvajajo zahteve za licenciranje glede izvoza, vnovičnega izvoza oz. prenosa blaga, programske opreme, tehnologije ali storitev, ki jih izda oz. uvede katera koli vlada, država ali regulativni organ Združenih držav Amerike, Singapurja, Združenega kraljestva, Evropske unije oz. katere koli države članice ali katere koli države, ki zahteva izpolnjevanje obveznosti iz te pogodbe ali v kateri je prisotna oz. deluje družba ESET ali katera koli od njenih hčerinskih družb ter

ii. katero koli gospodarsko, finančno, tržno ali drugo sankcijo, omejitev, embargo ali prepoved uvoza oz. izvoza ter katero koli prepoved prenosa sredstev oz. premoženja ali izvajanja storitev oz. morebitni enakovredni ukrep, ki ga uvede katera koli vlada, država ali regulativni organ Združenih držav Amerike, Singapurja, Združenega kraljestva, Evropske unije oz. katere koli države članice ali katere koli države, ki zahteva izpolnjevanje obveznosti iz te pogodbe ali v kateri je prisotna oz. deluje družba ESET ali katera koli od njenih hčerinskih družb.

(pravni akti v točkah i in ii zgoraj, skupno kot »zakonodaja o nadzoru trgovine«).

b) ESET ima pravico, da s takojšnjim učinkom začasno ali trajno opusti svoje obveznosti, ki izhajajo iz teh pogojev, če:

i. v obrazloženem mnenju ugotovi, da je uporabnik kršil ali bo verjetno kršil določilo člena 19 a) te pogodbe, ali

ii. za končnega uporabnika in/ali programsko opremo začne veljati zakonodaja o nadzoru trgovine in posledično ESET v obrazloženem mnenju ugotovi, da bi v primeru nadaljnjega izpolnjevanja svojih obveznosti iz te pogodbe družba ESET ali njena hčerinska družba kršila oz. imela negativne posledice na podlagi zakonodaje o nadzoru trgovine.

c) Nobeno določilo te pogodbe ne predvideva in se ga ne sme razumeti ali razlagati tako, da bi katero koli od pogodbenic spodbudilo oz. prisililo k delovanju ali opustitvi delovanja (ali k dogovoru glede delovanja oz. opustitve delovanja) na način, ki ni skladen z veljavno zakonodajo o nadzoru trgovine oz. jo ta kaznuje ali prepoveduje.

20. **Obvestila**. Vsa obvestila pošljite ter programsko opremo in dokumentacijo vrnite na naslov: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, ne da bi to vplivalo na pravico družbe ESET, da vam sporoči kakršne koli spremembe te pogodbe, pravilnikov o zasebnosti, pravilnika EOL in dokumentacije v skladu z 22. členom te pogodbe. Družba ESET vam lahko pošilja e-poštna sporočila, obvestila v aplikaciji prek programske opreme ali objavi obvestila na našem spletnem mestu. Soglašate, da boste od družbe ESET prejemali pravna obvestila v elektronski obliki, vključno z obvestili o spremembi pogojev, posebnih pogojev ali pravilnikov o zasebnosti, predlogi/sprejetjem pogodb ali povabili k obravnavi, obvestili ali drugimi pravnimi obvestili. Za tovrstno elektronsko komunikacijo se šteje, da je prejeta v pisni obliki, razen če veljavna zakonodaja zahteva drugačno obliko komunikacije.

21. **Veljavna zakonodaja**. To pogodbo ureja slovaška zakonodaja, skladno s katero se ta pogodba tudi razlaga. Končni uporabnik in ponudnik soglašata, da nasprotujoča določila veljavne zakonodaje in Konvencija Združenih

narodov o pogodbah glede mednarodne prodaje blaga ne veljajo. Izrecno soglašate, da se vsi spori ali zahteve, ki izhajajo iz te pogodbe glede ponudnika ali kakršen koli spor ali katere koli zahteve, ki se nanašajo na uporabo programske opreme, rešujejo na okrožnem sodišču v Bratislavi, I, in izrecno soglašate s pristojnostjo za odločanje navedenega sodišča.

22. **Splošna določila**. Če je katero koli določilo te pogodbe neveljavno ali neizvršljivo, to ne vpliva na veljavnost drugih določil te pogodbe, ki ostanejo veljavna in izvršljiva v skladu s pogoji, določenimi tukaj. Ta pogodba je bila sklenjena v angleščini. Če je pogodba prevedena v kateri koli jezik za lažje razumevanje ali za kateri koli drug namen, v primeru neskladja med jezikovnimi različicami te pogodbe prevlada angleška različica.

Družba ESET si pridržuje pravico, da lahko kadar koli spremeni programsko opremo te pogodbe, njene priloge, dodatke, pravilnik o zasebnosti, pravilnik EOL in dokumentacijo ali kateri koli del te dokumentacije tako, da zadevni dokument posodobi (i) v skladu s spremembami programske opreme ali načina poslovanja družbe ESET, (ii) iz pravnih, regulativnih ali varnostnih razlogov ali (iii) za preprečevanje zlorabe ali škode. O spremembah te pogodbe boste obveščeni prek e-pošte, obvestil v aplikaciji ali z drugimi elektronskimi sredstvi. Če se ne strinjate s predlaganimi spremembami pogodbe, jo lahko prekinete v skladu z 10. členom v 30 dneh po prejemu obvestila o spremembi. Če pogodbe ne prekinete v tem časovnem obdobju, bodo predlagane spremembe sprejete in bodo za vas postale veljavne od datuma, ko ste prejeli obvestilo o spremembi.

To je celotna pogodba med ponudnikom in vami, ki se nanaša na programsko opremo, ter v celoti nadomesti vse predhodne pravice, razprave, zaveze, komunikacije ali oglase, povezane s programsko opremo.

DODATEK K POGODBI

Ocena varnosti naprav, ki imajo vzpostavljeno povezavo z omrežjem. Dodatna določila, ki veljajo za oceno varnosti naprav, ki imajo vzpostavljeno povezavo z omrežjem:

Programska oprema vključuje funkcijo za preverjanje varnosti lokalnega omrežja končnega uporabnika in varnosti naprav v lokalnem omrežju, ki zahteva ime lokalnega omrežja in podatke o napravah v lokalnem omrežju, kot so prisotnost, vrsta, ime, naslov IP in naslov MAC naprave v lokalnem omrežju v povezavi s podatki o licenci. Podatki vključujejo tudi vrsto brezžične zaščite in vrsto brezžičnega šifriranja za usmerjevalnike. Ta funkcija lahko zagotovi tudi podatke o razpoložljivosti rešitve za varnostno programsko opremo za varovanje naprav v lokalnem omrežju.

Zaščita pred zlorabo podatkov. Dodatna določila, ki veljajo za zaščito pred zlorabo podatkov:

Programska oprema vključuje funkcijo, ki v primeru kraje računalnika preprečuje izgubo ali zlorabo pomembnih podatkov. Ta funkcija je v okviru privzetih nastavitev programske opreme izklopljena. Za aktiviranje te funkcije morate ustvariti račun ESET HOME, prek katerega funkcija aktivira zbiranje podatkov v primeru kraje računalnika. Če ste aktivirali to funkcijo programske opreme, se bodo zbirali podatki o ukradenem računalniku, ki bodo posredovani ponudniku. V te poslane podatke so lahko vključeni podatki o omrežni lokaciji računalnika, podatki o prikazani vsebini na računalniškem zaslonu, podatki o konfiguraciji računalnika ali podatki, ki jih zabeleži kamera, priključena na računalnik (v nadaljevanju »podatki«). Končni uporabnik lahko podatke, pridobljene s to funkcijo in zagotovljene prek računa ESET HOME, uporabi izključno za odpravo neugodne situacije zaradi kraje računalnika. Ponudnik izključno za namene te funkcije obdeluje podatke, kot je navedeno v pravilniku o zasebnosti in v skladu z ustreznimi pravnimi predpisi. Ponudnik dovoli končnemu uporabniku, da dostopa do podatkov v časovnem obdobju, ki ga potrebuje za dosego namena, za katerega je končni uporabnik pridobil podatke, vendar to obdobje ne more presegati obdobja hranjenja podatkov, navedenega v pravilniku o zasebnosti. Končni uporabnik lahko zaščito pred zlorabo podatkov uporablja izključno v računalnikih in računih, do katerih ima zakonit dostop. Vse vrste nezakonite uporabe bodo prijavljene pristojnim organom. Ponudnik bo ravnal skladno z ustreznimi zakoni in v primeru zlorabe pomagal organom kazenskega pregona. Potrjujete in soglašate, da ste odgovorni za zaščito gesla, s katerim dostopate do računa ESET HOME, in se strinjate, da svojega gesla ne boste razkrili nobeni tretji osebi. Končni uporabnik je odgovoren za vse odobrene ali neodobrene dejavnosti, v katerih sta uporabljena funkcija zaščite pred zlorabo podatkov in račun ESET HOME. Če je račun ESET HOME ogrožen, nemudoma

obvestite ponudnika. Dodatna določila za zaščito pred zlorabo podatkov veljajo samo za končne uporabnike izdelkov ESET Internet Security in ESET Smart Security Premium.

ESET Secure Data. Dodatna določila, ki veljajo za programsko opremo ESET Secure Data:

1. Opredelitve. V dodatnih določilih za funkcijo ESET Secure Data imajo navedene besede naslednji pomen:

a) »Informacije« vse informacije in podatki, šifrirani ali dešifrirani s programsko opremo;

b) »Izdelki« so programska oprema ESET Secure Data in dokumentacija;

c) »ESET Secure Data« je programska oprema za šifriranje in dešifriranje elektronskih podatkov;

Vse omembe v množini veljajo tudi za ednino in vse omembe v moškem spolu vključujejo tudi ženskega in srednjega ter obratno. Besede brez izrecne opredelitve so uporabljene v skladu z opredelitvami v pogodbi.

2. Dodatne izjave končnega uporabnika. Potrjujete in sprejemate naslednje:

a) ste sami odgovorni za zaščito, vzdrževanje in varnostno kopiranje podatkov;

b) morate varnostno kopirati vse podatke in informacije (vključno z vsemi ključnimi podatki, vendar ne omejeno na njih) v računalniku, preden namestite programsko opremo ESET Secure Data;

c) Obvezani ste na varnem hraniti vsa gesla in druge podatke, uporabljene za nastavitev in uporabo izdelka ESET Secure Data; prav tako morate izdelati varnostne kopije vseh šifrirnih ključev, kod licence, datotek s ključi in drugih generiranih podatkov ter jih shraniti v ločenem nosilcu podatkov;

d) Odgovorni ste za uporabo izdelkov. Ponudnik v nobenem primeru ni odgovoren za nobeno izgubo ali škodo, do katere pride v primeru kakršnega koli nepooblaščenega ali zmotnega šifriranja ali dešifriranja informacij ali drugih podatkov, kjer koli in kakor koli so ti podatki in informacije shranjeni;

e) Ne glede na to, da je ponudnik izvedel vse razumne ukrepe za zagotavljanje celovitosti in varnosti izdelka ESET Secure Data, izdelkov (ali katerega koli od njih) ni dovoljeno uporabljati v okolju, ki zahteva varnost brez izpada, ali je morebitno ali dejansko nevarno, med drugim v jedrskih obratih, pri usmerjanju letal, v nadzornih ali komunikacijskih sistemih, orožnih in obrambnih sistemih in sistemih za ohranjanje ali spremljanje življenjskih znakov;

f) Končni uporabnik je odgovoren, da zagotovi, da sta stopnji varnosti in šifriranja, ki ju zagotavljajo izdelki, ustrezni za njegove potrebe;

g) Odgovorni ste za lastno uporabo izdelkov (ali katerega koli od njih), vključno z zagotavljanjem, da je uporaba skladna z vsemi veljavnimi zakoni in uredbami Slovaške republike ali druge države, regije ali zvezne države, v kateri se izdelek uporablja. Pred katero koli uporabo izdelkov morate zagotoviti, da ne kršite morebitne državne prepovedi trgovanja (ki velja v Slovaški republiki ali drugi državi);

h) ESET Secure Data lahko občasno komunicira s ponudnikovimi strežniki in preveri licenčne podatke, razpoložljive popravke, servisne pakete in druge posodobitve, ki lahko izboljšajo, vzdržujejo, spremenijo ali nadgradijo delovanje izdelka ESET Secure Data, ter lahko pošilja splošne sistemske informacije v povezavi z delovanjem v skladu s pravilnikom o zasebnosti.

i) Ponudnik ni odgovoren za kakršno koli izgubo, škodo, strošek ali zahtevek, ki je posledica izgube, kraje, nepravilne uporabe, okvare, poškodbe ali uničenja gesel, nastavljenih informacij, šifrirnih ključev, kod za aktivacijo licence in drugih podatkov, generiranih ali shranjenih med uporabo programske opreme.

Dodatna določila za programsko opremo ESET Secure Data veljajo samo za končne uporabnike izdelka ESET Smart Security Premium.

Password Manager Programska oprema. Dodatna določila, ki veljajo za programsko opremo Password Manager:

1. Dodatne izjave končnega uporabnika. Potrjujete in sprejemate, da ne smete:

a) uporabljati programske opreme Password Manager za kakršno koli kritično pomembno aplikacijo, kjer je lahko ogroženo človeško življenje ali lastnina. Sprejemate, da programska oprema Password Manager ni namenjena za take namene in da bi njena napaka v teh primerih lahko povzročila smrt, telesne poškodbe ali hujšo škodo za lastnino ali okolje, za katero ponudnik ni odgovoren.

PROGRAMSKA OPREMA PASSWORD MANAGER NI IZDELANA, NAMENJENA ALI LICENCIRANA ZA UPORABO V NEVARNIH OKOLJIH, KI ZAHTEVAJO VARNOST IN NADZOR BREZ IZPADA, MED DRUGIM PRI NAČRTOVANJU, GRADNJI VZDRŽEVANJU ALI UPRAVLJANJU JEDRSKIH OBRATOV, USMERJANJU LETAL ALI KOMUNIKACIJSKIH SISTEMIH, NADZORU ZRAČNEGA PROSTORA, SISTEMIH ZA OHRANJANJE ŽIVLJENJSKIH ZNAKOV ALI OROŽNIH SISTEMIH. PONUDNIK POSEBEJ ZAVRAČA KAKRŠNO KOLI IZRECNO ALI NAKAZANO JAMSTVO GLEDE PRIMERNOSTI ZA UPORABO V TE NAMENE.

b) uporabljati programske opreme Password Manager na način, ki krši to pogodbo ali zakone Slovaške republike ali druge države. Še zlasti ne smete uporabljati programske opreme Password Manager za izvajanje ali spodbujanje nezakonitih dejavnosti, vključno z nalaganjem podatkov s škodljivo vsebino ali vsebino, ki bi lahko bila uporabljena za kakršne koli nezakonite dejavnosti ali ki na kakršen koli način krši zakone ali pravice drugih oseb (vključno z vsemi pravicami intelektualne lastnine), vključno z, vendar ne omejeno na kakršne koli poskuse za pridobitev dostopa do računov v shrambi (za namene teh dodatnih pogojev uporabe »shramba« programske opreme Password Manager pomeni prostor za shranjevanje podatkov, ki ga upravlja ponudnik ali druga oseba, ki ni ponudnik ali uporabnik, za namene omogočanja sinhronizacije in varnostnega kopiranja podatkov uporabnikov) ali katerih koli računov in podatkov drugih uporabnikov programske opreme Password Manager ali shrambe. Če prekršite te določbe, ima ponudnik pravico, da takoj prekine to pogodbo in na vas prenese strošek kakršnih koli potrebnih ukrepov, kakor tudi opravi vse potrebne ukrepe, da vam prepreči nadaljnjo uporabo programske opreme Password Manager brez možnosti vračila kupnine.

2. OMEJITEV ODGOVORNOSTI. PROGRAMSKA OPREMA PASSWORD MANAGER JE ZAGOTOVLJENA »V TAKŠNEM STANJU, KOT JE«. NOBENA JAMSTVA NISO IZRECNA ALI NAKAZANA. PROGRAMSKO OPREMO UPORABLJATE NA LASTNO ODGOVORNOST. PROIZVAJALEC NI ODGOVOREN ZA IZGUBO PODATKOV, ŠKODO, OMEJITEV RAZPOLOŽLJIVOSTI STORITEV, VKLJUČNO S PODATKI, KI JIH PROGRAMSKA OPREMA PASSWORD MANAGER POŠLJE V ZUNANJO SHRAMBO ZA NAMENE SINHRONIZACIJE PODATKOV IN VARNOSTNEGA KOPIRANJA. ŠIFRIRANJE PODATKOV S PROGRAMOM PASSWORD MANAGER NE POMENI NIKAKRŠNE ODGOVORNOSTI PONUDNIKA V ZVEZI Z VARNOSTJO TEH PODATKOV. IZRECNO SOGLAŠATE, DA JE DOVOLJENO PODATKE, PRIDOBLJENE, UPORABLJENE, ŠIFRIRANE, SHRANJENE, SINHRONIZIRANE ALI POSLANE S PROGRAMSKO OPREMO PASSWORD MANAGER, SHRANITI TUDI V STREŽNIKIH DRUGIH PONUDNIKOV (TO VELJA SAMO ZA UPORABO PROGRAMSKE OPREME PASSWORD MANAGER, PRI KATERI JE OMOGOČENO SINHRONIZIRANJE IN VARNOSTNO KOPIRANJE). ČE SE PONUDNIK PO LASTNI PRESOJI ODLOČI ZA UPORABO SHRAMBE, SPLETNEGA MESTA, SPLETNEGA PORTALA, STREŽNIKA ALI STORITVE DRUGEGA PONUDNIKA, PONUDNIK NI ODGOVOREN ZA KAKOVOST, VARNOST ALI RAZPOLOŽLJIVOST OMENJENE STORITVE DRUGEGA PONUDNIKA, PONUDNIK PRAV TAKO NI NIKAKOR ODGOVOREN ZA KAKRŠNO KOLI KRŠITEV POGODBENIH ALI ZAKONSKIH OBVEZNOSTI S STRANI DRUGEGA PONUDNIKA, NITI ZA ŠKODO, IZGUBO PROMETA, FINANČNO ALI NEFINANČNO ŠKODO ALI KAKRŠNO KOLI DRUGO IZGUBO, DO KATERE MORDA PRIDE PRI UPORABI TE PROGRAMSKE OPREME. PONUDNIK NI ODGOVOREN ZA VSEBINO KAKRŠNIH KOLI PODATKOV, PRIDOBLJENIH, UPORABLJENIH, ŠIFRIRANIH, SHRANJENIH, SINHRONIZIRANIH ALI POSLANIH S PROGRAMSKO OPREMO PASSWORD MANAGER ALI SHRANJENIH. SPREJEMATE, DA PONUDNIK NIMA DOSTOPA DO VSEBINE SHRANJENIH PODATKOV IN NE MORE NADZIRATI ALI ODSTRANJEVATI NEZAKONITE ŠKODLJIVE VSEBINE.

Ponudnik je lastnik vseh izboljšav, nadgradenj ali popravkov, povezanih s programsko opremo Password MANAGER (»izboljšave«), tudi v primeru, ko so te izboljšave izdelane na podlagi povratnih informacij, zamisli ali predlogov, ki ste jih v kakršni koli obliki posredovali ponudniku. Upravičeni niste do nobenega nadomestila, vključno s kakršnimi koli avtorskimi honorarji, povezanimi s temi izboljšavami.

PONUDNIKOVE ENTITETE IN DAJALCI LICENC NISO ODGOVORNI ZA KAKRŠNE KOLI ODŠKODNINSKE ZAHTEVKE ALI OBVEZNOSTI, KI SO POSLEDICA ALI SO KAKOR KOLI POVEZANE Z VAŠO UPORABO PROGRAMSKE OPREME PASSWORD MANAGER ALI UPORABO S STRANI DRUGIH OSEB, Z UPORABO ALI NEUPORABO KATERE KOLI BORZNOPOSREDNIŠKE DRUŽBE ALI AGENTA ALI V ZVEZI S PRODAJO ALI NAKUPOM KATERIH KOLI VREDNOSTNIH PAPIRJEV, NE GLEDE NA TO, ALI ODŠKODNINSKI ZAHTEVKI ALI OBVEZNOSTI TEMELJIJO NA TEORIJI PRAVA ALI ENAKOVREDNE OBRAVNAVE.

PONUDNIKOVE ENTITETE IN DAJALCI LICENC NISO V NOBENEM PRIMERU ODGOVORNI ZA KAKRŠNO KOLI NEPOSREDNO, NENAMERNO, POSEBNO, POSREDNO ALI POSLEDIČNO ŠKODO, KI JE POVZROČENA ALI POVEZANA S KAKRŠNO KOLI PROGRAMSKO OPREMO DRUGIH PROIZVAJALCEV, KAKRŠNIH KOLI PODATKOV, DO KATERIH STE DOSTOPALI S PROGRAMSKO OPREMO PASSWORD MANAGER, VAŠO UPORABO ALI NEZMOŽNOSTJO UPORABE PROGRAMSKE OPREME PASSWORD MANAGER ALI DOSTOPA DO NJE, ALI KATERIH KOLI DRUGIH PODATKOV, ZAGOTOVLJENIH PREK PROGRAMSKE OPREME PASSWORD MANAGER, NE GLEDE NA TO, ALI SO ODŠKODNINSKI ZAHTEVKI VLOŽENI V SKLADU S TEORIJO PRAVA ALI ENAKOVREDNE OBRAVNAVE. ODŠKODNINE, KI JIH TA DOLOČBA IZKLJUČUJE, MED DRUGIM VKLJUČUJEJO POVRAČILO ZA IZGUBO POSLOVNIH PRIHODKOV, POŠKODBE OSEB ALI LASTNINE, PREKINITVE POSLOVANJA, IZGUBE POSLA ALI OSEBNIH PODATKOV. ZAKONODAJE NEKATERIH DRŽAV NE DOVOLJUJEJO OMEJEVANJA ODGOVORNOSTI ZA NENAMERNO ALI POSLEDIČNO ŠKODO, ZATO TA OMEJITEV MORDA NE VELJA ZA VAS. V TEM PRIMERU JE ODGOVORNOST PONUDNIKA NAJNIŽJA MOŽNA, KOT JE DOLOČENA Z VELJAVNIMI ZAKONI.

INFORMACIJE, OBDELANE S PROGRAMSKO OPREMO PASSWORD MANAGER, VKLJUČNO S CENAMI DELNIC, ANALIZAMI, TRŽNIMI INFORMACIJAMI, NOVICAMI IN FINANČNIMI PODATKI, SO LAHKO ZAMUJENE, NETOČNE ALI VSEBUJEJO NAPAKE ALI IZPUSTITVE, IN V ZVEZI S TEM PONUDNIKOVE ENTITETE IN DAJALCI LICENC NE NOSIJO NOBENE ODGOVORNOSTI. PONUDNIK LAHKO KADAR KOLI BREZ PREDHODNEGA OBVESTILA SPREMENI ALI OPUSTI KATERI KOLI DEL ALI FUNKCIJO PROGRAMSKE OPREME PASSWORD MANAGER ALI UPORABO VSEH ALI KATERIH KOLI FUNKCIJ ALI TEHNOLOGIJ PROGRAMSKE OPREME PASSWORD MANAGER.

ČE SO DOLOČILA TEGA ČLENA IZ KATEREGA KOLI RAZLOGA NEVELJAVNA IN SE ŠTEJE, DA JE PONUDNIK PO VELJAVNI ZAKONODAJI ODGOVOREN ZA IZGUBO, ŠKODO ITD., SE POGODBENI STRANKI STRINJATA, DA JE OBVEZNOST PONUDNIKA DO VAS OMEJENA NA SKUPNI ZNESEK LICENČNIN, KI STE JIH PLAČALI.

SOGLAŠATE, DA BOSTE PONUDNIKA IN NJEGOVE ZAPOSLENE, PODRUŽNICE, POVEZANA IN PREDRUGAČENA PODJETJA TER DRUGE PARTNERJE ODVEZALI ODGOVORNOSTI, JIH ZAGOVARJALI IN OBRAVNAVALI KOT NEDOLŽNE, ČE BI KATERE KOLI DRUGE OSEBE (VKLJUČNO Z LASTNIKI NAPRAVE ALI OSEBAMI, KATERIH PRAVICE SO BILE OKRNJENE ZARADI PODATKOV, UPORABLJENIH V PROGRAMSKI OPREMI PASSWORD MANAGER ALI V SHRAMBI) ZAHTEVALE POVRAČILO ODGOVORNOSTI, OBVEZNOSTI, ŠKODE, IZGUBE, STROŠKOV ALI PLAČIL, KI BI JIH TE OSEBE UTRPELE ZARADI VAŠE UPORABE PROGRAMSKE OPREME PASSWORD MANAGER.

3. Podatki v programski opremi Password Manager. Razen v primeru, da se izrecno odločite drugače, so vsi podatki, ki jih vnesete v programsko opremo Password Manager in se shranijo v njeno zbirko podatkov, v šifrirani obliki shranjeni v vašem računalniku ali drugem nosilcu podatkov, ki ga določite. Sprejemate, da so v primeru izbrisa ali poškodovanja katere koli zbirke podatkov ali datoteke programske opreme Password Manager vsi podatki v njej nepovratno izgubljeni, ter da razumete in sprejemate tveganje take izgube. Vaši osebni podatki so v računalniku shranjeni v šifrirani obliki, vendar to ne pomeni, da oseba, ki ugotovi vaše glavno geslo ali pridobi dostop do uporabniško določene aktivacijske naprave za odpiranje zbirke podatkov, ne more ukrasti ali zlorabiti. Sami ste odgovorni za zagotavljanje varnosti vseh načinov dostopa.

4. Prenos osebnih podatkov k ponudniku ali v shrambo. Če izberete to možnost in samo za namene pravočasne

sinhronizacije in varnostnega kopiranja podatkov, programska oprema Password Manager prenese ali pošlje osebne podatke iz zbirke podatkov programske opreme Password Manager – gesla, poverilnice za prijavo, račune in identitete – prek interneta v shrambo. Podatki se prenašajo izključno v šifrirani obliki. Pri uporabi programske opreme Password Manager za izpolnjevanje spletnih obrazcev z gesli, uporabniškimi imeni ali drugimi podatki je morda potrebno pošiljanje podatkov prek interneta na spletno mesto, ki ga določite. Takega prenosa podatkov ne sproži programska oprema Password Manager, zato ponudnik ni odgovoren za varnost takih interakcij s katerim koli spletnim mestom, ki ga podpirajo drugi ponudniki. Vse transakcije po internetu, ne glede na to ali so povezane s programsko opremo Password Manager ali ne, izvajate po lastni presoji in na lastno odgovornost, zato ste izključno vi odgovorni za kakšno koli škodo v vašem računalniškem sistemu ali izgubo podatkov kot posledico prenosa in/ali uporabe kakršnega koli takega materiala ali storitve. Za zmanjšanje tveganja izgube dragocenih podatkov ponudnik priporoča, da stranke izvajajo redno varnostno kopiranje zbirke podatkov in drugih dragocenih podatkov v zunanje nosilce podatkov. Ponudnik vam ne more zagotoviti nikakršne pomoči pri obnavljanju izgubljenih ali poškodovanih podatkov. Če ponudnik ponuja storitve varnostnega kopiranja za datoteke uporabniških zbirk podatkov v primeru poškodbe ali izbrisa datotek v uporabniškem računalniku, je ta storitev obnovitve brez jamstva in ne pomeni, da ima ponudnik do vas kakršno koli odgovornost.

Z uporabo programske opreme Password Manager soglašate, da lahko programska oprema občasno komunicira s ponudnikovimi strežniki in preveri informacije o licenci, razpoložljivost popravkov, servisnih paketov in drugih posodobitev, ki lahko izboljšajo, vzdržujejo, spremenijo ali nadgradijo delovanje programske opreme Password Manager. Programska oprema bo morda pošiljala splošne sistemske informacije, povezane z delovanjem programske opreme Password Manager v skladu s pravilnikom o zasebnosti.

5. Informacije in navodila za odstranjevanje. Kakršne koli informacije iz zbirke podatkov, ki jih želite obdržati, morate izvoziti, preden odstranite programsko opremo Password Manager.

Dodatna določila za programsko opremo Password Manager Software veljajo samo za končne uporabnike izdelka ESET Smart Security Premium.

ESET LiveGuard. Dodatna določila, ki veljajo za programsko opremo ESET LiveGuard:

Programska oprema vsebuje funkcijo dodatne analize datotek, ki jih je poslal končni uporabnik. Ponudnik uporablja samo datoteke, ki jih je poslal končni uporabnik, in rezultate analize v skladu s pravilnikom o zasebnosti in v skladu z ustreznimi pravnimi predpisi.

Dodatna določila za programsko opremo ESET LiveGuard veljajo samo za končne uporabnike izdelka ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Pravilnik o zasebnosti

Za družbo ESET, spol. s r. o., s sedežem na naslovu Einsteinova 24, 851 01 Bratislava, Slovak Republic, ki je registrirana v trgovinskem registru okrožnega sodišča v Bratislavi, I, razdelek Sro, vnos št. 3586/B, in identifikacijsko številko podjetja 31333532 je varstvo osebnih podatkov izjemno pomembno kot upravljavec podatkov (»ESET« ali »mi«). Želimo izpolniti zahtevo po preglednosti, kot je pravno standardizirana v skladu s Splošno uredbo EU o varstvu podatkov (»GDPR«). Za dosego tega cilja objavljamo ta pravilnik o zasebnosti z edinim namenom, da svojo stranko (»končni uporabnik« ali »vi«) kot posameznika, na katerega se nanašajo osebni podatki, obvestimo o naslednjih temah o varstvu osebnih podatkov:

- pravna podlaga za obdelavo osebnih podatkov,
- deljenje podatkov in zaupnost,

- varnost podatkov,
- vaše pravice kot posameznika, na katerega se nanašajo osebni podatki,
- obdelava osebnih podatkov
- Podatki za stik.

Pravna podlaga za obdelavo osebnih podatkov

Za obdelavo podatkov velja le nekaj pravnih podlag, ki jih upoštevamo v skladu z veljavnim zakonodajnim okvirom, ki je povezan z varstvom osebnih podatkov. Obdelava osebnih podatkov v družbi ESET je potrebna predvsem za izvajanje Licenčno pogodbo za končnega uporabnika (»EULA«) s končnim uporabnikom (člen 6(1)(b) GDPR), ki velja za zagotavljanje izdelkov ali storitev družbe ESET, razen če ni izrecno navedeno drugače, npr:

- Pravna podlaga zakonitega interesa (člen 6(1)(f) GDPR) nam omogoča obdelavo podatkov o tem, kako stranke uporabljajo naše storitve, in njihovem zadovoljstvu, tako da lahko uporabnikom zagotovimo najboljšo zaščito, podporo in uporabniško izkušnjo. Veljavna zakonodaja tudi trženje obravnava kot zakoniti interes, zato se običajno na to sklicujemo pri trženjski komunikaciji s strankami.
- Soglasje (člen 6(1)(f) GDPR), ki ga lahko od vas zahtevamo v posebnih primerih, kadar menimo, da je ta pravna podlaga najprimernejša ali če to določa zakon.
- Skladnost s pravnimi obveznostmi (člen 6(1)(f) GDPR), npr. predpisovanjem obveznosti za elektronske komunikacije, hranjenje dokumentov za izdajo računov in zaračunavanje.

Deljenje podatkov in zaupnost

Vaših podatkov ne delimo s tretjimi osebami. Vendar družba ESET deluje po vsem svetu prek povezanih podjetij ali partnerjev v okviru mreže za zagotavljanje prodaje, storitev in podpore. Podatki o licenciranju, zaračunavanju in tehnični podpori, ki jih obdeluje družba ESET, se lahko prenesejo do in od povezanih podjetij ali partnerjev za namen izpolnjevanja licenčne pogodbe za končnega uporabnika, kot je zagotavljanje storitev ali podpore.

Družba ESET podatke raje obdeluje v Evropski uniji (EU). Vendar pa bo glede na vašo lokacijo (uporaba naših izdelkov in/ali storitev zunaj EU) in/ali storitev, ki jo izberete, morda treba vaše podatke prenesti v državo zunaj EU. Na primer, v povezavi z računalništvom v oblaku uporabljamo storitve tretjih oseb. V teh primerih skrbno izbiramo ponudnike storitev in s pogodbenimi ter tehničnimi in organizacijskimi ukrepi zagotavljamo ustrezno raven varstva podatkov. Praviloma se dogovorimo o standardnih pogodbenih klavzulah EU, po potrebi z dodatnimi pogodbenimi predpisi.

Za nekatere države zunaj EU, kot sta Združeno kraljestvo in Švica, je EU že določila primerljivo raven varstva podatkov. Zaradi primerljive ravni varstva podatkov za prenos podatkov v te države ni potrebno posebno dovoljenje ali dogovor.

Varnost podatkov

Družba ESET izvaja ustrezne tehnične in organizacijske ukrepe za zagotavljanje ravni varnosti, primerne morebitnim tveganjem. Po najboljših močeh se trudimo zagotavljati stalno zaupnost, celovitost, razpoložljivost in odpornost sistemov za obdelavo in storitev. Toda v primeru kršitve varnosti podatkov, zaradi katere so ogrožene vaše pravice in svoboščine, smo pripravljeni obvestiti ustrezne nadzorne organe in prizadete posameznike, na katere se podatki nanašajo.

Pravice posameznikov, na katere se podatki nanašajo

Pravice vsakega končnega uporabnika so pomembne in obveščamo vas, da imajo vsi končni uporabniki (iz katere koli države EU ali tretje države) naslednje pravice, ki jih zagotavlja družba ESET. Za uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, nas lahko kontaktirate prek obrazca za podporo ali po e-pošti na naslovu dpo@eset.sk. Za namene identifikacije vas prosimo za naslednje informacije: Ime in priimek, e-poštni naslov in – če je na voljo – licenčni ključ ali številko stranke ter pripadnost podjetju. Drugih osebnih podatkov, kot je datum rojstva, nam ne pošiljajte. Poudarjamo, da bomo za obdelavo zahteve in za namene identifikacije obdelali vaše osebne podatke.

Pravica do preklica soglasja. Pravica do preklica soglasja velja samo v primeru obdelave na podlagi soglasja. Če vaše osebne podatke obdelujemo na podlagi soglasja, imate pravico, da soglasje kadar koli prekličete brez navedbe razlogov. Preklic soglasja velja le za prihodnost in ne vpliva na zakonitost podatkov, obdelanih pred preklicem.

Pravica do ugovora. Pravica do ugovora obdelavi velja v primeru obdelave na podlagi zakonitega interesa družbe ESET ali tretje osebe. Če vaše osebne podatke obdelujemo za zaščito zakonitega interesa, imate kot posameznik, na katerega se nanašajo osebni podatki, pravico kadar koli ugovarjati zakonitemu interesu, ki smo ga navedli, in obdelavi vaših osebnih podatkov. Ugovor velja le za prihodnost in ne vpliva na zakonitost podatkov, obdelanih pred ugovorom. Če vaše osebne podatke obdelujemo za namene neposrednega trženja, ugovora ni treba utemeljiti. To velja tudi za profiliranje, če je povezano s takim neposrednim trženjem. V vseh drugih primerih vas prosimo, da nas na kratko obvestite o svojih ugovorih zoper zakoniti interes družbe ESET za obdelavo vaših osebnih podatkov.

Upoštevajte, da smo v nekaterih primerih kljub preklicu soglasja upravičeni do nadaljnje obdelave vaših osebnih podatkov na podlagi druge pravne podlage, na primer za izvajanje pogodbe.

Pravica do dostopa. Kot posameznik, na katerega se nanašajo osebni podatki, imate pravico, da kadar koli brezplačno pridobite informacije o svojih podatkih, ki jih hrani družba ESET.

Pravica do popravka. Če nehote obdelujemo napačne osebne podatke o vas, imate pravico do popravka.

Pravica do izbrisa in pravica do omejitve obdelave. Kot posameznik, na katerega se nanašajo osebni podatki, imate pravico zahtevati izbris ali omejitev obdelave vaših osebnih podatkov. Če obdelujemo vaše osebne podatke, na primer z vašim soglasjem, ga prekličete in ne obstaja druga pravna podlaga, na primer pogodba, vaše osebne podatke takoj izbrišemo. Vaše osebne podatke bomo izbrisali tudi takoj, ko jih ne bomo več potrebovali za namene, navedene za njih ob koncu obdobja hrambe.

Če vaše osebne podatke uporabljamo izključno za namen neposrednega trženja in ste preklicali doglasje ali ugovarjali osnovnemu zakonitemu interesu družbe ESET, bomo obdelavo vaših osebnih podatkov omejili do te mere, da bomo vaše kontaktne podatke vključili na naš interni črni seznam, da bi se izognili nezaželenim stikom. V nasprotnem primeru bodo vaši osebni podatki izbrisani.

Upoštevajte, da bomo morda morali vaše podatke hraniti do izteka obveznosti in rokov hrambe, ki jih je izdal zakonodajalec ali nadzorni organi. Obveznosti in obdobja hrambe lahko izhajajo tudi iz slovaške zakonodaje. Nato bodo ustrezni podatki rutinsko izbrisani.

Pravico do prenosljivosti podatkov. Z veseljem vam kot posamezniku, na katerega se nanašajo osebni podatki, posredujemo osebne podatke, ki jih obdeluje družba ESET, v obliki zapisa xls.

Pravica do vložitve pritožbe. Kot posameznik, na katerega se nanašajo osebni podatki, imate pravico, da kadar koli vložite pritožbo pri nadzornem organu. Za družbo ESET velja slovaška zakonodaja ter zakonodaja o varstvu

podatkov znotraj Evropske unije. Ustrezni nadzorni organ za varstvo podatkov je Urad za varstvo osebnih podatkov Slovaške republike s sedežem na naslovu Hraničná 12, 82007 Bratislava 27, Slovak Republic.

obdelava osebnih podatkov

Storitve, ki jih družba ESET zagotavlja v okviru svojih izdelkov, so zagotovljene na podlagi pogojev EULA, vendar je za nekatere morda potrebna dodatna obrazložitev. Želimo vam zagotoviti več podrobnosti o zbiranju podatkov v povezavi z zagotavljanjem naših storitev. Zagotavljamo različne storitve, ki so opisane v licenčni pogodbi za končnega uporabnika in dokumentaciji. Za zagotavljanje storitev moramo zbirati naslednje podatke:

Podatki o licenciranju in izdajanju računov. Ime, e-poštni naslov, licenčni ključ in (če je primerno) naslov, pripadnost podjetju in podatke o plačilu družba ESET zbira in obdeluje za lažjo aktivacijo licence, dostavo licenčnega ključa, opomnike o izteku veljavnosti, zahtevke za podporo, preverjanje pristnosti licence, zagotavljanje naših storitev in drugih obvestil, vključno s tržnimi sporočili v skladu z veljavno zakonodajo ali vašim soglasjem. Družba ESET je zakonsko zavezana hraniti podatke o izdajanju računov za obdobje 10 let, vendar bodo podatki o licenciranju anonimizirani najpozneje 12 mesecev po izteku licence.

Posodobitve in drugi statistični podatki. Obdelani podatki vključujejo podatke o postopku namestitve in vašem računalniku, vključno s platformo, na katero je nameščen naš izdelek, ter podatke o delovanju in funkcionalnosti naših izdelkov, kot so operacijski sistem, podatki o strojni opremi, ID namestitve, ID licence, naslov IP, naslov MAC, konfiguracijske nastavitve izdelka, se obdelujejo za namen zagotavljanja storitev posodobitve in nadgradnje ter za namen vzdrževanja, varnosti in izboljšanja naše zaledne infrastrukture.

Te informacije se hranijo ločeno od identifikacijskih informacij, ki so potrebne za namene licenciranja in izdajanja računov, saj ne zahtevajo identifikacije končnega uporabnika. Obdobje hrambe je do 4 leta.

ESET LiveGrid® Sistem ugleda. Podatke o enosmernih razpršitvah v povezavi z vdori v okviru sistema za preverjanje ugleda za namen ESET LiveGrid®, ki izboljšuje učinkovitost rešitev družbe ESET za zaščito pred zlonamerno programsko opremo tako, da primerja pregledane datoteke z zbirko varnih in blokiranih elementov v oblaku. Končni uporabnik med tem postopkom ni identificiran.

ESET LiveGrid® Sistem povratnih informacij. Sumljive zunanje vzorce in metapodatke v okviru sistema za povratne informacije ESET LiveGrid®, ki družbi ESET omogoča takojšen odziv na potrebe končnih uporabnikov in sposobnost odzivnosti na najnovejše grožnje. Zanašamo se na to, da nam pošiljate:

- Podatke o vdorih, kot so morebitni vzorci virusov in drugih zlonamernih programov, in podatke o sumljivih, problematičnih, morebitno nezaželenih oz. morebitno nevarnih predmetih, kot so izvedljive datoteke in e-poštna sporočila, ki jih sami označite kot nezaželena ali jih kot taka označi izdelek ESET,
- Podatke o uporabi interneta, kot so naslov IP in geografski podatki, paketi IP, URL-ji in ethernetni okvirji,
- Izvožene datoteke o zrušitvah in podatke v njih.

Drugih vaših podatkov ne želimo zbirati, vendar je to včasih nemogoče preprečiti. Nenamerno zbrani podatki so lahko vključeni v zlonamerno programsko opremo (zberejo se, ne da bi to vedeli ali odobrili) ali so del imen datotek oz. URL-jev. Teh podatkov v svojih sistemih nismo zbrali namerno in jih ne nameravamo obdelovati za namene, ki so navedeni v tem pravilniku o zasebnosti.

Vse informacije, pridobljene in obdelane prek sistema za povratne informacije ESET LiveGrid®, so namenjene uporabi brez identifikacije končnega uporabnika.

Ocena varnosti naprav, ki imajo vzpostavljeno povezavo z omrežjem. Za zagotavljanje funkcije ocenjevanja varnosti obdelujemo ime lokalnega omrežja in informacije o napravah v vašem lokalnem omrežju, kot so

prisotnost, vrsta, ime, naslov IP in naslov MAC naprave v vašem lokalnem omrežju v povezavi z informacijami o licenci. Podatki vključujejo tudi vrsto brezžične zaščite in vrsto brezžičnega šifriranja za usmerjevalnike. Informacije o licenci, ki identificirajo končnega uporabnika, bodo anonimizirane najpozneje 12 mesecev po izteku licence.

Tehnična podpora. Podatki za stik in licenciranje ter podatki iz vaših zahtev za podporo so lahko potrebni za storitve podpore. Glede na vaš izbrani način stika z nami lahko pridobimo tudi vaš e-poštni naslov, telefonsko številko, licenčne podatke, podatke o izdelku in opis vašega primera za podporo. Za uspešno zagotovitev storitev podpore vas lahko prosimo tudi za posredovanje drugih informacij. Podatki, obdelani za tehnično podporo, se hranijo 4 leta.

Zaščita pred zlorabo podatkov. Če je račun ESET HOME ustvarjen na naslovu https://home.eset.com in končni uporabnik aktivira funkcijo v povezavi s krajo računalnika, bodo zbrani in obdelani naslednji podatki: podatki o lokaciji, posnetki zaslona, podatki o konfiguraciji računalnika in podatki, ki jih je posnela kamera računalnika. Zbrani podatki so shranjeni v naših strežnikih ali strežnikih ponudnikov naših storitev z rokom hrambe 3 mesece.

Password Manager. Če se odločite aktivirati funkcijo Password Manager, se podatki, povezani z vašimi prijavnimi podatki, v šifrirani obliki shranijo samo v vašem računalniku ali drugi določeni napravi. Če aktivirate storitev sinhronizacije, se šifrirani podatki shranijo v naše strežnike ali strežnike ponudnikov naših storitev za namene zagotavljanja teh storitev. Niti družba ESET niti ponudnik storitev nima dostopa do šifriranih podatkov. Ključ za dešifriranje podatkov imate le vi. Podatki bodo odstranjeni ob deaktivaciji funkcije.

ESET LiveGuard. Če se odločite aktivirati funkcijo ESET LiveGuard, je treba predložiti vzorce, kot so datoteke, ki jih je vnaprej določil in izbral končni uporabnik. Vzorci, ki jih izberete za oddaljeno analizo, bodo naloženi v storitev ESET, rezultat analize pa bo poslan nazaj v vaš računalnik. Vsi sumljivi vzorci se obdelajo na način informacij, zbranih v sistemu ESET LiveGrid® za povratne informacije.

Program za izboljšanje izkušenj strank. Če ste se odločili aktivirati Program za izboljšanje izkušenj strank , se na podlagi vašega soglasja zbirajo in uporabljajo anonimni telemetrični podatki, povezani z uporabo naših izdelkov.

Upoštevajte, da če oseba, ki uporablja naše izdelke in storitve, ni končni uporabnik, ki je kupil izdelek ali storitev ter z nami sklenil licenčno pogodbo za končnega uporabnika (npr. zaposleni končnega uporabnika, družinski član ali oseba, ki jo končni uporabnik drugače pooblasti za uporabo izdelka ali storitve v skladu z licenčno pogodbo za končnega uporabnika), se obdelava podatkov izvaja v zakonitem interesu družbe ESET v skladu z Uredbo (ES) št. 6(1) f) Splošne uredbe o varstvu podatkov, da se uporabniku, ki ga je končni uporabnik pooblastil, omogoči uporaba izdelkov in storitev, ki jih zagotavljamo v skladu z licenčno pogodbo za končnega uporabnika.

Podatki za stik

Če želite uveljaviti svoje pravice, ki jih imate kot posameznik, na katerega se nanašajo podatki, ali imate vprašanje ali pomislek, nam pošljite sporočilo na naslov:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk