ESET Endpoint Antivirus

Vodič za korisnike

Kliknite ovdje za prikazivanje verzije mrežne pomoći dokumenta

Digital Security
Progress. Protected.

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

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

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

REV. 12.04.2024.

ESET Endpoint Antivirus

ESET Endpoint Antivirus predstavlja novi pristup potpuno integriranoj zaštiti računala. Najnovija verzija skenera ESET LiveGrid® brzo i precizno štiti vaše računalo. Rezultat je pametan sustav koji neprekidno vodi računa o napadima i zlonamjernom softveru koji bi mogao ugroziti vaše računalo.

ESET Endpoint Antivirus 9 potpuno je sigurnosno rješenje nastalo dugoročnim nastojanjima da se maksimalna zaštita kombinira s minimalnim utjecajem na sustav. Napredne tehnologije koje se temelje na umjetnoj inteligenciji mogu proaktivno eliminirati infiltraciju virusima, spywareom, virusom trojan, crvima, adwareom, rootkitima i drugim internetskim napadima, pri čemu nema negativnog utjecaja na rad vašeg sustava i računala.

program ESET Endpoint Antivirus prvenstveno je osmišljen za upotrebu na radnim stanicama u poslovnim okruženjima.

U odjeljku Instalacija možete pronaći teme pomoći podijeljene u nekoliko poglavlja i potpoglavlja koja vam mogu pružiti kontekst i olakšati snalaženje, uključujući Preuzimanje, Instalaciju i Aktivaciju.

Upotreba programa ESET Endpoint Antivirus s programom ESET PROTECT u poslovnom okruženju omogućuje vam jednostavno upravljanje klijentskim radnim stanicama, primjenu smjernica i pravila, nadzor otkrivanja i daljinsko konfiguriranje klijenata s bilo kojeg umreženog računala.

Ovo poglavlje bavi se najčešćim pitanjima i problemima s kojima se možete susresti.

Značajke i prednosti

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

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

Novosti

Što je novo u verziji 10.1 programa ESET Endpoint Antivirus

Intel® Threat Detection Technology

Hardverska tehnologija koja otkriva ransomware dok pokušava izbjeći detekciju u memoriji. Njezina integracija povećava zaštitu od ransomwarea, a održava ukupne performanse sustava visokima. Pogledajte podržane procesore.

Redizajn tamnog načina rada i korisničkog sučelja

Grafičko korisničko sučelje (GUI) u ovoj verziji redizajnirano je i modernizirano. S dodanim tamnim načinom rada možete odabrati svijetlu ili tamnu shemu boja za GUI programa ESET Endpoint Antivirus u elementima korisničkog sučelja.

Redizajnirano Napredno podešavanje

Napredno podešavanje redizajnirano je i postavke su sada grupirane radi boljeg korisničkog iskustva.

Razne ispravke pogrešaka i poboljšanja performansi

Sistemski preduvjeti

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

Podržani procesori

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

Operacijski sustavi

Microsoft® Windows® 11

Microsoft® Windows® 10

Detaljan popis podržanih verzija sustava Microsoft® Windows® 10 i Microsoft® Windows® 11 potražite u pravilima podrške za operacijski sustav Windows.

Pobrinite se da je vaš operacijski sustav nadograđen.

Podrška za potpisivanje koda za Azure mora biti instalirana na svim operacijskim sustavima Windows da biste instalirali ili nadogradili ESET-ove programe objavljene nakon srpnja 2023. Dodatne informacije.

Preduvjeti za funkcije programa ESET Endpoint Antivirus

U tablici u nastavku pogledajte sistemske preduvjete za određene funkcije programa ESET Endpoint Antivirus:

Funkcija	Preduvjeti
Intel® Threat Detection Technology	Pogledajte podržane procesore.
Specijalizirani čistač	Procesor koji se ne temelji na ARM64.
Sprječavanje ranjivosti	Procesor koji se ne temelji na ARM64.
Dubinski pregled ponašanja	Procesor koji se ne temelji na ARM64.

Instalacijski program ESET Endpoint Antivirus stvoren u programu ESET PROTECT podržava Windows 10 Enterprise za virtualne radne površine i način rada s više sesija sustava Windows 10.

Ostalo

- Ispunjeni su sistemski preduvjeti operacijskog sustava i drugog softvera koji je instaliran na računalu
- 0,3 GB slobodne sistemske memorije (pogledajte Napomenu 1)
- 1 GB slobodnog diskovnog prostora (pogledajte Napomenu 2)
- Minimalna razlučivost zaslona od 1024 x 768
- Internetska veza ili veza putem lokalne mreže s izvorom (pogledajte Napomenu 3) nadogradnji programa
- Dva antivirusna programa koja su istovremeno pokrenuta na jednom uređaju uzrokuju neizbježne sukobe upotrebe resursa sustava, kao što je usporavanje sustava zbog kojeg on postaje neupotrebljiv

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

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

Podržani jezici

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

Jezik	Kod jezika	LCID
Engleski (Sjedinjene Američke Države)	en-US	1033
Arapski (Egipat)	ar-EG	3073
Bugarski	bg-BG	1026
Kineski pojednostavljeni	zh-CN	2052
Kineski tradicionalni	zh-TW	1028
Hrvatski	hr-HR	1050
Češki	cs-CZ	1029
Estonski	et-EE	1061
Finski	fi-FI	1035
Francuski (Francuska)	fr-FR	1036
Francuski (Kanada)	fr-CA	3084
Njemački (Njemačka)	de-DE	1031
Grčki	el-GR	1032
*Hebrejski	he-IL	1037
Mađarski	hu-HU	1038
*Indonezijski	id-ID	1057
Talijanski	it-IT	1040
Japanski	ja-JP	1041
Kazaški	kk-KZ	1087
Korejski	ko-KR	1042
*Letonski	lv-LV	1062
Litavski	lt-LT	1063
Nederlands	nl-NL	1043
Norveški	nb-NO	1044
Poljski	pl-PL	1045
Portugalski, brazilski	pt-BR	1046
Rumunjski	ro-RO	1048
Ruski	ru-RU	1049
Španjolski (Čile)	es-CL	13322
Španjolski (Španjolska)	es-ES	3082
Švedski (Švedska)	sv-SE	1053
Slovački	sk-SK	1051
Slovenski	sl-SI	1060
Tajski	th-TH	1054
Turski	tr-TR	1055

Jezik	Kod jezika	LCID
Ukrajinski (Ukrajina)	uk-UA	1058
*Vijetnamski	vi-VN	1066

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

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

Dnevnik promjena

Prevencija

Prilikom upotrebe računala, osobito prilikom pretraživanja interneta, imajte na umu da nijedan antivirusni sustav ne može potpuno otkloniti opasnost od prijetnji i udaljenih napada. Za maksimalnu zaštitu i ugodan rad morate ispravno upotrebljavati antivirusni sustav i pridržavati se nekoliko korisnih pravila:

Redovito preuzimajte aktualizacije

Prema statistici sustava ESET LiveGrid® svakog se dana pojavljuje tisuće novih, jedinstvenih infiltracija koje njihovi autori stvaraju s ciljem zaobilaženja postojećih sigurnosnih mjera i ostvarivanja zarade nauštrb ostalih korisnika. Stručnjaci u laboratoriju ESET Virus Lab svakodnevno analiziraju te prijetnje te pripremaju i izdaju nadogradnje radi stalnog poboljšavanja razina zaštite korisnika. Da bi se postigla najveća učinkovitost, nadogradnje se moraju ispravno konfigurirati u sustavu. Dodatne informacije o konfiguriranju aktualizacija potražite u poglavlju Podešavanje aktualizacije.

Preuzimajte sigurnosne zakrpe

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

Sigurnosno kopiranje važnih podataka

Autori zlonamjernih programa obično ne mare za potrebe korisnika, a aktivnost zlonamjernih programa često dovodi do potpunog kvara operacijskog sustava i gubitka važnih podataka. Ključno je da redovito sigurnosno kopirate podatke na neki vanjski medij za pohranu, kao što je DVD ili vanjski tvrdi disk. Takve će mjere opreza uvelike pojednostavniti i ubrzati oporavak podataka u slučaju pada sustava.

Redovito skeniranjem provjeravajte postojanje virusa na računalu

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

Pridržavajte se osnovnih pravila sigurnosti

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

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

Stranice pomoći

Dobro došli u korisnički vodič za ESET Endpoint Antivirus. Ovdje navedene informacije upoznat će vas s programom i pomoći učiniti vaš rad na računalu sigurnijim.

Početak korištenja

Prije nego što počnete upotrebljavati ESET Endpoint Antivirus, imajte na umu da se programom može daljinski upravljati pomoću programaESET PROTECT. Preporučujemo i da se upoznate s raznim vrstama otkrivenih prijetnji i daljinskih napada s kojima se možete susresti prilikom upotrebe računala.

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

Korištenje stranica pomoći programa ESET Endpoint Antivirus

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

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

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

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

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

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

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

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

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

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

Dokumentacija za daljinski upravljane krajnje točke

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

ESET-ovi alati za daljinsko upravljanje

Programom ESET Endpoint Antivirus možete upravljati daljinski ili pomoću alata ESET PROTECT ili ESET PROTECT Cloud.

- Uvod u ESET PROTECT
- Uvod u ESET PROTECT Cloud

- ESET HUB – središnji pristupnik jedinstvenoj sigurnosnoj platformi servisa ESET PROTECT. Osigurava centralizirani identitet, pretplatu i upravljanje korisnicima za sve module ESET-ovih platformi. Pogledajte Upravljanje licencama programa ESET PROTECT za upute o tome kako aktivirati program. ESET HUB će u potpunosti zamijeniti programe ESET Business Account i ESET MSP Administrator.

- ESET Business Account – portal za upravljanje licencama ESET-ovih poslovnih programa. Pogledajte odjeljak Upravljanje licencama programa ESET PROTECT da biste pronašli upute za aktivaciju svojeg programa ili potražite više informacija o upotrebi računa ESET Business Account u pomoći na mreži za ESET Business Account. Ako već imate korisničko ime i lozinku koje je izdala tvrtka ESET i koje želite pretvoriti u licenčni ključ, pogledajte odjeljak Pretvaranje podataka o naslijeđenoj licenci.

Dodatni sigurnosni programi

- ESET Inspect – sveobuhvatni sustav za otkrivanje i odgovor sigurnosnog programa koji uključuje funkcije kao što su: otkrivanje incidenata, upravljanje incidentima i odgovor na incidente, prikupljanje podataka, pokazatelji otkrivanja kompromisa, otkrivanje anomalija, otkrivanje ponašanja i kršenja pravila.

- ESET Endpoint Encryption – sveobuhvatna sigurnosna aplikacija dizajnirana za zaštitu vaših podataka u mirovanju i tijekom prijenosa. Pomoću programa ESET Endpoint Encryption možete šifrirati datoteke, mape i e-poruke ili stvoriti šifrirane virtualne diskove, komprimirati arhive i uključiti drobilicu radne površine za sigurno brisanje datoteka.

Alati trećih strana za daljinsko upravljanje

- Daljinsko praćenje i upravljanje (RMM)

Najbolje prakse

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

Vodiči

- Korištenje načina nadjačavanja
- Instalacija programa ESET Endpoint Antivirus pomoću GPO-a ili SCCM-a

Uvod u ESET PROTECT

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

Služite se web konzolom ESET PROTECT da biste instalirali ESET-ova rješenja, upravljali zadacima, nametali sigurnosna pravila, nadgledali status sustava i brzo rješavali probleme ili prijetnje na udaljenim računalima. Isto tako pogledajte pregled arhitekturnih elemenata i elemenata infrastrukture za ESET PROTECT, Početak korištenja web konzole ESET PROTECT i Podržana okruženja za dodjeljivanje radne površine.

ESET PROTECT se sastoji od sljedećih komponenti:

- ESET PROTECT server – On komunicira s agentima te prikuplja i sprema podatke o aplikaciji u bazu podataka. ESET PROTECT server može se instalirati na Windows i Linux serverima, a dostupan je i kao virtualni uređaj.
- ESET PROTECT Web konzola – primarno je sučelje koje omogućuje upravljanje klijentskim računalima u vašoj okolini. Prikazuje pregled statusa klijenata na mreži i omogućuje daljinsku instalaciju rješenja tvrtke ESET na neupravljanim računalima. Nakon što instalirate ESET PROTECT server, možete pristupiti web konzoli s pomoću svojeg web preglednika. Ako odlučite omogućiti pristup web serveru putem interneta, možete upotrebljavati ESET PROTECT s bilo koje lokacije i/ili uređaja s internetskom vezom.
- ESET Management Agent – omogućava komunikaciju između ESET PROTECT servera i klijentskih računala. Agent morate instalirati na klijentsko računalo kako bi se mogla uspostaviti komunikacija između tog računala i ESET PROTECT servera. Budući da je smješten na klijentskom računalu i može pohraniti više sigurnosnih scenarija, korištenje ESET Management agenta znatno skraćuje vrijeme reakcije na nove prijetnje. Upotrebom ESET PROTECT web konzole možete instalirati ESET Management agent na neupravljana računala identificirana putem servisa Active Directory ili ESET RD Sensora. Također po potrebi

možete ručno instalirati ESET Management agent na klijentska računala.

- ESET Rogue Detection Sensor – otkriva neupravljana računala prisutna u vašoj mreži i šalje informacije o njima na ESET PROTECT server. To vam omogućuje upravljanje novim klijentskim računalima u programu ESET PROTECT bez potrebe za ručnim pretraživanjem i dodavanjem. Rogue Detection Sensor pamti računala koja su otkrivena i neće slati iste informacije dvaput.
- ESET Bridge – servis koji se može upotrebljavati u kombinaciji s programom ESET PROTECT za sljedeće:
    - Distribuciju nadogradnji na klijentska računala i instalacijskih paketa na ESET Management agent.
    - Prosljeđivanje komunikacije od ESET Management agenata do ESET PROTECT servera.
- Mobile Device Connector – komponenta koja omogućava upravljanje mobilnim uređajima s pomoću programa ESET PROTECT i pritom vam dopušta upravljanje mobilnim uređajima (Android i iOS) i primjenu programa ESET Endpoint Security za Android.
- ESET PROTECT Virtualni uređaj (VA) – namijenjen je za korisnike koji žele upotrebljavati program ESET PROTECT u virtualiziranom okruženju.
- ESET PROTECT Virtual Agent Host – komponenta programa ESET PROTECT koja virtualizira subjekte agenta za upravljanje virtualnim računalima bez agenta. Ovo rješenje aktivira automatizaciju, iskorištavanje dinamičkih grupa i istu razinu upravljanja zadacima kao i ESET Management agent na fizičkim računalima. Virtualni agent prikuplja informacije s virtualnih računala i šalje ih ESET PROTECT serveru.
- Mirror alat –potreban je za izvanmrežne nadogradnje modula. Ako klijentska računala nemaju internetsku vezu, možete upotrijebiti mirror alat za preuzimanje datoteka za nadogradnju s ESET-ovih servera za nadogradnju i pohraniti ih lokalno.
- ESET Remote Deployment Tool – instalira cjelovite pakete stvorene na <%PRODUCT%> web konzoli. Predstavlja praktičan način za distribuciju ESET Management agenta s ESET-ovim programom na računala putem mreže.

Dodatne informacije potražite u mrežnoj pomoći za ESET PROTECT.

Uvod u ESET PROTECT Cloud

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

ESET PROTECT Cloud se sastoji od sljedećih komponenti:

- ESET PROTECT Cloud Instanca – On komunicira s agentima te prikuplja i sprema podatke o aplikaciji u bazu podataka.
- ESET PROTECT Cloud Web konzola – primarno je sučelje koje omogućuje upravljanje klijentskim računalima u vašoj okolini. Prikazuje pregled statusa klijenata na mreži i omogućuje daljinsku instalaciju rješenja tvrtke ESET na neupravljanim računalima. ESET PROTECT Cloud možete upotrebljavati s bilo kojeg mjesta ili uređaja s internetskom vezom.
- ESET Management Agent – omogućava komunikaciju između ESET PROTECT Cloud i klijentskih računala. Agent morate instalirati na klijentsko računalo kako bi se mogla uspostaviti komunikacija između tog računala i ESET PROTECT Cloud. Budući da je smješten na klijentskom računalu i može pohraniti više sigurnosnih scenarija, korištenje ESET Management agenta znatno skraćuje vrijeme reakcije na nove prijetnje. Upotrebom ESET PROTECT Cloud web konzole možete instalirati ESET Management agent na neupravljana računala. Također po potrebi možete ručno instalirati ESET Management agent na klijentska računala.

- ESET Bridge – servis koji se može upotrebljavati u kombinaciji s programom ESET PROTECT Cloud za sljedeće:
    - Distribuciju nadogradnji na klijentska računala i instalacijskih paketa na ESET Management agent.
    - Prosljeđivanje komunikacije od ESET Management agenata do ESET PROTECT Cloud.
- Upravljanje mobilnim uređajima – komponenta koja omogućava upravljanje mobilnim uređajima s pomoću programa ESET PROTECT Cloud i pritom vam dopušta upravljanje mobilnim uređajima (Android i iOS) i primjenu programa ESET Endpoint Security za Android.
- Upravljanje zakrpama i ranjivosti – značajka dostupna u programu ESET PROTECT Cloud koja redovito skenira radnu stanicu kako bi otkrila instalirani softver koji bi mogao biti osjetljiv na sigurnosne rizike. Upravljanje zakrpama pomaže ispraviti ove rizike automatiziranim nadogradnjama softvera, čime čini uređaje sigurnijima.

Dodatne informacije potražite u mrežnoj pomoći za ESET PROTECT Cloud.

Postavke zaštićene lozinkom

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

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

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

Što su pravila

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

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

Pravila se primjenjuju redoslijedom statičkih grupa. Za dinamičke grupe pravila se najprije primjenjuju na podređene dinamičke grupe. Time se omogućuje da se pravila s većim učinkom primijene na vrh stabla grupa, a specifična pravila na podgrupe. Upotrebom zastavica korisnik programa ESET Endpoint Antivirus s pristupom grupama smještenima visoko na stablu može nadjačati pravila nižih grupa. Algoritam je objašnjen u odjeljku Mrežna pomoć za ESET PROTECT.

> Preporučuje se dodjeljivanje generičkih pravila (npr. pravila za server za nadogradnju) grupama koje su na višoj razini stabla grupa. Specifičnija pravila (npr. postavke za kontrolu uređaja) trebaju se dodijeliti niže na stablu grupa. Niže pravilo obično nadjačava postavke viših pravila nakon spajanja (osim ako je drugačije definirano zastavicama pravila).

Spajanje pravila

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

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

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

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

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

Za više informacija o spajanju pravila slijedite upute iz online korisničkog priručnika za ESET PROTECT i pogledajte primjer.

Kako funkcioniraju zastavice

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

Za svaku postavku možete odabrati jednu od sljedećih zastavica:

Nemoj primijeniti	Nemoj primijeniti – nijedna postavka s ovom zastavicom ne postavlja se pravilom. Budući da se postavka ne postavlja pravilom, može se promijeniti drugim pravilima primijenjenima naknadno.

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

Scenarij: *administrator* želi omogućiti korisniku *Johnu* da stvara ili uređuje pravila u svojoj glavnoj grupi i da vidi sva pravila koja stvori *administrator,* uključujući pravila koja imaju zastavice "Obavezno primijeni". *Administrator* želi omogućiti *Johnu* da vidi sva pravila, no ne i da uređuje postojeća pravila koja stvori *administrator*. *John* može stvarati ili uređivati pravila samo u svojoj glavnoj grupi naziva San Diego.
Rješenje: *administrator* mora slijediti ove korake:
Stvaranje prilagođenih statičkih grupa i skupova dopuštenja
1. Stvorite novu statičku grupu naziva *San Diego*.
2. Stvorite novi skup dopuštenja naziva *Pravilo – Sve John* s pristupom statičkoj grupi *Sve* i razinom dopuštenja **"čitanje"** za **"Pravila"**.
3. Stvorite novi skup dopuštenja naziva *Pravilo John* s pristupom statičkoj grupi *San Diego* i pristupom razini dopuštenja **"pisanje"** za **grupu i računala** i **pravila**. Taj skup dopuštenja omogućuje *Johnu* stvaranje ili uređivanje pravila u njegovoj glavnoj grupi *San Diego*.
4. Stvorite novog korisnika *Johna* pa u odjeljku **"Skupovi dopuštenja"** odaberite *Pravilo – Sve John* i *Pravilo John*.
Stvaranje pravila
5. Stvorite novo pravilo *Sve – aktiviraj firewall*, proširite odjeljak **Postavke**, odaberite **"ESET Endpoint za Windows"**, idite na **"Osobni firewall"** > **"Osnovno"** i primijenite sve postavke zastavicom **"Obavezno primijeni"**. Proširite odjeljak **"Dodjela"** i odaberite statičku grupu *Sve*.
6. Stvorite novo pravilo *Johnova grupa – aktiviraj firewall*, proširite odjeljak **"Podešavanje"**, odaberite **ESET Endpoint za Windows**, idite na **"Osobni firewall"** > **"Osnovno"** i primijenite sve postavke zastavicom **"Primijeni"**. Proširite odjeljak **"Dodjela"** i odaberite statičku grupu *San Diego*.
Rezultat
Prvo će se primijeniti pravila koja stvori *administrator* jer su na postavke pravila primijenjene zastavice **"Obavezno primijeni"**. Postavke s primijenjenom zastavicom "Obavezno primijeni" imaju prioritet i ne mogu se prebrisati drugim pravilom primijenjenim naknadno. Pravila koja stvori korisnik *John* primijenit će se nakon pravila koja stvori administrator.
Idite na **"Više** > **Grupe** > **San Diego"** da biste vidjeli konačan redoslijed pravila. Odaberite računalo i odaberite **"Prikaži pojedinosti"**. U odjeljku **"Konfiguracija"** kliknite **"Primijenjena pravila"**.

Instalacija

Postoji nekoliko metoda instalacije za program ESET Endpoint Antivirus na klijentsku radnu stanicu, osim ako daljinski ne instalirate program ESET Endpoint Antivirus na klijentske radne stanice putem programa ESET PROTECT ili ESET PROTECT Cloud.

Nadograditi možete s programa ESET Endpoint Antivirus na program ESET Endpoint Security pokretanjem instalacijskog programa ESET Endpoint Security pomoću već instaliranog programa ESET Endpoint Antivirus. Međutim, morate instalirati istu ili noviju verziju.

Metoda	Svrha	Link za preuzimanje
Instalacija pomoću programa ESET AV Remover	Alat ESET AV Remover pomoći će vam da uklonite gotovo sve antivirusne programe prethodno instalirane na sustavu prije nego što nastavite instalaciju.	Preuzmite 64-bitnu verziju Preuzmite 32-bitnu verziju
***Instalacija (.exe)	Instalacijski postupak bez alata ESET AV Remover.	Preuzmite 64-bitnu verziju Preuzmite 32-bitnu verziju
Instalacija (.msi)	U poslovnim okruženjima, instalacijski program .msi preferirani je instalacijski paket. To je prvenstveno zbog izvanmrežnih i daljinskih instalacija koje se koriste raznim alatima, kao što je ESET PROTECT.	Preuzmite 64-bitnu verziju Preuzmite 32-bitnu verziju
Instalacija putem naredbenog retka	ESET Endpoint Antivirus može se instalirati lokalno upotrebom naredbenog retka ili na daljinu upotrebom zadatka klijenta iz programa ESET PROTECT.	N/A
Instalacija pomoću GPO-a ili SCCM-a	Upotrijebite alate za upravljanje poput GPO-a ili SCCM-a da biste instalirali ESET Management Agent i program ESET Endpoint Antivirus na klijentske radne stanice.	N/A
Instalacija pomoću RMM alata	ESET-ovi DEM dodaci alata za daljinsko praćenje i upravljanje (RMM) omogućuju instalaciju programa ESET Endpoint Antivirus na klijentske radne stanice.	N/A

Program ESET Endpoint Antivirus dostupan je na više od 30 jezika.

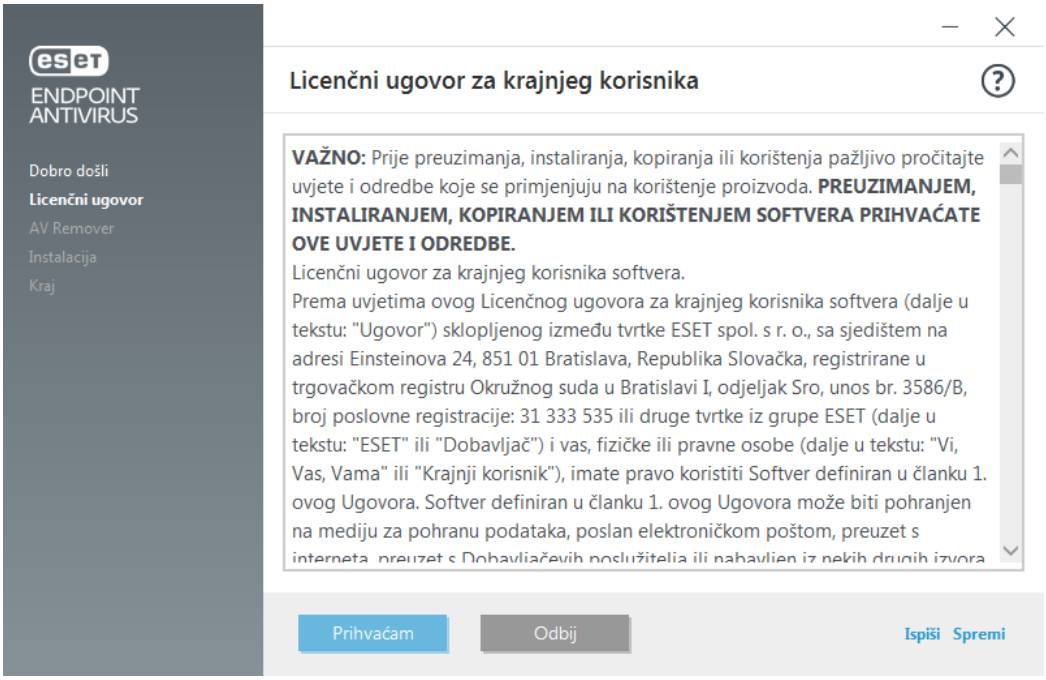
Instalacija pomoću programa ESET AV Remover

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

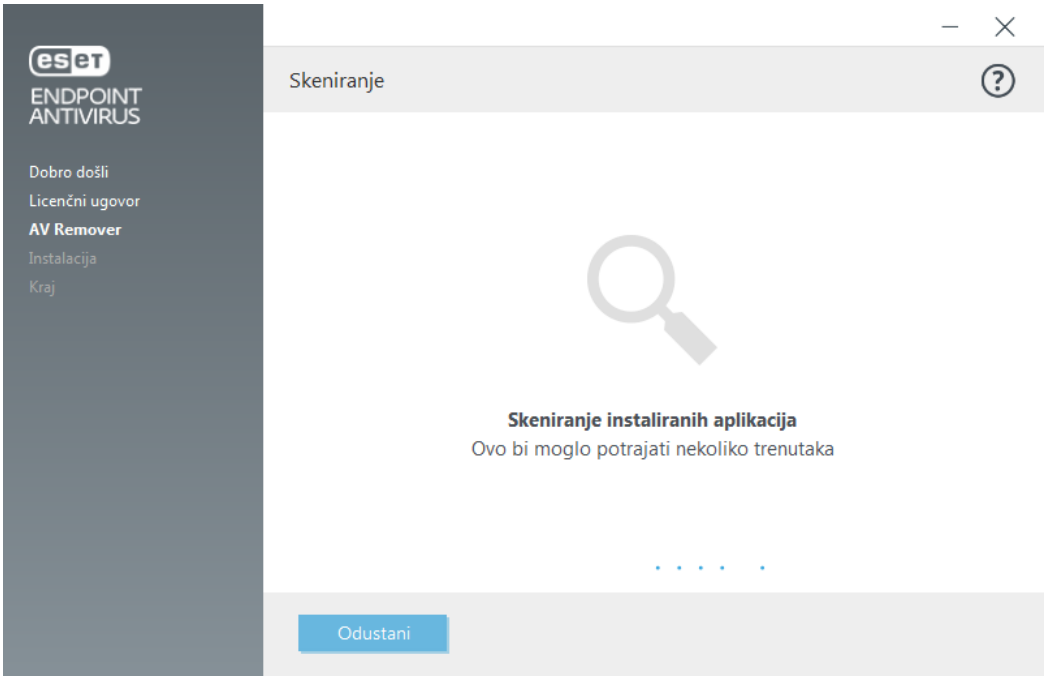
ESET AV Remover

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

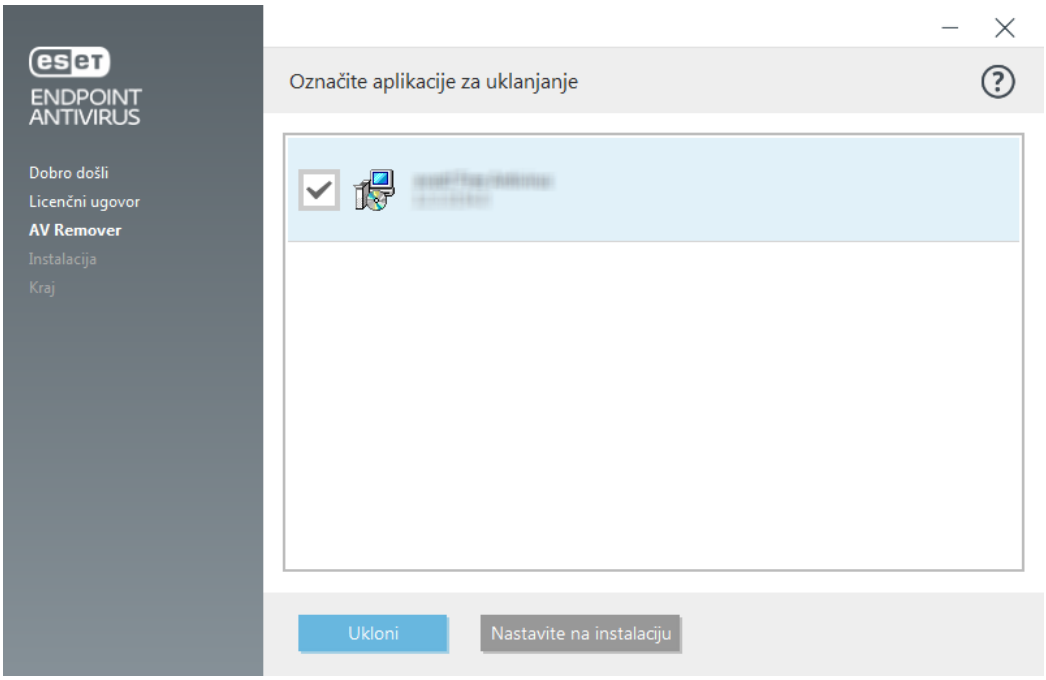
1. Da biste vidjeli popis antivirusnih programa koje program ESET AV Remover može ukloniti, pogledajte članak iz ESET-ove baze znanja.
2. Pročitajte Licenčni ugovor za krajnjeg korisnika i kliknite **Prihvati** da biste prihvatili uvjete. Ako kliknete **Odbij**, instalacija programa ESET Endpoint Antivirus nastavit će se bez uklanjanja postojećih sigurnosnih aplikacija s računala.



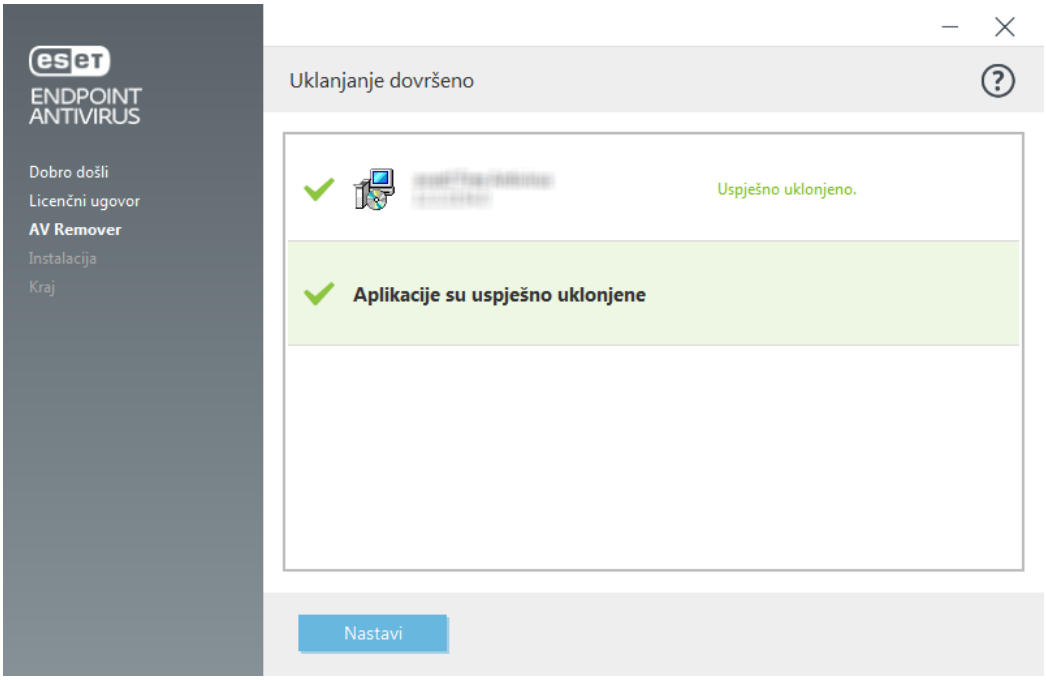
2. ESET AV Remover započet će pretraživanje vašeg sustava kako bi pronašao antivirusni softver.



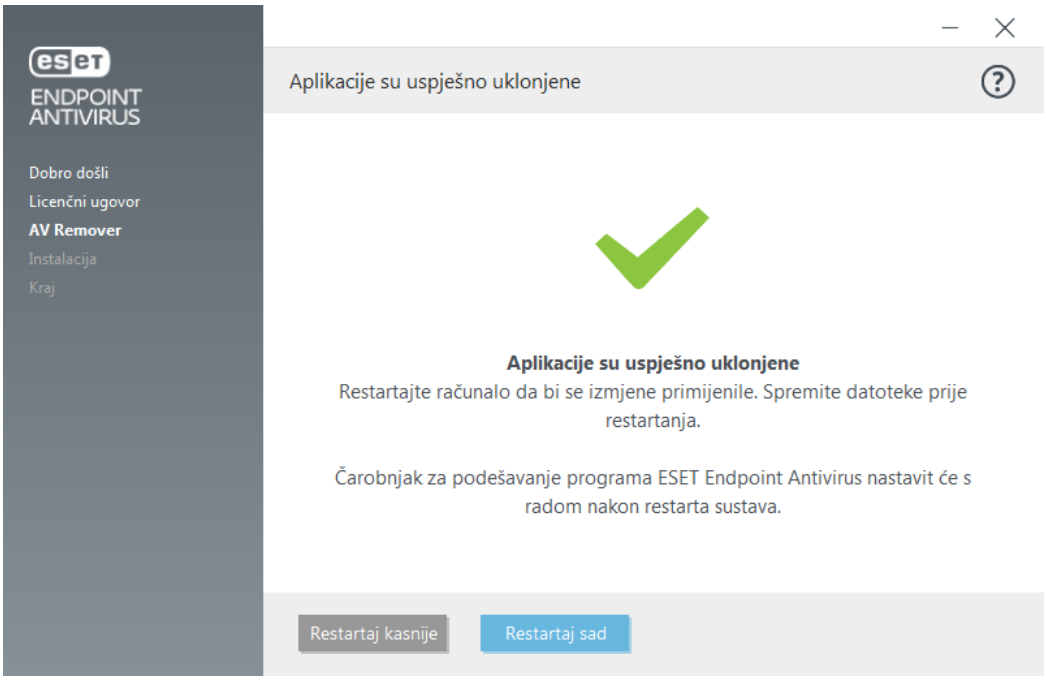
2. Odaberite bilo koju od antivirusnih aplikacija na popisu i kliknite **Ukloni**. Uklanjanje bi moglo potrajati nekoliko trenutaka.



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



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



Deinstalacija pomoću programa ESET AV Remover završila je s pogreškom

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

Ako deinstalacija sigurnosnog programa nije uspjela ili je neka od njegovih komponenti deinstalirana djelomično,

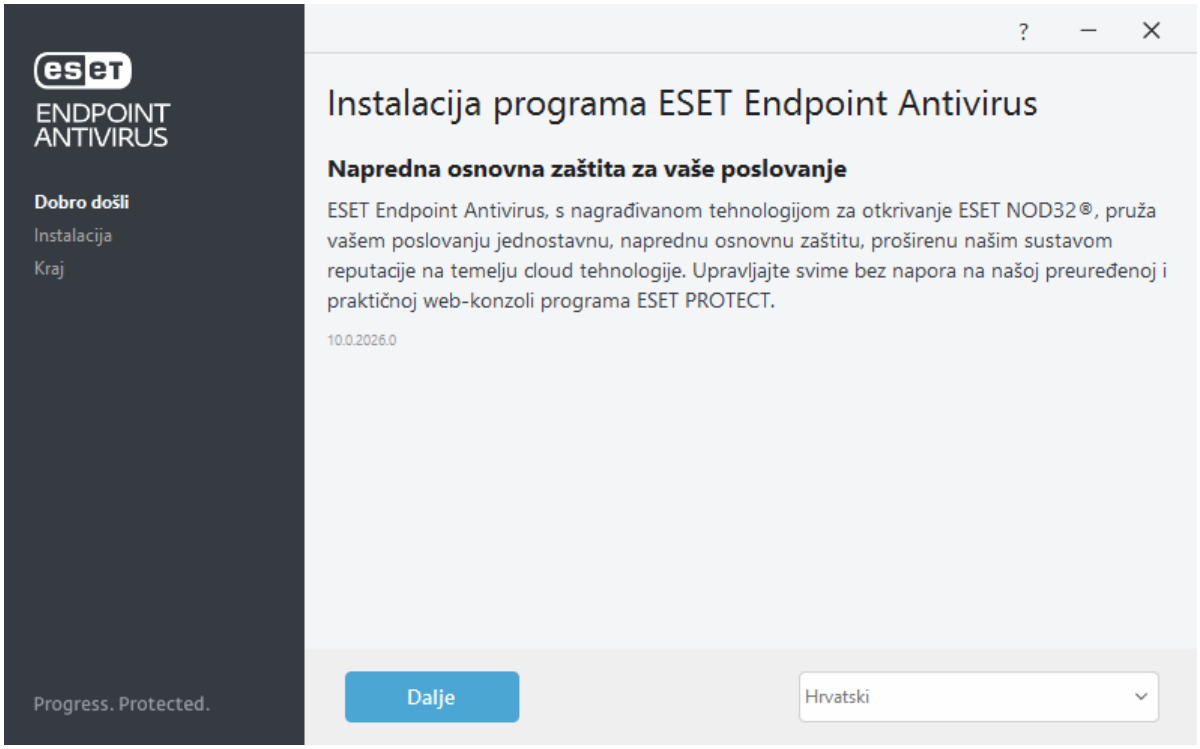
pojavit će se uputa **"Ponovno pokreni i ponovno skeniraj"**. Potvrdite kontrolu korisničkog računa (UAC) nakon pokretanja sustava i nastavite s postupkom skeniranja i deinstalacije.

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

Instalacija (.exe)

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

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



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

- Sustav za povratne informacije ESET LiveGrid®
- Detekcija potencijalno nepoželjne aplikacije

Ako kliknete **Nastavi** ili **Prihvati i nastavi**, prihvaćate Licenčni ugovor za krajnjeg korisnika i potvrđujete da ste suglasni s Pravilima privatnosti. Program ESET Endpoint Antivirus možete instalirati u određenu mapu tako da kliknete Promijeni mapu za instalaciju.

2. Nakon završetka instalacije od vas će se zatražiti da aktivirate program ESET Endpoint Antivirus.

Promjena instalacijske mape (.exe)

Tijekom instalacije možete odabrati opciju **Promjena instalacijske mape**. Odaberite mjesto za instalaciju programa ESET Endpoint Antivirus. Prema standardnim postavkama program se instalira u sljedeću mapu:

C:\Program Files\ESET\ESET Security

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

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

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

Kliknite **Natrag**, a zatim nastavite s postupkom instalacije.

Instalacija (.msi)

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

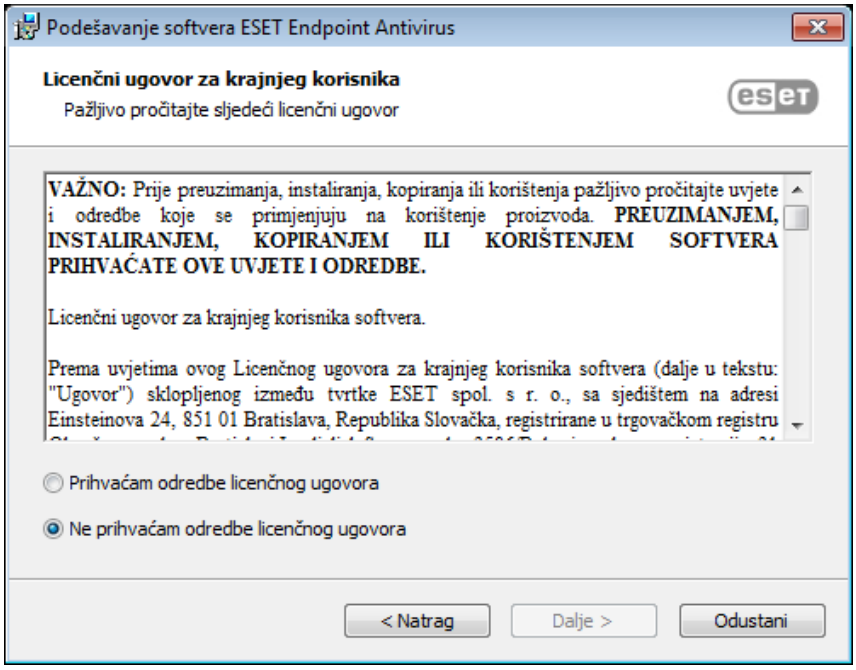
U poslovnim okruženjima, instalacijski program .msi preferirani je instalacijski paket. To je prvenstveno zbog izvanmrežnih i daljinskih instalacija koje se koriste raznim alatima, kao što je ESET PROTECT.

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

Instalacijski program ESET Endpoint Antivirus stvoren u programu ESET PROTECT podržava Windows 10 Enterprise za virtualne radne površine i način rada s više sesija sustava Windows 10.

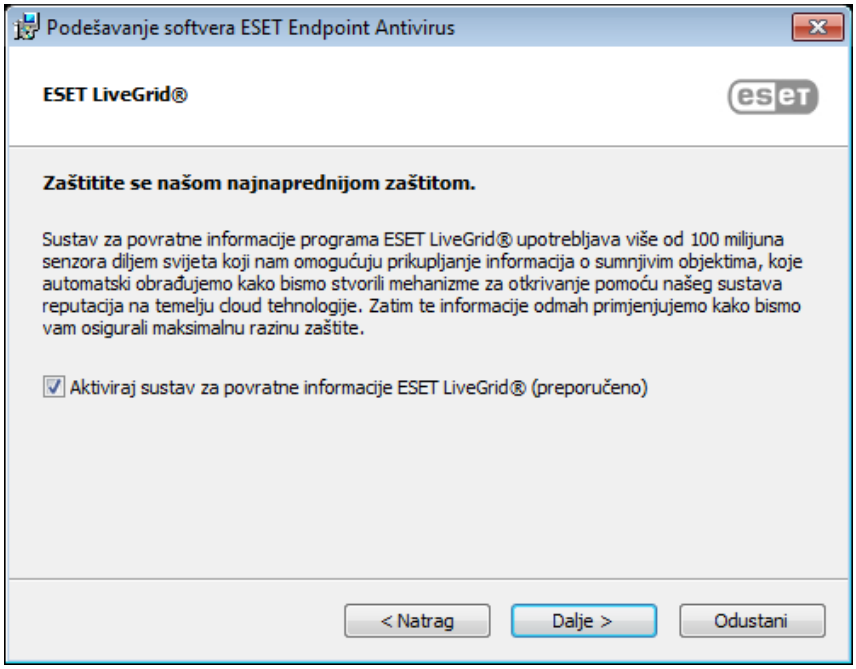
1. Odaberite željeni jezik i kliknite **Sljedeće**.

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



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

analiziraju, obrađuju i dodaju u modul detekcije. Kliknite **Napredne postavke** da biste konfigurirali dodatne instalacijske parametre.



4. Završni korak je potvrda instalacije klikom na **Instaliraj**. Nakon završetka instalacije od vas će se zatražiti da aktivirate program ESET Endpoint Antivirus.

Napredna instalacija (.msi)

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

1. Tijekom instalacije možete odabrati opciju **Promjena instalacijske mape**. Odaberite mjesto za instalaciju programa ESET Endpoint Antivirus. Prema standardnim postavkama program se instalira u sljedeću mapu:

C:\Program Files\ESET\ESET Security

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

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

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

2. Odaberite komponente proizvoda koje će se instalirati. Odaberite željene postavke za skeniranje računala i sve dostupne zaštite. Komponenta Aktualizacijski mirror može se upotrijebiti za aktualizaciju ostalih računala na vašoj mreži. Daljinsko praćenje i upravljanje (RMM) proces je nadgledanja i kontrole softverskih sustava koji upotrebljava lokalno instaliranog agenta kojemu može pristupiti davatelj usluga upravljanja.

3. Kliknite **Instaliraj** za pokretanje postupka instalacije.

Instalacija minimalnih modula

Kako bi se smanjio mrežni promet povezan s veličinom instalacijskog programa i uštedjeli resursi, ESET dolazi s instalacijskim programom minimalnih modula. Instalacijski program sadržava samo ključne module, a svi ostali moduli će se preuzeti tijekom početne nadogradnje modula nakon aktivacije programa. Njegova glavna prednost je znatno manji instalacijski program i uz to ESET Endpoint Antivirus preuzima samo najnovije module aplikacije kada aktivirate program.

Instalacijski program minimalnih modula i dalje sadržava sljedeće module:

- Učitavači
- Komunikacija Direct Cloud
- Podrška prijevoda
- Konfiguracija
- SSL

Nakon aktivacije programa vidjet ćete status **Pokretanje zaštite** koji će vas obavijestiti o pokretanju funkcija.

U slučaju problema s preuzimanjima modula (na primjer, postavke proxyja, bez mreže itd.) se prikazuje status upozorenja aplikacije **Potrebna je pozornost**. U glavnom prozoru programa kliknite **Nadogradi** > **Provjeri dostupnost nadogradnji** kako biste ponovno započeli postupak nadogradnje.

Nakon nekoliko neuspješnih pokušaja se prikazuje crveni status aplikacije **Podešavanje zaštite nije uspjelo**. Kliknite "Pokušaj ponovno" da biste ponovno pokrenuli podešavanje zaštite. Ako postupak pokretanja ne uspije i još uvijek ne možete preuzeti module, preuzmite potpune MSI instalacijske programe.

Ako klijentska računala nemaju internetsku vezu ili rade izvan mreže, a potrebna im je nadogradnja, upotrijebite sljedeće metode za preuzimanje datoteka s ESET-ovih servera za nadogradnju:
- Aktualizacija s mirrora
- Upotreba mirror alata

Instalacija putem naredbenog retka

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

Podržani parametri

APPDIR=<path>

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

APPDATADIR=<path>

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

MODULEDIR=<path>

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

ADDLOCAL=<list>

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

ADDEXCLUDE=<list>

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

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

U dokumentaciji za upotrijebljenu verziju **msiexec** potražite odgovarajuće parametre naredbenog retka.

Pravila

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

Komponente i funkcije

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

Funkcije se dijele u 4 kategorije:

- **Obavezno** – funkcija će se uvijek instalirati.
- **Nije obavezno** – odabir funkcije može se poništiti kako se ona ne bi instalirala.
- **Nevidljivo** – logična značajka obavezna za funkcioniranje ostalih značajki
- **Rezervirano mjesto** – značajka bez utjecaja na proizvod, ali mora se navesti s podznačajkama

U nastavku je naveden skup funkcija programa ESET Endpoint Antivirus:

Opis	Naziv značajke	Nadređena stavka funkcije	Prisutnost
Osnovne programske komponente	`Computer`		Rezervirano mjesto
Modul detekcije	`Antivirus`	`Computer`	Obavezno

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

Skup grupnih funkcija:

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

Dodatna pravila

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

Popis konfiguracijskih svojstava

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

LiveGrid® svojstvo

Prilikom instalacije programa ESET Endpoint Antivirus uz opcijuCFG_LIVEGRID_ENABLED, program će se ponašati na sljedeći način nakon instalacije:

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

Svojstvo ACTIVATION_DATA

Format	Metoda
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Aktivacija pomoću ESET-ova licenčnog ključa (potrebna je aktivna veza s internetom)
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	Aktivacija pomoću datoteke izvanmrežne licence

Svojstva jezika

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

Svojstvo	Vrijednost
PRODUCT_LANG=	LCID šifra (ID regionalnih postavki), primjerice 1033 za engleski (Sjedinjene Američke Države). Pogledajte popis kodova jezika.
PRODUCT_LANG_CODE=	LCID oznaka (naziv jezične kulture) malim slovima, primjerice en-us za engleski – Sjedinjene Američke Države. Pogledajte popis kodova jezika.

Svojstva za restart

Navedite sljedeće parametre za restart računala nakon instalacije:

Svojstvo	Vrijednost	Funkcija
REBOOT_WHEN_NEEDED=	0 – deaktivirano 1 – aktivirano	Ako je aktivirano, računalo će se restartati nakon instalacije.
REBOOT_CANCELABLE=	0 – deaktivirano 1 – aktivirano	Ako je aktivirano, korisnik može odustati od restarta računala.
REBOOT_POSTPONE=	vrijednost u sekundama	Maksimalno vrijeme u sekundama koje korisnik ima da odgodi restart računala.

REBOOT_CANCELABLE i REBOOT_POSTPONE su dostupni samo ako je opcija REBOOT_WHEN_NEEDED aktivirana.

Primjeri instalacije putem naredbenog retka

Obavezno pročitajte Licenčni ugovor za krajnjeg korisnika i provjerite imate li administratorske ovlasti prije pokretanja instalacije.

Izuzmite odjeljak **NetworkProtection** iz instalacije (morate isto tako navesti sve podređene funkcije):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

Ako želite da se program ESET Endpoint Antivirus automatski konfigurira nakon instalacije, možete navesti osnovne konfiguracijske parametre u instalacijskoj naredbi.
Instalirajte program ESET Endpoint Antivirus uz aktiviranESET LiveGrid®:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Instalirajte u drugu mapu za instalaciju aplikacije umjesto standardne mape.
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Instalirajte i aktivirajte program ESET Endpoint Antivirus pomoću ESET-ova licenčnog ključa.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Neprimjetna instalacija s detaljnim vođenjem dnevnika (korisno za otklanjanje poteškoća) i RMM samo s obaveznim komponentama:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Nametnuta neprimjetna instalacija na definiranom jeziku.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Opcije naredbenog retka nakon instalacije

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

Instalacija pomoću GPO-a ili SCCM-a

Osim izravne instalacije programa ESET Endpoint Antivirus na klijentsku radnu stanicu, možete ga instalirati i upotrebom alata za upravljanje kao što je objekt pravila grupe (GPO) ili programa Software Center Configuration Manager (SCCM), Symantec Altiris ili Puppet.

Upravljano (preporučeno)

Za upravljana računala najprije je potrebno instalirati ESET Management Agent, a zatim instalirati program ESET Endpoint Antivirus putem programa ESET PROTECT. ESET PROTECT mora biti instaliran na vašoj mreži.

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

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
- Instalirajte ESET Management Agent putem alata SCCM ili GPO
- Instalirajte ESET Management Agent putem objekta pravila grupe (GPO)

Neupravljano

Za neupravljana računala program ESET Endpoint Antivirus možete izravno instalirati na klijentske radne stanice. To se ne preporučuje zato što nećete moći pratiti i nametati pravila za sve ESET-ove sigurnosne programe na radnim stanicama.

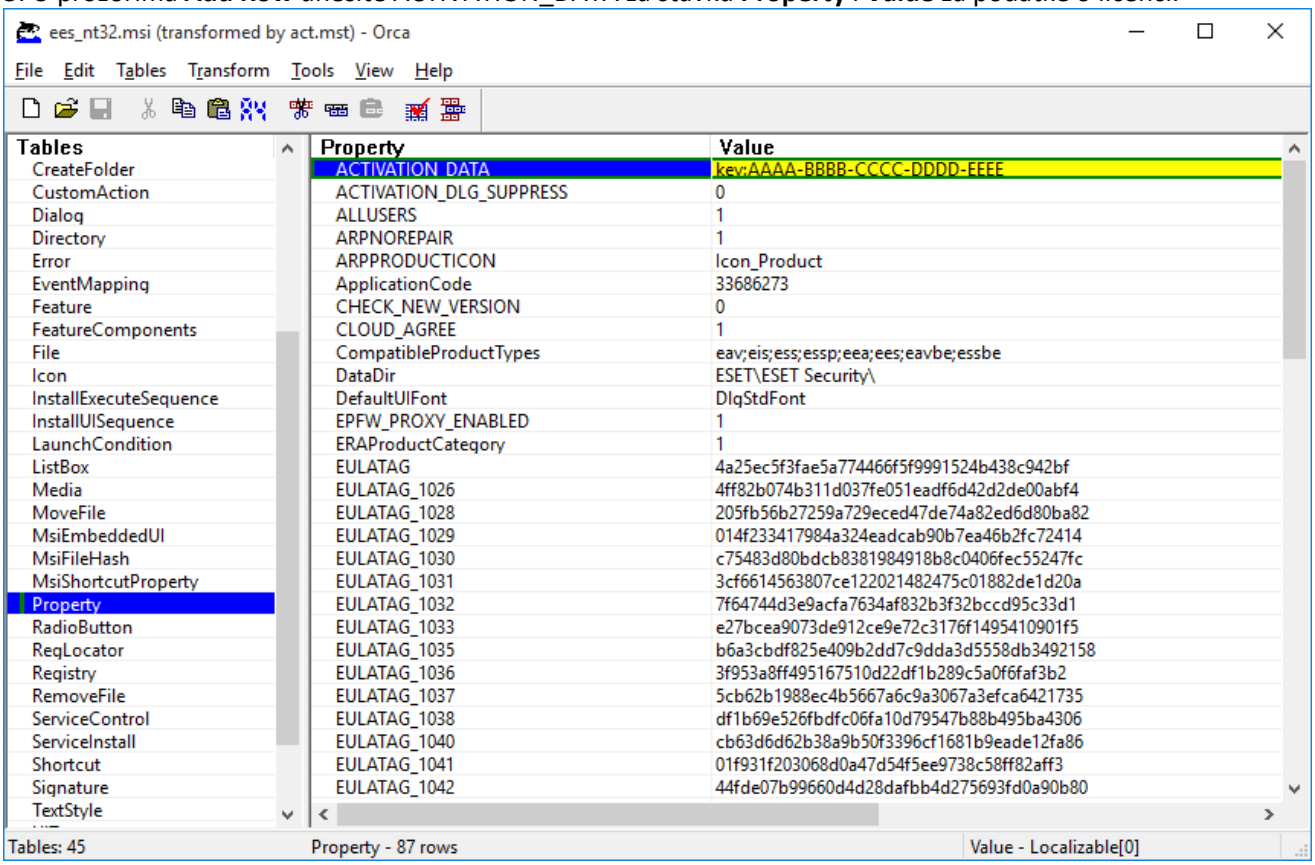
Prema standardnim postavkama program ESET Endpoint Antivirus nije aktiviran nakon instalacije i stoga ne funkcionira.

Opcija 1 (softverska instalacija)

1. Preuzmite instalacijski program .msi za program ESET Endpoint Antivirus.
2. Stvorite pretvorbeni paket .mst iz datoteke .msi (primjerice upotrebom uređivača Orca za .msi) da biste uključili svojstvo aktivacije programa (pogledajte `ACTIVATION_DATA` u odjeljku Instalacija putem naredbenog retka).

   Prikaz koraka za stvaranje paketa .mst u alatu Orca

1. Otvori stavku Orca
2. Učitajte instalacijski program .msi tako da kliknete **File** > **Open**.
3. Kliknite **Transform** > **New Transform**.
4. Kliknite **Property** u odjeljku **Tables** i zatim u izborniku **Tables** > **Add row**.
5. U prozorima **Add Row** unesite ACTIVATION_DATA za stavku **Property** i **Value** za podatke o licenci.



6. Kliknite **Pretvori** > **Generiraj pretvorbu** da biste spremili datoteku .mst.

1. Nije obavezno: za uvoz prilagođene konfiguracijske datoteke .xml za program ESET Endpoint Antivirus (npr. da biste aktivirali RMM ili konfigurirali postavke proxy servera), postavite datoteku cfg.xml na istu lokaciju kao i instalacijski program .msi.
2. Daljinski pokrenite instalacijski program .msi pomoću datoteke .mst upotrebljavajući GPO (putem softverske instalacije) ili SCCM.

Opcija 2 (upotreba zakazanog zadatka)

1. Preuzmite instalacijski program .msi za program ESET Endpoint Antivirus.
2. Pripremite skriptu za instalaciju putem naredbenog retka da biste uključili svojstvo aktivacija programa (pogledajte `ACTIVATION_DATA`).
3. Na mreži omogućite pristup instalacijskom programu .msi i skripti .cmd za sve radne stanice.
4. Nije obavezno: za uvoz prilagođene konfiguracijske datoteke .xml za program ESET Endpoint Antivirus (npr. da biste aktivirali RMM ili konfigurirali postavke proxy servera), postavite datoteku cfg.xml na istu lokaciju kao i instalacijski program .msi.
5. Primijenite pripremljenu skriptu za instalaciju putem naredbenog retka pomoću alata GPO ili SCCM.

    - Ako upotrebljavate GPO, upotrijebite Postavke grupnog pravila > Zakazani zadaci grupnog pravila > Zadatak koji se odmah izvršava

Ako ne želite upotrebljavati ESET PROTECT za daljinsko upravljanje ESET-ovim sigurnosnim programima, ESET Endpoint Antivirus sadrži ESET-ov dodatak za RMM kojim možete nadgledati i kontrolirati softverske sustave pomoću lokalno instaliranog agenta kojemu može pristupiti davatelj usluga upravljanja. Više informacija

Nadogradnja na noviju verziju

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

Nadogradnja na noviju verziju može se postići na nekoliko načina:

1. Automatski pomoću programa ESET PROTECT, ili ESET PROTECT Cloud.
2. Automatski, pomoću GPO-a ili SCCM-a.
3. Automatski, pomoću nadogradnje programa.
   Budući da se nadogradnja programa distribuira svim korisnicima i može utjecati na pojedine konfiguracije sustava, objavljuje se tek nakon dugoročnog testiranja kako bi se osigurala funkcionalnost sa svim mogućim konfiguracijama sustava. Ako trebate nadograditi na noviju verziju odmah nakon njenog izdavanja, upotrijebite jedan od načina u nastavku.
   Provjerite jeste li aktivirali **Način rada nadogradnje** u opciji Napredno podešavanje > **Nadogradnja** > **Profili** > **Nadogradnje programa**.
4. Ručno preuzimanjem i instaliranjem nove verzije preko prethodne.

Preporučeni scenariji nadogradnje

Upravljam ili želim upravljati svojim ESET programima na daljinu

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

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

Ručna nadogradnja na klijentskoj radnoj stanici

Da biste ručno nadogradili program ESET Endpoint Antivirus na pojedinačnim klijentskim radnim stanicama:

1. Provjerite je li podržana trenutačno instalirana verzija.
2. Provjerite je li vaš operacijski sustav podržan.

2. Preuzmite i instalirajte najnoviju verziju preko prethodne.

Uspješna instalacija najnovije verzije preko prethodne nije zajamčena za verzije s razinom podrške "istek trajanja". Pogledajte pravila o isteku trajanja da biste saznali razinu podrške svojeg programa ESET Endpoint Antivirus.
Da biste proveli nadogradnju iz nepodržanih verzija, najprije deinstalirajte program ESET Endpoint Antivirus. Za dodatne informacije o nadogradnji programa ESET Endpoint Antivirus na klijentskoj radnoj stanici pročitajte sljedeći članak iz ESET-ove baze znanja.

Automatska nadogradnja programa koji radi prema

starom standardu

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

Uobičajene teškoće prilikom instalacije

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

Da biste dovršili instalaciju:

1. Kliknite **Prihvati i nastavi** kako biste prihvatili Licenčni ugovor za krajnjeg korisnika i Pravila privatnosti. Ako se ne slažete s Licenčnim ugovorom za krajnjeg korisnika, kliknite **Deinstaliraj**. Ne možete se vratiti na prethodnu verziju.
2. Kliknite **Dopusti sve i nastavi** da biste dopustili Sustav za povratne informacije programa ESET LiveGrid® ili kliknite **Nastavi** ako ne želite sudjelovati.
3. Nakon aktivacije novog ESET-ovog programa pomoću licenčnog ključa prikazat će se početna stranica. Ako nije moguće pronaći vaše podatke o licenci, nastavite s novom probnom licencom. Ako licenca koju ste upotrebljavali za prethodni program nije valjana, aktivirajte ESET-ov program.
4. Za dovršetak instalacije potrebno je ponovno pokrenuti uređaj.

Nadogradnje za potrebe sigurnosti i stabilnosti

Nadogradnja programa ESET Endpoint Antivirus važan je dio osiguranja potpune zaštite od zlođudnih kodova. Svaka nova verzija programa ESET Endpoint Antivirus sadržava brojna poboljšanja i ispravke pogrešaka. Preporučujemo povremenu nadogradnju programa ESET Endpoint Antivirus kako bi se spriječila sigurnosna ranjivost i prijetnje. ESET Endpoint Antivirus nalazi se u određenoj fazi životnog ciklusa programa, kao i svi ostali ESET-ovi programi.

Pročitajte više o:
Pravila o isteku programa (poslovni programi)
Nadogradnje programa
Hitni popravci sigurnosti i stabilnosti
Dodatne informacije o promjenama programa ESET Endpoint Antivirus pročitajte u sljedećem članku u ESET-ovoj bazi znanja.

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

Aktivacija proizvoda

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

Program možete aktivirati na nekoliko načina. Dostupnost određenog scenarija aktivacije u prozoru aktivacije ovisi o zemlji i načinu distribucije instalacijske datoteke (ESET-ova stranica, vrsta instalacijskog programa .msi ili .exe itd.).

Aktivirati program ESET Endpoint Antivirus možete u glavnom prozoru programa > **Pomoć i podrška** > **Aktiviraj**

program ili **Status zaštite** > **Aktiviraj program**.

Možete koristiti bilo koji od sljedećih način za aktivaciju ESET Endpoint Antivirus:

- **Unesite kupljeni licenčni ključ** – Jedinstveni niz formata XXXX-XXXX-XXXX-XXXX-XXXX koji se koristi za identifikaciju vlasnika licence i za aktivaciju licence.
- **ESET HUB** – ESET HUB račun koji morate stvoriti. ESET HUB je središnji pristupnik jedinstvenoj sigurnosnoj platformi servisa ESET PROTECT. Osigurava centralizirani identitet, pretplatu i upravljanje korisnicima za sve module ESET-ovih platformi. Ovu opciju aktivacije možete upotrebljavati i za aktivaciju programa ESET Endpoint Antivirus pomoću starijih alata za upravljanje licencama: ESET Business Account ili ESET MSP Administrator.
- **Izvanmrežna licenca** – Automatski stvorena datoteka koja će se prenijeti u ESET-ov program kako bi pružila informacije o licenci. Ako licenca omogućuje preuzimanje datoteke izvanmrežne licence (.lf), ta datoteka može se upotrijebiti za izvanmrežnu aktivaciju. Broj izvanmrežnih licenci bit će oduzet od ukupnog broja dostupnih licenci. Dodatne informacije o stvaranju izvanmrežne datoteke potražite u online korisničkom priručniku za ESET Business Account.

Kliknite mogućnost **Aktiviraj kasnije** ako je vaše računalo član upravljane mreže i ako će vaš administrator obaviti daljinsku aktivaciju putem sučelja ESET PROTECT. Tu mogućnost možete upotrijebiti i ako klijenta želite aktivirati kasnije.

Ako imate korisničko ime i lozinku za aktivaciju starijih ESET programa, pretvorite svoje naslijeđene korisničke podatke u licenčni ključ.

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

ESET PROTECT može neprimjetno aktivirati klijentska računala koristeći se licencama koje je omogućio administrator. Upute potražite u pomoći na mreži programa ESET PROTECT.

Aktivacija programa nije uspjela?

Unos Licenčnog ključa prilikom aktivacije

Automatske nadogradnje važne su za vašu sigurnost. ESET Endpoint Antivirus primit će nadogradnje koje su aktivirane **licenčnim ključem**.

Ako nakon instalacije niste unijeli licenčni ključ, program se neće aktivirati. Možete promijeniti licencu u glavnom prozoru programa. Da biste to učinili, kliknite **Pomoć i podrška** > **Aktiviraj licencu** i unesite podatke licence koje ste primili sa sigurnosnim programom tvrtke ESET u prozor Aktivacije programa.

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

- Licenčni ključ jedinstveni je niz u formatu XXXX-XXXX-XXXX-XXXX-XXXX koji se koristi za identifikaciju vlasnika licence i aktivaciju licence.

Radi točnosti, preporučujemo da licenčni ključ kopirate i zalijepite iz e-pošte koju ste dobili prilikom registracije.

ESET HUB račun

ESET HUB je središnji pristupnik jedinstvenoj sigurnosnoj platformi servisa ESET PROTECT. Osigurava centralizirani identitet, pretplatu i upravljanje korisnicima za sve module ESET-ovih platformi. Pomoću programa ESET HUB možete:

- Pregled sigurnosnih pretplata
- Provjera upotrebe i statusa pretplaćenih usluga
- Dodjela i kontrola granularnog pristupa pojedinačnim ESET-ovim platformama
- Jedinstvena prijava za sve povezane ESET-ove platforme kojima se može pristupiti

Ovu opciju aktivacije možete upotrebljavati i za aktivaciju programa ESET Endpoint Antivirus pomoću starijih alata za upravljanje licencama: ESET Business Account ili ESET MSP Administrator.

Isto tako možete stvoriti ESET HUB račun i prijaviti se pomoću svoje **adrese e-pošte** i **lozinke**.

Ako ste zaboravili svoju lozinku, kliknite **Zaboravio/la sam lozinku** i bit ćete preusmjereni na ESET HUB. Unesite adresu e-pošte i kliknite **Prijava** da biste potvrdili. Zatim ćemo vam poslati poruku s uputama za ponovno postavljanje lozinke.

Upotreba podataka o staroj licenci za aktivaciju ESET-ova sigurnosnog programa

Ako već imate korisničko ime i lozinku i želite ključ licence, posjetite ESET Business Accountportal tvrtke ESET za administriranje licenci gdje svoje podatke možete pretvoriti u novi ključ licence.

Aktivacija nije uspjela

Ako aktivacija programa ESET Endpoint Antivirus nije uspješna, to se najčešće događa zbog sljedećeg:

- Licenčni ključ je već u upotrebi.
- Unijeli ste licenčni ključ koji nije valjan.
- Informacije u obrascu za aktivaciju nedostaju ili nisu valjane.
- Komunikacija sa serverom za aktivaciju nije uspjela.
- Nema veze s ESET-ovim serverima za aktivaciju ili je veza deaktivirana.

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

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

- Pokretanje postupka otklanjanja poteškoća za aktivaciju ESET-ova programa

Registracija

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

tvrtke ESET.

Napredak aktivacije

ESET Endpoint Antivirus se aktivira, ovo bi moglo potrajati nekoliko trenutaka.

Aktivacija je uspješna

Aktivacije je uspješno završena, program ESET Endpoint Antivirus sada je aktiviran. Od sad nadalje, ESET Endpoint Antivirus će primati redovite aktualizacije kako bi prepoznao najnovije prijetnje i štitio vaše računalo. Kliknite **Gotovo** da biste zatvorili program.

Uobičajene teškoće prilikom instalacije

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

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

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

Vodič za početnike

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

Ikona trake sustava

Neke od najvažnijih mogućnosti i značajki podešavanja dostupne su kada desnom tipkom miša kliknete ikonu trake sustava  .

> Da biste pristupili izborniku ikone trake sustava (područje obavijesti sustava Windows), provjerite je li način pokretanja funkcije Elementi korisničkog sučelja postavljen na Potpuno.

Pauziraj zaštitu – Prikazuje upit za potvrdu kojim se deaktivira Modul detekcije, koji štiti od napada kontrolirajući komunikaciju datoteka, weba i e-pošte. Padajući izbornik **Vremensko razdoblje** omogućuje vam da odredite koliko će dugo zaštita biti deaktivirana.

Napredno podešavanje – otvara napredno podešavanje programa ESET Endpoint Antivirus ***. Da biste otvorili Napredno podešavanje u glavnom prozoru programa, pritisnite F5 na svojoj tipkovnici i kliknite **Podešavanje** > **Napredno podešavanje**.

Dnevnici – dnevnici sadrže informacije o važnim događajima u programu koji su se pojavili i pružaju pregled otkrivenih prijetnji.

Otvori program ESET Endpoint Antivirus – Otvara glavni prozor programa ESET Endpoint Antivirus s ikone trake

(područje obavijesti sustava Windows).

Poništi raspored prozora – Vraća prozor programa ESET Endpoint Antivirus na standardnu veličinu i položaj na zaslonu.

Način boja – otvara postavke korisničkog sučelja gdje možete promijeniti boju za grafičko korisničko sučelje.

Provjeri dostupnost nadogradnji – pokreće nadogradnju modula ili programa kako biste bili sigurni da ste zaštićeni. ESET Endpoint Antivirus automatski provjerava ima li nadogradnji nekoliko puta dnevno.

O programu – pruža informacije o sustavu, detalje o instaliranoj verziji programa ESET Endpoint Antivirus, instaliranim modulima programa i informacije o datumu isteka licence te o operacijskom sustavu i sistemskim resursima.

Tipkovnički prečaci

Za bolju navigaciju u programu ESET Endpoint Antivirus možete upotrijebiti sljedeće tipkovne prečace:

Tipkovnički prečaci	Akcija
F1	otvara stranice pomoći
F5	otvara Napredno podešavanje
Strelica gore / strelica dolje	navigacija u stavkama padajućeg izbornika
TAB	prelazi na sljedeći element GUI-ja u prozoru
Shift+TAB	premješta na prethodni element GUI-ja u prozoru
ESC	zatvara aktivni dijaloški prozor
Ctrl+U	prikazuje informacije o licenci za ESET i vašem računalu (Detalji za tehničku podršku)
Ctrl+R	vraća prozor programa na standardnu veličinu i položaj na zaslonu
ALT + Strelica lijevo	vraća natrag
ALT + Strelica desno	kreće se naprijed
ALT+Home	ide na početak

Za navigaciju možete upotrebljavati i tipke miša naprijed ili natrag.

Profili

Upravljanje profilima koristi se na dva mjesta u programu ESET Endpoint Antivirus – u odjeljku **Skeniranje na zahtjev** i u odjeljku **Nadogradnja**.

Skeniranje računala

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

- **Smart skeniranje** – ovo je standardni napredni profil skeniranja. Profil Smart skeniranja upotrebljava tehnologiju Smart optimizacije koja isključuje datoteke za koje je tijekom prethodnog skeniranja utvrđeno da su čiste, a od tog skeniranja nisu izmijenjene. To omogućuje kraće vrijeme skeniranja s minimalnim utjecajem na sigurnost sustava.

- **Skeniranje iz kontekstnog izbornika** – iz kontekstnog izbornika možete započeti skeniranje bilo koje datoteke na zahtjev. Profil skeniranja iz kontekstnog izbornika omogućuje vam da definirate konfiguraciju skeniranja koja će se upotrebljavati kada pokrenete skeniranje na ovaj način.
- **Dubinsko skeniranje** – profil dubinskog skeniranja standardno ne upotrebljava Smart optimizaciju, tako da nijedna datoteka nije isključena iz skeniranja pomoću ovog profila.
- **Skeniranje računala** – ovo je standardni profil koji se upotrebljava za standardno skeniranje računala.

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

Za stvaranje novog profila otvorite stavke Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Skeniranje na zahtjev** > **Popis profila** > **Uredi**. Prozor **Upravljanje profilima** sadrži padajući izbornik **Odabrani profil** s postojećim profilima skeniranja i mogućnošću stvaranja novog. Pomoć pri stvaranju profila skeniranja koji odgovara vašim potrebama potražite u odjeljku ThreatSense, gdje možete pronaći opis svakog parametra podešavanja skeniranja.

Pretpostavimo da želite stvoriti vlastiti profil skeniranja i djelomično vam odgovara konfiguracija **Skenirajte svoje računalo**, no ne želite skenirati runtime arhivatore ni potencijalno nesigurne aplikacije te želite primijeniti **Uvijek ukloni prijetnju**. Unesite naziv novog profila u prozoru **Upravljanje profilima** i kliknite **Dodaj**. Odaberite novi profil iz padajućeg izbornika **Odabrani profil** i prilagodite preostale parametre kako vam odgovara te kliknite **U redu** da biste spremili novi profil.

Nadogradnja

Uređivač profila u odjeljku za podešavanje aktualizacije korisnicima omogućuje stvaranje novih aktualizacijskih profila. Stvarajte i koristite vlastite prilagođene profile (koji se razlikuju od standardnog predloška **Moj profil**) samo ako na računalu koristite više različitih načina povezivanja s aktualizacijskim serverima.

Na primjer, prijenosno računalo koje se obično povezuje s lokalnim serverom (mirrorom) u lokalnoj mreži, ali koje u slučaju prekida veze s lokalnom mrežom (tijekom, primjerice, poslovnog puta) preuzima aktualizacije izravno s aktualizacijskog servera tvrtke ESET, može koristiti dva profila: jedan za povezivanje s lokalnim serverom, a drugi za povezivanje sa serverima tvrtke ESET. Nakon konfiguracije tih profila idite na **Alati** > **Planer** i uredite parametre aktualizacijskog zadatka. Odredite jedan profil kao primarni, a drugi kao sekundarni.

Profil za nadogradnju – Profil za nadogradnju koji se trenutačno koristi. Da biste ga promijenili, odaberite neki profil s padajućeg izbornika.

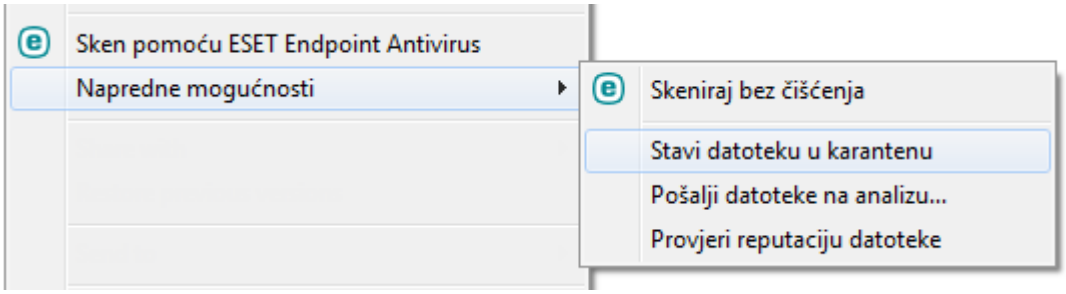
Popis profila – Stvorite nove ili uklonite postojeće profile za nadogradnju.

Kontekstni izbornik

Kontekstni izbornik prikazuje se kada desnom tipkom miša kliknete neki objekt (datoteku). Izbornik prikazuje sve akcije koje se mogu izvesti na objektu.

Elemente kontrole programa ESET Endpoint Antivirus možete integrirati u kontekstni izbornik. Opcije podešavanja za tu funkciju dostupne su u izborniku Napredno podešavanje > **Korisničko sučelje** > **Elementi korisničkog sučelja**.

Integriraj u kontekstni izbornik – Integrirajte kontrolne elemente programa ESET Endpoint Antivirus u kontekstni izbornik.

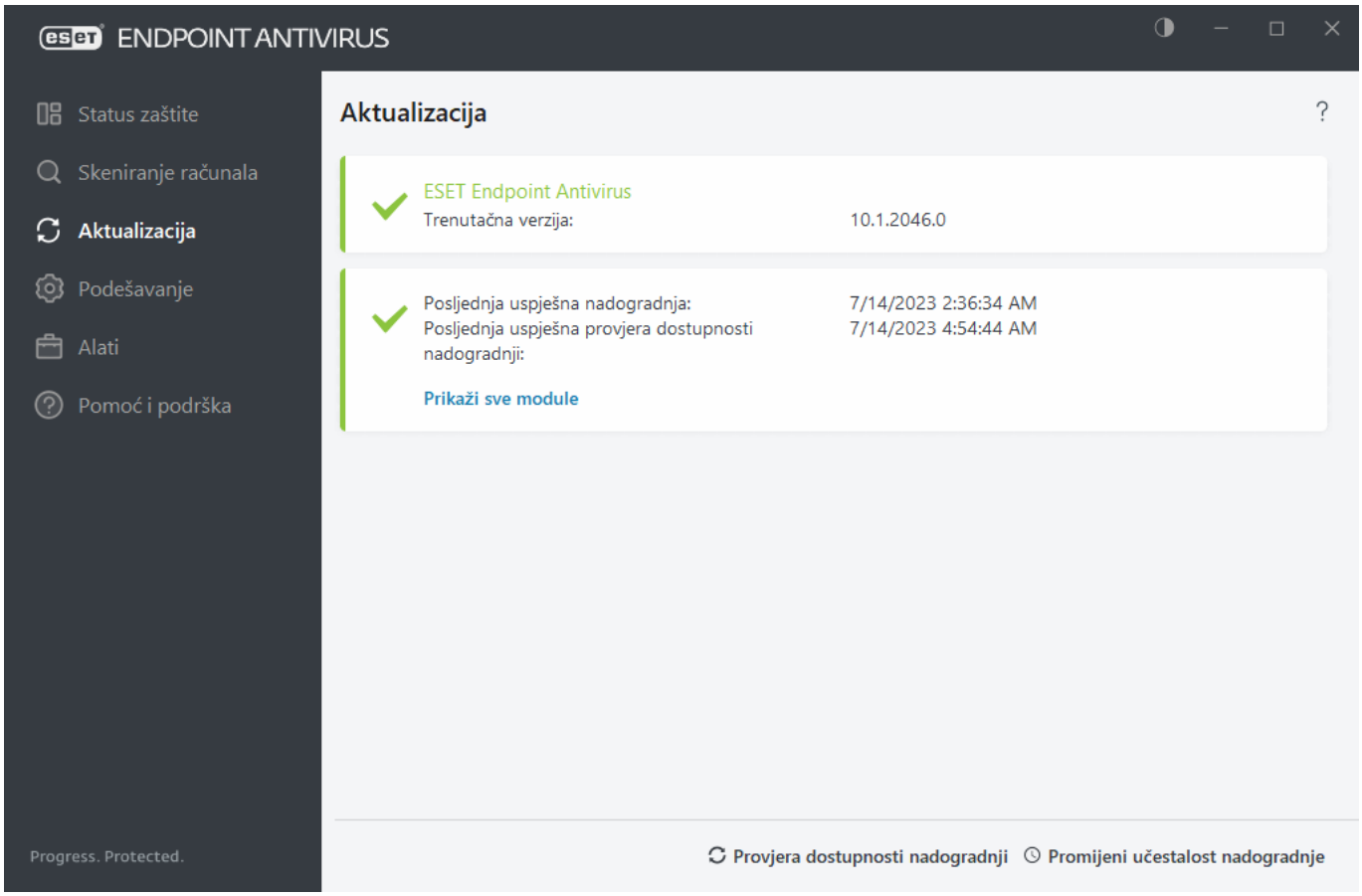


Podešavanje aktualizacije

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

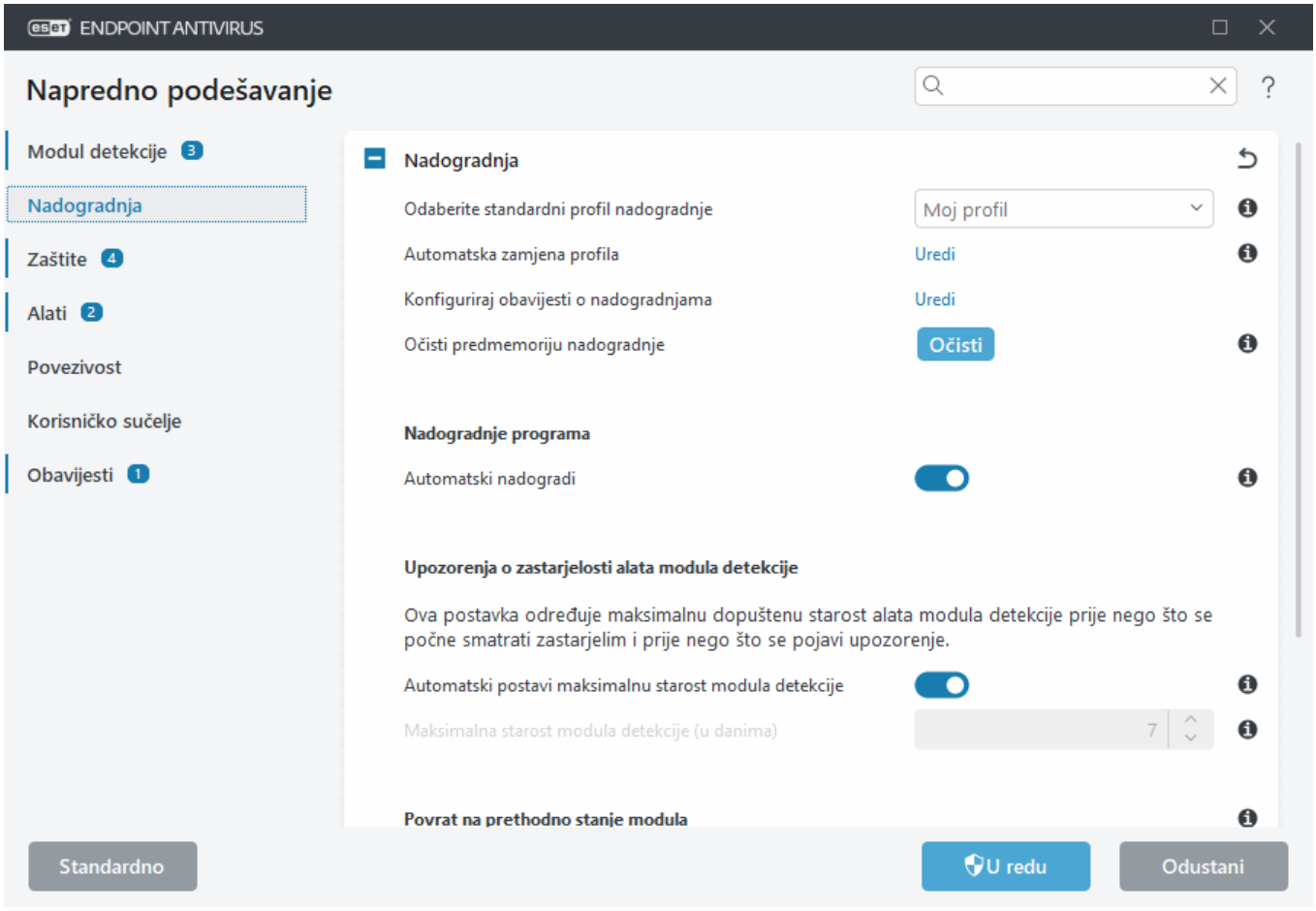
Klikom gumba **Aktualizacija** u glavnom prozoru programa možete provjeriti status trenutačne nadogradnje, datum i vrijeme zadnje uspješne nadogradnje te je li nadogradnja potrebna.

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



Napredno podešavanje > **Ažuriranje** sadrži dodatne mogućnosti ažuriranja, kao što su način ažuriranja, pristup proxy poslužitelju i LAN veze.

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

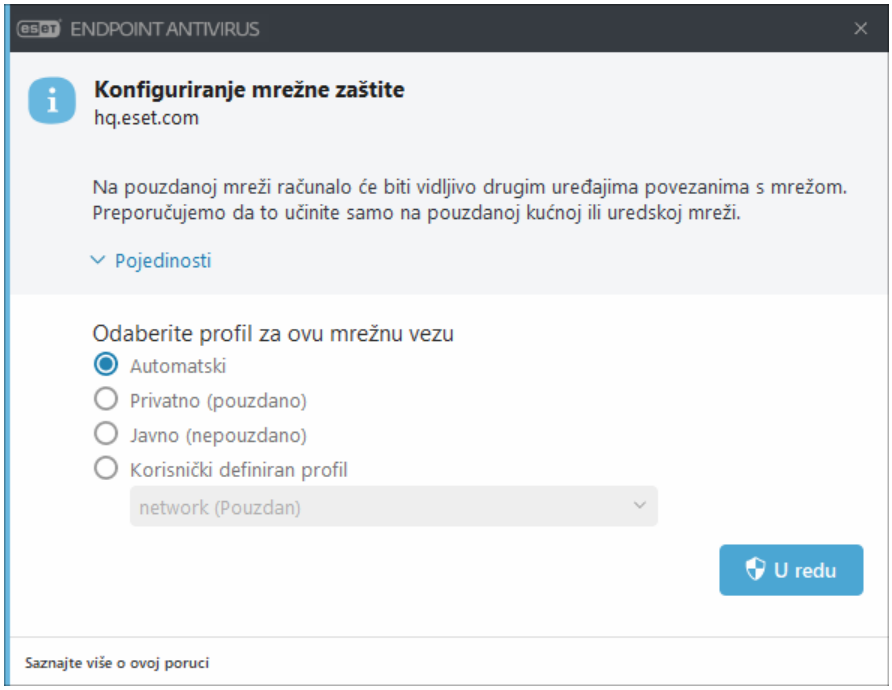


Opcija **odaberi automatski** u izborniku Napredno podešavanje > **Nadogradi** > **Profili** > **Nadogradnje** > **Nadogradnje modula** se aktivira prema standardnim postavkama. Ako upotrebljavate ESET-ov server za nadogradnju, preporučujemo da ostavite odabranu standardnu opciju.

Za optimalnu funkcionalnost program se mora automatski nadograditi. Automatske nadogradnje moguće su samo ako je točan licenčni ključ unesen pod **Pomoć i podrška** > **Aktiviraj program**. Ako nakon instalacije niste unijeli Ključ licence, možete to učiniti u bilo kojem trenutku. Detaljnije informacije o aktivaciji potražite u odjeljku Kako aktivirati program ESET Endpoint Antivirus.

Konfiguriranje mrežne zaštite

Prema zadanoj postavci, ESET Endpoint Antivirus upotrebljava postavke programa Windows kada se otkrije nova mreža. Da bi se prilikom otkrivanja nove mreže prikazivao dijaloški okvir, promijenite stavku Dodjela profila mrežne zaštite u **Pitaj**. Konfiguracija mrežne zaštite prikazat će se prilikom svakog povezivanja računala s novom mrežom.



Možete odabrati jedan od sljedećih profila mrežne veze:

Automatski – ESET Endpoint Antivirus automatski će odabrati profil na temelju aktivatora konfiguriranih za svaki profil.

Privatno – za pouzdane mreže (kućnu ili uredsku mrežu). Vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi su drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži (aktiviran je pristup zajedničkim datotekama i pisačima, aktivirana je dolazna RPC komunikacija i dostupno je daljinsko dijeljenje radne površine). Preporučujemo upotrebu ove postavke prilikom pristupa sigurnoj lokalnoj mreži. Ovaj se profil automatski dodjeljuje mrežnoj vezi ako je konfigurirana kao Domenska ili Privatna mreža u sustavu Windows.

Javno – za nepouzdane mreže (javnu mrežu). Datoteke i mape u vašem sustavu ne dijele se s drugim korisnicima na mreži niti su im vidljive i deaktivirano je dijeljenje resursa sustava. Preporučujemo upotrebu ove postavke prilikom pristupa bežičnim mrežama. Ovaj se profil automatski dodjeljuje bilo kojoj mrežnoj vezi koja nije konfigurirana kao Domenska ili Privatna mreža u sustavu Windows.

Korisnički definirani profil – na padajućem izborniku možete odabrati profil koji ste izradili . Ova je mogućnost dostupna samo ako ste izradili barem jedan prilagođeni profil.

⚠ Neispravna konfiguracija mreže može predstavljati sigurnosni rizik za računalo.

Blokirani hashevi

Upotreba servisa ESET Inspect u vašem okruženju omogućuje administratorima blokiranje pristupa određenim izvršnim datotekama na temelju njihovog hasha. Ako administrator blokira pristup izvršnoj datoteci i pokušate joj pristupiti, ESET Endpoint Antivirus prikazuje sljedeću obavijest:

Pristup datoteci je blokiran – aplikacija (prikazuje se naziv aplikacije) je pokušala pristupiti datoteci koju administrator ne dopušta.

Ako ste administrator i želite dopustiti pristup aplikaciji navedenoj u obavijesti, pročitajte članak Blokirani hashevi

u pomoći na mreži servisa ESET Inspect. Ako ste korisnik i želite promijeniti ponašanje aplikacije, obratite se administratoru.

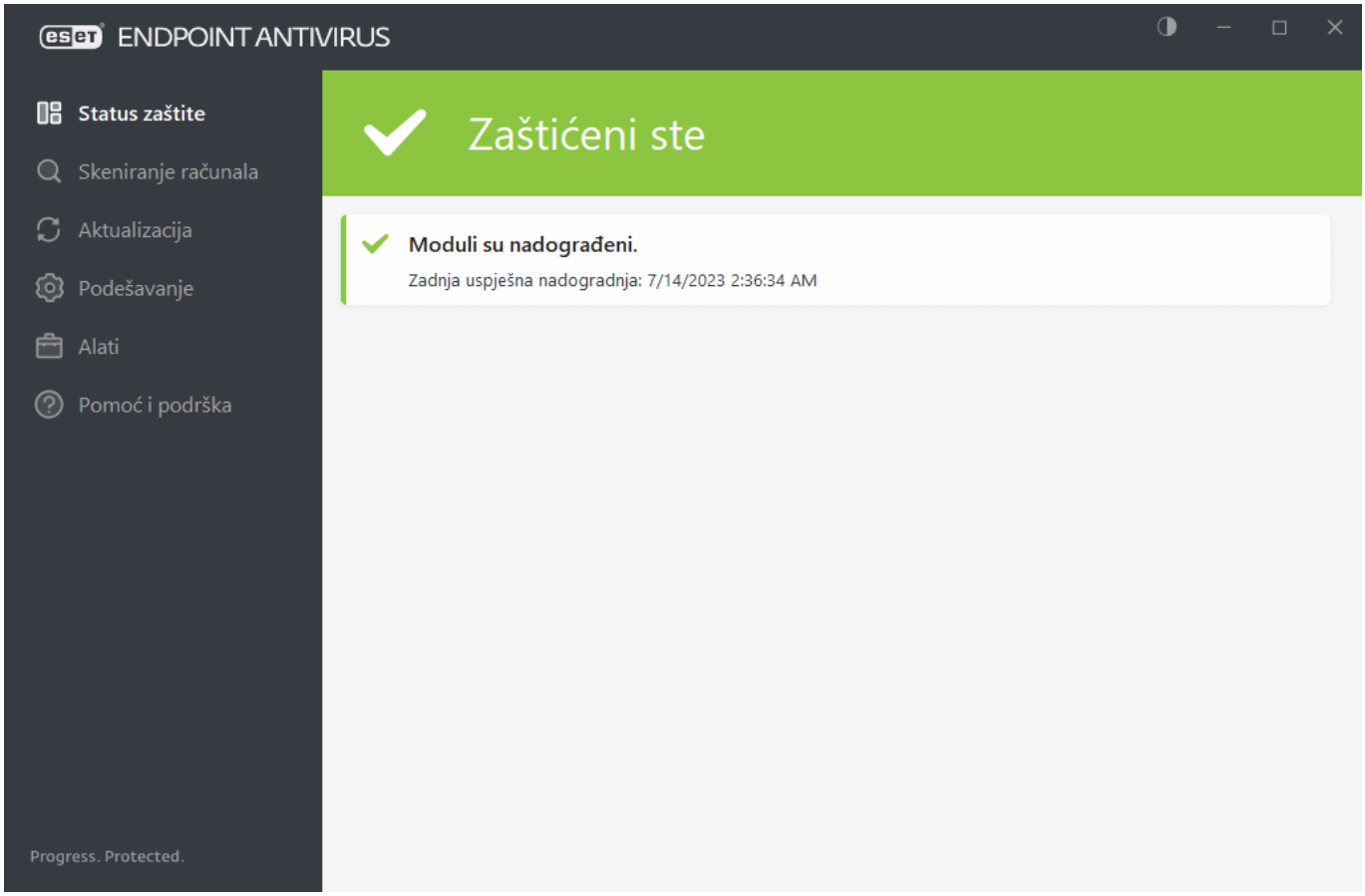
Rad s programom ESET Endpoint Antivirus

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

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

U gornjem desnom kutu glavnog prozora programa možete odabrati shemu boja grafičkog korisničkog sučelja programa ESET Endpoint Antivirus. Kliknite ikonu **sheme boja** (ikona se mijenja na temelju trenutačno odabrane sheme boja) pokraj ikone **smanjivanja** i u padajućem izborniku odaberite shemu boja:

- **Isto kao i boja sustava** – postavlja shemu boja programa ESET Endpoint Antivirus na temelju postavki operacijskog sustava.
- **Tamno** – program ESET Endpoint Antivirus će imati tamnu shemu boja (tamni način rada).
- **Svijetlo** – program ESET Endpoint Antivirus će imati standardnu, svijetlu shemu boja.



Opcije glavnog izbornika:

Status zaštite – Pruža informacije o statusu zaštite programa ESET Endpoint Antivirus.

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

Nadogradnja – prikazuje informacije o modulu i nadogradnjama modula detekcije.

Alati – Funkcije koji pomažu pojednostaviti administraciju programa i nude dodatne opcije za napredne korisnike.

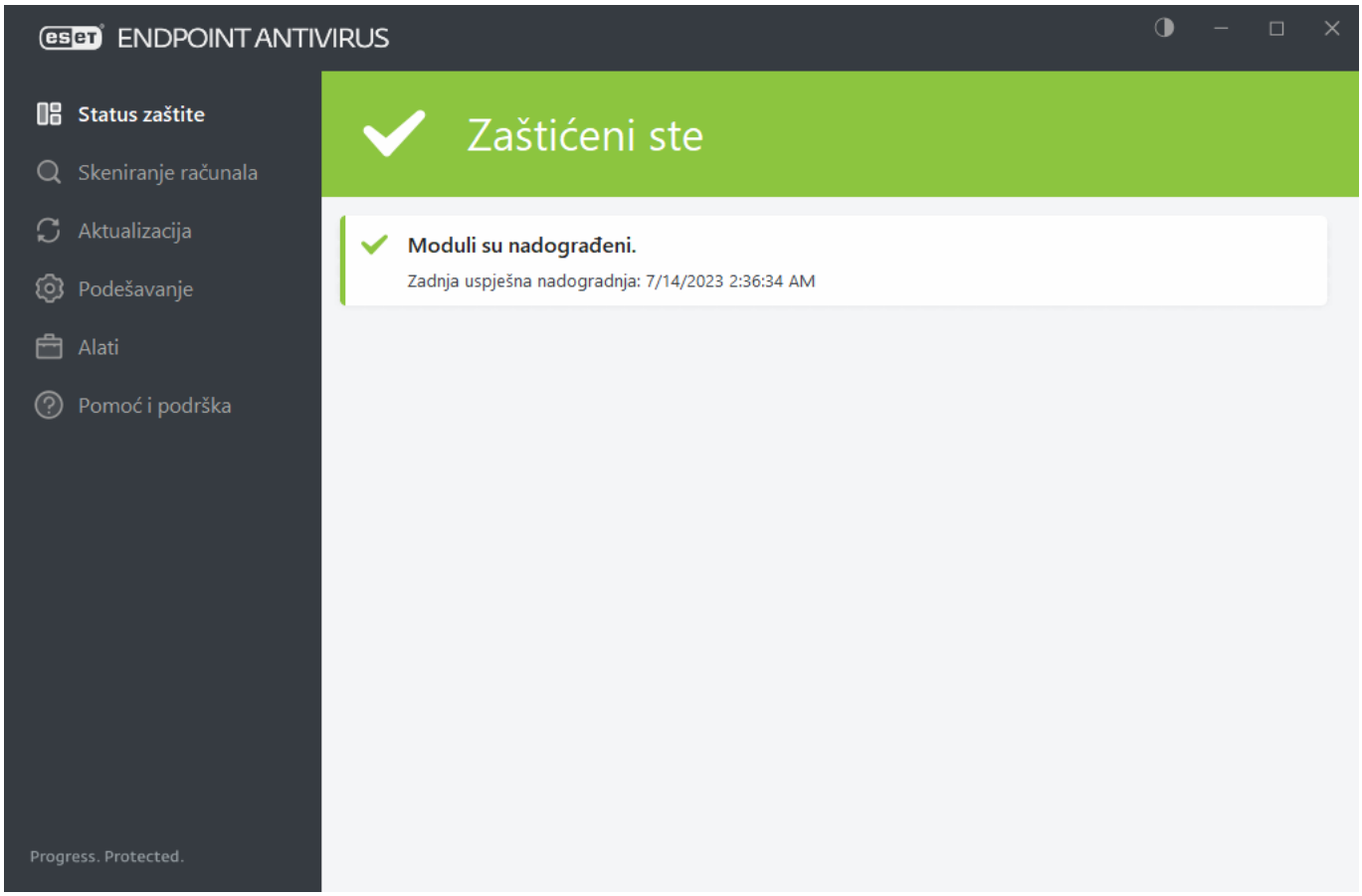
Podešavanje – pruža opcije konfiguracije za funkcije zaštite programa ESET Endpoint Antivirus i pristup opciji Napredno podešavanje.

Pomoć i podrška – prikazuje informacije o vašoj licenci, instaliranom ESET-ovom programu i vezama na pomoć na mreži, ESET-ovu bazu znanja i tehničku podršku.

Status zaštite

Prozor **Status zaštite** prikazuje informacije o trenutačnoj zaštiti računala i posljednjoj nadogradnji. Zeleni status **Maksimalna zaštita** znači da je osigurana maksimalna zaštita.

U prozoru **Status zaštite** se prikazuju obavijesti s detaljnim informacijama i preporučenim rješenjima za poboljšanje sigurnosti programa ESET Endpoint Antivirus, uključivanje dodatnih funkcija ili osiguranje maksimalne zaštite.

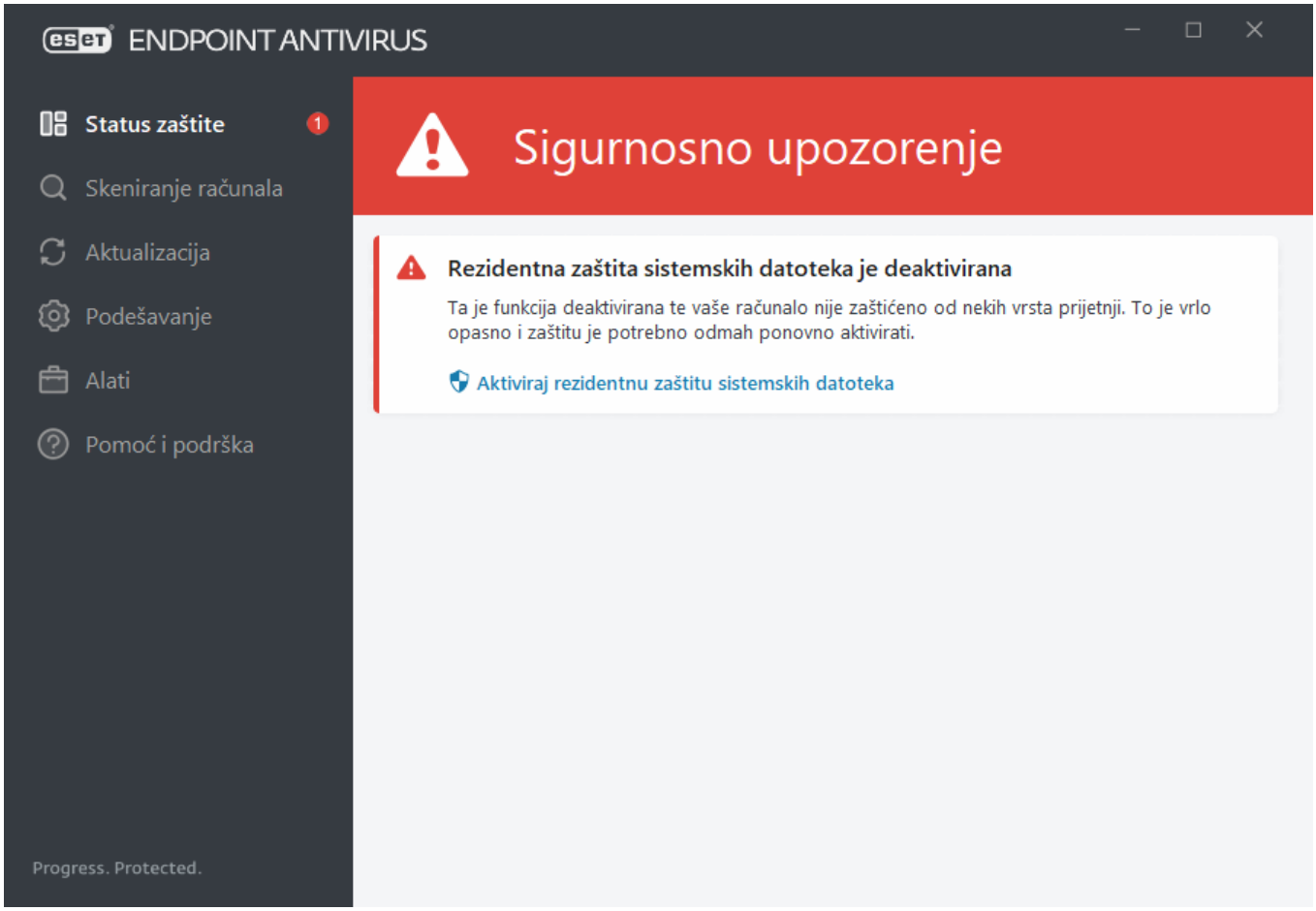


Zelena ikona i zeleni status **Zaštićeni ste** označavaju da je osigurana maksimalna zaštita.

Što učiniti ako program ne funkcionira ispravno?

Pokraj svih modula programa koji su u potpunosti funkcionalni prikazat će se zelena potvrdna kvačica. Ako je potrebno obratiti pozornost na modul, prikazuje se crveni uskličnik ili narančasta ikona s obavijesti. Dodatne informacije o modulu, uključujući i naše preporuke o tome kako vratiti sve funkcije, prikazane su u gornjem dijelu

prozora. Da biste promijenili status modula, na glavnom izborniku kliknite **Podešavanje** i kliknite željeni modul.



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

- **Antivirusna i antispyware zaštita je pauzirana** – kliknite **Pokreni sve module antivirusne i antispyware zaštite** da biste ponovno aktivirali antivirusnu i antispyware zaštitu u oknu **Status zaštite** ili **Aktiviraj antivirusnu i antispyware zaštitu** u oknu **Podešavanje** u glavnom programskom prozoru.
- Antivirusna je zaštita deaktivirana – pokretanje virusnog skenera nije uspjelo. Većina modula programa ESET Endpoint Antivirus neće ispravno raditi.
- **Antiphishing zaštita ne funkcionira** – funkcija ne funkcionira jer ostali potrebni moduli programa nisu aktivni.
- **Zastario je modul detekcije** – ta će se pogreška pojaviti nakon nekoliko neuspješnih pokušaja nadogradnje modula detekcije (prethodno baze podataka virusnih potpisa). Preporučujemo da provjerite aktualizacijske postavke. Najčešći je uzrok ove pogreške neispravan unos podataka za autentikaciju ili neispravna konfiguracija postavki povezivanja.
- **Program nije aktiviran** ili je **Licenca je istekla** – to označava crvena ikona statusa zaštite. Program se ne može nadograditi nakon što licenca istekne. Preporučujemo da pratite upute u prozoru upozorenja i obnovite svoju licencu.
- **Deaktiviran je sustav za sprečavanje upada (HIPS)** – Ovaj se problem javlja kada se HIPS deaktivira. Računalo nije zaštićeno od nekih vrsta prijetnji i potrebno je ponovno aktivirati zaštitu klikom opcije **Aktiviraj HIPS**.
- **Nisu zakazane redovne aktualizacije** – ESET Endpoint Antivirus neće provjeravati ili primati važne aktualizacije osim ako ne zakažete aktualizacijski zadatak.
- **Blokiran pristup mreži** – prikazuje se kad se pokrene zadatak klijenta **Izolacija računala s mreže** na ovoj

radnoj stanici iz programa ESET PROTECT. Obratite se svom administratoru sustava za više informacija.

- **Pauzirana je rezidentna zaštita** – korisnik je deaktivirao rezidentnu zaštitu. Vaše računalo nije zaštićeno od prijetnji. Kliknite Aktiviraj rezidentnu zaštitu da biste ponovno aktivirali tu funkciju.


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

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

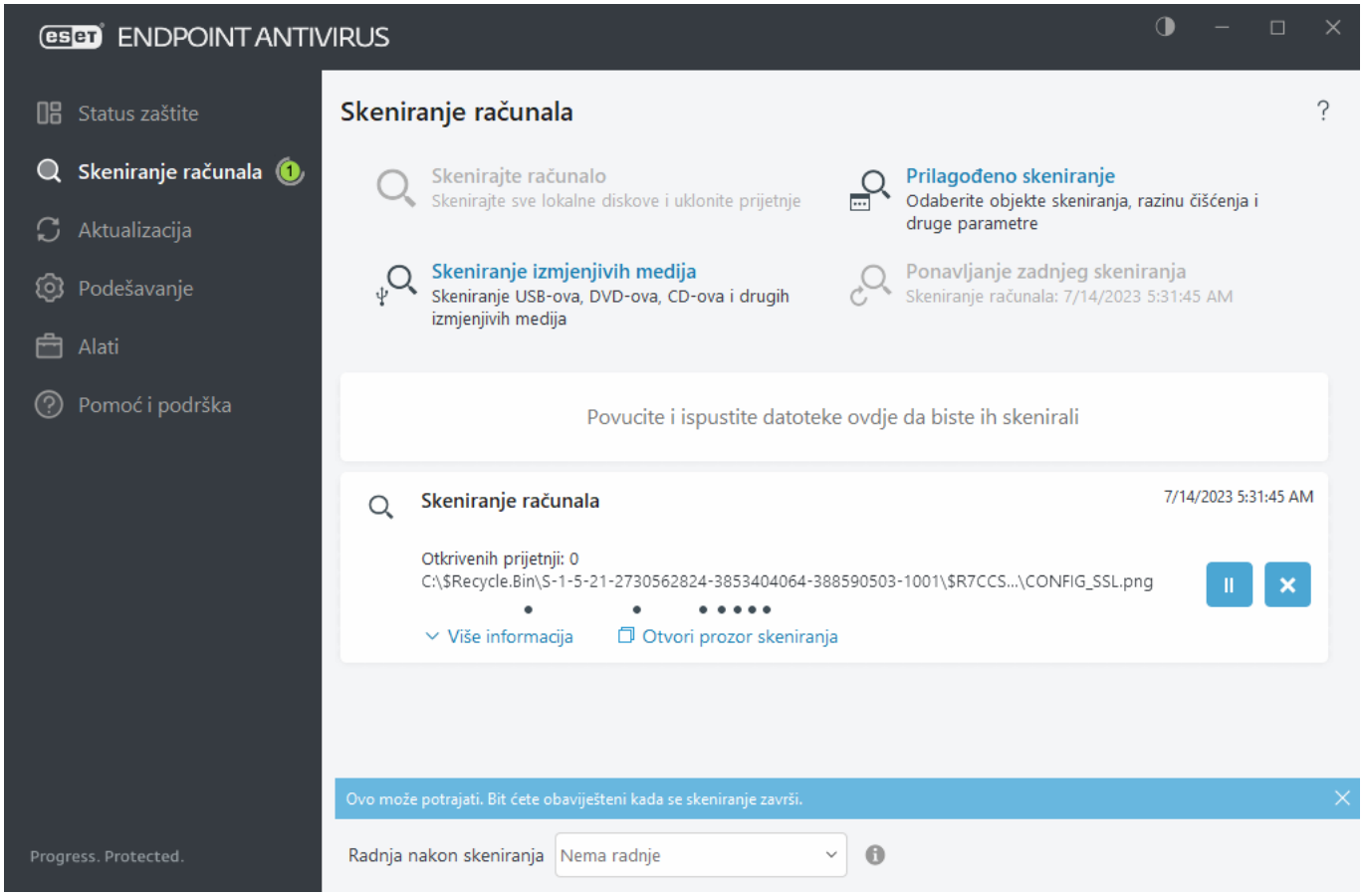
Za poboljšavanje vidljivosti statusa u programima u prvom okviru programa ESET Endpoint Antivirus pogledajte odjeljak Statusi aplikacije.

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

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

Skeniranje računala

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



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

Dodatne informacije o procesu skeniranja potražite u poglavlju Napredak skeniranja.

Skenirajte svoje računalo

Mogućnost „**Skenirajte računalo**" omogućuje brzo pokretanje skeniranja računala i čišćenje zaraženih datoteka bez potrebe za korisničkom intervencijom. Prednost mogućnosti "**Skenirajte svoje računalo**" jest to što je jednostavna za upotrebu i ne zahtijeva detaljnu konfiguraciju skeniranja. To skeniranje provjerava sve datoteke na lokalnim pogonima te automatski briše otkrivene infiltracije. Razina čišćenja automatski se postavlja na standardnu vrijednost. Dodatne informacije o vrstama čišćenja potražite u odjeljku Čišćenje.

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

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

Prilagođeno skeniranje

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

Skeniranje izmjenjivih medija

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

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

Ponavljanje zadnjeg skeniranja

Omogućuje brzo pokretanje prijašnjeg skeniranja upotrebom istih postavki kao i prije.

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

- **Bez radnje** – Kada skeniranje završi, neće se izvršiti nijedna radnja.
- **Isključi** – Kada skeniranje završi, računalo se isključuje.
- **Restartaj po potrebi** – računalo se restarta samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Ponovno pokreni** – Zatvara sve otvorene programe i restarta računalo kada završi skeniranje.
- **Prisilno restartaj po potrebi** – računalo se prisilno restarta samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Prisilno ponovno pokreni** – prisilno zatvara sve otvorene programa bez čekanja interakcije korisnika i ponovno pokreće računalo nakon što se skeniranje dovrši.
- **Spavanje** – Sprema vašu sesiju i stavlja računalo u privremeno stanje u kojem troši malo energije kako biste brzo mogli nastaviti s radom.
- **Hibernacija** – Prebacuje sve što radi na sistemskoj memoriji (RAM) u posebnu datoteku na tvrdom disku. Računalo se isključuje, ali će se prilikom sljedećeg pokretanja vratiti u svoje posljednje stanje prije isključenja.

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

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

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

Pokretač prilagođenog skeniranja

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

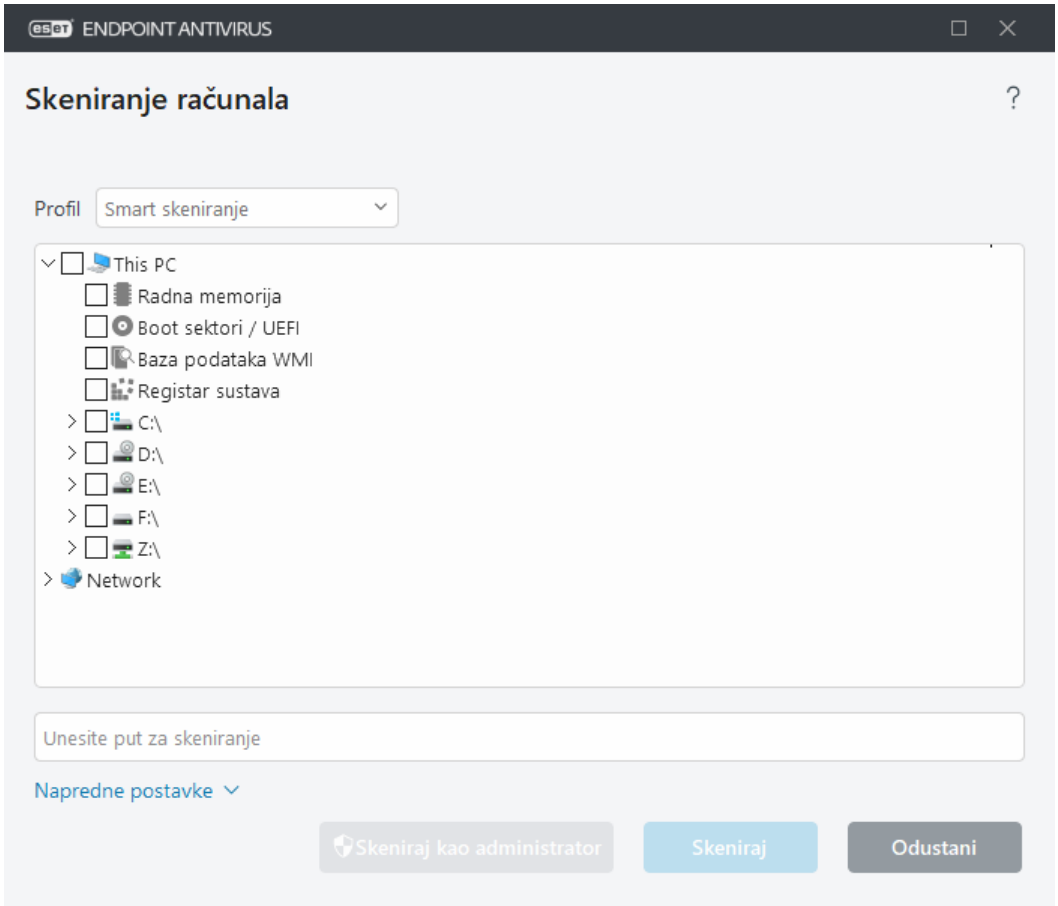
Iz padajućeg izbornika **Profil** možete odabrati profil koji ćete upotrebljavati za skeniranje određenih objekata. Standardni je profil **Smart skeniranje**. Postoje još tri unaprijed definirana profila skeniranja: **Dubinsko skeniranje**, **Skeniranje iz kontekstnog izbornika** i **Skeniranje računala**.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

Struktura mape (stablo) također sadrži specifične ciljeve skeniranja.

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

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

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



Možete konfigurirati parametre čišćenja za skeniranje u stavci Napredno podešavanje > **Modul detekcije** >

Skeniranje zlonamjernog softvera > **Skeniranje na zahtjev** > **ThreatSense** > **Čišćenje**. Da biste pokrenuli skeniranje bez čišćenja, odaberite mogućnost **Napredno podešavanje** > **Skeniranje bez čišćenja**. Povijest skeniranja sprema se u dnevnik skeniranja.

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

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

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

Kada se skeniranje dovrši, možete vidjeti dnevnik skeniranja računala klikom na mogućnost Prikaži dnevnik.

Napredak skeniranja

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

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

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

Tijek skeniranje – traka napretka prikazuje stanje pokrenutog skeniranja.

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

Otkrivene prijetnje – prikazuje ukupan broj skeniranih datoteka, pronađenih prijetnji i prijetnji koje su izbrisane tijekom skeniranja.

Kliknite Dodatne informacije da bi se prikazale sljedeće informacije:

- **Korisnik** – naziv korisničkog računa koji je započeo skeniranje.
- **Skenirani objekti** – broj već skeniranih objekata.
- **Trajanje** – proteklo vrijeme.

Ikona Pauziraj – pauzira skeniranje.

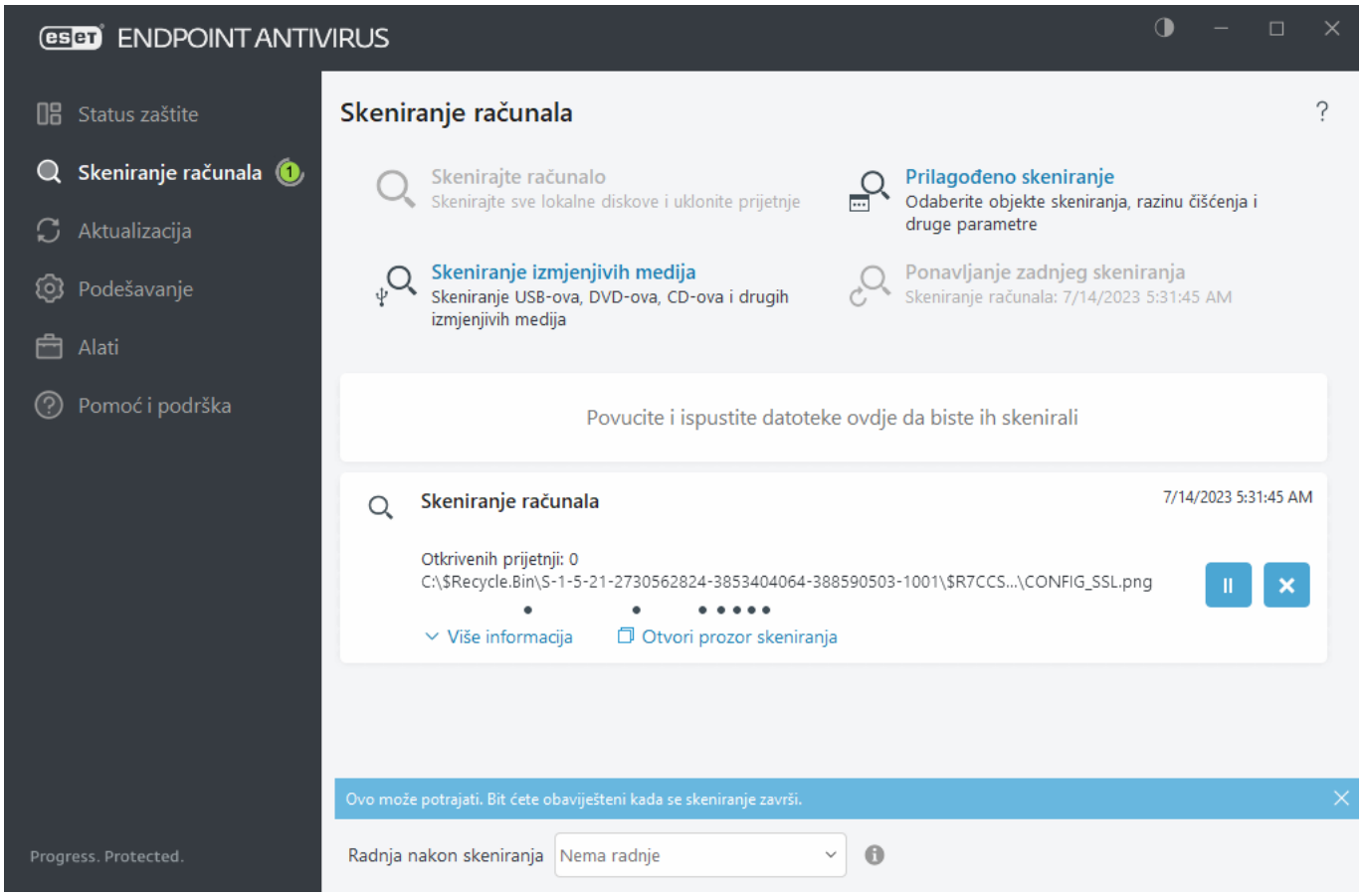
Nastavi – ta je opcija vidljiva kada je napredak skeniranja pauziran. Kliknite ikonu da biste nastavili skeniranje.

Ikona zaustavljanja – prekida skeniranje.

Kliknite **Otvori prozor** skeniranja da biste otvorili Dnevnik skeniranja računala s više detalja o skeniranju.

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

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



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

- **Bez radnje** – Kada skeniranje završi, neće se izvršiti nijedna radnja.
- **Isključi** – Kada skeniranje završi, računalo se isključuje.
- **Restartaj po potrebi** – računalo se restarta samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Ponovno pokreni** – Zatvara sve otvorene programe i restarta računalo kada završi skeniranje.
- **Prisilno restartaj po potrebi** – računalo se prisilno restarta samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Prisilno ponovno pokreni** – prisilno zatvara sve otvorene programa bez čekanja interakcije korisnika i ponovno pokreće računalo nakon što se skeniranje dovrši.
- **Spavanje** – Sprema vašu sesiju i stavlja računalo u privremeno stanje u kojem troši malo energije kako biste brzo mogli nastaviti s radom.
- **Hibernacija** – Prebacuje sve što radi na sistemskoj memoriji (RAM) u posebnu datoteku na tvrdom disku. Računalo se isključuje, ali će se prilikom sljedećeg pokretanja vratiti u svoje posljednje stanje prije isključenja.

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

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

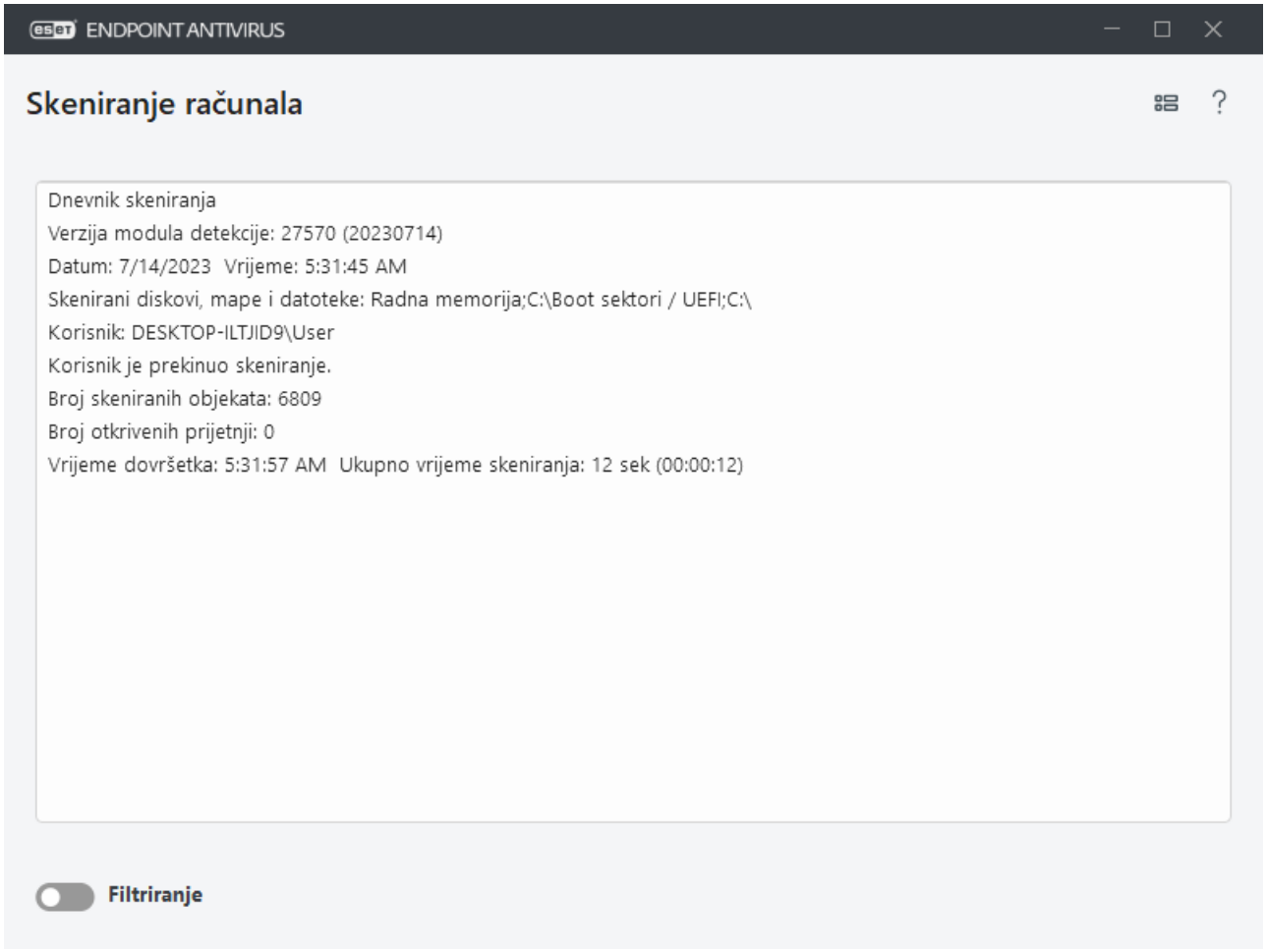
Dnevnik skeniranja računala

Detaljne informacije vezane uz određeno skeniranje možete pogledati u stavci Dnevnici. Dnevnik skeniranja sadrži sljedeće informacije:

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

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

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



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

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

Akcija	Korištenje
Filtriraj iste zapise	Aktivira filtriranje dnevnika. Dnevnik će prikazati samo zapise iste vrste kao što je odabrani.
Filtar	Ova opcija otvara prozor Filtriranje dnevnika i omogućuje vam da definirate kriterije za određene stavke u dnevniku. Prečac: `Ctrl+Shift+F`
Aktiviraj filtar	Aktivira postavke filtra. Ako prvi put aktivirate filtar, morate definirati postavke, nakon čega se otvara prozor Filtriranje dnevnika.
Deaktiviraj filtar	Isključuje filtar (isto kao i klik na prekidač u donjem dijelu).
Kopiraj	Kopira istaknute zapise u međuspremnik. Prečac: `Ctrl+C`
Kopiraj sve	Kopira sve zapise u prozoru.
Izvoz	Izvozi istaknute zapise u međuspremnik, u XML datoteku.
Izvezi sve	Ova opcija izvozi sve zapise u prozoru u XML datoteku.
Opis prijetnje	Otvara enciklopediju prijetnji tvrtke ESET koja sadrži detaljne informacije o opasnostima i simptomima istaknute infiltracije.

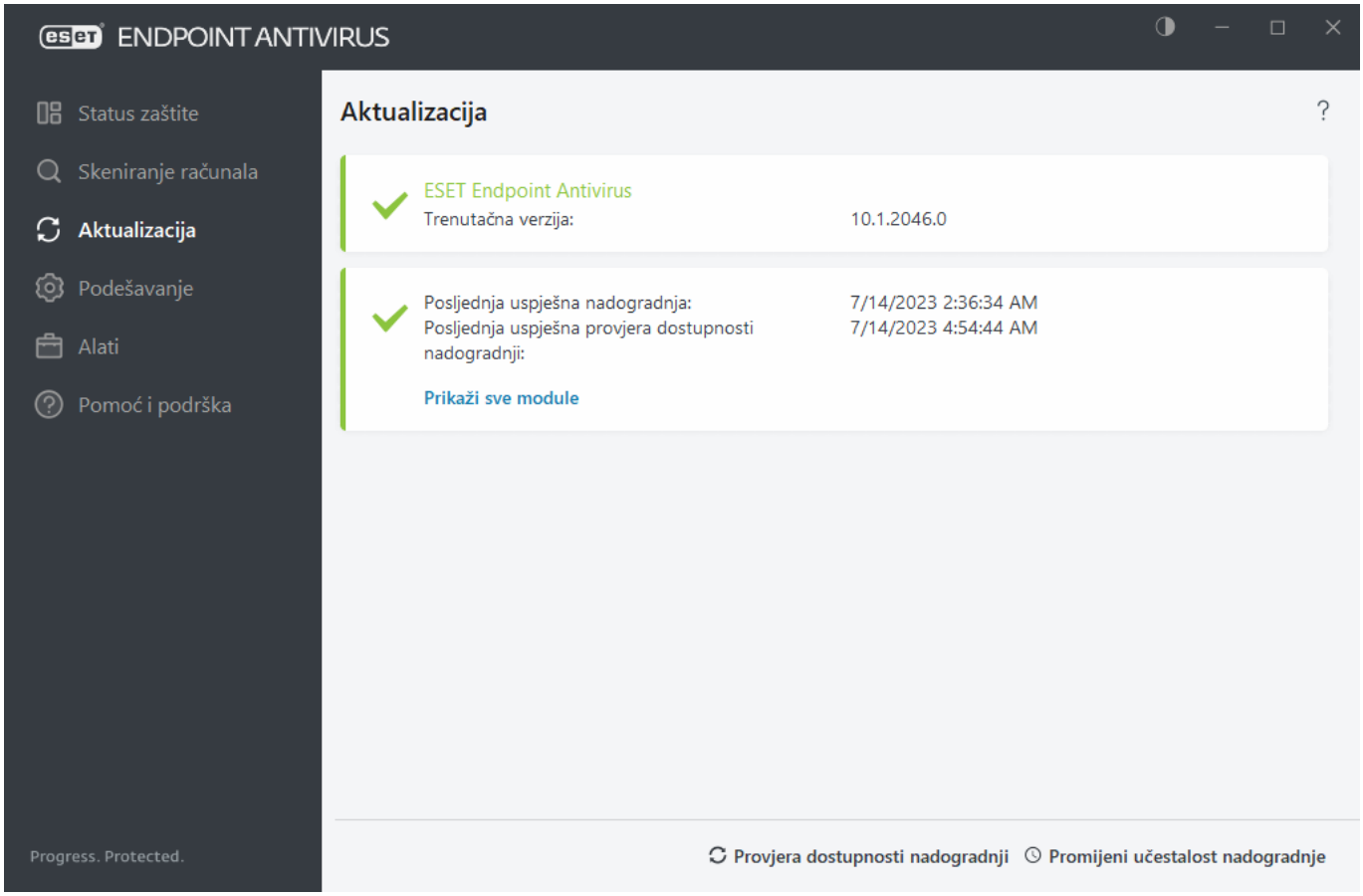
Nadogradnja

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

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

Osim automatskih nadogradnji, možete kliknuti opciju **Potraži nadogradnje** da biste pokrenuli ručnu nadogradnju. Redovite nadogradnje modula programa i komponenata imaju važnu ulogu u održavanju potpune zaštite od zlonamjernog koda. Obratite pozornost na konfiguraciju i rad modula programa. Za primanje nadogradnji morate aktivirati program pomoću licenčnog ključa. Ako to niste učinili tijekom instalacije, trebat ćete aktiviratiESET Endpoint Antivirus da biste pristupili serverima za nadogradnju tvrtke ESET za nadogradnju. Licenčni ključ primili ste e-poštom od tvrtke ESET nakon kupnje programa ESET Endpoint Antivirus.

Ako aktivirate program ESET Endpoint Antivirus pomoću datoteke izvanmrežne licence bez korisničkog imena i lozinke te pokušate izvršiti nadogradnju, crvena informacija **Nadogradnja modula nije uspjela** signalizira da možete preuzeti nadogradnje samo s mirrora.



Trenutačna verzija – Broj verzije programa ESET Endpoint Antivirus.

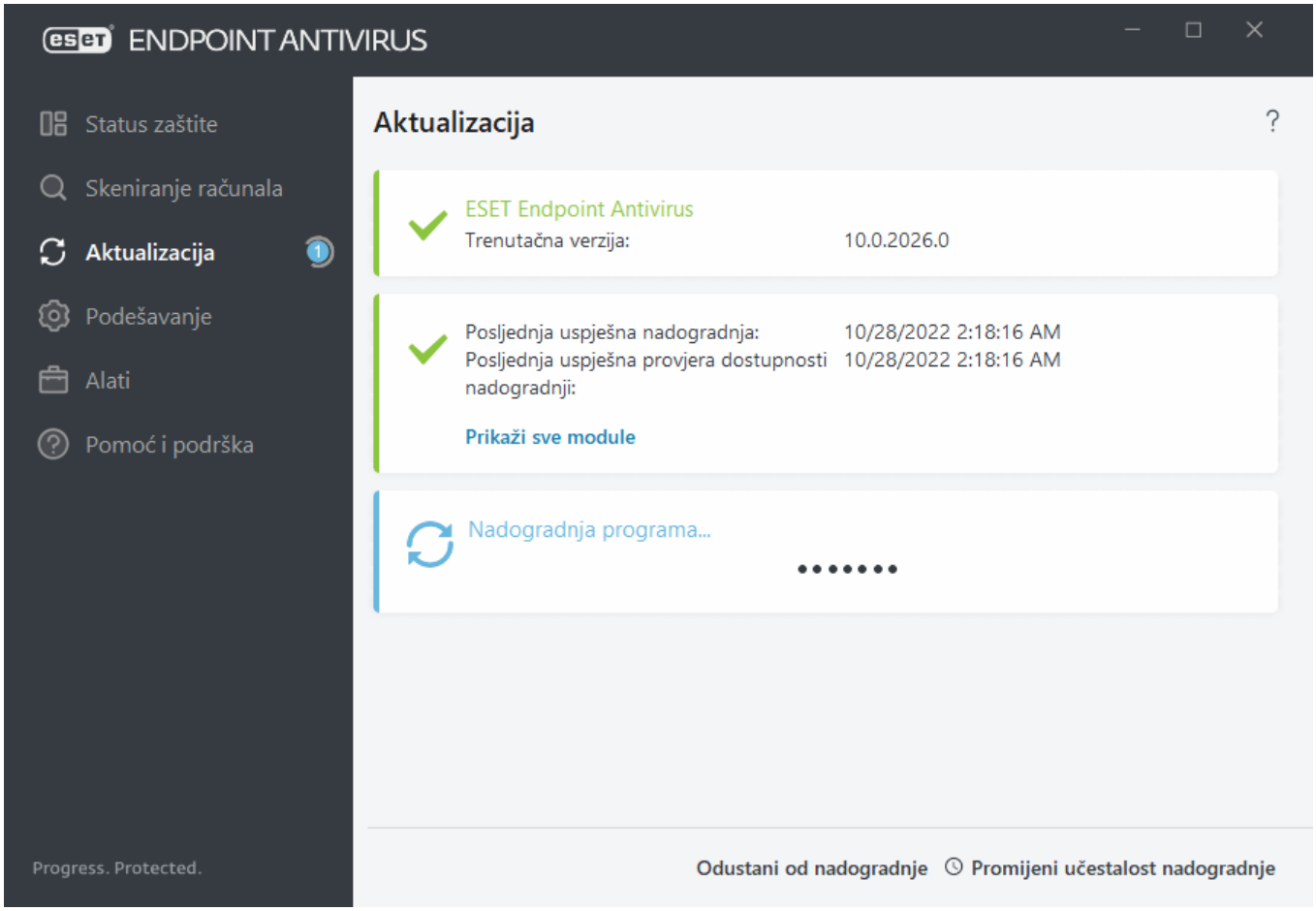
Posljednja uspješna nadogradnja – Datum i vrijeme posljednje uspješne nadogradnje. Pobrinite se da se odnosi na nedavan datum, što znači da modul za otkrivanje virusa nije zastario.

Posljednja uspješna provjera dostupnosti nadogradnji – Datum i vrijeme posljednjeg uspješnog pokušaja nadogradnje modula.

Prikaži sve module – Kliknite link kako biste otvorili popis instaliranih modula i provjerite verziju i posljednju aktualizaciju modula.

Proces aktualizacije

Nakon klika opcije **Potraži aktualizacije** pokreće se postupak preuzimanja. Prikazat će se traka napretka i preostalo vrijeme za preuzimanje. Da biste prekinuli aktualizaciju, kliknite **Odustani od aktualizacije**.



Pod uobičajenim okolnostima možete vidjeti zelenu oznaku potvrde u prozoru **Nadogradnja** koja označava da je program nadograđen. Ako ne vidite zelenu oznaku potvrde, program je zastario i izloženiji zarazama. Nadogradite module programa što prije.

Neuspješna nadogradnja

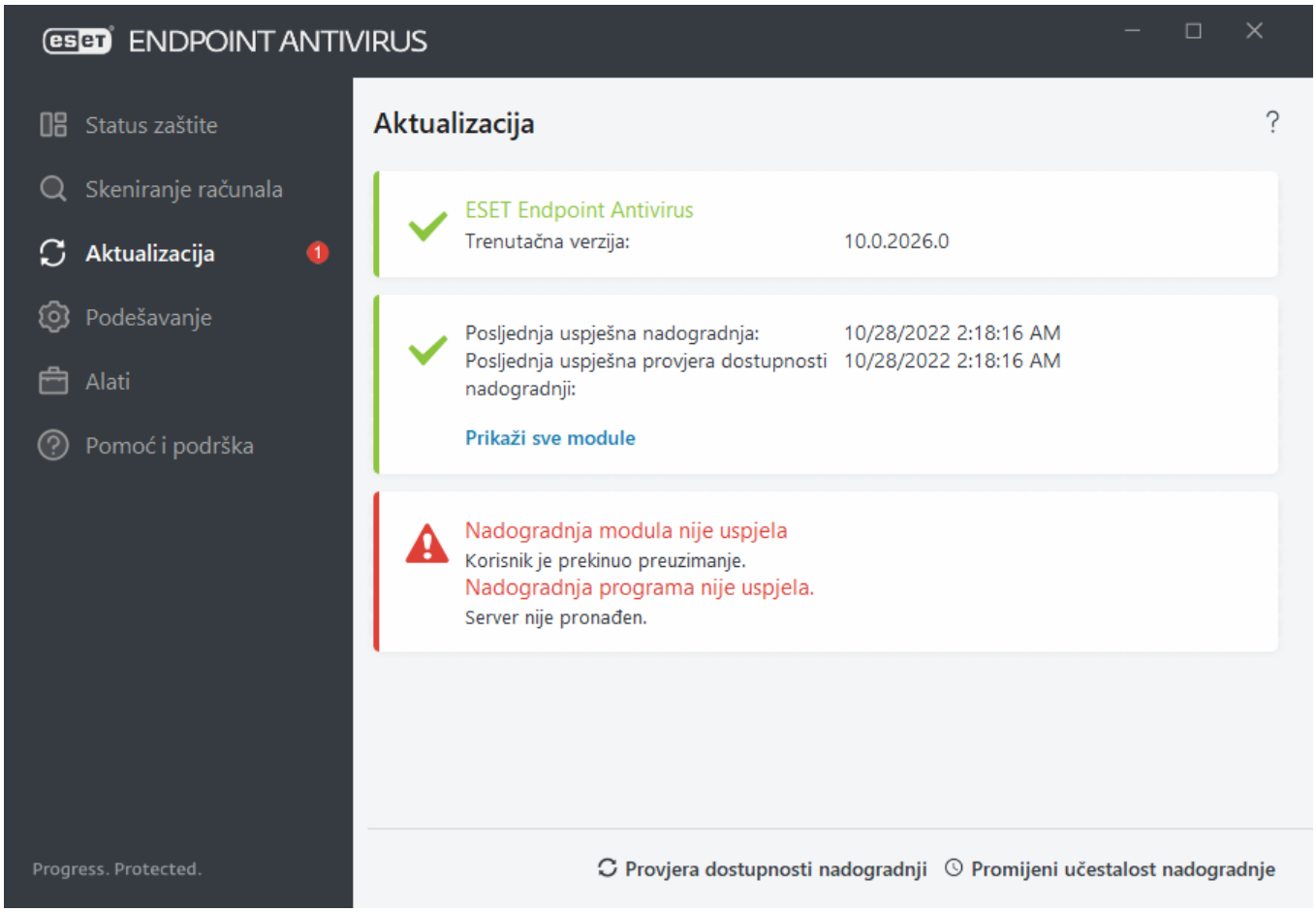
Modul detekcije je zastario – ova pogreška pojavit će se nakon nekoliko neuspješnih pokušaja nadogradnje modula. Preporučujemo da provjerite aktualizacijske postavke. Najčešći je uzrok ove pogreške neispravan unos podataka za autentikaciju ili neispravna konfiguracija postavki povezivanja.

Prethodna obavijest odnosi se na sljedeće dvije poruke **Nadogradnja modula nije uspjela** o neuspješnim nadogradnjama:

1. **Nevaljana licenca** – vaša licenca nije aktivna. Preporučujemo provjeru podataka za autorizaciju. Na

glavnom izborniku kliknite mogućnost **Pomoć i podrška** > **Promijeni licencu** da biste unijeli novi licenčni ključ.

2. **Došlo je do pogreške tijekom preuzimanja datoteka za aktualizaciju** – Mogući uzrok pogreške su Postavke internetske veze. Preporučujemo da provjerite vezu s internetom (primjerice, otvaranjem nekih web stranica u web pregledniku). Ako se web stranica ne otvori, vjerojatno nije uspostavljena internetska veza ili na računalu postoje problemi s povezivošću. Provjerite imate li aktivnu internetsku vezu davatelja internetskih usluga (ISP).



Dodatne informacije pogledajte u članku iz ESET-ove baze znanja.

Stvaranje aktualizacijskih zadataka

Aktualizacije se mogu ručno pokrenuti klikom opcije **Potraži aktualizacije** u primarnom prozoru koji se prikaže nakon što kliknete **Aktualizacija** u glavnom izborniku.

Aktualizacije je moguće pokretati i kao zakazane zadatke. Da biste konfigurirali planirani zadatak, kliknite **Alati** > **Planer**. Prema standardnim se postavkama u programu ESET Endpoint Antivirus aktiviraju sljedeći aktualizacijski zadaci:

- **Redovna automatska aktualizacija**
- **Automatska aktualizacija po prijavi korisnika**

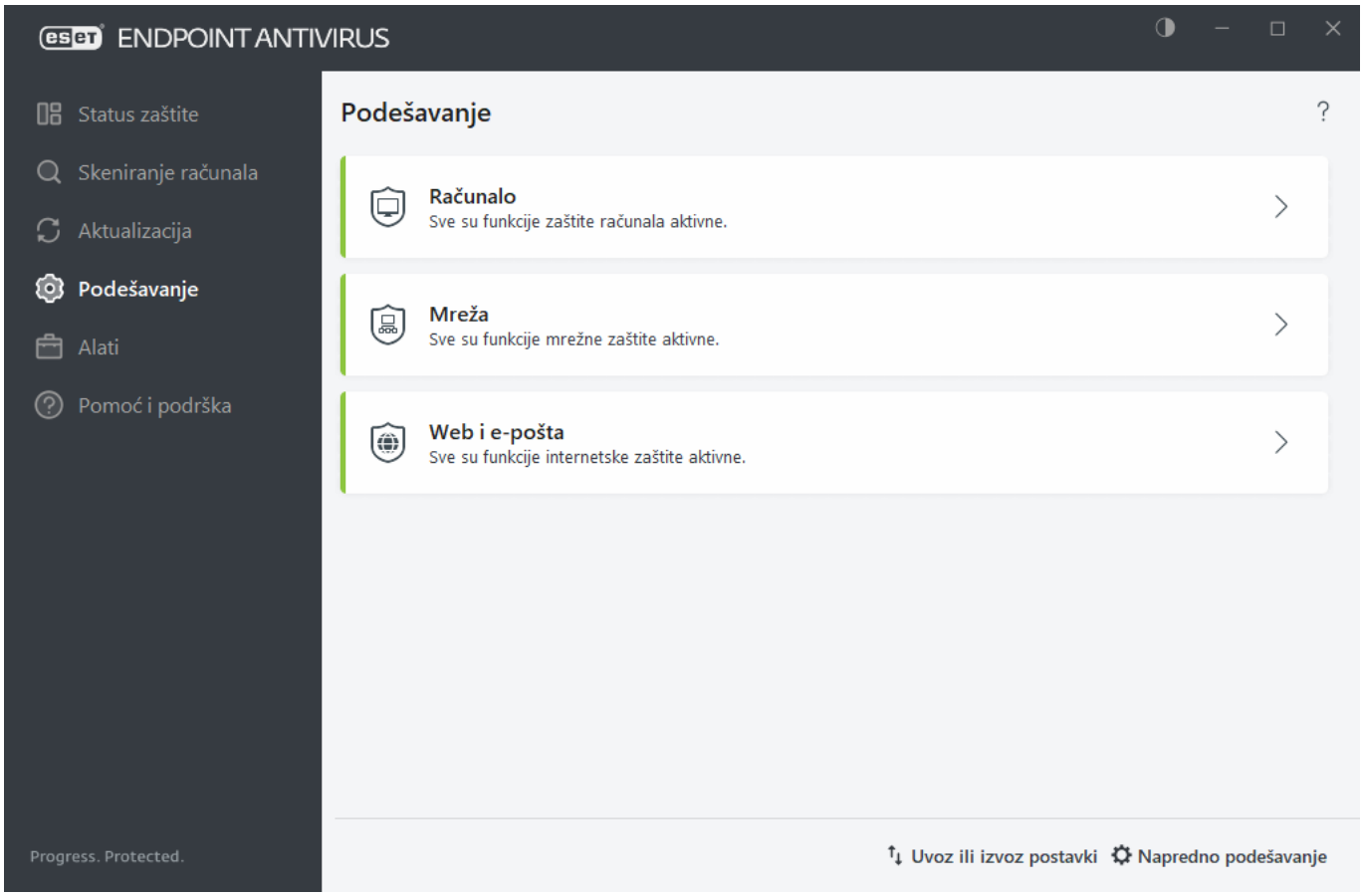
Svaki aktualizacijski zadatak moguće je izmijeniti u skladu s vašim potrebama. Osim standardnih aktualizacijskih zadataka možete stvarati i nove aktualizacijske zadatke s korisnički definiranom konfiguracijom. Detalje o

stvaranju i konfiguriranju zadataka nadogradnje potražite u odjeljku Planer.

Podešavanje

Grupe dostupnih značajki zaštite možete pronaći tako da otvorite prozor glavnog programa > **Podešavanje**.

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



Izbornik **Podešavanje** sadrži sljedeće odjeljke:

Računalo

Mreža

Web i e-pošta

Kada se primijeni ESET PROTECT pravilo, vidjet ćete ikonu za zaključavanje pokraj odgovarajuće komponente. Pravilo koje primijeni ESET PROTECT može lokalno nadjačati prijavljeni korisnik (npr. administrator) nakon autorizacije. Dodatne informacije potražite u mrežnoj pomoći za ESET PROTECT.

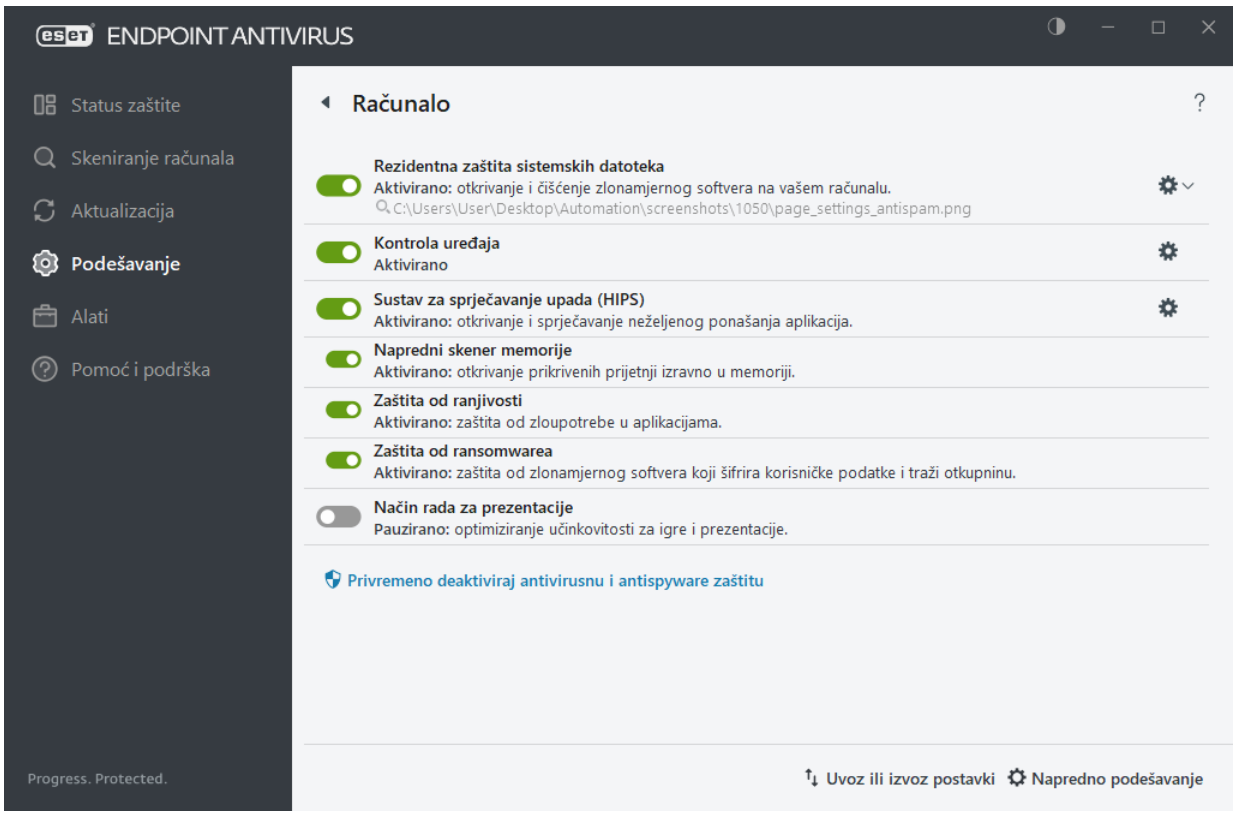
Tako će se sve deaktivirane mjere zaštite ponovno aktivirati nakon restarta računala.

Dodatne mogućnosti dostupne su u dnu prozora podešavanja. Kliknite Napredno postavljanje za konfiguraciju

detaljnijih parametara za svaki modul. Koristite značajku Uvoz ili izvoz postavki da biste učitali parametre podešavanja pomoću konfiguracijske datoteke .xml ili spremili trenutačne parametre podešavanja u konfiguracijsku datoteku.

Računalo

Kliknite **Računalo** u stavci glavni prozor programa > **Podešavanje** da biste vidjeli pregled svih modula zaštite:



U odjeljku **Računalo** možete aktivirati ili deaktivirati sljedeće komponente:

- Rezidentna zaštita – U svim se datotekama skeniranjem provjerava postojanje zlonamjernog koda u trenutku njihova otvaranja, stvaranja ili pokretanja na računalu. Kliknite zupčanik pokraj stavke Rezidentna zaštita sistemskih datoteka i kliknite Uredi izuzetke da biste otvorili prozor Podešavanje izuzetaka koji vam omogućuje da izuzmete datoteke i mape od skeniranja. Da biste otvorili napredno podešavanje Rezidentne zaštite sistemskih datoteka, kliknite Konfiguriraj.
- Kontrola uređaja – Omogućuje automatsku kontrolu uređaja (CD/DVD/USB/...). Taj modul omogućuje blokiranje ili prilagođavanje dodatnih filtara/ovlaštenja i odabir načina na koji korisnik pristupa određenom uređaju i radi s njim.
- Sustav za sprečavanje upada (HIPS) – Sustav HIPS nadzire događaje koji se događaju unutar operacijskog sustava i reagira na njih u skladu s prilagođenim skupom pravila.
- **Napredni skener memorije** – radi zajedno sa zaštitom od zloupotrebe na ojačavanju zaštite od zlonamjernog softvera koji je osmišljen tako da skrivanjem i/ili šifriranjem izbjegava da ga otkriju proizvodi za zaštitu od zlonamjernog softvera. Prema standardnim postavkama napredni je skener memorije aktiviran. Više o toj vrsti zaštite pročitajte u rječniku.
- **Zaštita od zloupotrebe** – Osmišljena je za ojačavanje zaštite često zloupotrebljavanih vrsta aplikacija kao što su web preglednici, PDF čitači, klijenti e-pošte i komponente sustava MS Office. Sprječavanje ranjivosti aktivirano je prema standardnim postavkama. Više o toj vrsti zaštite pročitajte u rječniku.
- **Zaštita od ransomwarea**– dodatan sloj zaštite koji djeluje kao dio funkcije HIPS. Reputacijski sustav ESET LiveGrid® mora biti aktiviran da bi zaštita od ransomwarea djelovala. Više o toj vrsti zaštite pročitajte.

- Način rada za prezentacije – funkcija za korisnike koji softver žele koristiti bez prekida, ne žele da ih ometaju obavijesti i žele smanjiti korištenje CPU-a. Nakon aktivacije Načina rada za prezentacije primit ćete poruku upozorenja (mogući sigurnosni rizik) i glavni će prozor postati narančast.

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

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

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

Otkrivena je prijetnja

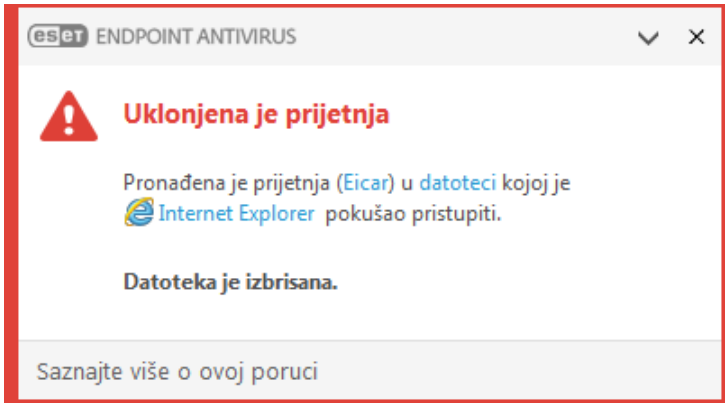
Infiltracije mogu doći do sustava iz raznih izvora: s web stranica, iz zajednički korištenih mapa, putem e-pošte ili s izmjenjivih uređaja (USB-ova, vanjskih diskova, CD-ova, DVD-ova, itd.).

Standardno ponašanje

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

- rezidentna zaštita
- zaštita web pristupa
- zaštita klijenta e-pošte
- Skeniranje računala na zahtjev

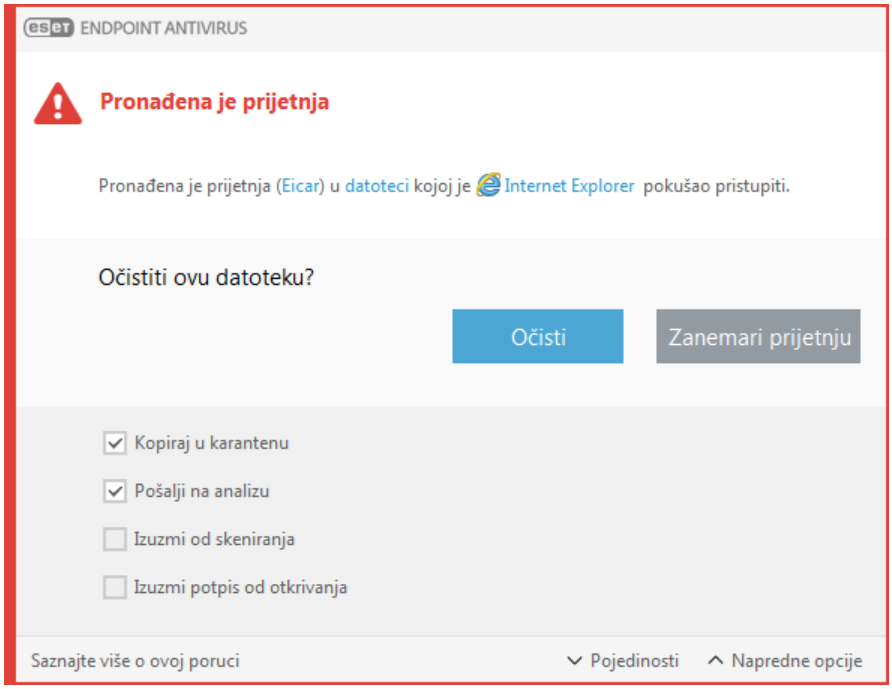
Svaka funkcija koristi standardnu razinu čišćenja i pokušat će očistiti datoteku i premjestiti je u karantenu ili prekinuti vezu. U području obavijesti u donjem desnom kutu zaslona prikazuje se prozor obavijesti. Detaljne informacije o otkrivenim/izbrisanim objektima potražite u opciji Dnevnici. Dodatne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



Čišćenje i brisanje

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

Iznimka su jedino datoteke za koje ste sigurni da su bezopasne i da su otkrivene pogreškom.



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

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

Vraćanje iz karantene

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

Datoteke u karanteni također se mogu vratiti na izvornu lokaciju:

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

Višestruke prijetnje

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

Brisanje datoteka u arhivama

U standardnom načinu čišćenja cijela se arhiva briše samo ako su sve datoteke u toj arhivi zaražene. Drugim

riječima, arhive se ne brišu ako sadrže i bezopasne čiste datoteke. Budite oprezni prilikom skeniranja potpunim čišćenjem – potpuno čišćenje briše svaku arhivu koja sadrži najmanje jednu zaraženu datoteku, bez obzira na status ostalih datoteka u arhivi.

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

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

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

Mreža

Otvorite prozor glavnog programa > **Podešavanje** > **Mreža** da biste konfigurirali osnovne postavke mrežne zaštite ili otklonili probleme s mrežnom komunikacijom.

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

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

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

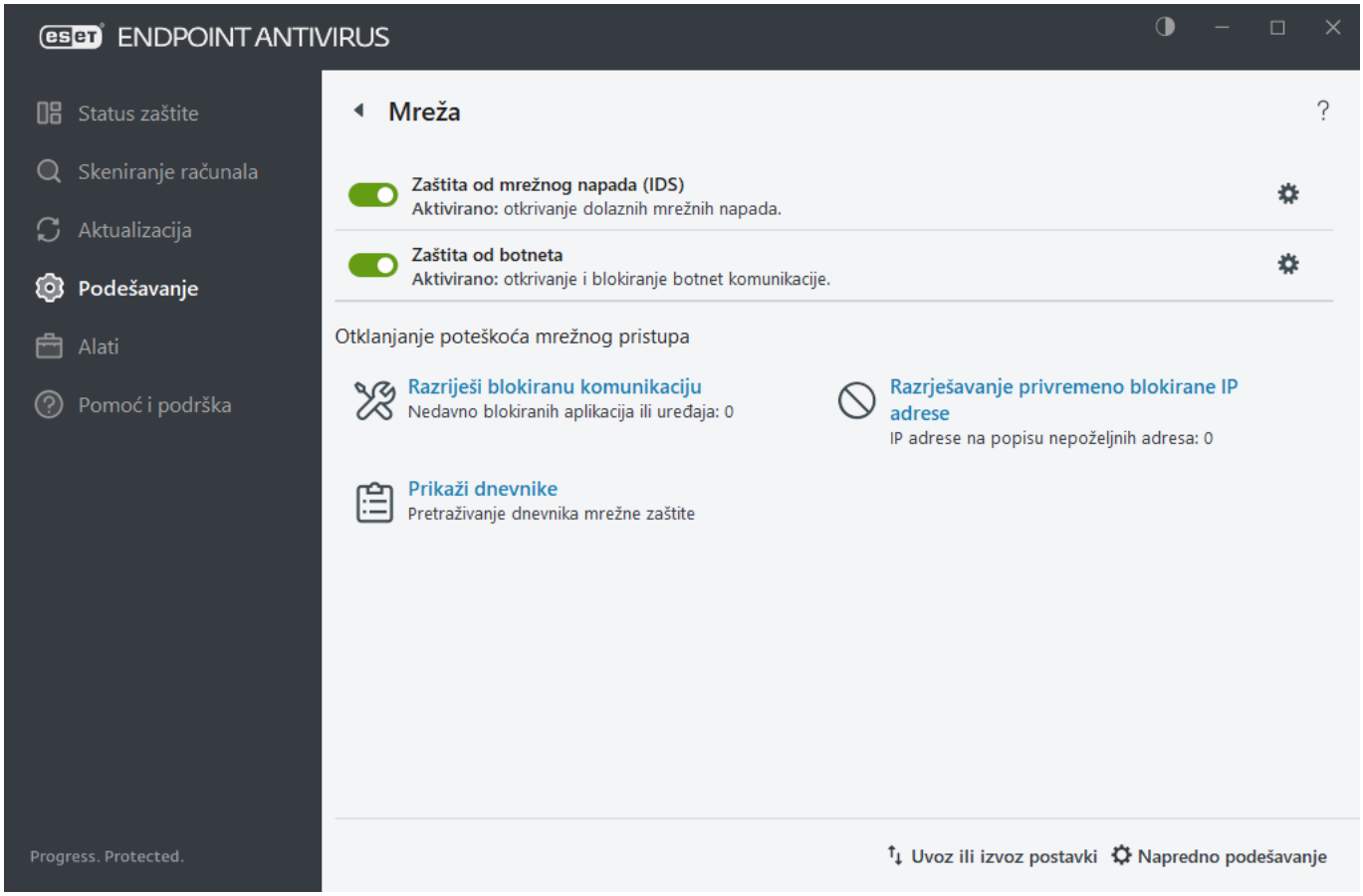
Zaštita od mrežnog napada (IDS) – Analizira sadržaj mrežnog prometa i štiti od mrežnih napada. Svaki promet koji se smatra štetnim je blokiran. ESET Endpoint Antivirus Obavještava vas kada se povežete s nezaštićenom bežičnom mrežom ili s mrežom sa slabom zaštitom.

Zaštita od botneta – brzo i točno identificira zlonamjerni softver u sustavu.

Razriješi blokiranu komunikaciju – pomaže u rješavanju problema s povezivanjem uzrokovanih ESET firewallom. Detaljnije informacije potražite u Čarobnjaku za otklanjanje poteškoća.

Razrješavanje privremeno blokiranih IP adresa – prikazuje popis IP adresa koje su prepoznate kao izvori napada te su dodane na popis blokiranih adresa radi sprečavanja povezivanja na određeno razdoblje

Prikaži dnevnike – otvara dnevnik mrežne zaštite.



Otklanjanje poteškoća s mrežnim pristupom

Čarobnjak za otklanjanje poteškoća pomaže vam riješiti probleme s povezivanjem koje je uzrokovao firewall. **Otklanjanje poteškoća s mrežnim pristupom** možete pronaći na glavnom programskom prozoru > **Podešavanje** > **Mreža** > **Razriješi blokiranu komunikaciju**.

Odaberite želite li prikazati blokiranu komunikaciju za **Lokalne aplikacije** ili blokiranu komunikaciju stavke **Udaljeni uređaji**.

Na padajućem izborniku odaberite vremensko razdoblje tijekom kojeg je komunikacija bila blokirana. Popis nedavno blokiranih komunikacija daje vam uvid u vrstu aplikacije ili uređaja te u reputaciju i ukupan broj aplikacija i uređaja blokiranih tijekom tog razdoblja. Za dodatne informacije o blokiranoj komunikaciji kliknite stavku **Detalji**. U sljedećem koraku trebate deblokirati aplikaciju ili uređaj s kojim imate teškoće u povezivanju.

Kada kliknete **Deblokiraj**, komunkacija koja je bila blokirana sada će biti dopuštena. Ako i dalje imate poteškoća s aplikacijom ili vaš uređaj ne radi u skladu s očekivanjima, kliknite **stvaranje drugog pravila**, pa će sve prethodno blokirane komunikacije za taj uređaj sada biti dopuštene. Ako problem i dalje postoji, ponovno pokrenite računalo.

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
- Dodavanje iznimke pomoću čarobnjaka za otklanjanje poteškoća

Ako se pravilo ne može stvoriti, primit ćete poruku o pogrešci. Kliknite **Pokušaj ponovno** i ponovite postupak da biste deblokirali komunikaciju ili stvorite drugo pravilo s popisa blokirane komunikacije.

Popis privremeno blokiranih IP adresa

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

Stupci

IP adresa – Prikazuje IP adresu koja je blokirana.

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

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

Kontrolni elementi

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

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

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

Dnevnici mrežne zaštite

Mrežna zaštita programa ESET Endpoint Antivirus sprema sve važne događaje u dnevnik. Da biste pogledali dnevnik, otvorite prozor glavnog programa > **Podešavanje** > **Mreža** > **Prikaži dnevnike**.

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

- Datum i vrijeme događaja
- Naziv događaja
- Izvor
- Ciljna mrežna adresa
- Protokol mrežne komunikacije
- Primijenjeno pravilo ili naziv crva, ako je otkriven
- Put i naziv aplikacije
- Hash
- Korisnik
- Potpisnik aplikacije (izdavač)
- Naziv paketa
- Naziv usluge

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

Iskorištavanje sigurnosnog propusta

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

Rješavanje problema s ESET-ovom mrežnom zaštitom

Ako doživite probleme s povezivanjem s instaliranim programom ESET Endpoint Antivirus, postoji nekoliko načina za otkrivanje uzrokuje li ESET Mrežna zaštita problem. Nadalje, ESET Mrežna zaštita može vam pomoći u stvaranju novih pravila ili izuzetaka za rješavanje problema u povezivanju.

Pogledajte sljedeće teme za pomoć u rješavanju problema s ESET Mrežna zaštita:

- Otklanjanje poteškoća s mrežnim pristupom
- Zapisivanje i stvaranje pravila ili izuzetaka iz dnevnika
- Napredno vođenje dnevnika Mrežne zaštite
- Rješavanje problema sa skenerom mrežnog prometa

Zapisivanje i stvaranje pravila ili izuzetaka iz dnevnika

Prema standardnim postavkama ESET Firewall ne zapisuje sve blokirane veze u dnevnik. Ako želite vidjeti što je blokirala Mrežna zaštita, otvorite Napredno podešavanje > **Alati** > **Dijagnostika** > **Napredno vođenje dnevnika** i aktivirajte opciju **Aktiviraj napredno vođenje dnevnika mrežne zaštite**. Ako u dnevniku vidite nešto što ne želite da firewall blokira, možete stvoriti pravilo ili IDS pravilo desnim klikom te stavke i odabirom opcije **Ubuduće ne blokiraj slične događaje**. Imajte na umu da dnevnik svih blokiranih veza može sadržavati tisuće stavki te može biti teško pronaći određenu vezu u tom dnevniku. Vođenje dnevnika možete isključiti nakon što otklonite problem.

Dodatne informacije o dnevniku potražite u stavci Dnevnici.

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

Stvori pravilo iz dnevnika

Nova verzija programa ESET Endpoint Antivirus omogućuje vam stvaranje pravila iz dnevnika. Na glavnom izborniku kliknite **Alati** > **Dnevnici**. Odaberite **Mrežna zaštita** iz padajućeg izbornika, kliknite željeni unos u dnevniku desnom tipkom i odaberite **Ubuduće ne blokiraj slične događaje** iz kontekstnog izbornika. Prozor s obavijestima prikazat će vaše novo pravilo.

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

1. Postavite minimalnu opširnost zapisivanja na **Dijagnostičko** u Naprednom podešavanju > **Alati** > **Dnevnici**.
2. Aktivirajte opciju **Obavijesti me o dolaznim prijetnjama za sigurnosne propuste** u stavci Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** > **Zaštita od mrežnog napada (IDS)** > **Napredne opcije** > **Otkrivanje upada**.

Napredno vođenje dnevnika Mrežne zaštite

Ova funkcija namijenjena je za pružanje složenijih dnevnika za ESET-ovu tehničku podršku. Upotrebljavajte ovu funkciju samo kada od vas to zatraži ESET-ova tehnička podrška jer bi se mogao stvoriti velik dnevnik i usporiti rad vašeg računala.

1. Idite na Napredno podešavanje > **Alati** > **Dijagnostika** i aktivirajte **Aktiviraj napredno vođenje dnevnika mrežne zaštite**.
2. Pokušajte ponoviti problem koji ste imali.
3. Deaktivirajte napredno vođenje dnevnika mrežne zaštite.
4. Dnevnik PCAP zapisivanja koji je izrađen u okviru naprednog vođenja dnevnika mrežne zaštite može se pronaći u istoj mapi gdje se stvaraju dijagnostičke slike stanja memorije: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Rješavanje problema sa skenerom mrežnog prometa

Ako imate problema s preglednikom ili klijentom e-pošte, prvi korak je provjeriti je li za to zaslužan skener mrežnog prometa. Da biste to učinili, pokušajte privremeno deaktivirati Skener mrežnog prometa u stavci Napredno podešavanje > **Modul detekcije** > **Skener mrežnog prometa** (sjetite se ponovno ga uključiti kada završite jer će u protivnom vaš preglednik i klijent e-pošte ostati nezaštićeni). Ako vaš problem nestane nakon isključivanja, ovdje je popis najčešćih problema i kako ih otkloniti:

Problemi s aktualizacijom ili sigurnosnom komunikacijom

Ako vaša aplikacija prigovara o nemogućnosti nadogradnja ili nezaštićenosti komunikacijskog kanala:

- Ako imate aktivirano filtriranje SSL protokolaSSL/TLS, pokušajte ga privremeno isključiti. Ako to pomaže, možete nastaviti koristiti SSL/TLS i obaviti aktualizaciju izuzimanjem problematične komunikacije: Deaktiviraj SSL/TLS Ponovno pokrenite aktualizaciju. Trebao bi se pojaviti dijaloški okvir koji vas informira o šifriranom mrežnom prometu. Provjerite odgovara li aplikacija onoj kojoj pokušavate otkloniti poteškoće i izgleda li certifikat kao da dolazi sa servera na kojem se izvršava aktualizacija. Zatim odaberite da se pamti akcija za ovaj certifikat i kliknite ignoriraj. Ako se ne prikazuje više važnih dijaloških okvira, možete prebaciti način filtriranja natrag na automatski i problem bi trebao biti otklonjen.
- Ako dotična aplikacija nije preglednik ni klijent e-pošte, možete je potpuno izuzeti iz stavke Zaštita web pristupa (da učinite ovako što za preglednik ili klijent e-pošte, bili biste izloženi riziku). Sve aplikacije čija se komunikacija filtrirala u prošlosti trebale bi već biti ponuđene u popisu kada dodajete izuzetke, tako da ručno dodavanje ne bi trebalo biti potrebno.

Problem u pristupanju uređaju na vašoj mreži

Ako ne možete upotrebljavati funkcionalnost uređaja na mreži (ovo može biti web stranica ili reprodukcija videozapisa na multimedijskom reproduktoru), pokušajte dodati njegove IPv4 i IPv6 adrese na popis izuzetih adresa.

Problemi s određenom web stranicom

Možete izuzeti određene web stranice iz stavke Zaštita web pristupa pomoću upravljanja URL adresama. Primjerice, ako ne možete pristupiti https://www.gmail.com/intl/en/mail/help/about.html, pokušajte dodati

gmail.com na popis izuzetih adresa.

Pogreška „Još uvijek rade neke aplikacije koje mogu uvesti root certifikat”

Kada aktivirate SSL/TLS, ESET Endpoint Antivirus provjerava vjeruju li instalirane aplikacije načinu kako se filtrira SSL protokol uvozom certifikata u njihovo spremište certifikata. Neke aplikacije mogu zahtijevati restart za uvoz certifikata. To uključuje aplikacije Firefox i Opera. Provjerite jesu li sve isključene (najbolji je način da otvorite upravitelj zadataka i provjerite da na kartici procesa ne postoje aktivni procesi firefox.exe ili opera.exe), a zatim pokušajte ponovno.

Pogreška o nepouzdanom izdavaču ili neispravnom potpisu

Ovo vjerojatno znači da je gore opisani uvoz bio neuspješan. Prvo provjerite da gore navedene aplikacije nisu aktivne. Zatim deaktivirajte SSL/TLS pa ga ponovno aktivirajte. To će ponovno pokrenuti uvoz.

Blokirana je mrežna prijetnja

Do ove situacije može doći kada neka aplikacija na vašem računalu pokušava prenijeti zlonamjerni promet drugome uređaju na mreži iskorištavajući sigurnosnu rupu ili čak ako se otkrije pokušaj skeniranja portova u vašem sustavu.

Vrstu prijetnje i IP adresu povezanog uređaja možete pronaći u obavijesti. Kliknite **Promijeni postupanje s ovom prijetnjom** da bi se prikazale sljedeće opcije:

Nastavi blokirati – Blokira otkrivenu prijetnju. Ako želite prestati primati obavijesti o ovoj vrsti prijetnje s određene udaljene adrese, odaberite izborni gumb pokraj opcije **Nemoj obavijestiti** prije nego što kliknete **Nastavi blokirati**. Time će se stvoriti pravilo za uslugu otkrivanja upada (IDS) sa sljedećom konfiguracijom: **Blokiraj** – standardno, **Obavijesti** – ne, **Zapiši u dnevnik** – ne.

Dopusti – stvara pravilo za uslugu otkrivanja upada (IDS) da bi se dopustila otkrivena prijetnja. Odaberite jednu od sljedećih opcija prije nego što kliknete **Dopusti** da biste odredili postavke pravila:

- **Obavijesti samo kada je ova prijetnja blokirana** – konfiguracija pravila: **Blokiraj** – ne, **Obavijesti** – ne, **Zapiši u dnevnik** – ne.
- **Obavijesti kad god se ova prijetnja pojavi** – konfiguracija pravila: **Blokiraj** – ne, **Obavijesti** – standardno, **Zapiši u dnevnik** – standardno.
- **Nemoj obavijestiti** – konfiguracija pravila: **Blokiraj** – ne, **Obavijesti** – ne, **Zapiši u dnevnik** – ne.

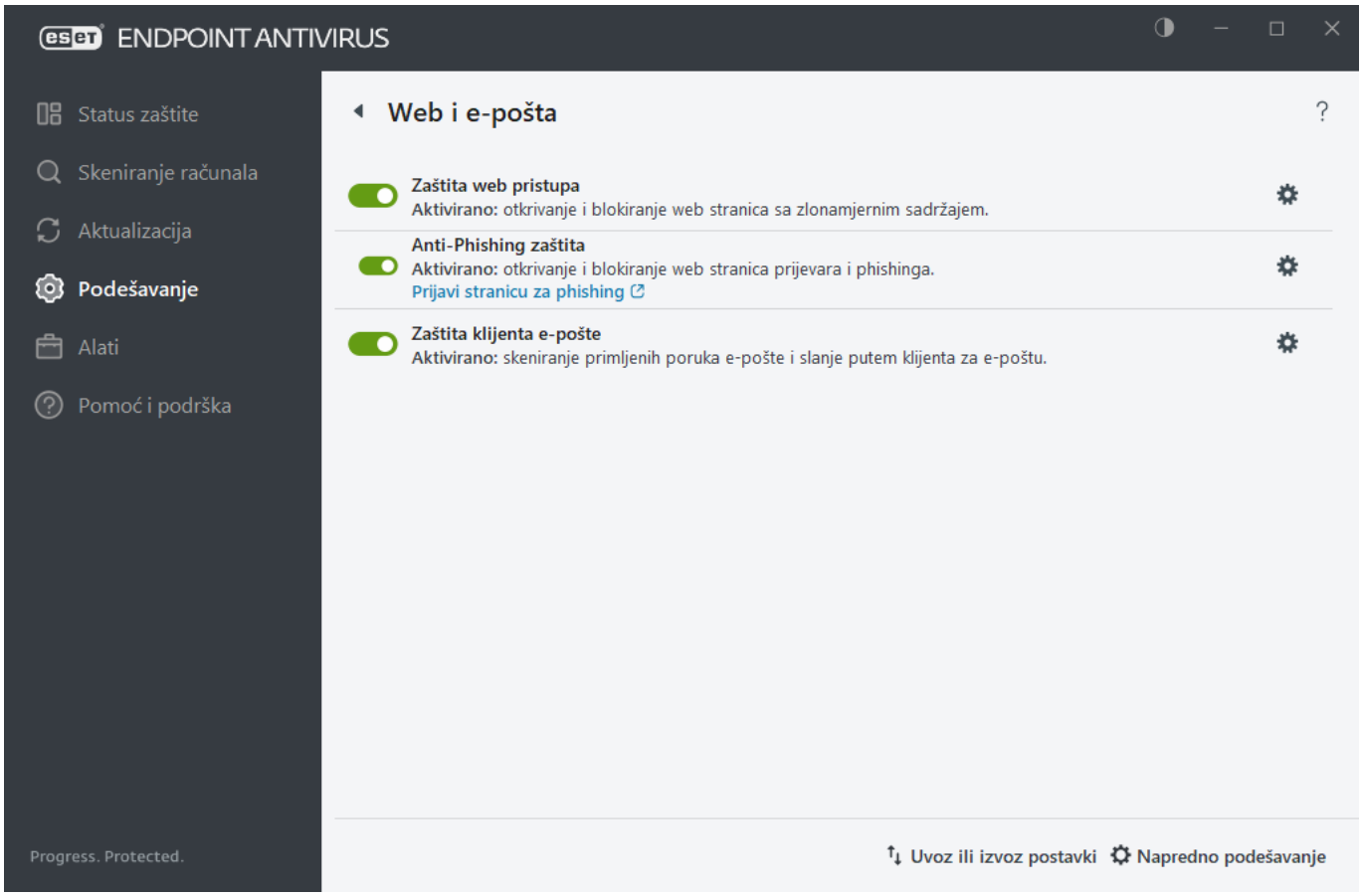
Informacije prikazane u prozoru obavijesti mogu se razlikovati ovisno o vrsti otkrivene prijetnje.
Više informacija o prijetnjama i drugim povezanim pojmovima potražite u odjeljku Vrste udaljenih napada ili Vrste otkrivenih prijetnji.
Da biste riješili **duplikate IP adresa na mreži**, pogledajte članak iz ESET-ove baza znanja.

Web i e-pošta

Internetska veza je standardna funkcija na osobnom računalu, ali i glavni medij za prijenos zlonamjernog koda. Otvorite glavni prozor programa > **Podešavanje** > **Web i Web i e-pošta** da biste konfigurirali funkcije programa ESET Endpoint Antivirus koje povećavaju internetsku zaštitu.

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

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



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

Zaštita web pristupa skenira HTTP/HTTPS komunikaciju za zlonamjerni softver i phishing. Zaštita web pristupa trebala bi biti isključena samo prilikom otklanjanja poteškoća.

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

Prijavi stranicu za phishing – prijavite web-stranicu tvrtki ESET kao stranicu za phishing ili zlonamjernu stranicu radi daljnje analize.

Prije slanja web stranice u ESET provjerite je li zadovoljen neki od sljedećih kriterija:
- Web stranica uopće nije otkrivena.
- Web stranica je neispravno otkrivena kao prijetnja. U tom slučaju možete prijaviti pogrešno blokiranu stranicu.

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

Anti-Phishing zaštita

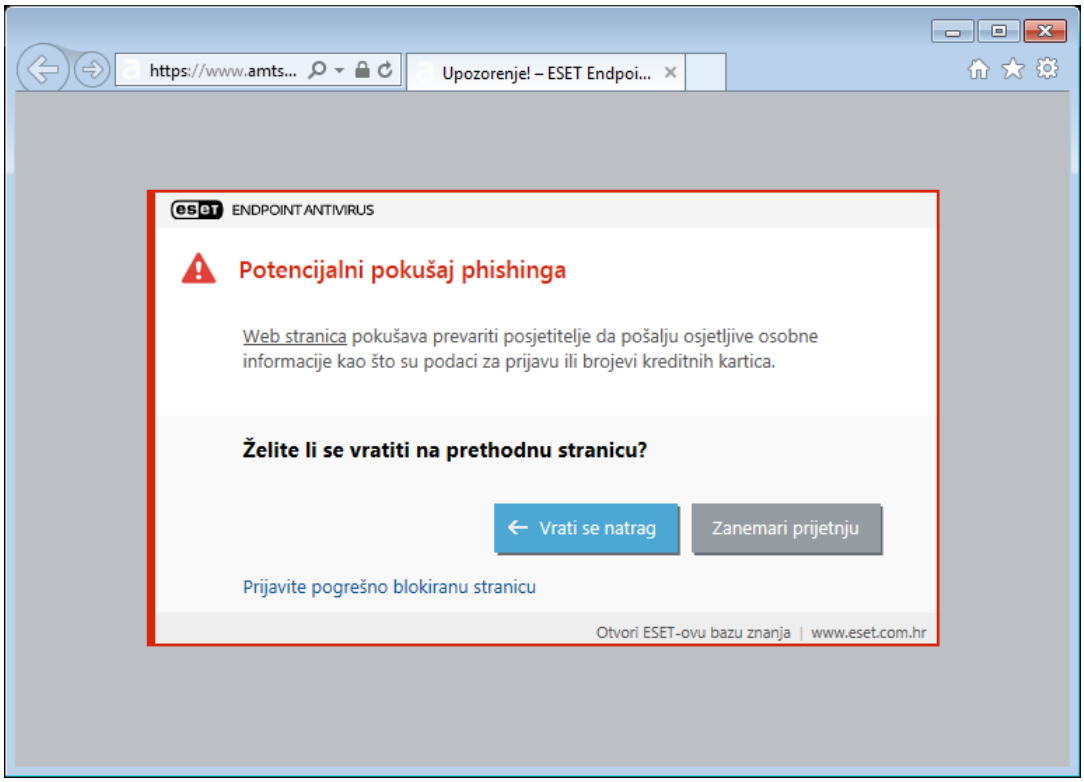
Phishing je protuzakonita aktivnost koja se temelji na društvenom inženjeringu (manipuliranju korisnicima radi dobivanja povjerljivih informacija). Phishing se koristi za pristup osjetljivim podacima kao što su brojevi bankovnih računa, PIN-ovi itd. Više informacija potražite u rječniku. ESET Endpoint Antivirus podržava anti-phishing zaštitu, pa je moguća blokada web stranica za koje se zna da distribuiraju takvu vrstu sadržaja.

Anti-Phishing zaštita je aktivirana prema standardnim postavkama. Ta se postavka može konfigurirati u opciji Napredno podešavanje > **Zaštite** > **Zaštita web pristupa**

Pogledajte članak u našoj bazi znanja kako biste saznali više o antiphishing zaštiti u programu ESET Endpoint Antivirus.

Pristupanje web stranici za phishing

Kada pristupite poznatoj web stranici za phishing, vaš će web preglednik prikazati sljedeći dijaloški okvir. Ako i dalje želite pristupiti toj web stranici, kliknite **Zanemari prijetnju** (ne preporučuje se).



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

Prijavi stranicu za phishing

Veza **Prijavi neispravno blokiranu stranicu** omogućuje vam prijavu web-stranice koja je pogrešno prepoznata kao prijetnja.

Web stranicu možete poslati i e-poštom. Pošaljite poruku e-pošte na adresu samples@eset.com. Napominjemo

da predmet poruke mora sadržavati opis, a sama poruka što više informacija o web stranici (primjerice, informacije o web stranici preko koje ste došli do nje, kako ste čuli za tu web stranicu itd.).

Uvoz i izvoz postavki

Možete uvesti ili izvesti svoju prilagođenu ESET Endpoint Antivirus .xml konfiguracijsku datoteku na izborniku **Podešavanje**.

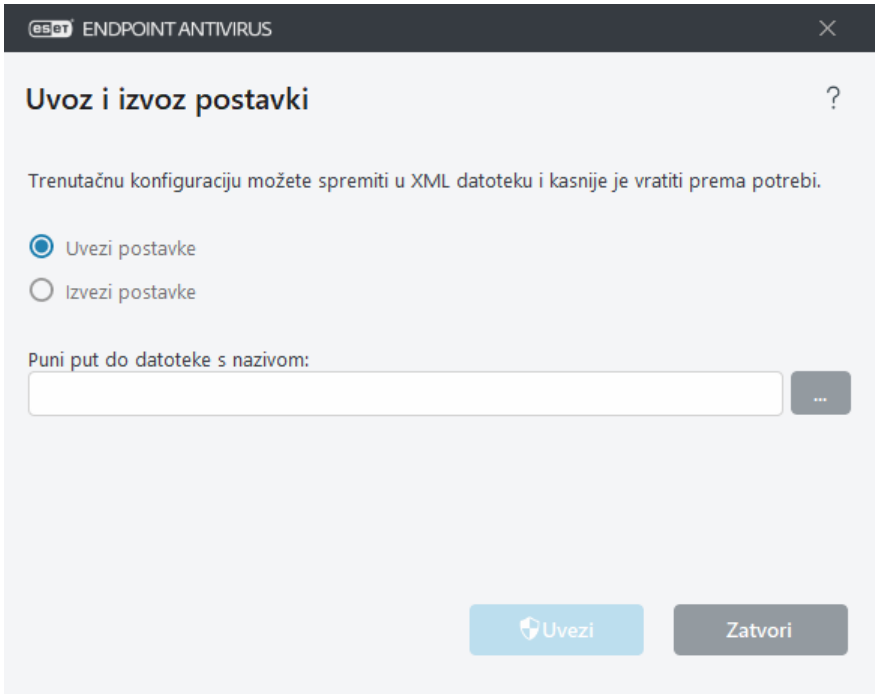
> **Ilustrirane upute**
> Pogledajte Uvoz ili izvoz postavki konfiguracije ESET-a pomoću .xml datoteke za ilustrirane upute dostupne na engleskom i nekoliko drugih jezika.

Uvoz i izvoz konfiguracijskih datoteka korisni su ako trebate izraditi sigurnosnu kopiju trenutne konfiguracije programa ESET Endpoint Antivirus da biste je mogli koristiti kasnije. Opcija izvoza postavki je praktična i kada želite koristiti svoju preferiranu konfiguraciju u više sustava. Možete uvesti .xml datoteku za prijenos tih postavki.

Za uvoz konfiguracije u glavnom programskom prozoru kliknite **Podešavanje** > **Uvoz ili izvoz postavki**, a zatim odaberite **Uvezi postavke**. Unesite naziv konfiguracijske datoteke ili kliknite gumb **...** da biste pronašli konfiguracijsku datoteku koju želite uvesti.

Za izvoz konfiguracije u glavnom programskom prozoru kliknite **Podešavanje** > **Uvoz ili izvoz postavki**. Odaberite **Izvezi postavke** i unesite puni put datoteke s nazivom. Kliknite **...** da biste otišli na mjesto na računalu gdje želite spremiti konfiguracijsku datoteku.

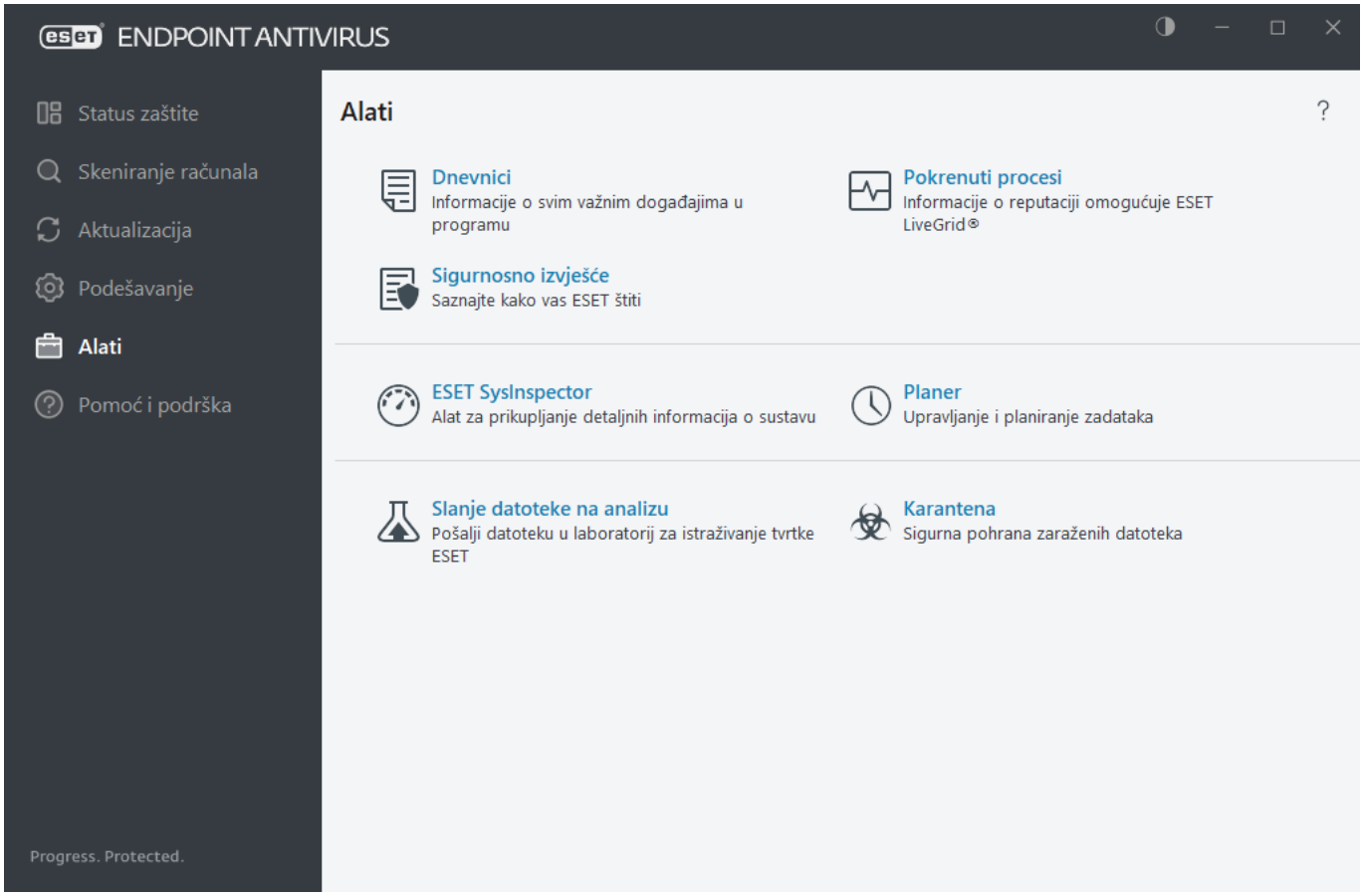
> Tijekom izvoza postavki može se pojaviti pogreška ako nemate dostatna prava za pisanje izvezene datoteke u navedeni direktorij.



Alati

Izbornik **Alati** sadrži module koji pojednostavnjuju administriranje programa i nude dodatne mogućnosti naprednim korisnicima.

- Dnevnici
- Procesi koji se izvršavaju (ako je ESET LiveGrid® aktiviran u programu ESET Endpoint Antivirus)
- Sigurnosno izvješće (za računala kojima se ne upravlja)
- ESET SysInspector
- Planer
- Slanje uzorka na analizu – Omogućuje slanje sumnjive datoteke na analizu u Laboratorij za istraživanje tvrtke ESET (možda neće biti dostupno ovisno o konfiguraciji za ESET LiveGrid®).
- Karantena



Dnevnici

Dnevnici sadrže informacije o svim važnim događajima u programu koji su se pojavili i pružaju pregled otkrivenih prijetnji. Dnevnici su ključan alat za analizu sustava, otkrivanje prijetnji te otklanjanje poteškoća. Zapisivanje se izvodi aktivno u pozadini bez korisničke intervencije. Podaci se bilježe na temelju trenutnih postavki opsega zapisivanja. Prikaz tekstualnih poruka i dnevnika moguć je izravno iz okruženja programa ESET Endpoint Antivirus. Moguće je i arhiviranje dnevnika.

Dnevnicima se pristupa iz glavnog prozora programa klikom na **Alati** > **Dnevnici**. Odaberite željenu vrstu dnevnika s padajućeg izbornika **Dnevnik**. Dostupni su sljedeći dnevnici:

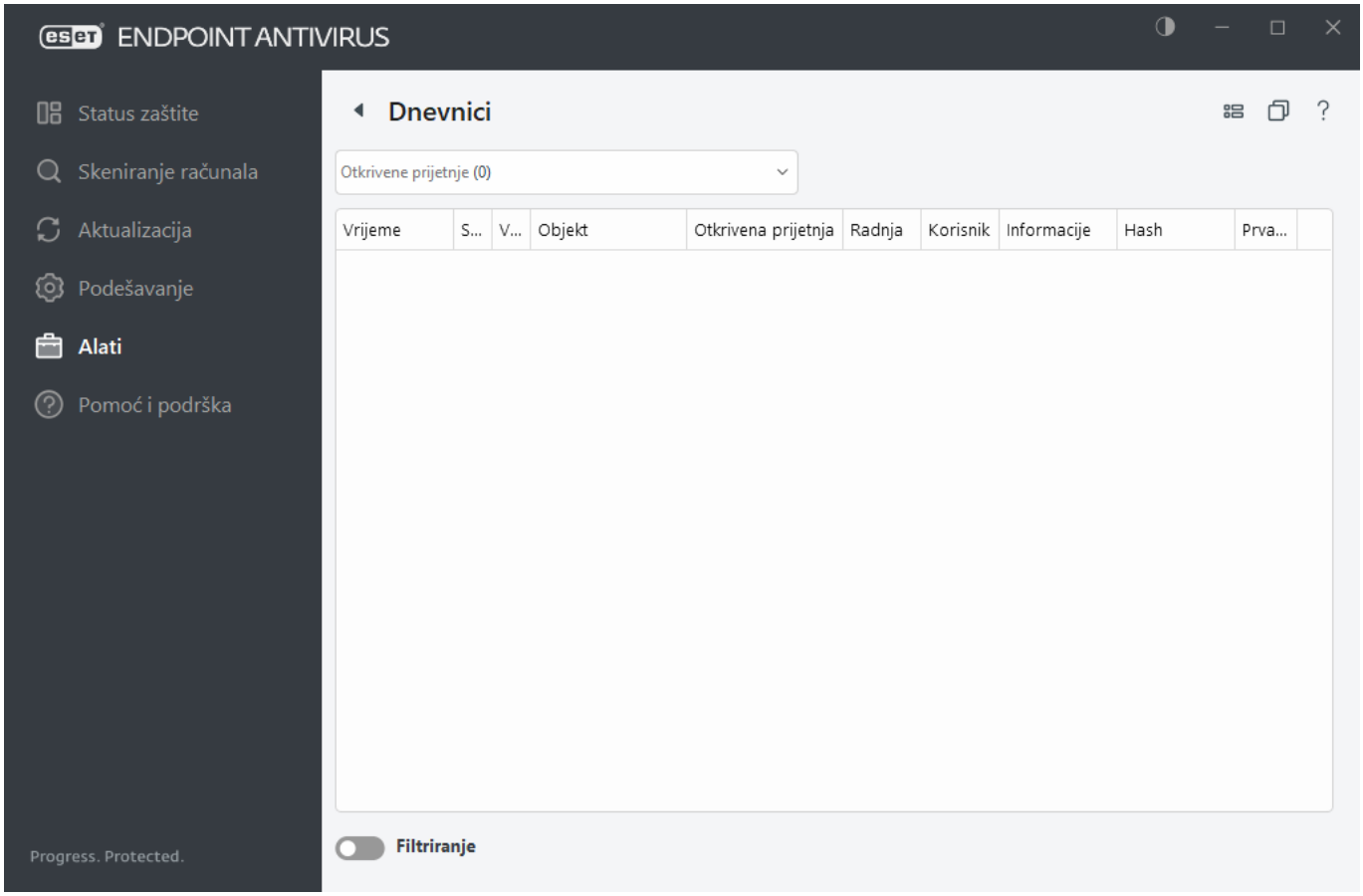
- **Otkrivene prijetnje** – Ovaj dnevnik pruža detaljne informacije o otkrivenim prijetnjama i infiltracijama koje

su otkrili moduli programa ESET Endpoint Antivirus. Ove informacije obuhvaćaju vrijeme i mjesto otkrivanja, naziv otkrivanja, izvršenu radnju te ime korisnika prijavljenog u trenutku otkrivanja prijetnje. Dvokliknite bilo koju stavku dnevnika da biste prikazali detalje u zasebnom prozoru. Neočišćene infiltracije uvijek su označene crvenim tekstom na svjetlocrvenoj pozadini, a očišćene infiltracije označene su žutim tekstom na bijeloj pozadini. Neočišćene potencijalno nepoželjne aplikacije ili potencijalno nesigurne aplikacije označene su žutim tekstom na bijeloj pozadini.

- **Događaji** – sve važne radnje koje je obavio ESET Endpoint Antivirus zabilježene su u dnevniku događaja. Dnevnik događaja sadrži informacije o događajima i pogreškama do kojih je došlo u programu. Namijenjen je za pomoć administratorima sustava i korisnicima za rješavanje problema. Te informacije često mogu olakšati iznalaženje rješenja za problem koji se pojavio u programu.
- **Skeniranje računala** – U ovom se prozoru prikazuju svi rezultati skeniranja. Svaki redak odgovara jednom izvršenom procesu skeniranja računala. Dvokliknite bilo koju stavku za prikaz detalja dotičnog skeniranja.
- **Blokirane datoteke** – sadrži zapise o blokiranim datotekama kojima se nije moglo pristupiti tijekom povezanosti s programom ESET Enterprise Inspector. Protokol prikazuje razlog i izvorni modul koji je blokirao datoteku, kao i aplikaciju korisnika koji ju je pokrenuo. Za više informacija pogledajte mrežni korisnički priručnik za ESET Enterprise Inspector.
- **Poslane datoteke** – Sadrži zapise datoteka koje su poslane sustavu ESET LiveGrid® ili ESET LiveGuard na analizu.
- **Dnevnici provjere** – svaki dnevnik sadrži podatke o datumu i vremenu promjene, vrsti promjene, opisu, izvoru i korisniku. Pogledajte odjeljak Dnevnici provjere za više detalja.
- **HIPS** – Sadrži zapise određenih pravila označenih za zapisivanje. Protokol pokazuje aplikaciju koja je pozvala operaciju, rezultat (je li pravilo bilo dopušteno ili zabranjeno) i naziv stvorenog pravila.
- **Mrežna zaštita** – dnevnik firewalla prikazuje sve udaljene napade koje je otkrila zaštita od mrežnog napada (IDS). Tu možete pronaći informacije o svim napadima na vaše računalo. U stupcu Događaj nalazi se popis otkrivenih napada. Stupac Izbor sadrži dodatne informacije o napadaču. Stupac Protokol otkriva komunikacijski protokol upotrijebljen u napadu. Analiza dnevnika mrežne zaštite može vam pomoći da na vrijeme otkrijete pokušaje infiltracije sustava kako biste spriječili neovlašten pristup sustavu. Više detalja o mrežnim napadima potražite u odjeljku IDS i napredne opcije.

- **Filtrirana web-mjesta**–ovaj je popis koristan ako želite pregledati popis web-mjesta koja je blokirala Zaštita web-pristupa. U tim dnevnicima možete vidjeti vrijeme, URL, korisnika i aplikaciju koja je stvorila vezu s određenom web stranicom.

- **Kontrola uređaja** – Sadrži zapise izmjenjivih medija ili uređaja koji su priključeni na računalo. U dnevnik se zapisuju samo uređaji s postavljenim pravilom kontrole uređaja. Ako pravilo ne odgovara priključenom uređaju, neće se stvoriti stavka dnevnika za priključeni uređaj. Tu možete vidjeti i pojedinosti kao što su vrsta uređaja, serijski broj, naziv proizvođača i veličina medija (ako je dostupno).



Odaberite sadržaj bilo kojeg dnevnika i pritisnite `Ctrl + C` **da biste ga kopirali u međuspremnik**. Držite `Ctrl + Shift` kako biste odabrali više unosa.

Kliknite **Filtriranje** da biste otvorili prozor Filtriranje dnevnika u kojem možete definirati kriterije za filtriranje.

Desnom tipkom miša kliknite određeni zapis kako biste otvorili kontekstni izbornik. Sljedeće mogućnosti dostupne su u kontekstnom izborniku:

- **Prikaži** – Prikazuje detaljne informacije o odabranom dnevniku u novom prozoru.
- **Filtriraj iste zapise** – Nakon aktiviranja tog filtra vidjet ćete samo zapise iste vrste (dijagnostika, upozorenja...).
- **Filtriraj** – Nakon što kliknete tu opciju, u prozoru Filtriranje dnevnika možete definirati kriterije za filtriranje za određene stavke u dnevniku.
- **Aktiviraj filtar** – Aktivira postavke filtra.
- **Deaktiviraj filtar** – Poništava sve postavke filtra (kao što je gore opisano).
- **Kopiraj / Kopiraj sve** – Kopira informacije o svim zapisima u prozoru.
- **Kopiraj ćeliju** – kopira sadržaj ćelije na koju ste kliknuli desnom tipkom miša.
- **Izbriši / Izbriši sve** – Briše odabrane zapise ili sve prikazane zapise – ova radnja zahtijeva administratorske ovlasti.
- **Izvezi** – Izvozi informacije o zapisima u XML obliku.
- **Izvezi sve** – Izvozi informacije o svim zapisima u XML obliku.
- **Pronađi / Pronađi sljedeće / Pronađi prethodno** – nakon što kliknete ovu opciju, možete definirati kriterije za filtriranje da biste istaknuli određen unos s pomoću prozora Filtriranje dnevnika.
- **Stvori izuzetak** – Stvorite novi izuzetak za detekciju pomoću čarobnjaka (nije dostupno za detekciju zlonamjernog softvera).

Filtriranje dnevnika

Kliknite **Filtriranje** na kartici **Alati** > **Dnevnici** za određivanje kriterija za filtriranje.

Značajka filtriranja dnevnika pomoći će vam da pronađete informacije koje tražite, posebice kada imate mnogo zapisa. Omogućuje vam sužavanje zapisa dnevnika, na primjer ako tražite određenu vrstu događaja, status ili vremensko razdoblje. Možete filtrirati zapise dnevnika navođenjem određenih opcija pretraživanja; u prozoru Dnevnika prikazat će se samo relevantni zapisi (prema navedenim opcijama pretraživanja).

Upišite ključnu riječ koju tražite u polje **Pronađi tekst**. Upotrijebite padajući izbornik **Traži u stupcima** kako biste suzili svoje pretraživanje. Odaberite jedan ili više zapisa iz padajućeg izbornika **Vrste zapisa dnevnika**. Odredite **Vremensko razdoblje** iz kojeg želite prikazati rezultate. Također možete upotrijebiti dodatne opcije pretraživanja, kao što su **Traži samo cijele riječi** ili **Osjetljivo na velika i mala slova**.

Pronađi tekst

Upišite niz teksta (riječ ili dio riječi). Prikazat će se samo zapisi koji sadrže taj niz. Ostali zapisi bit će izostavljeni.

Traži u stupcima

Odaberite stupce koji će se uzeti u obzir prilikom pretraživanja. Možete označiti jedan stupac ili više njih za pretraživanje.

Vrste zapisa

Odaberite jednu vrstu zapisa dnevnika ili više njih u padajućem izborniku:

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa te svi prethodno navedeni zapisi.
- **Informativno** – Zapisuju se sve informativne poruke, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke s upozorenjima.
- **Pogreške** – Zapisuju se pogreške kao što je „Pogreška preuzimanja datoteke” i kritične pogreške.
- **Kritično** – Zapisuju se samo kritične pogreške (pogreška pri pokretanju antivirusne zaštite

Vremensko razdoblje

Definirajte vremensko razdoblje od kojeg želite prikazati rezultate.

- **Nije određeno** (standardno) – Ne pretražuje unutar vremenskog razdoblja, već pretražuje čitav dnevnik.
- **Prošli dan**
- **Zadnje viđen**
- **Prošli mjesec**
- **Vremensko razdoblje** – Možete navesti točno vremensko razdoblje (Od: i Do:) da biste filtrirali samo zapise iz određenog vremenskog razdoblja.

Traži samo cijele riječi

Upotrijebite potvrdni okvir ako želite tražiti čitave riječi kako biste dobili preciznije rezultate.

Osjetljivo na velika i mala slova

Aktivirajte ovu opciju ako vam je važno da se velika i mala slova razlikuju tijekom filtriranja. Nakon što konfigurirate opcije filtriranja/pretraživanja, kliknite **U redu** da biste prikazali filtrirane zapise dnevnika ili Pronađi da biste započeli pretraživanje. Dnevnici se pretražuju od vrha prema dnu, počevši od trenutačnog položaja (zapis koji je istaknut). Pretraživanje se zaustavlja kada se pronađe prvi odgovarajući zapis. Pritisnite **F3** da biste tražili sljedeći zapis ili kliknite desnom tipkom miša i odaberite **Pronađi** da biste suzili opcije pretraživanja.

Dnevnici provjera

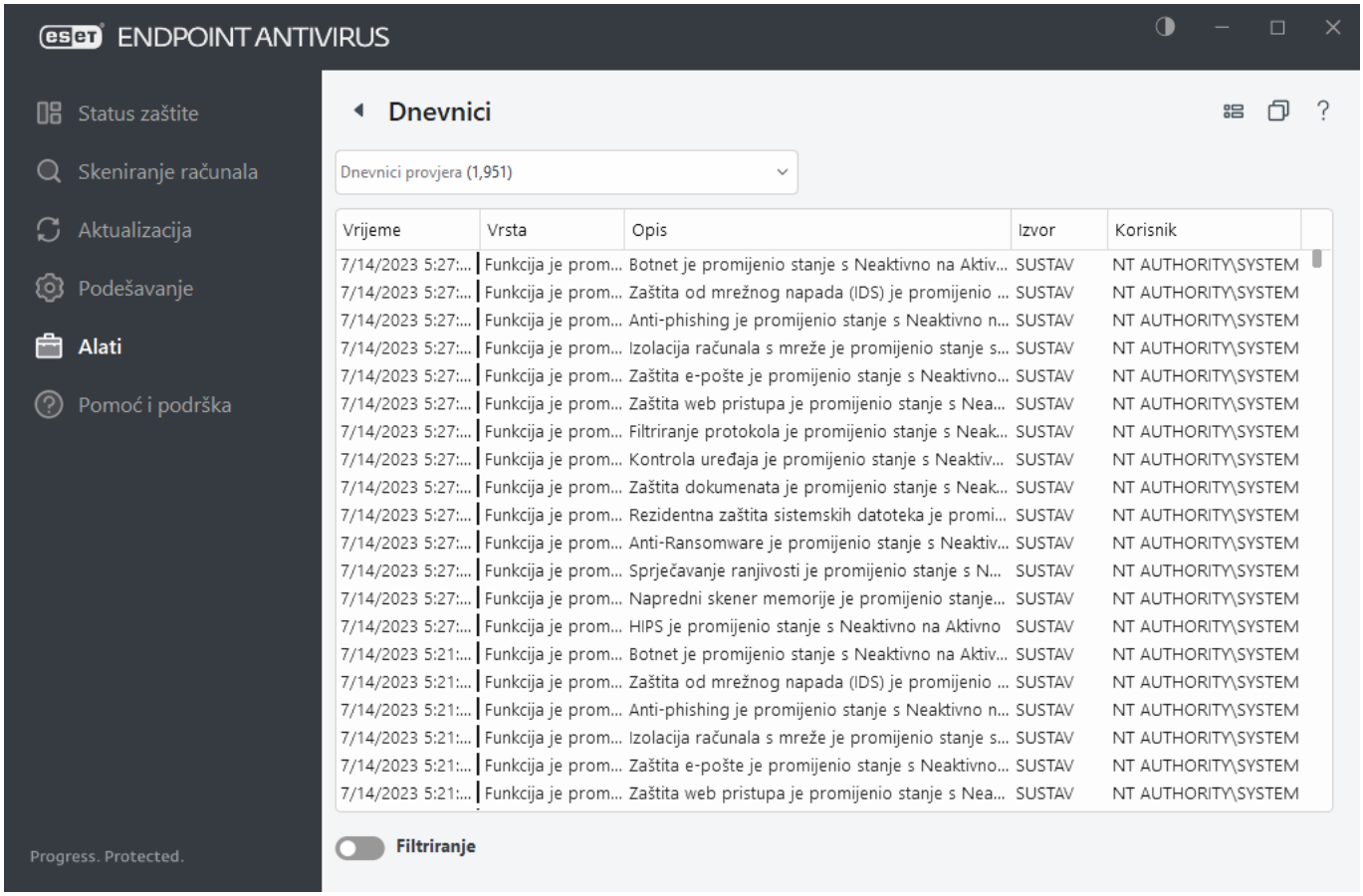
U korporativnom okruženju obično postoji više korisnika s definiranim pravima pristupa konfiguraciji krajnjih točaka. Preinaka konfiguracije programa može dramatično utjecati na rad programa i zato je vrlo važno da administratori prate promjene koje korisnici izvršavaju da bi brzo prepoznali i riješili problem te spriječili pojavu istog ili sličnih problema u budućnosti.

Dnevnik provjere nova je vrsta vođenja dnevnika u programu za prepoznavanje izvora problema. Dnevnik provjere prati promjene u konfiguraciji ili stanju zaštite i stvara snimke za kasniju upotrebu.

Da biste vidjeli **Dnevnik provjere**, kliknite **Alati** u glavnom izborniku te kliknite **Dnevnici** i odaberite **Dnevnici provjere** iz padajućeg izbornika.

Dnevnik provjere sadrži sljedeće podatke:

- Vrijeme – kada je promjena provedena
- Vrsta – koja je vrsta postavke ili funkcije promijenjena
- Opis – što se točno promijenilo, koji dio postavke se promijenio i broj promijenjenih postavki
- Izvor – gdje se nalazi izvor promjene
- Korisnik – tko je napravio promjenu



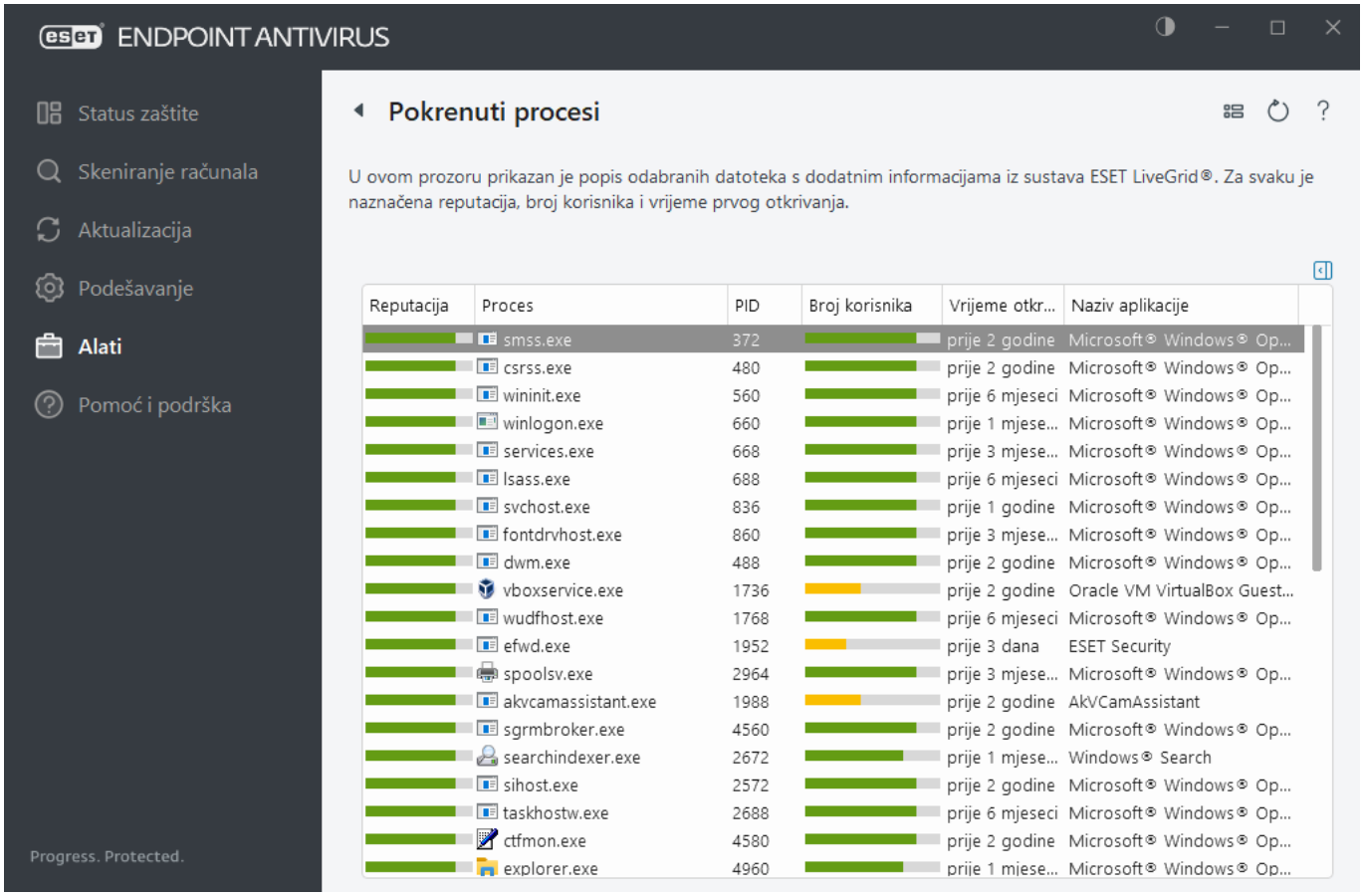
U prozoru Dnevnici desnom tipkom miša kliknite bilo koju vrstu dnevnika provjere s **promijenjenim postavkama** i odaberite **Pokaži promjene** iz kontekstnog izbornika za prikaz detaljnih podataka o provedenoj promjeni. Osim toga možete vratiti promjenu postavke tako da kliknete **Vrati** u kontekstnom izborniku (nije dostupno za programe kojima se upravlja pomoću programa ESET PROTECT). Ako odaberete **Obriši sve** u kontekstnom izborniku, stvorit će se dnevnik s podacima o toj radnji.

Ako je aktivirana opcija **Automatski optimiziraj dnevnike** u izborniku Napredno podešavanje > **Alati** > **Dnevnici**, dnevnici provjere automatski će se defragmentirati kao ostali dnevnici.

Ako je aktivirana opcija **Automatski obriši zapise starije od (u danima)** u izborniku Napredno podešavanje > **Alati** > **Dnevnici**, dnevnici provjere stariji od navedenog broja dana automatski će se obrisati.

Procesi koji se izvršavaju

Procesi koji se izvršavaju prikazuju programe i procese pokrenute na računalu i ESET se odmah i neprekidno obavještava o novim infiltracijama. ESET Endpoint Antivirus pruža detaljne informacije o procesima koji se izvršavaju kako bi zaštitio korisnike pomoću tehnologije ESET LiveGrid®.



Reputacija – u većini slučajeva ESET Endpoint Antivirus i tehnologija ESET LiveGrid® dodjeljuju razine rizika objektima (datotekama, procesima, ključevima registra itd.) s pomoću niza heurističkih pravila koja provjeravaju značajke svakog objekta i zatim procjenjuju moguću zlonamjernu aktivnost. Prema tim heurističkim pravilima objektima se dodjeljuje razina reputacije od 9 – najbolja reputacija (zeleno) do 0 – najgora reputacija (crveno).

Proces – Naziv slike programa ili procesa koji je trenutačno pokrenut na vašem računalu. Također možete upotrijebiti Windows Upravitelj zadataka za pregled svih procesa koji se izvršavaju na računalu. Upravitelj zadataka možete otvoriti tako da desnom tipkom miša kliknete prazno područje na programskoj traci i nakon toga kliknete Upravitelj zadataka, ili možete pritisnuti **Ctrl**+**Shift**+**Esc** na tipkovnici.

PID – To je ID procesa koji su pokrenuti u operacijskim sustavima Windows.

Poznate aplikacije označene zeleno definitivno su čiste (nalaze se na popisu pouzdanih adresa) i neće biti skenirane, čime se povećava brzina skeniranja računala na zahtjev ili rezidentne zaštite sistemskih datoteka na računalu.

Broj korisnika – Broj korisnika koji koriste danu aplikaciju. Te podatke prikuplja tehnologija ESET LiveGrid®.

Vrijeme otkrivanja – Vremensko razdoblje koje je proteklo otkada je tehnologija ESET LiveGrid® otkrila aplikaciju.

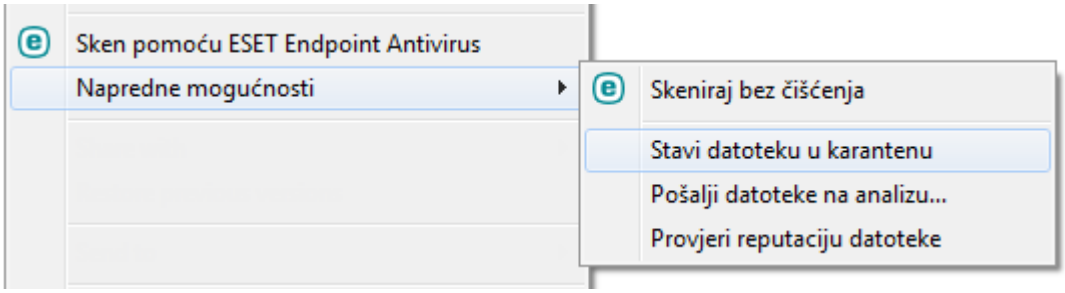
Kada je aplikacija označena kao aplikacija sigurnosne razine Nepoznato (narančasto), možda nije riječ o zlonamjernom softveru. Obično je samo riječ o novijoj aplikaciji. Ako za neku datoteku niste sigurni, možete poslati datoteku na analizu u laboratorij tvrtke ESET za otkrivanje virusa. Ako se ispostavi da je datoteka zlonamjerna aplikacija, njezino otkrivanje dodat će se jednoj od sljedećih aktualizacija modula za otkrivanje virusa.

Naziv aplikacije – Zadani naziv programa ili procesa.

Klikom na određenu aplikaciju na dnu, prikazat će se sljedeće informacije pri dnu prozora:

- **Put** – Lokacija aplikacije na vašem računalu.
- **Veličina** – Veličina datoteke u kB (kilobajtima) ili MB (megabajtima).
- **Opis** – Značajke datoteke temeljem opisa iz operacijskog sustava.
- **Tvrtka** – Naziv proizvođača ili procesa aplikacije.
- **Verzija** – informacije od izdavača aplikacije.
- **Program** – Naziv aplikacije i/ili poslovni naziv.
- **Stvoreno dana** – Datum i vrijeme kada je aplikacija stvorena.
- **Promijenjeno** – datum i vrijeme kada je aplikacija promijenjena.

Reputacija se može provjeriti i za datoteke koje ne djeluju kao programi/procesi koji se izvršavaju – označite datoteke koje želite provjeriti, kliknite ih desnom tipkom miša i iz kontekstnog izbornika odaberite **Napredne mogućnosti** > **Provjeri reputaciju datoteka pomoću sustava ESET LiveGrid®**.



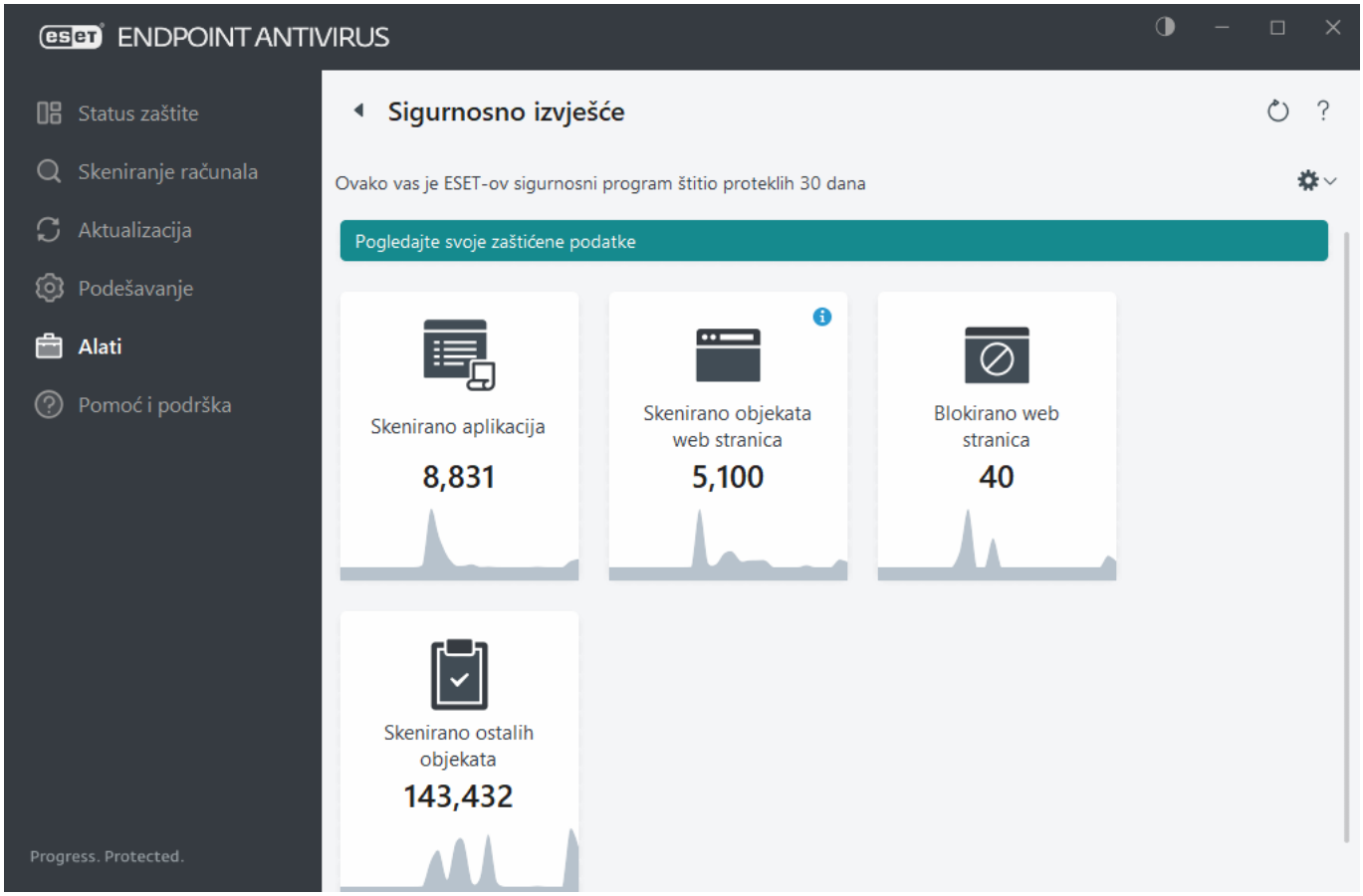
Sigurnosno izvješće

Ova funkcija pruža pregled statistika za sljedeće kategorije:

- **Blokirane web stranice** – Prikazuje broj blokiranih web stranica (URL-ovi koji su na popisu potencijalno neželjenih aplikacija, phishing, hakirani router, IP ili certifikat).
- **Otkriveni objekti zaražene e-pošte** – Prikazuje broj zaraženih objekata e-pošte koji su otkriveni.
- **Otkrivene potencijalno nepoželjne aplikacije** – prikazuje broj potencijalno nepoželjnih aplikacija (PUA).
- **Pregledani dokumenti** – Prikazuje broj skeniranih objekata dokumenata.
- **Skenirane aplikacije** – Prikazuje broj skeniranih izvršnih objekata.
- **Skenirani ostali objekti** – Prikazuje broj ostalih skeniranih objekata.
- **Pregledani objekti web stranica** – Prikazuje broj skeniranih objekata web stranica.
- **Skenirani objekti e-pošte** – prikazuje broj skeniranih objekata e-pošte.

Redoslijed ovih kategorija temelji se na numeričkoj vrijednosti od najviše prema najnižoj. Kategorije s nultom vrijednošću nisu prikazane. Kliknite **Prikaži više** za proširivanje i prikaz skrivenih kategorija.

Ako kliknite zupčanik u gornjem desnom kutu, možete **aktivirati/deaktivirati obavijesti sigurnosnog izvješća** ili odabrati hoće li se prikazivati podaci za zadnjih 30 dana ili za razdoblje otkada je program aktiviran. Ako je ESET Endpoint Antivirus instaliran manje od 30 dana, moguće je odabrati samo broj dana nakon instalacije. Razdoblje od 30 dana postavljeno je kao standardno.



Poništi podatke izbrisat će sve statistike i ukloniti postojeće podatke iz sigurnosnog izvješća. Ovu je radnju potrebno potvrditi, osim u slučaju kada ste odznačili opciju **Pitaj prije poništavanja statistike** u Napredno podešavanje > **Obavijesti** > **Interaktivna upozorenja** > **Poruke za potvrdu**.

ESET SysInspector

ESET SysInspector aplikacija je koja temeljito pregledava računalo i prikuplja detaljne informacije o komponentama sustava kao što su upravljački programi i aplikacije, mrežne veze ili važni unosi u registar te ocjenjuje razinu rizika svake komponente. Te informacije mogu olakšati određivanje uzroka sumnjivog ponašanja sustava do kojeg može doći zbog nekompatibilnosti softvera ili hardvera ili zbog zaraze zlonamjernim softverom. Da biste saznali kako upotrebljavati ESET SysInspector, pogledajte ESET SysInspector pomoć na mreži.

Prozor ESET SysInspector prikazuje sljedeće podatke o dnevnicima:

- **Vrijeme** – Vrijeme stvaranja dnevnika.
- **Komentar** – Kratki komentar.
- **Korisnik** – Ime korisnika koji je stvorio dnevnik.
- **Status** – Status stvaranja dnevnika.

Na raspolaganju su sljedeće akcije:

- **Prikaži** – otvara odabranu prijavu u sustav ESET SysInspector. Možete i desnom tipkom miša kliknuti dotični dnevnik i odabrati mogućnost **Prikaži** na kontekstnom izborniku.
- **Stvori** – Stvara novi dnevnik. Pričekajte dok se ESET SysInspector ne generira (status **Stvoreno**) prije nego što pokušate pristupiti dnevniku. Dnevnik se sprema u stavku C:\ProgramData\ESET\ESET Security\SysInspector.

- **Izbriši** – Briše odabrane dnevnike s popisa.

Ako odaberete jedan ili više dnevnika, na kontekstnom izborniku bit će dostupne sljedeće stavke:

- **Prikaži** – Otvara odabrani dnevnik u ESET SysInspector (ista funkcija kao i dvoklik dnevnika).
- **Stvori** – Stvara novi dnevnik. Pričekajte dok se ESET SysInspector ne generira (status **Stvoreno**) prije nego što pokušate pristupiti dnevniku.
- **Izbriši** – Briše odabrane dnevnike s popisa.
- **Izbriši sve** – Briše sve dnevnike.
- **Izvezi** – Izvozi dnevnik u .xml datoteku ili komprimiranu .xml datoteku.

Planer

planer upravlja planiranim zadacima s unaprijed definiranom konfiguracijom i svojstvima i pokreće ih.

Planeru se može pristupiti iz glavnog prozora programa ESET Endpoint Antivirus klikom na **Alati** > **Planer**. **Planer** sadrži popis svih zakazanih zadataka i njihova konfiguracijska svojstva, primjerice unaprijed definirani datum i vrijeme te profil skeniranja koji se upotrebljava.

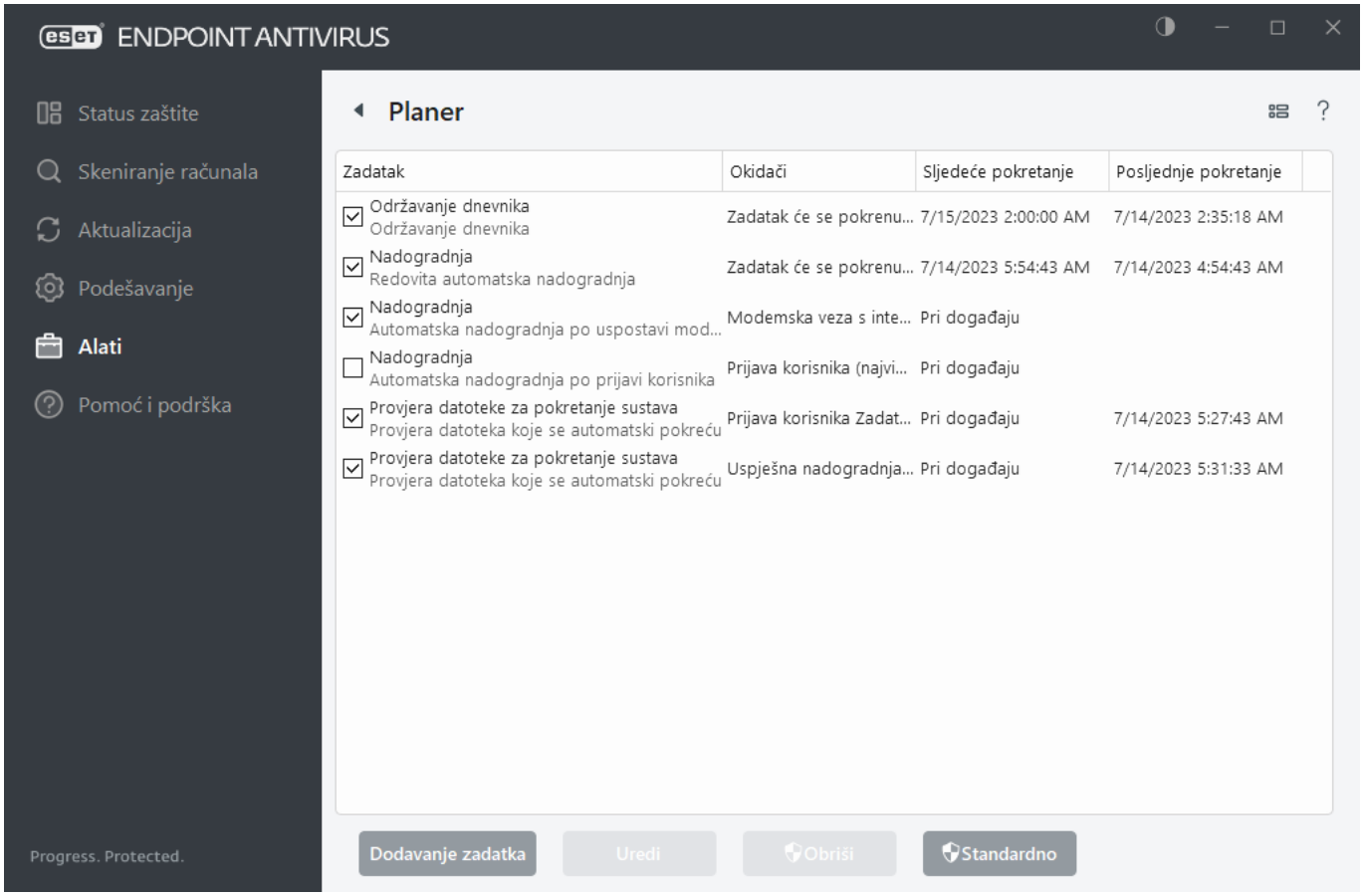
Planer služi za planiranje sljedećih zadataka: aktualizacije modula za otkrivanje virusa, zadatka skeniranja, provjeru datoteke pokretanja sustava i održavanje dnevnika. Možete dodavati i brisati zadatke izravno iz glavnog prozora Planera (klikom na gumb **Dodaj zadatak** ili **Izbriši** koji se nalaze u donjem dijelu). Kliknite desnom tipkom miša na bilo koji zadatak u Planeru da biste izvršili sljedeće akcije: prikazali detaljne informacije, odmah izvršili zadatak, dodali novi zadatak ili izbrisali postojeći. Potvrdnim okvirima na početku svakog unosa aktivirajte ili deaktivirajte zadatke.

Prema standardnim postavkama **Planer** prikazuje sljedeće planirane zadatke:

- **Održavanje dnevnika**
- **Redovna automatska aktualizacija**
- **Automatska aktualizacija po uspostavi modemske veze**
- **Automatska aktualizacija po prijavi korisnika**
- **Automatska provjera pokretačkih datoteka** (nakon prijave korisnika)
- **Automatska provjera datoteke pokretanja** (nakon uspješne aktualizacije modula)

> Mogućnost nasumične odgode izvršavanja zadataka u programu ESET PROTECT može se upotrebljavati za smanjenje opterećenja servera kod izvršavanja zadataka, posebno u velikim mrežama. Pomoću te mogućnosti možete definirati vremenski opseg tijekom kojeg zadatak treba izvršiti na cijeloj mreži, za razliku od izvršavanja zadatka na svim radnim stanicama na cijeloj mreži u isto vrijeme. Kada se zadatak pokrene, postavljena vremenska vrijednost nasumično se segmentira da bi se svakoj radnoj stanici na mreži dodijelilo jedinstveno vrijeme izvršavanja zadatka. To pomaže spriječiti preopterećenje servera i povezane probleme (npr. neki serveri mogu prijaviti DoS napad prilikom izvršavanja istovremene masovne nadogradnje na radnim stanicama na cijeloj mreži).

Da biste uredili konfiguraciju postojećeg zakazanog zadatka (standardnu ili korisnički definiranu), desnom tipkom miša kliknite zadatak i kliknite **Uredi** ili odaberite zadatak koji želite izmijeniti pa kliknite gumb **Uredi**.



Dodavanje novog zadatka

1. Kliknite **Dodaj zadatak** na dnu prozora.
2. Unesite naziv zadatka.
3. Odaberite željeni zadatak iz padajućeg izbornika:

- **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
- **Održavanje dnevnika** – Dnevnici sadrže i zaostatke već izbrisanih zapisa. Taj zadatak redovito optimizira zapise u dnevnicima radi učinkovitijeg rada.
- **Provjera datoteke za pokretanje sustava** – Provjerava datoteke kojima je dopušteno pokretanje prilikom pokretanja sustava ili prijave.
- **Stvori snimku statusa računala** – Stvara snimku računala pomoću programa ESET SysInspector – prikuplja detaljne informacije o komponentama sustava (primjerice upravljačkim programima, aplikacijama) i procjenjuje razinu rizika za svaku komponentu.
- **Skeniranje računala na zahtjev** – Izvodi skeniranje datoteka i mapa na računalu.
- **Aktualizacija** – Planira zadatak aktualizacije aktualizacijom modula za otkrivanje virusa i programskih modula.

4. Uključite prekidač **Aktiviraj** ako želite aktivirati zadatak (možete to učiniti kasnije odabirom potvrdnog okvira na popisu planiranih zadataka), a zatim kliknite **Sljedeće** i odaberite jednu od vremenskih mogućnosti:

- **Jednom** – Zadatak će se izvršiti na unaprijed definirani datum i vrijeme.
- **Opetovano** – Zadatak će se izvršavati u navedenim vremenskim intervalima.
- **Svakodnevno** – Zadatak će se izvršavati opetovano svakog dana u isto vrijeme.
- **Tjedno** – Zadatak će se izvršiti na određeni dan i u određeno vrijeme.
- **Pri događaju** – Zadatak će se izvršiti kod određenog događaja.

5. **Odaberite mogućnost Nemoj izvršavati zadatak ako računalo koristi bateriju** da biste minimizirali korištenje sistemskih resursa dok prijenosno računalo koristi bateriju. Zadatak će se izvršiti na datum i vrijeme zadani u poljima **Izvršavanje zadatka**. Ako se zadatak nije mogao izvršiti u unaprijed definirano vrijeme, možete navesti kada će se ponovno izvršiti odabirom sljedećih mogućnosti:

- **U sljedećem zakazanom terminu**
- **Što prije**
- **Odmah, ako vrijeme proteklo od zadnjeg izvršavanja premašuje određenu vrijednost** (interval se može definirati putem okvira za listanje **Vrijeme od zadnjeg izvršavanja**)

Da biste pregledali planirani zadatak, desnom tipkom miša kliknite zadatak i odaberite **Prikaži detalje zadatka**.

Opcije planiranog skeniranja

U ovom prozoru možete odrediti napredne opcije za zadatak zakazanog skeniranja računala.

Da biste pokrenuli skeniranje bez radnje čišćenja, kliknite **Napredne postavke** i odaberite **Skeniraj bez čišćenja**. Povijest skeniranja sprema se u dnevnik skeniranja.

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

S pomoću padajućeg izbornika možete postaviti radnju tako da se automatski izvršava nakon što se skeniranje dovrši:

- **Bez radnje** – Kada skeniranje završi, neće se izvršiti nijedna radnja.
- **Isključi** – Kada skeniranje završi, računalo se isključuje.
- **Ponovno pokreni** – Zatvara sve otvorene programe i restarta računalo kada završi skeniranje.
- **Ponovno pokreni po potrebi** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Prisilno ponovno pokreni** – prisilno zatvara sve otvorene programa bez čekanja interakcije korisnika i ponovno pokreće računalo nakon što se skeniranje dovrši.
- **Prisilno ponovno pokrenite ako je potrebno** – računalo se ponovno pokreće samo ako je to potrebno za dovršetak čišćenja otkrivenih prijetnji.
- **Spavanje** – Sprema vašu sesiju i stavlja računalo u privremeno stanje u kojem troši malo energije kako biste brzo mogli nastaviti s radom.
- **Hibernacija** – Prebacuje sve što radi na sistemskoj memoriji (RAM) u posebnu datoteku na tvrdom disku. Računalo se isključuje, ali će se prilikom sljedećeg pokretanja vratiti u svoje posljednje stanje prije isključenja.

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

Odaberite opciju **Skeniranje se ne može otkazati** da biste korisnicima koji nemaju posebne ovlasti onemogućili prekidanje radnji koje se poduzimaju nakon skeniranja.

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

Također pogledajte Napredak skeniranja.

Pregled zakazanog zadatka

Dijaloški prozor prikazuje detaljne informacije o označenim zakazanim zadacima kada dvokliknete na prilagođeni zadatak ili desnim klikom kliknete na prilagođeni zadatak planera i kliknete **Prikaži detalje zadatka**.

Pojedinosti zadatka

Upišite **naziv zadatka**, odaberite jednu od opcija **vrste zadataka**, a zatim kliknite **Dalje**:

- **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
- **Održavanje dnevnika** – Dnevnici sadrže i zaostatke već izbrisanih zapisa. Taj zadatak redovito optimizira zapise u dnevnicima radi učinkovitijeg rada.
- **Provjera datoteke za pokretanje sustava** – Provjerava datoteke kojima je dopušteno pokretanje prilikom pokretanja sustava ili prijave.
- **Stvori snimku statusa računala** – Stvara snimku računala pomoću programa ESET SysInspector – prikuplja detaljne informacije o komponentama sustava (primjerice upravljačkim programima, aplikacijama) i procjenjuje razinu rizika za svaku komponentu.
- **Skeniranje računala na zahtjev** – Izvodi skeniranje datoteka i mapa na računalu.
- **Nadogradnja** – Planira zadatak nadogradnje nadogradnjom modula.

Vrijeme pokretanja zadatka

Zadatak će se izvršavati opetovano u navedenim vremenskim intervalima. Odaberite jednu od vremenskih mogućnosti:

- **Jednom** – Zadatak će se izvršiti samo jednom, na unaprijed definirani datum i u unaprijed definirano vrijeme.
- **Opetovano** – Zadatak će se izvršavati u navedenim vremenskim intervalima (u satima).
- **Svakodnevno** – Zadatak će se izvršavati svakog dana u isto vrijeme.
- **Tjedno** – Zadatak će se izvršavati jednom ili nekoliko puta tjedno i to u odabrane dane i odabrano vrijeme.
- **Pri događaju** – Zadatak će se izvršiti nakon pojave određenog događaja.

Nemoj izvršavati zadatak ako računalo koristi bateriju – Zadatak se neće pokrenuti ako se računalo u trenutku pokretanja zadatka napaja iz baterije. To vrijedi i za računala koja se napajaju iz UPS-a.

Vrijeme pokretanja zadatka – jednom

Pokretanje zadatka – Određeni zadatak pokrenut će se samo jednom na određeni datum i u određeno vrijeme.

Vrijeme pokretanja zadatka – svakodnevno

Zadatak će se izvršavati svakog dana u isto vrijeme.

Vrijeme pokretanja zadatka – tjedno

Zadatak će se iznova pokretati svaki tjedan na odabrani dan ili dane i u odabrano vrijeme.

Vrijeme pokretanja zadatka – pokretanje prilikom događaja

Zadatak će se pokrenuti prilikom jednog od sljedećih događaja:

- **Prilikom svakog pokretanja računala**
- **Svakodnevno prilikom prvog pokretanja računala**
- **Modemska veza s internetom/VPN-om**
- **Uspješna nadogradnja modula**
- **Uspješna nadogradnja programa**
- **Prijava korisnika**
- **Otkrivanje prijetnji**

Prilikom zakazivanja zadatka koji će se pokrenuti s pojavom nekog događaja, možete navesti minimalni interval između dva dovršenja zadatka. Ako se, primjerice, na računalo prijavljujete nekoliko puta dnevno, odaberite 24 sata da bi se taj zadatak izvršio samo prilikom prve prijave u danu, a zatim ponovno sljedećeg dana.

Preskočeni zadatak

Zadatak se može preskočiti kada se računalo napaja putem baterije ili je isključeno. Odaberite kada se preskočeni zadatak treba izvršiti putem jedne od ovih opcija i kliknite **Dalje**:

- **U sljedećem zakazanom terminu** – zadatak će se pokrenuti ako je računalo uključeno u sljedećem zakazanom terminu.
- **Što prije** – zadatak će se pokrenuti kada je računalo uključeno.
- **Odmah, ako je vrijeme od posljednjeg zakazanog pokretanja više od (sati)** – predstavlja vrijeme proteklo od prvog preskočenog izvođenja zadatka. Ako se ovo vrijeme prekorači, zadatak će se odmah pokrenuti.

Odmah ako vrijeme od posljednjeg zakazanog pokretanja premašuje (u satima) – primjeri

Primjer zadatka je postavljen za izvođenje više puta svakih sat vremena. Opcija **Odmah, ako je vrijeme od zadnjeg zakazanog izvođenja dulje od (sati)** je odabrana i prekoračeno vrijeme je postavljeno na dva sata. Zadatak se pokreće u 13:00 h, a po završetku računalo odlazi u stanje mirovanja:

• Računalo se budi u 15:30 h. Prvo preskočeno pokretanje zadatka je bilo u 14:00 h. Prošlo je samo 1,5 sata od 14:00 h, tako da će se zadatak pokrenuti u 16:00 h.

• Računalo se budi u 16:30 h. Prvo preskočeno pokretanje zadatka je bilo u 14:00 h. Prošla su dva i pol sata od 14:00 h, tako da će se zadatak odmah pokrenuti.

Detalji o zadatku – nadogradnja

Ako program želite aktualizirati pomoću dva aktualizacijska servera, morate stvoriti dva različita aktualizacijska profila. Ako prvi server ne uspije u preuzimanju datoteka aktualizacije, program će se automatski prebaciti na

drugi server. To je primjerice pogodno za prijenosna računala čija se aktualizacija obično vrši putem aktualizacijskog servera na lokalnom LAN-u, no njihovi se vlasnici često povezuju s internetom pomoću drugih mreža. Dakle, ako prvi profil ne uspije, drugi će automatski preuzeti aktualizacijske datoteke s ESET-ovih aktualizacijskih servera.

Detalji o zadatku – pokretanje aplikacije

Ovaj zadatak zakazuje pokretanje vanjske aplikacije.

Izvršna datoteka – Odaberite izvršnu datoteku iz stabla direktorija, kliknite opciju **...** ili unesite put ručno.

Radna mapa – Definirajte radni direktorij vanjske aplikacije. Sve privremene datoteke odabrane **Izvršne datoteke** stvorit će se u tom direktoriju.

Parametri – Parametri naredbenog retka za aplikaciju (nije obavezno).

Kliknite **Završetak** da biste primijenili zadatak.

Slanje uzoraka na analizu

Ako na računalu pronađete sumnjivu datoteku ili na internetu pronađete sumnjivu web stranicu, možete ih poslati na analizu u Laboratorij za istraživanje tvrtke ESET (možda neće biti dostupno ovisno o konfiguraciji za ESET LiveGrid®).

Nemojte slati uzorak ako ne ispunjava barem jedan od sljedećih kriterija:
• Uzorak uopće nije otkriven ESET-ovim programom.
• Uzorak je neispravno otkriven kao prijetnja.
• Ne prihvaćamo osobne datoteke (za koje biste htjeli da ih ESET skenira u potrazi za zlonamjernim programima) kao uzorke (Laboratorij za istraživanje tvrtke ESET ne provodi skeniranja na zahtjev korisnika).
• Upotrijebite opisni redak naslova i priložite što je moguće više informacija o datoteci (npr. snimka zaslona ili web stranica s koje ste je preuzeli).

Slanje uzoraka omogućuje vam da pošaljete datoteku ili web stranicu ESET-u radi analize jednom od sljedećih metoda:

1. Upotrijebite prozor za slanje uzoraka koji se nalazi u izborniku **Alati** > **Slanje uzorka na analizu**.
2. Datoteku možete poslati i e-poštom. Ako želite upotrijebiti tu mogućnost, datoteku zapakirajte s pomoću programa WinRAR/ZIP, arhivsku datoteku zaštitite lozinkom "infected" i pošaljite je na adresu samples@eset.com.
3. Prijavljivanje spama ili lažno pozitivnih rezultata pogledajte naš članak iz ESET-ove baze znanja.

Dok je otvorena stavka **Odabir uzorka za analizu**, u padajućem izborniku **Razlog za slanje uzorka** odaberite opis koji najbolje odgovara vašoj poruci:

- Sumnjiva datoteka
- Sumnjiva stranica (web stranica koja je zaražena bilo kojim zlonamjernim softverom),
- Neispravno identificirana datoteka (datoteka koja je otkrivena kao zaražena, ali zapravo nije),
- Neispravno identificirana web stranica
- Ostalo

Datoteka/Stranica – Put do datoteke ili web stranice koju želite poslati.

Adresa e-pošte za kontakt – Adresa e-pošte za kontakt šalje se u ESET zajedno sa sumnjivim datotekama, a može se koristiti za komunikaciju u slučaju potrebe za dodatnim informacijama za analizu. Unos adrese e-pošte za kontakt nije obavezan. Odaberite **Pošalji anonimno** da bi polje ostalo prazno.

> Ako ne budu potrebne dodatne informacije, ESET vam neće poslati odgovor. Naši serveri svakodnevno primaju desetke tisuća datoteka, pa ne možemo odgovoriti na sve poruke.
> Ako se pokaže da je uzorak ustvari zlonamjerna aplikacija ili web stranica, njegovo će se otkrivanje dodati u jednu od sljedećih ESET-ovih nadogradnji.

Odabir uzorka za analizu – Sumnjiva datoteka

Primijećeni znakovi i simptomi zaraze zlonamjernim softverom – Unesite opis ponašanja sumnjive datoteke na svojem računalu.

Porijeklo datoteke (URL adresa ili dobavljač) – Unesite porijeklo (izvor) datoteke i kako ste došli do nje.

Napomene i dodatne informacije – Ovdje možete unijeti dodatne informacije ili opis koji će nam pomoći pri identifikaciji sumnjive datoteke.

> Prvi je parametar – **Primijećeni znakovi i simptomi zaraze zlonamjernim softverom** – obavezan, no navođenje dodatnih informacija našim će laboratorijima uvelike pomoći pri identifikaciji uzoraka.

Odabir uzorka za analizu – Sumnjiva web stranica

Odaberite jednu od sljedećih mogućnosti s padajućeg izbornika **Što nije u redu s web stranicom**:

- **Zaraženo** – Web stranica koja sadrži viruse ili drugi zlonamjerni softver koji se distribuira raznim metodama.
- **Phishing** – Phishing se često koristi za ostvarivanje pristupa tajnim podacima kao što su brojevi bankovnih računa, PIN kodovi itd. Više o toj vrsti napada pročitajte u rječniku.
- **Prijevara** – Web stranica čiji je sadržaj lažan ili obmanjujuć, posebno u svrhu ostvarivanja brze zarade.
- Odaberite **Ostalo** ako se iznad spomenute mogućnosti ne odnose na web stranicu koju želite poslati.

Napomene i dodatne informacije – Tu možete unijeti dodatne informacije ili opis koji će nam pomoći pri analizi sumnjive web stranice.

Odabir uzorka za analizu – Neispravno identificirana datoteka

Od vas tražimo da pošaljete datoteke koje su identificirane kao zaražene, no zapravo to nisu kako bismo poboljšali svoj antivirusni i antispyware modul te pomogli drugima da ostanu zaštićeni. Neispravno identificirane stranice (FP-ovi) mogu se pojaviti kad uzorak datoteke odgovara istom uzorku sadržanom u modulu za otkrivanje virusa.

Naziv i verzija aplikacije – Naslov i verzija programa (npr. broj, drugo ime ili kodno ime).

Porijeklo datoteke (URL adresa ili dobavljač) – Unesite porijeklo (izvor) datoteke i zabilježite kako ste došli do nje.

Svrha aplikacija – Općeniti opis aplikacije, vrsta aplikacije (npr. preglednik, multimedijski reproduktor...) i njena funkcionalnost.

Napomene i dodatne informacije – Ovdje možete unijeti dodatne informacije ili opis koji će nam pomoći pri obradi sumnjive datoteke.

> prva tri parametra obavezna su za identifikaciju legitimnih aplikacija i njihovo razlikovanje od zlonamjernog koda. Navođenjem dodatnih informacija našim ćete laboratorijima uvelike pomoći pri identifikaciji i obradi uzoraka.

Odabir uzorka za analizu – Neispravno identificirana web stranica

Od vas tražimo da pošaljete web stranice koje su identificirane kao zaražene ili kao stranice za prijevaru ili phishing, no zapravo to nisu. Neispravno identificirane stranice (FP-ovi) mogu se pojaviti kad uzorak datoteke odgovara istom uzorku sadržanom u modulu za otkrivanje virusa. Pošaljite nam takve web stranice da bismo poboljšali svoj antivirusni i antiphishing modul te pomogli drugima da ostanu zaštićeni.

Napomene i dodatne informacije – ovdje možete unijeti dodatne informacije ili opise koji će nam pomoći pri obradi sumnjive web stranice.

Odabir uzorka za analizu – Ostalo

Taj obrazac koristite ako se datoteka ne može definirati kao **Sumnjiva datoteka** ni kao **Neispravna identifikacija**.

Razlog slanja datoteke – Unesite detaljan opis i razlog slanja datoteke.

Karantena

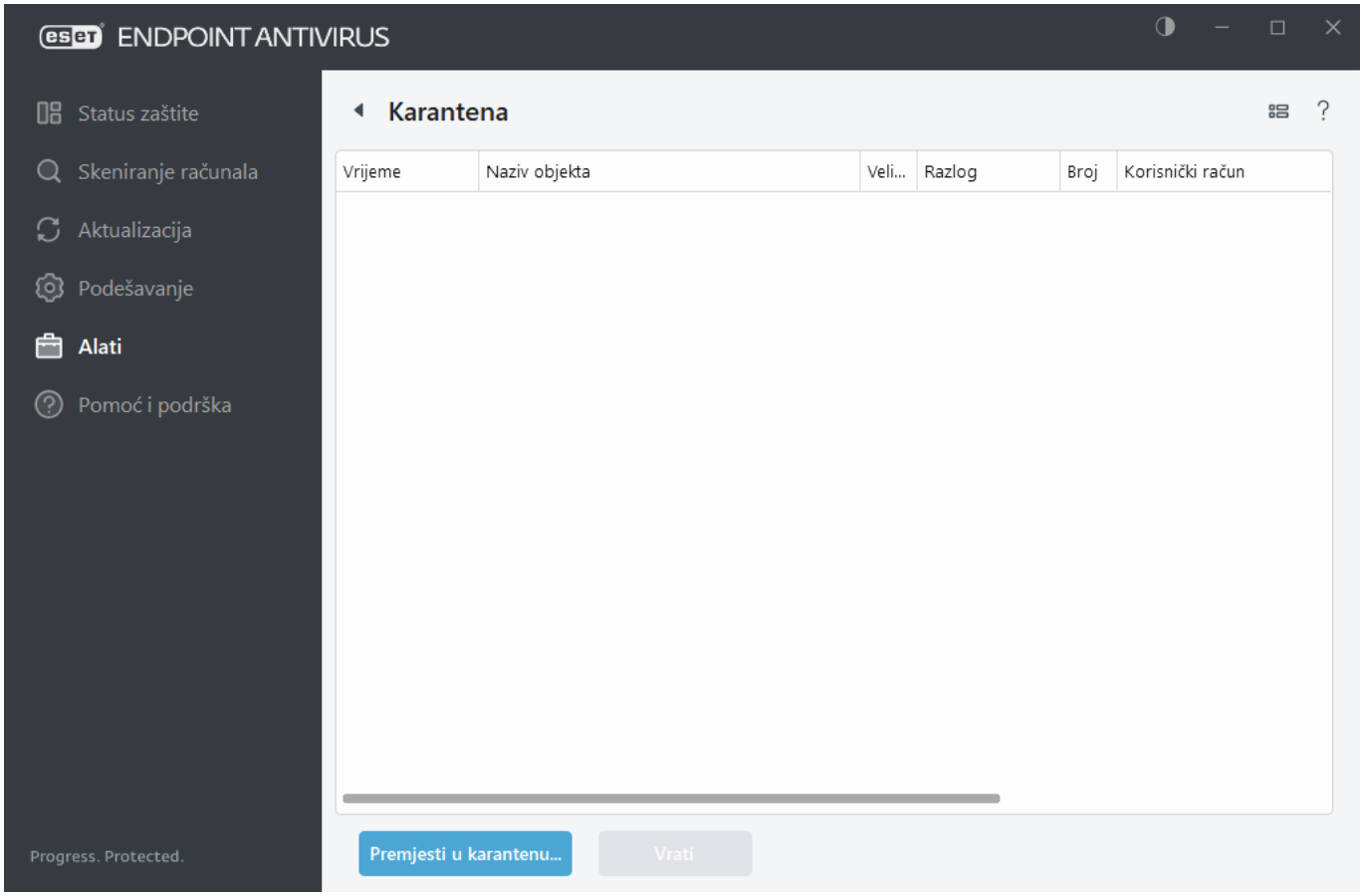
Glavna funkcija karantene je sigurna pohrana prijavljenih objekata (kao što su zlonamjerni programi, zaražene datoteke ili potencijalno nepoželjne aplikacije).

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

Datoteke pohranjene u mapi karantene mogu se pregledati u tablici koja prikazuje:

- datum i vrijeme karantene,
- put do izvorne lokacije datoteke,
- njezinu veličinu u bajtovima,
- razlog (na primjer, objekt koji je dodao korisnik),
- broj prijetnji (na primjer, duplikati prijetnji iste datoteke ili arhiva koja sadrži višestruke infiltracije).

Na daljinu upravljam karantenom na klijentskim radnim stanicama



Stavljanje datoteka u karantenu

ESET Endpoint Antivirus automatski stavlja obrisane datoteke u karantenu (ako niste onemogućili ovu opciju u prozoru s upozorenjima).

Dodatne datoteke treba staviti u karantenu:

- ako se ne mogu izbrisati,
- ako ih nije sigurno ili preporučljivo obrisati,
- ako ih ESET Endpoint Antivirus pogrešno otkrije,
- ili ako se datoteka ponaša sumnjivo, ali je skener ne otkrije.

Imate više opcija za stavljanje datoteke u karantenu:

- upotrijebite funkciju povlačenja i ispuštanja za ručno stavljanje datoteke u karantenu tako da kliknete datoteku, pomaknete pokazivač miša na označeno područje uz pritisnutu tipku miša, a zatim je ispustite. Nakon toga se aplikacija prebacuje u prvi plan.
- Kliknite **Prebaci u karantenu** iz glavnog prozora programa.
- U tu svrhu se također može upotrebljavati kontekstni izbornik; desnom tipkom miša kliknite prozor **Karantena** i odaberite **Karantena**.

Vraćanje iz karantene

Datoteke u karanteni također se mogu vratiti na izvornu lokaciju:

- U tu svrhu upotrijebite funkciju **Vrati**, koja je dostupna iz kontekstnog izbornika tako da desnom tipkom miša kliknete određenu datoteku u karanteni.

- Ako je datoteka označena kao potencijalno neželjena aplikacija, aktivirana je opcija **Vrati i izuzmi od skeniranja**. Također pogledajte odjeljak Izuzeci.
- Kontekstni izbornik također pruža opciju **Vrati na**, koja vam omogućuje vraćanje datoteke na lokaciju koja nije ista kao lokacija s koje je datoteka obrisana.
- Funkcija vraćanja nije dostupna u nekim slučajevima, na primjer, za datoteke koje se nalaze na zajedničkoj mreži samo za čitanje.

Brisanje iz karantene

Kliknite desnom tipkom miša na odabranu stavku i odaberite **Izbriši iz karantene** ili odaberite stavku koju želite izbrisati i pritisnite **Izbriši** na tipkovnici. Možete odabrati i više stavki odjednom i sve ih izbrisati. Izbrisane stavke trajno će se ukloniti s uređaja i iz karantene.

Slanje datoteke iz karantene

Ako ste u karantenu stavili sumnjivu datoteku koju program nije otkrio ili ako je datoteka neispravno procijenjena kao zaražena (npr. heurističkom analizom koda) i stavljena u karantenu, pošaljite uzorak na analizu u Laboratorij za istraživanje tvrtke ESET. Da biste poslali datoteku, kliknite je desnom tipkom miša i u kontekstnom izborniku odaberite **Pošalji na analizu**.

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
- Upravljanje karantenom u programu ESET PROTECT
- ESET-ov program obavijestio me o prijetnji – što trebam učiniti?

Pomoć i podrška

Kliknite **Pomoć i podrška** u prozoru glavnog programa da biste prikazali informacije o podršci i alate za otklanjanje poteškoća koji vam pomažu u rješavanju problema na koje možete naići.

Instalirani program

- O programu ESET Endpoint Antivirus – Prikazuje informacije o vašoj kopiji programa ESET Endpoint Antivirus.
- Otklanjanje poteškoća s programom – kliknite ovaj link da biste pronašli rješenja za najčešće probleme.
- Otklanjanje poteškoća s licencom – kliknite ovaj link da biste pronašli rješenja za probleme s aktivacijom ili promjenom licence.
- Promjena licence – Kliknite za pokretanje aktivacijskog prozora i aktivaciju programa.

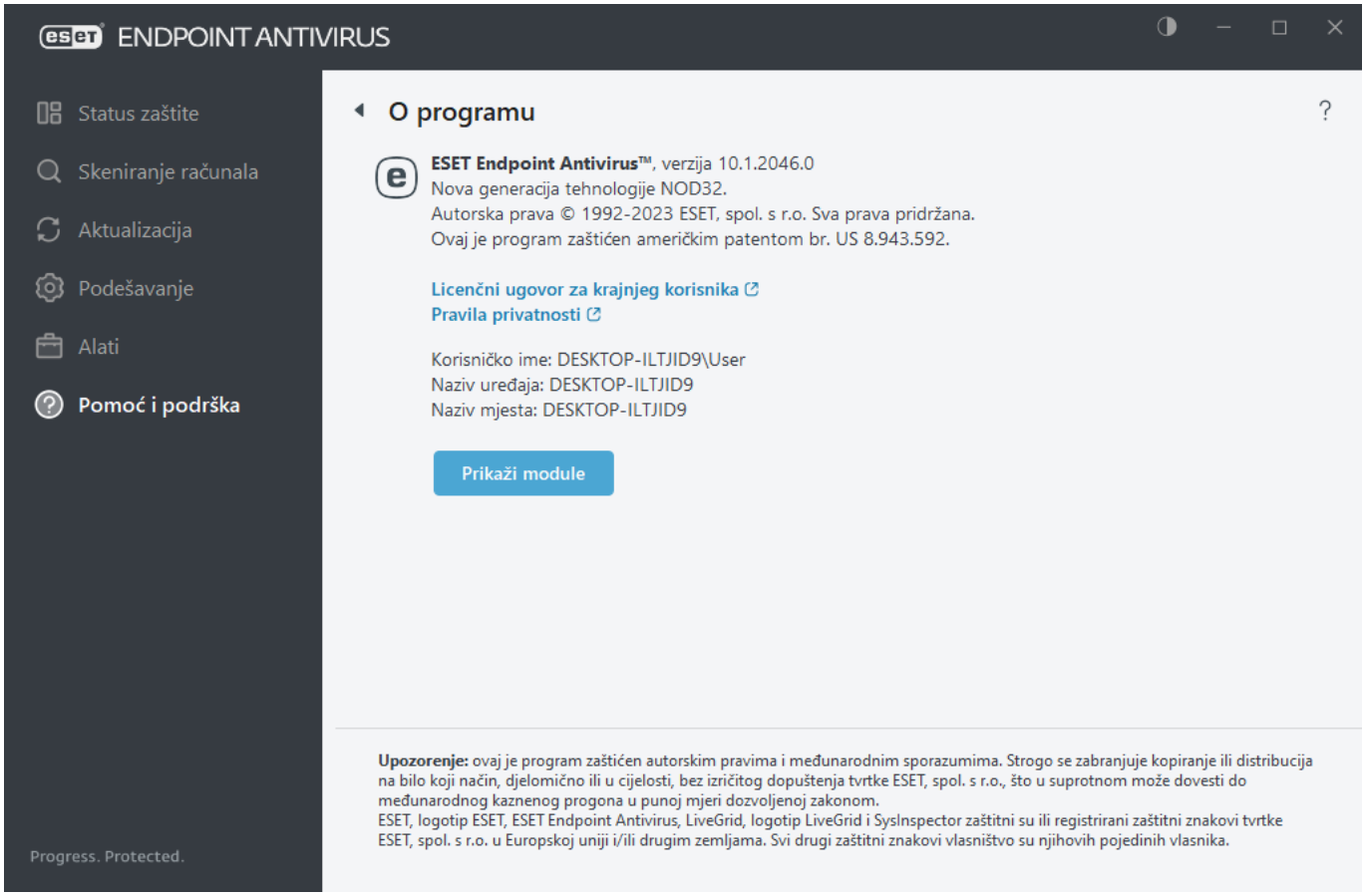
Stranica pomoći – Kliknite ovaj link da biste pokrenuli stranice pomoći programa ESET Endpoint Antivirus.

Tehnička podrška

Baza znanja – ESET-ova baza znanja sadrži odgovore na najčešće postavljana pitanja kao i preporučena rješenja za razne probleme. Stručnjaci tehničke podrške tvrtke ESET redovito nadograđuju bazu znanja, što je čini najpotpunijim alatom za rješavanje raznih problema.

O programu ESET Endpoint Antivirus

U ovom prozoru se navode pojedinosti o instaliranoj verziji programa ESET Endpoint Antivirus i vašem računalu.



Kliknite **Prikaži module** da biste vidjeli informacije o popisu učitanih modula programa.

- Informacije o modulima možete kopirati u međuspremnik tako da kliknete **Kopiraj**. To može biti korisno prilikom otklanjanja poteškoća ili kontaktiranja s tehničkom podrškom.
- Kliknite **Modul detekcije** u prozoru Moduli da biste otvorili ESET-ov virusni radar koji sadrži informacije o svakoj verziji ESET-ovog modula detekcije.

Slanje podataka o sistemskoj konfiguraciji

Radi pružanja što brže i preciznije pomoći, tvrtki ESET potrebne su informacije o konfiguraciji programa ESET Endpoint Antivirus, detaljne informacije o sustavu i procesima koji se izvršavaju (dnevnik značajke ESET SysInspector) te podaci iz registra. ESET te podatke koristi isključivo za osiguranje tehničke podrške za korisnike.

Nakon što pošaljete web-obrazac, tvrtki ESET bit će poslani podaci o konfiguraciji vašeg sustava. Odaberite opciju **Uvijek pošalji ove podatke** ako želite da se ta radnja zapamti za ovaj proces. Za slanje web obrasca bez slanja podataka kliknite **Ne šalji podatke** i nastavite.

Slanje podataka o konfiguraciji sustava možete konfigurirati u stavci Napredno podešavanje > **Alati** > **Dijagnostika** > Tehnička podrška.

Ako ste odlučili poslati podatke o konfiguraciji sustava, potrebno je ispuniti i poslati web-obrazac. U protivnom se kartica neće izraditi, a podaci o konfiguraciji sustava bit će izgubljeni. Ako se podaci o konfiguraciji sustava ne mogu poslati, popunite web-obrazac i pričekajte upute tehničke podrške.

Tehnička podrška

U glavnom prozoru programa kliknite **Pomoć i podrška** > **Tehnička podrška**.

Obratite se tehničkoj podršci

Zatražite podršku – ako ne možete pronaći odgovor na svoj problem, možete upotrijebiti ovaj obrazac koji se nalazi na web stranici tvrtke ESET da biste se brzo obratili ESET-ovoj tehničkoj podršci. Na temelju vaših postavki, prozor Pošalji podatke o konfiguraciji sustava prikazat će se prije ispunjavanja web obrasca.

Potražite informacije za tehničku podršku

Detalji za tehničku podršku – kada vam se prikaže upit, možete kopirati i poslati informacije ESET-ovoj tehničkoj podršci (kao što su detalji o licenci, naziv programa, verzija programa, operacijski sustav i podaci o računalu).

ESET Log Collector – Veza na članak iz ESET-ove baze znanja na kojem možete preuzeti uslužni alat ESET Log Collector, aplikaciju koja automatski prikuplja informacije i dnevnike s računala i omogućuje brže rješavanje problema. Za više informacija pogledajte mrežni korisnički priručnik za ESET Log Collector.

Aktivirajte **Napredno vođenje dnevnika** za izradu naprednih dnevnika za sve dostupne funkcije kako biste pomogli programerima u dijagnozi i rješavanju problema. Minimalna opširnost vođenja dnevnika postavljena je na razinu **Dijagnostičko**. Napredno vođenje dnevnika automatski će biti deaktivirano nakon dva sata, osim ako ga ne zaustavite ranije klikom na **Zaustavi napredno vođenje dnevnika**. Nakon što se izrade svi dnevnici, prikazat će se prozor obavijesti koji pruža izravan pristup mapi Dijagnostike s izrađenim dnevnicima.

Napredno podešavanje

Napredno postavljanje omogućuje vam konfiguriranje detaljnih ESET Endpoint Antivirus postavki prema vašim potrebama.

Da biste otvorili Napredno podešavanje, otvorite prozor glavnog programa i pritisnite tipku **F5** na tipkovnici ili kliknite **Podešavanje** > **Napredno podešavanje**.

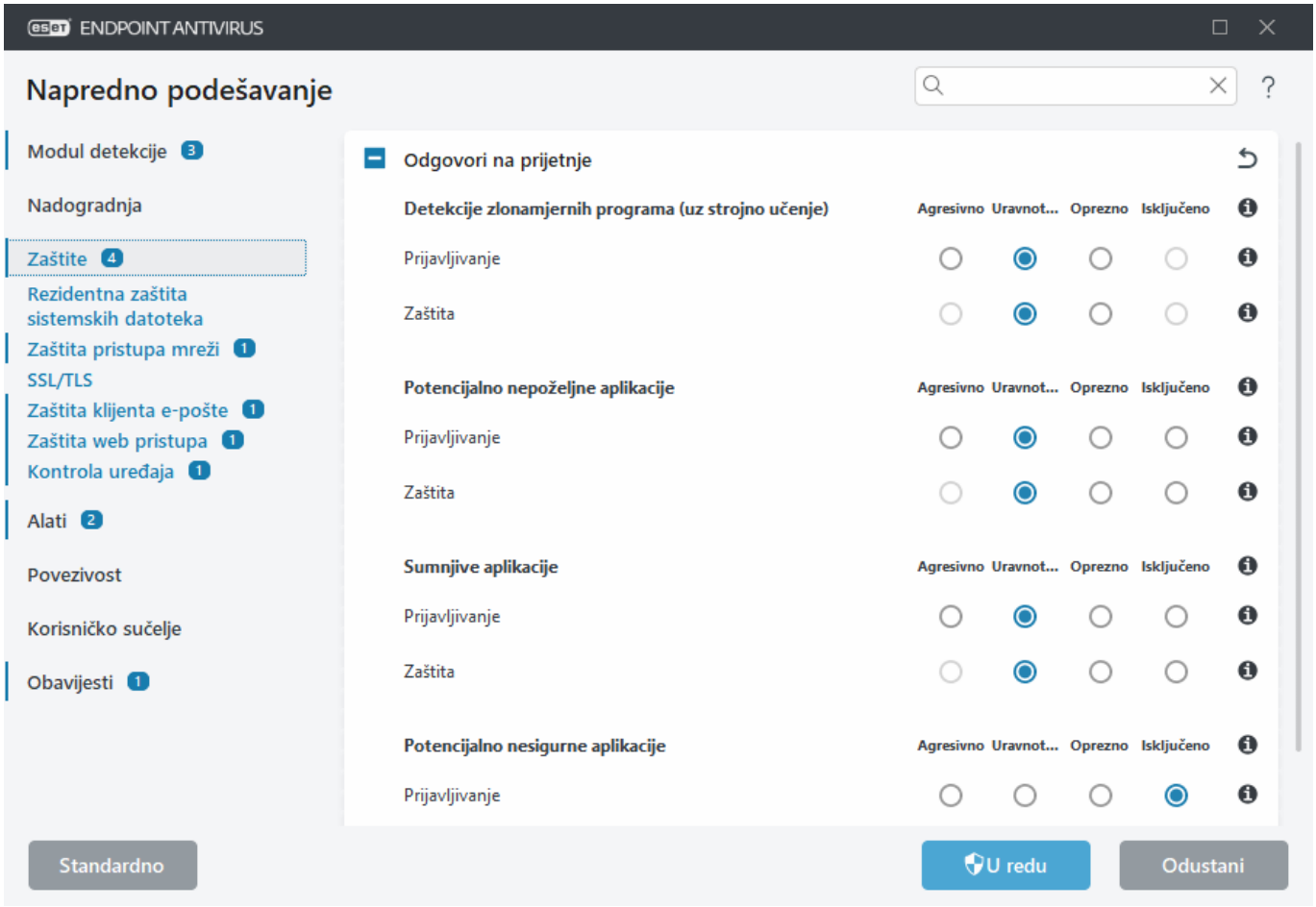
Prilikom stvaranja pravila u ESET PROTECT web konzoli možete odabrati zastavicu za svaku postavku. Postavke sa zastavicom "Obavezno primijeni" imaju prioritet i ne može ih prebrisati novije pravilo (čak i kada novo pravilo ima zastavicu "Obavezno primijeni"). Tako se osigurava da se ta postavka ne promijeni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

Na temelju postavljenog pristupa od vas će se možda zatražiti da upišete lozinku da biste otvorili Napredno podešavanje.

U Naprednom podešavanju možete konfigurirati sljedeće postavke:

- Modul detekcije

- Nadogradnja
- Zaštite
- Alati
- Povezivost
- Korisničko sučelje
- Obavijesti



Modul detekcije

Napredno podešavanje > **Modul detekcije** omogućuje konfiguriranje sljedećih opcija:

- Izuzeci
- Napredne opcije
- Skener mrežnog prometa

Izuzeci

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

Izuzeci radi poboljšanja performansi – izuzimaju datoteke i mape od skeniranja. Izuzeci radi poboljšanja performansi korisni su za izuzimanje skeniranja aplikacija za igranje na razini datoteke ili kada uzrokuju

nenormalno ponašanje sustava ili radi poboljšanja performansi.

Izuzeci detekcija poznatih prijetnji – izuzimaju objekte od čišćenja pomoću naziva prijetnje, puta ili hasha. Izuzeci detekcija poznatih prijetnji ne izuzimaju datoteke i mape iz skeniranja kao izuzetke radi poboljšanja performansi. Izuzeci detekcija poznatih prijetnji izuzimaju objekte samo kada ih otkrije modul detekcije i kad se na popisu izuzetaka nalazi odgovarajuće pravilo.

Ne smiju se pomiješati s drugim vrstama izuzetaka:

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

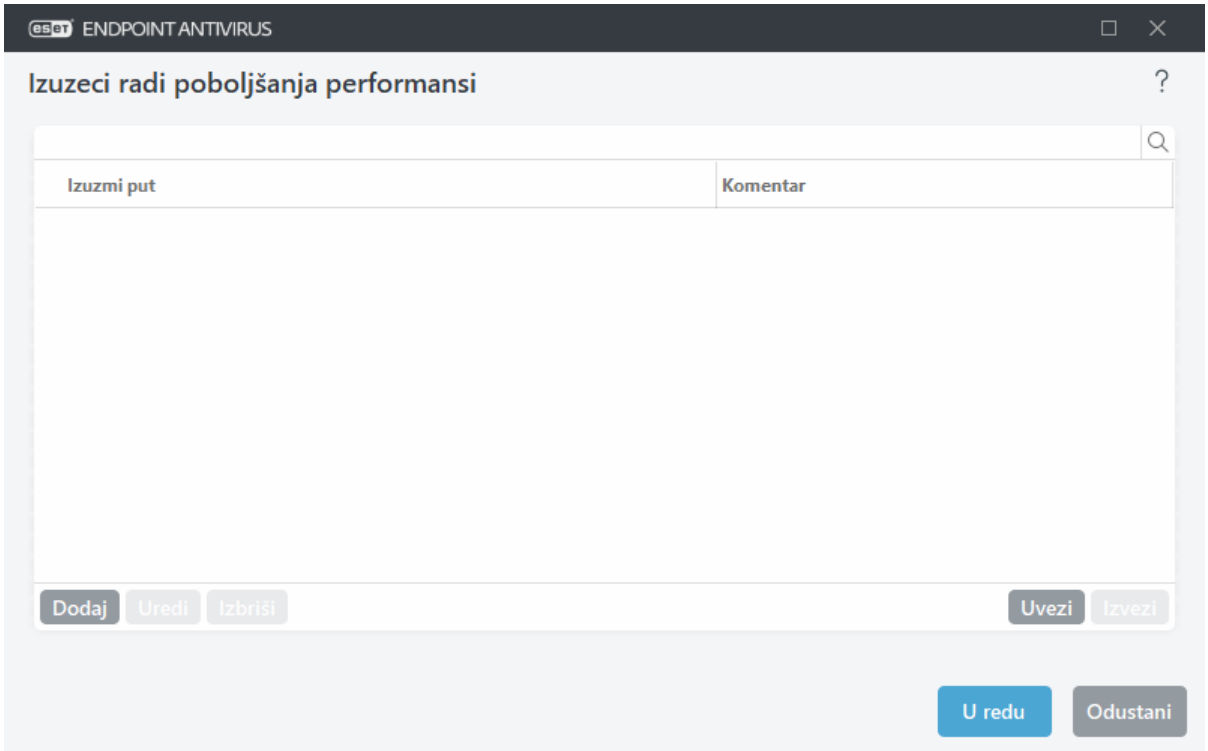
Izuzeci radi poboljšanja performansi

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

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

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

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



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

Kontrolni elementi

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

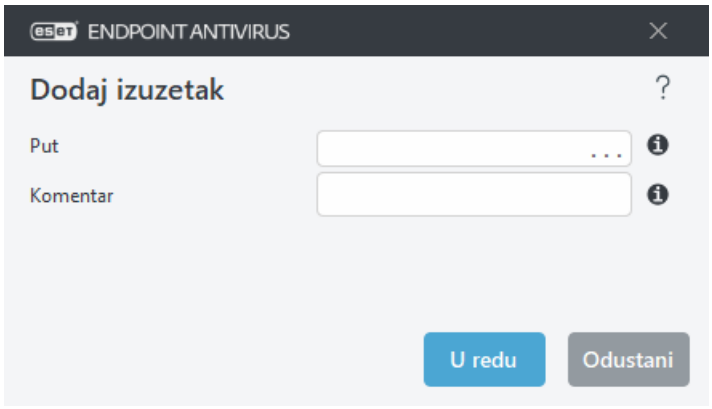
  Prikaz primjera formata datoteke za uvoz/izvoz

```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}

C:\Backup\*,custom comment

C:\pagefile.sys
```

Dodavanje ili uređivanje izuzetka radi poboljšanja performansi

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

Odaberite odgovarajući put tako da kliknete **...** u polju **Put**.
Kada unosite ručno, više primjera formata izuzetaka nalazi se u nastavku.



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

• Ako želite izuzeti sve datoteke i podmape u mapi, upišite put do mape i upotrijebite masku *
• Ako želite izuzeti samo datoteke s ekstenzijom doc, upotrijebite masku *.doc.
• Ako se naziv izvršne datoteke sastoji od određenog broja znakova (koji se međusobno razlikuju) i sigurni ste samo u prvi znak (primjerice "D"), upotrijebite sljedeći format:
D????.exe (upitnici zamjenjuju znakove koji nedostaju ili znakove koji su nepoznati)
Primjeri:
• *C:\Tools** – Put mora završiti obrnutom kosom crtom (\) i zvjezdicom (*) da bi se naznačilo da se radi o mapi te da će se sav sadržaj u mapi (datoteke i podmape) izuzeti.
• *C:\Tools*.** – Isto ponašanje kao *C:\Tools**
• *C:\Tools* – Mapa *Tools* neće biti izuzeta. Iz perspektive skenera, *Tools* može biti i naziv datoteke.
• *C:\Tools*.dat* – Izuzet će se .dat datoteke u mapi *Tools*.
• *C:\Tools\sg.dat* –Izuzet će se ova specifična datoteka koja se nalazi na točno tom putu.

Za definiranje izuzetaka od skeniranja možete upotrijebiti varijable sustava, primjerice *%PROGRAMFILES%*.
• Da biste izuzeli mapu Programske datoteke pomoću ove varijable sustava, upotrijebite put *%PROGRAMFILES%** (zapamtite dodati obrnutu kosu crtu I zvjezdicu na kraju puta) prilikom dodavanja izuzetaka.
• Da biste izuzeli sve datoteke i mape u podmapi *%PROGRAMFILES%*, upotrijebite put *%PROGRAMFILES%\Excluded_Directory**

Proširivanje popisa podržanih varijabla sustava

Sljedeće se varijable mogu upotrebljavati u formatu izuzetaka puta:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Varijable sustava specifične za korisnika (primjerice *%TEMP%* ili *%USERPROFILE%*) ili varijable okruženja (primjerice *%PATH%*) nisu podržane.

Upotreba zamjenskih znakova u sredini puta (na primjer, *C:\Tools*\Data\file.dat*) može funkcionirati, ali nije službeno podržana za izuzetke radi poboljšanja performansi. Pročitajte sljedeći članak iz baze znanja za više informacija.
Nema ograničenja upotrebe zamjenskih znakova usred puta kad upotrebljavate izuzetke detekcija poznatih prijetnji.

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

Format izuzetaka puta

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

• Ako želite izuzeti sve datoteke i podmape u mapi, upišite put do mape i upotrijebite masku *
• Ako želite izuzeti samo datoteke s ekstenzijom doc, upotrijebite masku *.doc.
• Ako se naziv izvršne datoteke sastoji od određenog broja znakova (koji se međusobno razlikuju) i sigurni ste samo u prvi znak (primjerice "D"), upotrijebite sljedeći format:
D????.exe (upitnici zamjenjuju znakove koji nedostaju ili znakove koji su nepoznati)
Primjeri:
• *C:\Tools** – Put mora završiti obrnutom kosom crtom (\) i zvjezdicom (*) da bi se naznačilo da se radi o mapi te da će se sav sadržaj u mapi (datoteke i podmape) izuzeti.
• *C:\Tools*.** – Isto ponašanje kao *C:\Tools**
• *C:\Tools* – Mapa *Tools* neće biti izuzeta. Iz perspektive skenera, *Tools* može biti i naziv datoteke.
• *C:\Tools*.dat* – Izuzet će se .dat datoteke u mapi *Tools*.
• *C:\Tools\sg.dat* –Izuzet će se ova specifična datoteka koja se nalazi na točno tom putu.

Za definiranje izuzetaka od skeniranja možete upotrijebiti varijable sustava, primjerice *%PROGRAMFILES%*.
• Da biste izuzeli mapu Programske datoteke pomoću ove varijable sustava, upotrijebite put *%PROGRAMFILES%** (zapamtite dodati obrnutu kosu crtu I zvjezdicu na kraju puta) prilikom dodavanja izuzetaka.
• Da biste izuzeli sve datoteke i mape u podmapi *%PROGRAMFILES%*, upotrijebite put *%PROGRAMFILES%\Excluded_Directory**

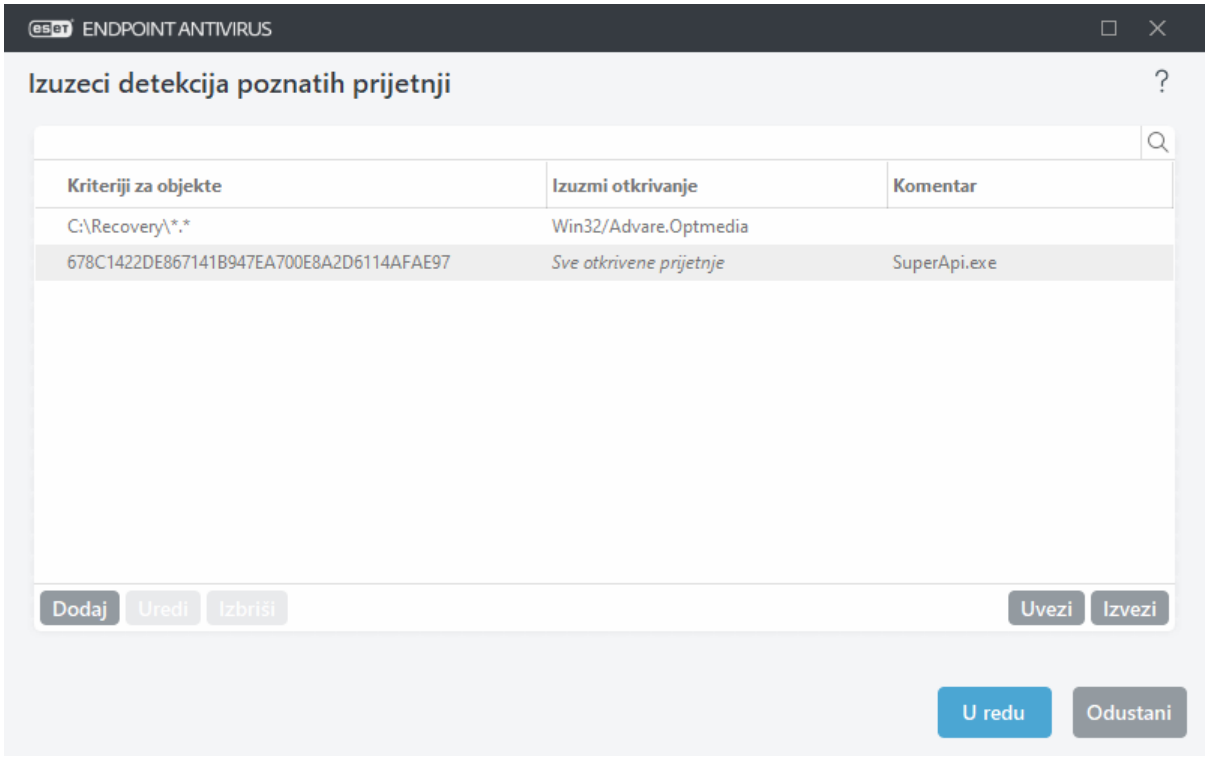
Proširivanje popisa podržanih varijabla sustava

Sljedeće se varijable mogu upotrebljavati u formatu izuzetaka puta:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Varijable sustava specifične za korisnika (primjerice *%TEMP%* ili *%USERPROFILE%*) ili varijable okruženja (primjerice *%PATH%*) nisu podržane.

Izuzeci detekcija poznatih prijetnji

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

Izuzeci detekcija poznatih prijetnji ne izuzimaju datoteke i mape iz skeniranja kao Izuzetke radi poboljšanja performansi. Izuzeci detekcija poznatih prijetnji izuzimaju objekte samo kada ih otkrije modul detekcije i kad se na popisu izuzetaka nalazi odgovarajuće pravilo.
Na (pogledajte prvi red na slici u nastavku), kad se objekt otkrije kao Win32/Adware.Optmedia i otkrivena je datoteka *C:\Recovery\file.exe*. U drugom redu svaka datoteka koja ima odgovarajući hash SHA-1 uvijek će biti izuzeta, bez obzira na naziv prijetnje.



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

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

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

Izuzetak prema nazivu prijetnje za potencijalno nepoželjne aplikacije i potencijalno nesigurne aplikacije može se stvoriti i na sljedeće načine:

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

Kriteriji za objekte koji su izuzete otkrivene prijetnje

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

Kontrolni elementi

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

  Prikaz primjera formata datoteke za uvoz/izvoz

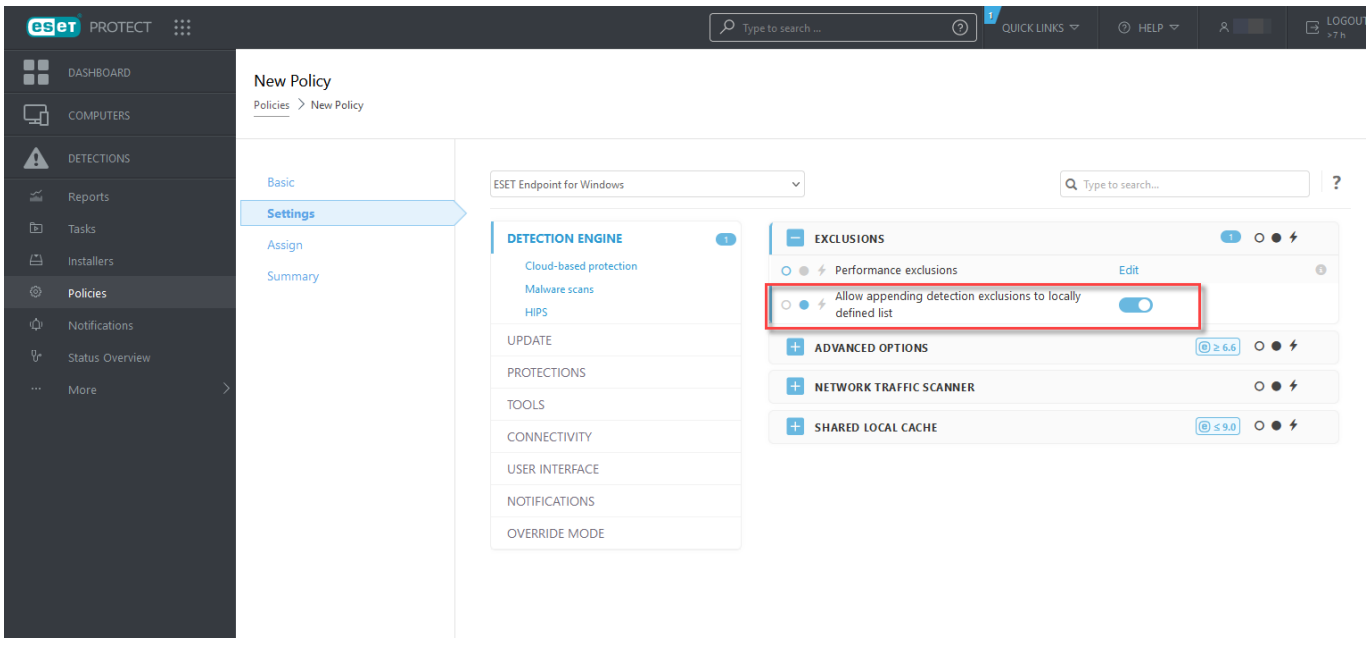
```
# {"product":"endpoint","version":"10.0.2034","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","File Hash"]}

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

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

Podešavanje izuzetih otkrivenih prijetnji u programu ESET PROTECT

Čarobnjak za upravljanje izuzecima detekcije poznatih prijetnji programa ESET PROTECT — stvorite izuzetak detekcije poznatih prijetnji i primijenite ga na više računala/grupa.

Moguće nadjačavanje izuzetih otkrivenih prijetnji iz programa ESET PROTECT

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

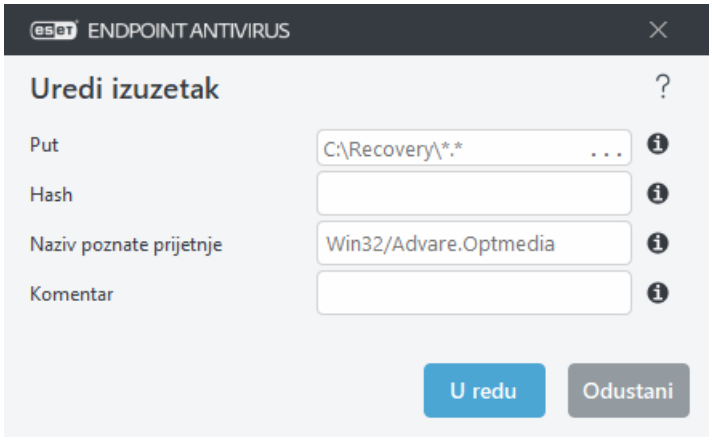


Dodavanje ili uređivanje izuzetih detekcija poznatih prijetnji

Izuzmi otkrivanje

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

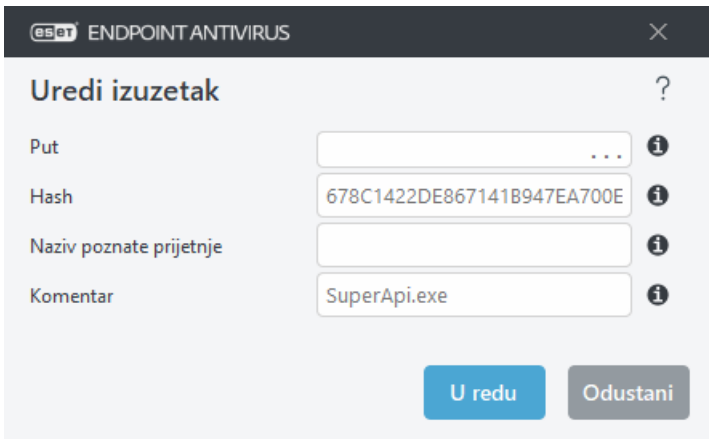
Također pogledajte Format izuzetaka puta.



Pogledajte primjer izuzetih detekcija poznatih prijetnji u nastavku.

Izuzmi hash

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



Da biste izuzeli određenu prijetnju prema nazivu, unesite valjani naziv otkrivene prijetnje: *Win32/Adware.Optmedia*
Kada izuzimate otkrivenu prijetnju iz prozora upozorenja programa ESET Endpoint Antivirus, možete upotrijebiti i sljedeći format:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Kontrolni elementi

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

Čarobnjak za stvaranje izuzetih detekcija poznatih prijetnji

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

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

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

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

Preporučena opcija unaprijed je odabrana na temelju prijetnje.

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

Napredne opcije modula detekcije

Aktiviraj napredno skeniranje putem AMSI-ja je alat Microsoft Antimalware Scan Interface koji omogućuje skeniranje PowerShell skripta, skripta koje pokreće Windows Script Host i podataka koji su skenirani pomoću AMSI SDK-a.

Skener mrežnog prometa

Skener mrežnog prometa pruža zaštitu od zlonamjernog softvera za aplikacijske protokole integracijom više naprednih tehnika skeniranja zlonamjernog softvera. Skener mrežnog prometa automatski skenira HTTP(S), POP3(S) i IMAP(S) protokole, bez obzira na internetski preglednik ili klijent e-pošte. Skener mrežnog prometa možete aktivirati/deaktivirati u stavci Napredno podešavanje > **Modul detekcije** > **Skener mrežnog prometa**.

Aktiviraj skener mrežnog prometa – ako deaktivirate tu mogućnost, HTTP(S), POP3(S) i IMAP (S) protokoli neće se skenirati. Imajte na umu da je za sljedeće ESET Endpoint Antivirus značajke aktiviran skener mrežnog prometa:

- Zaštita web pristupa
- SSL/TLS
- Anti-phishing zaštita
- zaštita klijenta e-pošte

Zaštita na bazi clouda

ESET LiveGrid® (konstruiran na temelju naprednog sustava ranog upozorenja ESET ThreatSense.Net) prikuplja podatke koje šalju korisnici ESET-ovih programa diljem svijeta i prosljeđuje ih u Laboratorij za istraživanje tvrtke ESET. Pružanjem sumnjivih uzoraka i metapodataka ESET LiveGrid® omogućuje nam da brzo reagiramo na potrebe svojih korisnika i da održimo ESET-ovu sposobnost reagiranja na najnovije prijetnje.

Dostupne su sljedeće opcije:

Opcija 1: aktiviraj sustav reputacije ESET LiveGrid®

Sustav reputacije ESET LiveGrid® omogućuje stvaranje popisa pouzdanih i nepoželjnih adresa na temelju cloud tehnologije.

Provjerite reputaciju pokrenutih procesa i datoteka izravno iz sučelja programa ili kontekstnog izbornika uz dodatne informacije koje su dostupne u sustavu ESET LiveGrid®.

Opcija 2: aktiviraj sustav za povratne informacije ESET LiveGrid®

Uz sustav reputacije ESET LiveGrid®, sustav za povratne informacije ESET LiveGrid® prikupljat će informacije o vašem računalu koje se odnose na nove pronađene prijetnje. Te informacije mogu obuhvaćati uzorak ili kopiju datoteke u kojoj se pojavila prijetnja, put do te datoteke, naziv datoteke, datum i vrijeme, proces u kojem se prijetnja pojavila na računalu i informacije o operacijskom sustavu računala.

Prema standardnim je postavkama sustav ESET Endpoint Antivirus konfiguriran tako da šalje sumnjive datoteke na detaljnu analizu u laboratorij tvrtke ESET za otkrivanje virusa. Datoteke s ekstenzijama kao što su *.doc* ili *.xls* uvijek se isključuju. Ako postoje određene datoteke koje vi ili vaša tvrtka ne želite slati, možete dodati i njihove ekstenzije.

Opcija 3: neaktiviranje sustava ESET LiveGrid®

Funkcionalnost softvera ostat će ista, ali u nekim slučajevima ESET Endpoint Antivirus možda će na nove prijetnje reagirati brže od nadogradnje baze podataka virusnih potpisa kada je aktiviran ESET LiveGrid®.

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

Konfiguracija zaštite utemeljene na cloudu u naprednom podešavanju

Da biste pristupili postavkama za ESET LiveGrid®, otvorite Napredno podešavanje > **Modul detekcije** > **Zaštita na bazi clouda**.

Aktiviraj sustav reputacije ESET LiveGrid® (preporučeno) – sustav reputacije ESET LiveGrid® poboljšava učinkovitost ESET-ovih rješenja za zaštitu od zlonamjernog softvera uspoređujući skenirane datoteke s bazom podataka popisa pouzdanih i nepouzdanih adresa u cloudu.

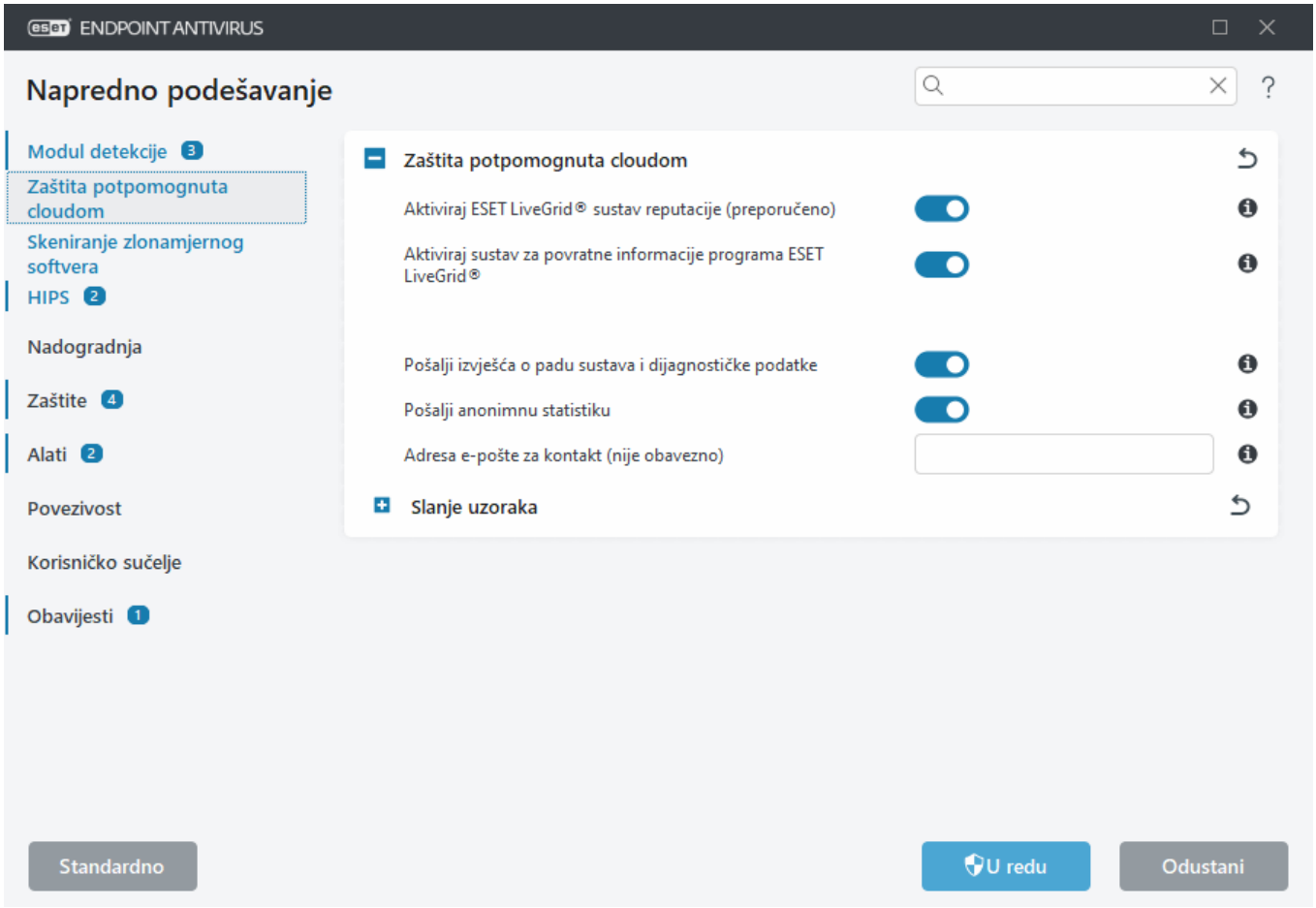
Aktiviraj sustav za povratne informacije ESET LiveGrid® – Šalje laboratoriju tvrtke ESET za istraživanje relevantne podatke (opisane u odjeljku **Slanje uzoraka** u nastavku) uz izvješća o padu sustava i statistiku radi daljnje analize.

Aktiviraj ESET LiveGuard (ESET LiveGuard je dodatna funkcija koju prodaje ESET i nije dostupna prema standardnim postavkama) –ESET LiveGuard je plaćeni servis koji omogućava ESET. Njegova je svrha dodati sloj zaštite koji je posebno osmišljen za ublažavanje novonastalih prijetnji. Sumnjive datoteke automatski se šalju u ESET-ov cloud. U cloudu ih analiziraju naši napredni moduli detekcije zlonamjernih programa. Korisnik koji je pružio uzorak primit će izvješće o ponašanju sa sažetkom ponašanja promatranog uzorka.

Pošalji izvješća o padu sustava i dijagnostičke podatke – Pošaljite dijagnostičke podatke povezane sa sustavom ESET LiveGrid® kao što su izvješća o padu sustava i slike stanja memorije modula. Preporučujemo da ostane aktiviran kako bi pomogao tvrtki ESET u dijagnostici problema, poboljšavanju programa i osiguravanju bolje zaštite krajnjih korisnika.

Pošalji anonimnu statistiku – Dopustite tvrtki ESET da prikupi informacije o novootkrivenim prijetnjama kao što su naziv prijetnje, datum i vrijeme otkrivanja, način otkrivanja i povezani metapodaci, verzija programa i konfiguracija, uključujući informacije o vašem sustavu.

E-pošta za kontakt (nije obavezno) – Vaša adresa e-pošte za kontakt može se uključiti uz sumnjive datoteke i može se koristiti ako za analizu budu potrebne dodatne informacije. Imajte na umu da vam ESET neće slati odgovor ako ne budu potrebne dodatne informacije.



Slanje uzoraka

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

Automatsko slanje otkrivenih uzoraka

Odaberite vrstu uzoraka koji će se slati tvrtki ESET na analizu i poboljšajte buduće otkrivanje prijetnji. Dostupne su sljedeće opcije:

- **Svi otkriveni uzorci** – svi objekti koje otkrije modul detekcije (uključujući potencijalno nepoželjne aplikacije kada je to aktivirano u postavkama skenera).
- **Svi uzorci osim dokumenata** – Svi otkriveni objekti osim **dokumenata** (pogledajte u nastavku).
- **Ne šalji** – Otkriveni objekti neće se poslati tvrtki ESET.

Automatsko slanje sumnjivih uzoraka

Ti uzorci će se također poslati ESET-u ako ih ne otkrije modul detekcije. Na primjer, uzorci koji gotovo nisu otkriveni ili uzorci koje jedan od modula zaštite programa ESET Endpoint Antivirus smatra sumnjivima ili nejasnima.

- **Izvršne datoteke** – Uključuje datoteke poput .exe, .dll, .sys.
- **Arhive** – Uključuje vrste datoteka poput .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Skripte** – Uključuje vrste datoteka poput .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Ostalo** – Uključuje vrste datoteka poput .jar, .reg, .msi, .sfw, .lnk.
- **Moguće neželjene poruke e-pošte** – Time će se omogućiti slanje mogućih neželjenih dijelova ili cjelovitih

neželjenih poruka e-pošte s privicima tvrtki ESET radi daljnje analize. Aktiviranjem ove opcije poboljšava se globalno otkrivanje neželjene pošte, kao i buduće otkrivanje vaše neželjene pošte.

- **Dokumenti** – Uključuje dokumente programa Microsoft Office ili PDF s aktivnim sadržajem ili bez njega.

Proširivanje popisa svih obuhvaćenih vrsta datoteka dokumenata

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Izuzeci

Filtar izuzetaka omogućuje vam da izuzmete određene datoteke/mape od slanja (primjerice, možete izuzeti datoteke koje mogu sadržavati povjerljive informacije, kao što su dokumenti ili proračunske tablice). Datoteke s popisa nikada se neće slati u laboratorije tvrtke ESET na analizu, čak ni ako sadrže sumnjiv kod. Najčešće vrste datoteka izostavljaju se prema standardnim postavkama (.doc itd.). Ako želite, na popis izuzetih datoteka možete dodati druge datoteke.

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

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

ESET LiveGuard

Za aktiviranje servisa ESET LiveGuard na klijentskom računalu pomoću ESET PROTECT web konzole pogledajte ESET LiveGuard konfiguraciju za ESET Endpoint Antivirus.

Ako ste ranije koristili sustav ESET LiveGrid® i deaktivirali ste ga, možda još uvijek ima pakete podataka koje treba poslati. Ti će se paketi slati tvrtki ESET čak i nakon deaktivacije. Nakon što sve trenutačne informacije budu poslane novi se paketi neće stvarati.

Filtar izuzetaka za zaštitu na bazi clouda

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

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

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

Skeniranja za zlonamjerne softvere

Odjeljak **Skeniranje zlonamjernog softvera** dostupan je u prozoru Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernog softvera**i dopušta vam konfiguriranje parametara skeniranja za profile skeniranja.

Skeniranje na zahtjev

Odabrani profil – Određeni skup parametara koje upotrebljava skener na zahtjev. Da biste stvorili novi profil, kliknite **Uredi** pored stavke **Popis profila**. Za više detalja pogledajte Profili skeniranja.

Kada odaberete profil skeniranja, možete konfigurirati sljedeće mogućnosti:

Ciljevi skeniranja – ako želite skenirati samo određeni cilj ili grupu ciljeva kliknite **Uredi** pored opcije **Ciljevi skeniranja** i odaberite jednu od opcija iz mape (stablaste strukture). Za više detalja pogledajte Ciljevi skeniranja.

Na zahtjev i Zaštita strojnog učenja – možete konfigurirati razine izvješćivanja i zaštite za svaki profil skeniranja. Prema zadanim postavkama profili skeniranja koriste istu postavku definiranu u stavki Rezidentna zaštita sistemskih datoteka. Deaktivirajte klizač uz stavku **Koristi postavke rezidentne zaštite** da biste konfigurirali prilagođene razine izvješćivanja i zaštite. Detaljno objašnjenje razina izvješćivanja i zaštite potražite u odjeljku Zaštita .

ThreatSense – Opcije naprednog podešavanja, kao što su ekstenzije datoteka koje želite kontrolirati i korištene metode detekcije. Za više informacije pogledajte ThreatSense.

Profili skeniranja

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

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

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

Za stvaranje novog profila otvorite stavke Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Skeniranje na zahtjev** > **Popis profila** > **Uredi**. Prozor **Upravljanje profilima** sadrži padajući izbornik **Odabrani profil** s postojećim profilima skeniranja i mogućnošću stvaranja novog. Pomoć pri stvaranju profila skeniranja koji odgovara vašim potrebama potražite u odjeljku ThreatSense, gdje možete pronaći opis svakog parametra podešavanja skeniranja.

> Pretpostavimo da želite stvoriti vlastiti profil skeniranja i djelomično vam odgovara konfiguracija **Skenirajte svoje računalo**, no ne želite skenirati runtime arhivatore ni potencijalno nesigurne aplikacije te želite primijeniti **Uvijek ukloni prijetnju**. Unesite naziv novog profila u prozoru **Upravljanje profilima** i kliknite **Dodaj**. Odaberite novi profil iz padajućeg izbornika **Odabrani profil** i prilagodite preostale parametre kako vam odgovara te kliknite **U redu** da biste spremili novi profil.

Ciljevi skeniranja

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

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

Struktura mape (stablo) također sadrži specifične ciljeve skeniranja.

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

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

Skeniranje u stanju mirovanja

Skener u stanju mirovanja može se aktivirati u stavci Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Skeniranje u stanju mirovanja**.

Skeniranje u stanju mirovanja

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

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

Aktivirajte klizač **Aktiviraj zapisivanje** u prozoru Napredno podešavanje da biste vidjeli rezultate skeniranja računala u odjeljku Dnevnici (u glavnom prozoru programa kliknite **Alati** > **Dnevnici** i odaberite **Skeniranje računala** s padajućeg izbornika **Dnevnik**).

Otkrivanje stanja mirovanja

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

ThreatSense – Opcije naprednog podešavanja, kao što su ekstenzije datoteka koje želite kontrolirati i korištene metode otkrivanja. Za više informacija pogledajte ThreatSense.

Otkrivanje stanja mirovanja

Postavke otkrivanja stanja mirovanja mogu se konfigurirati u stavci Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Skeniranje u stanju mirovanja** > **Otkrivanje stanja mirovanja**. Ove postavke određuju pokretač za Skeniranje u stanju mirovanja:

- **Isključen zaslon ili čuvar zaslona**
- **Zaključano računalo**
- **Odjava korisnika**

Pomoću klizača za svako pojedinačno stanje aktivirajte ili deaktivirajte različite pokretače otkrivanja stanja mirovanja.

Skeniranje pri pokretanju

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

Mogućnosti skeniranja pri pokretanju spadaju pod zadatak planera **Provjera datoteke za pokretanje sustava**. Za izmjenu postavki idite na **Alati** > **Planer** i kliknite **Automatska provjera pokretačke datoteke**, a zatim **Uredi**. U zadnjem koraku prikazat će se prozor Automatska provjera pokretačkih datoteka. Detaljne upute o stvaranju i upravljanju zadacima planera potražite u odjeljku Stvaranje novih zadataka.

ThreatSense – opcije naprednog podešavanja, kao što su ekstenzije datoteka koje želite kontrolirati i korištene metode detekcije. Za više informacija pogledajte ThreatSense.

Automatska provjera pokretačke datoteke

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

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

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

Obuhvaćene su i dvije određene grupe:

- **Datoteke pokrenute prije prijave korisnika** – Sadrži datoteke s mjesta kojima je moguće pristupiti bez prijave korisnika (obuhvaća gotovo sva mjesta za pokretanje kao što su servisi, pomoćni objekti

preglednika, obavijesti procesa Winlogon, stavke planera sustava Windows, poznati dll-ovi itd).

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

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

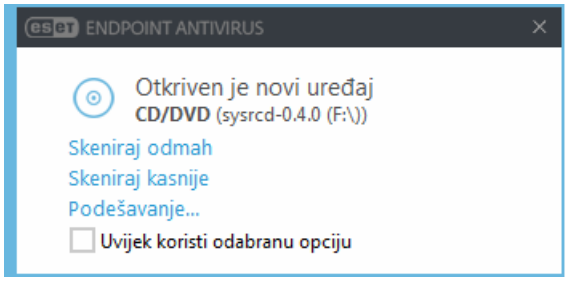
Prioritet provjere – Razina prioriteta pomoću koje se određuje kada započeti skeniranje:

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

Izmjenjivi mediji

ESET Endpoint Antivirus pruža automatsko skeniranje izmjenjivih medija (CD/DVD/USB/...) prilikom umetanja u računalo. To može biti korisno ako administrator računala želi korisnicima zabraniti uporabu izmjenjivih medija na kojima se nalazi nedopušten sadržaj.

Nakon umetanja izmjenjivog medija i podešavanja opcije **Prikaz opcija skeniranja** u prozoru Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernog softvera** > **Izmjenjivi mediji** prikazat će se sljedeći dijaloški okvir:



Opcije za ovaj prozor:

- **Skeniraj odmah** – Pokreće skeniranje izmjenjivih medija.
- **Ne skeniraj** – izmjenjivi mediji neće se skenirati.
- **Podešavanje** – Otvara napredno podešavanje.
- **Uvijek koristi odabranu opciju** – Ako je odabrana ova opcija, ista će se radnja izvršiti i kada se izmjenjivi medij umetne i drugi put.

Osim toga, ESET Endpoint Antivirus sadrži funkciju kontrole uređaja, koja pruža mogućnost definiranja pravila za korištenje vanjskih uređaja na određenom računalu. Dodatne pojedinosti o kontroli uređaja možete pronaći u odjeljku Kontrola uređaja.

Otvorite Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Izmjenjivi mediji** da biste pristupili postavkama skeniranja izmjenjivih medija.

Radnja koju treba napraviti nakon umetanja izmjenjivih medija – Odaberite standardnu radnju koja će se provesti kada se dostupan izmjenjivi medijski uređaj umetne u računalo (CD/DVD/USB). Odaberite željenu radnju nakon umetanja izmjenjivog medija u računalo:

- **Ne skeniraj** – Neće se provesti nikakva radnja i prozor **Prepoznat je novi uređaj** neće se otvoriti.
- **Automatsko skeniranje uređaja** – Provest će se skeniranje računala za umetnuti izmjenjivi medij.
- **Prisilno skeniranje uređaja** – provest će se skeniranje računala za umetnuti izmjenjivi medij i ne može se odustati od njega.
- **Prikaz mogućnosti skeniranja** – Otvara odjeljak podešavanja **izmjenjivih medija**.

Zaštita dokumenata

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

Da biste aktivirali zaštitu dokumenata, otvorite prozor Napredno podešavanje > **Modul detekcije** > **Skeniranje zlonamjernih programa** > **Zaštita dokumenata** i kliknite klizač uz opciju **Aktiviraj zaštitu dokumenata**.

ThreatSense – Opcije postavljanja naprednog podešavanja, kao što su ekstenzije datoteka koje želite kontrolirati i korištene metode detekcije. Pogledajte ThreatSense za više informacija.

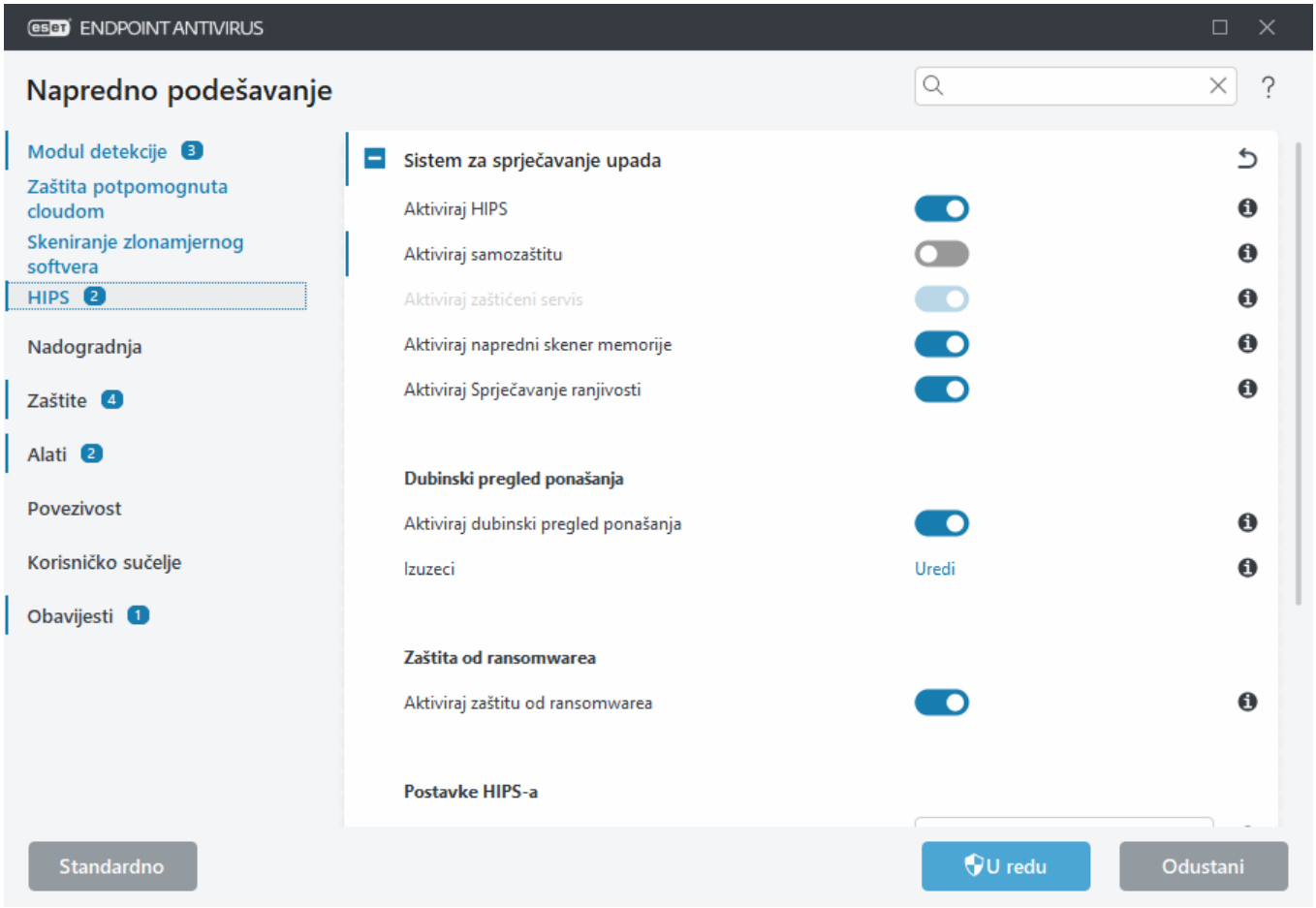
Tu funkciju aktiviraju aplikacije koje upotrebljavaju Microsoft Antivirus API (npr. sustav Microsoft Office 2000 i novije verzije ili preglednik Microsoft Internet Explorer 5.0 i novije verzije).

HIPS – sistem za sprečavanje upada)

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

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

Postavke za HIPS možete konfigurirati u stavci Napredno podešavanje > **Modul detekcije** > **HIPS** > **Sistem za sprječavanje upada**. Stanje značajke HIPS (aktivirano/deaktivirano) prikazuje se u stavci ESET Endpoint Antivirus prozor glavnog programa > **Podešavanje** > **Računalo**.



Sistem za sprječavanje upada

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

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

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

Aktiviraj napredni skener memorije – Radi zajedno sa sprječavanjem ranjivosti radi bolje zaštite od zlonamjernih programa koji su osmišljeni tako da skrivanjem i šifriranjem izbjegavaju da ih otkriju programi za zaštitu od zlonamjernih programa. Prema standardnim postavkama napredni je skener memorije aktiviran. Više o toj vrsti zaštite pročitajte u rječniku.

Aktiviraj zaštitu od zloupotrebe – Osmišljena je za ojačavanje zaštite često zloupotrebljavanih vrsta aplikacija kao što su web preglednici, PDF čitači, klijenti e-pošte i komponente sustava MS Office. Sprječavanje ranjivosti aktivirano je prema standardnim postavkama. Više o toj vrsti zaštite pročitajte u rječniku.

Dubinski pregled ponašanja

Aktiviraj dubinski pregled ponašanja – dodatan sloj zaštite u sklopu funkcije HIPS. Ova ekstenzija HIPS-a analizira

ponašanje svih programa pokrenutih na računalu i upozorava vas ako je ponašanje nekog procesa zloćudno.

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

Zaštita od ransomwarea

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

Aktiviraj Intel® Threat Detection Technology – pomaže u otkrivanju napada ransomwarea upotrebom jedinstvene telemetrije Intel CPU-a za povećanje učinkovitosti detekcija, smanjenje broja lažno pozitivnih upozorenja i proširenje vidljivosti kako bi se obuhvatile napredne tehnike izbjegavanja. Pogledajte podržane procesore.

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

Postavke HIPS-a

Način filtriranja može se izvesti na jedan od sljedećih načina:

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

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

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

možete pronaći u odjeljku Uređivanje HIPS pravila.

Izuzeci iz HIPS-a

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

Da biste uredili izuzetske iz HIPS-a, otvorite prozor Napredno podešavanje > **Modul detekcije** > **HIPS** > **Sistem za sprječavanje upada** > **Izuzeci** > **Uredi**.

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

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

HIPS napredno podešavanje

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

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

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

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

Upravljački programi koji se uvijek smiju učitati

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

Dodaj – Dodaje novi upravljački pogon.

Uredi – Uređuje odabrani upravljački pogon.

Ukloni – Uklanja upravljački pogon s popisa.

Poništi – Ponovno učitava skup upravljačkih programa sustava.

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

> Nakon instalacije popis upravljačkih programa je prazan. ESET Endpoint Antivirus s vremenom automatski ispunjava popis.

Upravljački programi kojima je uvijek dopušteno učitavanje specifični su za svaki uređaj i ne mogu se uređivati pomoću pravila za ESET PROTECT. Nakon instalacije popis upravljačkih programa je prazan. ESET Endpoint Antivirus s vremenom automatski ispunjava popis.

HIPS interaktivni prozor

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

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

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

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

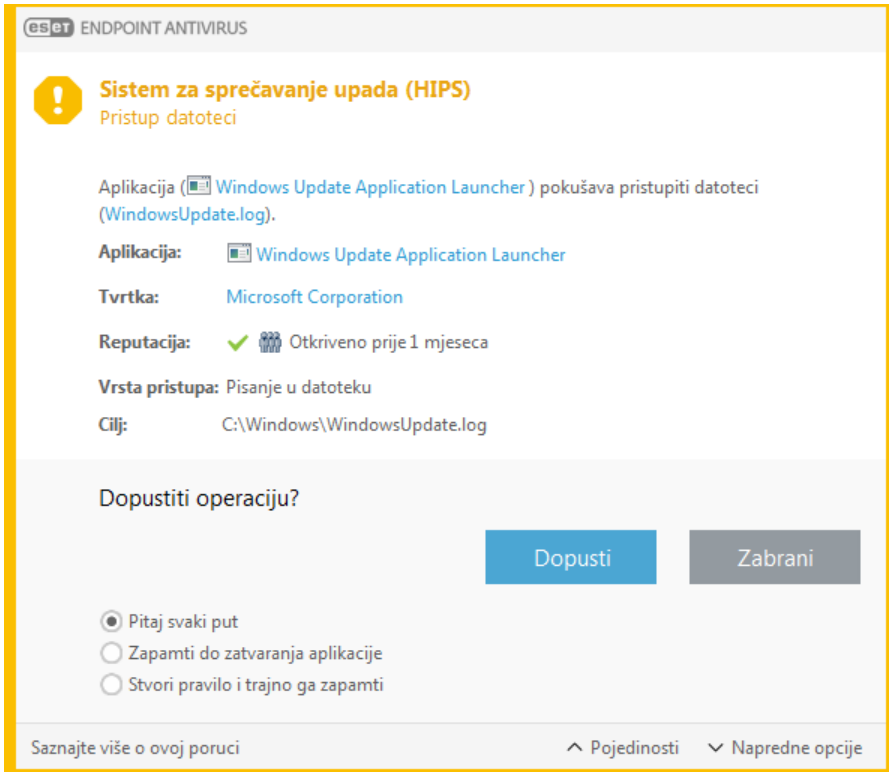
Opcija **Stvori pravilo i trajno ga zapamti** stvorit će novo HIPS pravilo koje se kasnije može mijenjati u odjeljku HIPS upravljanje pravilima (potrebne administratorske ovlasti).

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

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

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

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



Otkriveno je moguće ponašanje ransomwarea

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

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

ESET LiveGrid® mora biti aktiviran kako bi zaštita od ransomwarea ispravno radila.

HIPS upravljanje pravilima

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

Stupci

Pravilo – Korisnički definiran ili automatski odabran naziv pravila.

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

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

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

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

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

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

Kontrolni elementi

Dodaj – Stvara novo pravilo.

Uredi – Omogućuje vam uređivanje odabranih unosa.

Izbriši – Uklanja odabrane unose.

Prioriteti za HIPS pravila

Ne postoje opcije za podešavanje razine prioriteta HIPS pravila pomoću gumba gore/dolje.

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

Postavke HIPS pravila

Najprije pogledajte upravljanje HIPS pravilima.

Naziv pravila – Korisnički definiran ili automatski odabran naziv pravila.

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

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

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

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

Obavijesti korisnika – U donjem desnom kutu prikazat će se obavijest ako se pokrene događaj.

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

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

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

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

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

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

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

Operacije aplikacija

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

Operacije registra

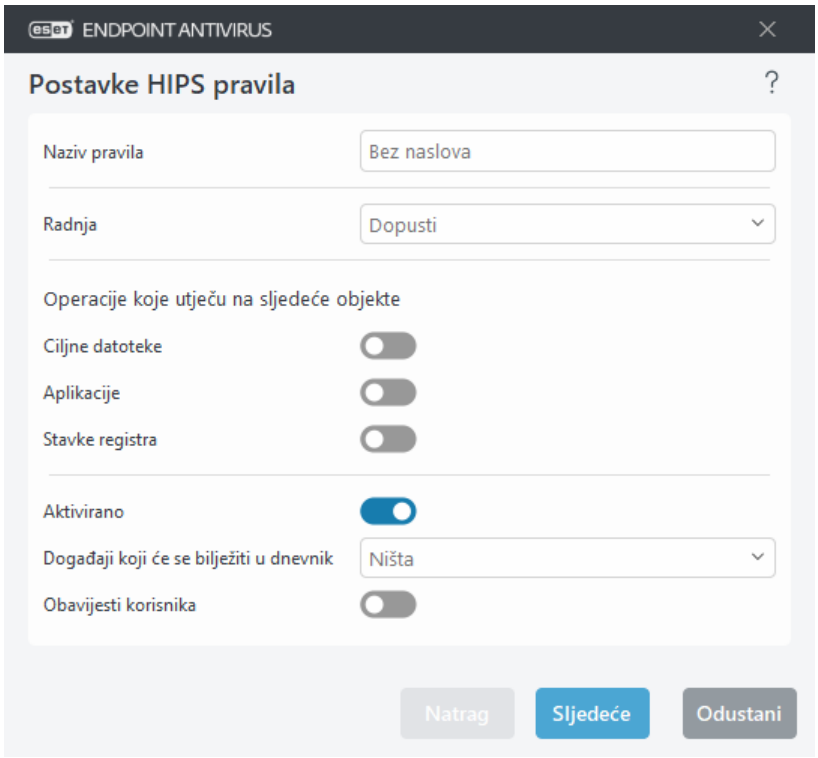
- **Preinači postavke pokretanja** – Bilo koja promjena postavki koja definira koje će se aplikacije pokrenuti prilikom pokretanja sustava Windows. One se mogu pronaći ako se, na primjer, potraži ključ Run u registru sustava Windows.
- **Izbriši iz registra** – Brisanje ključa registra ili njegove vrijednosti.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

Upotreba zamjenskih znakova u pravilima
Zvjezdica u pravilima može se upotrijebiti isključivo za zamjenu određenog ključa, npr. "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start". Ostali načini upotrebe zamjenskih znakova nisu podržani.
Stvaranje pravila koja se odnose na ključ HKEY_CURRENT_USER
Ovaj je ključ samo link za odgovarajući potključ HKEY_USERS koji je specifičan za korisnika koji se identificira SID-om (sigurnim identifikatorom). Da bi se stvorilo pravilo samo za trenutačnog korisnika, umjesto upotrebe puta do HKEY_CURRENT_USER upotrijebite put do HKEY_USERS\%SID%. Za SID možete upotrijebiti zvjezdicu da bi se pravilo primijenilo na sve korisnike.

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

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

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



Dodavanje puta aplikacije/registra za HIPS

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

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

Primjeri puta datoteke ili registra:

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

- *HKEY_LOCAL_MACHINE\system\ControlSet*

Nadogradnja

Mogućnosti podešavanja ažuriranja dostupne su u prozoru Napredno podešavanje > **Ažuriranje**. U ovom odjeljku navode se informacije o izvoru aktualizacije, na primjer aktualizacijski serveri i podaci za autorizaciju za te servere.

Da bi se aktualizacije pravilno preuzele, važno je pravilno navesti sve parametre. Ako koristite firewall, provjerite je li programu tvrtke ESET dopuštena komunikacija s internetom (npr. komunikacija putem HTTPS-a).

Nadogradnja

Profil nadogradnje koji se trenutačno upotrebljava prikazuje se u padajućem izborniku **Odaberite standardni profil nadogradnje**.

Da biste stvorili novi profil, pogledajte odjeljak Profili nadogradnje.

Konfiguriraj obavijesti o nadogradnjama – kliknite gumb Uredi da biste odabrali koje se obavijesti aplikacije prikazuju. Možete odabrati između opcija Prikaži na radnoj površini i/ili Pošalji e-poštom.

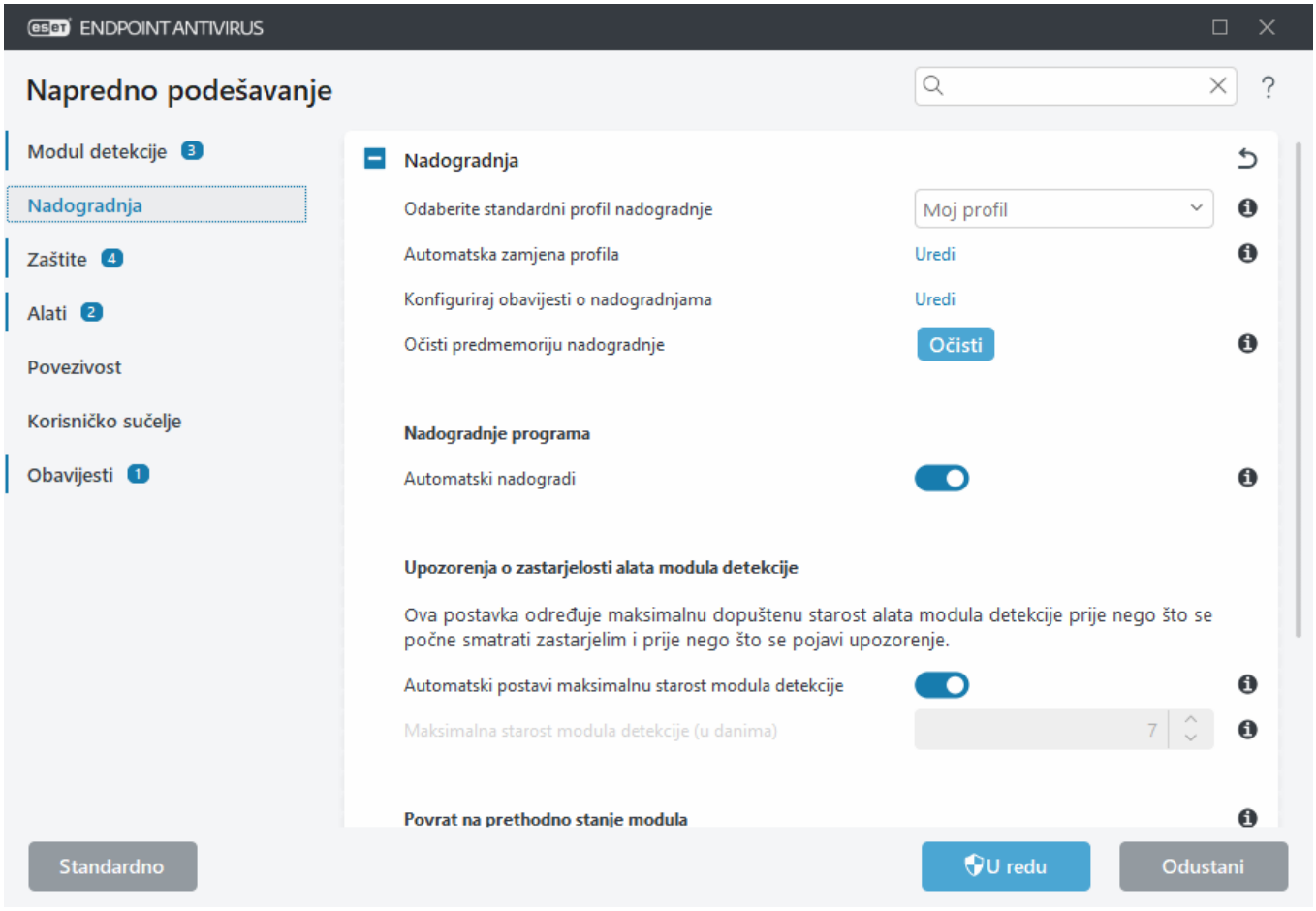
Ako imate poteškoća prilikom preuzimanja nadogradnji modula, kliknite **Očisti** pored stavke **Očisti predmemoriju nadogradnje** da biste izbrisali privremene datoteke/predmemoriju nadogradnje.

Upozorenja o zastarjelosti alata modula detekcije

Automatski postavi maksimalnu starost modula detekcije – Omogućuje postavljanje maksimalnog vremena (u danima) nakon kojeg će se modul za otkrivanje prijaviti kao zastario. Standardna vrijednost **maksimalne starosti modula detekcije (u danima)** iznosi 7 dana.

Povrat na prethodno stanje modula

Ako sumnjate da je nova aktualizacija modula za otkrivanje i/ili modula programa nestabilna ili oštećena, možete se vratiti na prethodnu verziju i na određeno vremensko razdoblje deaktivirati aktualizacije.



Profili

Aktualizacijske profile moguće je stvoriti za različite konfiguracije aktualizacije i zadatke. Stvaranje aktualizacijskih profila posebno je korisno za mobilne korisnike kojima je potreban alternativni profil za internetske veze čija se svojstva redovito mijenjaju.

Padajući izbornik **Odaberi profil za uređivanje** prikazuje trenutačno odabrani profil te je prema standardnim postavkama postavljen na **Moj profil**.

Da biste stvorili novi profil, kliknite **Uredi** uz **Popis profila**, a zatim unesite vlastiti **Naziv profila** te kliknite **Dodaj**.

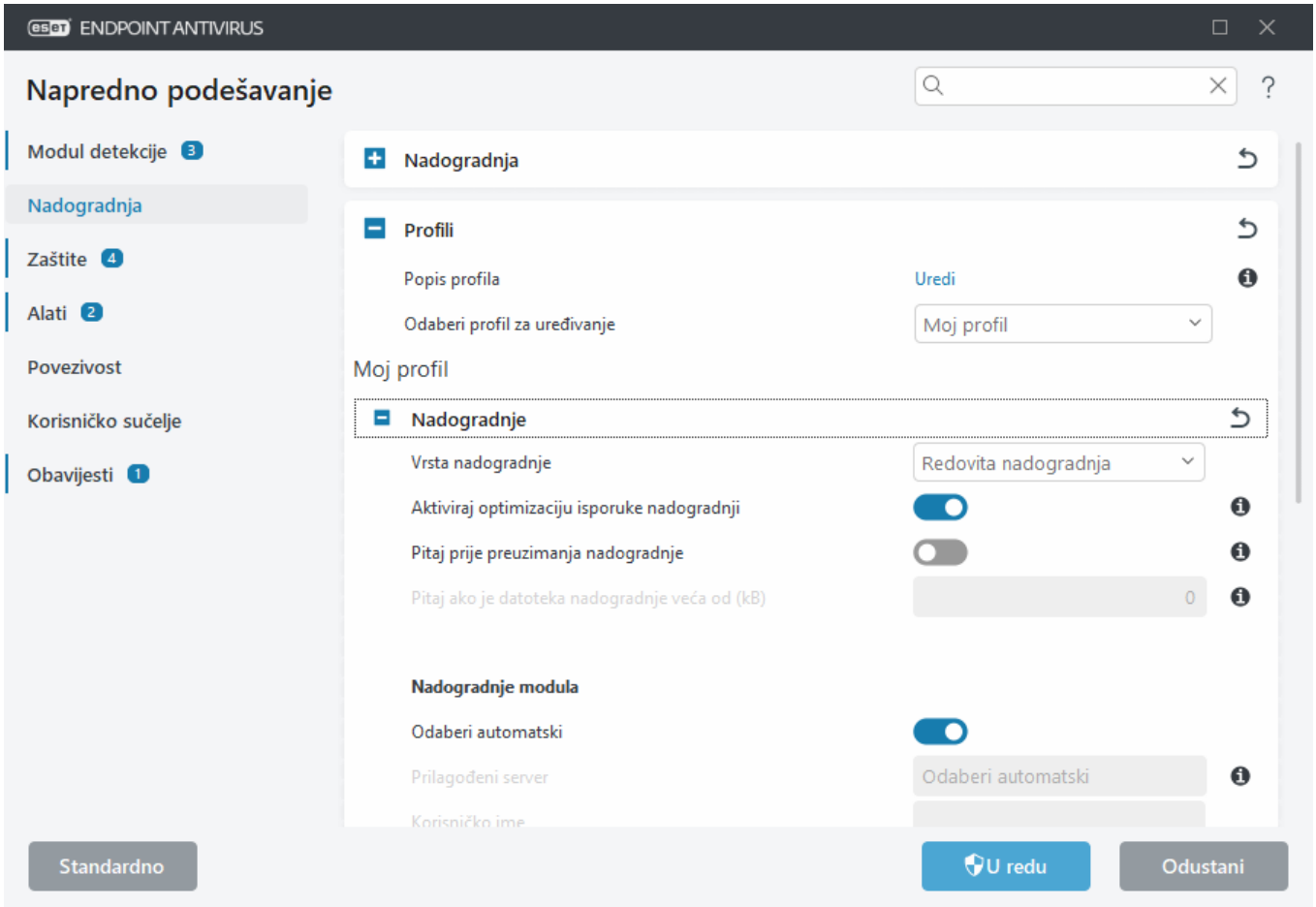
Nadogradnje

Prema standardnim postavkama **Vrsta aktualizacije** postavljena je na **Redovita aktualizacija** kako bi se osiguralo automatsko preuzimanje aktualizacijskih datoteka s ESET servera s najmanjim mrežnim prometom. Probni način rada (mogućnost **Probni način rada**) obuhvaća aktualizacije koje su prošle interno testiranje i koje će uskoro biti općenito dostupne. Ako aktivirate probni način rada, imat ćete pristup najnovijim metodama otkrivanja i popravcima. Međutim, probni način rada možda neće biti dovoljno stabilan cijelo vrijeme i NE PREPORUČUJE se njegovo korištenje na proizvodnim serverima i radnim stanicama gdje se traži maksimalna dostupnost i stabilnost. Odgođena aktualizacija omogućuje aktualizaciju s posebnih aktualizacijskih servera koji sadrže nove verzije baze podataka virusa s odgodom od barem X sati, (tj. baze podataka testirane su u stvarnom okruženju i smatraju se stabilnima).

Aktiviraj optimizaciju isporuke nadogradnji – Kad je ova opcija aktivirana, datoteke nadogradnje mogu se preuzeti iz CDN (mreže za isporuku sadržaja). Ako deaktivirate ovu postavku, može doći do prekida preuzimanja kada su namjenski ESET serveri za nadogradnju preopterećeni. Deaktivacija može biti korisna kad je firewall

ograničen samo na pristupanje IP adresama ESET servera za nadogradnju ili kad spajanje s uslugama CDN ne radi.

Pitaj prije preuzimanja nadogradnje – program će prikazati obavijest u kojoj možete potvrditi ili odbiti preuzimanja datoteka nadogradnje. Ako je datoteka za nadogradnju veća od vrijednosti navedene u polju Pitaj ako je datoteka za nadogradnju veća od (kB), program će prikazati upit za potvrdu. Ako je veličina datoteke za nadogradnju postavljena na 0 kB, program će uvijek prikazati upit za potvrdu.



Nadogradnje modula

Opcija **Odaberi automatski** postavljena je prema standardnim postavkama. Opcija **Prilagođeni server** mjesto je na kojemu se pohranjuju aktualizacije. Ako upotrebljavate ESET server za nadogradnju, preporučujemo da ostavite odabranu standardnu opciju.

Aktiviraj češće nadogradnje potpisa za otkrivanje – Potpisi za otkrivanje bit će nadograđivani u kraćim intervalima. Deaktivacija ove postavke može negativno utjecati na stopu otkrivanja.

Dopustite nadogradnje modula s izmjenjivog medija – Omogućuje nadogradnju s izmjenjivog medija ako sadrži stvoreni mirror. Kada je odabrana opcija Automatski, nadogradnja će se pokrenuti u pozadini. Ako želite da se prikažu dijaloški okviri za nadogradnju, odaberite stavku Uvijek pitaj.

Kada koristite lokalni HTTP server, poznat i kao mirror, server za nadogradnju treba postaviti na sljedeći način: *http://naziv_računala_ili_njegova_IP_adresa:2221*

Kada koristite lokalni HTTP server i SSL – server za nadogradnju treba postaviti na sljedeći način: *https://naziv_računala_ili_njegova_IP_adresa:2221*

Kada koristite lokalnu zajedničku mapu – server za nadogradnju treba postaviti na sljedeći način: *\\naziv_računala_ili_njegova_IP_adresa\zajednička_mapa*

Broj porta HTTP servera naveden u prethodnim primjerima ovisi o tome koji port osluškuje vaš HTTP/HTTPS server.

Nadogradnje programa

Pogledajte Nadogradnje programa.

Opcije veze

Pogledajte Opcije veze.

Mirror za aktualizaciju

Pogledajte Mirror za nadogradnju.

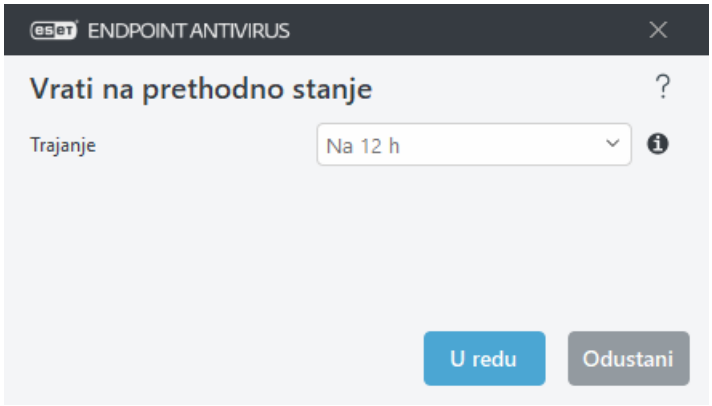
Vraćanje aktualizacije

Ako sumnjate da je nova nadogradnja modula detekcije nestabilna ili oštećena ili da su moduli programa nestabilni ili oštećeni, možete ih vratiti na prethodnu verziju i privremeno deaktivirati nadogradnje. Možete i aktivirati nadogradnje koje ste prethodno deaktivirali i odgodili na neograničeno vrijeme.

ESET Endpoint Antivirus bilježi snimke modula detekcije i modula programa za upotrebu s funkcijom vraćanja na prethodno stanje. Da biste stvorili snimke baze podataka virusa, funkcija **Stvori snimke modula** mora ostati aktivirana. Kada je aktivirana funkcija **Stvori snimke modula**, prva snimka stvara se tijekom prve nadogradnje. Sljedeća se stvara nakon 48 sati. U polju **Broj lokalno spremljenih snimki** naveden je broj spremljenih snimki modula detekcije.

Kada se dosegne maksimalna količina snimki (na primjer, tri), najstarija snimka zamjenjuje se novom svakih 48 sati. ESET Endpoint Antivirus vraća modul detekcije i verzije nadogradnji modula programa na najstariju snimku.

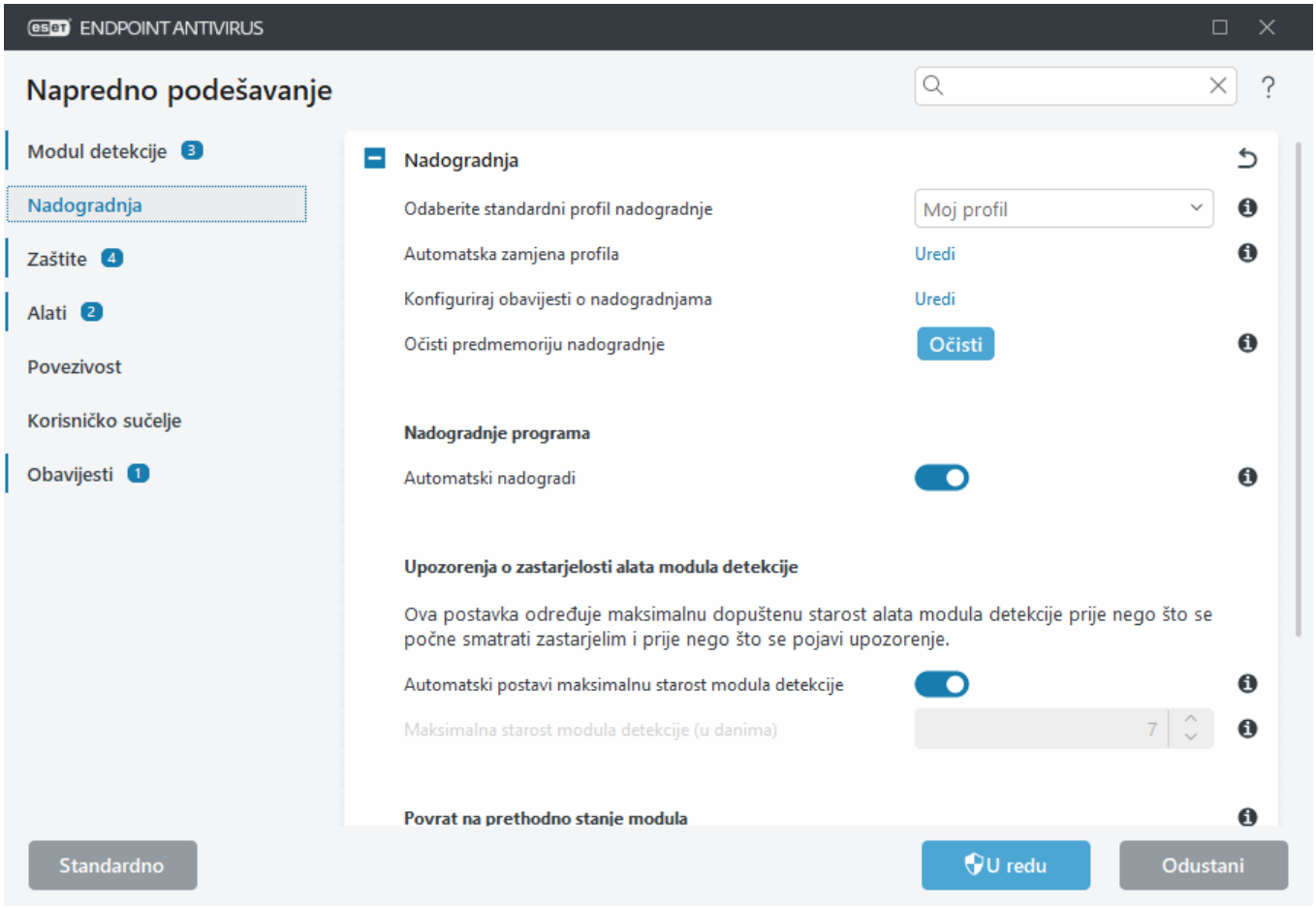
Otvorite Napredno podešavanje > **Nadogradnja** > **Nadogradi** > **Vraćanje modula na prethodno stanje** > **Vrati na prethodno stanje** da biste odabrali vremenski interval iz padajućeg izbornika **Trajanje**.



Odaberite **Do otkazivanja** da biste odgodili redovne nadogradnje na neodređeno vrijeme dok ručno ne vratite funkciju nadogradnje. Ne preporučujemo odabir te mogućnosti jer predstavlja mogući sigurnosni rizik.

Ako se vrši vraćanje na prethodno stanje, gumb **Vrati na prethodno stanje** pretvara se u **Dopusti nadogradnje**. Tijekom vremenskog intervala odabranog iz padajućeg izbornika **Obustava nadogradnji** nisu dopuštene

nadogradnje. Verzija modula detekcije vraćena je na najstariju dostupnu verziju i spremljena je kao snimka u datotečni sustav lokalnog računala.



Recimo da je broj 22700 najnovija verzija modula detekcije, a verzije 22698 i 22696 spremljene su kao snimke modula detekcije. Verzija 22697 nije dostupna. U ovom primjeru računalo je bilo isključeno tijekom nadogradnje verzije 22697 i pojavila se novija nadogradnja prije nego što je preuzeta verzija 22697. Ako je polje **Broj lokalno pohranjenih snimaka** postavljeno na 2 i kliknete **Vraćanje na prethodno stanje**, modul detekcije (uključujući module programa) bit će vraćen na verziju broj 22696. Taj postupak može potrajati. Provjerite je li verzija modula detekcije vraćena na stariju na zaslonu Nadogradnja.

Nadogradnje programa

Kartica **Nadogradnje programa** sadrži opcije povezane s nadogradnjama programa. Program vam omogućuje da unaprijed definirate njegovo ponašanje kada postane dostupna nova nadogradnja programa.

Nadogradnje programa uvode nove značajke ili mijenjaju one koje već postoje u prethodnim verzijama. Moguće ih je izvršiti automatski bez korisničke intervencije, ali korisnik može odabrati da ga se o tome obavijesti. Nakon instalacije nadogradnji programa moglo bi biti potrebno ponovno pokretanje računala.

Automatske nadogradnje – privremeno deaktiviranje automatskih nadogradnji za određene profile nadogradnji privremeno deaktivira automatske nadogradnje programa dok ste povezani s internetom pomoću drugih mreža ili veza s ograničenim prometom. Tu postavku ostavite aktiviranu kako biste imali stalan pristup najnovijim funkcijama i najvećoj mogućoj zaštiti. Za više informacija o automatskim nadogradnjama pogledajte Najčešća pitanja o automatskim nadogradnjama.

Prema standardnim postavkama nadogradnje programa preuzimaju se sa servera ESET repozitorija. U velikim

okruženjima ili okruženjima izvan mreže promet se može distribuirati radi omogućavanja unutarnjeg predmemoriranja datoteka programa.

Određivanje prilagođenog servera za nadogradnje programskih komponenti

1. Odredite put do nadogradnji programa u polju **Prilagođeni server**.
To može biti HTTP(S) link, put zajedničke mreže u SMB protokolu i put lokalnog diska ili izmjenjivog medija. Za mrežne pogone upotrijebite UNC umjesto slova mapiranog pogona.
2. Ostavite polja **Korisničko ime** i **Lozinka** praznima ako nisu obavezna.
Ako su obavezna, odredite odgovarajuće korisničke podatke za HTTP prijavu na prilagođeni web server.
3. Potvrdite promjene i provjerite postoje li nadogradnje programa pomoću standardne nadogradnje programa ESET Endpoint Antivirus.

Odabir najprikladnije opcije ovisi o radnoj stanici na kojoj se te postavke primjenjuju. Imajte na umu da postoje razlike između radnih stanica i servera, npr. automatskim ponovnim pokretanjem servera nakon nadogradnje programa moguće je nanijeti znatnu štetu tvrtki.

Opcije veze

Da biste pristupili mogućnostima postavljanja proxy servera za određeni profil ažuriranja, otvorite prozor Napredno podešavanje > **Ažuriranja** > **Profili** > **Ažuriranja** > **Opcije povezivanja**.

Proxy server

Kliknite padajući izbornik **Način rada proxy servera** i odaberite jednu od sljedećih triju opcija:

- Nemoj koristiti proxy server
- Veza putem proxy servera
- Koristi globalne postavke proxy servera

Odaberite opciju **Koristi globalne postavke proxy servera** za upotrebu opcija konfiguracije proxy servera koje su već definirane u odjeljku Napredno podešavanje > **Povezivost** > **Proxy server**.

Mogućnost **Nemoj koristiti proxy server** odaberite da biste odredili da se za nadogradnju programa ESET Endpoint Antivirus ne koristi proxy server.

Mogućnost **Veza putem proxy servera** treba se odabrati ako:

- Drugačiji proxy server od onog definiranog pod **Alati** > **Proxy server** upotrebljava se za nadogradnju programa ESET Endpoint Antivirus. U ovoj konfiguraciji, informacije za novi proxy trebale bi biti određene pod adresom **proxy servera**, komunikacijskim **portom** (3128 prema standardnim postavkama) te prema potrebi, **korisničkim imenom** i **lozinkom** za proxy server.
- Postavke proxy servera nisu postavljene globalno, no program ESET Endpoint Antivirus povezat će se s proxy serverom radi nadogradnje.
- Vaše računalo povezano je na internet putem proxy servera. Postavke se preuzimaju iz preglednika tijekom instalacije programa, no ako se promijene (npr. ako promijenite davatelja internetskih usluga), provjerite jesu li postavke za proxy ispravne u ovom prozoru. Program se inače neće moći povezati sa serverima za nadogradnje.

Standardna je postavka za proxy server **Koristi globalne postavke proxy servera**.

Upotrijebi izravnu vezu ako nije dostupan proxy – Ako nije dostupan, proxy će se zaobići tijekom nadogradnje.

Zajedničke mreže Windowsa

Pri aktualizaciji s lokalnog servera s operacijskim sustavom Windows NT, autorizacija je prema standardnim postavkama obavezna za svaku mrežnu vezu.

Za konfiguriranje takvog računa na padajućem izborniku odaberite **Poveži se s LAN-om kao**:

- **Sistemski račun (standardno)**,
- **Trenutačni korisnik**,
- **Određeni korisnik**.

Izaberite mogućnost **Sistemski račun (standardno)** da biste za autorizaciju koristili sistemski račun. Ako u glavnom odjeljku podešavanja aktualizacije nisu uneseni podaci za autorizaciju, obično nema nikakvog procesa autorizacije.

Da biste bili sigurni da će program autorizirati pomoću trenutno prijavljenog korisničkog računa, odaberite **Trenutni korisnik**. Nedostatak je tog rješenja taj što se program neće moći povezivati s aktualizacijskim serverom ako trenutno nije prijavljen nijedan korisnik.

Ako želite da program za autorizaciju koristi račun nekog točno određenog korisnika, odaberite **Određeni korisnik**. Tu metodu primijenite kada ne uspije povezivanje putem standardnog sistemskog računa. Imajte na umu da određeni korisnički račun mora imati pristup direktoriju s aktualizacijskim datotekama na lokalnom serveru. U suprotnome program neće moći uspostaviti vezu i preuzeti aktualizacije.

Postavke **korisničkog imena** i **lozinke** nisu obavezne.

> Kada su odabrane mogućnosti **Trenutni korisnik** ili **Određeni korisnik**, postoji mogućnost pogreške prilikom promjene identiteta programa na željenog korisnika. Preporučujemo da u glavni odjeljak podešavanja aktualizacije unesete podatke za autorizaciju LAN-a. U tom odjeljku podešavanja aktualizacije podatke za autorizaciju trebalo bi unijeti na sljedeći način: *naziv_domene**korisnik* (ako se radi o radnoj grupi, unesite *naziv_radnegrupe**naziv*) i lozinka. Pri aktualizaciji s HTTP verzije lokalnog servera nije potrebna nikakva autorizacija.

Odaberite opciju Nakon nadogradnje **prekini vezu** sa serverom da biste prinudno raskinuli vezu ako ona ostane aktivna nakon preuzimanja nadogradnje.

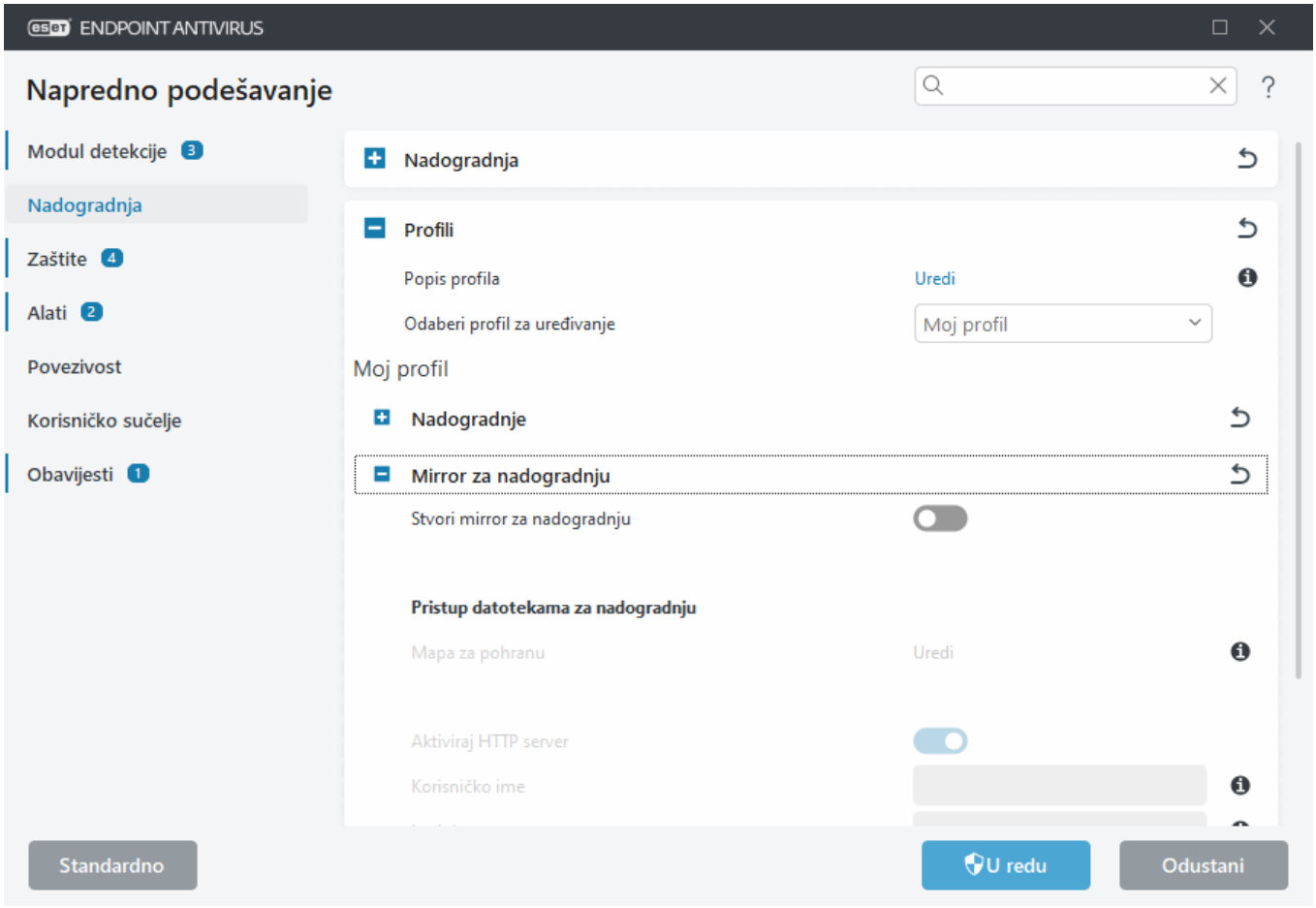
Mirror za aktualizaciju

ESET Endpoint Antivirus omogućuje stvaranje kopija aktualizacijskih datoteka koje se mogu koristiti za aktualizaciju drugih radnih stanica u mreži. Korištenje „mirrora”, kopije aktualizacijskih datoteka u lokalnoj mreži, praktično je jer se aktualizacijske datoteke ne moraju više puta preuzimati s proizvođačeva servera za nadogradnju te ih odatle ne mora preuzeti svaka radna stanica. One se preuzimaju centralizirano na lokalni mirror server, a zatim se distribuiraju svim radnim stanicama, čime se izbjegava mogući rizik od zagušenja mrežnog prometa. Aktualizacijom klijentskih radnih stanica s mirrora optimizira se opterećenje mreže i štedi propusnost internetske veze.

> Mirror za nadogradnju stvara kopije datoteka za nadogradnju koje se mogu koristiti za nadogradnju radnih stanica na kojima se koristi ista generacija programa ESET Endpoint Antivirus za Windows. (Primjerice, ESET Endpoint Antivirus za Windows verzije 10.x stvara datoteke za nadogradnju samo za verziju 10.x programa ESET Endpoint Antivirus za Windows i ESET Endpoint Security za Windows)

Kako biste smanjili internetski promet na mrežama na kojima se ESET PROTECT upotrebljava za upravljanje velikim brojem klijenata, preporučujemo da koristite ESET Bridge umjesto da konfigurirate klijent kao mirror. ESET Bridge se može instalirati uz program ESET PROTECT putem cjelovitog instalacijskog programa ili kao samostalna komponenta. Više informacija i razlike između ESET Bridge, Apache HTTP proxyja, mirror alata i izravne povezivosti potražite na stranici online pomoći za ESET PROTECT.

Opcije konfiguriranja za lokalni Mirror server dostupne su u izborniku Napredno podešavanje > **Nadogradi** > **Profili** > **Mirror za nadogradnju**.



Da biste stvorili mirror na klijentskom računalu, aktivirajte mogućnost **Stvori aktualizacijski mirror**. Aktivacijom te mogućnosti aktiviraju se druge mogućnosti konfiguracije mirrora kao što su način pristupa aktualizacijskim datotekama i aktualizacijski put do mirror datoteka.

Pristup aktualizacijskim datotekama

Omogući aktualizaciju putem internog HTTP servera – Ako je aktivirana, ova opcija omogućuje pristup aktualizacijskim datotekama preko HTTP-a bez unosa korisničkih podataka.

Načini pristupanja mirror serveru detaljno su opisani u odjeljku Aktualizacija s mirrora. Mirror je moguće konfigurirati na dva osnovna načina – mapa s datotekama za nadogradnju može biti zajednička mrežna mapa ili klijenti mogu pristupati mirroru na HTTP serveru.

Mapa namijenjena pohrani aktualizacijskih datoteka za mirror definira se u odjeljku **Mapa za mirror**. Za odabir druge mape kliknite **Očisti** da biste izbrisali unaprijed odabranu mapu *C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror* i kliknite **Uredi** da biste pronašli mapu na lokalnom računalu ili zajedničku mrežnu mapu. Ako je za navedenu mapu potrebna autorizacija, u polja **Korisničko ime** i **Lozinka** potrebno je unijeti podatke za

autorizaciju. Ako se odabrana odredišna mapa nalazi na mrežnom disku s verzijama operacijskog sustava Windows NT, 2000 ili XP, korisnik čije se korisničko ime i lozinka navedu mora imati prava pisanja za odabranu mapu. Korisničko ime treba unijeti u obliku *Domena/Korisnik* ili *Radna grupa/Korisnik*. Ne zaboravite unijeti odgovarajuće lozinke.

HTTP server i SSL za mirror

U odjeljku **HTTP server** na kartici **Mirror** možete odrediti **port servera** putem kojeg će HTTP server osluškivati te vrstu **autentikacije** koju će koristiti. Prema standardnim postavkama port servera postavljen je na **2221**.

Autentikacija– Definira način autentikacije koji se koristi za pristup datotekama za nadogradnju. Dostupne su sljedeće opcije: **Ništa**, **Osnovno** i **NTLM**. Da biste koristili base64 šifriranje s osnovnom autorizacijom putem korisničkog imena i lozinke, odaberite **Osnovno**. Mogućnost **NTLM** nudi šifriranje pomoću sigurne metode šifriranja. Za autorizaciju koristi se radna stanica koju je stvorio korisnik i na kojoj se zajednički koriste aktualizacijske datoteke. Standardna je postavka **Ništa**, a omogućuje pristup aktualizacijskim datotekama bez potrebe za autorizacijom.

Podaci za prijavu kao što su **korisničko ime** i **lozinka** namijenjeni su isključivo pristupanju mirror HTTP serveru. Ispunite ta polja samo ako su korisničko ime i lozinka obavezni.

Ako želite pokrenuti HTTP server s podrškom za HTTPS (SSL), dodajte svoju **Datoteku lanca certifikata** ili generirajte samopotpisani certifikat. Dostupne su sljedeće **vrste certifikata**: ASN, PEM i PFX. Za dodatnu zaštitu pri preuzimanju aktualizacijskih datoteka možete koristiti HTTPS protokol. Uz taj protokol gotovo je nemoguće pratiti prijenos podataka i podatke za prijavu. Opcija **Vrsta privatnog ključa** prema standardnim je postavkama postavljena na **Integrirano** (i zato je prema zadanim postavkama opcija **Datoteka privatnog ključa** deaktivirana). To znači da je privatni ključ dio odabrane datoteke lanca certifikata.

Samopotpisani certifikati za HTTPS mirror
Ako upotrebljavate HTTPS mirror server, morate uvesti njegov certifikat u pouzdano root spremište na svim klijentskim računalima. Pogledajte Instaliranje pouzdanog root certifikata u Windowsu.

Aktualizacija s mirrora

Postoje dva osnovna načina za konfiguriranje mirrora koji je zapravo repozitorij s kojeg klijenti mogu preuzimati aktualizacijske datoteke. Mapa s aktualizacijskim datotekama može biti zajednička mrežna mapa ili na HTTP serveru.

Mirror za nadogradnju stvara kopije datoteka za nadogradnju koje se mogu koristiti za nadogradnju radnih stanica na kojima se koristi ista generacija programa ESET Endpoint Antivirus za Windows. (Primjerice, ESET Endpoint Antivirus za Windows verzije 10.x stvara datoteke za nadogradnju samo za verziju 10.x programa ESET Endpoint Antivirus za Windows i ESET Endpoint Security za Windows)

Pristup mirroru putem internog HTTP servera

To je standardna konfiguracija, određena u unaprijed definiranoj konfiguraciji programa. Da biste omogućili pristup mirroru s pomoću HTTP servera, idite na "Napredno podešavanje" > **"Nadogradnja"** > **"Profili"** > **„Mirror za nadogradnju"** i odaberite **"Stvori mirror za nadogradnju"**.

U odjeljku **HTTP server** na kartici **Mirror** možete odrediti **port servera** putem kojeg će HTTP server osluškivati te vrstu **autentikacije** koju će koristiti. Prema standardnim postavkama port servera postavljen je na **2221**.

Autentikacija– Definira način autentikacije koji se koristi za pristup datotekama za nadogradnju. Dostupne su sljedeće opcije: **Ništa**, **Osnovno** i **NTLM**. Da biste koristili base64 šifriranje s osnovnom autorizacijom putem korisničkog imena i lozinke, odaberite **Osnovno**. Mogućnost **NTLM** nudi šifriranje pomoću sigurne metode šifriranja. Za autorizaciju koristi se radna stanica koju je stvorio korisnik i na kojoj se zajednički koriste aktualizacijske datoteke. Standardna je postavka **Ništa**, a omogućuje pristup aktualizacijskim datotekama bez potrebe za autorizacijom.

Ako želite dopustiti pristup aktualizacijskim datotekama putem HTTP servera, mapa mirrora mora se nalaziti na istom računalu na kojem se nalazi i instanca programa ESET Endpoint Antivirus koja je stvara.

Pogreška **Neispravno korisničko ime/lozinka** pojavit će se u oknu Aktualizacija u glavnom izborniku nakon nekoliko neuspješnih pokušaja aktualizacije modula za otkrivanje virusa s mirrora. Preporučujemo vam da idete do odjeljka Napredno podešavanje > **Aktualizacija** > **Profili** > **Mirror za nadogradnju** i provjerite korisničko ime i lozinku. Najčešći je razlog pojavljivanja te pogreške unos pogrešnih podataka za autorizaciju.

Nakon konfiguriranja mirror servera morate dodati novi aktualizacijski server na klijentske radne stanice. Da biste to učinili, slijedite ove korake:

- Otvorite Napredno podešavanje i kliknite **Aktualizacija** > **Profili** > **Osnovno** > **Nadogradnje modula**.
- Deaktivirajte odabir mogućnosti **Odaberi automatski** i dodajte novi poslužitelj **u polje** Aktualizacijski server u jednom od sljedećih formata:
  http://IP_adresa_servera:2221
  https://IP_adresa_servera:2221 (ako se koristi SSL)

Pristup mirroru putem zajedničkih mrežnih mjesta

Najprije treba stvoriti zajedničku mapu na lokalnom ili mrežnom uređaju. Kada stvarate mapu za mirror, potrebno je omogućiti pristup za „pisanje” za korisnika koji će spremiti aktualizirane datoteke u mapu i pristup za „čitanje” za korisnika koji će aktualizirati ESET Endpoint Antivirus iz mape mirror.

Zatim konfigurirajte pristup mirroru tako da na kartici Napredno podešavanje > **Nadogradnja** > **Profili** > **Mirror za nadogradnju** deaktivirate opciju **Aktiviraj HTTP server**. Ta je opcija prema standardnim postavkama aktivirana u instalacijskom paketu programa.

Ako se zajednička mapa nalazi na nekom drugom računalu u mreži, morate unijeti podatke za prijavu za pristup tom drugom računalu. Za unos podataka za prijavu otvorite Napredno podešavanje i kliknite **Nadogradnja** > **Profili** > **Nadogradnje** > **Opcije povezivanja** > **Zajedničke mreže Windowsa** > **Poveži se s LAN-om kao**. Ta je postavka ista kao i za nadogradnju, kao što je opisano u odjeljku Poveži se s LAN-om kao.

Za pristup mapi mirrora to se mora učiniti s istoga računa koji je upotrijebljen za prijavu na računalo na kojemu je stvoren mirror. Ako se računalo nalazi u domeni, treba se upotrijebiti korisničko ime "domain\user". Ako računalo nije u domeni, treba upotrijebiti "IP_address_of_your_server\user" ili "hostname\user".

Nakon završetka konfiguracije mirrora, nastavite na radnim stanicama i postavite *\\UNC\PATH* kao aktualizacijski server slijedeći korake u nastavku:

1. Otvorite Napredno podešavanje i kliknite **Aktualizacija** > **Profili** > **Osnovno**.
2. Deaktivirajte odabir opcije **Odaberi automatski** pored **Nadogradnji modula** i dodajte novi server u polju

Server za nadogradnju koristeći se formatom *UNC**PATH*.

Radi pravilnog funkcioniranja put do mape mirrora potrebno je odrediti kao UNC put. Aktualizacije s mapiranih pogona možda neće raditi.

Stvaranje mirrora pomoću mirror alata
Struktura mapa koju stvara mirror alat razlikuje se od onoga što čini mirror Endpoint programa. Svaka mapa sadržava datoteke za nadogradnju za skupinu programa. U postavkama nadogradnje programa koji se služi mirrorom morate navesti cijeli put do točne mape.
Primjerice, da biste s mirrora nadogradili ESET PROTECT, postavite server za nadogradnju na sljedeću adresu (prema osnovnoj lokaciji HTTP servera):
`http://your_server_address/mirror/eset_upd/ep10`

U zadnjem se odjeljku nalaze postavke za upravljanje programskim komponentama (PCU-ovima). Prema standardnim postavkama preuzete komponente programa se pripremaju za kopiranje u lokalni mirror. Ako je aktivirana mogućnost **Nadogradnja programa**, nije potrebno kliknuti **Nadogradi** jer se datoteke automatski kopiraju na lokalni mirror kada postanu dostupne. Dodatne informacije o nadogradnji programa potražite u odjeljku Način nadogradnje.

Otklanjanje poteškoća s mirror aktualizacijom

U većini su slučajeva problemi tijekom aktualizacije s mirror servera izazvani neispravnim određivanjem mogućnosti mape za mirror, neispravnim podacima za autorizaciju pri pristupu mapi za mirror, neispravnom konfiguracijom na lokalnim radnim stanicama koje pokušavaju preuzeti aktualizacijske datoteke s mirrora ili kombinacijom navedenih razloga. Slijedi pregled najčešćih problema koji se mogu pojaviti tijekom aktualizacije s mirrora.

ESET Endpoint Antivirus prijavljuje pogrešku pri povezivanju s mirror serverom– Taj je problem vjerojatno prouzročilo neispravno određivanje aktualizacijskog servera (mrežnog puta do mape za mirror) s kojega lokalne radne stanice preuzimaju nadogradnje. Da biste provjerili mapu, u sustavu Windows kliknite **Start**, zatim **Pokreni**, unesite naziv mape pa kliknite **U redu**. Trebao bi se prikazati sadržaj mape.

ESET Endpoint Antivirus zahtijeva korisničko ime i lozinku – Problem se vjerojatno pojavio zbog neispravnog unosa podataka za autentikaciju (korisničkog imena i lozinke) u odjeljku nadogradnje. Korisničko ime i lozinka služe za omogućivanje pristupa aktualizacijskom serveru s kojega se program aktualizira. Provjerite jesu li podaci za autorizaciju točni i jesu li uneseni u pravilnom obliku. Na primjer, Domena/Korisničko ime ili Radna stanica/Korisničko ime te odgovarajuće lozinke. Ako je mirror server dostupan „svima”, imajte na umu da to ne znači da je svim korisnicima omogućen pristup. Pod pojmom „svi” ne podrazumijeva se bilo koji neovlašteni korisnik, već se podrazumijeva da mapi mogu pristupiti svi korisnici domene. Zbog toga je, čak i ako mapi mogu pristupiti „svi”, u odjeljak podešavanja nadogradnje potrebno unijeti korisničko ime i lozinku.

ESET Endpoint Antivirus prijavljuje pogrešku pri povezivanju s mirror serverom – Na portu definiranom za pristup HTTP verziji mirrora blokirana je komunikacija.

ESET Endpoint Antivirus prijavljuje pogrešku prilikom preuzimanja datoteka za nadogradnju – taj je problem vjerojatno uzrokovalo neispravno određivanje servera za nadogradnju (mrežnog puta do mape za mirror) s kojega lokalne radne stanice preuzimaju nadogradnje.

Zaštite

Zaštite štite sustav od zlonamjernih napada kontrolom datoteka, e-pošte i internetske komunikacije. Primjerice, ako se otkrije objekt klasificiran kao zlonamjerni program, započet će ispravljanje. Zaštite ga mogu eliminirati blokiranjem, a zatim čišćenjem, brisanjem ili premještanjem u karantenu.

Da biste detaljno konfigurirali zaštite, otvorite Napredno podešavanje > **Zaštite**.

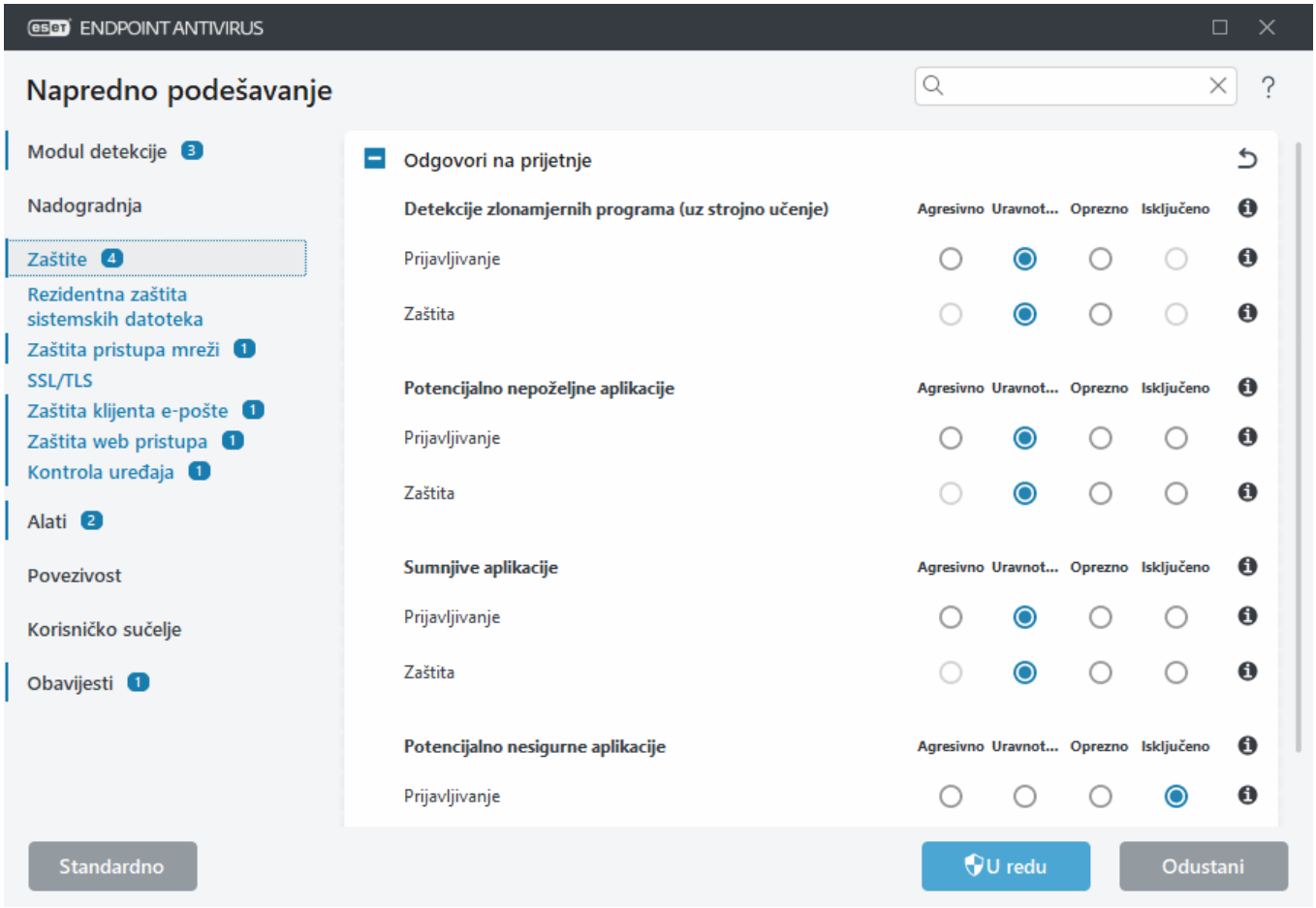
Samo bi iskusan korisnik trebao mijenjati zaštite. Neispravna konfiguracija postavki može dovesti do smanjene razine zaštite.

U ovom odjeljku:

Odgovori na prijetnje

Odgovori na otkrivanje omogućuju konfiguriranje razina izvješćivanja i zaštite za sljedeće kategorije:

- **Detekcije zlonamjernih programa (uz strojno učenje)** – računalni virus primjerak je zlonamjernog koda koji se dodaje ispred ili uz postojeće datoteke na računalu. Međutim, pojam „virus” često se pogrešno upotrebljava. A točniji bi termin bio „zlonamjerni program”. Zlonamjerni programi otkrivaju se uz pomoć modula detekcije u kombinaciji s komponentom strojnog učenja. Više o tim vrstama aplikacija pročitajte u rječniku.
- **Potencijalno nepoželjne aplikacije** – Grayware ili potencijalno nepoželjne aplikacije (PUA) široka su kategorija softvera čija namjera nije nedvosmisleno zlonamjerna poput drugih vrsta zlonamjernih programa, kao što su virusi ili trojanci. Međutim, takvi programi mogu instalirati dodatne neželjene programe, promijeniti rad digitalnog uređaja ili provesti aktivnosti koje korisnik nije dopustio ili koje ne očekuje. Više o tim vrstama aplikacija pročitajte u rječniku.
- **Sumnjive aplikacije** – uključuju programe komprimirane s pomoću packer ili protector programa Autori zlonamjernih programa često iskorištavaju te vrste programa kako bi spriječili otkrivanje.
- **Potencijalno nesigurne aplikacije** – Naziv je koji se odnosi na legitiman komercijalni softver koji bi se mogao zloupotrijebiti. Primjeri potencijalno nesigurnih aplikacija (PUA) obuhvaćaju alate za daljinski pristup, aplikacije za probijanje lozinki i keyloggere (programe koji bilježe svaki korisnikov pritisak tipke). Više o tim vrstama aplikacija pročitajte u rječniku.



Poboljšana zaštita

Napredno strojno učenje sada je sastavni dio zaštita kao napredni sloj zaštite kojim se poboljšava otkrivanje prijetnji na temelju strojnog učenja. Više o ovoj vrsti zaštite potražite u rječniku.

Podešavanje izvješćivanja

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

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

1. Otkrivanje zlonamjernog softvera
2. Potencijalno nepoželjne aplikacije
3. Potencijalno nesigurne
4. Sumnjive aplikacije

Izvještavanje putem modula detekcije, uključujući komponentu strojnog učenja. Postaviti možete i viši prag za prijavljivanje od trenutačnog praga zaštite. Ove postavke ne utječu na blokiranje, čišćenje ni uklanjanje objekata.

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

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

Dostupnost modula za zaštitu programa ESET Endpoint Antivirus

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

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

*Nije preporučeno.

Određivanje verzije programa, modula programa i datuma podverzije

1. Kliknite **Pomoć i podrška** > **O programu ESET Endpoint Antivirus**.
2. Na zaslonu **O programu**, prvi redak teksta prikazuje broj verzije vašeg ESET programa.
3. Kliknite **Instaliraj komponente** da biste pristupili informacijama o određenim modulima.

Osnovne bilješke

Nekoliko osnovnih bilješki za postavljanje odgovarajućeg praga za vaše okruženje:

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

Podešavanje zaštite

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

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

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

Najbolje prakse

NEUPRAVLJANO (radna stanica pojedinačnog klijenta)

Zadržite standardne preporučene vrijednosti kakve jesu.

UPRAVLJANO OKRUŽENJE

Ove se postavke obično primjenjuju na radne stanice pomoću pravila.

1. Početna faza

Ova faza može potrajati do jednog tjedna.

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

2. Faza prijelaza

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

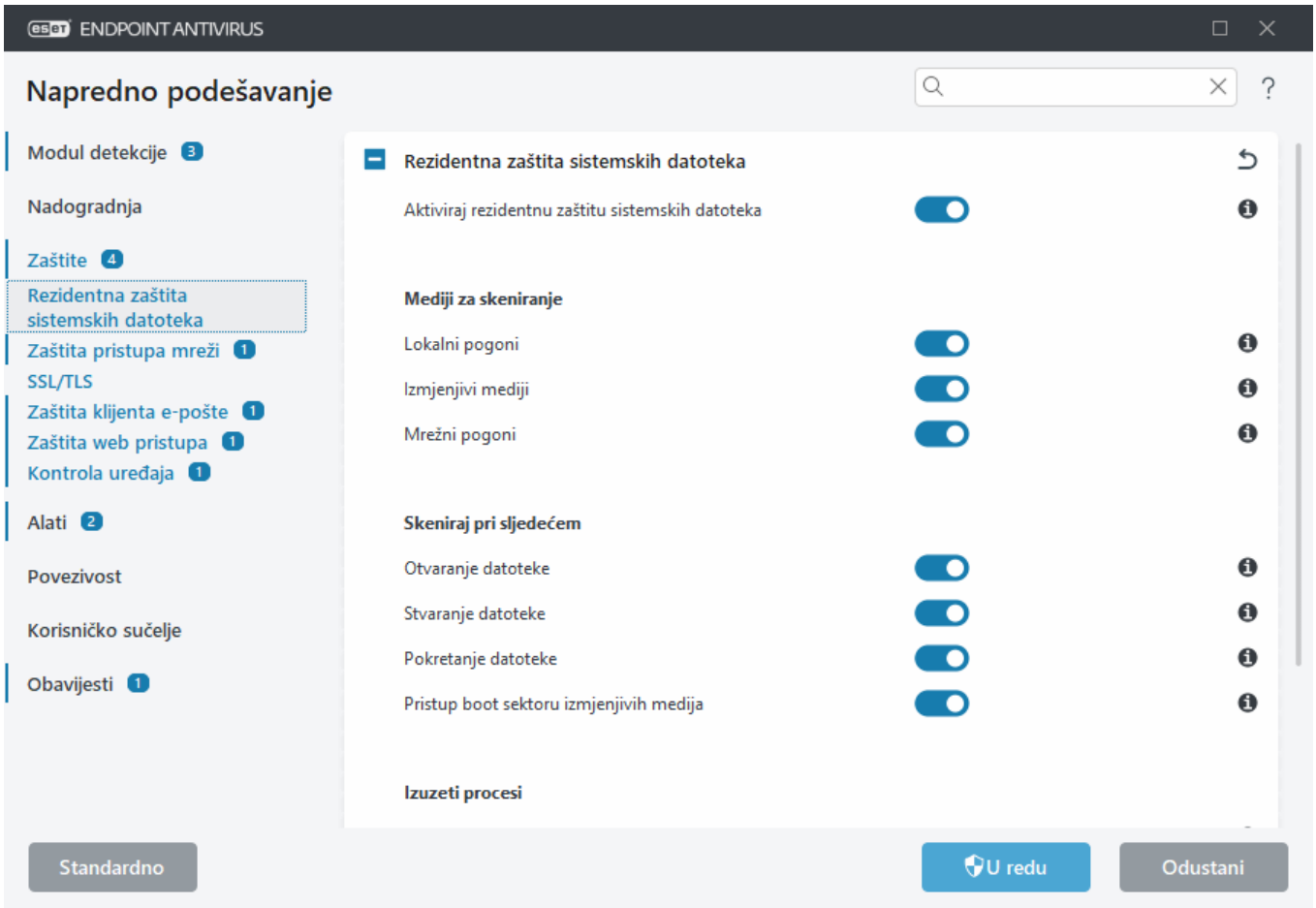
3. Faza produkcije

- Postavite sve pragove **Zaštite** na **Uravnoteženo**.
- Prilikom daljinskog upravljanja upotrijebite odgovarajuće unaprijed definirano pravilo za antivirus za program ESET Endpoint Antivirus.

- Prag zaštite **Agresivno** može se postaviti ako su potrebne najveće stope otkrivanja prijetnji i ako su prihvaćeni lažno prepoznati objekti.
- Provjerite Dnevnik otkrivenih prijetnji ili izvješća programa ESET PROTECT kako biste pronašli moguće prijetnje koje nedostaju.

rezidentna zaštita

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



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

Mediji za skeniranje

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

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

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

Skeniraj pri

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

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

Izuzeti procesi

Pogledajte stavku Izuzeti procesi.

ThreatSense

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

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

Rezidentna zaštita datotečnog sustava također vam omogućuje konfiguriranje dodatnih ThreatSense parametara.

Izuzeti procesi

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

čega su proširena dopuštenja dopuštena samo u modulu rezidentne zaštite.

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

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

Izvršne datoteke možete dodati na popis izuzetih procesa u stavci Napredno podešavanje > **Zaštite** > **Rezidentna zaštita sistemskih datoteka** > **Rezidentna zaštita sistemskih datoteka** > **Izuzeti procesi**.

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

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

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

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

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

Dodavanje ili uređivanje izuzetih procesa

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

Odaberite put datoteke izuzete aplikacijetako da kliknete na ... (na primjer *C:\Program Files\Firefox\Firefox.exe*). NEMOJTE upisati vrstu aplikacije.
Čim se datoteka *.exe* doda izuzecima, ESET Endpoint Antivirus više ne prati aktivnost tog procesa i ne provodi se skeniranje operacija s datotekama tog procesa.

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

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

Kada treba izmijeniti konfiguraciju rezidentne zaštite

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

Nakon instalacije programa ESET Endpoint Antivirus sve postavke optimizirane su tako da se korisnicima pruži maksimalna razina zaštite sustava. Da biste vratili standardne postavke, kliknite ↩ pored stavke Napredno podešavanje > **Zaštite** > **Odgovori na prijetnje**.

Provjera rezidentne zaštite

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

Datoteka se može preuzeti s adrese http://www.eicar.org/download/eicar.com.
Nakon što unesete ovaj URL u svoj preglednik, trebali biste vidjeti poruku da je prijetnja uklonjena.

Što ako rezidentna zaštita ne funkcionira

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

Rezidentna zaštita je deaktivirana

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

Ako se rezidentna zaštita ne pokrene prilikom pokretanja sustava, vjerojatno je deaktivirana mogućnost **Aktiviraj rezidentnu zaštitu**. Kako biste bili sigurni da je ta opcija aktivirana, otvorite Napredno podešavanje > **Zaštite** > **Rezidentna zaštita sistemskih datoteka**.

Ako rezidentna zaštita ne otkriva ni ne čisti infiltracije

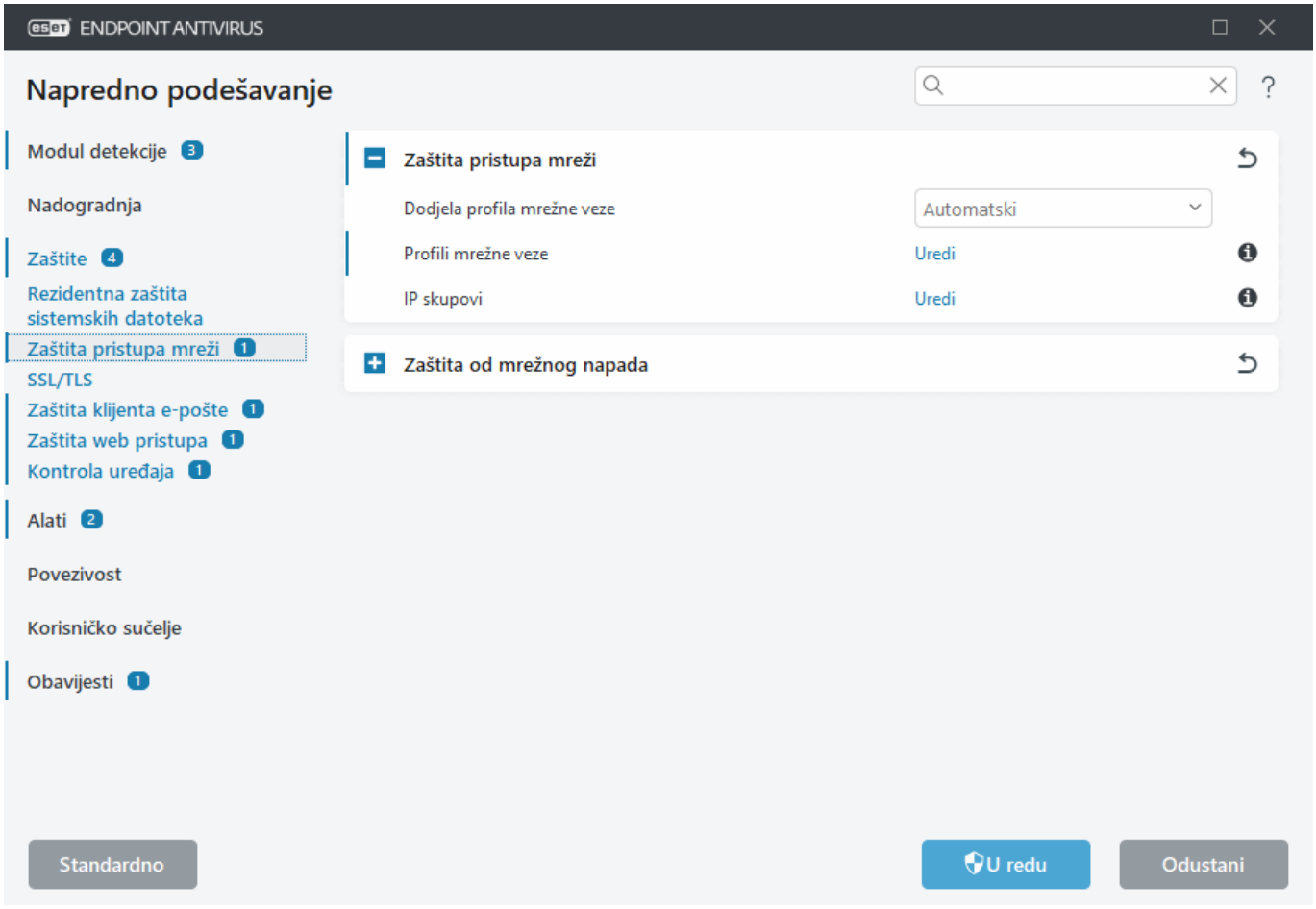
Provjerite nije li na računalu instaliran još neki antivirusni program. Ako su istodobno instalirana dva antivirusna programa, moguće je da će se međusobno sukobljavati. Preporučujemo da prije instalacije programa ESET deinstalirate sve druge antivirusne programe.

Rezidentna zaštita se ne pokreće

Ako se rezidentna zaštita ne pokrene prilikom pokretanja sustava (a opcija **Aktiviraj rezidentnu zaštitu sistemskih datoteka** je aktivirana), možda je došlo do sukoba s drugim programima. Da biste riješili ovaj problem, stvorite ESET SysInspector dnevnik i pošaljite ga ESET-ovoj tehničkoj podršci na analizu.

Zaštita pristupa mreži

Zaštita pristupa mreži omogućuje konfiguriranje svih mrežnih veza. Prema zadanim postavkama, program ESET Endpoint Antivirus ima unaprijed konfigurirana pravila za zaštitu pristupa mreži uz maksimalnu sigurnost. Međutim, određena okruženja možda će trebati prilagođenu konfiguraciju. Promjenu zadanih postavki trebao bi izvršiti samo iskusni korisnik.



Sljedeće postavke možete konfigurirati pod opcijom Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** (Kliknite veze u nastavku za detaljan opis pojedinačne opcije zaštite pristupa mreži):

Zaštita pristupa mreži

Profili mrežne veze – profili mrežne veze se mogu upotrebljavati za kontrolu zaštite pristupa mreži za određene mrežne veze.

IP skupovi – možete definirati kolekcije IP adresa koje tvore jednu logičku grupu IP adrese koje se zatim mogu dodati u pouzdanu zonu ili izuzeti iz zaštite od mrežnog napada (IDS).

Zaštita od mrežnog napada

Profili mrežne veze

Profili se mogu upotrebljavati za kontrolu ponašanja Zaštite pristupa mreži programa ESET Endpoint Antivirus za određene mrežne veze. Prilikom izrade ili uređivanja IDS pravila, pravila zaštite od napada grubom silom, pravilo

možete dodijeliti određenom profilu ili ga primijeniti na sve profile. Kada je profil aktivan na mrežnoj vezi, primjenjuju se samo globalna pravila (pravila za koja profil nije naveden) i pravila dodijeljena tom profilu.

Profile i zadatke mrežne veze možete konfigurirati u opciji Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** > **Zaštita pristupa mreži**.

Dodjela profila mrežne veze – omogućuje vam da odaberete hoće li novootkrivene mrežne veze automatski (na padajućem izborniku odaberite **Automatski**) dodijeliti unaprijed definirani ili prilagođeni profil na temelju aktivatora konfiguriranih u profilima mrežne veze ili želite da vas se pita (na padajućem izborniku odaberite **Pitaj**) da izvršite konfiguriranje zaštite mreže i ručno dodjeljivanje profila svaki puta kada se detektira nova mrežna veza.

Možete i ručno dodijeliti određeni profil mrežne veze tako da otvorite prozor glavnog programa > **Podešavanje** > **Mreža** > **Mrežne veze**. Zadržite pokazivač miša iznad određene mrežne veze i kliknite ikonu izbornika > **Uredi** da biste otvorili prozor Konfiguriranje mrežne zaštite pa odaberite profil.

Profili mrežnih veza – kliknite **Uredi** za dodavanje ili uređivanje profila mrežne veze.

Sljedeći profili unaprijed su definirani i ne mogu se uređivati/brisati:

Privatno – za pouzdane mreže (kućnu ili uredsku mrežu). Vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi su drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži (aktiviran je pristup zajedničkim datotekama i pisačima, aktivirana je dolazna RPC komunikacija i dostupno je daljinsko dijeljenje radne površine). Preporučujemo upotrebu ove postavke prilikom pristupa sigurnoj lokalnoj mreži. Ovaj se profil automatski dodjeljuje mrežnoj vezi ako je konfigurirana kao Domenska ili Privatna mreža u sustavu Windows.

Javno – za nepouzdane mreže (javnu mrežu). Datoteke i mape u vašem sustavu ne dijele se s drugim korisnicima na mreži niti su im vidljive i deaktivirano je dijeljenje resursa sustava. Preporučujemo upotrebu ove postavke prilikom pristupa bežičnim mrežama. Ovaj se profil automatski dodjeljuje bilo kojoj mrežnoj vezi koja nije konfigurirana kao Domenska ili Privatna mreža u sustavu Windows.

Kad se mrežna veza prebaci na drugi profil, pojavit će se obavijest u donjem desnom kutu zaslona.

Dodavanje ili uređivanje profila mrežne veze

Profile mrežne veze možete dodavati i uređivati u prozoru Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** > **Zaštita pristupa mreži** > **Profili mrežne veze** > **Uredi**. Da biste uredili profil, morate ga odabrati na popisu u prozoru **Profili mrežne veze** .

Sljedeći profili su unaprijed definirani i ne mogu se uređivati/brisati:

Privatno – za pouzdane mreže (kućnu ili uredsku mrežu). Vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi su drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži (aktiviran je pristup zajedničkim datotekama i pisačima, aktivirana je dolazna RPC komunikacija i dostupno je daljinsko dijeljenje radne površine). Preporučujemo upotrebu ove postavke prilikom pristupa sigurnoj lokalnoj mreži. Ovaj se profil automatski dodjeljuje mrežnoj vezi ako je konfigurirana kao Domenska ili Privatna mreža u sustavu Windows.

Javno – za nepouzdane mreže (javnu mrežu). Datoteke i mape u vašem sustavu ne dijele se s drugim korisnicima na mreži niti su im vidljive i deaktivirano je dijeljenje resursa sustava. Preporučujemo upotrebu ove postavke prilikom pristupa bežičnim mrežama. Ovaj se profil automatski dodjeljuje bilo kojoj mrežnoj vezi koja nije

konfigurirana kao Domenska ili Privatna mreža u sustavu Windows.

Odozgo / gore / odozdo / dolje  – omogućuje podešavanje razine prioriteta profila mrežne veze (profili mrežne veze procjenjuju se i primjenjuju prema njihovom prioritetu. Uvijek se primjenjuje prvi odgovarajući profil).

Dodavanje ili uređivanje profila

Prilagođeni profil mrežne veze omogućuje primjenu zaštite od napada grubom silom i definiranje dodatnih postavki za konkretne mrežne veze. Određujete mrežne veze kojima će se dodijeliti prilagođeni profil u odjeljku Aktivatori.

Da biste otvorili uređivač profila, u prozoru **Profili mrežne veze** učinite sljedeće:

- Kliknite **Dodaj**.
- Odaberite jedan od postojećih profila i kliknite **Uredi**.
- Odaberite jedan od postojećih profila i kliknite **Kopiraj**.

Naziv – prilagođeni naziv za vaš profil.

Opis – opis profila koji olakšava identifikaciju profila.

Dodatne pouzdane adrese –adrese koje definirate u ovoj stavci dodaju se u pouzdanu zonu mrežne veze na koju se ovaj profil primjenjuje (bez obzira na vrstu zaštite mreže).

Pouzdana veza – vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi su drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži (omogućen je pristup zajedničkim datotekama i pisačima, omogućena je dolazna RPC komunikacija i dostupno je daljinsko dijeljenje radne površine). Preporučujemo korištenje ove postavke prilikom izrade profila za sigurnu lokalnu mrežnu vezu. Sve izravno povezane podmreže određene mreže također se smatraju pouzdanima. Na primjer, ako je mrežni adapter povezan na mrežu s IP adresom 192.168.1.5 i maska podmreže je 255.255.255.0, u pouzdanu zonu adaptera dodaje se podmreža 192.168.1.0/24. Ako adapter ima više adresa/podmreža, sve će se smatrati pouzdanima.

Upozori na slabu razinu šifriranja Wi-Fi mreže – ESET Endpoint Antivirus će prikazati obavijest na radnoj površini ada se povežete s nezaštićenom bežičnom mrežom ili s mrežom sa slabom zaštitom.

Aktivatori – prilagođeni uvjeti koji moraju biti ispunjeni da bi se ovaj profil mrežne veze dodijelio mrežnoj vezi. Za detaljna objašnjenja pogledajte odjeljak Aktivatori.

Aktivatori

Aktivatori su prilagođeni uvjeti koji moraju biti ispunjeni da bi se mrežni profil veze dodijelio . Ako povezana mreža ima iste atribute koji su definirani u aktivatorima za povezani mrežni profil, profil će se primijeniti na mrežu. Profil mrežne veze može imati jedan ili više aktivatora. Ako postoji više aktivatora, primjenjuje se logika OR (mora biti ispunjen barem jedan uvjet). Aktivatore možete definirati u uređivaču profila mrežne veze. Izradu prilagođenih profila mrežne veze trebao bi vršiti iskusni korisnik.

Dostupni su sljedeći Aktivatori:

Adapter

Vrsta adaptera – primijenite profil ako je mrežna veza uspostavljena na odabranoj vrsti adaptera.
Naziv adaptera – primijenite profil ako se naziv mrežnog adaptera podudara.
IP adaptera – primijenite profil ako se IP adresa mrežnog adaptera podudara.

DNS

DNS sufiks – primijenite profil ako se naziv domene podudara.
DNS IP – primijenite profil ako se IP adresa DNS servera podudara.

WINS

Primijenite profil ako se mapirana IP adresa za Windows Internet Name Service (WINS) podudara.

DHCP

DHCP IP – – podudaranje IP adrese DHCP servera.

Standardni gateway

IP – primijenite profil ako se IP adresa zadanog gatewaya podudara.
MAC adresa – primijenite profil ako se MAC za standardni gateway podudara.

Wi-Fi

SSID – primijenite profil ako se SSID (naziv Wi-Fi veze) podudara.
Naziv profila – primijenite profil ako se naziv W--Fi profila podudara.
Vrsta sigurnosti – primijenite profil ako vrsta sigurnosti odgovara onoj odabranoj na padajućem izborniku. (Ako želite uskladiti više aktivatora, izradite drugi aktivator).
Vrsta šifriranja – primijenite profil ako vrsta šifriranja odgovara onoj odabranoj na padajućem izborniku. (Ako želite uskladiti više aktivatora, izradite drugi aktivator).
Mrežna sigurnost – primijenite profil ako je mreža **otvorena/zaštićena**.

Profil sustava Windows

Primijenite profil ako je mreža konfigurirana u sustavu Windows kao **domena/privatna mreža/javna mreža**.

Autorizacija

Autorizacija mreže traži određeni server u mreži i koristi asimetrično šifriranje (RSA) da bi ga autorizirala. Naziv mreže za provjeru autentičnosti mora odgovarati skupu naziva u postavkama servera za provjeru autentičnosti. Naziv je osjetljiv na velika i mala slova. Naziv servera može se upisati kao IP adresa, DNS ili NetBios naziv.
Preuzmite ESET-ov autorizacijski server.
Javni se ključ može uvesti uporabom bilo kojeg od sljedećih tipova datoteka:
• PEM šifrirani javni ključ (.pem); taj ključ možete generirati pomoću ESET-ovog servera za provjeru autentičnosti
• Šifrirani javni ključ
• Certifikat javnog ključa (.crt)
Kliknite **Test** za testiranje postavki. Ako se autorizacija uspješno izvrši, prikazat će se obavijest Autorizacija servera uspješno je dovršena. Ako autorizacija nije ispravno konfigurirana, prikazat će se jedna od sljedećih poruka o pogreškama:
Autorizacija servera nije uspjela. Digitalni potpis nije ispravan ili se ne podudara.
Potpis servera ne odgovara unesenom javnom ključu.
Autorizacija servera nije uspjela. Naziv mreže ne odgovara.
Naziv konfigurirane mreže ne odgovara nazivu zone autorizacijskog servera. Pregledajte oba naziva i provjerite jesu li identični.
Autorizacija servera nije uspjela. Odgovor sa servera nije ispravan ili ga nema.
Ako server nije uključen ili je nedostupan, ne može se primiti odgovor. Odgovor može biti neispravan ako drugi HTTP server radi na navedenoj adresi.
Unesen je nevaljan javni ključ.
Provjerite je li uneseni javni ključ ispravan.

IP skupovi

IP skup je zbirka IP adresa koje stvaraju jednu logičku grupu IP adresa, korisnih pri ponovnoj upotrebi istog skupa adresa u više pravila zaštite od napada grubom silom. ESET Endpoint Antivirus sadržava i unaprijed definirane IP skupove za koje se primjenjuju interna pravila. Primjer takve grupe je **Pouzdana zona**. Pouzdana zona predstavlja grupu mrežnih adresa na kojima su vaše računalo i zajedničke datoteke pohranjene na vašem računalu vidljivi drugim korisnicima mreže, a resursi sustava dostupni su drugim korisnicima na mreži.

Da biste dodali IP skup:

1. Otvorite Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** > **IP skupovi** > **Uredi**.
2. Kliknite **Dodaj**, upišite **naziv** i **opis** zone te udaljenu IP adresu u odjeljak **Adresa udaljenog računala (IPv4/IPv6, raspon, maska)**.
3. Kliknite **U redu**.

Dodatne informacije potražite u odjeljku Uređivanje IP skupova.

Uređivanje IP skupova

Dodatne informacije o IP skupovima potražite u odjeljku IP skupovi.

Stupci

Naziv – Naziv grupe udaljenih računala.

Opis – Općeniti opis grupe.

IP adrese – udaljene IP adrese koje pripadaju IP skupu.

Kontrolni elementi

Kada **dodajete** ili **uređujete** IP skup, dostupna su sljedeća polja:

Naziv – Naziv grupe udaljenih računala.

Opis – Općeniti opis grupe.

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

Izbriši – Uklanja zonu s popisa.

Unaprijed definirane IP skupove nije moguće ukloniti.

Primjeri IP adresa

Dodaj IPv4 adresu:

Jedna adresa – dodaje IP adresu pojedinačnog računala (na primjer, *192.168.0.10*).

Raspon adresa – unesite početnu i završnu IP adresu da biste odredili raspon IP adresa za nekoliko računala (na primjer *od 192.168.0.1 do 192.168.0.99*).

Podmreža – Podmreža (grupa računala) definira se putem IP adrese i maske. Na primjer, 255.255.255.0 mrežna je maska za podmrežu 192.168.1.0. Za isključivanje cijele vrste podmreže *192.168.1.0/24.*

Dodaj IPv6 adresu:

Jedna adresa – dodaje IP adresu pojedinačnog računala (na primjer, *2001:718:1c01:16:214:22ff:fec9:ca5*).

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

Zaštita od mrežnog napada (IDS)

Zaštita od mrežnog napada (IDS) poboljšava otkrivanje zlouporaba poznatih ranjivosti. Više o zaštiti od mrežnog napada pročitajte u Rječniku. Da biste konfigurirali zaštitu od mrežnog napada, otvorite Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** > **Zaštita od mrežnog napada**.

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

Aktiviraj zaštitu od botneta – Otkriva i blokira komunikaciju sa zlćudnim naredbama i kontrolnim serverima na temelju tipičnih obrazaca kada je računalo zaraženo i bot pokušava komunicirati. Pročitajte više o zaštiti od botneta u rječniku.

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

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

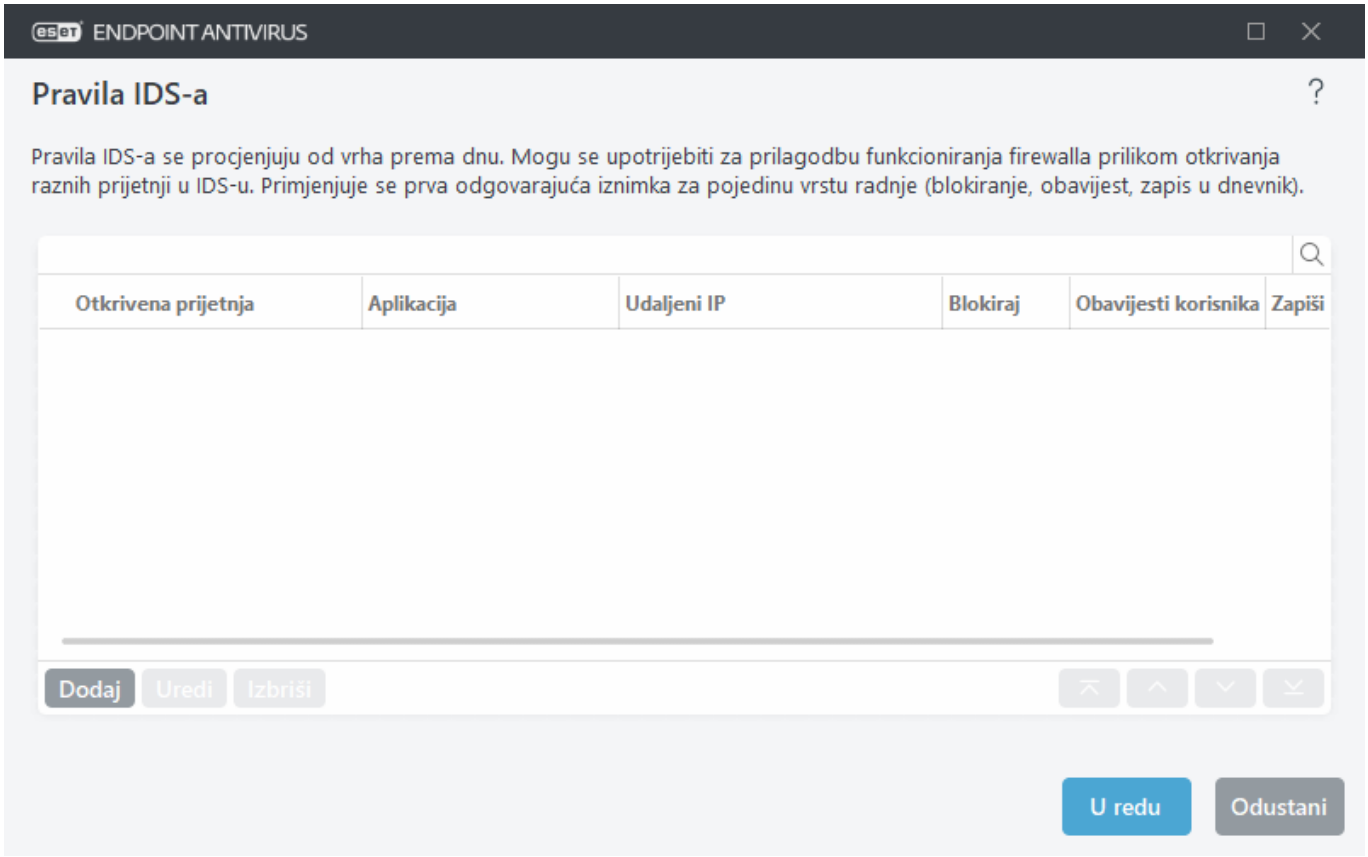
Pravila IDS-a

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

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
- Stvaranje pravila IDS-a o klijentskim radnim stanicama u programu ESET Endpoint Antivirus
- Izrada pravila IDS-a za klijentske radne stanice u programu ESET PROTECT

Upravljanje pravilima IDS-a

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



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

Uređivač pravila

Prijetnja – vrsta prijetnje.

Naziv prijetnje – možete navesti naziv prijetnje za neke od dostupnih detekcija.

Aplikacija – Odaberite put datoteke izuzete aplikacijetako da kliknete na ... (na primjer *C:\Program Files\Firefox\Firefox.exe*). NEMOJTE upisati vrstu aplikacije.

Udaljena IP adresa – popis udaljenih IPv4 ili IPv6 adresa / raspona / podmreža. Adrese moraju biti odvojene zarezom.

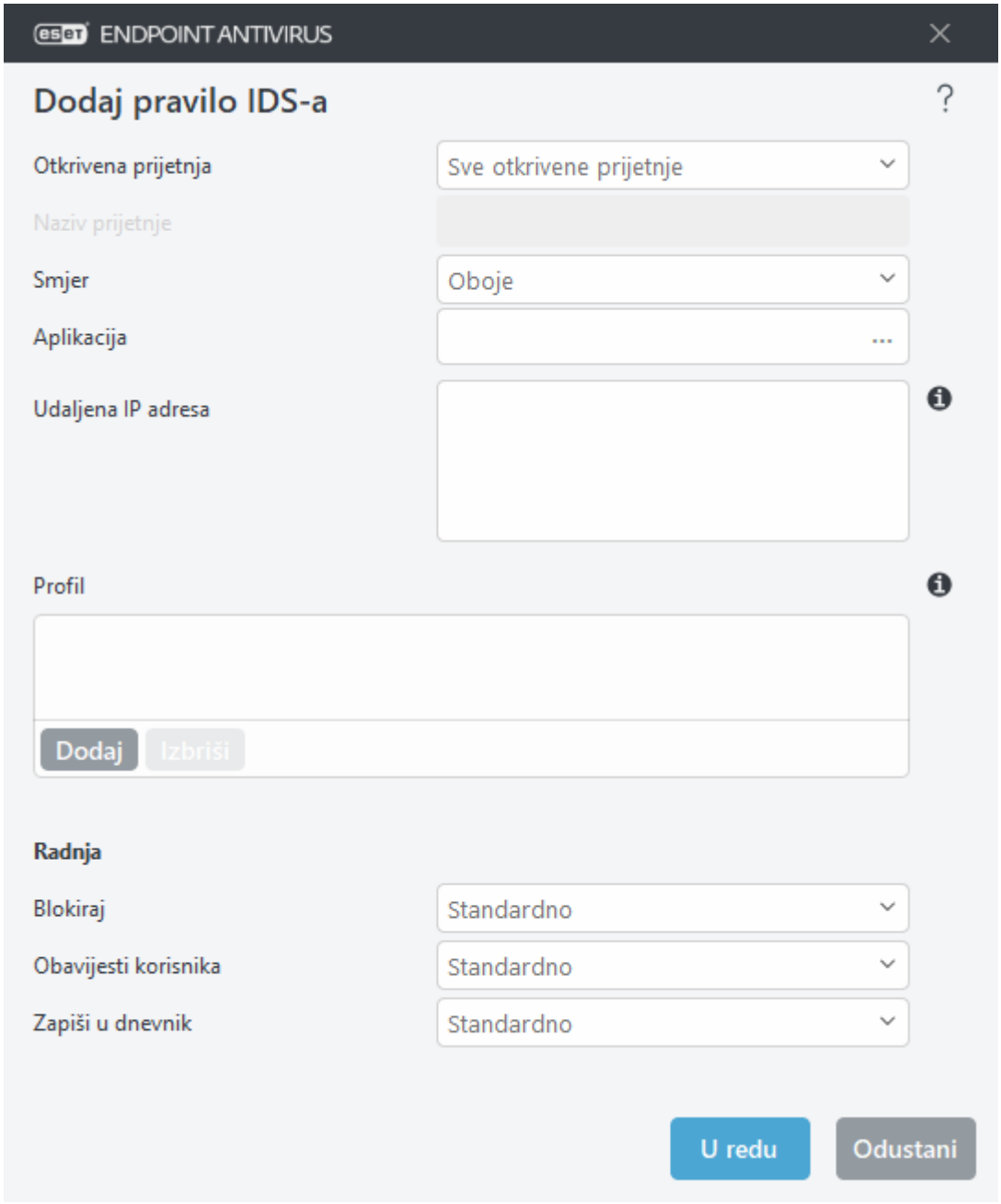
Profil možete odabrati profil mrežne veze na koji će se ovo pravilo primjenjivati.

Akcija

Blokiraj – Svaki sistemski proces ima svoje standardno ponašanje i dodijeljenu radnju (blokiranje ili dopuštanje). Da biste nadjačali standardno ponašanje za program ESET Endpoint Antivirus, putem padajućeg izbornika možete odabrati želite li blokirali ili dopustiti.

Obavijesti – Odaberite Da za prikaz Obavijesti na radnoj površini na računalu. Odaberite Ne ako ne želite obavijesti na radnoj površini. Dostupne su vrijednosti Standardno/Da/Ne.

Dnevnik – Odaberite **Da** za zapisivanje događaja u dnevnike programa ESET Endpoint Antivirus. Odaberite **Ne** ako ne želite zapisivati događaje u dnevnik. Dostupne su vrijednosti **Standardno**/**Da**/**Ne**.



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

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

Ako želite ukloniti učestale obavijesti za vrstu prijetnje za koju smatrate da nije prijetnja:
1. Kliknite **Dodaj** da biste dodali novu IDS iznimku.
2. Odaberite određenu prijetnju iz padajućeg izbornika **upozorenje**, na primjer **SMB sesija bez sigurnosnih ekstenzija**.
3. Odaberite **Ulaz** iz padajućeg izbornika smjera u slučaju da potječe od dolazne komunikacije.
4. Postavite padajući izbornik **Obavijesti** na **Ne**.
5. Postavite padajući izbornik **Dnevnik** na **Da**.
6. Ostavite stavku **Aplikacija** praznom.
7. Ako komunikacija ne dolazi s određene IP adrese, ostavite stavku **Udaljene IP adrese** praznom.
8. Kliknite **U redu** da biste spremili ovu obavijest.

Zaštita od napada grubom silom

Zaštita od napada grubom silom blokira napade pogađanjem lozinke za RDP i SMB servise. Napad grubom silom je metoda otkrivanja ciljane lozinke koja obuhvaća sustavno isprobavanje svih kombinacija slova, brojeva i simbola. Da biste konfigurirali zaštitu od napada grubom silom, otvorite opciju Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** > **Zaštita od mrežnog napada** > **Zaštita od napada grubom silom**.

Aktiviraj zaštitu od napada grubom silom – ESET Endpoint Antivirus provjerava sadržaj mrežnog prometa i blokira pokušaje napada pogađanjem lozinki.

Pravila – omogućuju vam da stvarate, uređujete i pregledavate pravila za dolazne i odlazne mrežne veze. Za više informacija pogledajte Pravila.

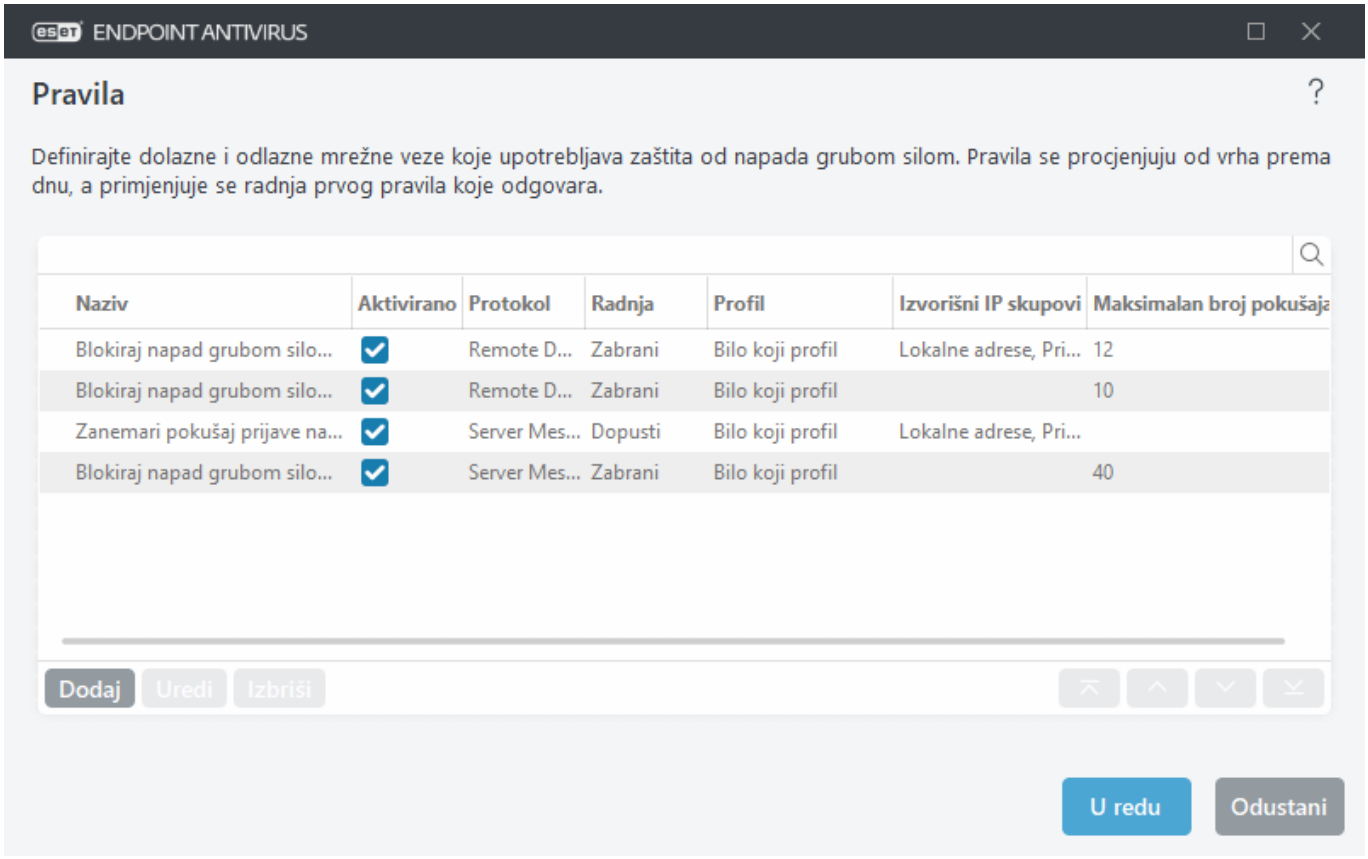
Izuzeci – popis izuzetih prijetnji koje se definiraju s pomoću IP adrese ili puta aplikacije. Možete stvarati i uređivati izuzetke na ESET PROTECT. Za više informacija pogledajte Izuzeci.

Pravila

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

Upravljanje pravilima zaštite od napada grubom silom

- **Dodaj** – kliknite da biste stvorili novo pravilo zaštite od napada grubom silom.
- **Uredi** – kliknite da biste uredili postojeće pravilo zaštite od napada grubom silom.
- **Ukloni** – označite i kliknite ako želite ukloniti postojeću iznimku s popisa pravila IDS-a.
-  **Vrh/gore/dolje/dno** – prilagodite razinu prioriteta pravila.



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

Uređivač pravila

Naziv – naziv pravila.

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

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

Protokol – komunikacijski protokol koji će ovo pravilo pregledati.

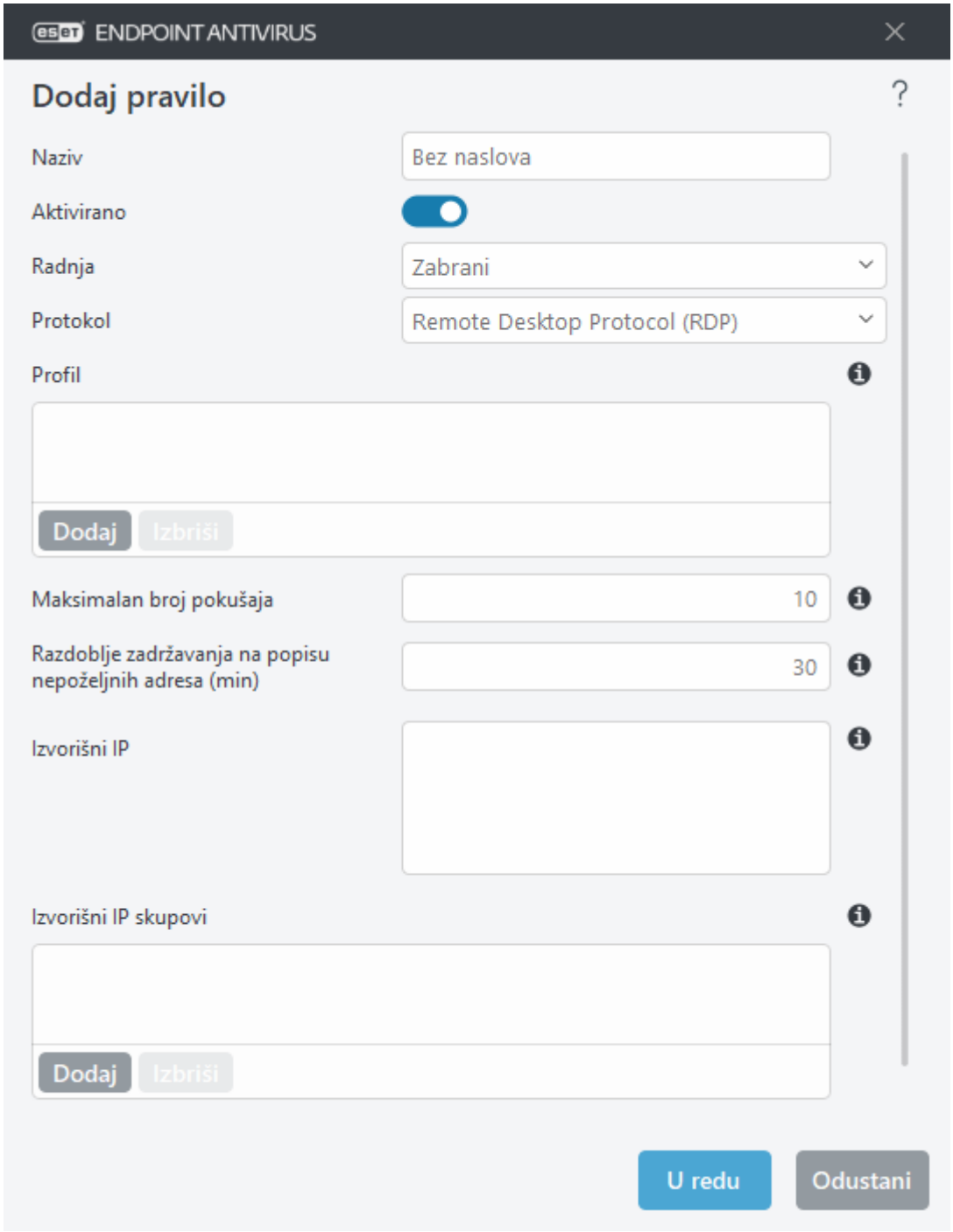
Profil možete odabrati profil mrežne veze na koji će se ovo pravilo primjenjivati.

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

Razdoblje zadržavanja na popisu nepoželjnih adresa (u minutama) – postavlja vrijeme nakon kojeg se adresa uklanja s popisa nepoželjnih adresa.

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

Izvorišni IP skupovi – skup IP adresa koje ste već definirali u stavci IP skupovi.



Izuzeci

Izuzeci napada grubom silom mogu se upotrijebiti za suzbijanje prijetnji napada grubom silom za određene kriterije. Ti izuzeci se stvaraju u programu ESET PROTECT na temelju prijetnje napada grubom silom.

Stupci

- **Prijetnja** – vrsta prijetnje.
- **Aplikacija** – Odaberite put datoteke izuzete aplikacijetako da kliknete na ... (na primjer *C:\Program Files\Firefox\Firefox.exe*). NEMOJTE upisati vrstu aplikacije.
- **Udaljeni IP** – Popis udaljenih IPv4 ili IPv6 adresa/raspona/podmreža. Adrese moraju biti odvojene zarezom.

Upravljanje izuzecima

Izuzeci će se prikazati ako administrator stvori izuzetke napada grubom silom u ESET PROTECT web konzoli. Izuzeci napada grubom silom mogu sadržavati samo dopuštajuća pravila i procjenjuju se prije pravila IDS-a.

Napredne opcije

U opciji Napredno podešavanje > **Zaštite** > **Zaštita pristupa mreži** > **Zaštita od mrežnog napada** > **Napredne opcije** možete aktivirati ili deaktivirati detekciju nekoliko vrsta napada i izrabljivanja koje mogu oštetiti vaše računalo.

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

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

Otkrivanje upada

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

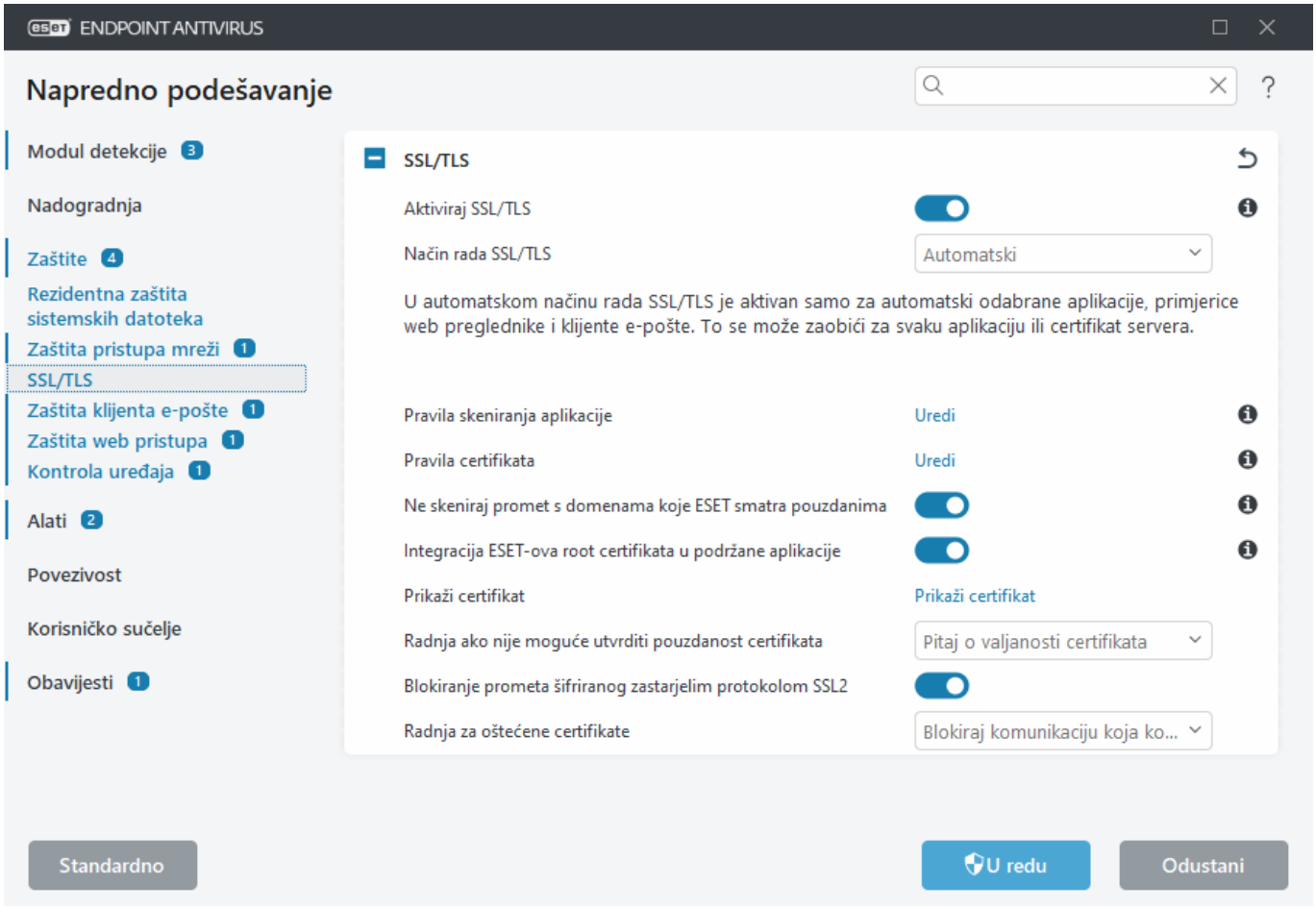
Provjera paketa

- **Dopusti dolaznu vezu za zajedničke mreže u SMB protokolu** – Zajedničke mreže odnose se ovdje na standardne zajedničke mreže koje dijele particije tvrdog diska (*C$*, *D$*, ...) u sustavu zajedno s mapom sustava (*ADMIN$*). Deaktiviranje veze sa zajedničkim mrežama trebalo bi smanjiti mnoge sigurnosne rizike. Primjerice, crv Conficker vrši napade "dictionary attack" kako bi uspostavio vezu sa zajedničkim mrežama.

- **Zabrani stare (nepodržane) SMB dijalekte** – Odbija se SMB sesija sa starim SMB dijalektom koji IDS ne podržava. Suvremeni operacijski sustavi Windows podržavaju stare SMB dijalekte zahvaljujući unazadnoj kompatibilnosti sa starim operacijskim sustavima kao što je Windows 95. Napadač može koristiti stari dijalekt u SMB sesiji kako bi izbjegao provjeru prometa. Zabranite stare SMB dijalekte ako računalo ne treba zajednički koristiti datoteke (ili SMB komunikaciju općenito) s računalom koje koristi staru verziju sustava Windows.
- **Zabrani SMB sesije bez povećane sigurnosti** – Povećana sigurnost može se koristiti tijekom pregovaranja SMB sesije kako bi se osigurao mehanizam autentikacije koji je sigurniji od autentikacije izazovom/odgovorom LAN upravitelja (LM). LM shema smatra se slabom i ne preporučuje se za upotrebu.
- **Dopusti komunikaciju sa servisom Security Account Manager** – Više informacija o ovom servisu pogledajte ovdje [MS-SAMR].
- **Dopusti komunikaciju sa servisom Local Security Authority** – Više informacija o ovom servisu pogledajte ovdje [MS-LSAD] i ovdje [MS-LSAT].
- **Dopusti komunikaciju sa servisom Remote Registry** – Više informacija o ovom servisu pogledajte ovdje [MS-RRP].
- **Dopusti komunikaciju sa servisom Service Control Manager** – Više informacija o ovom servisu pogledajte ovdje [MS-SCMR].
- **Dopusti komunikaciju sa servisom Server** – Više informacija o ovom servisu pogledajte ovdje [MS-SRVS].
- **Dopusti komunikaciju s drugim servisima** – Drugi MSRPC servisi. MSRPC je Microsoftova implementacija mehanizma DCE RPC. Osim toga, MSRPC može za prijenos (ncacn_np transport) koristiti cijevi s nazivom koje su prenesene u protokol SMB (zajedničko korištenje mrežnih datoteka). MSRPC servisi nude sučelja za udaljeno pristupanje i upravljanje prozorima. Otkriveno je i iskorišteno "in the wild" nekoliko sigurnosnih slabosti u sustavu Windows MSRPC (Na primjer: crv Conficker, crv Sasser...). Deaktivirajte komunikaciju s MSRPC servisima koja vam nije potrebna kako biste umanjili mnoge sigurnosne rizike (kao što je udaljeno izvršavanje koda ili napad uskraćivanjem usluge).

SSL/TLS

ESET Endpoint Antivirus može provjeriti komunikacijske prijetnje koje koriste SSL protokol. Možete koristiti različite načine skeniranja za pregled komunikacije s SSL zaštitom uz pouzdane certifikate, nepoznate certifikate ili certifikate koji su isključeni iz provjere komunikacije s SSL zaštitom. Da biste uredili SSL/TLS postavke, otvorite Napredno podešavanje > **Zaštite** > **SSL/TLS**.



Aktivirajte SSL/TLS – ako je značajka deaktivirana, ESET Endpoint Antivirus neće skenirati komunikaciju putem SSL/TLS protokola.

SSL/TLS način dostupan je u sljedećim opcijama:

Način filtriranja	Opis
Automatski	Standardni način rada skenirat će samo odgovarajuće aplikacije kao što su web preglednici i klijenti e-pošte. Možete ga nadjačati odabirom aplikacija u kojima se skenira komunikacija.
Interaktivno	Ako unesete novu web stranicu s SSL zaštitom (s nepoznatim certifikatom), prikazat će se prozor za odabir radnje. Taj način rada omogućuje vam stvaranje popisa SSL certifikata / aplikacija koji će se izuzeti od skeniranja.
Na temelju pravila	Odaberite ovu opciju da biste skenirali svu komunikaciju s SSL zaštitom osim komunikacije koja je zaštićena certifikatima izuzetima od provjere. Ako se uspostavi nova komunikacija koja koristi nepoznati potpisani certifikat, nećete primiti obavijest i komunikacija će se automatski filtrirati. Kada pristupite serveru s nepouzdanim certifikatom koji ste sami označili kao pouzdan (nalazi se na popisu pouzdanih certifikata), komunikacija sa serverom se dopušta i sadržaj komunikacijskog kanala se filtrira.

Pravila skeniranja aplikacija – omogućuje prilagodbu funkcioniranja programa ESET Endpoint Antivirus za određene aplikacije.

Popis poznatih certifikata – omogućuje prilagodbu ponašanja programa ESET Endpoint Antivirus za određene SSL certifikate.

Ne skeniraj promet s domenama koje ESET smatra pouzdanima – kada je značajka aktivirana, komunikacija s pouzdanim domenama bit će izuzeta iz skeniranja. Ugrađeni popis adresa koje ESET smatra pouzdanima određuje

pouzdanost domene.

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

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

Radnja koju treba poduzeti ako se ne može utvrditi pouzdanost certifikata – u nekim slučajevima certifikat web-stranice nije moguće provjeriti pomoću odredišta pouzdanih korijenskih ustanova za izdavanje certifikata (TRCA) (na primjer, certifikat je istekao, certifikat nije pouzdan, certifikat nije valjan za određenu domenu ili potpis koji se može raščlaniti, ali ne potpisuje certifikat ispravno). Legitimne web-stranice uvijek će koristiti pouzdane certifikate. Ako ga ne koriste, to može značiti da napadač nastoji dešifrirati vašu komunikaciju ili web-stranica ima tehničkih poteškoća.

Ako je odabrana opcija **Pitaj o valjanosti certifikata** (standardna postavka), morate odabrati radnju koja će se provesti prilikom uspostavljanja šifrirane komunikacije. Prikazat će se dijaloški okvir za odabir radnje u kojem certifikat možete označiti kao pouzdan ili izuzet. Ako se certifikat ne nalazi na TRCA popisu, prozor će biti crven. Ako se certifikat nalazi na TRCA popisu, prozor će biti zelen.

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

Blokiranje prometa šifriranog zastarjelim SSL2 protokolom – komunikacija pomoću starije verzijeSSL protokola automatski će biti blokirana.

Radnja koju treba poduzeti za oštećene certifikate – oštećeni certifikat znači da certifikat koristi format koji nije prepoznao ESET Endpoint Antivirus ili je oštećen (na primjer, slučajno prebrisan podacima). U tom slučaju preporučujemo da opcija **Blokiraj komunikaciju koja upotrebljava certifikat** ostane odabrana. Ako je odabrana opcija **Pitaj o valjanosti certifikata** , od korisnika će se zatražiti da odabere radnju koja će se provesti prilikom uspostavljanja šifrirane komunikacije.

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

Pravila skeniranja aplikacije

Pravila skeniranja aplikacije mogu se upotrebljavati za podešavanje funkcioniranja programa ESET Endpoint Antivirus za određene aplikacije i za pamćenje radnji koje su odabrane kada je **Način rada SSL/TLS protokola** postavljen na **Interaktivni način**. Popis se može pregledavati i uređivati u stavci Napredno podešavanje > **Zaštite** > **SSL/TLS** > **Pravila skeniranja aplikacije** > **Uredi**.

Prozor **Pravila skeniranja aplikacije** sadržava sljedeće stavke:

Stupci

Aplikacija – Odaberite izvršnu datoteku iz stabla direktorija, kliknite opciju **...** ili unesite put ručno.

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

Kontrolni elementi

Dodaj – Dodajte filtriranu aplikaciju.

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

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

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

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

Pravila certifikata

Pravila certifikata mogu se koristiti za prilagodbu funkcioniranja programa ESET Endpoint Antivirus za određene SSL certifikate i za pamćenje radnji odabranih kada je **Način rada SSL/TLS protokola** postavljen na **Interaktivni**. Popis se može pregledavati i uređivati u stavci Napredno podešavanje > **Zaštite** > **SSL/TLS** > **Pravila certifikata** > **Uredi**.

Prozor **Pravila certifikata** sadržava sljedeće stavke:

Stupci

Naziv – Naziv certifikata.

Izdavač certifikata – Naziv izdavača certifikata.

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

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

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

Kontrolni elementi

Dodaj – Dodajte novi certifikat i prilagodite njegove postavke za opcije pristupa i skeniranja.

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

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

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

Šifrirani mrežni promet

Ako je računalo konfigurirano za uporabu SSL/TLS skeniranja, u sljedeće dvije situacije prikazat će se dijaloški okvir s upitom o daljnjim radnjama:

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

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

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

U oba slučaja korisnik može odabrati upamćivanje odabrane akcije. Spremljene radnje pohranjuju se u stavci Pravila certifikata.

Zaštita klijenta e-pošte

Da biste konfigurirali zaštitu klijenta e-pošte otvorite Napredno podešavanje > **Zaštite** > **Zaštita klijenta e-pošte** i odaberite jednu od sljedećih konfiguracijskih opcija:

- Zaštita prijenosa e-pošte
- Zaštita poštanskog sandučića
- ThreatSense

Zaštita prijenosa e-pošte

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

ESET Endpoint Antivirus omogućuje zaštitu tih protokola neovisno o korištenom klijentu e-pošte i bez potrebe za ponovnom konfiguracijom klijenta e-pošte. Prema standardnim postavkama sva se komunikacija putem protokola POP3 i IMAP skenira, neovisno o standardnim brojevima portova protokola POP3/IMAP.
Protokol MAPI nije skeniran. Međutim, komunikacija s Microsoft Exchange serverom može se skenirati integracijskim modulom u klijentima e-pošte kao što je Microsoft Outlook.

ESET Endpoint Antivirus podržava i skeniranje protokola IMAPS (585, 993) i POP3S (995) koji koriste šifrirani kanal za prijenos informacija između servera i klijenata. ESET Endpoint Antivirus provjerava komunikaciju koja koristi protokole SSL (Secure Socket Layer) i TLS (Transport Layer Security).
Šifrirana komunikacija skenirat će se prema standardnim postavkama. Da biste pogledali podešavanje skenera, otvorite Napredno podešavanje > **Zaštite** > SSL/TLS.

Da biste konfigurirali zaštitu prijenosa pošte, otvorite Napredno podešavanje > **Zaštite** > **Zaštita klijenta e-pošte** > **Zaštita prijenosa e-pošte**.

Aktiviraj zaštitu prijenosa e-pošte – kada je aktivirano, komunikacija prijenosa e-pošte skenira se programom ESET Endpoint Antivirus.

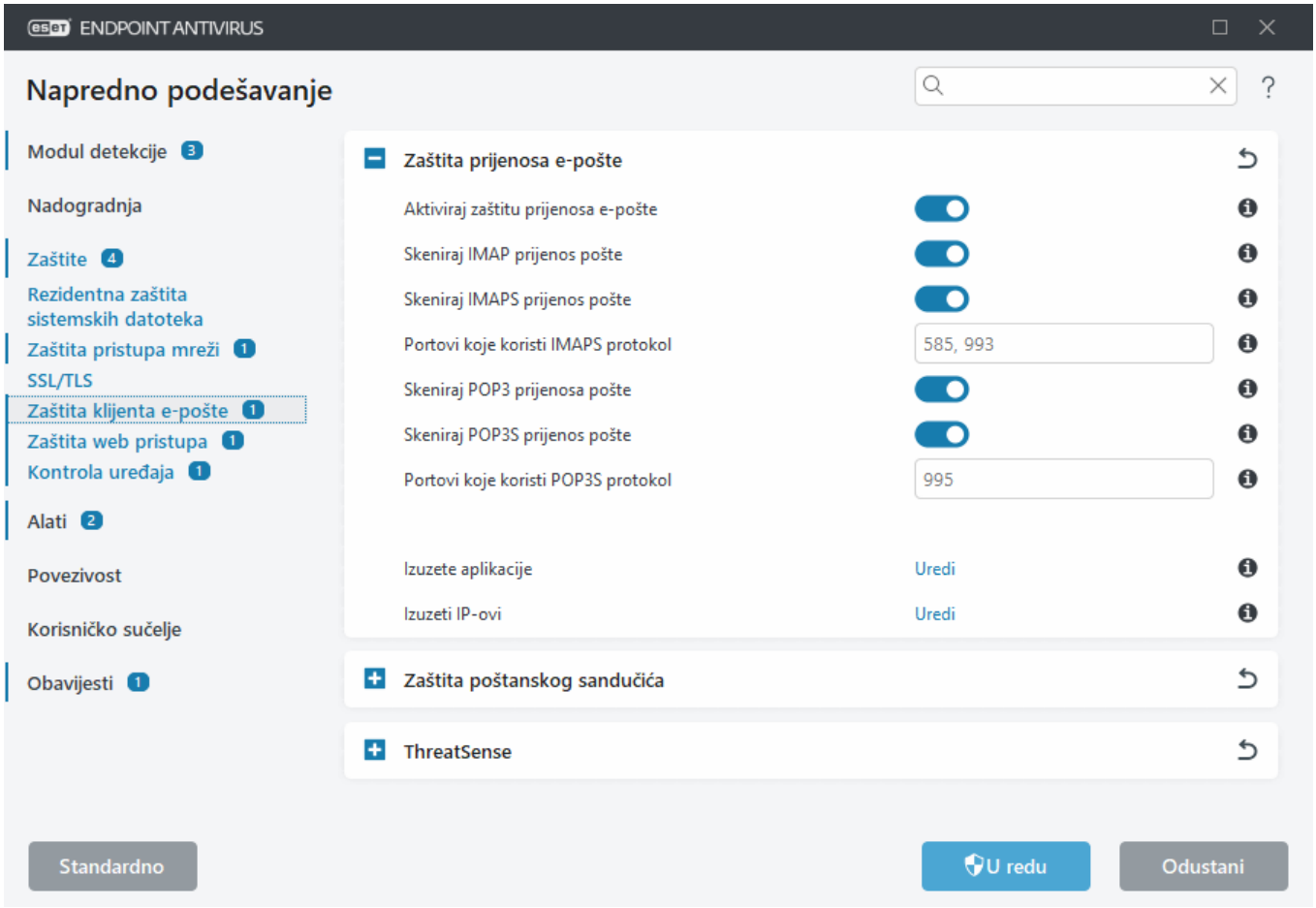
Možete odabrati koji će se protokoli za prijenos e-pošte skenirati klikom na klizač pored sljedećih opcija (prema zadanim postavkama aktivirano je skeniranje svih protokola):

- **Skeniraj IMAP prijenos pošte**
- **Skeniraj IMAPS prijenos pošte**
- **Skeniraj POP3 prijenos pošte**
- **Skeniraj POP3S prijenos pošte**

Prema zadanim postavkama ESET Endpoint Antivirus skenira IMAPS i POP3S komunikaciju na standardnim priključcima. Da biste dodali prilagođene priključke za IMAPS i POP3S protokole, dodajte ih u tekstualno polje pokraj **priključaka koje koristi IMAPS protokol** ili **priključaka koje koristi POP3S protokol**. Višestruke brojeve portova potrebno je razgraničiti zarezima.

Izuzete aplikacije – omogućuje vam da izuzmete određene aplikacije iz skeniranja zaštitom prijenosa pošte. Ta je opcija korisna kada zaštita web pristupa uzrokuje probleme s kompatibilnošću.

Izuzeti IP-ovi – omogućuje vam da isključite određene udaljene adrese iz skeniranja zaštite prijenosa pošte. Ta je opcija korisna kada zaštita web pristupa uzrokuje probleme s kompatibilnošću.



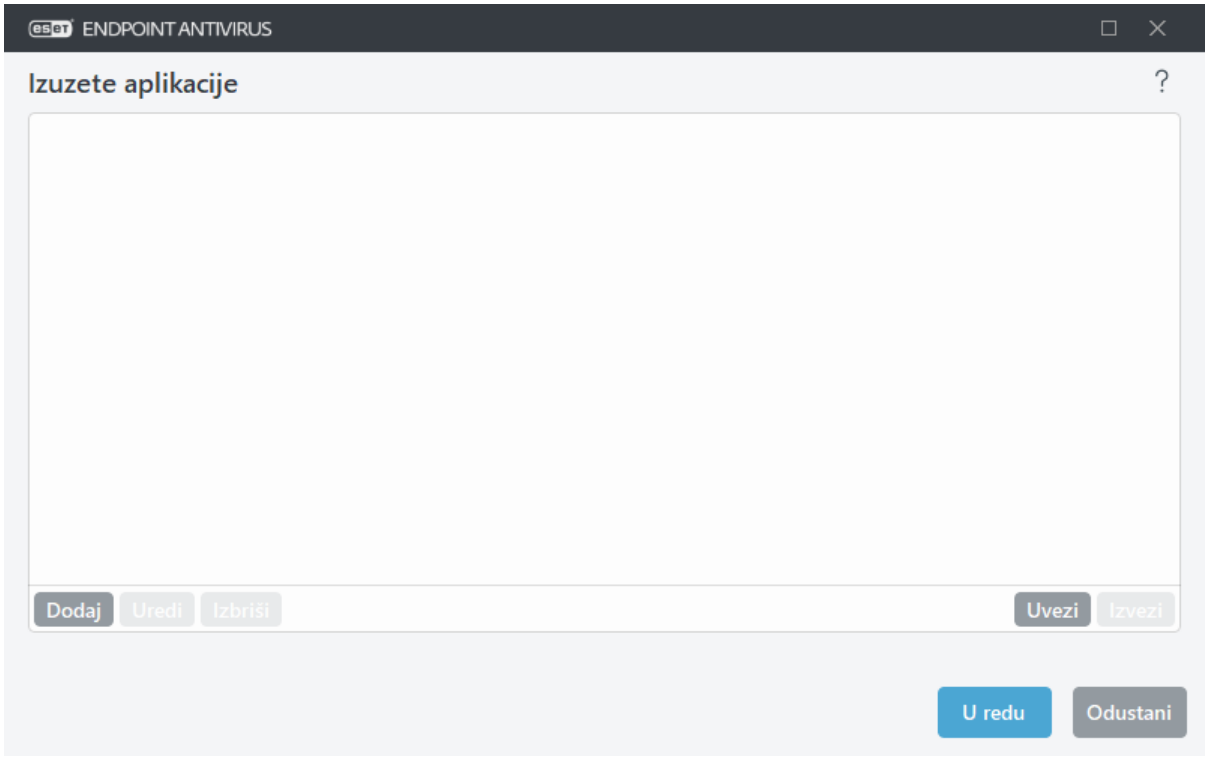
Izuzete aplikacije

Da biste izuzeli određene aplikacije iz skeniranja komunikacije, dodajte ih na popis. HTTP(S)/POP3(S)/IMAP(S) komunikacija odabranih aplikacija neće se provjeravati da bi se pronašle prijetnje. Preporučujemo da tu mogućnost koristite samo za aplikacije koje ne rade ispravno ako se njihova komunikacija provjerava.

Aplikacije i servisi koji se izvršavaju ovdje će biti automatski dostupni nakon što kliknete **Dodaj**. Kliknite **...** i idite do aplikacije da biste ručno dodali izuzetak.

Uredi – Uređivanje odabranih unosa na popisu.

Ukloni – Uklanjanje odabranih unosa s popisa.



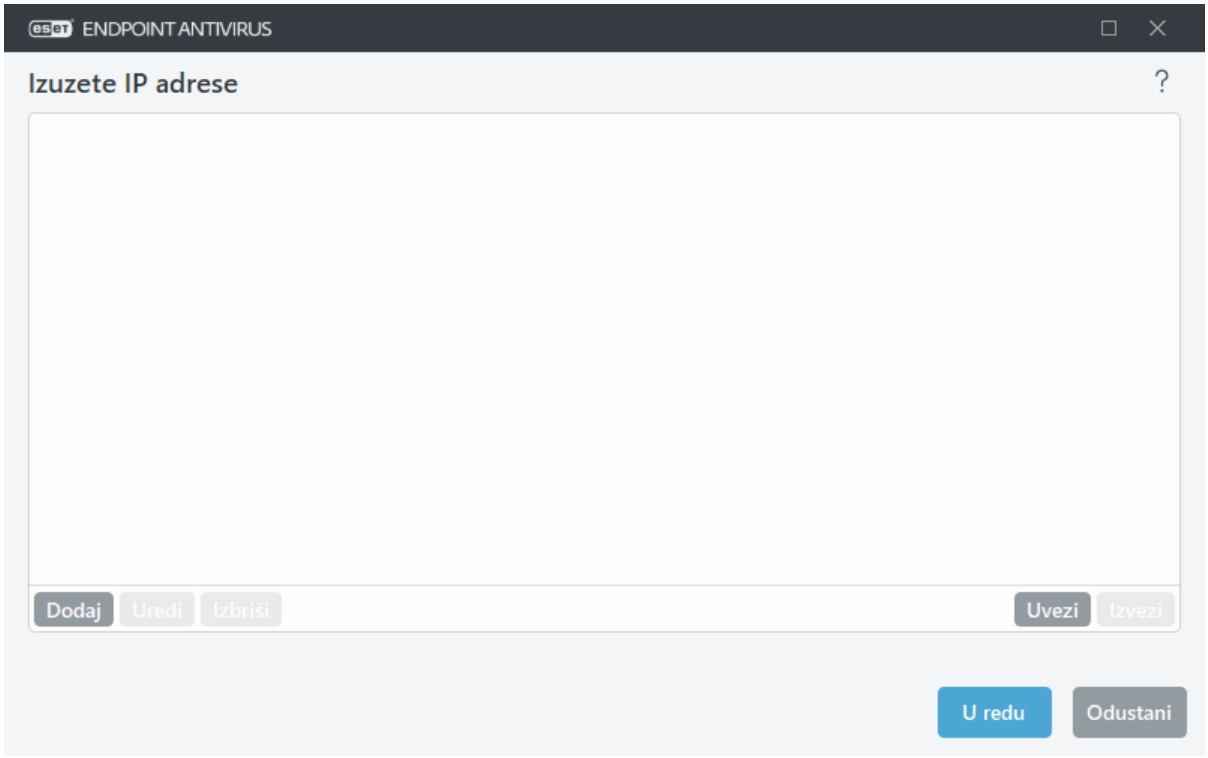
Izuzeti IP-ovi

Unosi na popisu izuzet će se iz skeniranja. HTTP(S)/POP3(S)/IMAP(S) komunikacija s/na odabrane adrese neće se provjeravati da bi se pronašle prijetnje. Preporučujemo da tu mogućnost koristite samo za pouzdane adrese.

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

Uredi – Uređivanje odabranih unosa na popisu.

Ukloni – Uklanjanje odabranih unosa s popisa.



Primjeri IP adresa

Dodaj IPv4 adresu:

Jedna adresa – dodaje IP adresu pojedinačnog računala (na primjer, *192.168.0.10*).

Raspon adresa – unesite početnu i završnu IP adresu da biste odredili raspon IP adresa za nekoliko računala (na primjer *od 192.168.0.1 do 192.168.0.99*).

Podmreža – Podmreža (grupa računala) definira se putem IP adrese i maske. Na primjer, 255.255.255.0 mrežna je maska za podmrežu 192.168.1.0. Za isključivanje cijele vrste podmreže *192.168.1.0/24.*

Dodaj IPv6 adresu:

Jedna adresa – dodaje IP adresu pojedinačnog računala (na primjer, *2001:718:1c01:16:214:22ff:fec9:ca5*).

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

Zaštita poštanskog sandučića

Integracija programa ESET Endpoint Antivirus s klijentom e-pošte povećava razinu aktivne zaštite od zlonamjernog koda u poštanskom sandučiću.

Da biste konfigurirali zaštitu poštanskog sandučića, otvorite Napredno postavljanje > **Zaštite** > **Zaštita klijenta e-pošte** > **Zaštita poštanskog sandučića**.

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

Odaberite e-poruke za skeniranje:

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

Preporučujemo da aktivirate opciju **Aktiviraj zaštitu e-pošte klijentskim dodacima**. Čak i ako integracija nije aktivirana ili funkcionalna, komunikacija e-poštom svejedno je zaštićena značajkom Zaštita prijenosa e-pošte (IMAP/IMAPS i POP3/POP3S).

Integracije – aktivira integraciju zaštite poštanskog sandučića u klijent e-pošte. Pogledajte Integracije za dodatne informacije.

Odgovor – omogućuje prilagodbu upravljanja neželjenim porukama. Pogledajte Odgovor za dodatne informacije.

Integracije

Integracija programa ESET Endpoint Antivirus s klijentom e-pošte povećava razinu aktivne zaštite od zlonamjernog koda u porukama e-pošte. Ako je klijent e-pošte podržan, integraciju možete aktivirati u programu ESET Endpoint Antivirus. Nakon integracije u klijent e-pošte alatna traka programa ESET Endpoint Antivirus umeće se izravno u klijent e-pošte za učinkovitiju zaštitu e-pošte. Da biste uredili postavke integracije, otvorite stavku Napredno podešavanje > **Zaštite** > **Zaštita klijenta e-pošte** > **Zaštita poštanskog sandučića** > **Integracija**.

Integriraj u Microsoft Outlook – Microsoft Outlook trenutačno je jedini podržani klijent za e-poštu. Zaštita e-pošte funkcionira kao dodatak. Glavna je prednost dodatka to da on ne ovisi o protokolu koji se koristi. Kada klijent e-pošte primi šifriranu poruku, ona se dešifrira i šalje skeneru virusa. Pogledajte potpuni popis podržanih verzija za Microsoft Outlook u sljedećem članku ESET-ove baze znanja.

Napredna obrada klijenta e-pošte – obrađuje dodatne Outlook Messaging API (MAPI) događaje: Objekt je izmijenjen (`fnevObjectModified`) i Objekt je izrađen (`fnevObjectCreated`). Ako primijetite da sustav radi sporije kada se služite klijentom e-pošte, deaktivirajte ovu opciju.

Alatna traka za Microsoft Outlook

Zaštita programa Microsoft Outlook radi kao dodatni modul. Nakon instalacije programa ESET Endpoint Antivirus ova alatna traka koja sadrži antivirusnu zaštitu dodaju se u Microsoft Outlook:

ESET Endpoint Antivirus – dvokliknite ikonu da biste otvorili glavni prozor programa ESET Endpoint Antivirus.

Ponovno skeniraj poruke – Omogućuje ručno pokretanje provjere e-pošte. Možete odrediti koje poruke želite skenirati te ponovno pokrenuti skeniranje primljene e-pošte. Za više informacija pogledajte odjeljak Zaštita poštanskog sandučića.

Podešavanje skenera – prikazuje opcije za podešavanje stavke Zaštita poštanskog sandučića.

Dijaloški okvir s potvrdom

Ta obavijest služi kao potvrda da korisnik zaista želi izvršiti odabranu akciju čime bi se trebale eliminirati moguće pogreške.

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

Ponovno skeniranje poruka

Antivirusna alatna traka sustava ESET Endpoint Antivirus integrirana u klijente e-pošte korisnicima omogućuje da navedu nekoliko mogućnosti provjere poruka e-pošte. Mogućnost **Ponovno skeniraj poruke** nudi dva načina skeniranja:

Sve poruke u trenutačnoj mapi – Skenira poruke u mapi koja je trenutačno prikazana.

Samo odabrane poruke – Skenira samo one poruke koje je korisnik označio.

Potvrdni okvir **Ponovno skeniraj već skenirane poruke** korisniku nudi mogućnost pokretanja novog skeniranja poruka koje su ranije već skenirane.

Odgovor

Na temelju rezultata skeniranja poruke ESET Endpoint Antivirus može premještati skenirane poruke ili dodavati prilagođeni tekst predmetu. Te postavke možete konfigurirati u stavci Napredno podešavanje > **Zaštite** > **Zaštita klijenta e-pošte** > **Zaštita poštanskog sandučića** > **Odgovor**.

Ako postoji poruka koja sadrži parametar za otkrivanje, prema zadanim postavkama ESET Endpoint Antivirus pokušat će očistiti poruku. Ako se poruka ne može očistiti, možete odabrati **radnju koju treba poduzeti ako čišćenje nije moguće**:

- **Bez radnje** – ako je aktivirana ova opcija, program će prepoznavati zaražene privitke, ali neće poduzimati nikakve radnje na e-pošti.
- **Izbriši poruku e-pošte** – Program će obavještavati korisnika o infiltracijama i izbrisati poruku.
- **Premjesti poruku e-pošte u mapu s izbrisanim stavkama** – Zaražene poruke e-pošte automatski će se premjestiti u mapu Izbrisane stavke.
- **Premjesti poruku e-pošte u mapu** – Zaražene poruke e-pošte automatski će se premjestiti u navedenu mapu.

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

Nakon provjere, poruci e-pošte može se dodati obavijest s rezultatima skeniranja. Možete odabrati opciju **Dodaj oznake primljenim i pročitanim porukama e-pošte** ili **Dodaj oznake poslanim porukama e-pošte**. Imajte na umu da se u rijetkim slučajevima oznake mogu izostaviti u problematičnim HTML porukama ili ako ih zlonamjerni programi krivotvore. Oznake se mogu dodati primljenoj i pročitanoj e-pošti, poslanoj e-pošti ili objema. Dostupne su sljedeće opcije:

- **Nikad** – Neće se dodavati obavijesti uz poruke.
- **Kada se otkrije prijetnja** – Kao provjerene će se označavati samo one poruke koje sadrže zlonamjerni softver (standardna postavka).
- **Za svu e-poštu kada se skenira** – Program će dodati oznake svim skeniranim porukama e-pošte.

Ažuriraj naslov primljene i pročitane e-pošte / **Ažuriraj naslov poslane e-pošte** – aktivirajte ovu opciju ako u poruku želite dodati tekst naveden u nastavku.

Tekst koji se dodaje u naslov zaražene poruke e-pošte – Uredite predložak ako želite promijeniti format prefiksa koji se dodaje predmetu zaražene poruke e-pošte. Ova funkcija zamijenit će predmet poruke "Hello" u sljedeći format: "[prijetnja %DETECTIONNAME%] Hello". Varijabla %DETECTIONNAME% predstavlja otkrivenu prijetnju.

ThreatSense

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

Mogućnosti podešavanja tehnologije ThreatSense omogućuju vam određivanje nekoliko parametara skeniranja:

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

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

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

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

Objekti za skeniranje

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

Radna memorija – Skenira prijetnje koje napadaju radnu memoriju sustava.

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

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

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

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

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

podržava i mnoge druge vrste arhivatora.

Mogućnosti skeniranja

Odaberite postupke koji će se koristiti za skeniranje sustava radi otkrivanja infiltracija. Dostupne su sljedeće opcije:

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

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

Čišćenje

Postavke čišćenja određuju funkcioniranje programa ESET Endpoint Antivirus prilikom čišćenja objekata.

Izuzeci

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

Ostalo

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

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

Pokreni pozadinska skeniranja s niskim prioritetom – Svaki slijed skeniranja troši izvjesnu količinu sistemskih resursa. Ako radite s programima koji obilato koriste sistemske resurse, možete aktivirati pozadinsko skeniranje niskog prioriteta da biste resurse sačuvali za ostale aplikacije.

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

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

Sačuvaj vremensku oznaku zadnjeg pristupa – Odaberite ovu opciju ako želite sačuvati vrijeme zadnjeg pristupa

skeniranim datotekama umjesto njihove nadogradnje (npr. za korištenje sa sustavima sigurnosnog kopiranja).

Ograničenja

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

Postavke objekta

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

Maksimalno vrijeme skeniranja za objekt (u sekundama) – definira maksimalnu vremensku vrijednost za skeniranje datoteka u spremišnom objektu (kao što je RAR/ZIP arhiva ili e-poruka s više privitaka). Ova postavka se ne odnosi na samostalne datoteke. Ako je unesena korisnički definirana vrijednost i to vrijeme je proteklo, skeniranje će se zaustaviti što je prije moguće, neovisno o tome je li skeniranje svih datoteka u spremišnom objektu dovršeno. U slučaju arhive s velikim datotekama skeniranje će se zaustaviti tek nakon što se raspakira datoteka iz arhive (na primjer, kada je korisnički definirana varijabla 3 sekunde, ali raspakiravanje datoteke traje 5 sekundi). Ostale datoteke u arhivi se neće skenirati kada to vrijeme istekne. Da biste ograničili vrijeme skeniranja, uključujući veće arhive, upotrijebite opcije **Maksimalna veličina objekta** i **Maksimalna veličina datoteke u arhivi** (ne preporučuje se zbog mogućih sigurnosnih rizika). Standardna vrijednost: neograničeno.

Podešavanje skeniranja arhive

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

Maksimalna veličina datoteke u arhivi – Ova opcija omogućuje vam da odredite maksimalnu veličinu (raspakiranih) datoteka sadržanih u arhivama koje želite skenirati. Maksimalna vrijednost je 3 GB.

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

Zaštita web pristupa

Zaštita web-pristupa omogućuje konfiguriranje naprednih postavki modula Internetska zaštita . Sljedeće mogućnosti dostupne su u prozoru Napredno podešavanje > **Zaštite** > **Zaštita web pristupa** > **Zaštita web pristupa**:

Aktiviraj zaštitu web pristupa – Nakon deaktivacije te opcije zaštita web pristupa i Anti-Phishing zaštita neće raditi.

> Preporučujemo da zaštitu web pristupa ostavite aktiviranom i da u zadanim postavkama ne izuzimate nijednu aplikaciju ili IP adresu.

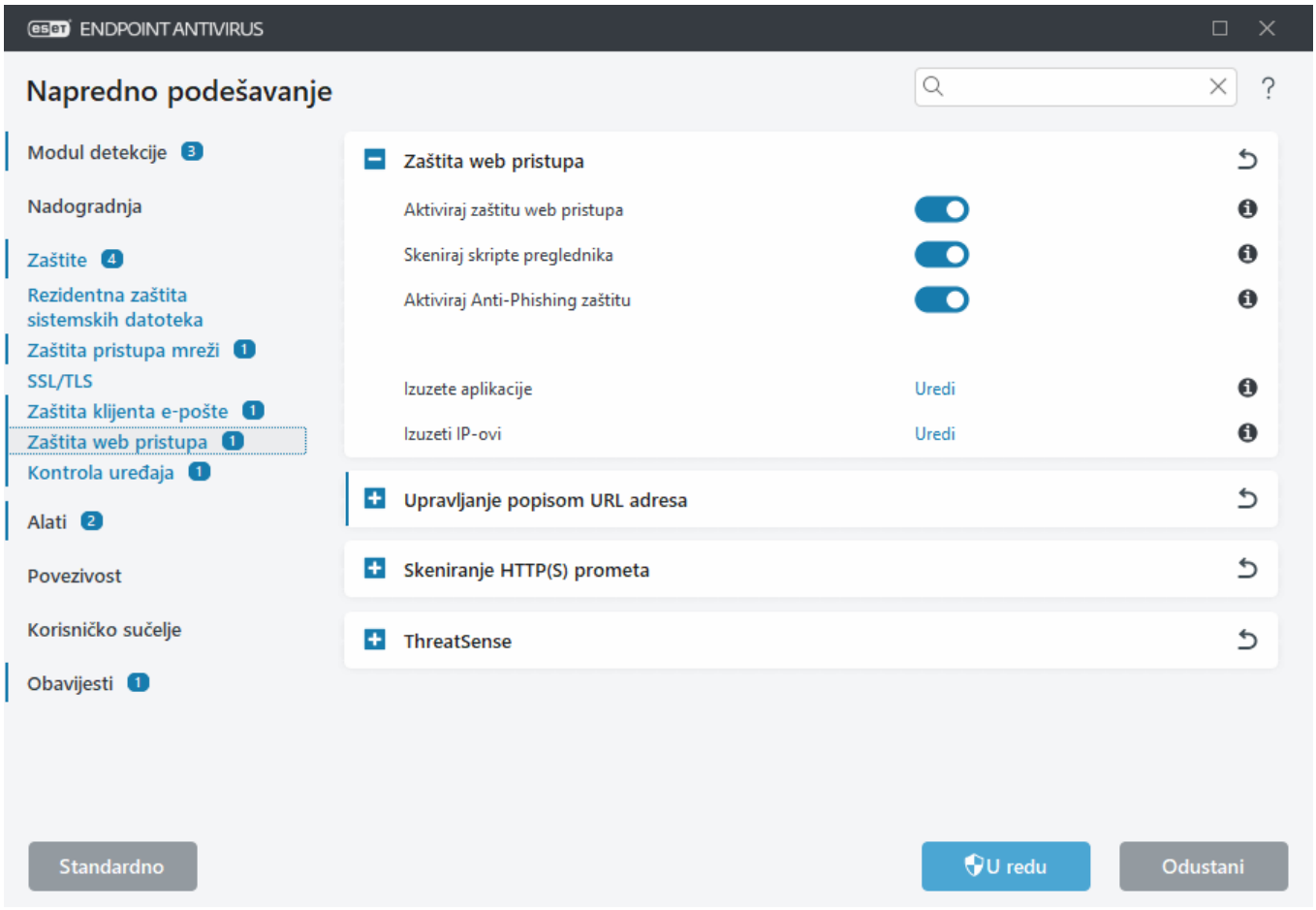
Skeniranje skripti preglednika – kada je značajka aktivirana, modul detekcije provjerava sve JavaScript programe koje izvršavaju web-preglednici.

Omogući anti-phishing zaštitu – kada značajka aktivirana, phishing web-stranice se blokiraju. Za više informacija

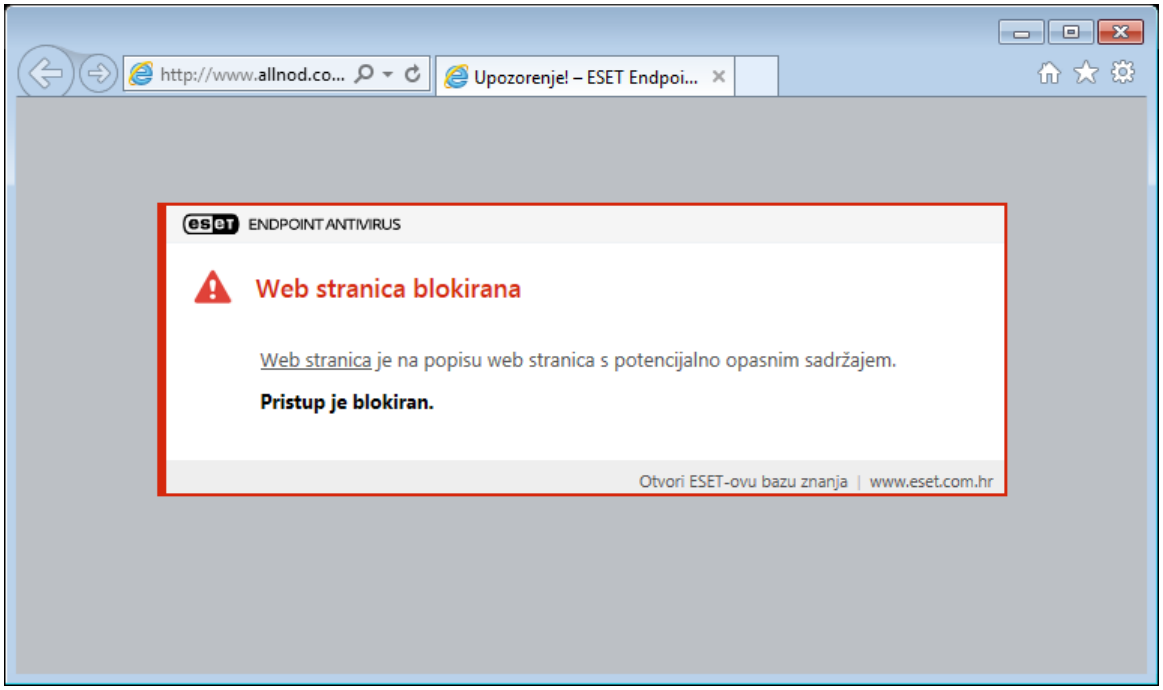
pogledajte članak Antiphishing zaštita.

Izuzete aplikacije – omogućuje vam da izuzmete određene aplikacije iz skeniranja zaštitom web pristupa. Ta je opcija korisna kada zaštita web pristupa uzrokuje probleme s kompatibilnošću.

Izuzeti IP-ovi – omogućuje vam da isključite određene udaljene adrese iz skeniranja zaštite web pristupa. Ta je opcija korisna kada zaštita web pristupa uzrokuje probleme s kompatibilnošću.



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



Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
- Deblokirajte sigurnu stranicu na pojedinačnoj radnoj stanici u programu ESET Endpoint Antivirus

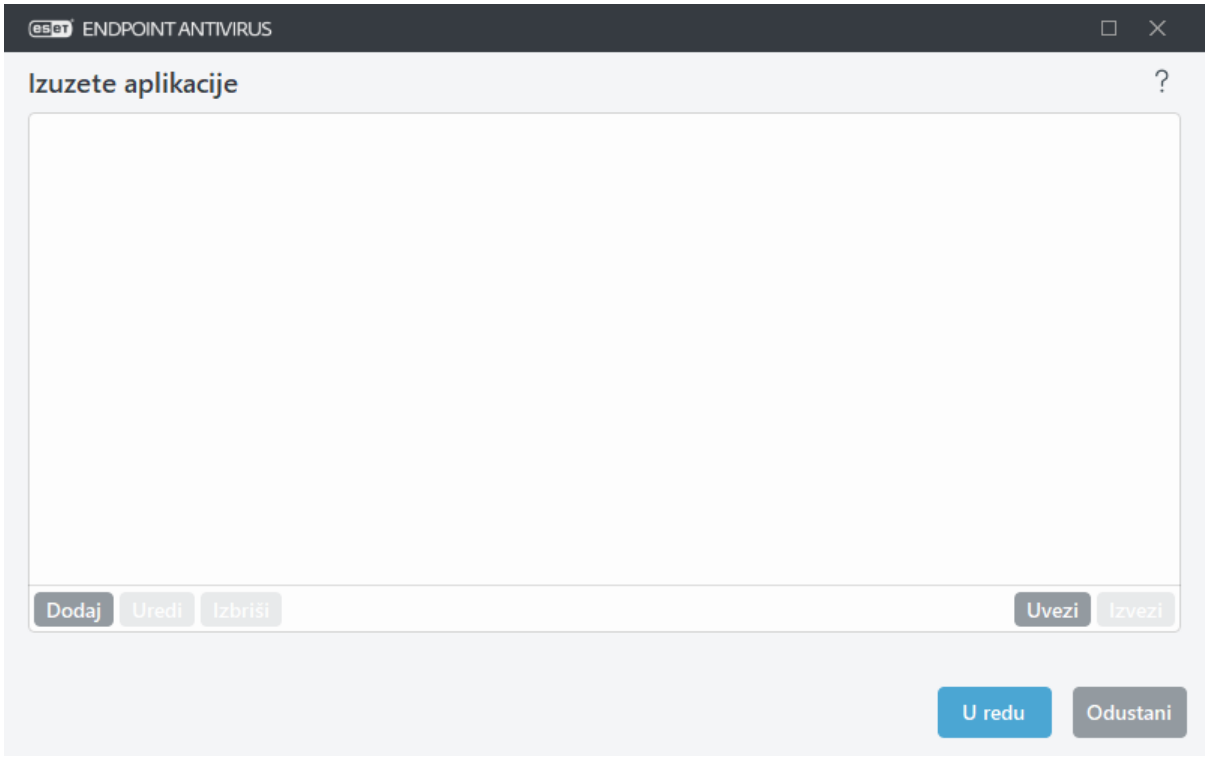
Izuzete aplikacije

Da biste izuzeli određene aplikacije iz skeniranja komunikacije, dodajte ih na popis. HTTP(S)/POP3(S)/IMAP(S) komunikacija odabranih aplikacija neće se provjeravati da bi se pronašle prijetnje. Preporučujemo da tu mogućnost koristite samo za aplikacije koje ne rade ispravno ako se njihova komunikacija provjerava.

Aplikacije i servisi koji se izvršavaju ovdje će biti automatski dostupni nakon što kliknete **Dodaj**. Kliknite **...** i idite do aplikacije da biste ručno dodali izuzetak.

Uredi – Uređivanje odabranih unosa na popisu.

Ukloni – Uklanjanje odabranih unosa s popisa.



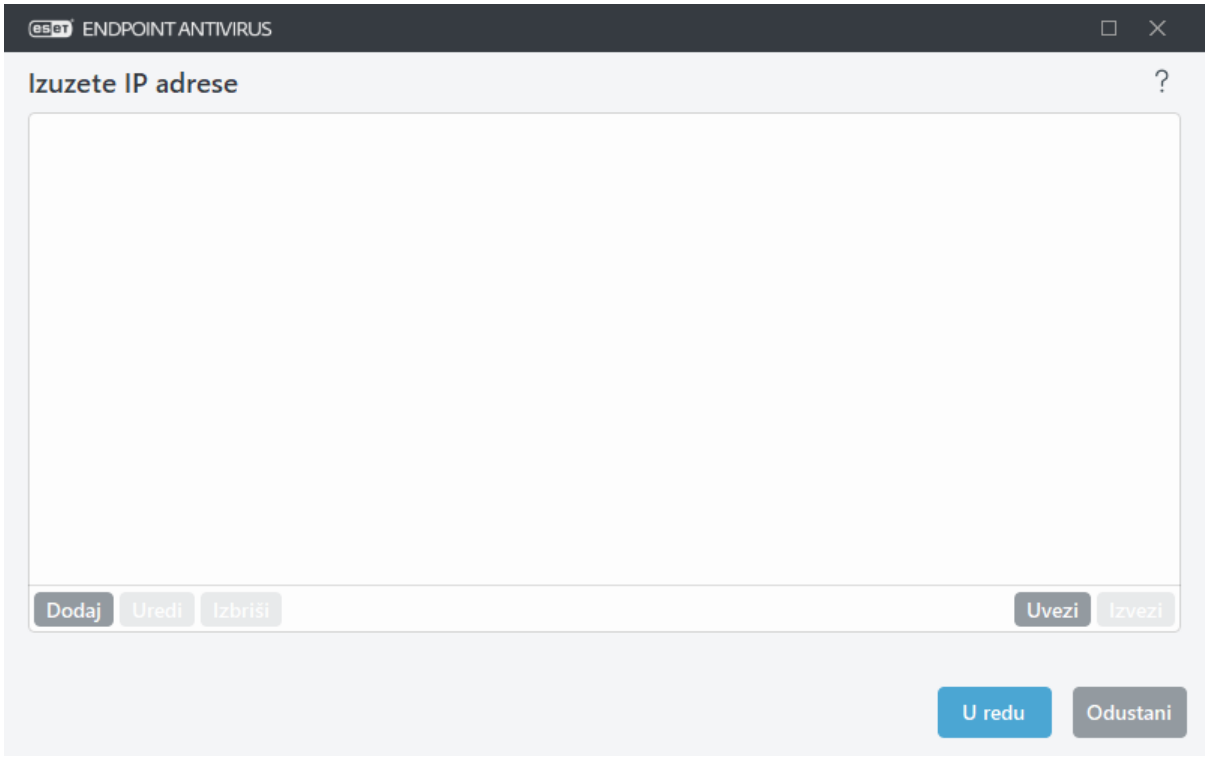
Izuzeti IP-ovi

Unosi na popisu izuzet će se iz skeniranja. HTTP(S)/POP3(S)/IMAP(S) komunikacija s/na odabrane adrese neće se provjeravati da bi se pronašle prijetnje. Preporučujemo da tu mogućnost koristite samo za pouzdane adrese.

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

Uredi – Uređivanje odabranih unosa na popisu.

Ukloni – Uklanjanje odabranih unosa s popisa.



Primjeri IP adresa

Dodaj IPv4 adresu:
Jedna adresa – dodaje IP adresu pojedinačnog računala (na primjer, *192.168.0.10*).
Raspon adresa – unesite početnu i završnu IP adresu da biste odredili raspon IP adresa za nekoliko računala (na primjer *od 192.168.0.1 do 192.168.0.99*).
Podmreža – Podmreža (grupa računala) definira se putem IP adrese i maske. Na primjer, 255.255.255.0 mrežna je maska za podmrežu 192.168.1.0. Za isključivanje cijele vrste podmreže *192.168.1.0/24.*
Dodaj IPv6 adresu:
Jedna adresa – dodaje IP adresu pojedinačnog računala (na primjer, *2001:718:1c01:16:214:22ff:fec9:ca5*).
Podmreža – Podmreža (grupa računala) definira se putem IP adrese i maske (na primjer: *2002:c0a8:6301:1::1/64*).

Upravljanje popisom URL adresa

Upravljanje popisom URL-ova u stavci Napredno podešavanje > **Zaštite** > **Zaštita web pristupa** omogućuje vam da odrediteHTTP adrese koje želite blokirati, dopustiti ili izuzeti iz skeniranja sadržaja.

SSL/TLS mora biti aktiviran ako želite filtrirati i HTTPS adrese uzHTTP adrese. U suprotnom će se dodati samo domene posjećenih HTTPS stranica, ali ne i puna URL adresa.

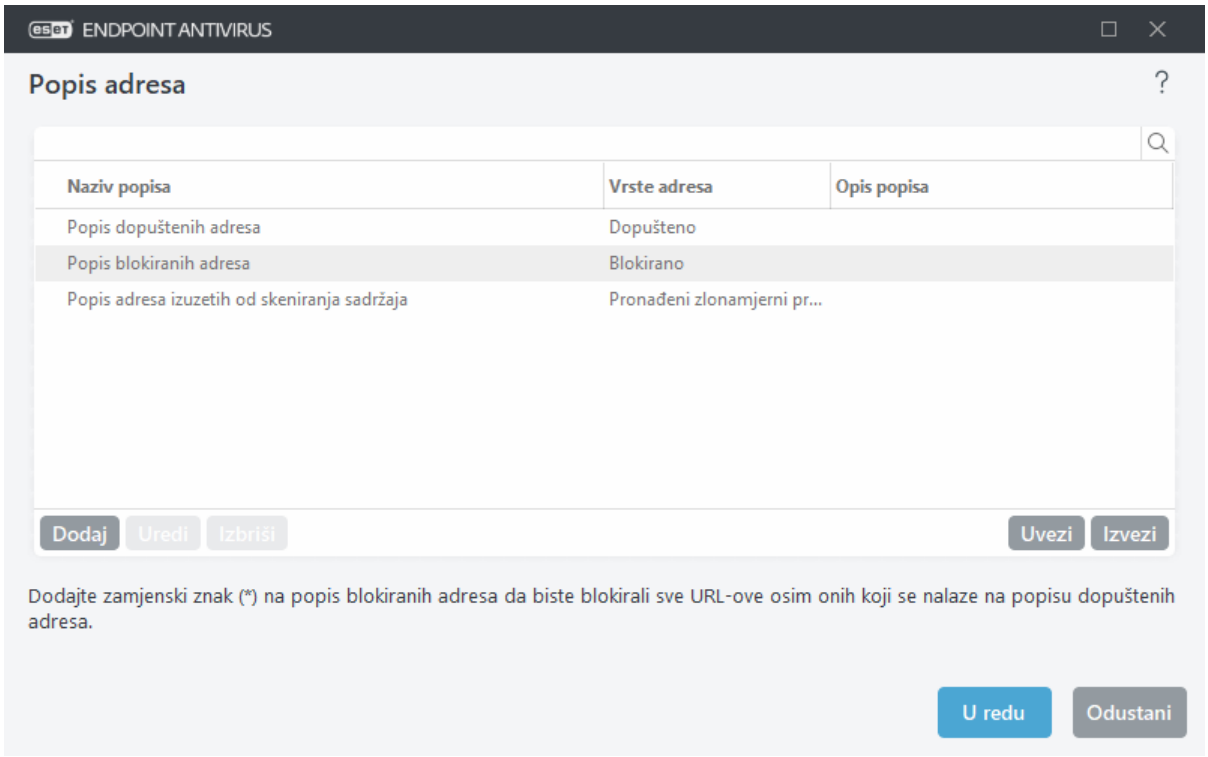
Web stranice s **popisa blokiranih adresa** neće biti dostupne, osim ako su uključene na **popis dopuštenih adresa**. Web stranice s **popisa adresa izuzetnih iz skeniranja sadržaja** bit će dostupne bez skeniranja za zlonamjernim kodom.

Ako želite blokirati sve HTTP adrese osim adresa prisutnih na aktivnom **popisu dopuštenih adresa**, dodajte * na aktivni **popis blokiranih adresa**.

Na tim popisima moguća je upotreba posebnih simbola * (zvjezdica) i ? (upitnik). Zvjezdica zamjenjuje bilo koji niz znakova, a upitnik zamjenjuje bilo koji pojedini znak. Obratite pozornost prilikom određivanja izuzetih adresa jer bi popis trebao sadržavati samo pouzdane i sigurne adrese. Treba obratiti pozornost i na to da se simboli * i ?

pravilno koriste na popisu. Pogledajte Dodavanje HTTP adrese / maske domene kako biste saznali kako sigurno uskladiti čitavu domenu zajedno sa svim poddomenama. Da biste aktivirali popis, odaberite mogućnost **Aktivan popis**. Ako želite primiti obavijest kada upišete adresu s trenutačnog popisa, aktivirajte mogućnost **Obavijesti prilikom primjene**.

> **Adrese kojima ESET vjeruje**
> Ako je aktivirana opcija **Ne skeniraj promet s domenama koje ESET smatra pouzdanima** postavljena na SSL/TLS, na domene na popisu popis pouzdanih adresa neće utjecati konfiguracija upravljanja URL adresama.



Kontrolni elementi

Dodaj – Stvara novi popis uz one koji su prethodno definirani. To može biti posebno korisno ako želite logički podijeliti različite skupine adresa. Primjerice, jedan popis blokiranih adresa može sadržavati adrese vanjskog javnog popisa spam adresa, a drugi može sadržavati vaš osobni popis spam adresa, čime je lakše ažurirati vanjski popis dok vaš ostaje netaknut.

Uredi – Uređuje postojeće popise. Upotrijebite da biste dodali ili uklonili adrese.

Izbriši – Briše postojeće popise. To je dostupno samo za popise stvorene stavkom **Dodaj**, ne i za standardne.

Popis adresa

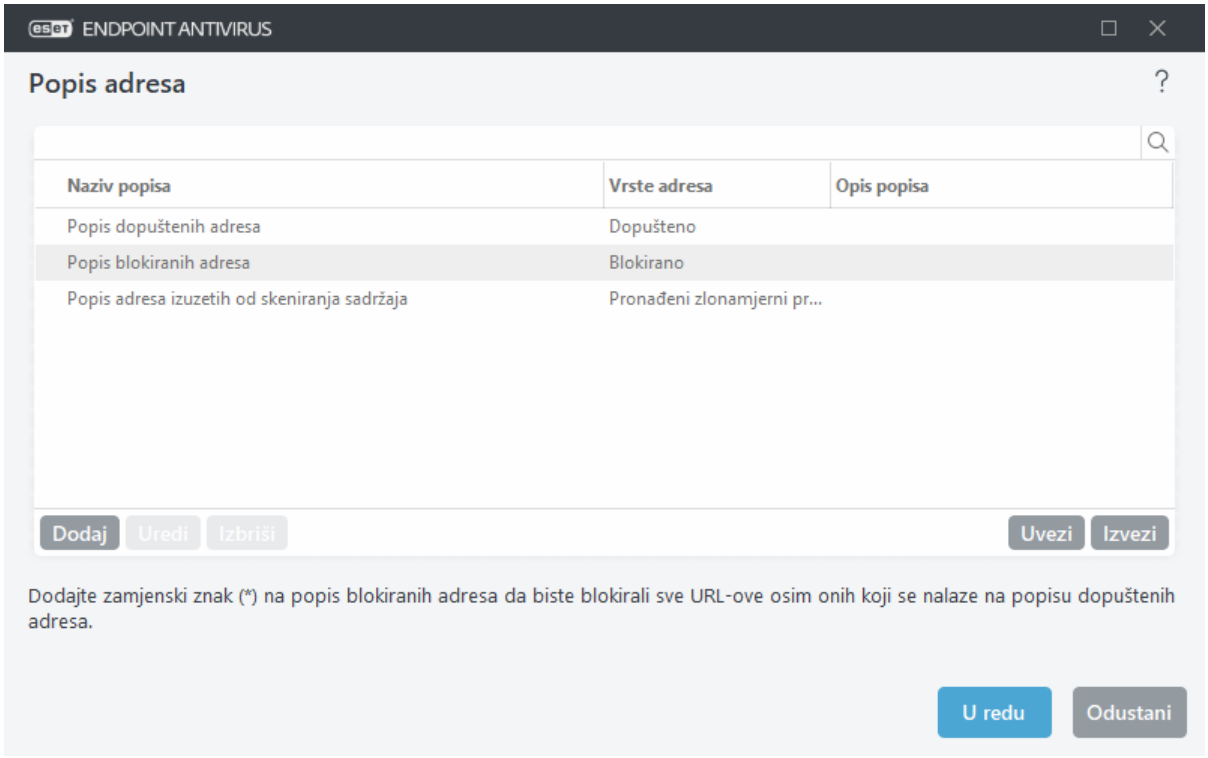
U ovom odjeljku možete zadati popis HTTP(S) adresa koje će biti blokirane, dopuštene ili izuzete iz provjere.

Prema standardnim postavkama dostupna su sljedeća tri popisa:

- **Popis adresa koje su izuzete od provjere** – Za adrese s ovog popisa neće se izvršiti provjera zlonamjernog koda.
- **Popis dopuštenih adresa** – Ako je aktivirana značajka Dopusti pristup samo HTTP adresama s popisa

dopuštenih adresa, a popis blokiranih adresa sadrži * (univerzalni znak), korisniku će biti dopušten pristup samo adresama koje je naveo na tom popisu. Adrese s popisa bit će dopuštene čak i ako se nalaze na popisu blokiranih adresa.
- **Popis blokiranih adresa** – Korisnik neće moći pristupati adresama s popisa ako iste nisu na popisu dopuštenih adresa.

Kliknite **Dodaj** da biste stvorili novi popis. Kliknite **Izbriši** da biste izbrisali odabrane popise.



Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
- Deblokirajte sigurnu stranicu na pojedinačnoj radnoj stanici u programu ESET Endpoint Antivirus

Više informacija potražite u odjeljku Upravljanje URL adresama.

Stvaranje novog popisa URL adresa

Ovaj dijaloški prozor omogućuje konfiguriranje novog popisa URL adresa / maski koje će biti blokirane, dopuštene ili izuzete iz provjere.

Možete konfigurirati sljedeće opcije:

Vrsta popisa adresa – Dostupne su tri vrste popisa:

- **Pronađeni zlonamjerni programi su zanemareni** – Provjera zlonamjernog koda ne izvršava se ni za jednu adresu dodanu na popis.
- **Blokirano** – pristup adresama navedenima na ovom popisu bit će blokiran.
- **Dopušteno** – pristup adresama navedenima na ovom popisu bit će dopušten. Adrese s popisa bit će dopuštene čak i ako odgovaraju onima na popisu blokiranih adresa.

Naziv popisa – Navedite naziv popisa. Ovo polje neće biti dostupno prilikom uređivanja jednog od unaprijed definiranih popisa.

Opis popisa – Unesite kratak opis popisa (nije obavezno). Nije dostupno prilikom uređivanja jednog od unaprijed definiranih popisa.

Da bite aktivirali popis, odaberite **Aktivan popis** pored njega. Ako želite primiti obavijest kada se prilikom pristupa web mjestima koristi određeni popis, odaberite **Obavijesti pri primjeni**. Primjerice, primit ćete obavijest ako je web stranica blokirana ili dopuštena jer se nalazi na popisu blokiranih ili dopuštenih adresa. Obavijest sadrži naziv popisa.

Opseg vođenja dnevnika – odaberite opseg vođenja dnevnika iz padajućeg izbornika. Zapise koji sadrže Upozorenja o opsegu može prikupiti ESET PROTECT.

Opseg vođenja dnevnika informacija i upozorenja dostupan je samo za pravila koja sadrže najmanje dvije komponente bez zamjenskih znakova unutar domene. Na primjer:
- *.domain.com/*
- *www.domain.com/*

Kontrolni elementi

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

Uredi – Uređuje postojeće adrese na popisu. Dostupno samo za adrese stvorene pomoću opcije **Dodaj**.

Ukloni – Briše postojeće adrese s popisa. Dostupno samo za adrese stvorene pomoću opcije **Dodaj**.

Uvezi – Služi za uvoz datoteke s URL adresama (vrijednosti morate odvojiti prijelomom retka, na primjer *.txt s kodiranjem UTF-8).

Informacije potražite u poglavlju Kako dodati URL masku.

Kako dodati URL masku

Prije nego što upišete željenu adresu / masku domene pogledajte upute u ovom dijaloškom okviru.

Program ESET Endpoint Antivirus korisnicima omogućuje blokiranje pristupa određenim web stranicama i sprečavanje prikazivanja njihova sadržaja u web pregledniku. Možete i navesti adrese koje se izuzimaju od provjere. Ako nije poznat cijeli naziv udaljenog servera ili korisnik želi obuhvatiti čitavu skupinu udaljenih servera, za identifikaciju takve skupine mogu se koristiti tzv. maske. Maske sadrže simbole „?” i „*”:

- ? zamjenjuje bilo koji znak
- * zamjenjuje tekstualni znakovni niz.

Primjerice, znakovni niz *.c?m obuhvaća sve adrese kojima zadnji dio počinje slovom c, završava slovom m i sadrži nepoznat znak između njih (.com, .cam itd.).

Primjerice, maska *x? označava svaku adresu u kojoj je x predzadnji znak. Za podudaranje s cijelom domenom upišite je u obliku **.domain.com/**. Definiranje prefiksa protokola *http://*, *https://* u maski nije obavezno. Ako se izostavi, maska će obuhvatiti sve protokole. S nizom koji započinje s "*." postupa se na poseban način ako se koristi na početku naziva domene. Kao prvo, u tom slučaju zamjenski znak * ne odgovara znaku kose crte ('/'). To je tako kako bi se spriječilo zaobilaženje maske, primjerice, maska **.domain.com* neće se podudarati s *http://anydomain.com/anypath#.domain.com* (taj se nastavak može pridružiti bilo kojem URL-u bez učinka na preuzimanje). A kao drugo, u tom posebnom slučaju "*." znači isto kao prazan niz. To je tako kako bi se omogućilo

usklađivanje čitave domene zajedno sa svim poddomenama pomoću jedne maske. Primjerice, maska **.domain.com* se podudara i s *http://domain.com*. Korištenje maske **domain.com* bi bilo netočno jer bi se podudaralo i s *http://anotherdomain.com*.

Opseg vođenja dnevnika informacija i upozorenja dostupan je samo za pravila koja sadrže najmanje dvije komponente bez zamjenskih znakova unutar domene. Na primjer:
- *.domain.com/*
- *www.domain.com/*

Skeniranje HTTP(S) prometa

Prema zadanim postavkama ESET Endpoint Antivirus konfiguriran je za skeniranje HTTP i HTTPS prometa koji koriste internetski preglednici i druge aplikacije. Skeniranje prometa trebali biste onemogućiti samo ako imate problema sa softverom treće strane i želite znati je li uzrok problema ESET Endpoint Antivirus.

Aktiviraj skeniranje HTTP prometa – HTTP promet uvijek se nadzire na svim portovima za sve aplikacije.

Aktiviraj skeniranje HTTPS prometa – HTTPS komunikacija koristi šifrirani kanal za prijenos informacija između servera i klijenta. ESET Endpoint Antivirus provjerava komunikaciju pomoću protokola SSL (Secure Socket Layer) i TLS (Transport Layer Security). Program skenira promet samo na portovima definiranim u opciji **Portovi koje koristi HTTPS protokol**, neovisno o verziji operacijskog sustava (uz unaprijed definirane 443 i 0-65535 možete dodati i druge portove).

ThreatSense

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

Mogućnosti podešavanja tehnologije ThreatSense omogućuju vam određivanje nekoliko parametara skeniranja:

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

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

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

Parametri sustava ThreatSense optimizirani su za svaki modul, a njihova izmjena može znatno utjecati na rad

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

Objekti za skeniranje

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

Radna memorija – Skenira prijetnje koje napadaju radnu memoriju sustava.

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

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

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

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

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

Mogućnosti skeniranja

Odaberite postupke koji će se koristiti za skeniranje sustava radi otkrivanja infiltracija. Dostupne su sljedeće opcije:

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

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

Čišćenje

Postavke čišćenja određuju funkcioniranje programa ESET Endpoint Antivirus prilikom čišćenja objekata.

Izuzeci

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

Ostalo

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

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

Pokreni pozadinska skeniranja s niskim prioritetom – Svaki slijed skeniranja troši izvjesnu količinu sistemskih resursa. Ako radite s programima koji obilato koriste sistemske resurse, možete aktivirati pozadinsko skeniranje niskog prioriteta da biste resurse sačuvali za ostale aplikacije.

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

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

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

Ograničenja

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

Postavke objekta

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

Maksimalno vrijeme skeniranja za objekt (u sekundama) – definira maksimalnu vremensku vrijednost za skeniranje datoteka u spremišnom objektu (kao što je RAR/ZIP arhiva ili e-poruka s više privitaka). Ova postavka se ne odnosi na samostalne datoteke. Ako je unesena korisnički definirana vrijednost i to vrijeme je proteklo, skeniranje će se zaustaviti što je prije moguće, neovisno o tome je li skeniranje svih datoteka u spremišnom objektu dovršeno. U slučaju arhive s velikim datotekama skeniranje će se zaustaviti tek nakon što se raspakira datoteka iz arhive (na primjer, kada je korisnički definirana varijabla 3 sekunde, ali raspakiravanje datoteke traje 5 sekundi). Ostale datoteke u arhivi se neće skenirati kada to vrijeme istekne. Da biste ograničili vrijeme skeniranja, uključujući veće arhive, upotrijebite opcije **Maksimalna veličina objekta** i **Maksimalna veličina datoteke u arhivi** (ne preporučuje se zbog mogućih sigurnosnih rizika). Standardna vrijednost: neograničeno.

Podešavanje skeniranja arhive

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

Maksimalna veličina datoteke u arhivi – Ova opcija omogućuje vam da odredite maksimalnu veličinu (raspakiranih) datoteka sadržanih u arhivama koje želite skenirati. Maksimalna vrijednost je 3 GB.

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

Kontrola uređaja

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

Podržani vanjski uređaji:

- Pohrana na disku (HDD, izmjenjivi USB disk)
- CD/DVD
- USB Pisač
- FireWire Spremište
- Bluetooth Uređaj
- Čitač pametnih kartica
- Uređaj za obradu slike
- Modem
- LPT/COM port
- Prijenosni uređaj (uređaji na baterije kao što su multimedijski reproduktor, pametni telefoni, uređaji "uključi i radi" itd.)
- Sve vrste uređaja

Mogućnosti podešavanja kontrole uređaja mogu se izmijeniti pod Napredno podešavanje > **Zaštite** > **Kontrola uređaja**.

Kliknite klizač **Aktiviraj kontrolu uređaja** da biste aktivirali značajku kontrole uređaja u programu ESET Endpoint Antivirus; da bi se izmjena primijenila, morate ponovno pokrenuti računalo. Nakon što se kontrola uređaja aktivira, možete definirati **pravila** u prozoru Uređivač pravila.

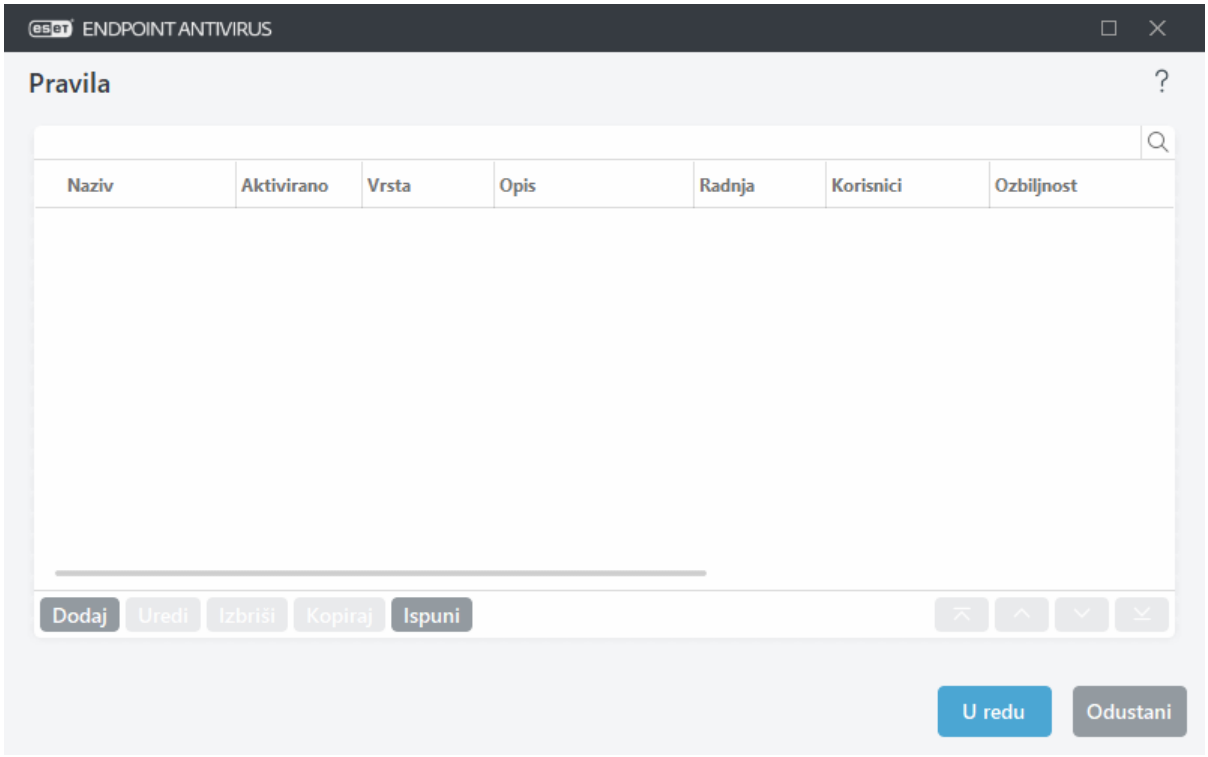
Pomoću planera možete uvesti grupu za kontrolu uređaja s pravilima iz xml datoteke. Dodatne informacije i detaljan vodič potražite u našem članku iz ESET-ove baze znanja.

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

Uređivač pravila kontrole uređaja

Prozor **Uređivač pravila kontrole uređaja** prikazuje postojeća pravila i omogućuje preciznu kontrolu vanjskih uređaja koje korisnici povezuju s računalom. Također pogledajte stavku Dodavanje pravila kontrole uređaja.

Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
Dodavanje i izmjena pravila kontrole uređaja ESET-ovim sigurnosnim programima



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

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

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

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

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

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

Otkriveni uređaji

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

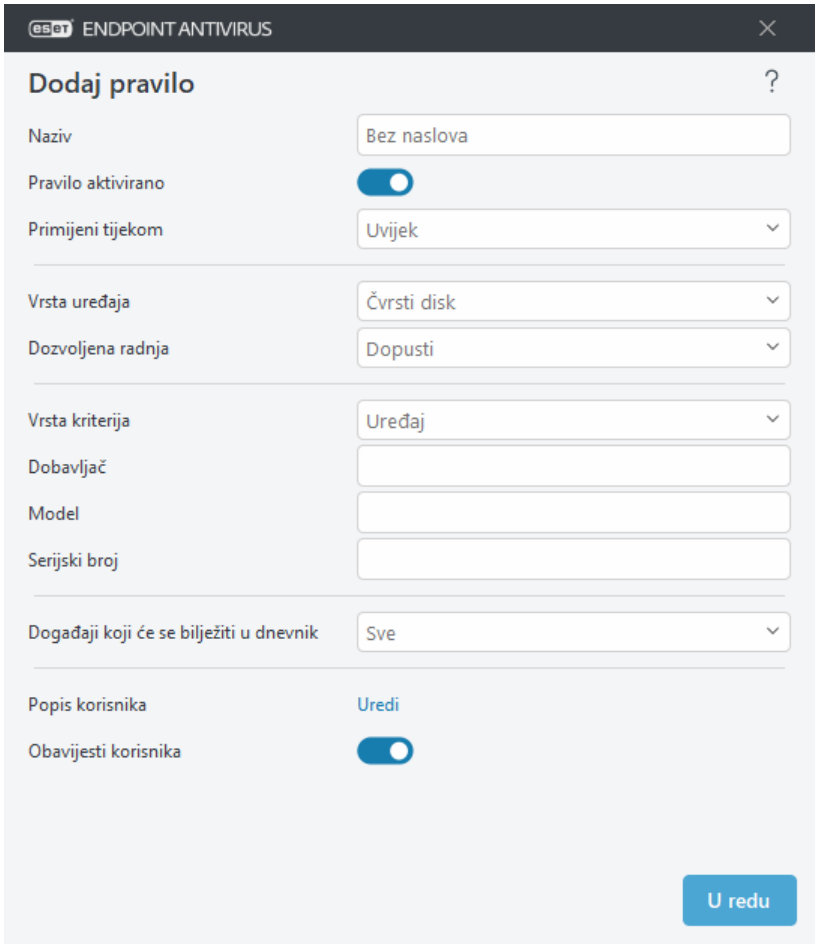
Odaberite uređaj s popisa otkrivenih uređaja i kliknite **U redu** kako biste dodali pravilo kontrole uređaja s unaprijed definiranim informacijama (sve postavke se mogu prilagoditi).

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

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

Dodavanje pravila kontrole uređaja

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



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

Primijeni tijekom – omogućuje vam da primijenite stvoreno pravilo tijekom određenog vremena. Iz padajućeg izbornika odaberite stvoreno vremensko razdoblje. Pogledajte više informacija o vremenskim razdobljima.

Vrsta uređaja

Odaberite vrstu vanjskog uređaja s padajućeg izbornika (Pohrana na disku/Prijenosni uređaj/Bluetooth/FireWire/...). Informacije o vrsti uređaja preuzimaju se iz operacijskog sustava i mogu se vidjeti u upravitelju uređaja sustava ako je uređaj priključen na računalo. Uređaji za pohranu obuhvaćaju vanjske diskove ili konvencionalne čitače memorijskih kartica povezane putem USB-a ili sučelja FireWire. Čitači pametnih kartica obuhvaćaju čitače pametnih kartica s ugrađenim elektroničkim integriranim krugom, kao što su SIM kartice ili

kartice za autorizaciju. Primjeri su uređaja za obradu slike skeneri i kamere. Budući da ti uređaji daju samo informacije o svojim radnjama, bez informacija o korisnicima, mogu se samo globalno blokirati.

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

Akcija

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

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

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

Vrsta uvjeta

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

Pravila za različite uređaje se mogu detaljno konfigurirati pomoću ostalih parametara navedenih u nastavku. Svi parametri su osjetljivi na velika i mala slova i podržavaju zamjenske znakove (*, ?):

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

Ako ovi parametri nisu definirani, pravilo će pri određivanju podudaranja ignorirati ta polja. Filtriranje parametara u svim tekstnim poljima je osjetljivo na velika i mala slova i podržava zamjenske znakove (upitnik (?) predstavlja jedan znak, a zvjezdica (*) znakovni niz od nula ili više znakova).

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

Minimalna opširnost zapisivanja

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

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

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

> **Ograničenja popisa korisnika**
> Popis korisnika ne može se definirati za pravila s određenim vrstama uređaja:
> - USB pisač
> - Bluetooth uređaj
> - Čitač pametnih kartica
> - Uređaj za obradu slike
> - Modem
> - LPT/COM port

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

Grupe uređaja

> Uređaj povezan s vašim računalom može predstavljati sigurnosni rizik.

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

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

Kontrolni elementi

Dodaj – grupu možete dodati tako da upišete njezin naziv ili možete dodati uređaj u postojeću grupu ovisno o tome na kojem ste dijelu prozora kliknuli gumb.

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

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

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

- Svaki uređaj počinje novim retkom.
- **Dobavljač**, **Model** i **Serijski broj** moraju biti navedeni za svaki uređaj i odvojeni zarezom.

> Slijedi primjer sadržaja tekstne datoteke:
> ```
> Kingston,DT 101 G2,001CCE0DGRFC0371
> 04081-0009432,USB2.0 HD WebCam,20090101
> ```

Izvezi – Izvozi popis uređaja u datoteku.

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

Pomoću planera možete uvesti grupu za kontrolu uređaja s pravilima iz xml datoteke. Dodatne informacije i detaljan vodič potražite u našem članku iz ESET-ove baze znanja.

Dodavanje uređaja

Kliknite Dodaj u desnom prozoru da biste dodali uređaj u postojeću grupu. Pravila za različite uređaje se mogu detaljno konfigurirati pomoću ostalih parametara navedenih u nastavku. Svi parametri su osjetljivi na velika i mala slova i podržavaju zamjenske znakove (*, ?):

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

Ako ovi parametri nisu definirani, pravilo će pri određivanju podudaranja ignorirati ta polja. Filtriranje parametara u svim tekstnim poljima je osjetljivo na velika i mala slova i podržava zamjenske znakove (upitnik (?) predstavlja jedan znak, a zvjezdica (*) znakovni niz od nula ili više znakova).

Kliknite **U redu** da biste spremili promjene. Kliknite **Odustani** ako želite zatvoriti prozor **Grupe uređaja** bez spremanja promjena.

Nakon što kreirate grupu uređaja, morate dodati novo pravilo kontrole uređaja za kreiranu grupu uređaja i odabrati akciju koju želite poduzeti.

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

ThreatSense

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

Mogućnosti podešavanja tehnologije ThreatSense omogućuju vam određivanje nekoliko parametara skeniranja:

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

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

- Rezidentna zaštita sistemskih datoteka
- Skeniranje u stanju mirovanja
- Skeniranje pri pokretanju

- Zaštita dokumenata
- zaštita klijenta e-pošte
- zaštita web pristupa
- Skeniranje računala

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

Objekti za skeniranje

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

Radna memorija – Skenira prijetnje koje napadaju radnu memoriju sustava.

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

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

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

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

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

Mogućnosti skeniranja

Odaberite postupke koji će se koristiti za skeniranje sustava radi otkrivanja infiltracija. Dostupne su sljedeće opcije:

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

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

Čišćenje

Postavke čišćenja određuju funkcioniranje programa ESET Endpoint Antivirus prilikom čišćenja objekata.

Izuzeci

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

Ostalo

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

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

Pokreni pozadinska skeniranja s niskim prioritetom – Svaki slijed skeniranja troši izvjesnu količinu sistemskih resursa. Ako radite s programima koji obilato koriste sistemske resurse, možete aktivirati pozadinsko skeniranje niskog prioriteta da biste resurse sačuvali za ostale aplikacije.

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

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

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

Ograničenja

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

Postavke objekta

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

Maksimalno vrijeme skeniranja za objekt (u sekundama) – definira maksimalnu vremensku vrijednost za skeniranje datoteka u spremišnom objektu (kao što je RAR/ZIP arhiva ili e-poruka s više privitaka). Ova postavka se ne odnosi na samostalne datoteke. Ako je unesena korisnički definirana vrijednost i to vrijeme je proteklo, skeniranje će se zaustaviti što je prije moguće, neovisno o tome je li skeniranje svih datoteka u spremišnom objektu dovršeno. U slučaju arhive s velikim datotekama skeniranje će se zaustaviti tek nakon što se raspakira datoteka iz arhive (na primjer, kada je korisnički definirana varijabla 3 sekunde, ali raspakiravanje datoteke traje 5 sekundi). Ostale datoteke u arhivi se neće skenirati kada to vrijeme istekne. Da biste ograničili vrijeme skeniranja, uključujući veće arhive, upotrijebite opcije **Maksimalna veličina objekta** i **Maksimalna veličina datoteke u arhivi**

(ne preporučuje se zbog mogućih sigurnosnih rizika). Standardna vrijednost: neograničeno.

Podešavanje skeniranja arhive

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

Maksimalna veličina datoteke u arhivi – Ova opcija omogućuje vam da odredite maksimalnu veličinu (raspakiranih) datoteka sadržanih u arhivama koje želite skenirati. Maksimalna vrijednost je 3 GB.

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

Razine čišćenja

Da biste promijenili postavke razine čišćenja željenog modula za zaštitu, proširite stavku **ThreatSense** (na primjer, **Rezidentna zaštita sistemskih datoteka**), a zatim na padajućem izborniku odaberite razinu u stavci **Razina čišćenja**.

ThreatSense ima sljedeće razine ispravljanja (tj. čišćenja).

Ispravljanje u programu ESET Endpoint Antivirus

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

Datotečne ekstenzije izuzete od skeniranja

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

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

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

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

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

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

Da biste vidjeli točnu ekstenziju (ako postoji) datoteke u operacijskom sustavu Windows, morate označiti potvrdni okvir **Ekstenzije naziva datoteka** u odjeljku **Windows Explorer** > **Prikaz** (kartica).

Dodatni ThreatSense parametri

Da biste uredili te postavke, otvorite Napredno podešavanje > **Zaštite** > **Rezidentna zaštita sistemskih datoteka** > **Dodatni ThreatSense parametri**.

Dodatni ThreatSense parametri za novostvorene i izmijenjene datoteke

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

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

Dodatni ThreatSense parametri za pokrenute datoteke

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

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

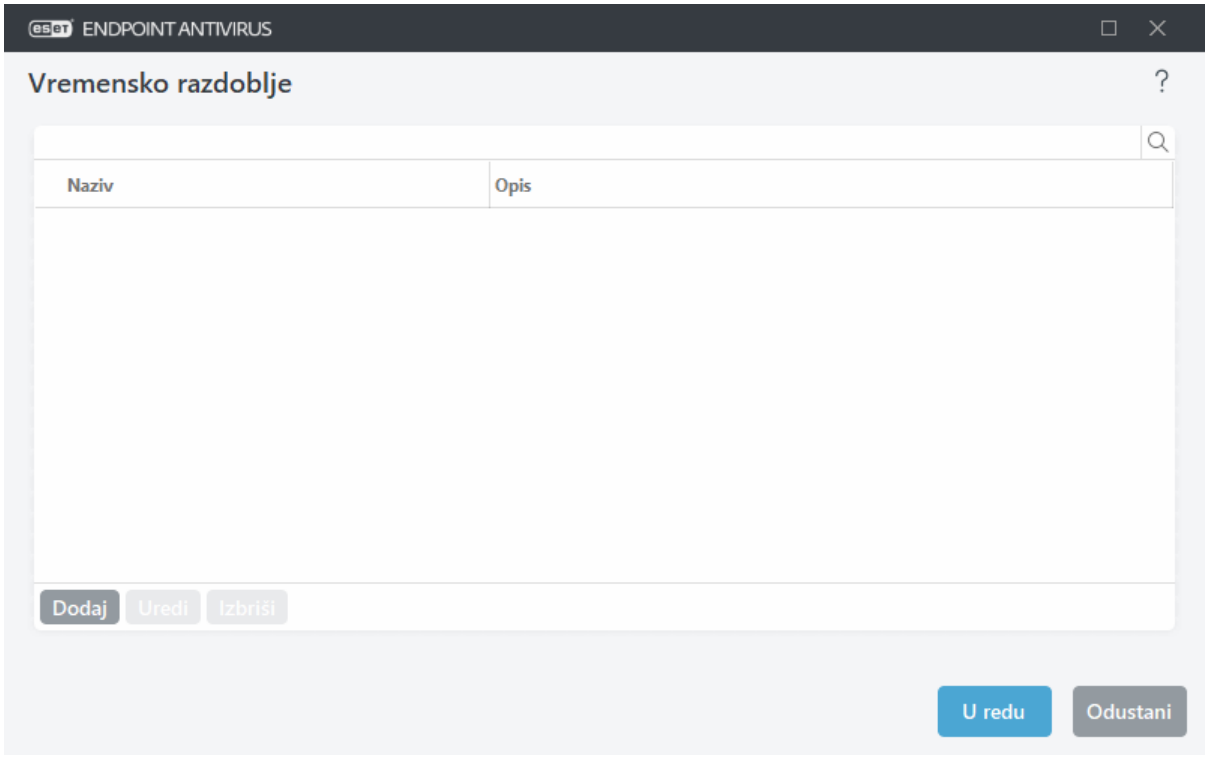
Alati

Možete konfigurirati napredne postavke za značajke koje pružaju dodatnu sigurnost i pojednostavniti administraciju programa ESET Endpoint Antivirus u prozoru Napredno podešavanje > **Alati**.

- Vremensko razdoblje
- Nadogradnja sustava Microsoft Windows
- ESET CMD
- Daljinsko praćenje i upravljanje
- Interval provjere licence
- Dnevnici
- Način rada za prezentacije
- Dijagnostika

Vremensko razdoblje

Vremenska razdoblja se mogu stvarati i zatim dodjeljivati pravilima za **Kontrolu uređaja**. Postavka **vremenskih razdoblja** nalazi se pod "Napredno podešavanje" > **"Alati"**. Ova opcija omogućuje vam definiranje najčešćih vremenskih razdoblja (npr. radno vrijeme, vikend itd.) i njihovu jednostavnu ponovnu upotrebu bez ponovnog definiranja vremenskih raspona za svako pravilo. Vremensko razdoblje primjenjivo je za svaku relevantnu vrstu pravila koje podržava kontrolu utemeljenu na vremenu.



Za stvaranje vremenskog razdoblja učinite sljedeće:

1. Kliknite **"Uredi"** > **"Dodaj"**.
2. Unesite naziv i **opis** vremenskog razdoblja i kliknite **"Dodaj"**.
3. Navedite dan i vrijeme početka/završetka za vremensko razdoblje ili odaberite **"Cijeli dan"**.
4. Kliknite **U redu** za potvrdu.

Jedno vremensko razdoblje može se definirati s jednim ili više vremenskih raspona na temelju dana i vremena. Kada se vremensko razdoblje stvori, ono će se prikazati u padajućem izborniku **Primijeni tijekom** u prozoru uređivača pravila kontrole uređaja.

Nadogradnja sustava Microsoft Windows

Mogućnost nadogradnje sustava Windows važan je element za zaštitu korisnika od zlonamjernog softvera. Iz tog razloga izuzetno je važno nadogradnje sustava Microsoft Windows instalirati čim one postanu dostupne. ESET Endpoint Antivirus vas obavještava o nadogradnjama koje nedostaju u skladu s razinom koju definirate. Dostupne su sljedeće razine:

- **Nema nadogradnji** – Neće se navoditi nadogradnje sustava za preuzimanje.
- **Dodatne nadogradnje** – Za preuzimanje će biti ponuđene nadgradnje koje imaju oznaku niskog i višeg prioriteta.
- **Preporučene nadogradnje** – Za preuzimanje će biti ponuđene nadgradnje koje imaju oznaku uobičajenog i višeg prioriteta.
- **Važne nadogradnje** – Za preuzimanje će biti ponuđene nadgradnje koje imaju oznaku visokog i višeg prioriteta.
- **Kritične nadogradnje** – Samo će kritične nadogradnje biti ponuđene za preuzimanje.

Kliknite **U redu** da biste spremili promjene. Prozor za nadogradnje sustava prikazat će se nakon verifikacije statusa putem servera za nadogradnju. Prema tome, informacije o nadogradnji sustava možda neće biti dostupne odmah po spremanju promjena.

Dijaloški prozor – nadogradnje operacijskog sustava

Ako su dostupne nadogradnje za vaš operacijski sustav, ESET Endpoint Antivirus početni prozor prikazuje obavijest. Kliknite **Više informacija** za otvaranje prozora nadogradnje sustava.

U prozoru o sistemskim nadogradnjama prikazan je popis dostupnih nadogradnji koje su spremne za preuzimanje i instalaciju. Vrsta nadogradnje prikazana je pokraj naziva nadogradnje.

Dvaput kliknite bilo koji redak nadogradnje kako bi se prikazao prozor Informacije o nadogradnji s dodatnim informacijama.

Kliknite **Pokreni nadogradnju sustava** da biste preuzeli i instalirali sve navedene nadogradnje operacijskog sustava.

Aktualiziranje podataka

U prozoru o sistemskim nadogradnjama prikazan je popis dostupnih nadogradnji koje su spremne za preuzimanje i instalaciju. Razina prioriteta aktualizacije prikazana je pokraj naziva aktualizacije.

Kliknite **Pokreni nadogradnju sustava** da biste pokrenuli preuzimanje i instalaciju nadogradnje operacijskog sustava.

Kliknite bilo koji redak nadogradnje desnom tipkom miša i kliknite **Prikaži informacije** za prikaz novog prozora s dodatnim informacijama.

ESET CMD

Ovom se funkcijom aktiviraju napredne ecmd naredbe. Možete izvoziti i uvoziti postavke upotrebom naredbenog retka (ecmd.exe). Dosad je bilo moguće izvoziti postavke samo uporabom GUI-ja. ESET Endpoint Antivirus konfiguracija se može izvesti u datoteci .xml*.xml*.

Kada aktivirate ESET CMD, dostupne su dvije metode autorizacije:

- **Ništa** – nema autorizacije. Ne preporučujemo ovu metodu jer omogućuje uvoz svih nepotpisanih konfiguracija, što predstavlja potencijalni rizik.
- **Lozinka naprednog podešavanja** – potrebna je lozinka za uvoz konfiguracije iz datoteke *.xml*, ta datoteka mora biti potpisana (pogledajte potpisivanje konfiguracijske datoteke *.xml* u nastavku). Lozinka navedena u Podešavanju pristupa mora se navesti kako bi bilo moguće uvesti novu konfiguraciju. Ako podešavanje pristupa nije aktivirano, lozinka ne odgovara ili konfiguracijska datoteka *.xml* nije potpisana, konfiguracija se neće uvesti.

Kad se aktivira ESET CMD, možete upotrijebiti naredbeni redak za uvoz ili izvoz konfiguracija ESET Endpoint Antivirus. To možete učiniti ručno ili možete stvoriti skriptu radi automatizacije postupka.

Da biste se mogli koristiti naprednim ecmd naredbama, morate ih pokrenuti s administratorskim ovlastima ili otvoriti naredbeni redak sustava Windows (cmd) opcijom **Pokreni kao administrator**. U protivnom ćete primiti poruku **Error executing command**. Isto tako, kada izvozite konfiguraciju, mora postojati odredišna mapa. Naredba izvoza i dalje radi kad se postavka ESET CMD isključi.

Napredne ecmd naredbe se mogu pokrenuti samo lokalno. Pauziranje ecmd naredbi se može izvoditi samo putem zadatka klijenta **Izvrši naredbu** pomoću programa ESET PROTECT.

Naredba izvoza postavki:
`ecmd /getcfg c:\config\settings.xml`
Naredba uvoza postavki:
`ecmd /setcfg c:\config\settings.xml`

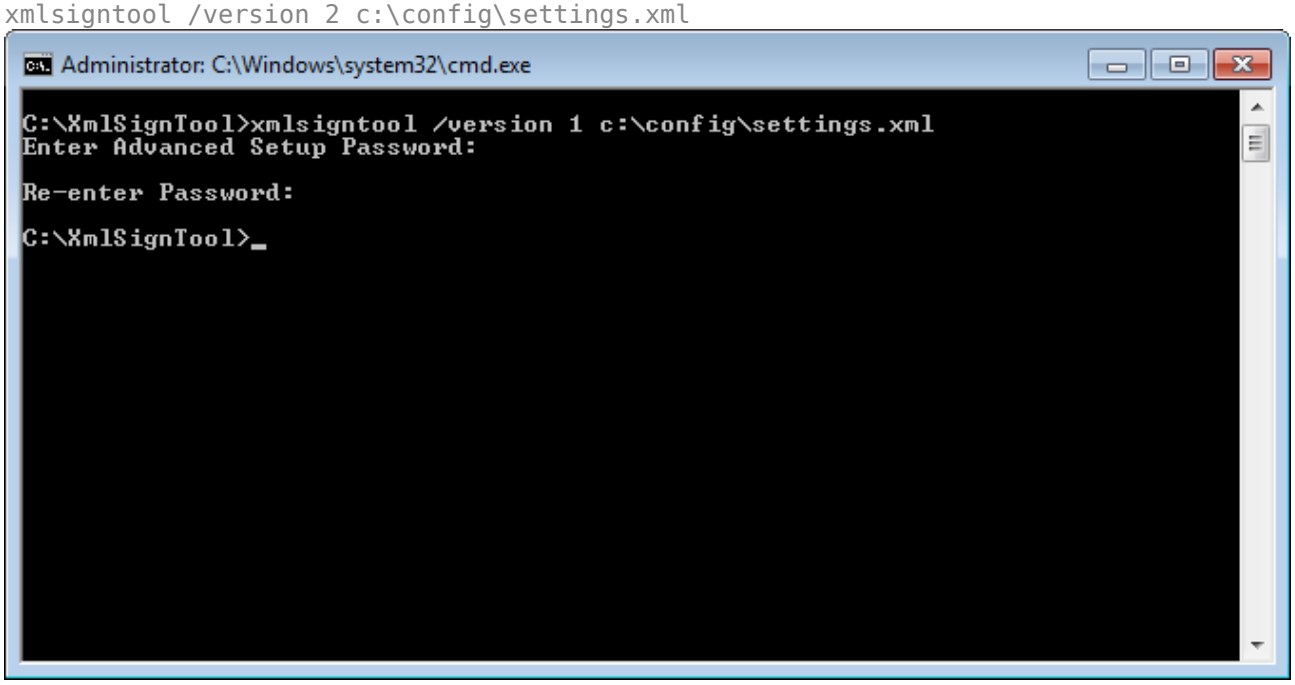
Potpisivanje konfiguracijske datoteke *.xml*:

1. Preuzmite izvršnu datoteku XmlSignTool.
2. Otvorite naredbeni redak sustava Windows (cmd) opcijom **Pokreni kao administrator**.
3. Idite na lokaciju gdje je spremljena datoteka `xmlsigntool.exe`
4. Izvršite naredbu da biste potpisali konfiguracijsku datoteku *.xml*, upotreba: `xmlsigntool /version 1|2 <xml_file_path>`

Vrijednost parametra `/version` ovisi o vašoj verziji programa ESET Endpoint Antivirus. Upotrebljavajte vrijednost `/version 2` za verziju 7 i novije verzije.

5. Dvaput unesite lozinku za napredno podešavanje kada vas XmlSignTool to zatraži. Vaša konfiguracijska datoteka *.xml* sada je potpisana i možete je upotrijebiti za uvoz druge instance programa ESET Endpoint Antivirus programom ESET CMD upotrebom metode autorizacije lozinkom.

Potpišite izvezenu naredbu konfiguracijske datoteke:
`xmlsigntool /version 2 c:\config\settings.xml`



Ako se vaša lozinka za podešavanje pristupa promijeni i želite uvesti konfiguraciju koja je ranije potpisana starijom lozinkom, morate ponovno potpisati konfiguracijsku datoteku *.xml* svojom trenutačnom lozinkom. To vam omogućuje upotrebu starije konfiguracijske datoteke bez potrebe da je izvozite na drugi uređaj s programom ESET Endpoint Antivirus prije uvoza.

Ne preporučuje se aktiviranje programa ESET CMD bez autorizacije jer će se time omogućiti uvoz svih nepotpisanih konfiguracija. Postavite lozinku pod Napredno podešavanje > **Korisničko sučelje** > **Podešavanje pristupa** da biste spriječili korisnike da provode neovlaštene izmjene.

Popis JSON naredbi

Pojedinačne sigurnosne funkcije mogu se aktivirati i privremeno deaktivirati pomoću naredbe za pokretanje ESET PROTECT zadatka klijenta. Naredbe neće nadjačati postavke pravila i sve pauzirane postavke vratit će se u izvorno stanje nakon izvršenja naredbe ili ponovnog pokretanja uređaja. Da biste iskoristili ovu funkciju, naredbeni redak koji će se izvršiti navedite u polju istog naziva.

Pregledajte popis naredbi za svaku sigurnosnu funkciju u nastavku:

Sigurnosna funkcija	Naredba za privremenu pauzu	Naredba za aktivaciju
rezidentna zaštita	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Zaštita dokumenata	ecmd /setfeature document pause	ecmd /setfeature document enable
Kontrola uređaja	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Način rada za prezentacije	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Osobni firewall	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Zaštita od mrežnog napada (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Zaštita od botneta	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Kontrola weba	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
zaštita web pristupa	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
zaštita klijenta e-pošte	ecmd /setfeature email pause	ecmd /setfeature email enable

Sigurnosna funkcija	Naredba za privremenu pauzu	Naredba za aktivaciju
Antispam za klijent e-pošte	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Anti-phishing zaštita	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Daljinsko praćenje i upravljanje

Daljinsko praćenje i upravljanje (RMM) proces je nadgledanja i kontrole softverskih sustava koji upotrebljava lokalno instaliranog agenta kojemu može pristupiti davatelj usluga upravljanja.

ERMM – ESET-ov dodatak za RMM

- Standardna instalacija programa ESET Endpoint Antivirus sadrži datoteku `ermm.exe` koja se nalazi u Endpoint aplikaciji u sljedećoj mapi:
  C:\Program Files\ESET\ESET Security\ermm.exe
- `ermm.exe` je naredbeni redak za uslužni program kojemu je cilj olakšati upravljanje sigurnosnim programima i komunikaciju s bilo kojim RMM dodatkom.
- `ermm.exe` razmjenjuje podatke s RMM dodatkom, koji komunicira s RMM agentom povezanim na RMM server. Alat ESET RMM deaktiviran je prema standardnim postavkama.

Dodatni resursi

- ERMM naredbeni redak
- Popis ERMM JSON naredbi

- Kako aktivirati daljinsko praćenje i upravljanjeESET Endpoint Antivirus

Dodaci ESET Direct Endpoint Management za RMM rješenja trećih strana

RMM server pokrenut je kao usluga na serveru treće strane. Više informacija potražite u sljedećim online korisničkim vodičima za ESET Direct Endpoint Management:

- Dodatak ESET Direct Endpoint Management za ConnectWise Automate
- Dodatak ESET Direct Endpoint Management za Datto RMM
- ESET Direct Endpoint Management za Solarwinds N-Central
- ESET Direct Endpoint Management za NinjaRMM

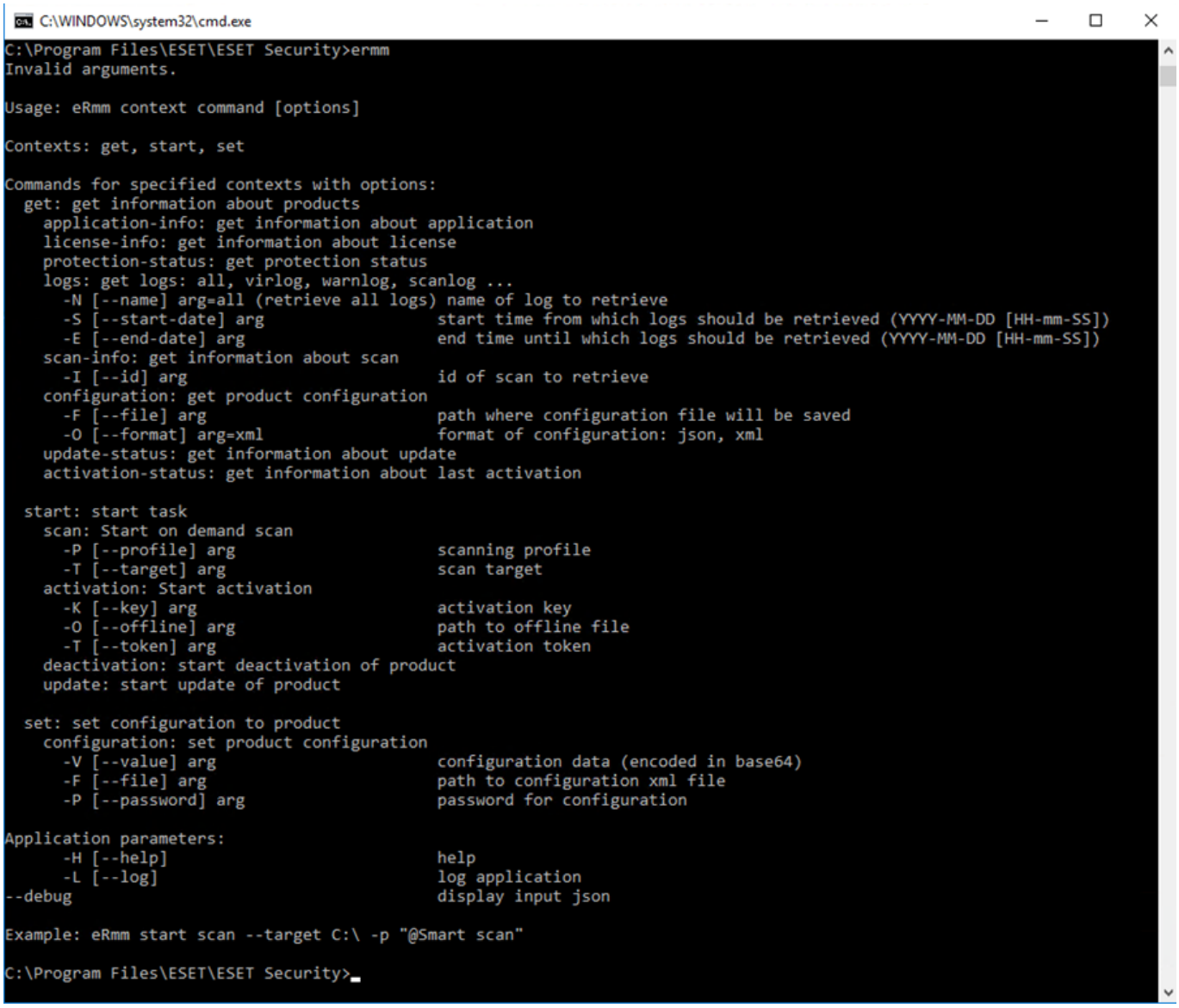
ERMM naredbeni redak

Daljinsko praćenje i upravljanje pokreće se pomoću sučelja naredbenog retka. Standardna instalacija programa ESET Endpoint Antivirus sadrži datoteku ermm.exe koja se nalazi u Endpoint aplikaciji u sljedećoj mapi: *c:\Program Files\ESET\ESET Security*.

Pokrenite naredbeni redak (cmd.exe) kao administrator i idite na navedeni put (da biste otvorili naredbeni redak, pritisnite gumb Windows + R na tipkovnici, upišite cmd u prozor "Pokreni" i pritisnite Enter).

Sintaksa naredbe je: `ermm context command [options]`

Parametri dnevnika razlikuju velika i mala slova.



ermm.exe koristi tri osnovna konteksta: "Dohvati" (Get), "Pokreni" (Start) i "Postavi" (Set). U donjoj tablici možete pronaći primjere sintakse naredbi. Kliknite vezu u stupcu "Naredba" da biste vidjeli dodatne opcije, parametre i primjere upotrebe. Nakon uspješnog izvršenja naredbe prikazat će se izlazni dio (rezultat). Da biste vidjeli ulazni dio, u naredbu dodajte parametar `--debug`.

Kontekst	Naredba	Opis
get		**Dohvaćanje informacija o programima**
	application-info	Dohvaćanje informacija o programu
	license-info	Dohvaćanje informacija o licenci
	protection-status	Nabavi status zaštite
	logs	Nabavi dnevnike
	scan-info	Dohvaćanje informacija o pokretanju skeniranja
	configuration	Dobiti proizvod konfiguracije
	update-status	Dohvaćanje informacija o nadogradnji
	activation-status	Dohvaćanje informacija o posljednjoj aktivaciji
start		**Pokretanje zadatka**
	scan	Pokretanje skeniranja na zahtjev

Kontekst	Naredba	Opis
	activation	Pokretanje aktivacije programa
	deactivation	Pokretanje deaktivacije programa
	update	Pokretanje nadogradnje programa
set		**Postavljanje opcija za program**
	configuration	Postavljanje konfiguracije za program

U izlaznom rezultatu svake naredbe prva prikazana informacija je ID rezultata. Da biste bolje razumjeli informacije o rezultatima, provjerite tablicu ID-ova u nastavku.

ID pogreške	Pogreška	Opis
0	Success	
1	Command node not present	Čvor "Naredba" nije prisutan u ulaznom JSON-u
2	Command not supported	Naredba nije podržana
3	General error executing the command	Pogreška tijekom izvršavanja naredbe
4	Task already running	Traženi zadatak već je pokrenut i nije započet
5	Invalid parameter for command	Neispravan korisnički unos
6	Command not executed because it's disabled	RMM nije aktiviran u naprednim postavkama niti ga je pokrenuo administrator

Popis ERMM JSON naredbi

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info
- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

Naredbeni redak

```
ermm.exe get protection-status
```

Parametri

None

Primjer

call

```
{
"command":"get_protection_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

Get information about the installed application

Naredbeni redak

```
ermm.exe get application-info
```

Parametri

None

Primjer

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Naredbeni redak

```
ermm.exe get license-info
```

Parametri

None

Primjer

call


```
{
"command":"get_license_info",
"id":1,
"version":"1"
}
```


result


```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```


get logs

Get logs of the product

Naredbeni redak

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parametri

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Primjer

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be { success, running, failure }

Naredbeni redak

```
ermm.exe get activation-status
```

Parametri

None

Primjer

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Dohvaćanje informacija o pokretanju skeniranja.

Naredbeni redak

```
ermm.exe get scan-info
```

Parametri

Ništa

Primjer

poziv

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

rezultat

```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Naredbeni redak

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parametri

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Primjer

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Naredbeni redak

```
ermm.exe get update-status
```

Parametri

None

Primjer

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Naredbeni redak

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parametri

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Primjer

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Naredbeni redak

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parametri

Name	Value
key	Activation key

offline	Path to offline file

Primjer

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start deactivation

Start deactivation of the product

Naredbeni redak

```
ermm.exe start deactivation
```

Parametri

None

Primjer

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Naredbeni redak

```
ermm.exe start update
```

Parametri

None

Primjer

call

```
{
"command":"start_update",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Naredbeni redak

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parametri

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Primjer

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

Interval provjere licence

ESET Endpoint Antivirus se mora automatski povezivati s ESET-ovim licenčnim serverima. Broj veza s ESET-ovim licenčnim serverom možete ograničiti u izborniku Napredno podešavanje > **Alati** > **Licenca**. Prema standardnim postavkama **Interval provjere** je postavljen na **Automatski** i veza se uspostavlja nekoliko puta svaki sat. U slučaju povećanog mrežnog prometa promijenite postavke za **Interval provjere** na **Ograničeno** da biste smanjili preopterećenje. Kada je odabrana opcija **Ograničeno**, ESET Endpoint Antivirus provjerava server licenci samo jednom dnevno ili prilikom ponovnog pokretanja računala.

Ako je **interval provjere** postavljen na **Ograničeno**, može potrajati do jedan dan prije nego što se sve promjene u vezi s licencom koje se izvrše putem programa ESET HUB /ESET MSP Administrator primijene na postavke programa ESET Endpoint Antivirus.

Dnevnici

Konfiguracija zapisivanja za ESET Endpoint Antivirus je dostupna u opciji Napredno podešavanje > **Alati** > **Dnevnici**. Odjeljak dnevnika koristi se za definiranje načina upravljanja dnevnicima. Da bi oslobodio prostor na tvrdom disku, program automatski briše starije zapise. Za dnevnike možete definirati sljedeće mogućnosti:

Minimalni opseg vođenja dnevnika – Tu se određuje minimalni opseg podataka za događaje koji se zapisuju u dnevnik.

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa te svi prethodno navedeni zapisi.
- **Informativno** – Zapisuju se sve informativne poruke, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisi.
- **Upozorenja** – Zapisuju se kritične pogreške i poruke s upozorenjima.
- **Pogreške** – Zapisuju se pogreške kao što je „Pogreška preuzimanja datoteke” i kritične pogreške.

- **Kritično** – Zapisuju se samo kritične pogreške (pogreška pri pokretanju antivirusne zaštite itd.)

Kada odaberete razinu opsega **dijagnostike**, zapisat će se sve blokirane veze.

Unosi u dnevniku koji su stariji od broja dana definiranog u polju **Automatski izbriši zapise starije od (dana)** automatski će se izbrisati.

Automatski optimiziraj dnevnike – Kada je ova opcija aktivirana, dnevnici će se automatski defragmentirati ako je postotak fragmentacije viši od vrijednosti naznačene u polju **Ako broj nekorištenih zapisa premašuje (%)**.

Kliknite **Optimiziraj** za pokretanje defragmentiranja dnevnika. Uklanjaju se svi prazni unosi u dnevnik kako bi se poboljšala radna svojstva i brzina obrade. To poboljšanje primjećuje se osobito ako dnevnici sadrže velik broj unosa.

Mogućnost **Aktiviraj tekstualni protokol** omogućuje pohranu dnevnika u drugom formatu, zasebno od dnevnika:

- **Ciljani direktorij** – Odaberite direktorij u kojem će se pohraniti dnevnici (odnosi se samo na Tekst/CSV). Možete kopirati put ili odabrati drugi direktorij klikom na **Očisti**. Svaki odjeljak dnevnika ima vlastitu datoteku s unaprijed definiranim nazivom datoteke (primjerice, *virlog.txt* za odjeljak **Otkrivene prijetnje** u dnevniku ako želite koristiti običan format tekstualne datoteke za pohranu dnevnika).
- **Vrsta** – ako odaberete format datoteke **Tekst**, dnevnici će se pohraniti u tekstualnoj datoteci i podaci će se razdvojiti na kartice. Isto se primjenjuje za podatke odvojene zarezom u **CSV** datoteci. Ako odaberete **Događaj**, dnevnici će se umjesto u datoteku pohranjivati u dnevnik Windows Event (može se pregledati uz pomoć programa Event Viewer na upravljačkoj ploči).
- **Izbriši sve dnevnike** – briše sve pohranjene dnevnike koji su trenutačno odabrani u padajućem izborniku **Vrsta**. Prikazat će se obavijest o uspješnom brisanju dnevnika.

Aktiviraj praćenje konfiguracijskih promjena u dnevniku provjere – informira vas o svakoj promjeni konfiguracije. Pogledajte odjeljak Dnevnici provjere za više informacija.

Kako biste pomogli u bržem rješavanju problema, tvrtka ESET od vas može zatražiti dnevnike s vašeg računala. ESET Log Collector omogućuje lako prikupljanje potrebnih informacija. Dodatne informacije o alatu ESET Log Collector potražite u našem članku iz ESET-ove baze znanja.

Način rada za prezentacije

Način rada za prezentacije funkcija je za igrače koji softver žele koristiti bez prekida, ne žele biti ometani prozorima obavijesti/upozorenja te žele smanjiti korištenje CPU-a. Način rada za prezentacije može se koristiti i tijekom prezentacija koje se ne smiju prekidati antivirusnim aktivnostima. Aktiviranjem te funkcije deaktiviraju se svi skočni prozori, a aktivnost planera u potpunosti se prekida. Zaštita sustava i dalje se izvodi u pozadini, no ne zahtijeva nikakvu aktivnost korisnika.

Način rada za prezentacije možete aktivirati ili deaktivirati u glavnom prozoru programa, u odjeljku **Podešavanje** > **Računalo**, tako da kliknete  ili  uz opciju **Način rada za prezentacije**. Aktiviranje načina rada za prezentacije predstavlja mogući sigurnosni rizik pa će ikona statusa zaštite na programskoj traci postati narančasta i prikazat će se upozorenje. To upozorenje vidjet ćete i u glavnom prozoru programa u kojem će opcija **Aktivan je Način rada za prezentacije** biti označena narančastom bojom.

Aktivirajte **Automatski aktiviraj Način rada za prezentacije prilikom izvršavanja aplikacija u načinu rada cijelog zaslona** u odjeljku Napredno podešavanje > **Alati** > **Način rada za prezentacije** da bi se način rada za prezentacije

pokrenuo svaki put kada pokrenete aplikaciju na cijelom zaslonu i da bi se prekinuo nakon što zatvorite aplikaciju.

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

Dijagnostika

Dijagnostika omogućuje stvaranje slike stanja memorije u slučaju pada aplikacija za ESET procese (primjerice, ekrn). Ako dođe do pada aplikacije, generira se slika stanja memorije. To razvojnim programerima može pomoći ukloniti poteškoće i riješiti razne ESET Endpoint Antivirus probleme.

Kliknite padajući izbornik pored stavke **Vrsta slike stanja memorije** i odaberite jednu od tri dostupne opcije:

- Odaberite **Deaktiviraj** da biste deaktivirali funkciju.
- **Mini** – Bilježi najmanji skup korisnih informacija pomoću kojih bi se mogao prepoznati razlog neočekivanog pada aplikacije. Takva datoteka dumpa može biti korisna ako je prostor ograničen, no budući da sadrži ograničene informacije, pogreške koje nisu izravno uzrokovane nizom koji je bio pokrenut u vrijeme kada se problem pojavio možda se neće moći otkriti analizom takve datoteke.
- **Kompletan** – Bilježi cjelokupan sadržaj sistemske memorije kada aplikacija neočekivano prestane s radom. Dump cijele memorije može sadržavati podatke iz procesa koji su bili pokrenuti prilikom prikupljanja dumpa memorije.

Ciljani direktorij – Direktorij u kojem će se tijekom pada sustava generirati sliku stanja memorije.

Otvori mapu dijagnostike – Kliknite **Otvori** da biste otvorili ovaj direktorij u *novom prozoru Windows explorer*.

Stvori dijagnostički dump – kliknite **Stvori** da biste stvorili dijagnostičke datoteke slike stanja memorije u **ciljnom direktoriju**.

Napredno vođenje dnevnika

Aktiviraj napredno vođenje dnevnika skenera računala – Bilježi sve događaje koji se dogode tijekom skeniranja datoteka i mapa pomoću skeniranja računala ili rezidentne zaštite sistemskih datoteka.

Aktiviraj napredno vođenje dnevnika kontrole uređaja – Bilježi sve događaje koji se dogode u kontroli uređaja. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s kontrolom uređaja.

Aktiviraj napredno vođenje dnevnika o programu Direct Cloud – Zabilježite svu komunikaciju između programa i servera programa Direct Cloud.

Aktiviraj napredno vođenje dnevnika zaštite dokumenata – bilježi sve događaje koji se dogode u zaštiti dokumenata kako bi se omogućilo dijagnosticiranje i rješavanje problema.

Aktiviraj napredno vođenje dnevnika zaštite klijenta e-pošte – zabilježite sve događaje koji se dogode u zaštiti klijenta e-pošte i dodatku za klijent e-pošte kako biste dopustili dijagnosticiranje i rješavanje problema.

Aktiviraj napredno vođenje dnevnika jezgre – bilježi sve događaje koji se dogode na usluzi ESET Kernel (ekrn) radi dijagnostike i rješavanja problema.

Aktiviraj napredno vođenje dnevnika licenciranja – bilježi svu komunikaciju programa s ESET-ovim aktivacijskim i serverima za licenciranje.

Aktiviraj praćenje memorije – Zapisivanje svih događaja koji će razvojnim inženjerima pomoći u dijagnosticiranju curenja memorije.

Aktiviraj napredno vođenje dnevnika mrežne zaštite – Bilježi sve mrežne podatke koji prolaze kroz firewall u PCAP formatu kako bi se razvojnim programerima pomoglo u dijagnozi i popravku problema povezanih s firewallom.

Omogući napredno zapisivanje skenera mrežnog prometa – bilježi sve mrežne podatke koji prolaze kroz skener mrežnog prometa u PCAP formatu kako bi se razvojnim programerima pomoglo u dijagnozi i popravku problema povezanih sa skenerom mrežnog prometa.

Aktiviraj napredno vođenje dnevnika operacijskog sustava – Prikupljat će se dodatne informacije o operacijskom sustavu kao što su pokrenuti procesi, aktivnost procesora, operacije diska. To može pomoći razvojnim programerima u dijagnostici i otklanjanju problema povezanih s ESET-ovim programom koji radi na vašem operacijskom sustavu.

Aktiviraj napredno vođenje dnevnika automatskih poruka – Zabilježite sve događaje koji se događaju tijekom slanja automatskih poruka da biste omogućili dijagnostiku i rješavanje problema.

Aktiviraj napredno vođenje dnevnika rezidentne zaštite sistemskih datoteka – bilježi sve događaje koji se događaju u rezidentnoj zaštiti sistemskih datoteka da bi se omogućilo dijagnosticiranje i rješavanje problema.

Aktiviraj napredno vođenje dnevnika modula za nadogradnju – Bilježi sve događaje do kojih dolazi tijekom nadogradnje. To može pomoći razvojnim programerima u dijagnostici i otklanjaju problema povezanih s modulom za nadogradnju.

Aktiviraj napredno vođenje dnevnika za Upravljanje zakrpama i ranjivosti – zapišite sve događaje u stavku Upravljanje zakrpama i ranjivosti. Ova postavka se prikazuje samo ako je Upravljanje zakrpama i ranjivosti aktivirano u vašem okruženju (aktivirano u programu ESET PROTECT Cloud).

Dnevnici se nalaze u mapi *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Tehnička podrška

Kada se obratite ESET-ovoj tehničkoj podršci iz programa ESET Endpoint Antivirus, možete poslati podatke o sistemskoj konfiguraciji. Odaberite **Uvijek pošalji** iz padajućeg izbornika **Slanje podataka o sistemskoj konfiguraciji** da biste automatski poslali podatke ili odaberite **Pitaj prije slanja** da bi vam se poslao upit prije slanja podataka.

Povezivost

U određenim mrežama proxy server može posredovati u komunikaciji između vašeg računala i interneta. Ako koristite proxy server, morate definirati sljedeće postavke. U suprotnom, ESET Endpoint Antivirus i njegovi moduli neće se moći automatski ažurirati. U programu ESET Endpoint Antivirus postavljanje proxy servera dostupno je u dva različita odjeljka u opciji Napredno podešavanje.

Globalne postavke proxy servera možete konfigurirati u opciji Napredno podešavanje > **Alati** > **Proxy server**. Određivanjem proxy servera na toj razini definiraju se globalne postavke proxy servera za cijeli program ESET Endpoint Antivirus. Parametre koji se tu nalaze koristit će svi moduli kojima je potrebna internetska veza.

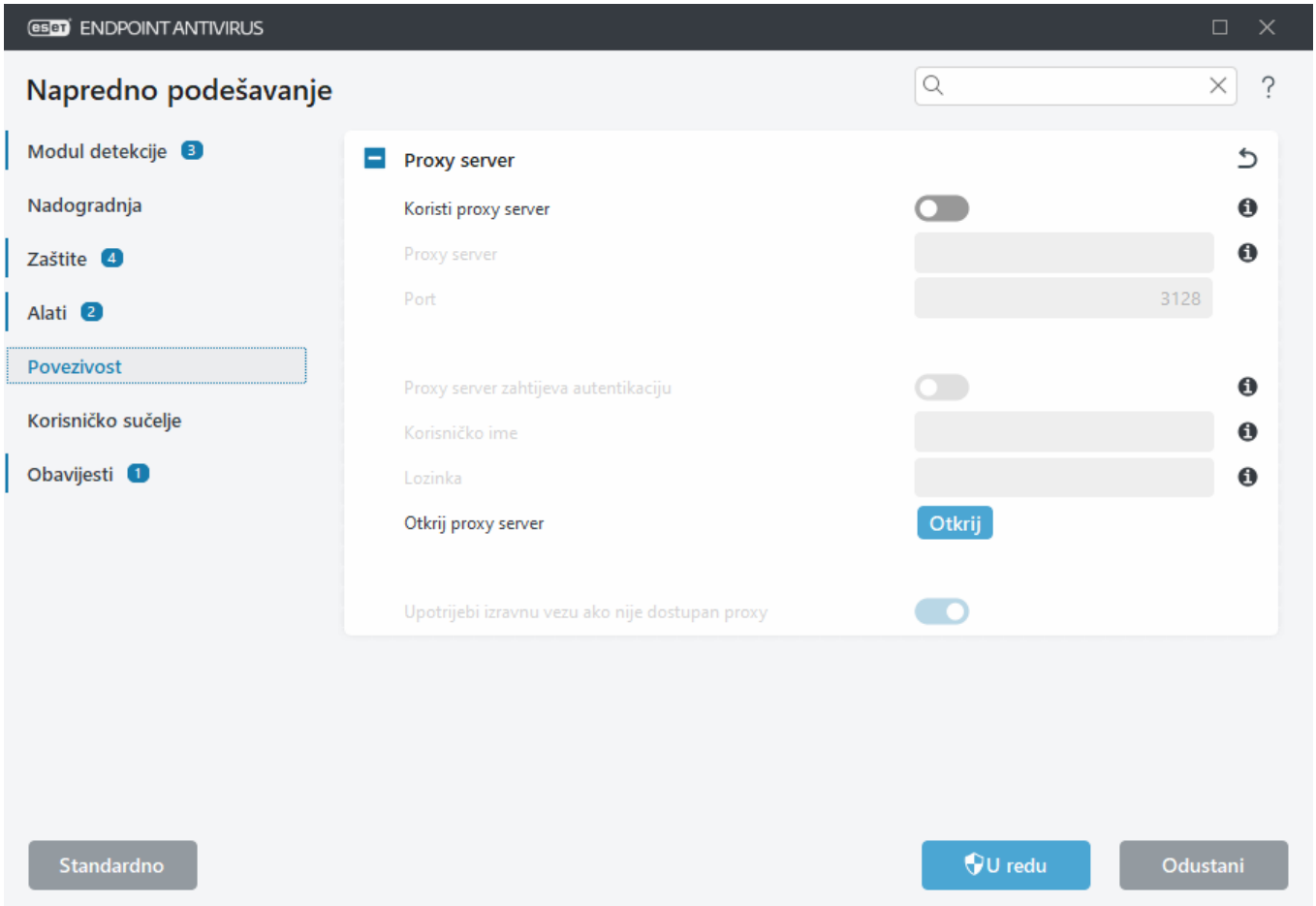
Da biste odredili globalne postavke proxy servera, aktivirajte opciju **Koristi proxy server** i upišite adresu **proxy servera** zajedno s brojem **priključka** proxy servera.

Ako je za komunikaciju s proxy serverom potrebna autorizacija, odaberite opciju **Proxy server zahtijeva prijavu** i u odgovarajuća polja unesite valjano **korisničko ime** i **lozinku**. Kliknite **Otkrij proxy server** da biste automatski prepoznali i ispunili postavke proxy servera. Da biste pronašli postavke proxyja u svojem operacijskom sustavu, pritisnite tipkovne prečace **Windows + I** i kliknite **Mreža i internet** > **Proxy**. ESET Endpoint Antivirus će kopirati parametre određene u internetskim opcijama za Internet Explorer ili Google Chrome.

Korisničko ime i lozinku morate ručno unijeti u postavke **proxy servera**.

Upotrijebi izravnu vezu ako nije dostupan proxy – ako je ESET Endpoint Antivirus konfiguriran za povezivanje putem proxyja, a proxy nije dostupan, program ESET Endpoint Antivirus zaobići će ga i komunicirati izravno s ESET-ovim serverima.

Postavke proxy servera moguće je konfigurirati u stavci Napredno podešavanje > **Ažuriranje** > **Profili** > **Ažuriranja** > **Opcije povezivanja** odabirom opcije **Veza putem proxy servera** s padajućeg izbornika **Proxy način rada**). Ova se konfiguracija primjenjuje samo na ažuriranja i preporučuje se za prijenosna računala koja primaju ažuriranja modula s udaljenih mjesta. Dodatne informacije potražite u odjeljku Podešavanje naprednog ažuriranja.



Korisničko sučelje

Da biste konfigurirali funkcioniranje grafičkog korisničkog sučelja (GUI-ja) programa, otvorite stavku Napredno podešavanje > **Korisničko sučelje**.

Vizualni izgled programa i efekte možete podesiti u odjeljku Elementi korisničkog sučelja na zaslonu Napredno podešavanje.

Za maksimalnu sigurnost sigurnosnog softvera možete spriječiti deinstalaciju ili bilo koje neovlaštene promjene tako da zaštitite postavke putem lozinke s pomoću alata Podešavanje pristupa.

> Da biste konfigurirali ponašanje obavijesti sustava, upozorenja o prijetnjama i statusa aplikacije, pogledajte odjeljak Obavijesti.

Način rada za prezentacije koristan je za korisnike koji žele raditi s aplikacijom, a da ih pritom ne prekidaju skočni prozori, planirani zadaci i bilo koje komponente koje bi mogle opteretiti procesor i RAM.

Također pogledajte Kako minimizirati korisničko sučelje programa ESET Endpoint Antivirus (korisno za upravljana okruženja).

Elementi korisničkog sučelja

Mogućnosti konfiguriranja korisničkog sučelja u programu ESET Endpoint Antivirus omogućuju vam da radno okruženje prilagodite svojim potrebama. Tim konfiguracijskim opcijama može se pristupiti u opcijama **Napredno podešavanje** (F5) > **Korisničko sučelje** > **Elementi korisničkog sučelja**.

U odjeljku **Elementi korisničkog sučelja** možete prilagoditi radno okruženje. S pomoću padajućeg izbornika **Način rada za pokretanje** odaberite neki od sljedećih načina rada za pokretanje grafičkog korisničkog sučelja (GUI-ja):

Sve – Prikazat će se cijeli GUI.

Minimalno – GUI radi, ali korisniku se prikazuju samo obavijesti.

Ručno – GUI se ne pokreće automatski pri prijavi. Svaki ga korisnik može ručno pokrenuti.

Tiho – neće se prikazivati obavijesti ni upozorenja. GUI može pokrenuti samo administrator. Ovaj način rada koristan je za upravljana okruženja ili situacije u kojima trebate sačuvati resurse sustava.

> Ako napravite restart računala dok je odabran minimalni način rada za pokretanje GUI-ja, obavijesti će se prikazati, ali ne i grafičko sučelje. Za vraćanje na način punog korisničkog sučelja pokrenite GUI iz izbornika Start u **Svi programi** > **ESET** > ESET Endpoint Antivirus kao administrator, ili to možete učiniti putem programa ESET PROTECT s pomoću pravila.

Način boja – odaberite shemu boja za ESET Endpoint Antivirus GUI iza padajućeg izbornika:

- **Isto kao i boja sustava** – shema boja programa ESET Endpoint Antivirus postavit će se na temelju postavki operacijskog sustava.
- **Tamno** – program ESET Endpoint Antivirus će imati tamnu shemu boja (tamni način rada).
- **Svijetlo** – program ESET Endpoint Antivirus će imati standardnu, svijetlu shemu boja.

> U gornjem desnom kutu glavnog prozora programa također možete odabrati shemu boja grafičkog korisničkog sučelja programa ESET Endpoint Antivirus.

Ako želite deaktivirati uvodni prozor programa ESET Endpoint Antivirus, poništite odabir **Prikaži uvodni prozor pri pokretanju programa**.

Ako želite da se program ESET Endpoint Antivirus oglasi zvučnim signalom u slučaju važnih događaja tijekom skeniranja, na primjer kada se otkrije prijetnja ili kada se skeniranje završi, odaberite **Koristi zvučni signal**.

Integriraj u kontekstni izbornik – Integrirajte kontrolne elemente programa ESET Endpoint Antivirus u kontekstni izbornik.

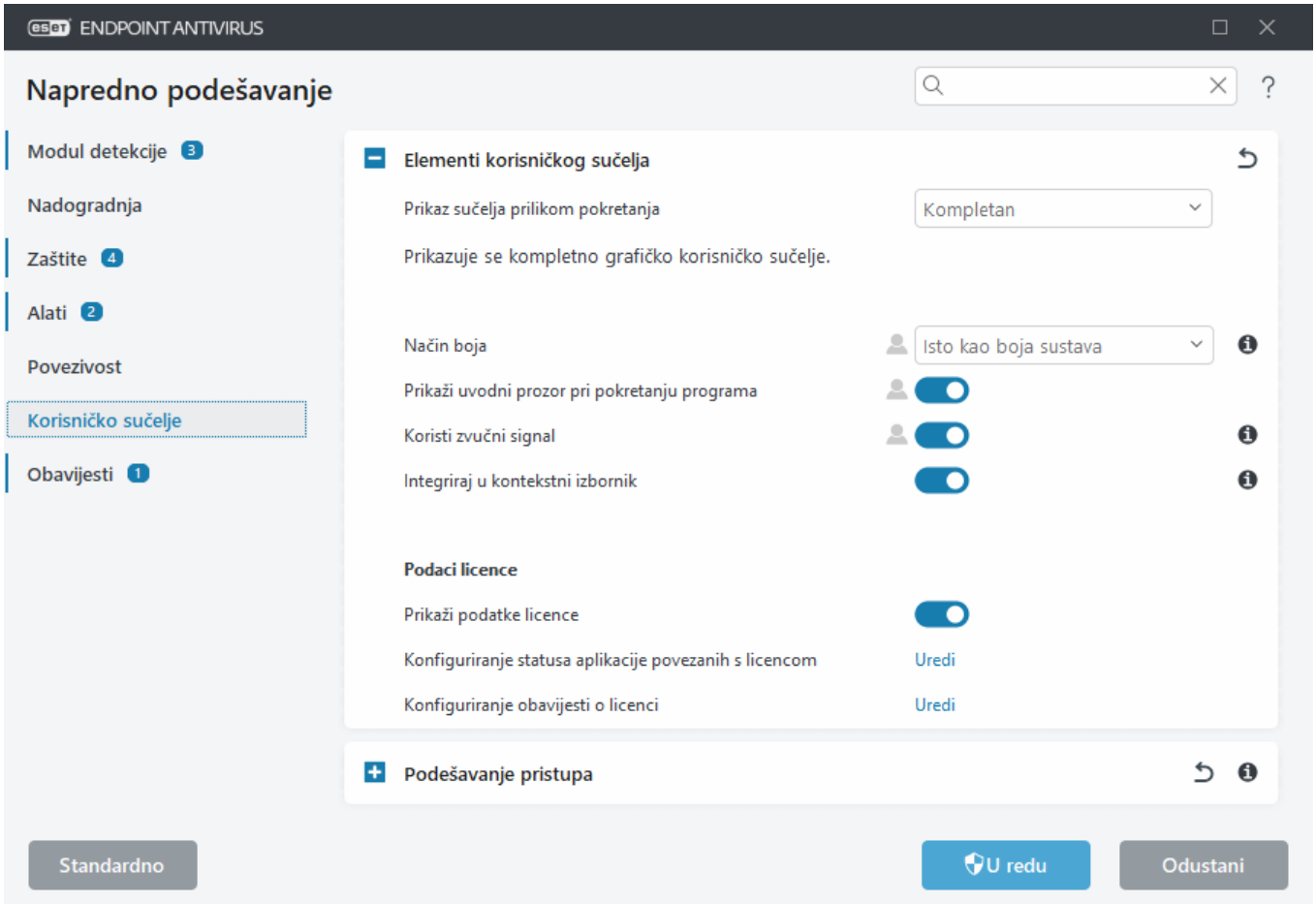
Informacije o licenci

Prikaži informacije o licenci – Kada je ova opcija deaktivirana, informacije o licenci na zaslonu **Status zaštite** i **Pomoć i podrška** neće biti prikazane.

Konfiguriranje statusa aplikacija povezanih s licencom – otvara popis statusa aplikacije povezanih s licencom.

Prikaži poruke i obavijesti u vezi s licencom – Kada je ova opcija deaktivirana, obavijesti i poruke prikazat će se samo kada licenca istekne.

Postavke podataka o licenci primjenjuju se, ali nisu dostupne za proizvod ESET Endpoint Antivirus aktiviran pomoću MSP licence.



Podešavanje pristupa

ESET Endpoint Antivirus postavke su ključan dio vaših sigurnosnih pravila. Neovlaštene izmjene mogu ugroziti stabilnost i zaštitu vašeg sustava. Da bi se izbjegle neovlaštene preinake, parametre podešavanja programa ESET Endpoint Antivirus i njegovu deinstalaciju moguće je zaštititi lozinkom. Postavke pristupa mogu se konfigurirati u stavci Napredno podešavanje > **Korisničko sučelje** > **Podešavanje pristupa**.

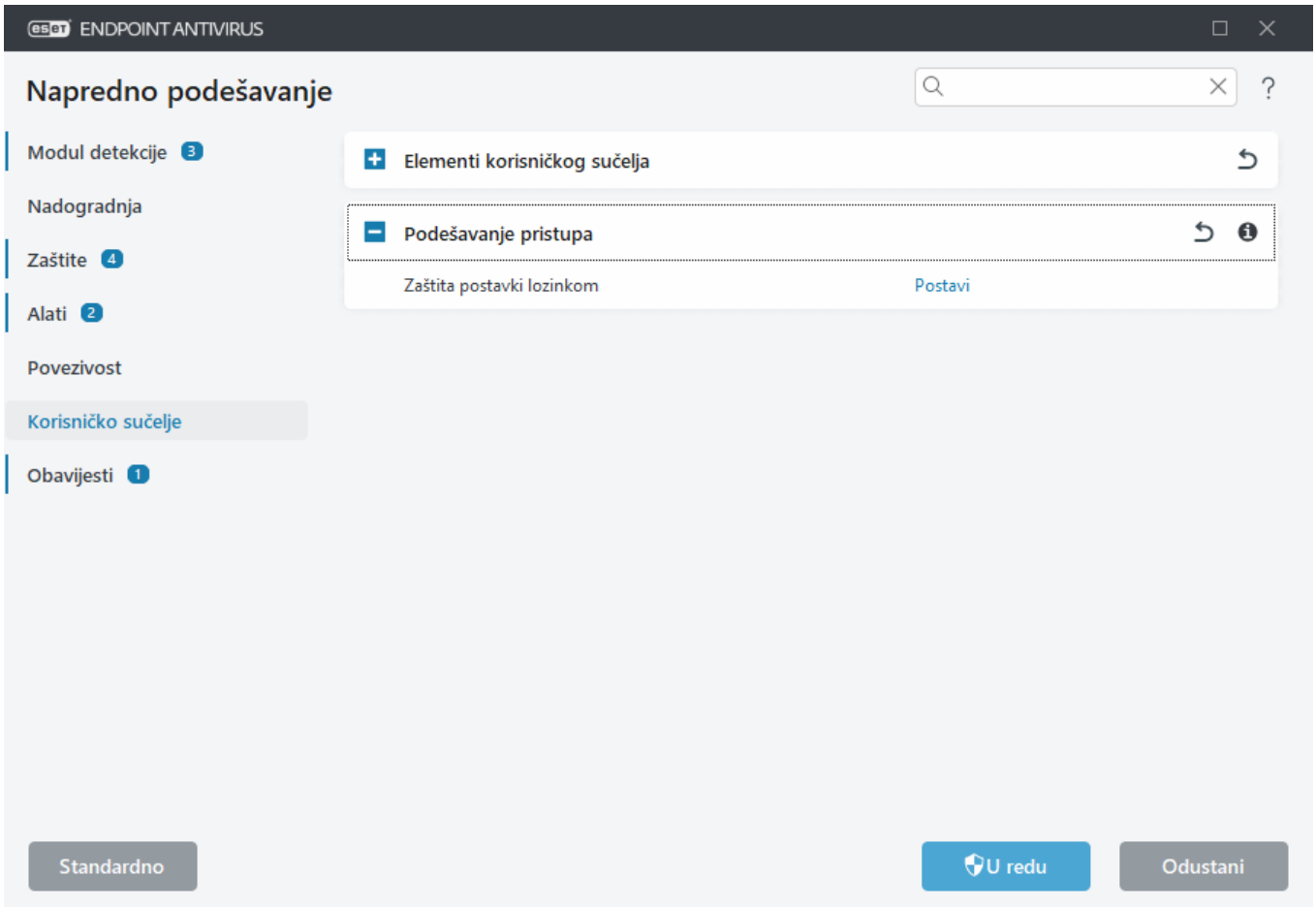
Da biste postavili lozinku za zaštitu parametara podešavanja programa ESET Endpoint Antivirus i njegovu deinstalaciju, kliknite **Postavi** pored stavke **Zaštita postavki lozinkom**.

Da biste promijenili lozinku, kliknite **Promijeni lozinku** pored stavke **Zaštita postavki lozinkom**.

Da biste uklonili lozinku, kliknite **Ukloni** pored stavke **Zaštita postavki lozinkom**.

Upravljana okruženja

Administrator može stvoriti pravilo da bi lozinkom zaštitio postavke programa ESET Endpoint Antivirus na povezanim klijentskim računalima. Za stvaranje novog pravila pogledajte Postavke zaštićene lozinkom.



Lozinka za napredno podešavanje

Da biste zaštitili napredno podešavanje programa ESET Endpoint Antivirus i izbjegli neovlaštene izmjene, upišite novu lozinku u polja **Nova lozinka** i **Potvrda lozinke**. Kliknite **U redu**.

Upravljana okruženja

Administrator može stvoriti pravilo da bi lozinkom zaštitio postavke programa ESET Endpoint Antivirus na povezanim klijentskim računalima. Za stvaranje novog pravila pogledajte Postavke zaštićene lozinkom.

Neupravljano

Ako želite promijeniti postojeću lozinku:

1. Utipkajte staru lozinku u polje **Stara lozinka**.
2. Unesite novu lozinku u polja **Nova lozinka** i **Potvrda nove lozinke**.
3. Kliknite **U redu**.

Ta lozinka morat će se unijeti prilikom budućih preinaka programa ESET Endpoint Antivirus.

Ako ste zaboravili lozinku, pogledajte Otključavanje lozinke za postavke u ESET-ovim Endpoint programima.

Da biste vratili izgubljeni ESET-ov licenčni ključ, datum isteka licence ili druge informacije o licenci za ESET Endpoint Antivirus, pogledajte Izgubio/la sam korisničko ime i lozinku / licenčni ključ.

Lozinka

Da bi se izbjegle neovlaštene izmjene, parametre podešavanja programa ESET Endpoint Antivirus moguće je zaštititi lozinkom.

Sigurni način rada

Ako se grafičko sučelje programa ESET Endpoint Antivirus pokrene u sigurnom načinu rada, prikazat će se dijaloški prozor s napomenom da će se aplikacija pokrenuti u sigurnom načinu rada. Budući da su u sigurnom načinu rada funkcije svih programa ograničene, otvaranje grafičkog sučelja programa ESET Endpoint Antivirus kao u standardnom načinu rada neće biti moguće.

Prikazani prozor osigurava pokretanje skeniranja računala. Ako želite provjeriti postojanje zlonamjernog koda na računalu, odaberite **Da**.

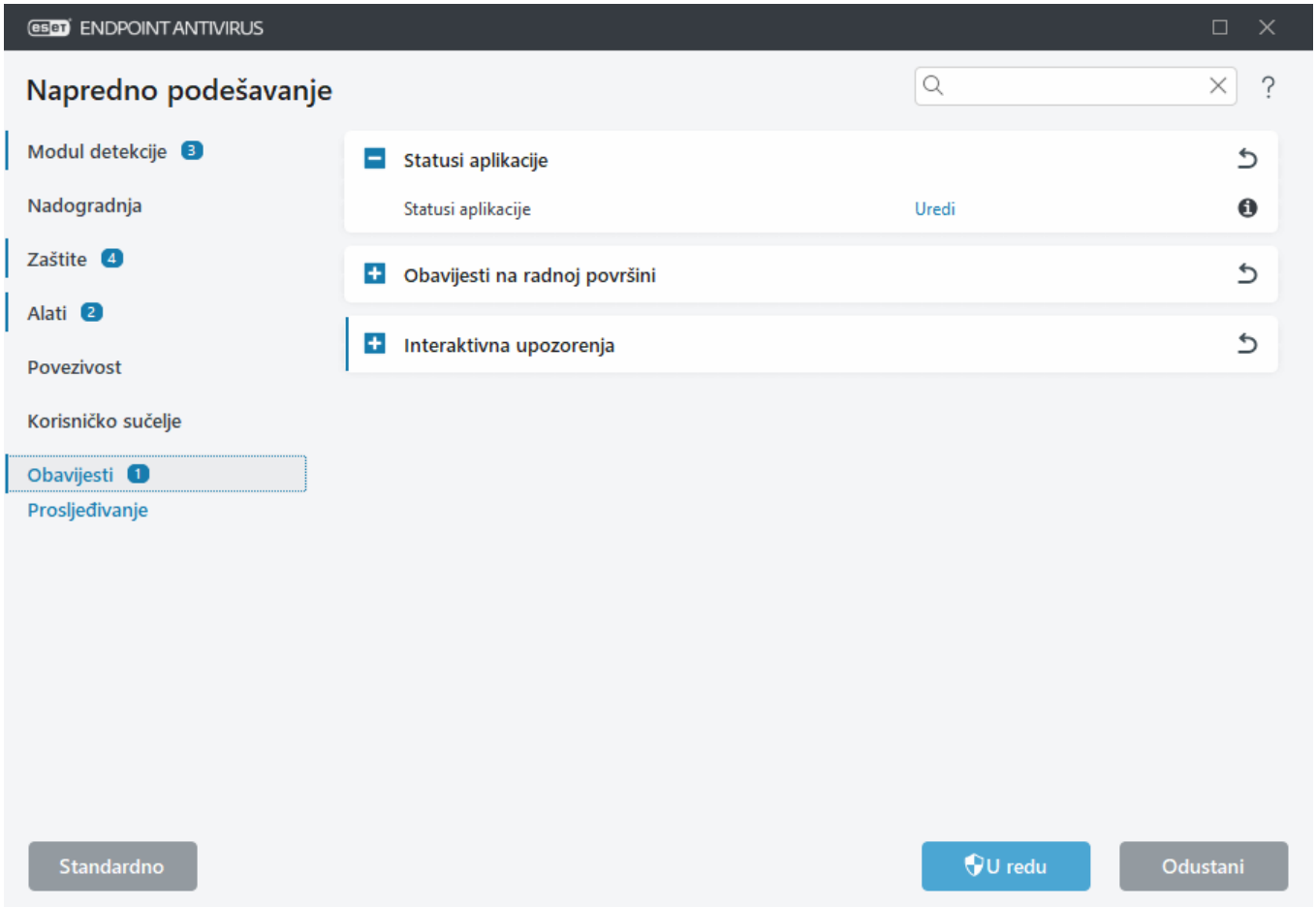
Time ćete u zasebnom prozoru pokrenuti skeniranje s istim parametrima kakve sadrži standardni profil za skeniranje računala nakon instalacije programa ESET Endpoint Antivirus.

Odaberite **Ne** da biste zatvorili dijaloški prozor; ESET Endpoint Antivirus tada neće izvršiti nikakvu akciju.

Obavijesti

Za upravljanje obavijestima programa ESET Endpoint Antivirus otvorite Napredno podešavanje > **Obavijesti**. Možete konfigurirati sljedeće vrste obavijesti:

- Statusi aplikacije – obavijesti prikazane u početnom odjeljku glavnog prozora programa.
- Obavijesti na radnoj površini – mali prozori obavijesti pokraj programske trake sustava.
- Interaktivna upozorenja – prozori s upozorenjima i okviri s porukama koji zahtijevaju interakciju korisnika.
- Prosljeđivanje (obavijesti e-poštom) – obavijesti e-poštom šalju se na određenu adresu e-pošte.
- Prilagodba obavijesti – možete dodati prilagođenu poruku, npr. za obavijest na radnoj površini.



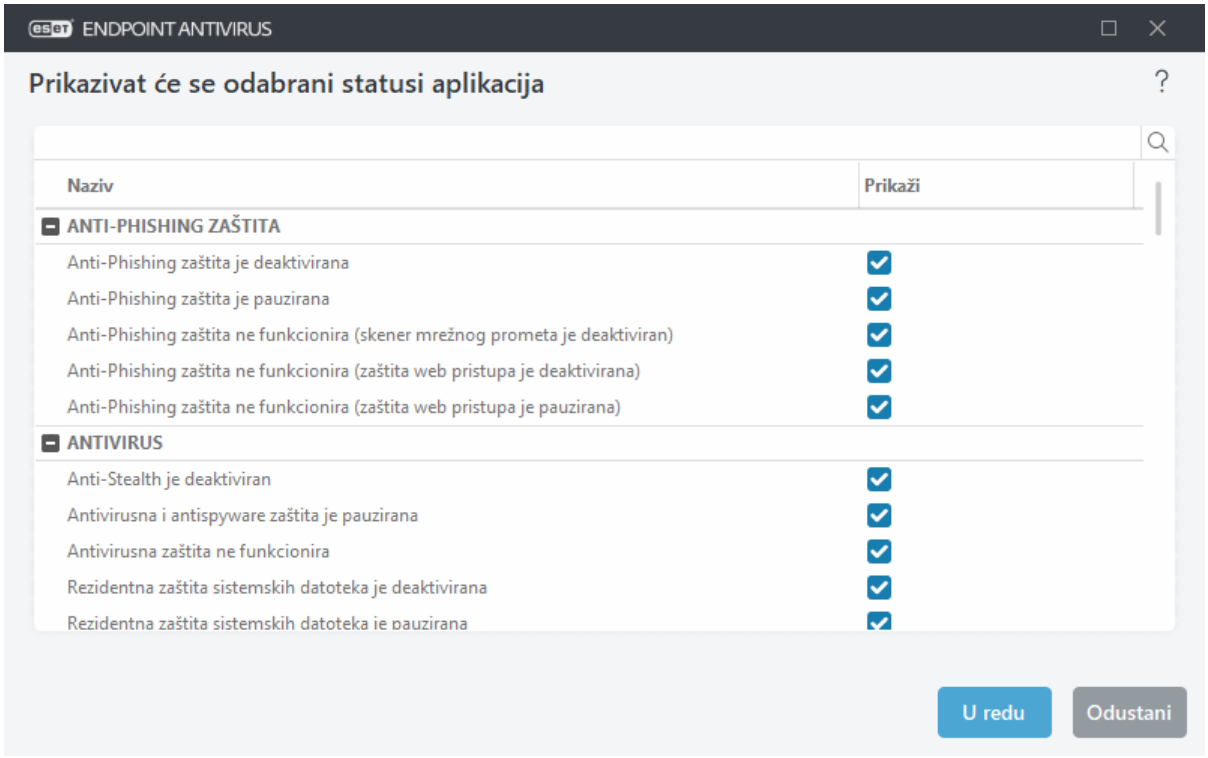
Statusi aplikacije

Statusi aplikacije – kliknite **Uredi** da biste odabrali koji će se statusi aplikacije prikazivati u početnom odjeljku glavnog prozora programa.

Statusi aplikacije

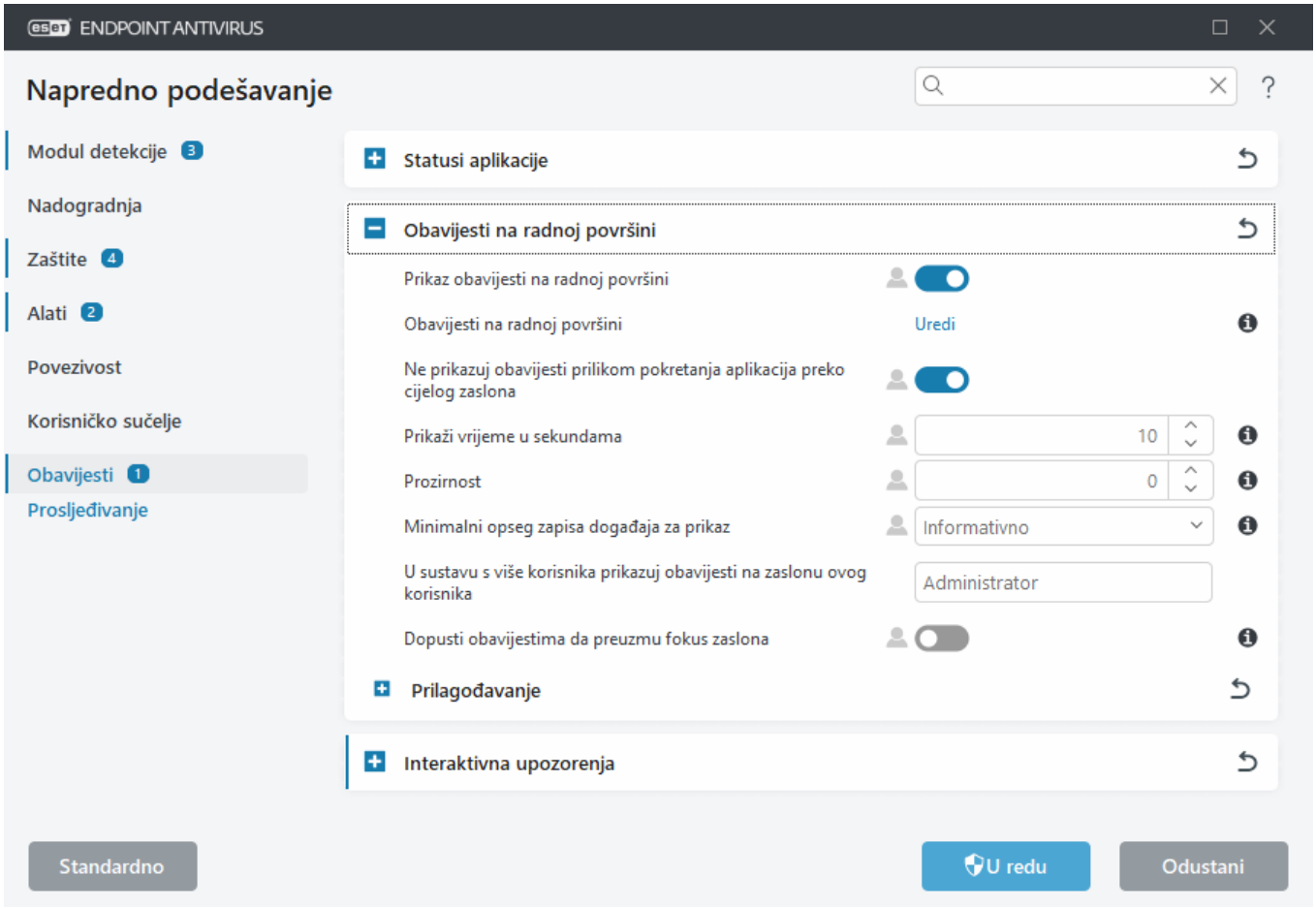
Da biste konfigurirali koji će se statusi aplikacija prikazati (na primjer, kada pauzirate antivirusnu i antispyware zaštitu ili aktivirate način rada za prezentacije), otvorite Napredno podešavanje > **Obavijesti** i kliknite **Uredi** pokraj **statusa aplikacija**.

Status aplikacije prikazat će se i ako program nije aktiviran ili ako je licenca istekla. Ta se postavka može promijeniti pomoću pravila programa ESET PROTECT.



Obavijesti na radnoj površini

Obavijest na radnoj površini prikazuje se kao mali prozor obavijesti pokraj programske trake sustava. Prema standardnim postavkama prikazuje se na 10 sekundi, a zatim postupno nestaje. To je glavni način na koji program ESET Endpoint Antivirus obavještava korisnika o uspješnim nadogradnjama programa, novim povezanim uređajima, dovršetku skeniranja virusa ili novim pronađenim prijetnjama.



Prikaži obavijesti na radnoj površini – preporučujemo da ne deaktivirate tu opciju da biste mogli primati obavijesti programa o novim događajima.

Obavijesti na radnoj površini – kliknite **Uredi** da biste aktivirali ili deaktivirali određene Obavijesti na radnoj površini.

Ne prikazuj obavijesti prilikom pokretanja aplikacija preko cijelog zaslona – isključite sve obavijesti koje nisu interaktivne prilikom pokretanja aplikacija preko cijelog zaslona.

Trajanje u sekundama – postavite trajanje vidljivosti obavijesti. Vrijednost mora biti između 3 i 30 sekundi.

Prozirnost – postavite postotak prozirnosti obavijesti. Podržani raspon je od 0 (nema prozirnosti) do 80 (vrlo visoka prozirnost).

Minimalni opseg zapisa događaja za prikaz – postavite razinu ozbiljnosti prikazane obavijesti. U padajućem izborniku odaberite jednu od sljedećih opcija:

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa te svi prethodno navedeni zapisi.
- **Informacije** – Zapisuju se sve informativne poruke kao što su nestandardni mrežni događaji, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisi.
- **Upozorenja** – zapisuju se kritične pogreške i poruke s upozorenjima (na primjer, neuspjela nadogradnja).
- **Pogreške** – Zapisuju se pogreške (zaštita dokumenata nije pokrenuta) i kritične pogreške.
- **Kritično** – Zapisuju se samo kritične pogreške pri pokretanju antivirusne zaštite ili ako je sustav zaražen.

U sustavu s više korisnika prikazuj obavijesti na zaslonu ovog korisnika – dopušta odabranom računu da prima obavijesti na radnoj površini. Na primjer, ako ne upotrebljavate administratorski račun, upišite puni naziv računa i

obavijesti na radnoj površini prikazat će se za navedeni račun. Samo jedan korisnički račun može primati obavijesti na radnoj površini.

Dopusti obavijestima da preuzmu fokus zaslona – obavijesti će preuzeti fokus zaslona i bit će dostupne pritiskom na Alt+Tab.

Prilagodba obavijesti

U ovom prozoru možete prilagoditi poruke iz obavijesti.

Tekst standardne obavijesti – Standardna poruka koja se prikazuje u podnožju obavijesti.

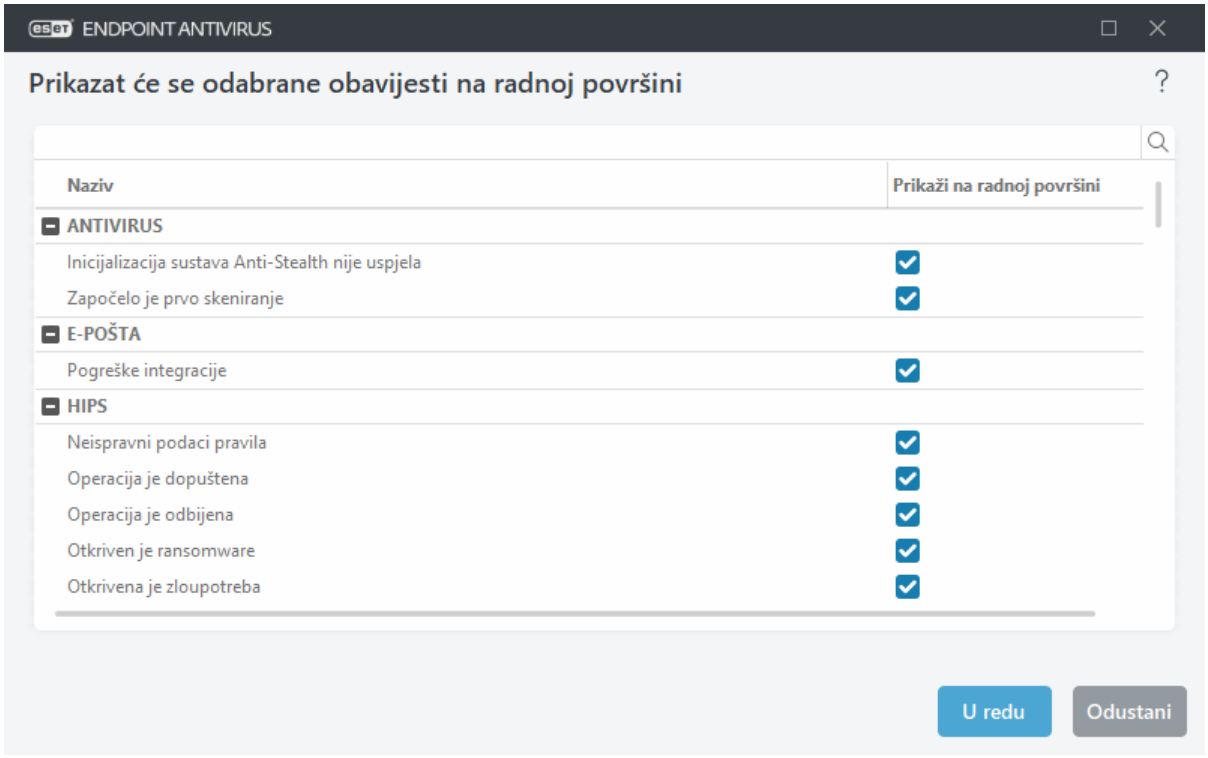
Otkrivene prijetnje

Ako želite da obavijesti o zlonamjernom softveru ostanu na zaslonu sve dok ih ručno ne zatvorite, aktivirajte mogućnost **Nemoj automatski zatvarati obavijesti o zlonamjernom softveru**.

Za korištenje prilagođenih poruka obavijesti deaktivirajte **Koristi standardnu poruku** i unesite vlastitu poruku u polje **Poruka obavijesti o prijetnji**.

Dijaloški prozor – obavijesti na radnoj površini

Da biste podesili vidljivost obavijesti na radnoj površini (koje se prikazuju u donjem desnom kutu zaslona), otvorite Napredno podešavanje > **Obavijesti** > **Obavijesti na radnoj površini**. Kliknite **Uredi** uz opciju **Obavijesti na radnoj površini** i odaberite odgovarajući potvrdni okvir opcije **Prikaži na radnoj površini**.



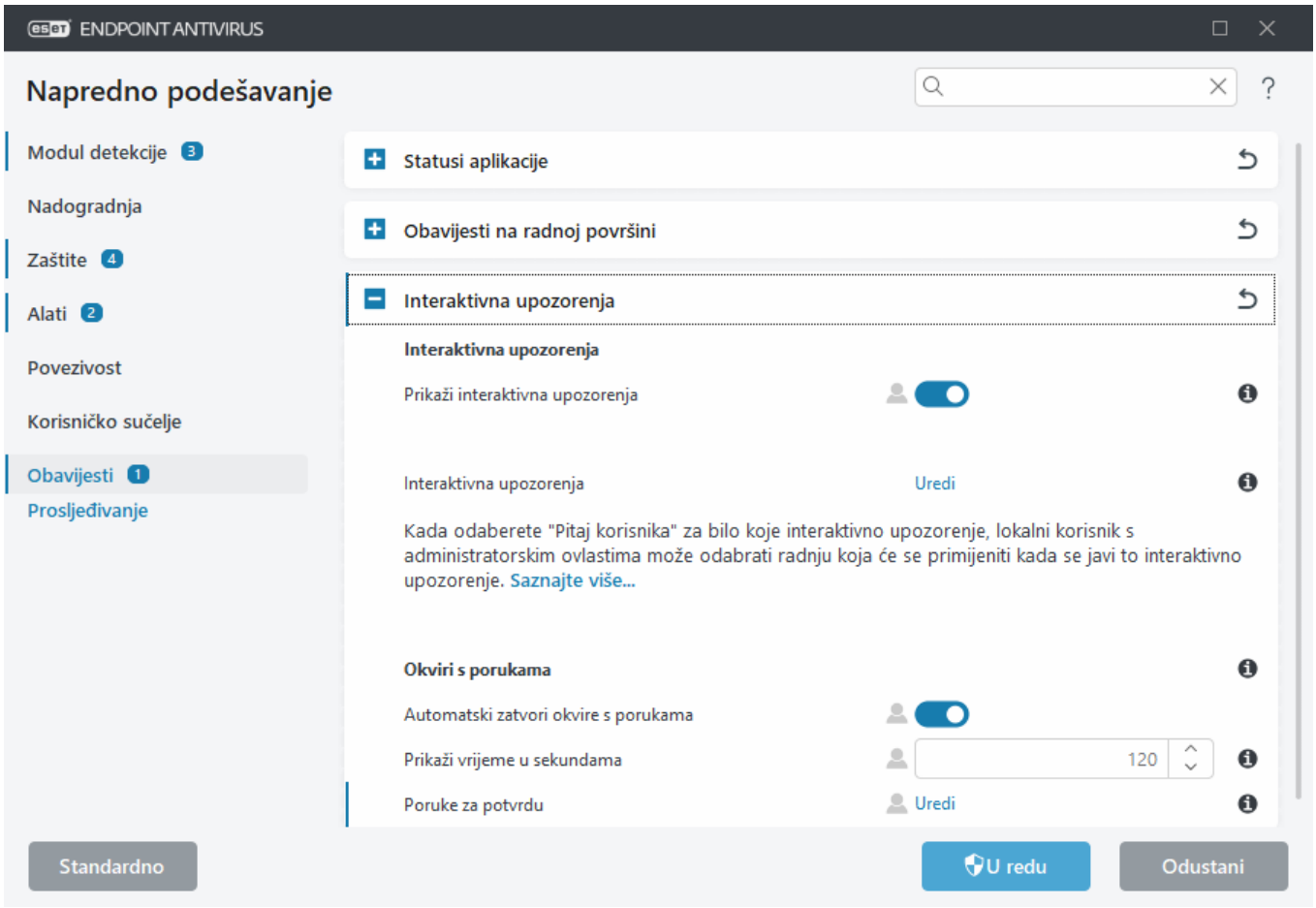
Ako želite postaviti obavijesti **Datoteka analizirana** i **Datoteka nije analizirana** tijekom upotrebe programa ESET LiveGuard, Proaktivna zaštita mora biti postavljena na **Blokiranje pokretanja do primanja rezultata analize**.

Interaktivna upozorenja

Tražite informacije o čestim upozorenjima i obavijestima?

- Pronađena je prijetnja
- Adresa je blokirana
- Program nije aktiviran
- Dostupna je nadogradnja
- Informacije o nadogradnji nisu dosljedne
- Otklanjanje poteškoća za poruku "Nadogradnja modula nije uspjela"
- 'Oštećena datoteka' ili 'Preimenovanje datoteke nije uspjelo'
- Odbijen certifikat web stranice
- Blokirana je mrežna prijetnja
- Datoteka blokirana zbog analize

Odjeljak **Interaktivna upozorenja** u dijelu Napredno podešavanje > **Obavijesti** omogućuje vam da konfigurirate kako ESET Endpoint Antivirus upravlja okvirima s porukama i interaktivnim upozorenjima za prijetnje u slučaju kada korisnik treba donijeti odluku (na primjer, potencijalna web stranica za phishing).



Interaktivna upozorenja

Deaktiviranjem opcije **Prikaži interaktivna upozorenja** sakrit će se svi prozori upozorenja i dijaloški okviri u pregledniku, što je prikladno samo za ograničen broj specifičnih situacija.

- Za korisnike kojima se ne upravlja preporučujemo da se ova opcija ostavi u standardnoj postavci (aktivirano).
- Za korisnike kojima se upravlja ova postavka treba ostati aktivirana te odaberite unaprijed definiranu radnju za korisnika na popisu interaktivnih upozorenja.

Interaktivna upozorenja – kliknite **Uredi** da biste odabrali koja će se interaktivna upozorenja prikazivati.

Okviri s porukama

Da biste automatski zatvorili okvire s porukama nakon određenog vremena, odaberite opciju **Automatski zatvori okvire s porukama**. Ako se okviri ne zatvore ručno, prozori upozorenja automatski se zatvaraju nakon isteka određenog vremenskog razdoblja.

Istek vremena u sekundama – postavlja trajanje vidljivosti upozorenja. Vrijednost mora biti između 10 i 999 sekundi.

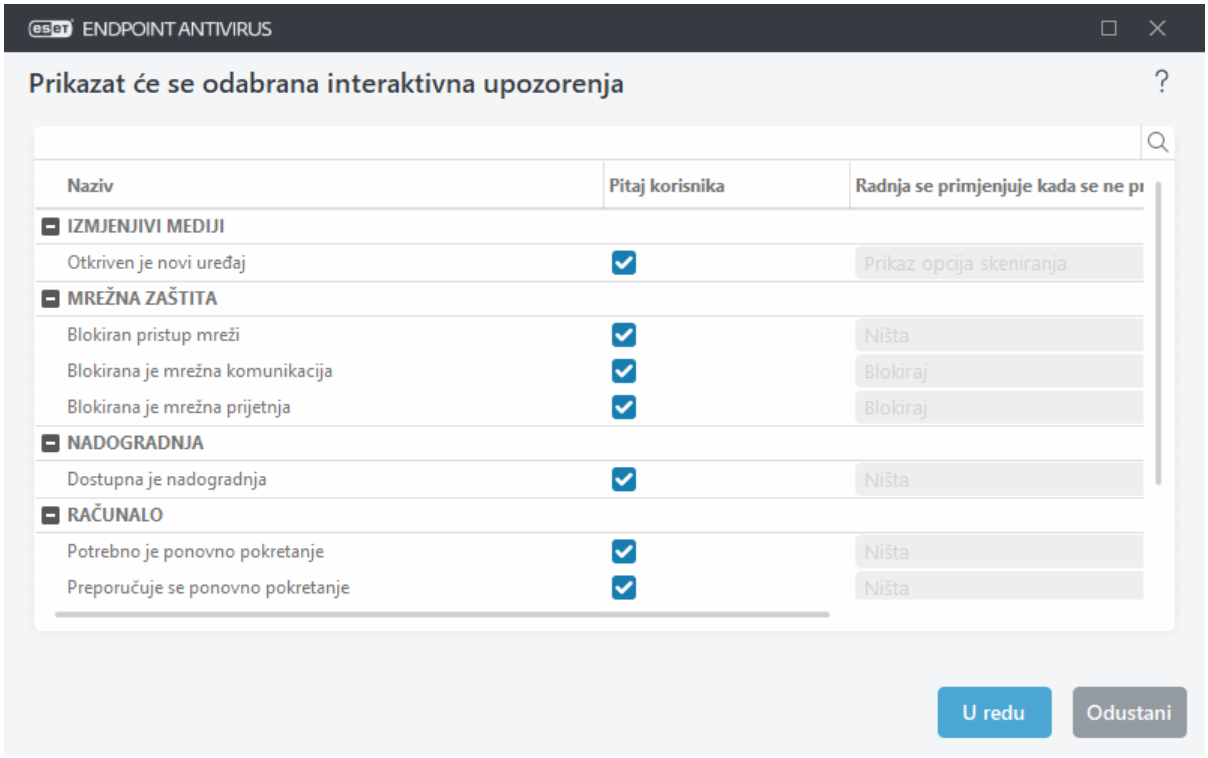
Poruke za potvrdu – kliknite **Uredi** za prikaz popisa poruka za potvrdu na kojem možete odabrati hoće li se poruke prikazivati ili ne.

Popis interaktivnih upozorenja

U ovom je odjeljku istaknuto nekoliko prozora s interaktivnom upozorenjima koja će ESET Endpoint Antivirus prikazati prije provođenja bilo koje radnje.

Da biste podesili ponašanje interaktivnih upozorenja koja se mogu konfigurirati, otvorite Napredno podešavanje > **Obavijesti** > **Interaktivna upozorenja** i kliknite **Uredi** pored opcije **Interaktivna upozorenja**.

> Korisno za upravljana okruženja gdje administrator svugdje može poništiti odabir opcije **Pitaj korisnika** i odabrati unaprijed definiranu radnju kad se prikažu prozori s interaktivnim upozorenjima.



Provjerite ostale odjeljke pomoći u kojima se navodi određeni prozor s interaktivnim upozorenjem:

Izmjenjivi mediji

- Otkriven je novi uređaj

Mrežna zaštita

- Blokiran pristup mreži prikazuje se kad se pokrene zadatak klijenta **Izolacija računala s mreže** na ovoj radnoj stanici iz programa ESET PROTECT.
- Blokirana je mrežna komunikacija
- Blokirana je mrežna prijetnja

Upozorenja web preglednika

- Pronađen je potencijalno neželjen sadržaj
- Web stranica blokirana zbog phishinga

Računalo

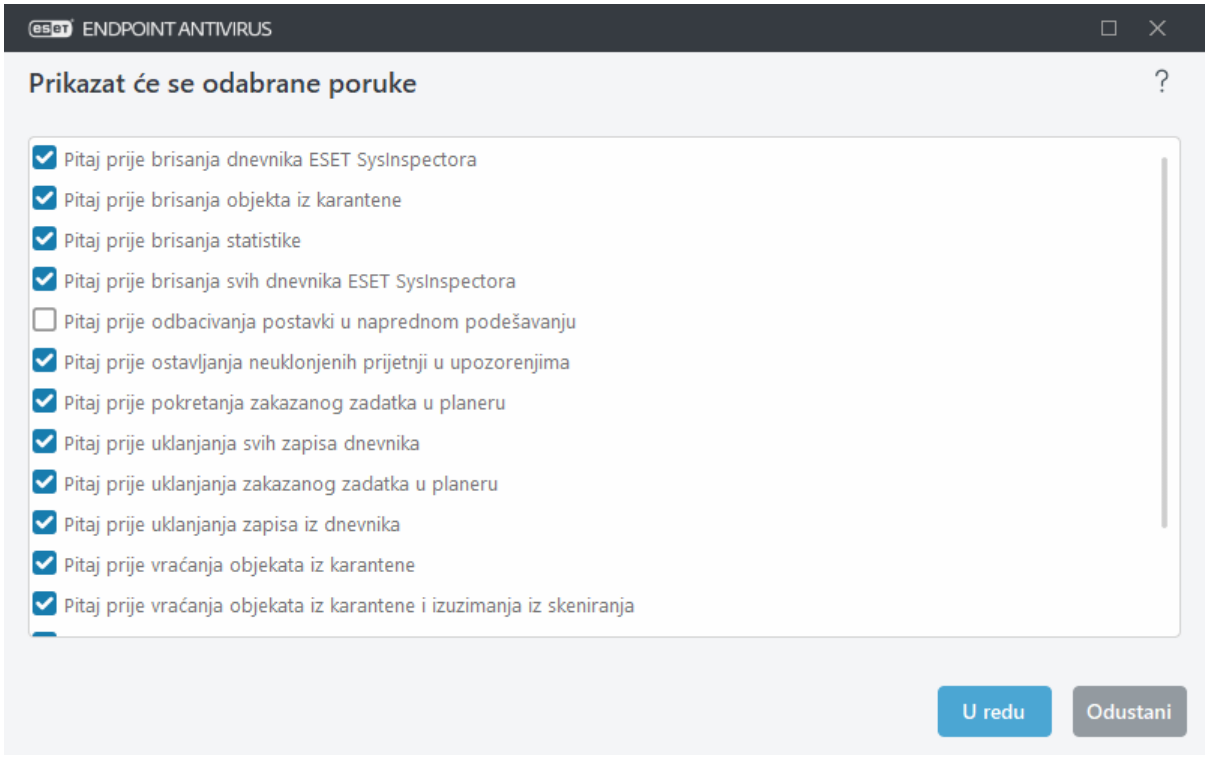
Zbog prisutnosti ovih upozorenja promijenit će se boja korisničkog sučelja:

- Ponovno pokreni računalo (obavezno)
- Ponovno pokreni računalo (preporučeno)

Interaktivna upozorenja ne sadrže interaktivne prozore modula detekcije, HIPS-a ni firewalla jer se njihovo ponašanje može pojedinačno konfigurirati u određenoj funkciji.

Poruke za potvrdu

Da biste podesili poruke za potvrdu, idite na Napredno podešavanje > **Obavijesti** > **Interaktivna upozorenja** i kliknite **Uredi** pored opcije **Poruke za potvrdu**.



U ovom se dijaloškom prozoru prikazuju poruke za potvrdu koje program ESET Endpoint Antivirus prikazuje prije provođenja bilo kakve akcije. Da biste dopustili prikaz neke poruke za potvrdu ili je deaktivirali, odaberite ili poništite odabir potvrdnog okvira pored nje.

Saznajte više o određenoj funkciji povezanoj s porukama za potvrdu:

- Pitaj prije brisanja dnevnika programa ESET SysInspector
- Pitaj prije brisanja svih dnevnika programa ESET SysInspector
- Pitaj prije brisanja objekta iz karantene
- Pitaj prije odbacivanja postavki u naprednom podešavanju
- Pitaj prije ostavljanja neuklonjenih prijetnji u upozorenjima
- Pitaj prije uklanjanja zapisa iz dnevnika
- Pitaj prije uklanjanja zakazanog zadatka u planeru
- Pitaj prije uklanjanja svih zapisa dnevnika
- Pitaj prije brisanja statistike
- Pitaj prije vraćanja objekata iz karantene
- Pitaj prije vraćanja objekata iz karantene i izuzimanja iz skeniranja
- Pitaj prije pokretanja zakazanog zadatka u planeru
- Prikaži potvrdne dijaloške okvire za Outlook Express i Windows Mail
- Prikaži potvrdne dijaloške okvire za Windows Live Mail
- Prikaži potvrdne dijaloške okvire za Outlook

Pogreška zbog sukoba naprednih postavki

Do ove pogreške može doći ako neka komponenta (na primjer, HIPS (npr. HIPS) i korisnik stvore pravila u interaktivnom načinu rada ili načinu rada za učenje istovremeno.

Preporučujemo da promijenite način filtriranja u standardni **Automatski način rada** ako želite sami stvarati svoja pravila. Pročitajte više o HIPS-u i HIPS načinima filtriranja.

Potrebno je ponovno pokretanje

Restartanje računala je potrebno nakon nadogradnje na novu verziju programa ESET Endpoint Antivirus ili nakon primjene zakrpa na aplikacije pomoću upravljanja zakrpama i ranjivosti. Nove verzije programa ESET Endpoint Antivirus izdaju se radi instalacije poboljšanja ili popravka problema koji se ne mogu riješiti automatskom nadogradnjom modula programa.

Kliknite **Restartaj odmah** da biste restartali računalo. Ako planirate restartati računalo kasnije, kliknite **Podsjeti me kasnije**. Kasnije možete ručno restartati računalo iz odjeljka **Status zaštite** u glavnom prozoru programa.

Da biste deaktivirali upozorenje „Potrebno je ponovno pokretanje” ili „Preporučuje se ponovno pokretanje”, pratite korake u nastavku:

1. Otvorite **Napredno podešavanje** (F5) > **Obavijesti** > **Interaktivna upozorenja**.
2. Kliknite **Uredi** pokraj stavke **Interaktivna upozorenja**. U odjeljku **Računalo** odznačite okvire pored odjeljka **Ponovno pokreni računalo (obavezno)** i **Ponovno pokreni računalo (preporučeno)**.
3. Kliknite **U redu** za spremanje promjena u oba otvorena prozora.
4. Upozorenja se više neće prikazivati na krajnjem uređaju.
5. (nije obavezno) Da biste deaktivirali status aplikacije u glavnom prozoru programa ESET Endpoint Antivirus, u prozoru Status aplikacija odznačite okvire pored odjeljaka **Potrebno je ponovno pokretanje računala** i **Preporučuje se ponovno pokretanje računala**.

Preporučuje se ponovno pokretanje

Nakon nadogradnje programa ESET Endpoint Antivirus na novu verziju potrebno je restartati računalo. Nove verzije programa ESET Endpoint Antivirus izdaju se radi instalacije poboljšanja ili popravka problema koji se ne mogu riješiti automatskom nadogradnjom modula programa.

Kliknite **Restartaj odmah** da biste restartali računalo. Ako planirate restartati računalo kasnije, kliknite **Podsjeti me kasnije**. Kasnije možete ručno restartati računalo iz odjeljka **Status zaštite** u glavnom prozoru programa.

Da biste deaktivirali upozorenje „Potrebno je ponovno pokretanje” ili „Preporučuje se ponovno pokretanje”, pratite korake u nastavku:

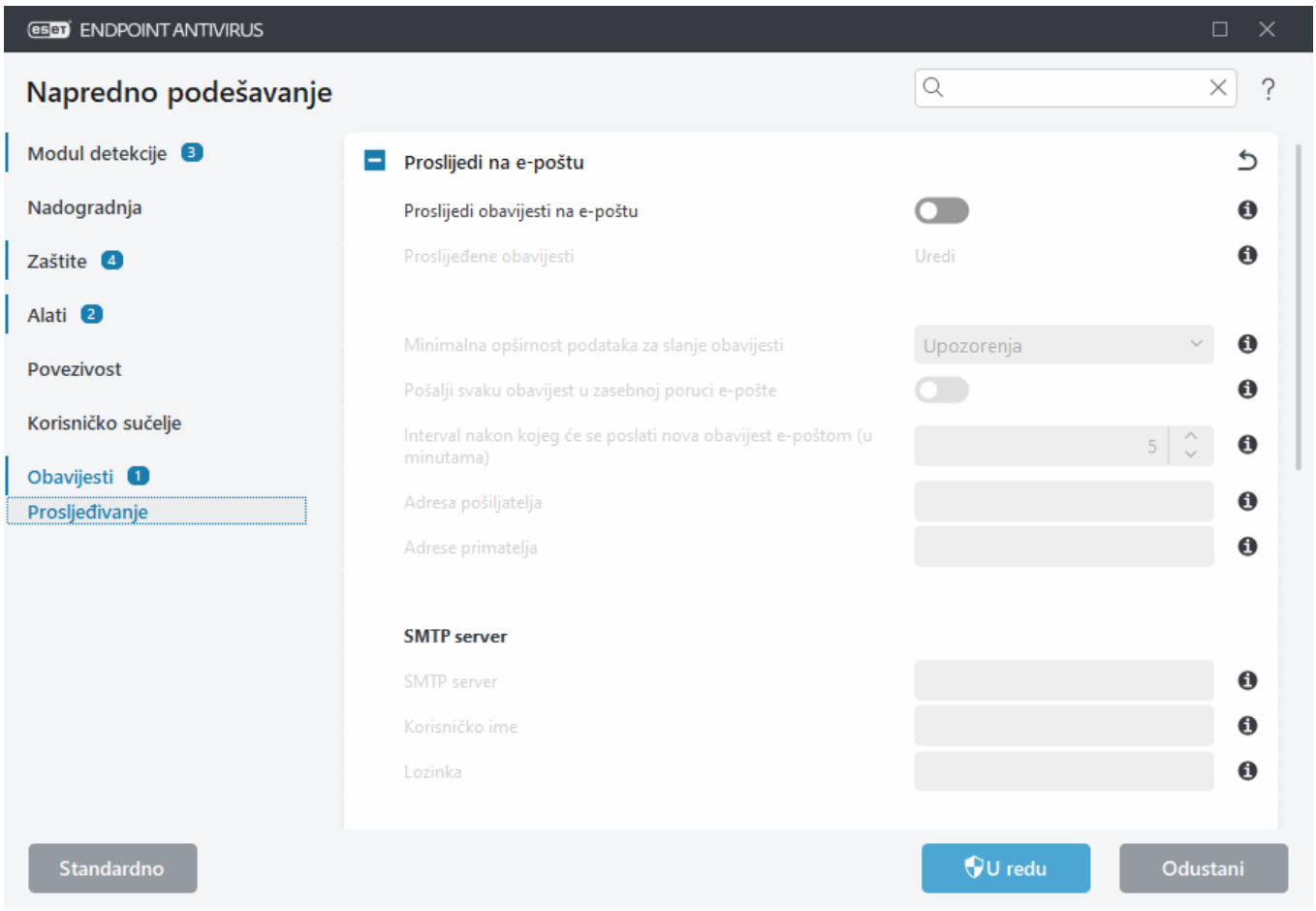
1. Otvorite **Napredno podešavanje** (F5) > **Obavijesti** > **Interaktivna upozorenja**.
2. Kliknite **Uredi** pokraj stavke **Interaktivna upozorenja**. U odjeljku **Računalo** odznačite okvire pored odjeljka **Ponovno pokreni računalo (obavezno)** i **Ponovno pokreni računalo (preporučeno)**.
3. Kliknite **U redu** za spremanje promjena u oba otvorena prozora.
4. Upozorenja se više neće prikazivati na krajnjem uređaju.
5. (nije obavezno) Da biste deaktivirali status aplikacije u glavnom prozoru programa ESET Endpoint Antivirus,

u prozoru Status aplikacija odznačite okvire pored odjeljaka **Potrebno je ponovno pokretanje računala** i **Preporučuje se ponovno pokretanje računala**.

Prosljeđivanje

ESET Endpoint Antivirus može automatski slati obavijesti e-poštom ako dođe do događaja s odabranom razinom opširnosti. U odjeljku Napredno podešavanje > **Obavijesti** > **Prosljeđivanje** > **Proslijedi na e-poštu** aktivirajte stavku **Proslijedi obavijesti na e-poštu** da biste aktivirali obavijesti e-poštom.

Proslijeđene obavijesti – odaberite obavijesti na radnoj površini koje se prosljeđuju na e-poštu.



Na padajućem izborniku **Minimalna opširnost za obavijesti** možete odabrati početnu razinu ozbiljnosti za obavijesti.

- **Dijagnostički** – Zapisuju se sve informacije potrebne za detaljno konfiguriranje programa te svi prethodno navedeni zapisi.
- **Informacije** – Zapisuju se sve informativne poruke kao što su nestandardni mrežni događaji, uključujući uspješne aktualizacije, te svi prethodno navedeni zapisi.
- **Upozorenja** – zapisuju se kritične pogreške i poruke s upozorenjima (na primjer, neuspjela nadogradnja).
- **Pogreške** – Zapisuju se pogreške (zaštita dokumenata nije pokrenuta) i kritične pogreške.
- **Kritično** – bilježi samo kritične pogreške (na primjer, Pogreška pri pokretanju antivirusne zaštite ili Pronađena prijetnja).

Pošalji svaku obavijest u zasebnoj poruci e-pošte – kada je ova opcija aktivirana, primatelj će primiti novu poruku e-pošte za svaku obavijest. To može dovesti do primitka velikog broja poruka e-pošte u kratkom vremenskom

razdoblju.

Interval nakon kojeg će biti poslana obavijest e-poštom (min) – Interval u minutama nakon kojeg će nove obavijesti biti poslane e-poštom. Ako ovu vrijednost postavite na 0, obavijesti će biti odmah poslane.

Adresa pošiljatelja – U tom se polju navodi adresa pošiljatelja koja se prikazuje u zaglavlju poruka e-pošte s obavijestima.

Adrese primatelja – u tom se polju navode adrese primatelja koje se prikazuju u zaglavlju poruka e-pošte s obavijestima. Podržano je više vrijednosti. Upotrijebite točku sa zarezom za odvajanje.

SMTP server

SMTP server – SMTP server koji se upotrebljava za slanje obavijesti (npr. *smtp.provider.com:587*, prethodno definirani port je 25).

Program ESET Endpoint Antivirus podržava SMTP servere s TLS šifriranjem.

Korisničko ime i lozinka – Ako SMTP zahtjeva autorizaciju, ova se polja trebaju popuniti ispravnim korisničkim imenom i lozinkom kako bi se moglo pristupiti SMTP serveru.

Adresa pošiljatelja – U tom se polju navodi adresa pošiljatelja koja se prikazuje u zaglavlju poruka e-pošte s obavijestima.

Adresa primatelja – U ovom polju navode se adrese primatelja koje će biti prikazana u zaglavlju obavijesti e-poštom. Upotrijebite točku sa zarezom „;” da biste odvojili više adresa e-pošte.

Aktiviraj TLS – Aktivira slanje upozorenja i poruka obavijesti koje podržavaju TLS šifriranje.

Oblik poruke

Komunikacija između programa i udaljenog korisnika ili administratora sustava odvija se putem e-pošte ili poruka u LAN-u (putem servisa za razmjenu poruka sustava Windows). Standardni oblik za poruke upozorenja i obavijesti optimalan je za većinu situacija. U nekim ćete okolnostima možda morati promijeniti oblik poruka o događajima.

Oblik poruka o događaju – Format poruka o događaju koje su prikazane na udaljenim računalima.

Oblik poruka s upozorenjem o prijetnji – poruke s upozorenjem o prijetnji i poruke s obavijestima imaju unaprijed definirani standardni oblik. Preporučujemo da ne mijenjate taj oblik. Međutim, u nekim ćete okolnostima (na primjer, ako upotrebljavate automatizirani sustav za obradu e-pošte) možda morati promijeniti oblik poruka.

Charset – Pretvara poruku e-pošte u ANSI kodiranje znakova na temelju regionalnih postavki sustava Windows (npr. windows-1250, Unicode (UTF-8), ACSII 7-bit ili japanski (ISO-2022-JP)). Zbog toga će "á" biti promijenjeno u "a", a nepoznati simbol u "?".

Koristi Quoted-printable kodiranje znakova – Izvor poruke e-pošte bit će kodiran u oblik Quoted-printable (QP) koji koristi ASCII znakove i može ispravno e-poštom prenijeti posebne znakove u 8-bitnom obliku (čććžšđ).

Ključne riječi (nizovi odvojeni znakovima %) u poruci zamjenjuju se stvarnim podacima koji se odnose na to upozorenje. Dostupne su sljedeće ključne riječi:

- **%TimeStamp%** – datum i vrijeme događaja
- **%Scanner%** – modul o kojem je riječ
- **%ComputerName%** – naziv računala na kojem se pojavilo upozorenje
- **%ProgramName%** – program koji je generirao upozorenje
- **%InfectedObject%** – naziv zaražene datoteke, poruke itd.
- **%VirusName%** – identifikacija zaraze
- **%Action%** – radnja koja se poduzima nakon infiltracije
- **%ErrorDescription%** – opis događaja koji nije izazvan virusom

Ključne riječi **%InfectedObject%** i **%VirusName%** koriste se samo u porukama s upozorenjima o prijetnjama, a **%ErrorDescription%** se koristi samo u porukama o događajima.

Vrati sve postavke na standardne

Kliknite **Standardno** u prozoru Napredno podešavanje kako biste vratili sve postavke programa za sve module. Ponovo će se postaviti na status koji bi imale nakon nove instalacije.

Također pogledajte Uvoz i izvoz postavki.

Želite li vratiti sve postavke u ovom odjeljku

Kliknite zakrivljenu strelicu da biste vratili sve postavke u trenutačnom odjeljku za standardne postavke koje određuje ESET.

Imajte na umu, sve promjene koje ste učinili izgubit će se nakon što kliknete **Vrati na standardne postavke**.

Vrati sadržaj tablica – Kad je aktivirano, sva pravila, zadaci ili profili dodani u tablice, bilo ručno ili automatski, bit će izgubljeni.

Također pogledajte Uvoz i izvoz postavki.

Pogreška prilikom spremanja konfiguracije

Ta poruka o pogrešci znači da postavke nisu ispravno spremljene jer je došlo do pogreške.

To obično znači da korisnik koji je pokušao promijeniti parametre programa:

- nema dovoljna prava pristupa ili nema ovlasti operacijskog sustava koje su potrebne za promjenu datoteka konfiguracije i registra sustava.
  > Za izvođenje željenih izmjena mora se prijaviti administrator sustava.
- nedavno je aktivirao način rada za učenje u HIPS-u ili firewallu i pokušao izvršiti promjene u naprednom podešavanju.
  > Da biste spremili konfiguraciju i izbjegli konflikt konfiguracije, zatvorite Napredno podešavanje bez spremanja i pokušajte ponovno izvršiti željene promjene.

Drugi je najčešći slučaj taj da program više ne radi ispravno, oštećen je i potrebno ga je reinstalirati.

Skener naredbenog retka

Modul za antivirusnu zaštitu programa ESET Endpoint Antivirus moguće je pokrenuti iz naredbenog retka – ručno (pomoću naredbe „ecls”) ili pomoću skupne datoteke („bat”).

Upotreba ESET skenera iz naredbenog retka:

```
ecls [MOGUĆNOSTI..] DATOTEKE..
```

Kada se skeniranje na zahtjev pokreće iz naredbenog retka, potrebno je koristiti sljedeće parametre:

Mogućnosti

/base-dir=MAPA	učitaj module iz MAPE
/quar-dir=MAPA	MAPA karantene
/exclude=MASKA	izuzmi iz skeniranja datoteke koje odgovaraju MASKI
/subdir	skeniraj podmape (standardno)
/no-subdir	ne skeniraj podmape
/max-subdir-level=RAZINA	maksimalna podrazina mapa unutar mapa za skeniranje
/symlink	slijedi simboličke veze (standardno)
/no-symlink	preskoči simboličke veze
/ads	skeniraj ADS-ove (standardno)
/no-ads	ne skeniraj ADS-ove
/log-file=DATOTEKA	zapiši izlaz u DATOTEKU
/log-rewrite	prebriši izlaznu datoteku (standardno – dopuni)
/log-console	zapiši izlaz u konzolu (standardno)
/no-log-console	ne zapisuj izlaz u konzolu
/log-all	zapiši i čiste datoteke
/no-log-all	ne zapisuj čiste datoteke (standardno)
/aind	prikaži indikator aktivnosti
/auto	automatski skeniraj i očisti sve lokalne diskove

Mogućnosti skenera

/files	skeniraj datoteke (standardno)
/no-files	ne skeniraj datoteke
/memory	skeniraj memoriju
/boots	skeniraj boot sektore
/no-boots	ne skeniraj boot sektore (standardno)
/arch	skeniraj arhive (standardno)
/no-arch	ne skeniraj arhive
/max-obj-size=VELIČINA	skeniraj samo datoteke manje od VELIČINE u megabajtima (standardno 0 = neograničeno)

/max-arch-level=RAZINA	maksimalna podrazina arhiva unutar arhiva (ugniježđene arhive) za skeniranje
/scan-timeout=OGRANIČENJE	skeniraj arhive najviše do OGRANIČENJA u sekundama
/max-arch-size=VELIČINA	skeniraj samo datoteke u arhivi ako su manje od VELIČINE (standardno 0 = neograničeno)
/max-sfx-size=VELIČINA	skeniraj samo datoteke u samoraspakirajućim arhivama ako su manje od VELIČINE u megabajtima (standardno 0 = neograničeno)
/mail	skeniraj datoteke e-pošte (standardno)
/no-mail	ne skeniraj datoteke e-pošte
/mailbox	skeniraj poštanske sandučiće (standardno)
/no-mailbox	ne skeniraj poštanske sandučiće
/sfx	skeniraj samoraspakirajuće arhive (standardno)
/no-sfx	ne skeniraj samoraspakirajuće arhive
/rtp	skeniraj runtime arhivatore (standardno)
/no-rtp	ne skeniraj runtime arhivatore
/unsafe	skeniraj potencijalno nesigurne aplikacije
/no-unsafe	ne skeniraj potencijalno nesigurne aplikacije (standardno)
/unwanted	skeniraj potencijalno neželjene aplikacije
/no-unwanted	ne skeniraj potencijalno neželjene aplikacije (standardno)
/suspicious	skeniraj sumnjive aplikacije (standardno)
/no-suspicious	ne skeniraj sumnjive aplikacije
/pattern	koristi potpise (standardno)
/no-pattern	ne koristi potpise
/heur	aktiviraj heuristiku (standardno)
/no-heur	deaktiviraj heuristiku
/adv-heur	aktiviraj naprednu heuristiku (standardno)
/no-adv-heur	deaktiviraj naprednu heuristiku
/ext-exclude=EKSTENZIJE	izuzmi iz skeniranja EKSTENZIJE datoteka razgraničene dvotočkom
/clean-mode=NAČIN	koristi NAČIN čišćenja za zaražene objekte Dostupne su sljedeće opcije: • `none` (standardno) – Automatsko čišćenje neće se izvršiti. • `standard` – ecls.exe automatski će pokušati očistiti ili izbrisati zaražene datoteke. • `strict (strogo)` – ecls.exe automatski će pokušati očistiti ili izbrisati zaražene datoteke bez intervencije korisnika (neće se prikazati odzivnik prije brisanja datoteka). • `rigorozno` – ecls.exe izbrisat će datoteke bez pokušaja čišćenja, neovisno o tome o kakvim se datotekama radi. • `delete (brisanje)` – ecls.exe će izbrisati datoteke bez pokušaja čišćenja, ali neće izbrisati osjetljive datoteke poput onih sustava Windows.
/quarantine	kopiraj zaražene datoteke (ako su očišćene) u karantenu (dopunjuje akciju koja se izvršava prilikom čišćenja)
/no-quarantine	ne kopiraj zaražene datoteke u karantenu

Općenite mogućnosti:

/help	prikaži pomoć i izađi
/version	prikaži informacije o verziji i izađi
/preserve-time	sačuvaj vremensku oznaku zadnjeg pristupa

Izlazni kodovi

0	nisu pronađene prijetnje
1	prijetnje su pronađene i očišćene
10	neke datoteke nisu se mogle skenirati (mogu biti prijetnje)
50	pronađena je prijetnja
100	pogreška

Izlazni kodovi veći od 100 znače da datoteka nije skenirana pa bi stoga mogla biti zaražena.

Najčešća pitanja

Ovo poglavlje bavi se najčešćim pitanjima i problemima s kojima se možete susresti. Kliknite naslov teme da biste saznali rješenje problema:

- Aktualizacija programa ESET Endpoint Antivirus
- Aktivacija programa ESET Endpoint Antivirus
- ESET Endpoint Antivirus je otkrio prijetnju
- Uklanjanje virusa s računala
- Stvaranje novog zadatka u Planeru
- Zakazivanje tjednog skeniranja računala
- Upravljanje obavijestima i interaktivnim upozorenjima
- Povezivanje proizvoda s programom ESET PROTECT
  –Korištenje načina nadjačavanja
  –Primjena preporučenog pravila za program ESET Endpoint Antivirus
- Konfiguriranje mirrora
- Kako nadograditi na Windows 10 s proizvodom ESET Endpoint Antivirus
- Kako aktivirati daljinsko praćenje i upravljanje
- Kako blokirati preuzimanje specifičnih vrsti datoteka s interneta
- Kako minimizirati korisničko sučelje programa ESET Endpoint Antivirus

Ako vaš problem nije naveden na gornjim stranicama pomoći, pokušajte tražiti ključnu riječ ili pojam koji opisuje vaš problem te pretražite stranice pomoći za program ESET Endpoint Antivirus.

Ako ne pronađete rješenje za svoj problem/odgovor na pitanje na stranicama pomoći, posjetite ESET-ovu bazu znanja u kojoj su dostupni odgovori na najčešća pitanja i rješenja za najčešće probleme.

- Kako deinstalirati ESET Endpoint Antivirus
- Najbolje prakse za zaštitu od zlonamjernog programa poznatog kao filecoder (ransomware)
- Najčešća pitanja za ESET Endpoint Security i ESET Endpoint Antivirus
- Koje adrese i portovi moraju biti otvoreni u firewallu treće strane da bi proizvod tvrtke ESET bio u potpunosti funkcionalan?

Ako želite, svoje pitanje ili problem možete uputiti našoj korisničkoj službi. Veza na web obrazac za kontakt nalazi se u oknu **Pomoć i podrška** u glavnom programskom prozoru.

Najčešća pitanja o automatskim nadogradnjama

Dodatne informacije o nadogradnji programa ESET Endpoint Antivirus pročitajte u sljedećem članku u ESET-ovoj bazi znanja.
- Koje su različite vrste nadogradnji i izdanja programa tvrtke ESET?

Hoće li se računala automatski nadograditi? Preuzima li se nadogradnja prije ili nakon restarta?

Preuzimanje se događa prije restarta i nadograđene datoteke se isto tako pripremaju u ovoj fazi. Nakon restarta nadograđene datoteke i dalje su pripremljene samo za upotrebu, a trenutačno instalirana verzija pruža neprekidnu zaštitu. Promjene se primjenjuju nakon sljedećeg pokretanja ESET Endpoint Antivirus.

Imam oko 3000 računala. Hoće li sva računala istovremeno preuzeti nadogradnje? Mogu li upotrijebiti proxy za automatske nadogradnje za toliko računala?

ESET nudi mirror alat i proxy rješenja za veće mreže, tako da se nadogradnje preuzimaju samo jednom s interneta, a zatim distribuiraju lokalno. Nadogradnje su manje, obično od 5 do 10 MB, i ESET će ograničiti nadogradnje tijekom prvih nekoliko tjedana dostupnosti. Stoga neće svi klijenti pokrenuti preuzimanje istovremeno kada se povežu izravno s ESET-ovim serverima.

Mogu li odlučiti koliko će se računala ili koja će se računala automatski nadograditi? Ne želim preuzimati nadogradnju za više od deset računala na sat ili trenutačno želim nadograditi samo deset računala i još jedno računalo nakon nekoliko dana.

Upravljana okruženja imaju pravilo automatske nadogradnje u kojem možete odrediti željenu najnoviju verziju. Podržani su i zamjenski znakovi (na primjer, 9.0.2032.*). Za više informacija pogledajte poglavlje Automatske nadogradnje u mrežnoj pomoći na internetu ESET PROTECT ili ESET PROTECT Cloud. Nažalost, trenutačno nisu dostupne druge opcije za ograničavanje automatske nadogradnje. Možete dodijeliti više pravila za više grupa.

Konfiguriraju li se automatske nadogradnje samo putem pravila? Mogu li deaktivirati pravilo ako ne želim nadogradnju ESET-ovog programa?

Ako postoji hitni popravak sigurnosti i stabilnosti za krajnju točku ESET-ovog programa, program će se nadograditi čak i kada su automatske nadogradnje deaktivirane prema uvjetima navedenima u primjenjivom Licenčnom ugovoru za krajnjeg korisnika. ESET upotrebljava hitne popravke sigurnosti i stabilnosti za rješavanje ključnih problema i osiguranje maksimalne sigurnosti i stabilnosti vašeg ESET-ovog programa.

Pravilo automatske nadogradnje možete dodijeliti bilo kojoj skupini krajnjih točaka, bez obzira na njihovu trenutačnu konfiguraciju automatske nadogradnje. U okruženjima kojima se ne upravlja korisnik može lokalno

konfigurirati automatsku nadogradnju na zaslonu Napredno podešavanje krajnje točke ESET-ovog programa.

Što ako konfiguriram pravilo za upotrebu najstarije dostupne verzije? Hoće li ESET čak i tada nadograditi moje programe?

Hitni popravci i kritični hitni popravci (nadogradnje sigurnosti i stabilnosti) su dvije različite kategorije nadogradnje. Redoviti hitni popravci dodjeljuju se automatskim nadogradnjama sa standardnim prioritetom kada su korisničke postavke prihvaćene. Kritični hitni popravci su glavni prioritet, bez obzira na korisničke postavke.

Kako će nadogradnje funkcionirati u izvanmrežnim scenarijima? Kada korisnici upotrebljavaju izvanmrežni repozitorij?

Izvanmrežni repozitorij sadržava još i .dup i .fup datoteke. Odjeljak repozitorija mora se preuzeti pomoću mirror alata, a ne nadogradnjom modula. Dodatne informacije potražite u temi Izvanmrežni repozitorij u pomoći na mreži za ESET PROTECT.

Kako ESET-ovi programi znaju da je nadogradnja potrebna? Iz repozitorija? Šalju li se podaci serverima? Ako ESET planira izvršiti nadogradnju mjesec dana nakon objave verzije, mogu li ESET-ovi serveri podnijeti globalnu objavu?

ESET-ovi programi preuzimaju automatske nadogradnje iz repozitorija. Serveri su spremni za to jer kritične nadogradnje iznose svega nekoliko kilobajta. ESET neće ograničavati kritične nadogradnje na serverima repozitorija. Međutim, postoji opcija ograničavanja nadogradnji servera ako su automatske nadogradnje veće. U tablici u nastavku se nalaze primjeri veličina hitnih popravaka u slučaju diferencijalne automatske nadogradnje:

Prethodna verzija	Nova verzija	Veličina
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

Ako diferencijalna automatska nadogradnja iz nekog razloga ne uspije, vaš ESET-ov program može pokrenuti potpunu nadogradnju. To je još uvijek automatska nadogradnja s jamstvom funkcionalnosti, ali umjesto .dup datoteke će se preuzeti .fup datoteka. Za verziju 9.0.2032.2 to iznosi 27 MB. Međutim, takav scenarij je rijedak.

Hoće li se nadogradnja programa ESET Endpoint Antivirus objaviti s ograničavanjem? Ako da, koliko dugo će nadogradnja biti ograničavana nakon objave?

ESET ograničava nadogradnje prvih nekoliko tjedana nakon objave nove verzije kako bi smanjio opterećenje servera i ravnomjerno distribuirao novu verziju.

Automatska nadogradnja će postati jedan od primarnih načina nadogradnje. Kako to funkcionira detaljno?

ESET-ovo je nastojanje da što više kupaca upotrebljava nadogradnju automatskom nadogradnjom. Teško je podržavati toliko starih verzija. Funkcija automatske nadogradnje funkcionira na jednostavan način – .dup datoteke se preuzimaju tijekom prve provjere nadogradnje modula. Tijekom postupka nadogradnje program je potpuno funkcionalan i štiti računalo. Nova verzija se aktivira nakon restarta. U sustavu ESET PROTECT (na strani servera) možete upotrijebiti pravilo kako biste odredili najnoviju verziju na koju želite nadograditi ili možete upotrijebiti zamjenske znakove. Za više informacija pogledajte poglavlje Automatske nadogradnje u mrežnoj pomoći na internetu ESET PROTECT ili ESET PROTECT Cloud.

Je li točno da automatska nadogradnja radi za 1/10? Sada upotrebljavam ESET Endpoint Security 8.0.2028.1. Ako se pokrenu automatske nadogradnje, na koju će se verziju nadograditi?

Nadogradnja programa pomoću automatske nadogradnje može se odgoditi zbog ograničavanja na repozitorijskim serverima. Ako se nadogradnja programa objavi s ograničavanjem, automatske provjere nadogradnje možda je neće odmah primiti. Ako se nadogradnja smatra sigurnom i stabilnom, ograničavanje se može smanjiti ili potpuno ukloniti kako bi svi preostali klijenti primili nadogradnju.

Postupak ograničavanja može trajati različitu količinu vremena za svaku nadogradnju. Razlikuje se ovisno o tome koliko klijenata zatraži nadogradnju, koliki je promet na našim serverima i drugim čimbenicima. Ovaj se postupak uvijek razvija i stalno se mijenja.

Kada će automatska nadogradnja započeti ako pokrenem računalo u 8.45 h i isključim ga u 17.00 h?

Pri sljedećoj uspješno zakazanoj nadogradnji modula, najviše jednom svaka 24 sata.

Kada će se nadogradnja pokrenuti sljedeći put ako se računalo isključi dok se provodi automatska nadogradnja?

Nadogradnja će se pokrenuti tijekom pojave okvira sljedeće zakazane nadogradnje. Za postupak automatske nadogradnje (ranije uPCU) postoji robusni mehanizam zakazivanja (eng. „fail-safe”). Nakon preuzimanja nadogradnje i restarta računala, nadograđene datoteke i dalje su pripremljene samo za upotrebu, a trenutačno instalirana verzija pruža neprekidnu zaštitu. Promjene se primjenjuju nakon sljedećeg pokretanja krajnje točke ESET-ovog programa.

Kako mogu odmah pokrenuti automatsku nadogradnju bez čekanja na redovitu vezu u 24 sata? Postoji li neki drugi način da kliknem Provjeri dostupnost nadogradnji?

Postupak automatske nadogradnje možete pokrenuti ručno samo kada otvorite prozor glavnog programa i kliknete **Nadogradi** > **Provjeri dostupnost nadogradnji**. Svi ostali načini pokretanja nadogradnje modula poštuju pravilo Planera automatske nadogradnje svaka 24 sata. Preuzimanje automatske nadogradnje ne možete pokrenuti automatski u bilo kojem trenutku. Ovu funkciju ćemo dodati u budućnosti.

Kako nadograditi program ESET Endpoint Antivirus

Program ESET Endpoint Antivirus može se nadograditi ručno ili automatski. Da biste pokrenuli nadogradnju, kliknite **Nadogradi** u glavnom prozoru programa i zatim kliknite **Potraži nadogradnje**.

Standardnom se instalacijom stvara automatski zadatak nadogradnje koji se izvršava svakog sata. Ako želite promijeniti interval, idite na stavku **Alati** > Planer.

Uklanjanje virusa s računala

Ako računalo pokazuje simptome zaraze zlonamjernim softverom, npr. sporije radi ili se često "zamrzava", preporučujemo sljedeće:

1. U glavnom prozoru programa kliknite **Skeniranje računala**.
2. Kliknite **Smart skeniranje** da biste pokrenuli skeniranje sustava.
3. Nakon završetka skeniranja u dnevniku pogledajte koliko je skeniranih, zaraženih i očišćenih datoteka.
4. Ako želite skenirati samo određeni dio diska, odaberite **Prilagođeno skeniranje** te zatim ciljeve u kojima će se tražiti virusi.

Dodatne informacije možete pronaći u ovom redovito ažuriranom članku ESET-ove baze znanja.

Stvaranje novog zadatka u Planeru

Da biste stvorili novi zadatak u odjeljku **Alati** > **Planer**, kliknite **Dodaj zadatak** ili kliknite desnom tipkom miša i odaberite **Dodaj** na kontekstnom izborniku. Na raspolaganju je sedam vrsta planiranih zadataka:

- **Pokreni vanjsku aplikaciju** – Zakazuje pokretanje vanjske aplikacije.
- **Održavanje dnevnika** – Dnevnici sadrže i zaostatke već izbrisanih zapisa. Taj zadatak redovito optimizira zapise u dnevnicima radi učinkovitijeg rada.
- **Provjera datoteke za pokretanje sustava** – Provjerava datoteke kojima je dopušteno pokretanje prilikom pokretanja sustava ili prijave.
- **Stvori snimku statusa računala** – Stvara snimku računala pomoću programa ESET SysInspector – prikuplja detaljne informacije o komponentama sustava (primjerice upravljačkim programima, aplikacijama) i procjenjuje razinu rizika za svaku komponentu.
- **Skeniranje računala na zahtjev** – Izvodi skeniranje datoteka i mapa na računalu.
- **Aktualizacija** – Planira zadatak aktualizacije aktualizacijom modula.

Budući da je **Aktualizacija** jedan od najčešće korištenih planiranih zadataka, u nastavku slijedi objašnjenje kako dodati novi zadatak aktualizacije:

S padajućeg izbornika **Planirani zadatak** odaberite **Aktualizacija**. Unesite naziv zadatka u polje **Naziv zadatka** i kliknite **Dalje**. Odaberite učestalost zadatka. Dostupne su sljedeće opcije: **Jednom**, **Opetovano**, **Svakodnevno**, **Tjedno** i **Pri događaju. Odaberite mogućnost Nemoj izvršavati zadatak ako računalo koristi bateriju** da biste minimizirali korištenje sistemskih resursa dok prijenosno računalo koristi bateriju. Zadatak će se izvršiti na datum i vrijeme zadani u poljima **Izvršavanje zadatka**. Zatim definirajte akciju koju treba poduzeti ako se zadatak ne može izvršiti ili dovršiti u zakazano vrijeme. Na raspolaganju su sljedeće mogućnosti:

- **U sljedećem zakazanom terminu**

- **Što prije**
- **Odmah, ako vrijeme proteklo od zadnjeg izvršavanja premašuje određenu vrijednost** (interval se može definirati putem okvira za listanje **Vrijeme od zadnjeg izvršavanja**).

U sljedećem koraku prikazuje se prozor sažetaka informacija o trenutno planiranom zadatku. Kliknite **Završetak** kada završite s unošenjem promjena.

Pojavit će se dijaloški okvir gdje korisnik može izabrati profile koji će se koristiti za planirani zadatak. Tu možete postaviti primarni i alternativni profil. Alternativni profil koristi se u slučaju da zadatak nije moguće dovršiti pomoću primarnog profila. Potvrdite klikom na **Završetak** , čime se novi planirani zadatak dodaje na popis trenutno planiranih zadataka.

Zakazivanje tjednog skeniranja računala

Da biste zakazali redoviti zadatak, otvorite glavni prozor programa > **Alati** > **Planer**. U nastavku se nalaze kratke upute o zakazivanju zadatka koji će skenirati lokalne pogone svakog tjedna. Dodatne upute potražite u našem članku iz baze znanja.

Da biste zakazali zadatak skeniranja:

1. Na glavnom zaslonu Planera kliknite **Dodaj zadatak**.
2. S padajućeg izbornika odaberite **Skeniranje računala na zahtjev**.
3. Upišite naziv zadatka pa odaberite mogućnost **Tjedno za učestalost zadatka**.
4. Odaberite vrijeme i dan za izvršenje zadatka.
5. Odaberite **Izvrši zadatak čim to bude moguće** za kasnije izvršenje zadatka u slučaju da se zakazani zadatak iz nekog razloga ne izvrši (primjerice, računalo je bilo isključeno).
6. Pregledajte sažetak planiranog zadatka pa kliknite **Završetak**.
7. S padajućeg izbornika **Ciljevi** odaberite **Lokalni pogoni**.
8. Kliknite **Završetak** da biste primijenili zadatak.

Povezivanje programa ESET Endpoint Antivirus s alatom ESET PROTECT

Ako je na računalu instaliran program ESET Endpoint Antivirus i želite se povezati putem programa ESET PROTECT, provjerite je li i na klijentskoj radnoj stanici instaliran ESET Management Agent. To je ključan dio svakog klijentskog rješenja koje komunicira s ESET PROTECT serverom.

- Instalirajte ESET Management Agent na klijentske radne stanice

Pogledajte i:

- Dokumentacija za daljinski upravljane krajnje točke
- Korištenje načina nadjačavanja
- Primjena preporučenog pravila za program ESET Endpoint Antivirus

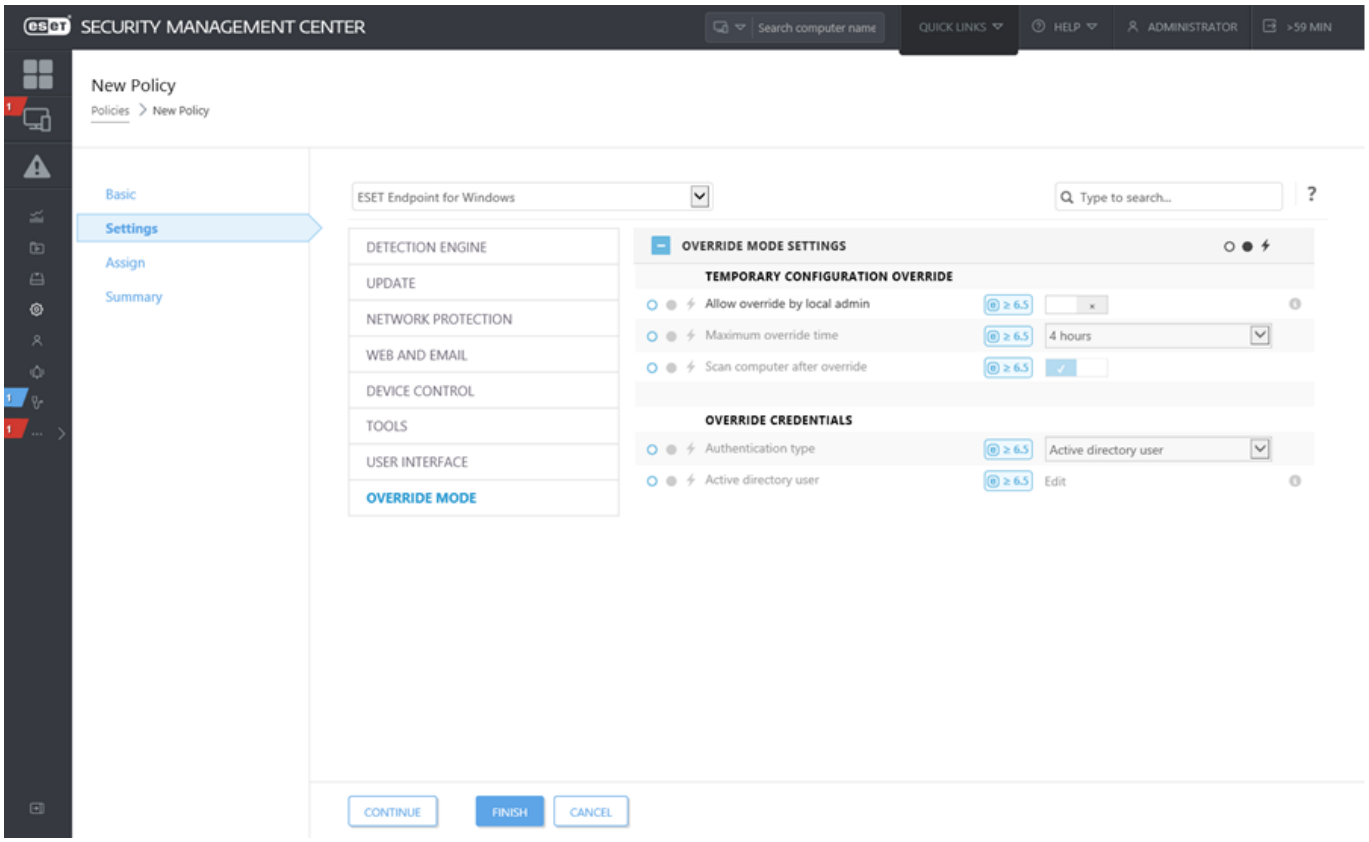
Korištenje načina nadjačavanja

Korisnici koji na uređaju imaju ESET-ove Endpoint programe (verzija 6.5 i novije) za Windows mogu se koristiti funkcijom nadjačavanja. Način nadjačavanja omogućuje korisnicima na razini klijentskog računala da promijene postavke instaliranog ESET-ovog programa, čak i ako se na te postavke primjenjuje pravilo. Način nadjačavanja može se aktivirati za određene AD korisnike ili može biti zaštićen lozinkom. Funkcija ne može biti aktivirana dulje od četiri uzastopna sata.

Kad je aktiviran način nadjačavanja, ne može se zaustaviti iz ESET PROTECT web konzole. Način nadjačavanja deaktivirat će se automatski nakon isteka razdoblja nadjačavanja. Moguće ga je isključiti i na klijentskom računalu.
Korisnik koji upotrebljava način nadjačavanja također mora imati administratorska prava za Windows. U suprotnome korisnik ne može spremiti promjene u postavkama programa ESET Endpoint Antivirus.
Podržana je grupna autentikacija servisa Active Directory.

Da biste postavili **način nadjačavanja**:

1. Idite na **Pravila** > **Novo pravilo**.
2. U odjeljku **Osnovno** upišite **naziv** i **opis** pravila.
3. U odjeljku **Postavke** odaberite **ESET Endpoint za Windows**.
4. Kliknite na opciju **Način nadjačavanja** i konfigurirajte pravila za način nadjačavanja.
5. U odjeljku **Dodijeli** odaberite računalo ili skupinu računala na koja će se pravilo primjenjivati.
6. Pregledajte postavke u odjeljku **Sažetak** i kliknite **Završi** da biste primijenili pravilo.



Ako *John* ima problem jer mu sigurnosne postavke blokiraju neku važnu funkciju ili pristup webu na njegovom uređaju, administrator može omogućiti korisniku *John* da nadjača postojeće sigurnosno pravilo i ručno podesi postavke na svom uređaju. ESET PROTECT nakon toga može zatražiti te nove postavke da bi administrator mogao iz njih stvoriti novo pravilo.
Da biste to učinili, slijedite ove korake:
1. Idite na **Pravila** > **Novo pravilo**.
2. Ispunite polja **Naziv** i **Opis**. U odjeljku **Postavke** odaberite **ESET Endpoint za Windows**.
3. Kliknite **Način nadjačavanja**, aktivirajte ga na sat vremena i odaberite stavku *John* kao AD korisnika.
4. Dodijelite pravilo *Johnovom računalu* i kliknite **Završi** da biste spremili pravilo.
5. *John* mora aktivirati **način nadjačavanja** u ESET-ovom sigurnosnom programu i ručno promijeniti postavke na svom uređaju.
6. Na ESET PROTECT web-konzoli idite do opcije **Računala**, odaberite *Johnovo računalo* i kliknite **Prikaži detalje**.
7. U odjeljku **Konfiguracija** kliknite **Zatraži konfiguraciju** da biste zakazali zadatak klijenta i odmah dobili konfiguraciju od klijenta.
8. Ubrzo će se pojaviti nova konfiguracija. Kliknite na program čije postavke želite spremiti i potom kliknite **Otvori konfiguraciju**.
9. Možete pregledati postavke, a zatim kliknite **Pretvori u pravilo**.
10. Ispunite polja **Naziv** i **Opis**.
11. U odjeljku **Postavke** prema potrebi možete promijeniti postavke.
12. U odjeljku **Dodijeli** možete dodijeliti to pravilo *Johnovom računalu* (ili drugima).
13. Kliknite **Završi** da biste spremili postavke.
14. Nemojte zaboraviti ukloniti pravilo nadjačavanja kada više ne bude potrebno.

Primjena preporučenog pravila za program ESET Endpoint Antivirus

Nakon što povežete programe ESET Endpoint Antivirus i ESET PROTECT, najbolja je praksa primijeniti preporučeno ili prilagođeno pravilo.

Postoji nekoliko ugrađenih pravila za program ESET Endpoint Antivirus:

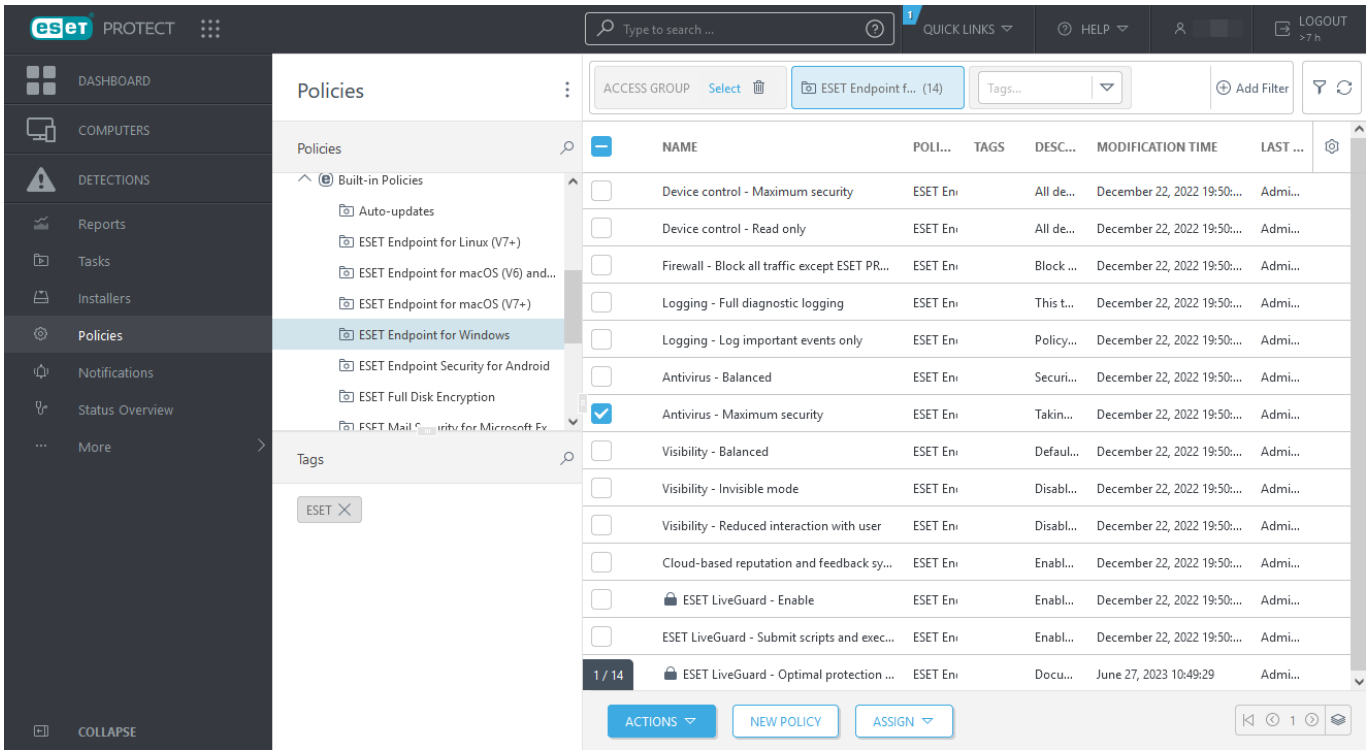
Pravilo	Opis
Antivirus – Uravnoteženo	Preporučena sigurnosna konfiguracija za većinu postavki.
Antivirus – maksimalna sigurnost	Iskorištava prednosti strojnog učenja, dubinskog pregleda ponašanja i filtriranja SSL protokola. Utječe na otkrivanje potencijalno nesigurnih, neželjenih i sumnjivih aplikacija.
Sustav reputacije i povratnih informacija na temelju cloud tehnologije	Aktivira sustav reputacije i povratnih informacija na temelju cloud tehnologije ESET LiveGrid® za poboljšanje otkrivanja najnovijih prijetnji te kao pomoć u dijeljenju zloćudnih ili nepoznatih potencijalnih prijetnji za daljnju analizu.
Kontrola uređaja – Maksimalna sigurnost	Svi su uređaji blokirani. Za povezivanje bilo kojeg uređaja potrebno je dopuštenje administratora.
Kontrola uređaja – samo za čitanje	Svi se uređaji mogu samo čitati. Zapisivanje nije dopušteno.
Firewall – Blokiraj sav promet osim veze s ESET PROTECT-om i ESET Inspect-om	Blokira sav promet osim veze s programom ESET PROTECT i serverom programa ESET Inspect Server (samo ESET Endpoint Security).

Pravilo	Opis
Vođenje dnevnika – Potpuno dijagnostičko zapisivanje	Ovaj predložak osigurava da će svi dnevnici biti dostupni administratoru kada mu budu potrebni. Zapisivat će sve uz minimalnu opširnost zapisivanja, uključujući HIPS i ThreatSense te firewall. Dnevnici se automatski brišu nakon 90 dana.
Vođenje dnevnika – Zapiši samo važne događaje	Ovo pravilo osigurava da će se zapisati upozorenja, pogreške i kritični događaji. Dnevnici se automatski brišu nakon 90 dana.
Vidljivost – Uravnoteženo	Standardna postavka za vidljivost. Aktivirani su statusi i obavijesti.
Vidljivost – Nevidljivi način	Deaktivirane su obavijesti, upozorenja, GUI i integracija u kontekstni izbornik. Datoteka egui.exe neće se pokrenuti. Prikladno za upravljanje isključivo s ESET PROTECT Cloud-e.
Vidljivost – Smanjena interakcija s korisnikom	Deaktivirani su statusi i obavijesti, GUI se prikazuje.

Slijedite korake u nastavku da biste postavili pravilo s nazivom **Antivirus – maksimalna sigurnost**, koje provodi više od 50 preporučenih postavki za program ESET Endpoint Antivirus instaliran na vašim radnim stanicama:

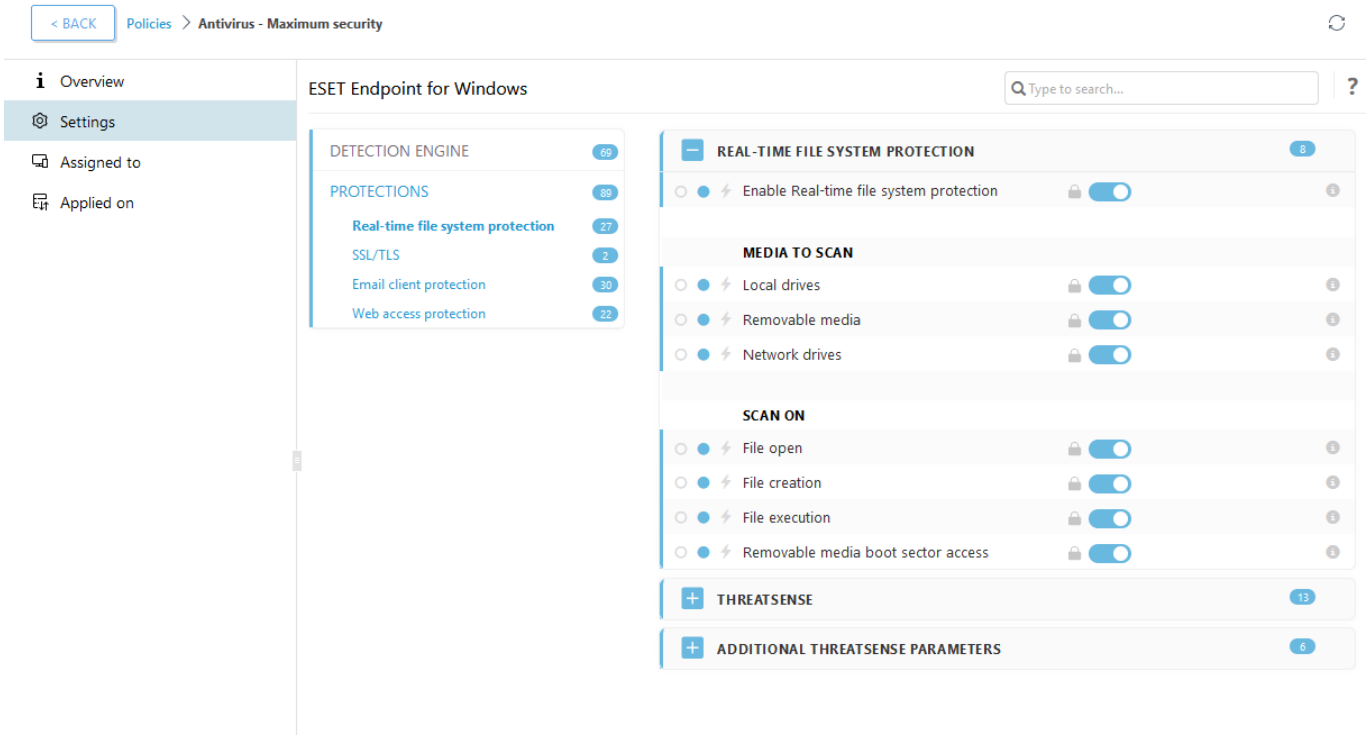
> Sljedeći članci iz ESET-ove baze znanja možda će biti dostupni samo na engleskom jeziku:
> Upotrijebite ESET PROTECT za primjenu preporučenog ili unaprijed definiranog pravila za program ESET Endpoint Antivirus

1. Otvorite ESET PROTECT web konzolu.
2. Idite na **Pravila** i proširite stavku **Ugrađena pravila** > **ESET Endpoint za Windows**.
3. Kliknite **Antivirus – maksimalna sigurnost – preporučeno**.
4. Na kartici **Dodijeljeno** kliknite **Dodijeli klijente** ili **Dodijeli grupe** i odaberite odgovarajuća računala za koje želite primijeniti ovo pravilo.



Da biste vidjeli koje su postavke primijenjene za ovo pravilo, kliknite karticu **Postavke** i proširite stablo odjeljka Napredno podešavanje.

- Plava točka označava izmijenjenu postavku za ovo pravilo
- Broj u plavom okviru označava broj postavki koje je ovo pravilo promijenilo
- Možete pročitati više o ESET PROTECT pravilima



Konfiguriranje mirrora

ESET Endpoint Antivirus može se konfigurirati da sprema kopije datoteka za nadogradnju modula detekcije i distribuira nadogradnje na druge radne stanice na kojima se koristi ESET Endpoint Antivirus ili ESET Endpoint Security.

Mirror za nadogradnju stvara kopije datoteka za nadogradnju koje se mogu koristiti za nadogradnju radnih stanica na kojima se koristi ista generacija programa ESET Endpoint Antivirus za Windows. (Primjerice, ESET Endpoint Antivirus za Windows verzije 10.x stvara datoteke za nadogradnju samo za verziju 10.x programa ESET Endpoint Antivirus za Windows i ESET Endpoint Security za Windows)

Konfiguriranje programa ESET Endpoint Antivirus kao mirror servera za aktualizacije putem internog HTTP servera

1. Pritisnite **F5** da biste pristupili Naprednom podešavanju i proširite stavku **Nadogradnja** > **Profili** > **Mirror za nadogradnju**.
2. Proširite **Nadogradnje** i provjerite je li aktivirana opcija **Odaberi automatski** pod stavkom **Nadogradnje modula**.
3. Proširite **Mirror za nadogradnju** i aktivirajte stavke **Stvori mirror za nadogradnju** i **Aktiviraj HTTP server**.

Za više informacija pogledajte:
- Aktualizacijski mirror
- Aktualizacija s mirrora

Konfiguriranje mirror poslužitelja za aktualizacije putem zajedničke mrežne mape

1. Stvorite zajedničku mapu na lokalnom ili mrežnom uređaju. Mapa mora biti dostupna za čitanje svim korisnicima koji upotrebljavaju sigurnosna rješenja tvrtke ESET i slobodna za pisanje s lokalnog SISTEMSKOG računa.
2. Aktivirajte **Stvori mirror za nadogradnju** pod stavkom **Napredno podešavanje** > **Nadogradnja** > **Profili** > **Mirror za nadogradnju**.
3. Odaberite odgovarajuću **mapu za pohranu** tako da kliknete **Očisti** i zatim **Uredi**. Potražite i odaberite stvorenu zajedničku mapu.

Ako ne želite pružati nadogradnje modula putem internog HTTP servera, deaktivirajte opciju **Aktiviraj HTTP server**.

Kako nadograditi na Windows 10 s proizvodom ESET Endpoint Antivirus

Toplo preporučujemo da nadogradite svoj ESET-ov program na posljednju verziju, a zatim preuzmete najnovije aktualizacije modula prije nadogradnje na Windows 10. To će osigurati maksimalnu zaštitu i sačuvati vaše programske postavke i licenčne informacije tijekom nadogradnje na Windows 10.

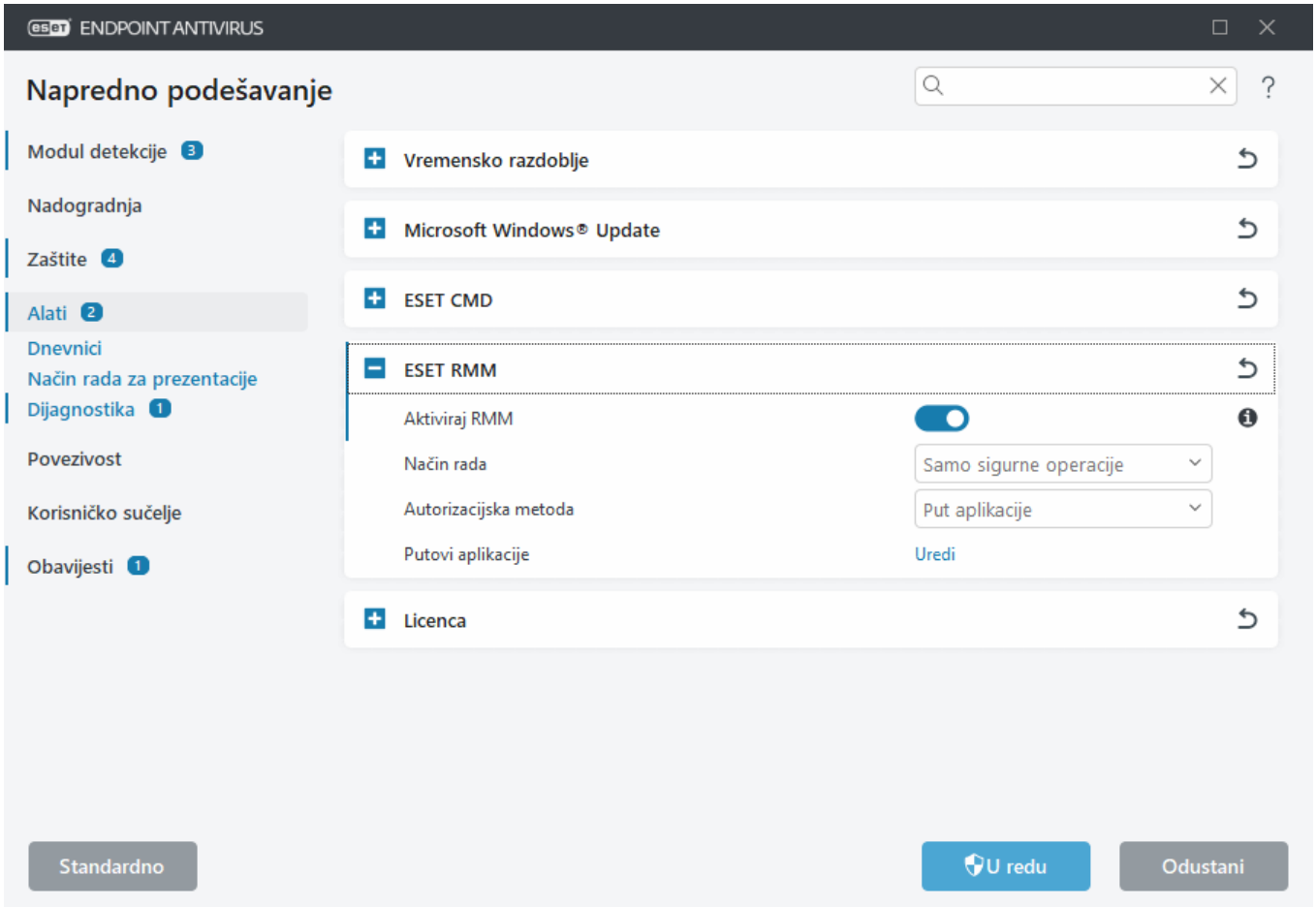
Verzije na drugim jezicima:

Ako tražite verziju ESET-ova endpoint proizvoda na nekom drugom jeziku, posjetite našu stranicu za preuzimanje.

Dodatne informacije o kompatibilnosti ESET-ovih poslovnih programa sa sustavom Windows 10.

Kako aktivirati daljinsko praćenje i upravljanje

Daljinsko praćenje i upravljanje (RMM) proces je nadgledanja i kontrole softverskih sustava (poput onih na radnoj površini, serverima i mobilnim uređajima) koji upotrebljava lokalno instaliran agent kojemu može pristupiti davatelj usluga upravljanja. RMM može upravljati programom ESET Endpoint Antivirus od verzije 6.6.2028.0.



ESET RMM standardno je deaktiviran. Da biste aktivirali ESET RMM, otvorite Napredno podešavanje > **Alati** > **ESET RMM** i aktivirajte klizač pored opcije **Aktiviraj RMM**.

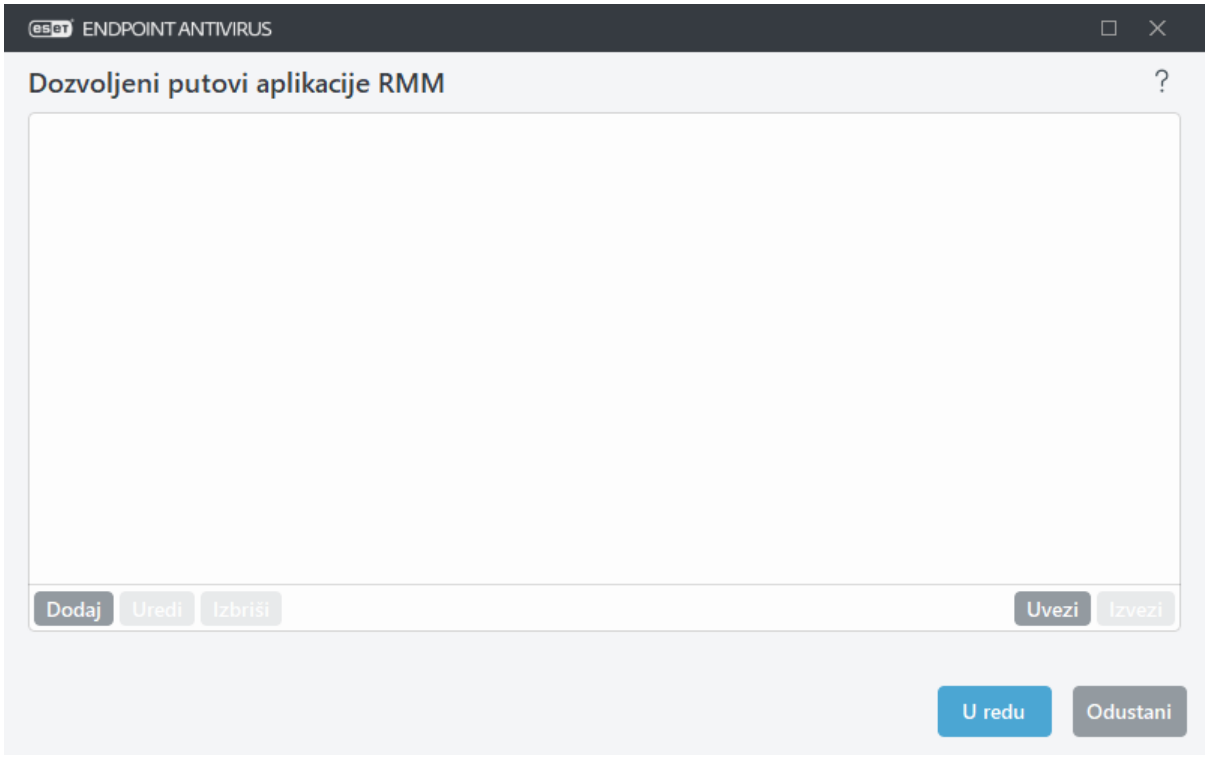
Radni način – odaberite **Samo sigurne operacije** ako želite aktivirati sučelje RMM za sigurne operacije i operacije samo za čitanje. Odaberite **Sve operacije** ako želite aktivirati sučelje RMM za sve operacije.

Operacija	Način samo sigurnih operacija	Način svih operacija
Nabavi aplikaciju-informacije	✔	✔
Nabavi konfiguraciju	✔	✔
Nabavi podatke o licenci	✔	✔
Nabavi dnevnike	✔	✔
Nabavi status zaštite	✔	✔
Nabavi status nadogradnje	✔	✔
Postavi konfiguraciju		✔
Pokreni aktivaciju		✔
Pokreni skeniranje	✔	✔
Pokreni nadogradnju	✔	✔

Način autorizacije – Postavite način autorizacije RMM-a. Za upotrebu autorizacije odaberite **Put aplikacije** iz padajućeg izbornika, u suprotnome odaberite **Ništa**.

RMM uvijek treba upotrebljavati autorizaciju kako zlonamjerni softver ne bi mogao deaktivirati ili zaobići zaštitu programom ESET Endpoint.

Putovi aplikacije – određena aplikacija koja smije pokrenuti RMM. Ako ste odabrali **Put aplikacije** kao način autorizacije, kliknite **Uredi** da biste otvorili konfiguracijski prozor **Dopušteni putovi aplikacije RMM**.



Dodaj – Stvorite novi dopušteni put aplikacije RMM. Unesite put ili kliknite gumb **...** za odabir izvršne datoteke.

Uredi – Preinačite postojeći dopušteni put. Koristite **Uredi** ako se lokacija izvršne datoteke promijenila u drugu mapu.

Izbriši – Izbrišite postojeći dopušteni put.

Standardna instalacija programa ESET Endpoint Antivirus sadrži datoteku ermm.exe koja se nalazi u direktoriju Endpoint aplikacije (standardni put *C:\Program Files\ESET\ESET Security*). ermm.exe razmjenjuje podatke s dodatkom RMM, koji komunicira s RMM agentom, povezanim s RMM serverom.

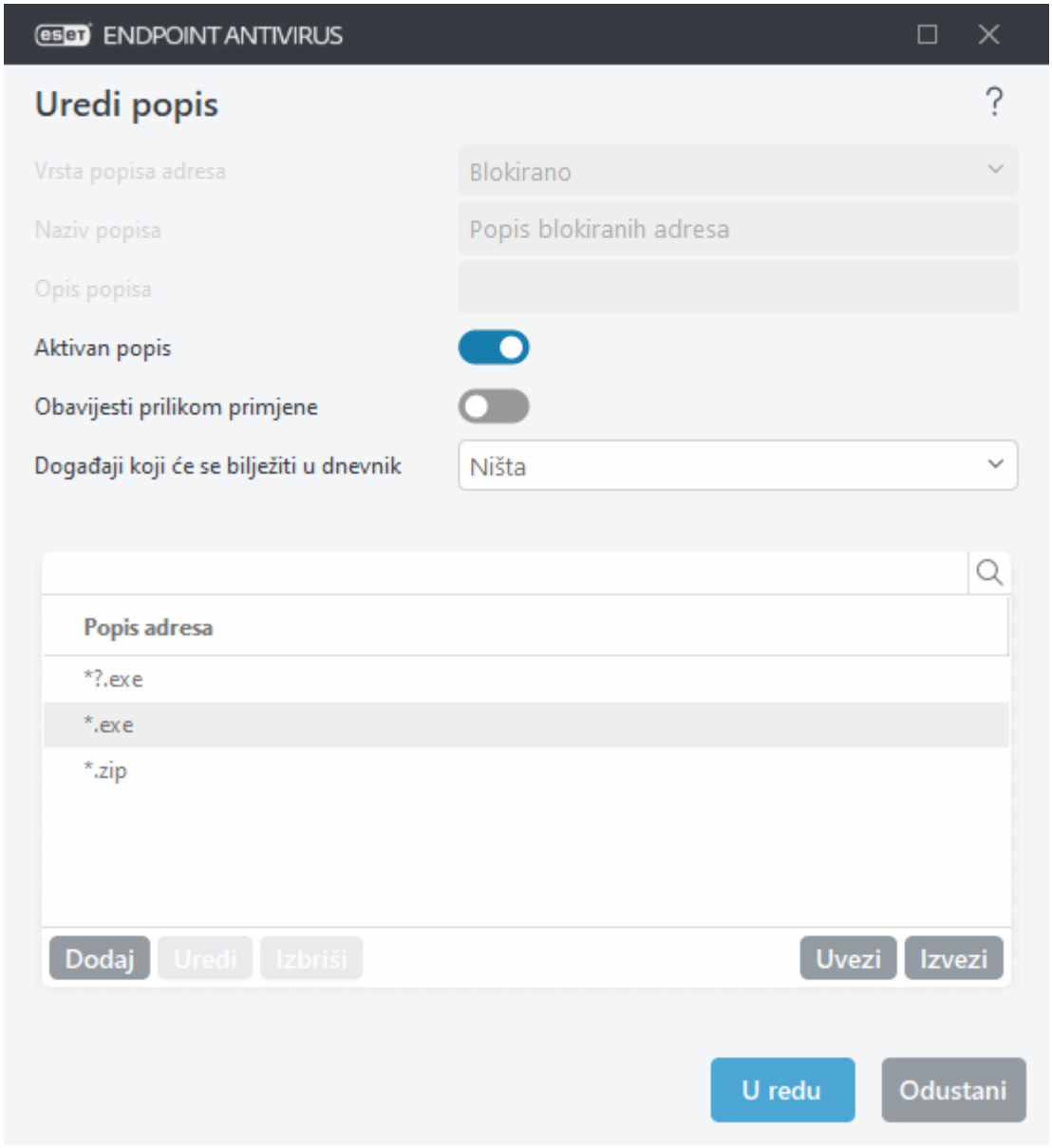
- ermm.exe – naredbeni redak za uslužni program koji je razvio ESET, a koji omogućuje upravljanje Endpoint programima i komunikaciju s bilo kojim RMM dodatkom.
- RMM dodatak jest aplikacija treće strane koja je pokrenuta lokalno na sustavu Endpoint Windows. Dodatak je dizajniran kako bi komunicirao s određenim RMM agentom (npr. samo Kaseya) i s ermm.exe.
- RMM agent aplikacija je treće strane (npr. od Kaseye) koja je pokrenuta lokalno na sustavu Endpoint Windows. Agent komunicira s RMM dodatkom i RMM serverom.

Kako blokirati preuzimanje specifičnih vrsti datoteka s interneta

Ako ne želite dopustiti preuzimanje određenih vrsta datoteka (npr. exe, pdf ili zip) s interneta, upotrijebite Upravljanje URL adresama s kombinacijom zamjenskih znakova. Pritisnite tipku F5 da biste pristupili odjeljku **Napredno podešavanje**. Kliknite "**Web i e-pošta**" > "**Zaštita web pristupa**" i proširite odjeljak **Upravljanje URL adresama**. Kliknite "**Uredi**" pored stavke "**Popis adresa**".

U prozoru **Popis adresa** odaberite **Popis blokiranih adresa** i kliknite **Uredi** ili **Dodaj** kako biste stvorili/uredili popis. Otvorit će se novi prozor. Ako stvarate novi popis, odaberite **"Blokirano**" u padajućem izborniku **"Vrsta popisa adresa**" i navedite naziv popisa. Ako želite primiti obavijest prilikom pristupa nekoj vrsti datoteke s trenutačnog popisa, omogućite traku klizača **"Obavijesti" prilikom primjene**. Odaberite **Opseg vođenja dnevnika** iz padajućeg izbornika. ESET PROTECT može prikupljati zapise s opsegom **upozorenja**.

Opseg vođenja dnevnika informacija i upozorenja dostupan je samo za pravila koja sadrže najmanje dvije komponente bez zamjenskih znakova unutar domene. Na primjer:
- *.domain.com/*
- *www.domain.com/*



Kliknite "**Dodaj**" da biste unijeli masku koja određuje vrste datoteka čije preuzimanje želite blokirati. Unesite potpunu URL adresu ako želite blokirati preuzimanje određene datoteke s određene web stranice, primjerice *http://example.com/file.exe*. Možete upotrijebiti zamjenske znakove da biste obuhvatili grupu datoteka. Upitnik (?) predstavlja jedan varijabilni znak, a zvjezdica (*) varijabilni znakovni niz od nula ili više znakova. Na primjer, maska **/*.zip* blokira preuzimanje svih komprimiranih zip datoteka.

Imajte na umu da pomoću ove metode možete blokirati preuzimanje određenih vrsta datoteka ako je ekstenzija datoteke dio URL-a datoteke. Ako web stranica upotrebljava URL-ove za preuzimanje datoteka, primjerice

www.example.com/download.php?fileid=42, preuzet će se bilo koja datoteka koja se nalazi na ovom linku, čak i ako ste blokirali njezinu ekstenziju.

Kako minimizirati korisničko sučelje programa ESET Endpoint Antivirus

Prilikom daljinskog upravljanja možete primijeniti unaprijed definirano pravilo "Vidljivost".

Ako to nije moguće, izvršite korake ručno.

1. Pritisnite **F5** da biste pristupili Naprednom podešavanju i proširite **Korisničko sučelje** > **Elementi korisničkog sučelja**.
2. Postavite opciju **Način rada za pokretanje** na željenu vrijednost. Više informacija o načinima rada za pokretanje.
3. Deaktivirajte opcije **Prikaži uvodni prozor pri pokretanju programa** i **Koristi zvučni signal**.
4. Konfigurirajte Obavijesti.
5. Konfigurirajte dio Statusi aplikacije.
6. Konfigurirajte dio Poruke za potvrdu.
7. Konfigurirajte dio Upozorenja i okviri s porukama.

Licenčni ugovor za krajnjeg korisnika

Stupa na snagu 19. listopada 2021..

VAŽNO: Prije preuzimanja, instaliranja, kopiranja ili korištenja pažljivo pročitajte uvjete i odredbe koje se primjenjuju na korištenje programa. **PREUZIMANJEM, INSTALIRANJEM, KOPIRANJEM ILI UPORABOM SOFTVERA PRIHVAĆATE OVE UVJETE I ODREDBE I POTVRĐUJETE PRAVILA PRIVATNOSTI.**

Licenčni ugovor za krajnjeg korisnika

Prema uvjetima ovog Licenčnog ugovora za krajnjeg korisnika („Ugovor”) sklopljenog između tvrtke ESET, spol. s r. o., sa sjedištem na adresi Einsteinova 24, 85101 Bratislava, Slovak Republic, registrirane u trgovačkom registru Okružnog suda u Bratislavi I, odjeljak Sro, unos br. 3586/B, registracijski broj tvrtke: 31333532 (dalje u tekstu: „ESET” ili „dobavljač”) i vas, fizičke ili pravne osobe („vi” ili „krajnji korisnik”), imate pravo na upotrebu softvera utvrđenog u članku 1. ovog Ugovora. Softver definiran u članku 1. ovog Ugovora može se pohraniti na nosaču podataka, poslati elektroničkom poštom, preuzeti s interneta, preuzeti s Dobavljačevih servera ili nabaviti iz nekih drugih izvora u skladu s uvjetima i odredbama navedenima u daljnjem tekstu.

OVO JE UGOVOR O PRAVIMA KRAJNJEG KORISNIKA, A NE UGOVOR O PRODAJI. Dobavljač ostaje vlasnikom kopije Softvera i fizičkog medija za pohranu koji se nalazi u prodajnom pakiranju te svih drugih kopija koje Krajnji korisnik ima pravo izraditi prema odredbama ovog Ugovora.

Klikom na gumb „Prihvaćam” ili „Prihvaćam...” tijekom instaliranja, preuzimanja, kopiranja ili upotrebe softvera izražavate suglasnost s uvjetima i odredbama ovog Ugovora i slažete se s Pravilima privatnosti. Ako se ne slažete s nekim od uvjeta ili nekom od odredbi Ugovora i/ili Pravila privatnosti, odmah kliknite na opciju za odustajanje, odustanite od instalacije ili preuzimanja odnosno uništite ili vratite softver, instalacijski medij, popratnu dokumentaciju i račun dobavljaču ili na lokaciju na kojoj ste nabavili softver.

SUGLASNI STE DA VAŠE KORIŠTENJE SOFTVERA ZNAČI DA STE PROČITALI OVAJ UGOVOR, DA GA RAZUMIJETE TE

DA STE SUGLASNI UVJETE I ODREDBE KOJE SADRŽI SMATRATI OBVEZUJUĆIMA.

1. **Softver.** Prema načinu na koji se upotrebljava u Ugovoru pojam „Softver" znači sljedeće: (i) računalni program koji se isporučuje s ovim Ugovorom i svi njegovi dijelovi; (ii) cjelokupan sadržaj diskova, CD-ROM-ova, DVD-ova, poruka e-pošte i svih privitaka ili ostalih medija uz koje je priložen ovaj Ugovor, uključujući oblik objektnog koda Softvera isporučenog na nosaču podataka, putem elektroničke pošte ili preuzimanjem putem interneta; (iii) svi povezani pisani materijali s objašnjenjima i sva moguća dokumentacija povezana sa Softverom, iznad svega, svi opisi Softvera, njegove specifikacije, svi opisi svojstava ili rada Softvera, svi opisi radnog okruženja u kojemu se Softver upotrebljava, upute za upotrebu ili instalaciju Softvera ili bilo kakav opis načina upotrebe Softvera („Dokumentacija"); (iv) kopije Softvera, eventualne popravke pogrešaka u Softveru, dodatke i proširenja Softvera, izmijenjene verzije Softvera, moguće nadogradnje komponenti Softvera za koje Vam Dobavljač daje licencu u skladu s člankom 3. ovog Ugovora. Softver se isporučuje isključivo u obliku izvršnog objektnog koda.

2. **Instalacija, Računalo i Licenčni ključ**. Softver isporučen na nosaču podataka, poslan elektroničkom poštom, preuzet s interneta, preuzet s Dobavljačevih servera ili nabavljen iz nekih drugih izvora potrebno je instalirati. Softver se mora instalirati na ispravno konfigurirano Računalo koje zadovoljava preduvjete navedene u Dokumentaciji. Način instalacije opisan je u Dokumentaciji. Na Računalu na kojem instalirate Softver ne smiju biti instalirani nikakvi računalni programi ni hardver koji bi mogli negativno utjecati na Softver. Računalo znači hardver, uključujući bez ograničenja osobna računala, prijenosna računala, radne stanice, dlanovnike, pametne telefone, ručne elektroničke uređaje ili druge elektroničke uređaje za koje je osmišljen Softver i na kojima će se instalirati i/ili upotrebljavati. Licenčni ključ znači jedinstveni niz simbola, slova, brojeva ili posebnih znakova pružen Krajnjem korisniku kako bi se dopustila zakonita upotreba Softvera, njegovih verzija ili produžetak trajanja Licence u skladu s ovim Ugovorom.

3. **Licenca**. Pod uvjetom da ste suglasni s uvjetima i odredbama ovog Ugovora i poštujete sve ugovorne uvjete i odredbe, Dobavljač Vam dodjeljuje sljedeća prava ("Licenca"):

a) **Instalacija i korištenje.** Dobavljač Vam daje neisključivo i neprenosivo pravo da instalirate Softver na tvrdi disk računala ili na neki drugi medij za trajnu pohranu podataka, da instalirate i pohranite Softver u memoriju računalnog sustava te da primjenjujete, pohranjujete i prikazujete Softver.

b) **Odredba o broju licenci.** Pravo na korištenje Softvera povezano je s brojem Krajnjih korisnika. Smatrat će se da jedan Krajnji korisnik označava: (i) instalaciju Softvera na jednom računalnom sustavu ili (ii) ako je opseg licence povezan s brojem poštanskih pretinaca, jedan Krajnji korisnik označava računalnog korisnika koji primi elektroničku poštu putem agenta korisnika pošte (Mail User Agent, „MUA"). Ako MUA prihvati elektroničku poštu i zatim je automatski distribuira većem broju korisnika, broj Krajnjih korisnika određuje se prema stvarnom broju korisnika kojima se distribuira ta elektronička pošta. Ako server za poštu vrši funkciju poštanskog pristupnika, broj Krajnjih korisnika bit će jednak broju korisnika servera za poštu za koje pristupnik obavlja tu funkciju. Ako se neodređen broj adresa elektroničke pošte usmjerava prema jednom korisniku i prihvaća ih jedan korisnik (primjerice putem zamjenskih naziva, alias), a klijent ne distribuira poruke automatski većem broju korisnika, potrebna je Licenca za samo jedno računalo. Jedna se Licenca istodobno smije koristiti samo na jednom računalu. Krajnji korisnik ima pravo unijeti Licenčni ključ Softvera samo u mjeri u kojoj ima pravo upotrebljavati Softver u skladu s ograničenjima koja proizlaze iz broja Licenci koje je dodijelio Dobavljač. Licenčni ključ smatra se povjerljivim te ga ne smijete dijeliti s trećim stranama ili dopustiti trećim stranama upotrebu Licenčnog ključa, osim ako to nije dopušteno Ugovorom ili ako to dopušta Dobavljač. Ako je Licenčni ključ ugrožen, odmah o tome obavijestite Dobavljača.

c) **Home/Business Edition.** Home Edition verzija softvera mora se upotrebljavati isključivo u privatnim i/ili nekomercijalnim okruženjima i isključivo za osobne ili obiteljske potrebe. Za korištenje softvera u komercijalnom okruženju te za korištenje softvera na serverima za poštu, relejima za poštu, pristupnicima za poštu ili internetskim pristupnicima potrebno je nabaviti Business Edition verziju softvera.

d) **Trajanje Licence.** Vaše pravo korištenja Softvera vremenski je ograničeno.

e) **OEM Softver.** Softver klasificiran kao „OEM" ograničen je na računalo s kojim ste ga pribavili. Ne smije se prenositi na drugo računalo.

f) **NFR, TRIAL softver.** Softver koji je klasificiran kao verzija koja nije za daljnju prodaju (Not-for-resale, dalje u tekstu: NFR) ili probna verzija (TRIAL) ne smije se drugima dodjeljivati uz naknadu i smije se koristiti samo u svrhu demonstracije ili testiranja značajki Softvera.

g) **Prekid valjanosti Licence.** Valjanost Licence prekida se automatski na kraju razdoblja za koje je dodijeljena. Ako se Vi ne pridržavate bilo koje odredbe ovog Ugovora, Dobavljač ima pravo povući se iz Ugovora bez utjecaja na bilo koje pravo ili pravni lijek dostupan Dobavljaču u takvom slučaju. U slučaju poništavanja Licence morate bez odgode izbrisati, uništiti ili o vlastitom trošku vratiti Softver i sve sigurnosne kopije tvrtki ESET ili na prodajno mjesto na kojemu ste nabavili Softver. Nakon prekida Licence, Dobavljač također ima pravo poništiti pravo Krajnjeg korisnika na upotrebu funkcija Softvera koje zahtijevaju povezivanje na servere Dobavljača ili trećih strana.

4. **Funkcije koje zahtijevaju prikupljanje podataka i internetsku vezu.** Za pravilno funkcioniranje Softvera potrebna je veza s internetom i povezivanje sa serverima Dobavljača ili trećih strana u redovitim intervalima te primjenjivo prikupljanje podataka u skladu s Pravilima privatnosti. Veza s internetom i primjenjivo prikupljanje podataka neophodni su za sljedeće funkcije Softvera:

a) **Aktualizacija Softvera.** Dobavljač ima pravo povremeno izdavati aktualizacije ili nadogradnje softvera („aktualizacije"), ali nije obvezan nuditi aktualizacije. Ta je funkcija aktivirana u standardnim postavkama softvera te se aktualizacije instaliraju automatski, osim ako krajnji korisnik deaktivira automatsko instaliranje aktualizacija. U svrhu pružanja aktualizacija potrebno je provjeriti autentičnost licence, uključujući podatke o računalu i/ili platformi na kojoj je instaliran softver u skladu s Pravilima privatnosti.

Pružanje aktualizacija može biti podložno Pravilima o isteku vijeka trajanja („Pravila o isteku vijeka trajanja") koja su dostupna na https://go.eset.com/eol_business. Aktualizacije se neće pružati nakon što softver ili bilo koja njegova funkcija dosegne datum isteka vijeka trajanja koji je naveden u Pravilima o isteku vijeka trajanja.

b) **Prosljeđivanje infiltracija i informacija Dobavljaču.** Softver sadrži funkcije koje prikupljaju uzorke računalnih virusa i ostalih zlonamjernih računalnih programa i sumnjive, problematične, potencijalno neželjene ili potencijalno nesigurne objekte kao što su datoteke, URL adrese, IP paketi i ethernet okviri („Infiltracije"), a zatim ih šalju Dobavljaču, uključujući, ali ne isključivo, informacije o instalacijskom postupku, Računalu i/ili platformi na kojoj je Softver instaliran te informacije o operacijama i funkcionalnosti Softvera („Informacije"). Informacije i infiltracije mogu sadržavati podatke (uključujući nasumično ili slučajno prikupljene osobne podatke) o krajnjem korisniku ili drugim korisnicima računala na kojem je softver instaliran i datoteke koje su pod utjecajem infiltracija s povezanim metapodacima.

Informacije i Infiltracije mogu se prikupljati sljedećim funkcijama Softvera:

i. Funkcija LiveGrid Reputation System uključuje prikupljanje i slanje jednostranih ključeva vezanih uz Infiltracije Dobavljaču. Ta funkcija je prema standardnim postavkama Softvera aktivirana.

ii. Funkcija LiveGrid Feedback System uključuje prikupljanje i slanje Infiltracija s povezanim metapodacima i Informacijama Dobavljaču. Tu funkciju može aktivirati Krajnji korisnik tijekom postupka instalacije Softvera.

Dobavljač primljene Informacije i Infiltracije upotrebljava samo za analizu i istraživanje Infiltracija i poboljšanje Softvera i provjere autentičnosti Licence te poduzima odgovarajuće mjere kako bi osigurao da primljene Infiltracije i Informacije ostanu sigurne. Aktivacijom ove funkcije Softvera Dobavljač može prikupljati i obrađivati Infiltracije i Informacije kao što je navedeno u Pravilima privatnosti i u skladu s važećim zakonskim propisima. Ove

funkcije možete deaktivirati u bilo kojem trenutku.

Za potrebe ovog Ugovora potrebno je prikupljati, obrađivati i pohranjivati podatke pomoću kojih Vas Dobavljač može identificirati u skladu s Pravilima privatnosti. Ovime se slažete da Dobavljač može vlastitim sredstvima provjeravati upotrebljavate li Softver u skladu s odredbama ovog Ugovora. Ovime se slažete s tim da je za potrebe ovog Ugovora potrebno prenositi podatke tijekom komunikacije između Softvera i Dobavljačevih računalnih sustava ili računalnih sustava poslovnih partnera u sklopu Dobavljačeve distribucijske mreže i mreže podrške kako bi se osigurala funkcionalnost Softvera i autorizacija za upotrebu Softvera te za zaštitu Dobavljačevih prava.

Nakon prihvaćanja ovog Ugovora Dobavljač ili bilo koji poslovni partner u sklopu Dobavljačeve distribucijske mreže ili mreže podrške ima pravo na prijenos, obradu i pohranu osnovnih podataka koji Vas identificiraju u svrhu fakturiranja, izvršavanja ovog Ugovora i slanja obavijesti na vaše Računalo.

Pojedinosti o privatnosti, zaštiti osobnih podataka i svojim pravima kao sudionik možete potražiti u Pravilima privatnosti koje su dostupne na web-stranici Dobavljača i kojima se može izravno pristupiti tijekom postupka instalacije. Također im možete pristupiti putem odjeljka pomoći u Softveru.

5. **Ostvarivanje prava Krajnjeg korisnika**. Prava Krajnjeg korisnika morate ostvarivati osobno ili putem svojih zaposlenika. Pravo na upotrebu Softvera imate isključivo u svrhu zaštite poslovanja i Računala ili računalnih sustava za koje ste nabavili Licencu.

6. **Ograničenja prava.** Softver ne smijete kopirati, distribuirati, izvlačiti komponente iz njega ni stvarati izvedene radove koji se temelje na Softveru. Pri korištenju Softvera dužni ste poštovati sljedeća ograničenja:

a) Smijete stvoriti jednu arhivsku sigurnosnu kopiju Softvera na mediju za trajnu pohranu podataka pod uvjetom da tu arhivsku sigurnosnu kopiju ne instalirate i ne koristite na bilo kojem drugom računalu. Bilo kakve druge kopije Softvera predstavljat će povredu ovog Ugovora.

b) Ne smijete koristiti, mijenjati, prevoditi, reproducirati ni prenositi prava na korištenje Softvera ili kopija Softvera ni na koji način koji nije izričito dopušten ovim Ugovorom.

c) Softver ne smijete prodavati, podlicencirati, davati u zakup ili najam niti ga posuđivati, odnosno koristiti za pružanje komercijalnih usluga.

d) Softver ne smijete dekompilirati, na njemu vršiti obrnuti inženjering ni obrnuto kompiliranje niti na drugi način pokušati otkriti izvorni kod Softvera, osim u mjeri u kojoj je ovo ograničenje izrijekom zakonski zabranjeno.

e) Suglasni ste Softver koristiti na način sukladan svim nadležnim zakonima u jurisdikciji u kojoj koristite Softver, uključujući, ali ne ograničavajući se na primjenjiva ograničenja koja se odnose na zaštitu autorskih prava i drugih prava na zaštitu intelektualnog vlasništva.

f) Suglasni ste da ćete Softver i njegove funkcije koristiti na način koji ne ograničava mogućnost drugih Krajnjih korisnika da pristupaju tim uslugama. Dobavljač zadržava pravo ograničavanja isporučenih usluga pojedinačnim Krajnjim korisnicima, a kako bi omogućio korištenje usluga što većem mogućem broju Krajnjih korisnika. Ograničavanje usluga također znači mogućnost potpunog ukidanja mogućnosti korištenja bilo koje funkcije softvera i brisanje podataka i informacija na proxy serverima Dobavljača ili serverima trećih strana koji se odnose na određenu funkciju Softvera.

g) Pristajete da se nećete baviti nikakvim aktivnostima koje uključuju upotrebu Licenčnog ključa protivno uvjetima ovog Ugovora ili za koje se Licenčni ključ ustupa bilo kojoj osobi koja nema pravo upotrebljavati Softver, kao što je prijenos iskorištenih ili neiskorištenih Licenčnih ključeva u bilo kojem obliku, neautorizirana reprodukcija ili distribucija dupliciranih ili generiranih Licenčnih ključeva ili upotreba Softvera koja proizlazi iz upotrebe Licenčnog ključa koji je nabavljen iz izvora koji nije Dobavljač.

7. **Autorska prava**. Softver i sva prava, uključujući bez ograničenja pravo vlasništva i pripadajuća prava intelektualnog vlasništva, vlasništvo su tvrtke ESET i/ili njezinih davatelja licence. Ti su entiteti zaštićeni odredbama međunarodnih sporazuma i svim ostalim nadležnim zakonima zemlje u kojoj se Softver koristi. Struktura, organizacija i kôd Softvera vrijedne su poslovne tajne i povjerljive informacije tvrtke ESET i/ili njezinih davatelja licence. Ne smijete kopirati Softver, osim u slučaju opisanom u članku 6 (a). Bilo kakve kopije koje prema ovom Ugovoru smijete stvarati moraju sadržavati iste obavijesti o zaštiti autorskih prava i vlasništvu koje se pojavljuju na Softveru. Ako dekompilirate Softver, na njemu vršite obrnuti inženjering ili na drugi način pokušate otkriti izvorni kôd Softvera, kršeći time odredbe ovog Ugovora, ovime se slažete da se sve tako dobivene informacije automatski i neopozivo smatraju prenesenima Dobavljaču i postaju u potpunosti njegovo vlasništvo od trenutka nastanka tih informacija, bez utjecaja na prava Dobavljača u odnosu na kršenje ovog Ugovora.

8. **Pridržavanje prava**. Dobavljač ovime pridržava sva prava na Softver, s izuzetkom prava izrijekom dodijeljenih Vama kao Krajnjem korisniku Softvera prema odredbama ovog Ugovora.

9. **Višejezične verzije, Softver na dva nosača podataka, veći broj kopija**. U slučaju da Softver podržava više platformi ili jezika, odnosno ako dobijete više kopija Softvera, Softver smijete koristiti samo na onom broju računalnih sustava za koji imate Licence te smijete koristiti samo verzije za koje imate Licencu. Verzije ili kopije Softvera koje ne koristite ne smijete prodati, dati u najam ili zakup, podlicencirati, posuđivati ni prenijeti na treće strane.

10. **Početak i prekid Ugovora.** Ovaj Ugovor stupa na snagu s datumom Vašeg prihvaćanja ovog Ugovora. Ovaj Ugovor možete u bilo kojem trenutku prekinuti tako da trajno deinstalirate, uništite ili o vlastitom trošku vratite Softver, sve sigurnosne kopije i sve povezane materijale koje ste dobili od Dobavljača ili njegovih poslovnih partnera. Vaše pravo na korištenje softvera i svih njegovih funkcija može biti podložno Pravilima o isteku vijeka trajanja. Nakon što softver ili bilo koja njegova funkcija dosegne datum isteka vijeka trajanja koji je naveden u Pravilima o isteku vijeka trajanja, nećete više imati pravo na korištenje softvera. Bez obzira na način prekida ovog Ugovora, odredbe članaka 7., 8., 11., 13., 19. i 21. primjenjuju se bez vremenskog ograničenja.

11. **IZJAVE KRAJNJEG KORISNIKA**. KAO KRAJNJI KORISNIK PRIHVAĆATE ČINJENICU DA SE SOFTVER ISPORUČUJE „U ZATEČENOM STANJU“, BEZ IKAKVOG JAMSTVA, IZRIČITOG ILI IMPLICIRANOG, TE U MAKSIMALNOJ MJERI DOPUŠTENOJ NADLEŽNIM ZAKONOM. DOBAVLJAČ, NJEGOVI DAVATELJI LICENCE NI POVEZANA DRUŠTVA, KAO NI NOSITELJI AUTORSKIH PRAVA, NE DAJU NIKAKVE IZJAVE NI JAMSTVA, IZRIČITA ILI IMPLICIRANA, UKLJUČUJUĆI BEZ OGRANIČENJA JAMSTVO UTRŽIVOSTI ILI PRIKLADNOSTI ZA ODREĐENU NAMJENU, JAMSTVO DA SOFTVER NE POVRJEĐUJE PATENTE, AUTORSKA PRAVA, TRŽIŠNE ZNAKOVE ILI NEKA DRUGA PRAVA TREĆIH STRANA. DOBAVLJAČ NI BILO KOJA DRUGA STRANA NE DAJE NIKAKVA JAMSTVA DA ĆE FUNKCIJE KOJE SOFTVER SADRŽI BITI U SKLADU S VAŠIM POTREBAMA NI DA ĆE SOFTVER FUNKCIONIRATI BEZ POTEŠKOĆA I POGREŠAKA. VI PREUZIMATE POTPUNU ODGOVORNOST I RIZIK KOJI PROIZLAZE IZ ODABIRA SOFTVERA RADI POSTIZANJA REZULTATA KOJE ŽELITE, KAO I ZA INSTALIRANJE I KORIŠTENJE SOFTVERA TE TAKO DOBIVENE REZULTATE.

12. **Odsutnost ostalih obveza**. Ovaj Ugovor ne stvara nikakve obveze Dobavljača i njegovih davatelja licence osim onih izrijekom navedenih u ovom Ugovoru.

13. **OGRANIČENJE ODGOVORNOSTI**. U NAJVEĆOJ MJERI DOPUŠTENOJ MJERODAVNIM ZAKONIMA, NI DOBAVLJAČ, NI NJEGOVI ZAPOSLENICI NI DAVATELJI LICENCE NE SNOSE ODGOVORNOST NI ZA KAKAV GUBITAK PRIHODA, DOBITI ILI PRODAJE, GUBITAK PODATAKA NI ZA TROŠKOVE NASTALE NABAVOM ZAMJENSKIH PROIZVODA ILI USLUGA, ZA OŠTEĆENJE IMOVINE, OSOBNE ŠTETE, PREKID POSLOVANJA, GUBITAK POSLOVNIH PODATAKA, KAO NI ZA BILO KAKVE POSEBNE, IZRAVNE, NEIZRAVNE, SLUČAJNE, GOSPODARSKE, KOMPENZACIJSKE, KAZNENE ILI POSLJEDIČNE ŠTETE, ODNOSNO ŠTETE NASTALE NA BILO KOJI NAČIN, NASTALE NA TEMELJU UGOVORA, NAMJERNOG DJELOVANJA, NEPAŽNJOM ILI NEKOM DRUGOM ČINJENICOM NA KOJOJ SE TEMELJI ODGOVORNOST, NASTALE INSTALACIJOM, KORIŠTENJEM ILI NEMOGUĆNOŠĆU KORIŠTENJA SOFTVERA, ČAK I U SLUČAJU DA SU DOBAVLJAČ ILI NJEGOVI DAVATELJI LICENCE ILI POVEZANA DRUŠTVA UPOZORENI NA MOGUĆNOST TAKVE ŠTETE. BUDUĆI DA ODREĐENE DRŽAVE I JURISDIKCIJE NE DOPUŠTAJU IZUZEĆE OD

ODGOVORNOSTI, ALI MOGU DOPUSTITI NJENO OGRANIČENJE, U TAKVIM SLUČAJEVIMA ODGOVORNOST DOBAVLJAČA, NJEGOVIH ZAPOSLENIKA ILI DAVATELJA LICENCE BIT ĆE OGRANIČENA NA IZNOS KOJI STE PLATILI ZA LICENCU.

14. Nijedna odredba ovog Ugovora nema utjecaja na zakonska prava bilo koje strane koja je u svojstvu potrošača u slučaju da je protivna tim pravima.

15. **Tehnička podrška**. ESET i treće strane koje ESET angažira pružat će tehničku podršku prema vlastitom nahođenju, bez ikakvih jamstava ili izjava. Tehnička podrška se prestaje pružati nakon što softver ili bilo koja njegova funkcija dosegne datum isteka vijeka trajanja koji je naveden u Pravilima o isteku vijeka trajanja. Krajnji korisnik dužan je prije primanja tehničke podrške izraditi sigurnosnu kopiju svih postojećih podataka, softvera i programa. ESET i/ili treće strane koje je angažirao ESET ne mogu prihvatiti odgovornost za štete ili gubitke podataka, vlasništva, softvera ili hardvera ni gubitak dobiti do kojeg može doći uslijed pružanja tehničke podrške. ESET i/ili treće strane koje je angažirao ESET pridržavaju pravo na odluku da tehnička podrška ne obuhvaća rješavanje određenog problema. ESET pridržava pravo na odbijanje, privremeni prekid ili trajni prekid davanja tehničke podrške po vlastitom nahođenju. Podaci o Licenci, Informacije i drugi podaci u skladu s Pravilima privatnosti mogu biti potrebni za pružanje tehničke podrške.

16. **Prijenos Licence**. Softver se smije prenositi s jednog računalnog sustava na drugi, osim ako je to u suprotnosti s odredbama ovog Ugovora. Ako to nije u suprotnosti s odredbama Ugovora, Krajnji korisnik ima pravo trajno prenijeti Licencu i sva prava koja proizlaze iz ovog Ugovora drugom Krajnjem korisniku isključivo uz odobrenje Dobavljača te pod uvjetom (i) da izvorni Krajnji korisnik ne zadrži nijednu kopiju Softvera, (ii) da je prijenos prava izravan, tj. od izvornog Krajnjeg korisnika novom Krajnjem korisniku, (iii) da novi Krajnji korisnik preuzme sva prava i obveze koje je, prema odredbama ovog Ugovora, imao izvorni Krajnji korisnik; (iv) da izvorni Krajnji korisnik novom Krajnjem korisniku dostupnim učini dokumentaciju koja omogućuje provjeru izvornosti Softvera kako je to navedeno u članku 17.

17. **Provjera izvornosti Softvera.** Krajnji korisnik može dokazati svoje pravo na upotrebu Softvera na sljedeće načine: (i) pomoću certifikata o licenci koji je izdao Dobavljač ili treća strana koju je Dobavljač angažirao, (ii) pomoću pisanog licenčnog ugovora, ako je takav ugovor sklopljen, (iii) slanjem poruke e-pošte koju je poslao Dobavljač i koja sadrži pojedinosti o licenciranju (korisničko ime i lozinku). Podaci o Licenci i podaci za identifikaciju Krajnjeg korisnika u skladu s Pravilima privatnosti mogu biti potrebni za provjeru izvornosti Softvera.

18. **Licenciranje za javna tijela i vlasti SAD-a**. Softver se javnim tijelima, uključujući vlasti SAD-a, daje na korištenje uz prava i ograničenja opisana u ovom Ugovoru.

19. **Usklađenost s kontrolom trgovine**.

(a) Slažete se da nećete izravno ili neizravno izvoziti, ponovno izvoziti, prenositi ili drugim metodama staviti Softver na raspolaganje bilo kojoj osobi ili ga upotrebljavati na bilo koji način ili sudjelovati u bilo kojoj radnji kojom bi ESET ili njegovi holdinzi, podružnice i podružnice bilo kojeg njegova holdinga, kao i subjekti koje holdinzi kontroliraju ("Povezana društva"), kršili zakone o kontroli trgovine ili trpjeli negativne posljedice na temelju njih, što uključuje

i. bilo koje zakone kojima se kontroliraju, ograničavaju ili nameću uvjeti licenciranja za izvoz, ponovni izvoz ili prijenos robe, softvera, tehnologije ili usluga, koje izdaju ili donose bilo koje državne uprave, državna ili regulatorna tijela Sjedinjenih Američkih Država, Singapura, Ujedinjenog Kraljevstva, Europske Unije ili bilo koje njezine države članice ili bilo koje države u kojoj se provode obveze iz Ugovora ili u kojoj su tvrtka ESET ili bilo koja njegova Povezana društva osnovani ili posluju („Zakoni kontrole izvoza") te

ii. bilo koje ekonomske, financijske, trgovačke ili druge sankcije, ograničenja, embarga, zabrane uvoza ili izvoza, zabrane prijenosa sredstava ili imovine ili zabrane pružanja usluga ili ekvivalentne mjere koje propisuju bilo koja državna uprava, državna ili regulatorna tijela Sjedinjenih Američkih Država, Singapura, Ujedinjenog Kraljevstva,

Europske Unije ili bilo koje njezine države članice ili bilo koje države u kojoj se provode obveze iz Ugovora ili u kojoj su tvrtka ESET ili bilo koja Povezana društva osnovana ili posluju.

(zakonski akti navedeni u točkama i. i ii. iznad zajednički se nazivaju „Zakoni o kontroli trgovine").

b) ESET ima pravo privremeno ili trajno obustaviti svoje obveze iz ovih Uvjeta s trenutnim učinkom u slučaju da:

i. ESET utvrdi da je korisnik, prema mišljenju tvrtke, prekršio ili bi mogao prekršiti odredbe članka 19. a) ovog Ugovora ili

ii. krajnji korisnik i/ili Softver budu podložni zakonima o kontroli trgovine i ESET na temelju toga utvrdi da bi, prema njegovu mišljenju, nastavkom provedbe korisnikovih obveza iz ovog Ugovora tvrtka ESET ili njezina Povezana društva mogla kršiti zakone o kontroli trgovine ili trpjeti negativne posljedice na temelju njih.

c) Nijedna odredba ovog Ugovora nije predviđena da se tumači i nijedna se odredba ne smije tumačiti tako da navodi ili zahtijeva od druge strane da djeluje ili da se suzdržava od djelovanja (ili da pristane djelovati ili suzdržati se od djelovanja) na bilo koji način koji je nedosljedan, kažnjiv ili zabranjen prema bilo kojim važećim zakonima o kontroli trgovine.

20. **Obavijesti**. Sve obavijesti, softver koji se vraća i dokumentacija šalju se na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, ne dovodeći u pitanje pravo tvrtke ESET da vam priopći bilo kakve izmjene ovog Ugovora, Pravila privatnosti, Pravila o isteku vijeka trajanja i dokumentacije u skladu s čl. 22. Ugovora. ESET vam može slati e-poruke, obavijesti u aplikacijama putem softvera ili objaviti komunikaciju na svojoj web stranici. Pristajete primati komunikaciju o pravnim pitanjima od ESET-a u elektroničkom obliku, uključujući svaku komunikaciju koja se odnosi na izmjene Uvjeta, posebnih uvjeta ili Pravila privatnosti, sve prijedloge/prihvaćanja ugovora ili pozive na ponudu, obavijesti ili druge vrste komunikacije o pravnim pitanjima. Takva elektronička komunikacija smatra se primljenom u pisanom obliku, osim ako važeći zakoni izričito ne zahtijevaju drugačiji oblik komunikacije.

21. **Nadležni zakon**. Na ovaj Ugovor i njegovo tumačenje primjenjivat će se zakoni Republike Slovačke. Krajnji korisnik i Dobavljač suglasni su da se neće primjenjivati principi sukoba zakonskih nadležnosti ni Konvencija Ujedinjenih naroda o ugovorima o međunarodnoj prodaji robe. Izričito se slažete da će za sve sporove i sva potraživanja koja proizlaze iz ovog Ugovora, a odnose se na Dobavljača te sve sporove i sva potraživanja koja se odnose na korištenje Softvera nadležan biti Okružni sud u Bratislavi I te se izričito slažete s pravom navedenog suda da provodi svoju nadležnost.

22. **Opće odredbe**. Ako se bilo koja odredba ovog Ugovora pokaže nevaljanom ili neprovedivom, to neće utjecati na valjanost ostalih odredbi Ugovora, koje ostaju valjane i provedive sukladno uvjetima iz Ugovora. Ovaj je Ugovor sklopljen na engleskom jeziku. U slučaju prevođenja Ugovora radi praktičnosti ili bilo koje druge svrhe ili u slučaju odstupanja između različitih jezičnih verzija ovog Ugovora, mjerodavna je verzija na engleskom jeziku.

ESET zadržava pravo izmjene softvera te izmjene uvjeta ovog Ugovora, njegovih priloga, dodataka, Pravila privatnosti, Pravila o isteku vijeka trajanja i dokumentacije ili bilo kojih njihovih dijelova u svakom trenutku tako da ažurira relevantni dokument (i) u svrhu odražavanja izmjena softvera ili načina na koji ESET posluje, (ii) iz pravnih, regulatornih ili sigurnosnih razloga ili (iii) u svrhu sprječavanja zloupotrebe ili štete. O svakoj izmjeni ovog Ugovora bit ćete obaviješteni putem e-pošte, obavijesti unutar aplikacije ili drugim elektroničkim putem. Ako se ne slažete s predloženim izmjenama Ugovora, možete ga raskinuti u skladu s čl. 10. u roku od 30 dana od primitka obavijesti o promjeni. Ako ne raskinete Ugovor u tom roku, predložene promjene smatrat će se prihvaćenima i stupit će na snagu od datuma primitka obavijesti o promjeni.

Ovo je cjelokupan Ugovor između Vas i Dobavljača koji se odnosi na Softver i kao takav potpuno nadomješta sve prijašnje tvrdnje, pregovore, obveze, izvješća ili oglase u vezi sa Softverom.

EULAID: EULA-PRODUCT-LG; 3537.0

Pravila privatnosti

ESET, spol. s.r. o, s registriranim uredom na adresi Einsteinova 24, 851 01 Bratislava, Republika Slovačka, tvrtka registrirana u trgovačkom registru Okružnog suda u Bratislavi I, odjeljak Sro, unos br. 3586/B, broj poslovne registracije: 31333532, kao voditelj obrade podataka („ESET" ili „Mi") želi biti transparentna u vezi s obradom osobnih podataka i privatnosti svojih korisnika. Radi postizanja tog cilja objavljujemo ova Pravila privatnosti isključivo u svrhu informiranja svojih korisnika („Krajnji korisnik" ili „Vi") o sljedećim temama:

- obradi osobnih podataka,
- povjerljivosti podataka,
- pravima ispitanika.

Obrada osobnih podataka

Usluge koje pruža ESET implementirane u naš program pružaju se pod uvjetima Licenčnog ugovora za krajnjeg korisnika („EULA"), ali neki od njih mogu zahtijevati posebnu pažnju. Želimo vam pružiti više detalja o prikupljanju podataka u vezi s uslugama koje vam pružamo. Pružamo različite usluge opisane u EULA-i i dokumentaciji programa, kao što su usluge nadogradnje, sustava ESET LiveGrid®, zaštite od zloupotrebe podataka, podrške itd. Kako bi usluge funkcionirale, moramo prikupljati sljedeće podatke:

- Statistike o nadogradnji i druge statistike koje obuhvaćaju informacije o procesu instalacije i vašem računalu, uključujući platformu na kojoj je instaliran naš program i informacije o operacijama i funkcijama naših programa kao što su operacijski sustav, informacije o hardveru, instalacijski ID-ovi, ID-ovi licenci, IP adresa, MAC adresa i postavke konfiguracije programa.
- Jednostrani hashevi povezani s infiltracijama kao dio sustava reputacije ESET LiveGrid® koji poboljšava učinkovitost naših rješenja protiv zlonamjernih programa usporedbom skeniranih datoteka i baze podataka pouzdanih i nepoželjnih stavki u cloudu.
- Sumnjivi uzorci i metapodaci iz divljine kao dio sustava za povratne informacije ESET LiveGrid® koji omogućuje tvrtki ESET da odmah reagira na potrebe naših krajnjih korisnika i da održi našu sposobnost reagiranja na najnovije prijetnje. Ovisimo o tome da nam šaljete
  - infiltracije kao što su potencijalni uzorci virusa i drugih zlonamjernih programa i sumnjive, problematične, potencijalno neželjene ili potencijalno nesigurne objekte kao što su izvršne datoteke, poruke e-pošte koje ste prijavili kao spam ili koje je kao takve označio naš program;
  - informacije o uređajima u lokalnoj mreži kao što su vrsta, dobavljač, model i/ili naziv uređaja;
  - informacije o upotrebi interneta kao što su IP adresa i geografske informacije, IP paketi, URL-ovi i ethernet okviri;
  - datoteke sa stanjem nakon pada sustava i informacije u njima.

Ne želimo prikupljati vaše podatke izvan tog opsega, ali ponekad je to nemoguće spriječiti. Slučajno prikupljeni podaci mogu biti uključeni u samim zlonamjernim programima (prikupljeni bez vašeg znanja ili odobrenja) ili kao dio naziva datoteka ili URL-ova i nije nam namjera da oni budu dio naših sustava niti da ih obrađujemo u svrhu opisanu u ovim Pravilima privatnosti.

- Informacije o licenciranju, kao što su ID licence i osobni podaci poput imena, prezimena, adrese i adrese e-

pošte, potrebni su za potrebe fakturiranja, provjeru izvornosti licence i pružanje naših usluga.

• Za pružanje usluge podrške mogu biti potrebni kontaktni podaci i podaci koji se nalaze u vašim zahtjevima za podršku. Ovisno o kanalu koji odaberete za kontakt s nama, možemo prikupiti Vašu adresu e-pošte, telefonski broj, licenčne informacije, podatke o programu i opis Vašeg slučaja za podršku. Možemo od vas zatražiti i druge podatke radi olakšavanja pružanja usluge podrške.

Povjerljivost podataka

ESET je tvrtka koja djeluje diljem svijeta putem povezanih subjekata ili partnera kao dio naše mreže za distribuciju, usluge i podršku. Informacije koje ESET obrađuje mogu se prenijeti povezanim subjektima ili partnerima ili preuzeti od njih radi provedbe Licenčnog ugovora za krajnjeg korisnika, uključujući npr. pružanje usluga ili podrške ili naplatu. Ovisno o Vašoj lokaciji i usluzi koju odaberete, može biti potrebno da prenesemo Vaše podatke u zemlju u kojoj ne postoji odluka Europske komisije o odgovarajućoj zaštiti. Čak i u tom slučaju svaki prijenos informacija podložan je zakonodavstvu o zaštiti podataka i izvršava se samo ako je to potrebno. Standardne ugovorne klauzule, obvezujuća korporativna pravila ili druga odgovarajuća zaštita moraju se utvrditi bez iznimke.

Dajemo sve od sebe kako bismo spriječili pohranjivanje podataka dulje nego što je potrebno tijekom pružanja usluga prema Licenčnom ugovoru za krajnjeg korisnika. Vrijeme zadržavanja može biti duže od valjanosti vaše licence kako bismo vam pružili dovoljno vremena za jednostavnu i pravovremenu obnovu licence. Minimizirane i pseudonimizirane statistike i drugi podaci iz sustava ESET LiveGrid® mogu se dalje obrađivati u statističke svrhe.

ESET provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao odgovarajuću razinu sigurnosti za potencijalne opasnosti. Činimo sve što možemo kako bismo zajamčili kontinuiranu povjerljivost, cjelovitost, dostupnost i otpornost sustava i usluga obrade. Međutim, u slučaju povrede osobnih podataka koja uzrokuje opasnosti za Vaša prava i slobode, spremni smo obavijestiti nadzorno tijelo, kao i osobe čiji se podaci obrađuju. Kao ispitanik imate pravo podnijeti prigovor nadzornom tijelu.

Pravima ispitanika.

Tvrtka ESET podložna je zakonskim odredbama Slovačke Republike i obvezuje nas zakonodavstvo o zaštiti podataka kao dio Europske unije. Podložno uvjetima utvrđenima primjenjivim zakonima za zaštitu podataka, kao ispitanik imate sljedeća prava:

- pravo zatražiti od tvrtke ESET pristup svojim osobnim podacima,
- pravo na ispravak svojih osobnih podataka ako su netočni (također imate pravo na dopunu nepotpunih osobnih podataka),
- pravo zatražiti brisanje svojih osobnih podataka,
- pravo zatražiti ograničenje obrade svojih osobnih podataka,
- pravo uložiti prigovor na obradu,
- pravo podnijeti pritužbu i
- pravo na prenosivost podataka.

Smatramo da su svi podaci koje obrađujemo vrijedni i neophodni za svrhu našeg legitimnog interesa, a to je pružanja usluga i programa korisnicima.

Ako želite ostvariti svoje pravo kao ispitanik ili ako imate pitanja, pošaljite nam poruku na:

ESET, spol. s r.o.

Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk