ESET Endpoint Security

Vartotojo vadovas

Jei norite peržiūrėti šio dokumento internetinę versiją spustelėkite čia

Digital Security
Progress. Protected.

Autorių teisės ©2023 pagal ESET, spol. s r.o.

ESET Endpoint Security sukūrė ESET, spol. s r.o.

Norėdami gauti daugiau informacijos, apsilankykite https://www.eset.com.

Visos teisės saugomos. Jokia šių dokumentų dalis negali būti atgaminama, saugoma paieškos sistemoje ar perduodama bet kokia forma ar bet kokiomis priemonėmis, elektronine, mechanine, kopijavimo, įrašymo, nuskaitymo ar kitokia forma be autoriaus raštiško leidimo.

ESET, spol. s r.o. pasilieka teisę keisti bet kurią iš aprašytų taikomųjų programų be išankstinio įspėjimo.

Techninė pagalba: https://support.eset.com

REV. 2023.3.19

1 ESET Endpoint Security 9 1
1.1 Kas naujo šioje versijoje? 2
1.2 Sistemos reikalavimai 3
1.2 Palaikomos kalbos 4
1.3 Prevencija 5
1.4 Žinyno puslapiai 6
2 Dokumentai apie nuotoliniu būdu valdomus galutinius taškus 7
2.1 Įvadas į ESET PROTECT 8
2.2 Įvadas į ESET PROTECT Cloud 9
2.3 Slaptažodžiu apsaugoti nustatymai 10
2.4 Kas yra politikos 11
2.4 Politikų suliejimas 11
2.5 Kaip veikia vėliavėlės 12
3 Kaip naudoti ESET Endpoint Security pačiam 13
3.1 Diegimo būdai 13
3.1 Diegimas naudojant ESET AV Remover 14
3.1 ESET AV Remover 14
3.1 Išdiegimas naudojant ESET AV Remover baigtas įvykus klaidai 17
3.1 Diegimas (.exe) 17
3.1 Keisti diegimo aplanką (.exe) 19
3.1 Diegimas (.msi) 19
3.1 Išplėstinis diegimas (.msi) 21
3.1 Minimalus modulių diegimas 23
3.1 Diegimas naudojant komandinę eilutę 23
3.1 Diegimas naudojant GPO arba SCCM 28
3.1 Naujinimas į naujesnę versiją 30
3.1 Saugos ir stabilumo atnaujinimai 31
3.1 Dažniausios diegimo problemos 31
3.1 Suaktyvinti nepavyko 31
3.2 Produkto aktyvinimas 32
3.3 Kompiuterio nuskaitymas 32
3.4 Pradedančiojo vadovas 32
3.4 Vartotojo sąsaja 32
3.4 Naujinimo nustatymai 36
3.4 Zonų nustatymai 37
3.4 Saityno kontrolės įrankiai 38
4 Darbas su ESET Endpoint Security 38
4.1 Kompiuteris 40
4.1 Aptikimo modulis 42
4.1 Aptikimo modulio išplėstinės parinktys 46
4.1 Aptiktas įsiskverbimas 47
4.1 Failų sistemos apsauga realiuoju laiku 49
4.1 Apsaugos realiuoju laiku tikrinimas 50
4.1 Kada keisti apsaugos realiuoju laiku konfigūraciją 51
4.1 Ką daryti, jeigu apsauga realiuoju laiku neveikia 51
4.1 Kompiuterio nuskaitymas 51
4.1 Pasirinktinio nuskaitymo paleidimo priemonė 53
4.1 Nuskaitymo eiga 55
4.1 Kompiuterio nuskaitymo žurnalas 56
4.1 Kenkėjiškų programų nuskaitymai 56

4.1 Nuskaitymas laukimo būsenoje 57
4.1 Nuskaitymo profiliai 57
4.1 Nuskaitymo tikslai 58
4.1 Išplėstinės nuskaitymo parinktys 59
4.1 Įrenginio kontrolė 59
4.1 Įrenginio kontrolės taisyklių rengyklė 60
4.1 Aptikti įrenginiai 61
4.1 Įrenginių grupės 61
4.1 Įrenginio kontrolės taisyklių pridėjimas 62
4.1 Pagrindinio kompiuterio apsaugos nuo įsilaužimo sistema (HIPS) 64
4.1 HIPS interaktyvusis langas 67
4.1 Aptiktas potencialus „Ransomware“ viruso elgesys 68
4.1 HIPS taisyklių tvarkymas 68
4.1 HIPS taisyklės parametrai 69
4.1 HIPS išplėstinis nustatymas 71
4.1 Tvarkyklės, kurias leidžiama įkelti visada 72
4.1 Pristatymo režimas 72
4.1 Nuskaitymas paleidžiant 73
4.1 Automatinė paleidimo failo patikra 73
4.1 Dokumentų apsauga 74
4.1 Išimtys 74
4.1 Našumo išimtys 74
4.1 Pridėti arba redaguoti našumo išimtis 76
4.1 Kelio išskyrimo formatas 77
4.1 Aptikimo išimtys 78
4.1 Pridėti arba redaguoti aptikimo išimtį 80
4.1 Aptikimo išimčių kūrimo vedlys vedlį 81
4.1 Išimtys (7.1 ir senesnis) 82
4.1 Procesų išimtys 82
4.1 Pridėti arba redaguoti procesų išskyrimus 83
4.1 HIPS išimtys 83
4.1 ThreatSense parametrai 84
4.1 Valymo lygiai 86
4.1 Failų plėtiniai, kurie nebus nuskaitomi 87
4.1 Papildomi „ThreatSense“ parametrai 87
4.2 Tinklas 88
4.2 Užkarda 89
4.2 Mokymosi režimas 91
4.2 Tinklo apsauga nuo atakų 92
4.2 Apsauga nuo grubios jėgos atakų 93
4.2 Taisyklės 93
4.2 Išimtys 95
4.2 Išplėstinės filtravimo parinktys 95
4.2 IDS taisyklės 98
4.2 Užblokuota įtartina grėsmė 99
4.2 Tinklo apsaugos trikčių šalinimas 99
4.2 Prijungti tinklai 100
4.2 Žinomi tinklai 100
4.2 Žinomų tinklų rengyklė 101
4.2 Tinklo autentiškumo patvirtinimas – serverio konfigūravimas 103
4.2 Užkardos profiliai 104

4.2 Profiliai, priskirti tinklo adapteriams ... 104
4.2 Programos modifikavimo aptikimas ... 105
4.2 Į modifikavimo aptikimo procesą neįtrauktos programos ... 105
4.2 Taisyklių konfigūravimas ir naudojimas ... 106
4.2 Užkardos taisyklių sąrašas ... 106
4.2 Užkardos taisyklių įtraukimas arba redagavimas ... 107
4.2 Užkardos taisyklės – vietinis ... 109
4.2 Užkardos taisyklės – nuotolinis ... 110
4.2 Laikinas IP adresų juodasis sąrašas ... 111
4.2 Patikima zona ... 111
4.2 Zonų konfigūravimas ... 112
4.2 Užkardos zonos ... 112
4.2 Užkardos žurnalas ... 112
4.2 Ryšio nustatymas – aptikimas ... 113
4.2 ESET užkardos problemų sprendimas ... 114
4.2 Trikčių šalinimo vedlys ... 115
4.2 Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo ... 115
4.2 Sukurti taisyklę iš žurnalo ... 115
4.2 Išimčių kūrimas iš užkardos pranešimų ... 116
4.2 Tinklo apsaugos išplėstinį registravimą ... 116
4.2 Problemų sprendimas naudojant protokolų filtravimą ... 116
4.3 Saitynas ir el. paštas ... 117
4.3 Protokolų filtravimas ... 119
4.3 Neįtrauktos programos ... 119
4.3 Neįtraukti IP adresai ... 120
4.3 SSL/TLS ... 121
4.3 Sertifikatai ... 122
4.3 Šifruotas tinklo srautas ... 123
4.3 Žinomų sertifikatų sąrašas ... 123
4.3 Filtruojamų SSL/TLS taikomųjų programų sąrašas ... 124
4.3 El. pašto programų apsauga ... 124
4.3 El. pašto protokolai ... 126
4.3 El. laiškų žymos ... 127
4.3 Integravimas su el. pašto programomis ... 128
4.3 „Microsoft Outlook“ įrankių juosta ... 128
4.3 „Outlook Express“ ir „Windows Mail“ įrankių juosta ... 129
4.3 Patvirtinimo dialogas ... 129
4.3 Nuskaityti iš naujo laiškus ... 130
4.3 Apsauga nuo brukalo ... 130
4.3 Apsaugos nuo brukalo adresų knygelės ... 131
4.3 Juodasis sąrašas / baltasis sąrašas / išimčių sąrašas ... 132
4.3 Juodojo sąrašo / baltojo sąrašo / išimčių adresų pridėjimas ... 133
4.3 Prieigos prie saityno apsauga ... 133
4.3 Prieigos prie saityno apsaugos išplėstinis nustatymas ... 136
4.3 Saityno protokolai ... 136
4.3 URL adresų valdymas ... 137
4.3 URL adresų sąrašas ... 138
4.3 Kurti naują sąrašą ... 139
4.3 Kaip pridėti URL kaukę ... 140
4.3 Apsauga nuo sukčiavimo apsimetant ... 141
4.3 Saugios naršyklės išplėstinis nustatymas ... 142

4.3 Apsaugotos svetainės ... 143
4.3 Naršyklės pranešimas ... 143
4.4 Saityno kontrolė ... 144
4.4 Saityno kontrolės taisyklės ... 145
4.4 Saityno kontrolės taisyklių pridėjimas ... 146
4.4 Kategorijų grupės ... 148
4.4 URL grupės ... 149
4.4 Užblokuoto tinklalapio pranešimo tinkinimas ... 150
4.5 Programos naujinimas ... 152
4.5 Naujinimo nustatymai ... 156
4.5 Naujinimo atšaukimas ... 159
4.5 Produkto naujinimai ... 161
4.5 Ryšio parinktys ... 161
4.5 Naujinimo veidrodinis atspindys ... 163
4.5 Veidrodžio HTTP serveris ir SSL ... 164
4.5 Naujinimas iš veidrodinio atspindžio ... 164
4.5 Veidrodžio naujinimo trikčių šalinimas ... 166
4.5 Kaip sukurti naujinimo užduotis ... 167
4.6 Įrankiai ... 167
4.6 Žurnalo failai ... 168
4.6 Žurnalo filtravimas ... 171
4.6 Prisijungimo konfigūracija ... 172
4.6 Audito žurnalai ... 173
4.6 Planuoklė ... 174
4.6 ESET SysInspector ... 176
4.6 Debesimi paremta apsauga ... 177
4.6 Debesimi paremtos apsaugos išimčių filtras ... 180
4.6 Vykdomi procesai ... 180
4.6 Saugumo ataskaita ... 182
4.6 Tinklo ryšiai ... 183
4.6 ESET SysRescue Live ... 185
4.6 Pavyzdžių pateikimas analizuoti ... 185
4.6 Pasirinkti pavyzdį analizei – įtartinas failas ... 186
4.6 Pasirinkti pavyzdį analizei – įtartinas svetainė ... 186
4.6 Pasirinkti pavyzdį analizei – klaidingai aptiktas failas ... 187
4.6 Pasirinkti pavyzdį analizei – klaidingai aptikta svetainė ... 187
4.6 Pasirinkti pavyzdį analizei – kitas ... 187
4.6 Karantinas ... 187
4.6 Įgaliotojo serverio nustatymas ... 189
4.6 Laiko intervalai ... 190
4.6 „Microsoft Windows“ naujinimas ... 191
4.6 Licencijos intervalų patikra ... 192
4.7 Vartotojo sąsaja ... 192
4.7 Naudotojo sąsajos elementai ... 192
4.7 Prieigos nustatymas ... 194
4.7 Išplėstinio nustatymo slaptažodis ... 195
4.7 Sistemos dėklo piktograma ... 196
4.7 Kontekstinis meniu ... 197
4.7 Žinynas ir palaikymas ... 197
4.7 Apie ESET Endpoint Security ... 198
4.7 Sistemos konfigūracijos duomenų pateikimas ... 199

4.7 Techninė pagalba ... 199
4.8 Pranešimai ... 200
4.8 Programos būsenos ... 200
4.8 Darbalaukio pranešimai ... 201
4.8 Dialogo langas - darbalaukio pranešimai ... 202
4.8 Pranešimų tinkinimas ... 202
4.8 Interaktyvūs įspėjimai ... 202
4.8 Interaktyvių įspėjimų sąrašas ... 204
4.8 Patvirtinimo pranešimai ... 205
4.8 Išplėstinių nustatymų nesuderinamumo klaida ... 206
4.8 Leisti toliau naudoti numatytąją naršyklę ... 206
4.8 Nešiojamoji laikmena ... 206
4.8 Reikia iš naujo paleisti kompiuterį ... 207
4.8 Rekomenduojama iš naujo paleisti kompiuterį ... 208
4.8 Peradresavimas ... 209
4.8 Profilių tvarkytuvas ... 212
4.8 Spartieji klavišai ... 212
4.8 Diagnostika ... 213
4.8 Komandos eilutės skaitytuvas ... 214
4.8 ESET CMD ... 217
4.8 Laukimo būsenos aptikimas ... 219
4.8 Parametrų importavimas ir eksportavimas ... 219
4.8 Grąžinti visus parametrus į numatytuosius ... 220
4.8 Atkurti visus esamojo skyriaus parametrus ... 220
4.8 Klaida išsaugant konfigūraciją ... 221
4.8 Nuotolinis stebėjimas ir valdymas ... 221
4.8 ERMM komandinė eilutė ... 222
4.8 ERMM JSON komandų sąrašas ... 223
4.8 gauti apsaugos būseną ... 224
4.8 gauti informaciją apie programą ... 224
4.8 gauti informaciją apie licenciją ... 227
4.8 gauti žurnalus ... 227
4.8 gauti aktyvinimo būseną ... 228
4.8 gauti nuskaitymo informaciją ... 229
4.8 gauti konfigūraciją ... 230
4.8 gauti naujinimo būseną ... 231
4.8 pradėti nuskaitymą ... 232
4.8 pradėti aktyvinimą ... 232
4.8 pradėti išaktyvinimą ... 233
4.8 pradėti naujinimą ... 234
4.8 nustatyti konfigūraciją ... 234
5 Dažnai užduodami klausimai ... 235
5.1 DUK apie automatinius naujinimus ... 236
5.2 Kaip naujinti ESET Endpoint Security ... 238
5.3 Kaip suaktyvinti ESET Endpoint Security ... 239
5.3 Licencijos rakto įvedimas aktyvinimo metu ... 239
5.3 Prisijungimas prie ESET Business Account ... 240
5.3 Kaip naudoti pasenusius licencijos duomenis naujesniam ESET įrenginio produktui aktyvini ... 240
5.4 Kaip pašalinti virusą iš mano kompiuterio ... 240
5.5 Kaip leisti ryšį tam tikroms taikomosioms programoms ... 240
5.6 Kaip sukurti naują užduotį planuoklėje ... 241

5.6 Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą 242
5.7 Kaip prijungti ESET Endpoint Security prie ESET PROTECT 243
5.7 Kaip naudoti nepaisymo režimą 243
5.7 Kaip taikyti rekomenduojamą politiką ESET Endpoint Security 245
5.8 Kaip sukonfigūruoti veidrodį 247
5.9 Kaip atnaujinti į „Windows 10“, naudojant ESET Endpoint Security 247
5.10 Kaip suaktyvinti nuotolinio stebėjimo ir valdymo funkciją 248
5.11 Kaip blokuoti konkrečių failų tipų atsisiuntimą iš interneto 250
5.12 Kaip sumažinti ESET Endpoint Security naudotojo sąsają 251
5.13 Kaip išspręsti klaidą „Secure Browser could not be redirected to the requested web page“ (saugios naršyklės nepavyko nukreipti į pageidaujamą tinklalapį) 252
6 Galutinio vartotojo licencijos sutartis 253
7 Privatumo politika 260

ESET Endpoint Security 9

„ESET Endpoint Security 9“ atspindi naują požiūrį į iš tikrųjų integruotą kompiuterio apsaugą. Naujausia ESET LiveGrid® nuskaitymo variklio versija, suderinta su mūsų pasirinktine užkarda ir apsaugos nuo brukalo moduliais, užtikrina greitį ir tikslumą, kad jūsų kompiuteris būtų saugus. Rezultatas – išmani sistema, kuri yra nuolat pasiruošusi atremti atakas ir apsaugoti nuo kenkimo programinės įrangos, keliančios pavojų jūsų kompiuteriui.

„ESET Endpoint Security 9“ yra išsamus apsaugos sprendimas, kilęs iš mūsų ilgalaikių pastangų suderinti maksimalią apsaugą ir minimalų sistemos pėdsaką. Pažangios dirbtiniu intelektu pagrįstos technologijos leidžia aktyviai pašalinti įsiskverbiančius virusus, šnipinėjimo programas, Trojos arklius, kirminus, reklamos programas, kenkėjiškas prieigos programas ir kitas internetines atakas, netrukdydamos sistemos veikimui ir nesutrikdydamos kompiuterio darbo.

ESET Endpoint Security 9 pirmiausia skirta naudoti darbo vietose, esančiose smulkių įmonių aplinkoje.

Skyriuje Kaip naudoti ESET Endpoint Security pačiam žinyno temos yra suskirstytos į keletą skyrių ir poskyrių, kad būtų lengviau orientuotis ir susipažinti su turiniu, įskaitant Atsisiuntimas, Diegimas ir Aktyvinimas.

Naudojant ESET Endpoint Security su ESET PROTECT įmonės aplinkoje, galima lengvai valdyti bet kokį kliento darbo vietų skaičių, taikyti strategijas ir taisykles, stebėti aptikimus ir nuotoliniu būdu konfigūruoti klientus iš bet kurio prie tinklo prijungto kompiuterio.

Skyriuje Bendrieji klausimai pateikiami kai kurie dažniausiai užduodami klausimai ir problemos, su kuriomis susiduriama.

Funkcijos ir privalumai

Naujas vartotojo sąsajos dizainas	Šios versijos vartotojo sąsajos dizainas iš esmės pakeistas ir supaprastintas vadovaujantis patogaus naudojimo bandymais. Visas GUI tekstas ir pranešimai atidžiai peržiūrėti, o sąsaja dabar palaiko iš dešinės į kairę skaitomas kalbas, tokias kaip hebrajų ir arabų. Interneto žinynas dabar integruotas į ESET Endpoint Security ir pateikia dinamiškai atnaujinamą pagalbos turinį.
Apsauga nuo virusų ir šnipinėjimo programų	Aktyviai aptinka ir valo daugiau žinomų ir nežinomų virusų, kirminų, Trojos arklių ir kenkėjiškų prieigos programų. Pažangi euristika pažymi net anksčiau niekada nematytas kenkėjiškas programas ir apsaugo jus nuo nežinomų grėsmių, neutralizuoja jas, kol nepridarė jokios žalos. Saityno prieigos apsauga ir Apsauga nuo sukčiavimo apsimetant veikia stebėdama ryšį tarp interneto naršyklių ir nuotolinių serverių (įskaitant SSL). El. pašto programos apsauga kontroliuoja el. pašto ryšį, gaunamą POP3(S) ir IMAP(S) protokolais.
Reguliarūs naujinimai	Reguliariai naujinti aptikimo modulį (anksčiau vadintą „virusų kodų duomenų baze“) ir programos modulius yra geriausias būdas užtikrinti maksimalų saugos lygį kompiuteryje.
ESET LiveGrid® (Debesų išteklius naudojanti reputacija)	Jūs galite patikrinti vykdomų procesų ir failų reputaciją tiesiai iš ESET Endpoint Security.

Nuotolinis valdymas	ESET PROTECT leidžia valdyti „ESET“ produktus prie tinklo prijungtose darbo vietose, serveriuose ir mobiliuosiuose įrenginiuose iš vienos centrinės vietos. Naudodami ESET PROTECT tinkle valdomą konsolę (ESET PROTECT tinkle valdomą konsolę), galite diegti ESET sprendimus, valdyti užduotis, pritaikyti saugumo politiką, stebėti sistemos būseną ir greitai reaguoti į nuotolinių kompiuterių problemas ar jiems iškilusias grėsmes.
Tinklo apsauga nuo atakų	Analizuoja tinklo srauto turinį ir saugo nuo atakų iš tinklo. Blokuojamas bet koks žalingu laikomas turinys.
Saityno kontrolė (tik ESET Endpoint Security)	Saityno kontrolė leidžia blokuoti interneto puslapius, kuriuose gali būti galimai įžeidžiančios žalingos informacijos. Be to, darbdaviai arba sistemos administratoriai gali uždrausti prieigą prie daugiau nei 27 iš anksto nustatytų svetainių kategorijų ir daugiau nei 140 subkategorijų.

Kas naujo šioje versijoje?

ESET Endpoint Security 9 versija išleista ir ją galima atsisiųsti.

Automatiniai atnaujinimai

- užtikrina, kad visada naudosite naujausią produkto versiją
- išmanus sprendimas, sumažinantis ESET Endpoint Security techninę priežiūrą iki visiško minimumo

- įjungta pagal numatytuosius nustatymus ir naudojant mikroprogramos komponento naujinimą
- iš naujo įdiegia produkto be neigiamų aspektų, pavyzdžiui, išregistravimo iš sistemos proceso metu, įskaitant konfigūracijos perkėlimą
- atsisiunčia mažiau duomenų (diferencinis atnaujinimas)
- pateikiama su lengvai naudojamu ar visiškai suprantamu naudotojui skirtu priminimu ir yra visiškai suderinama su valdomaisiais tinklais

Susieti galutinio naudotojo licencijos sutarties pakeitimai

- nauja galutinio naudotojo licencijos sutartis pateikiama nepriklausomai nuo diegimo proceso, naudojant informatyvų elementą konsolėje arba ESET Endpoint Security naudotojo sąsajoje
- supaprastina produkto automatinio atnaujinimo procesą ir padaro jūsų naudotojo patirtį geresnę, nes jums nebereikės sutikti su galutinio naudotojo licencijos sutartimi kaskart, kai jūsų ESET produktas atnaujinamas į naujesnę versiją

Apsauga nuo grubios jėgos atakų

- kaip pertvarkytos apsaugos nuo tinklo atakų dalis, apsauga nuo grubios jėgos atakų tikrina tinklo duomenų srauto turinį ir blokuoja slaptažodžio spėjimo atakų bandymus
- stebimi pakartotiniai bandymai su šaltinio IP adresu, o laikinajame IP adreso juodajame sąraše sukuriamas žurnalo įrašas, kuris padeda stebėti situaciją
- po tam tikro laiko netinkamo elgesio šaltinio IP adresas galiausiai gali būti pašalintas iš juodojo sąrašo, jei ryšys yra teisėtas
- konfigūruojama dideliuose tinkluose

Vietinė ARM64 komponavimo versija

- 9 versijoje siūloma ARM64 komponavimo versija

Šiame leidime yra įvairių klaidų ištaisymų ir našumo patobulinimų.

Norėdami gauti papildomos informacijos apie naujas ESET Endpoint Security funkcijas, taip pat ekrano kopijas, skaitykite šį ESET žinių bazės straipsnį:

- Kas naujo ESET Endpoint Security 9 versijoje?

Sistemos reikalavimai

Kad ESET Endpoint Security sklandžiai veiktų, sistema turi atitikti šiuos aparatūros ir programinės įrangos reikalavimus (numatytieji produkto nustatymai):

Palaikomi procesoriai

Intel arba AMD procesorius, 32 bitų (x86) su SSE2 instrukcijų rinkiniu arba 64bit (x64), 1 GHz arba daugiau
ARM64 pagrindu pagamintas procesorius, 1 GHz arba spartesnis

Operacinės sistemos

Microsoft® Windows® 11

Microsoft® Windows® 10

Išsamų palaikomų Microsoft® Windows® 10 ir Microsoft® Windows® 11 versijų sąrašą rasite „Windows“ operacinės sistemos palaikymo politikoje.

„Azure“ kodo pasirašymo palaikymas turi būti įdiegtas visose "Windows" operacinėse sistemose, kad būtų galima įdiegti arba naujovinti ESET produktus, išleistus po 2023 m. liepos mėn. Daugiau informacijos.

Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 su naujausiais „Windows“ atnaujinimais (bent KB4474419 ir KB4490628)

„ESET Endpoint Security“ 9.1 versija yra paskutinė, palaikanti „Windows 7“ ir „Windows 8.1“. Daugiau informacijos.

Windows XP ir Windows Vista nebepalaikomos.

Visada stenkitės užtikrinti, kad jūsų operacinė sistema būtų atnaujinta.

ESET Endpoint Security diegimo programa, sukurta ESET PROTECT 8.1 ir naujesnėmis versijomis, palaiko „Windows 10 Enterprise for Virtual Desktops“ ir „Windows 10“ kelių seansų režimą.

Kita

- Turi atitikti operacinės sistemos ir kitos kompiuteryje įdiegtos programinės įrangos sistemos reikalavimus
- 0,3 GB laisvos vietos sistemoje (žr. 1 pastabą)

- 1 GB laisvos vietos diske (žr. 2 pastabą)
- Min. ekrano raiška – 1024 x 768
- Interneto ryšys arba vietinio tinklo ryšys su produkto naujinimų šaltiniu (žr. 3 pastabą)
- Dvi antivirusinės programos, vienu metu veikiančios viename įrenginyje, sukelia neišvengiamus sistemos išteklių konfliktus, pvz., sulėtina sistemą taip, kad jos nebegalima valdyti

Nors produktą gali pavykti įdiegti ir paleisti sistemose, kurios neatitinka šių reikalavimų, pagal veikimo reikalavimus rekomenduojame atlikti išankstinį naudojimo bandymą.

(1): vieta diske, kurios reikia diegimo programai atsisiųsti, produktui įdiegti ir diegimo paketo kopijai programos duomenyse išsaugoti bei produkto naujinimų atsarginėms kopijoms saugoti, kad juos būtų galima panaudoti grąžinimo funkcijai.
(2): vieta diske, kurios reikia diegimo programai atsisiųsti, produktui įdiegti ir diegimo paketo kopijai programos duomenyse išsaugoti bei produkto naujinimų atsarginėms kopijoms saugoti, kad juos būtų galima panaudoti grąžinimo funkcijai. Esant tam tikroms aplinkybėms (pvz., kai saugomos produkto naujinimo atsarginės kopijos versijos, atminties iškelties failai ar didžiuliai registravimo įrašų kiekiai) arba užkrėstame kompiuteryje (pvz., naudojant karantino funkciją) gali būti naudojama daugiau vietos diske. Rekomenduojame pasirūpinti, kad diske būtų pakankamai vietos, kad būtų diegiami operacinės sistemos ir ESET produktų naujinimai.
(3): nors ir nerekomenduojama, produktas gali būti naujinamas rankiniu būdu naudojant keičiamąją laikmeną.

Palaikomos kalbos

ESET Endpoint Security galima atsisiųsti ir įdiegti šiomis kalbomis.

Kalba	Kalbos kodas	LCID
Anglų (Jungtinės Valstijos)	en-US	1033
Arabų (Egiptas)	ar-EG	3073
Bulgarų	bg-BG	1026
Kinų supaprastinta	zh-CN	2052
Kinų (tradicinė)	zh-TW	1028
Kroatų	hr-HR	1050
Čekų	cs-CZ	1029
Estų	et-EE	1061
Suomių	fi-FI	1035
Prancūzų (Prancūzija)	fr-FR	1036
Prancūzų (Kanados)	fr-CA	3084
Vokiečių (Vokietija)	de-DE	1031
Graikų	el-GR	1032
Hebrajų	he-IL	1037
Vengrų	hu-HU	1038
*Indoneziečių	id-ID	1057
Italų	it-IT	1040
Japonų	ja-JP	1041
Kazachų	kk-KZ	1087

Kalba	Kalbos kodas	LCID
Korėjiečių	ko-KR	1042
*Latvių	lv-LV	1062
Lietuva	lt-LT	1063
Nederlands	nl-NL	1043
Norvegų	nb-NO	1044
Lenkų	pl-PL	1045
Portugalų (Brazilų)	pt-BR	1046
Rumunų	ro-RO	1048
Rusų	ru-RU	1049
Ispanų (Čilė)	es-CL	13322
Ispanų (Ispanija)	es-ES	3082
Švedų (Švedija)	sv-SE	1053
Slovakų	sk-SK	1051
Slovėnų	sl-SI	1060
Tajų	th-TH	1054
Turkų	tr-TR	1055
Ukrainiečių k. (Ukraina)	uk-UA	1058
*Vietnamiečių	vi-VN	1066

* ESET Endpoint Security galima šia kalba, išskyrus internetinį vadovą (nukreipia į versija anglų k.).

Norėdami pakeisti šio internetinio vadovo kalbą, žr. kalbos pasirinkimo langelį (viršutiniame dešiniajame kampe).

Prevencija

Kai dirbate su kompiuteriu ir ypač – kai naršote internete – atsiminkite, kad jokia antivirusinė sistema pasaulyje negali visiškai pašalinti pavojaus, kurį kelia aptikimai ir nuotolinės atakos. Kad būtų užtikrinta maksimali apsauga ir patogus naudojimas, itin svarbu teisingai naudoti antivirusinį sprendimą ir laikytis keleto naudingų taisyklių.

Reguliariai naujinkite

Pagal ESET LiveGrid® statistiką, kasdien sukuriama tūkstančiai naujų, unikalių įsiskverbimų, bandančių apeiti esamas apsaugos priemones ir siekiančių duoti pelno jų autoriams – visa tai vykdoma kitų vartotojų sąskaita. ESET virusų laboratorijos specialistai kasdien analizuoja šias grėsmes ir paruošia bei išleidžia naujinimus, kad būtų nuolatos gerinamas mūsų vartotojų apsaugos lygis. Kad būtų užtikrintas maksimalus šių naujinimų efektyvumas, svarbu, kad naujinimai būtų tinkamai sukonfigūruoti jūsų sistemoje. Jeigu norite rasti daugiau informacijos, kaip konfigūruoti naujinimus, žiūrėkite skyrių Naujinimo nustatymai.

Atsisiųskite saugos pataisas

Kenkėjiškų programų autoriai dažnai išnaudoja įvairias sistemos spragas, kad galėtų efektyviau platinti kenkėjišką kodą. Atsižvelgdamos į tai programinės įrangos įmonės atidžiai ieško bet kokių spragų savo programose ir reguliariai išleidžia saugos naujinimus, kurie apsaugo nuo galimų grėsmių. Svarbu atsisiųsti šiuos saugos naujinimus, kai jie išleidžiami. „Microsoft Windows“ ir tokios interneto naršyklės kaip „Internet Explorer“ yra du

programų, kurioms saugos naujinimai išleidžiami reguliariai, pavyzdžiai.

Svarbių duomenų atsarginių kopijų kūrimas

Kenkimo programinės įrangos kūrėjai paprastai nekreipia dėmesio į vartotojų poreikius: kenkimo programų veikla dažnai sukelia kritines operacinės sistemos klaidas ir sugadina svarbius duomenis. Svarbu reguliariai daryti svarbių ir slaptų duomenų atsargines kopijas į išorinį šaltinį, tokį kaip DVD arba išorinį standųjį diską. Tai leidžia lengviau ir greičiau atkurti duomenis įvykus sistemos gedimui.

Reguliariai nuskaitykite kompiuterį tikrindami, ar jame nėra virusų

Daugiau žinomų ir nežinomų virusų, kirminų, Trojos arklių ir kenkėjiškų prieigos programų aptikimą vykdo failų sistemos apsaugos realiuoju laiku modulis. Tai reiškia, kad kaskart, kai pasiekiate failą arba jį atidarote, jis nuskaitomas dėl kenkėjiškų veiksmų. Mes rekomenduojame atlikti viso kompiuterio nuskaitymą bent vieną kartą per mėnesį, nes kenkėjiškų programų kodai kinta, aptikimo modulis kasdien savaime atsinaujina.

Laikykitės pagrindinių saugos taisyklių

Tai pati naudingiausia ir pati veiksmingiausia taisyklė – visada būkite atsargūs. Šiandien, daugeliui įsiskverbimų reikalingi vartotojo veiksmai, kad jie galėtų veikti ir būti platinami. Jeigu būsite atidūs atidarydami naujus failus, sutaupysite daug laiko ir pastangų, reikalingų išvalyti įsiskverbimams. Čia pateikiama keletas naudingų nurodymų:

- Nesilankykite įtartinose svetainėse su daug iškylančiųjų langų ir mirksinčiais reklaminiais skelbimais.
- Būkite atidūs diegdami nemokamas programas, kodekų paketus ir t. t. Naudokite tik saugias programas ir lankykitės tik saugiose interneto svetainėse.
- Būkite atsargūs atidarydami el. laiškų priedus, ypač kai gaunate laiškus, skirtus daugeliui gavėjų, arba gaunamus iš nežinomų siuntėjų.
- Nenaudokite administratoriaus paskyros kasdieniam darbui su kompiuteriu.

Žinyno puslapiai

Sveiki! Tai ESET Endpoint Security žinyno failai. Čia pateikiama informacija supažindins jus su gaminiu ir padės padaryti jūsų kompiuterį saugesnį.

Pradžia

Prieš pradėdami naudoti ESET Endpoint Security, atminkite, kad mūsų produktą gali naudoti vartotojai, prisijungę per ESET PROTECT, arba pati programa. Rekomenduojame susipažinti su įvairiais aptikimo tipais ir nuotolinėmis atakomis, kurios gali užpulti kompiuterį.

Žr. naujos funkcijos, kur rasite informacijos apie šioje ESET Endpoint Security versijoje pristatytas naujoves. Be to, mes paruošėme vadovą, kuris padės jums nustatyti ir pritaikyti savo reikmėms pagrindinius ESET Endpoint Security parametrus.

Kaip naudoti ESET Endpoint Security žinyno puslapius

Žinyno temos yra suskirstytos į keletą skyrių ir poskyrių, kad būtų lengviau orientuotis ir susipažinti su turiniu. Reikiamos informacijos galite rasti naršydami žinyno puslapių struktūrą.

Norėdami daugiau sužinoti apie kurį nors programos langą, paspauskite **F1**. Bus rodomas žinyno puslapis, susijęs su langu, kurį šiuo metu peržiūrite.

Žinyno puslapius galima naršyti naudojant raktažodžius arba įvedant žodžius ir frazes. Šie du metodai skiriasi tuo, kad raktažodis gali būti logiškai susietas su žinyno puslapiais, kurių tekste gali nebūti šio konkretaus raktažodžio. Ieškant pagal žodžius ar frazes, bus ieškoma visuose puslapiuose ir rodomi tik tie puslapiai, kuriuose yra ieškomas žodis ar frazė.

Siekiant išlaikyti nuoseklumą ir išvengti painiavos, šiame vadove vartojama terminija yra sudaryta pagal ESET Endpoint Security parametrų pavadinimus. Be to, ypač reikšmingoms ar svarbioms temoms išskirti naudojame vienodą simbolių rinkinį.

Pastaba yra tiesiog trumpas paaiškinimas. Nors galite jas praleisti, pastabose pateikiama vertingos informacijos, pavyzdžiui, tam tikros funkcijos arba nuorodos į kai kurias susijusias temas.

Į tai reikia atkreipti dėmesį, todėl šios informacijos raginame nepraleisti. Paprastai čia pateikiama ne pati svarbiausia, bet svarbi informacija.

Tai informacija, kuriai reikalingas ypatingas dėmesys ir dėl kurios reikia būti itin atsargiems. Įspėjimai dažniausiai pateikiami siekiant jus perspėti, kad nepadarytumėte galimai pavojingų klaidų. Perskaitykite ir įsigilinkite į įspėjimuose pateikiamą tekstą, nes jis skirtas itin jautriems sistemos parametrams arba kam nors pavojingam.

Tai – konkretus panaudojimo būdas arba praktinis pavyzdys, padedantis suprasti, kaip galima naudotis tam tikra funkcija ar galimybe.

Sutartinis pavadinimas	Reikšmė
Paryškintasis tipas	Sąsajos elementų pavadinimai, pvz., langų ir parinkčių mygtukų.
Pasvirasis tipas	Vietos rezervavimo ženklai jūsų pateikiamai informacijai. Pavyzdžiui, failo pavadinimas arba kelias reiškia, kad reikia įvesti tikrą kelią ar failo pavadinimą.
`Courier New`	Kodo pavyzdžiai arba komandos.
Hipersaitas	Leidžia greitai ir lengvai pasiekti nurodomas temas ar išorines saityno vietas. Hipersaitai yra paryškinti mėlynai ir gali būti pabraukti.
%ProgramFiles%	„Windows“ sistemos katalogas, kuriame saugomos „Windows“ sistemoje įdiegtos programos.

Internetinis žinynas yra pagrindinis žinyno turinio šaltinis. Kai būsite prisijungę prie veikiančio interneto ryšio, bus rodoma naujausia internetinio žinyno versija.

Dokumentai apie nuotoliniu būdu valdomus galutinius taškus

ESET produktus verslui ir ESET Endpoint Security galima valdyti klientų darbo stotyse, serveriuose ir mobiliuosiuose įrenginiuose tinklo aplinkoje iš vienos centrinės vietos. Sistemos administratoriai, kurie valdo daugiau kaip 10 klientų darbo vietų gali įdiegti vieną iš ESET nuotolinio valdymo įrankių, kad galėtų diegti ESET sprendimus, valdyti užduotis, taikyti saugos politikas, stebėti sistemos būseną ir greitai reaguoti į problemas arba grėsmes nuotoliniuose kompiuteriuose iš vienos centrinės vietos.

ESET nuotolinio valdymo įrankiai

ESET Endpoint Security gali būti valdoma nuotoliniu būdu naudojant ESET PROTECT arba ESET Cloud Administrator.

- Įvadas į ESET PROTECT
- Įvadas į ESET PROTECT Cloud

Trečiųjų šalių nuotolinio valdymo įrankiai

- Nuotolinis stebėjimas ir valdymas (RMM)

Geriausios praktikos

- Prijunkite visus įrenginius su ESET Endpoint Security prie ESET PROTECT
- Apsaugokite Išplėstinio nustatymo nustatymus prijungtuose kliento kompiuteriuose, kad apsisaugotumėte nuo savavališkų pakeitimų
- Taikykite rekomenduojamą politiką, kad pritaikytumėte galimas saugos funkcijas
- Minimizuokite naudotojo sąsają, kad sumažintumėte arba apribotumėte naudotojo sąveiką su ESET Endpoint Security

Instrukcijos

- Kaip naudoti nepaisymo režimą
- Kaip įdiegti ESET Endpoint Security naudojant GPO arba SCCM

Įvadas į ESET PROTECT

ESET PROTECT leidžia valdyti „ESET“ produktus prie tinklo prijungtose darbo vietose, serveriuose ir mobiliuosiuose įrenginiuose iš vienos centrinės vietos.

Naudodami ESET PROTECT tinkle valdomą konsolę, galite diegti ESET sprendimus, valdyti užduotis, taikyti apsaugos politikas, stebėti sistemos būseną ir greitai reaguoti į problemas arba aptikimus nuotoliniuose kompiuteriuose. Taip pat žr. ESET PROTECT architektūros ir infrastruktūros elementų apžvalgą, Darbo pradžia su ESET PROTECT tinkle valdoma konsole ir Palaikomos darbalaukio aprūpinimo aplinkos.

ESET PROTECT skirtas šiems komponentams:

- ESET PROTECT Serveris. „ESET PROTECT“ serveris gali būti įdiegtas „Windows“ bei „Linux“ serveriuose, taip pat jis gali būti virtualus prietaisas. Jis tvarko ryšį su agentais, kaupia ir saugo programos duomenis duomenų bazėje.
- „ESET PROTECT“ saityno pultas. „ESET PROTECT“ yra pagrindinė sąsaja, leidžianti valdyti kliento kompiuterius jūsų aplinkoje. Jis rodo klientų būsenų jūsų tinkle apžvalgą ir leidžia nuotoliniu būdu įdiegti „ESET“ sprendimus nevaldomiems kompiuteriams. Įdiegę ESET PROTECT serverį („ serverį), galite pasiekti saityno pultą naudodamiesi savo žiniatinklio naršykle. Jei pasirinksite, kad žiniatinklio serveris būtų prieinamas internetu, galite naudoti „ESET PROTECT“ iš bet kurios vietos ir (arba) įrenginio su interneto ryšiu.
- ESET Management Agentas. „ESET Management“ agentas palengvina komunikaciją tarp „ESET PROTECT“ serverio ir kliento kompiuterių. Agentas turi būti įdiegtas kliento kompiuteryje, kad būtų sukurtas ryšys tarp to kompiuterio ir „ESET PROTECT“ serverio. Kadangi jis yra kliento kompiuteryje ir gali saugoti daugiau nei

vieną apsaugos scenarijų, naudojant „ESET Management“ agentą, ženkliai sumažinamas reakcijos į naujus aptikimus laikas. Naudodami „ESET PROTECT“ saityno pultą, galite įdiegti „ESET Management“ agentą į nevaldomus kompiuterius, identifikuotus pagal „Active Directory“ arba „ESET“ RD jutiklį. Taip pat galite rankiniu būdu įdiegti „ESET Management“ agentą kliento kompiuteriuose, jei to reikia.

- „ESET Rogue Detection Sensor“. „ESET Rogue Detection (RD) Sensor“ aptinka jūsų tinkle esančius nevaldomus kompiuterius ir siunčia jų informaciją į „ESET PROTECT“ serverį. Taip galima lengvai pridėti naujus kliento kompiuterius prie apsaugoto tinklo. RD jutiklis prisimena kompiuterius, kurie buvo aptikti, ir du kartus neišsiunčia tos pačios informacijos.
- „Apache“ HTTP tarpinis serveris – tai paslauga, kuri gali būti naudojama kartu su „ESET PROTECT“, kad būtų galima:
    - Paskirstyti naujinimus kliento kompiuteriams ir diegimo paketus „ESET Management“ agentui;
    - Persiųsti komunikaciją iš „ESET Management“ agentų į „ESET PROTECT“ serverį.
- Mobiliojo įrenginio jungtis – tai komponentas, leidžiantis valdyti mobilųjį įrenginį su „ESET PROTECT“, suteikiančiu jums teisę valdyti mobiliuosius įrenginius („Android“ bei „iOS“) ir administruoti „Android“ skirtą „ESET Endpoint Security“.
- ESET PROTECT Virtualus prietaisas (VA). „ESET PROTECT“ VA skirtas vartotojams, kurie nori paleisti „ESET PROTECT“ virtualioje aplinkoje.
- „ESET PROTECT“ Virtual Agent Host – „ESET PROTECT“ komponentas, kuris virtualizuoja agento objektus, kad būtų galima valdyti virtualias mašinas be agentų. Šis sprendimas užtikrina automatizavimą, dinamišką grupių naudojimą ir tokį patį užduočių valdymo lygį kaip „ESET Management“ agento fiziniuose kompiuteriuose. Virtualusis agentas surenka informaciją iš virtualių mašinų ir nusiunčia ją į „ESET PROTECT“ serverį.
- Veidrodžio įrankis – Veidrodžio įrankis reikalingas moduliams neprisijungus naujinti. Jei jūsų kliento kompiuteriuose nėra interneto ryšio, galite naudoti veidrodžio įrankį naujinimo failams iš „ESET“ naujinimo serverių atsisiųsti ir saugoti juos vietoje.
- „ESET Remote Deployment Tool“ – šis įrankis skirtas universaliesiems paketams, sukurtiems „<%PRODUCT%>“ saityno pulte, įdiegti. Tai patogus būdas paskirstyti „ESET Management“ agentą su „ESET“ produktu tinkle esantiems kompiuteriams.
- „ESET Business Account“ - Naujasis licencijavimo portalas „ESET“ verslo produktams leidžia valdyti licencijas. Žr. šio dokumento skyrių „ESET Business Account“, kuriame pateikiami nurodymai, kaip suaktyvinti produktą, arba „ESET Business Account“ naudojimo vadovą, kuriame rasite daugiau informacijos apie „ESET Business Account“ naudojimą. Jei jau turite „ESET“ išduotą vartotojo vardą ir slaptažodį, kurį norite konvertuoti į licencijos raktą, žr. skyrių „Konvertuokite senosios licencijos kredencialus“.
- „ESET Inspect“ – visapusiška galinio punkto aptikimo ir reagavimo sistema, apimanti tokias funkcijas kaip incidentų aptikimas, incidentų valdymas ir atsakas, duomenų rinkimas, pažeidimo aptikimo rodikliai, anomalijų aptikimas, elgesio aptikimas ir politikos pažeidimai.

Naudodami ESET PROTECT tinkle valdomą konsolę, galite diegti ESET sprendimus, valdyti užduotis, taikyti apsaugos politikas, stebėti sistemos būseną ir greitai reaguoti į problemas arba grėsmes nuotoliniuose kompiuteriuose.

ℹ Daugiau informacijos rasite ESET PROTECT internetiniame naudotojo vadove.

Įvadas į ESET PROTECT Cloud

ESET PROTECT Cloud leidžia valdyti ESET produktus prie tinklo prijungtose darbo vietose ir serveriuose iš vienos centrinės vietos be fizinio arba virtualaus serverio, kaip, pvz., ESET PROTECT. Naudodami (ESET PROTECT

Cloudsaityno pultą), galite diegti ESET sprendimus, valdyti užduotis, pritaikyti saugumo politikas, stebėti sistemos būseną ir greitai reaguoti į nuotolinių kompiuterių problemas ar jiems iškilusias grėsmes.

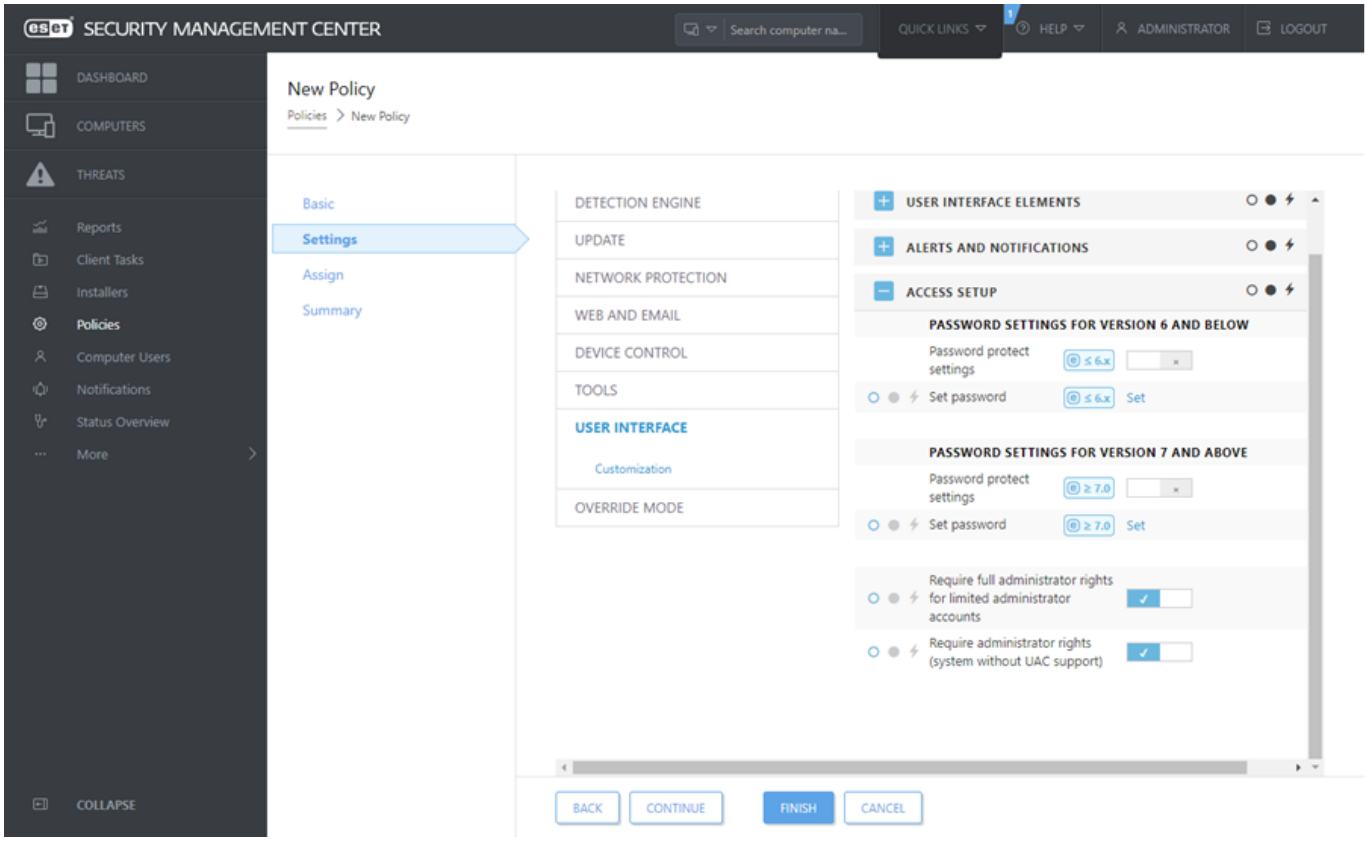
- Daugiau apie tai skaitykite ESET PROTECT Cloud internetiniame vartotojo vadove

Slaptažodžiu apsaugoti nustatymai

Kad užtikrintumėte didžiausią savo sistemos saugumą, „ESET Endpoint Security“ reikia tinkamai sukonfigūruoti. Bet koks nekvalifikuotas pakeitimas ar nustatymas gali sumažinti kliento saugumą ir apsaugos lygį. Norėdamas apriboti vartotojo prieigą prie išplėstinių nustatymų, administratorius gali nustatymus apsaugoti slaptažodžiu.

Administratorius gali sukurti politiką, skirtą slaptažodžiu apsaugoti prijungtuose kliento kompiuteriuose esančio ESET Endpoint Security išplėstinio nustatymo nustatymus. Norėdami sukurti naują politiką, atlikite toliau nurodytus veiksmus.

1. ESET PROTECT Tinkle valdomoje konsolėje spustelėkite kairiajame pagrindinio meniu šone esančią parinktį **Politikos**.
2. Spustelėkite „**New Policy**“ (nauja politika).
3. Pavadinkite savo naująją politiką ir, jei norite, pateikite trumpą jos aprašymą. Spustelėkite mygtuką „**Continue**“ (tęsti).
4. Iš produktų sąrašo pasirinkite „**ESET Endpoint for Windows**“ („Windows“ skirta „ESET Endpoint“).
5. Spustelėkite **Vartotojo sąsaja** sąraše **Nustatymai** ir išplėskite **Prieigos nustatymai**.
6. Pagal ESET Endpoint Security versiją spustelėkite slankiklio juostą, kad įjungtumėte **Slaptažodis nustatymams apsaugoti**. Atkreipkite dėmesį, kad „ESET Endpoint“ produktų 7 versija suteikia didesnę apsaugą. Jei tinkle turite tiek 7, tiek 6 versijos „Endpoint“ produktų, kiekvienai versijai rekomenduojame nustatyti dvi atskiras politikas su skirtingais slaptažodžiais.
7. Laikinajame lange sukurkite naują slaptažodį, patvirtinkite jį ir spustelėkite „**OK**“ (gerai). Spustelėkite **Tęsti**.
8. Priskirkite naują politiką klientams. Spustelėkite **Priskirti** ir pasirinkite kompiuterius ar jų grupes, kad apsaugotumėte slaptažodžiu. Spustelėdami **Gerai** patvirtinkite pasirinkimą.
9. Patikrinkite, ar visi pageidaujami kliento kompiuteriai yra tiksliniame sąraše ir spustelėkite „**Continue**“ (tęsti).
10. Peržiūrėkite politikos nustatymus santraukoje ir spustelėkite „**Finish**“, kad išsaugotumėte naują politiką.



Kas yra politikos

Administratorius gali įdiegti tam tikras konfigūracijas į „ESET“ produktus, kurie veikia kliento kompiuteriuose, naudodamas „ESET PROTECT“ saityno pulto politikas. Politika gali būti taikoma tiesiogiai atskiriems kompiuteriams ir kompiuterių grupėms. Taip pat kompiuteriui ar grupei galite priskirti kelias politikas.

Norėdamas sukurti naują politiką, vartotojas turi turėti šias teises: „**Read**“ (skaityti) – teisė skaityti politikų sąrašą, „**Use**“ (naudoti) – teisė priskirti politikas tiksliniams kompiuteriams, o „**Write**“ (rašyti) – teisė kurti, modifikuoti ir redaguoti politikas.

Politikos taikomos tokia tvarka, kokia išdėstytos statinės grupės. Tai netinka dinaminėms grupėms, nes politikos pirmiausia taikomos vaikų dinaminėms grupėms. Taip politikas galima taikyti darant didesnį poveikį grupės medžio viršūnei, ir galima pogrupiams taikyti konkretesnes politikas. Naudodamas vėliavėles, prie aukščiau medyje esančių grupių prieigą turintis „ESET Endpoint Security“ vartotojas gali perrašyti žemesniųjų grupių politikas. Šis algoritmas paaiškintas ESET PROTECT internetiniame žinyne.

> Rekomenduojame priskirti bendresnę politiką (pvz., serverio naujinimo politiką) grupėms, kurios yra aukščiau grupių medyje. Konkretesnes politikas (pvz., įrenginio kontrolės nustatymus) reikėtų priskirti giliau grupės medyje. Suliejus, žemiau esanti politika paprastai perrašo aukščiau esančių politikų nustatymus (jei neapibrėžta kitaip, naudojant politikos vėliavėles).

Politikų suliejimas

Klientui taikoma politika paprastai yra įvairių politikų suliejimo į vieną galutinę politiką rezultatas. Politikos suliejamos po vieną. Suliejant politikas, galioja bendroji taisyklė, kad vėlesnė politika visada pakeičia ankstesniosios nustatymus. Norėdami pakeisti šią elgseną, galite naudoti politikos vėliavėles (siūloma kiekvienam nustatymui).

Kurdami politikas pastebėsite, kad kai kuriuose nustatymuose yra papildoma taisyklė (pakeisti / papildyti / pridėti), kurią galite konfigūruoti.

- **Pakeisti** – pakeičiamas visas sąrašas, pridedamos naujos vertės ir pašalinamas ankstesnysis.
- **Papildyti** – elementai pridedami šiuo metu taikomo sąrašo apačioje (turi būti kita politika, vietinis sąrašas visada perrašomas).
- **Pridėti** – elementai pridedami sąrašo viršuje (vietinis sąrašas perrašomas).

ESET Endpoint Security palaiko vietinių nustatymų suliejimą su nuotolinėmis politikomis nauju būdu. Jei nustatymas yra sąrašas (pvz., blokuojamų svetainių sąrašas) ir nuotolinė politika prieštarauja esamam vietiniam nustatymui, nuotolinė politika jį perrašo. Galite pasirinkti, kaip derinti vietinius ir nuotolinius sąrašus, pasirinkdami skirtingas suliejimo taisykles:

- nuotolinių politikų nustatymams sulieti;
- nuotolinėms ir vietinėms politikoms sulieti – vietiniams nustatymams ir gautai nuotolinei politikai.

Norėdami daugiau sužinoti apie politikų suliejimą, vadovaukitės ESET PROTECTinternetiniu vartotojo žodynu ir peržiūrėkite pavyzdį.

Kaip veikia vėliavėlės

Kliento kompiuteryje taikoma politika paprastai yra įvairių politikų suliejimo į vieną galutinę politiką rezultatas. Kai suliejate politikas, galite pakoreguoti numatomą galutinės politikos elgesį dėl taikomų politikų tvarkos, naudodami politikos vėliavėles. Vėliavėlės apibrėžia, kaip politika tvarkys konkretų nustatymą.

Kiekvienam nustatymui galite pasirinkti vieną iš toliau nurodytų vėliavėlių.

Netaikyti	Bet koks nustatymas su šia vėliavėle nėra parinktas politikos. Kadangi nustatymo politika neparinko, jį gali pakeisti kitos vėliau pritaikytos politikos.
Taikyti	Nustatymai su „**Apply**“ (taikyti) vėliavėle bus taikomi kliento kompiuteryje. Tačiau suliejant politikas juos gali perrašyti kitos vėliau pritaikytos politikos. Kai politika siunčiama į kliento kompiuterį, kuriame yra šia vėliavėle pažymėtų nustatymų, šie nustatymai pakeičia kliento kompiuterio vietinę konfigūraciją. Kadangi nustatymas nėra priverstinai taikomas, jį vis tiek gali pakeisti kitos vėliau pritaikytos politikos.
Priversti	Nustatymams su vėliavėle „**Force**“ (priversti), suteikiama pirmenybė ir jų negali perrašyti jokia vėliau pritaikyta politika (net jei ji taip pat pažymėta vėliavėle „**Force**“ (priversti). Taip užtikrinama, kad kitos vėliau pritaikytos politikos negalėtų pakeisti šio nustatymo suliejimo metu. Kai politika siunčiama į kliento kompiuterį, kuriame yra šia vėliavėle pažymėtų nustatymų, šie nustatymai pakeičia kliento kompiuterio vietinę konfigūraciją.

Scenarijus. *Administratorius* nori leisti vartotojui *Jonui* kurti arba redaguoti politikas savo namų grupėje ir matyti visas *administratoriaus* sukurtas politikas, įskaitant politikas, kurios pažymėtos vėliavėle „Force“ (priversti). *Administratorius* nori, kad *Jonas* galėtų matyti visas politikas, bet ne redaguoti esamas politikas, kurias sukūrė *administratorius*. *Jonas* gali kurti arba redaguoti politikas savo namų grupėje „San Diego“.
Sprendimas. *Administratorius* turi atlikti toliau nurodytus veiksmus.
Sukurti tinkintas statines grupes ir teisių rinkinius.
1. Sukurti naują statinę grupę pavadinimu „*San Diego*“.
2. Sukurti naują teisių rinkinį pavadinimu „*Policy - All Jonas*“ su prieiga prie statinės grupės „*All*“ ir teise „**Read**“ (skaityti), skirta „**Policies**“ (politikos).
3. Sukurti naują teisių rinkinį pavadinimu „*Policy Jonas*“ su prieiga prie statinės grupės „*San Diego*“ ir prieigos prie funkcijų teise „**Write**“ (rašyti), skirta „**Group & Computers**“ (grupė ir kompiuteriai) bei „**Policies**“ (politikos). Ši teisė leidžia *Jonui* kurti arba redaguoti politikas savo namų grupėje „*San Diego*“.
4. Sukurti naują vartotoją „*Jonas*“, o skiltyje „**Permission Sets**“ (teisių rinkiniai) pasirinkti „*Policy - All Jonas*“ ir „*Policy Jonas*“.
„Create policies“ (kurti politikas)
5. Sukurkite naują politiką „*All- Enable Firewall*“, išplėskite skiltį „**Settings**“ (nustatymai), pasirinkite „**ESET Endpoint for Windows**“ („Windows“ skirta „Esset Endpoint“), pereikite prie „**Personal Firewall**“ (asmeninė užkarda) > „**Basic**“ (standartinė) ir pritaikykite visus nustatymus vėliavėle „**Force**“ (priversti). Išplėskite skiltį „**Assign**“ (priskirti) ir pasirinkite statinę grupę „*All*“.
6. Sukurkite naują politiką „*Jonas Group- Enable Firewall*“, išplėskite skiltį „**Settings**“ (nustatymai), pasirinkite „**ESET Endpoint for Windows**“ („Windows“ skirta „Esset Endpoint“), pereikite prie „**Personal Firewall**“ (asmeninė užkarda) > „**Basic**“ (standartinė) ir pritaikykite visus nustatymus vėliavėle „**Apply**“ (taikyti). Išplėskite skiltį „**Assign**“ (priskirti) ir pasirinkite statinę grupę „*San Diego*“.
Rezultatas
Administratoriaus sukurtos politikos bus taikomos nuo tada, kai politikų nustatymams bus pritaikytos vėliavėlės „**Force**“ (priversti). Nustatymams su vėliavėle „Force“ (priversti) teikiama pirmenybė, todėl jų vėliau negali perrašyti kita vėliau pritaikyta politika. Vartotojo „*Jonas*“ sukurtos politikos bus taikomos po administratoriaus sukurtų politikų.
Norėdami pamatyti galutinę politikų tvarką, pereikite prie „**More**“ (daugiau) > „**Groups**“ (grupės) > „**San Diego**“. Pasirinkite kompiuterį ir tada pasirinkite „**Show details**“ (rodyti išsamią informaciją). Skiltyje „**Configuration**“ (konfigūracija) spustelėkite „**Applied policies**“ (taikomos politikos).

Kaip naudoti ESET Endpoint Security pačiam

Šis vartotojo vadovo skyrius ir skyrius Darbas su ESET Endpoint Security, skirtas vartotojams, besinaudojantiems ESET Endpoint Security be ESET PROTECT arba ESET PROTECT Cloud. Visos ESET Endpoint Security savybės ir funkcijos yra pasiekiamos priklausomai nuo vartotojo paskyros teisių.

Diegimo būdai

Įdiegti ESET Endpoint Security 9.x versiją kliento darbo vietoje galima keliais būdais, nebent diegiate ESET Endpoint Security nuotoliniu būdu kliento darbo vietoje per ESET PROTECT arba ESET PROTECT Cloud.

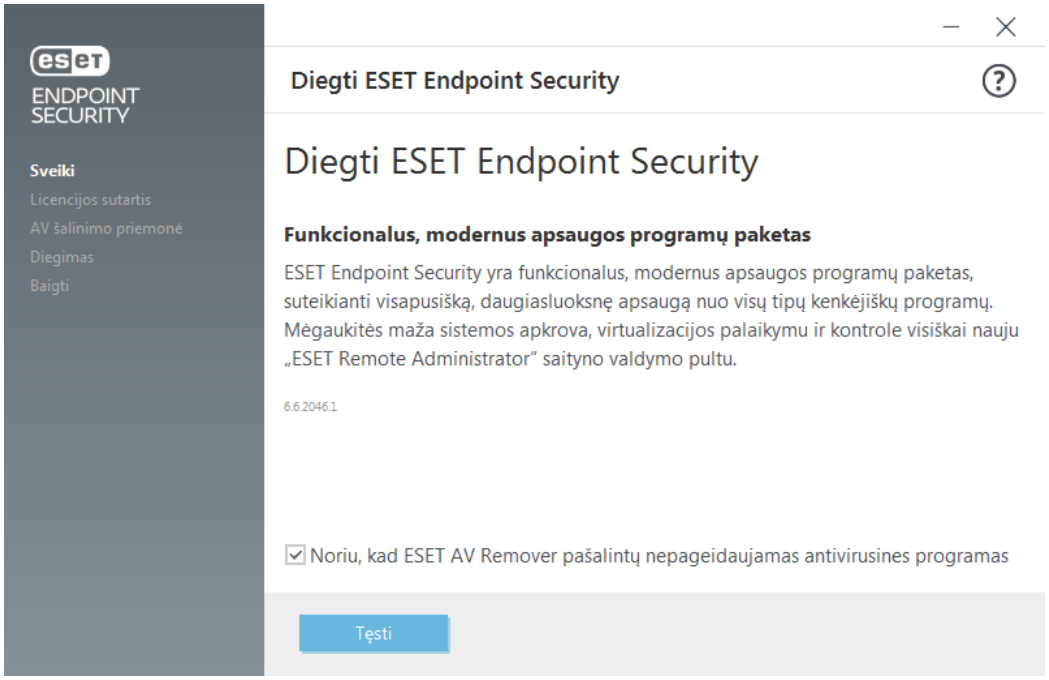
Būdas	Tikslas	Atsisiuntimo nuoroda
Diegimas naudojant ESET AV Remover	Įrankis ESET AV Remover padės jums pašalinti beveik bet kokią anksčiau sistemoje įdiegtą antivirusinę programinę įrangą prieš pradedant diegimą.	Atsisiųsti 64 bitų Atsisiųsti 32 bitų
*** Diegimas (.exe)	Diegimo procesas be ESET AV Remover.	N/A

Būdas	Tikslas	Atsisiuntimo nuoroda
Diegimas (.msi)	Verslo aplinkoje rekomenduojamas .msi diegimo programos paketas. Daugiausiai dėl to, kad juo galima diegti neprisijungus ir nuotoliniu būdu, naudojant įvairius įrankius, pvz., ESET PROTECT.	Atsisiųsti 64 bitų Atsisiųsti 32 bitų
Diegimas naudojant komandinę eilutę	ESET Endpoint Security galima įdiegti vietoje naudojant komandinę eilutę arba nuotoliniu būdu, naudojant kliento užduotį programoje ESET PROTECT.	N/A
Diegimas naudojant GPO arba SCCM	Naudokite tolius valdymo įrankius, kaip GPO arba SCCM, kad įdiegtumėte ESET valdymo agentą ir ESET Endpoint Security kliento darbo vietose.	N/A
Diegimas naudojant RMM įrankius	ESET DEM priedai nuotolinio valdymo ir stebėjimo (RMM) įrankiui suteikia galimybę diegti ESET Endpoint Security kliento darbo vietose.	N/A

ESET Endpoint Security yra pasiekiama daugiau kaip 30 kalbų.

Diegimas naudojant ESET AV Remover

Prieš tęsiant įdiegimo procesą svarbu iš kompiuterio išdiegti bet kokias esamas saugos programas. Pažymėkite langelį šalia **Noriu, kad ESET AV Remover pašalintų nepageidaujamas antivirusines programas** ir ESET AV Remover nuskaitys jūsų sistemą bei pašalins bet kokias palaikomas saugos programas. Jei langelio nepažymėsite ir spustelėsite **Tęsti**, ESET Endpoint Security bus įdiegta nepaleidus ESET AV Remover.

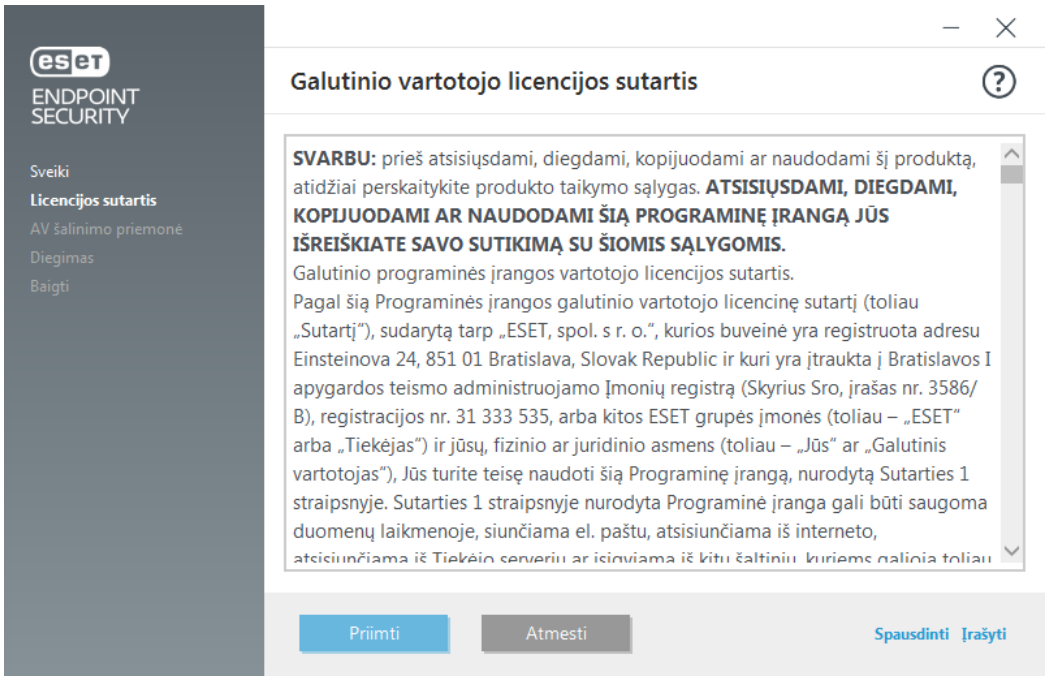


ESET AV Remover

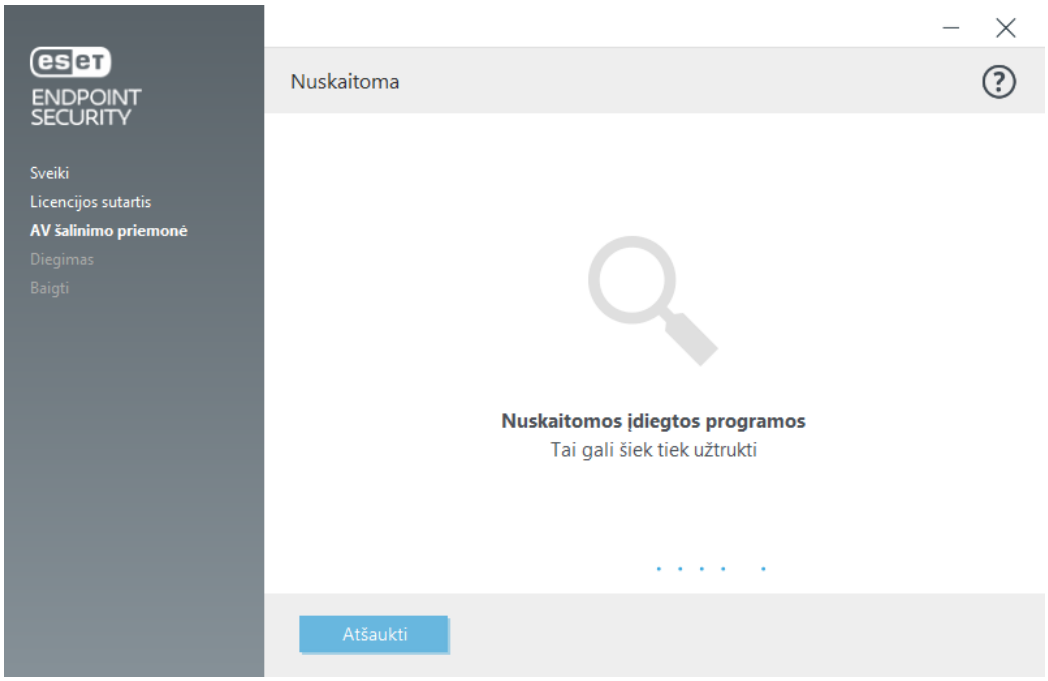
ESET AV Remover Įrankis padės pašalinti beveik bet kokią antivirusinę programinę įrangą, anksčiau įdiegtą jūsų sistemoje. Jei norite naudodamiesi ESET AV Remover pašalinti esamą antivirusinę programą, vadovaukitės toliau pateiktais nurodymais:

1. Jei norite pamatyti antivirusinės programinės įrangos, kurią gali pašalinti ESET AV Remover, sąrašą, atsidarykite ESET žinių bazės straipsnį.

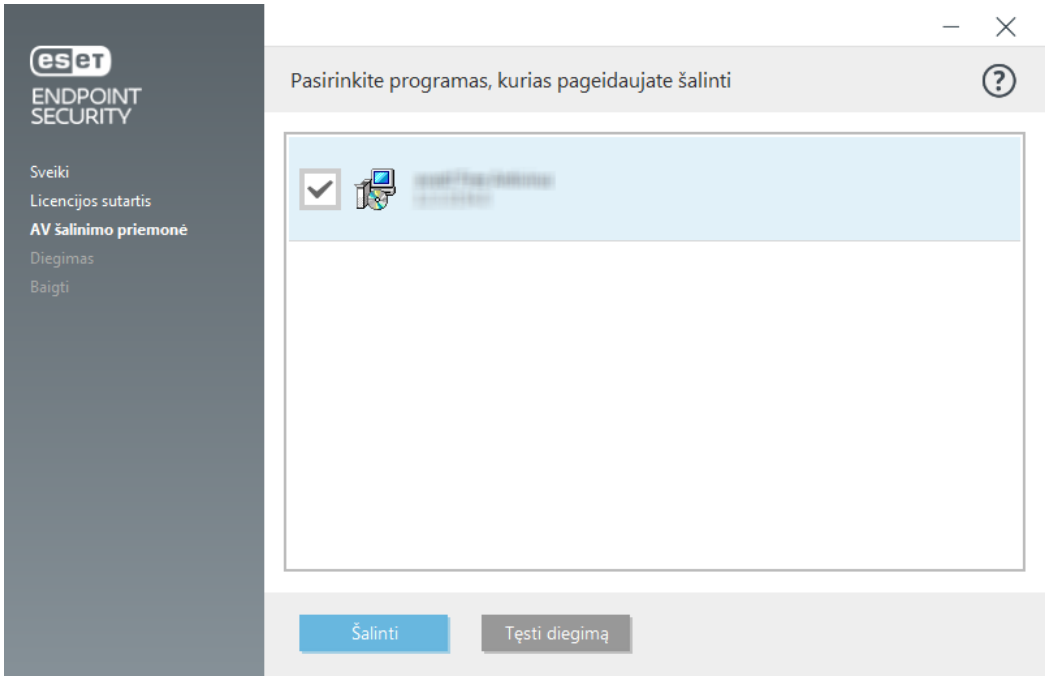
2. Perskaitykite galutinio naudotojo licencijos sutartį ir spustelėkite **Priimti**, kad patvirtintumėte savo sutikimą. Jei spustelėsite **Atmesti**, ESET Endpoint Security bus diegiama toliau, tačiau esama saugos programa iš kompiuterio nebus pašalinta.



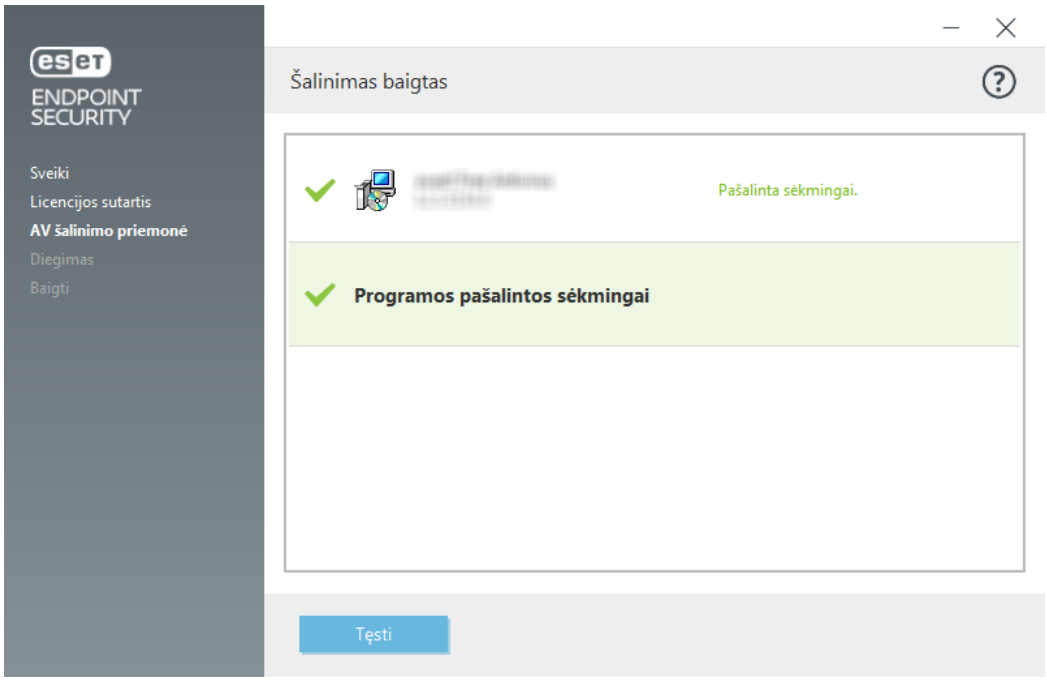
2. ESET AV Remover pradės jūsų kompiuteryje ieškoti antivirusinės programinės įrangos.



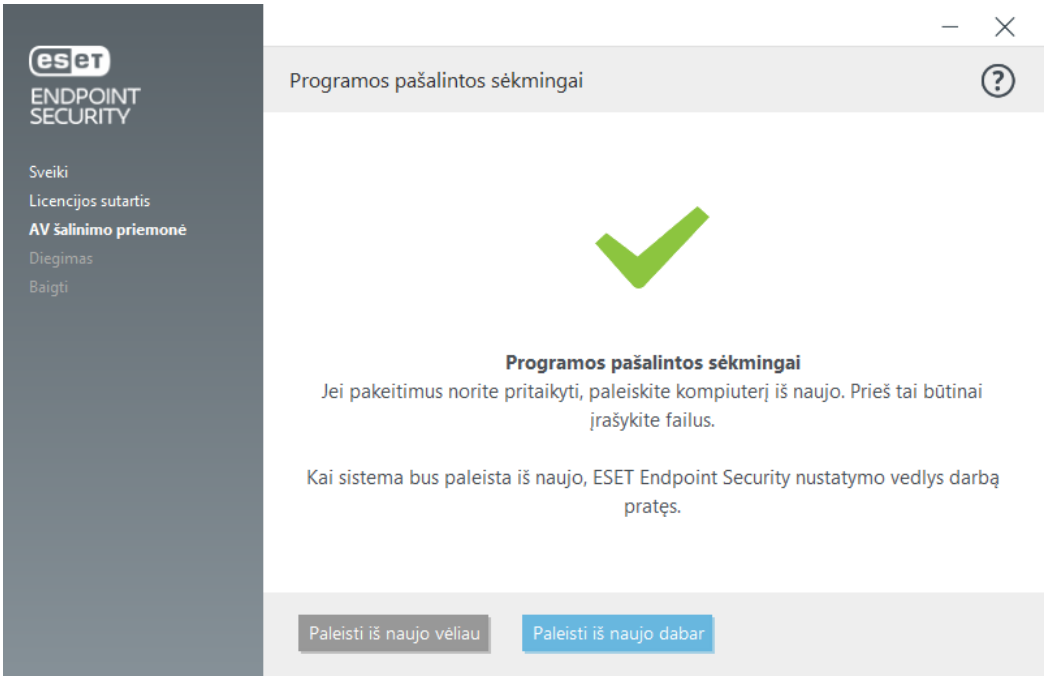
2. Pasirinkite visas nurodytas antivirusines programas ir spustelėkite **Šalinti**. Šalinimas gali šiek tiek užtrukti.



2. Kai šalinimas sėkmingai užbaigiamas, spustelėkite **Tęsti**.



6. Paleiskite kompiuterį iš naujo, kad pakeitimai būtų pritaikyti, o ESET Endpoint Security diegimas – pratęstas. Jei išdiegti nepavyksta, žr. šio vadovo skyrių Išdiegimas naudojant ESET AV Remover baigtas įvykus klaidai.



Išdiegimas naudojant ESET AV Remover baigtas įvykus klaidai

Jei naudojantis ESET AV Remover pašalinti antivirusinės programos nepavyksta, jums bus parodytas pranešimas, kad programa, kurią mėginate pašalinti, galbūt nedera su ESET AV Remover. Jei norite sužinoti, ar šią konkrečią programą galima pašalinti, peržiūrėkite palaikomų produktų sąrašą arba dažniausiai naudojamų „Windows“ antivirusinių programų šalinimo priemones, nurodytas ESET žinių bazėje.

Jei nepavyko išdiegti apsaugos produkto arba jei jo komponento dalis liko neišdiegta, jūsų bus paprašyta „**Restart and rescan**“ (paleisti ir nuskaityti iš naujo). Paleidę kompiuterį patvirtinkite UAC, kad nuskaitymo ir išdiegimo procesas būtų pratęstas.

Jei reikia, susisiekite su ESET techninės pagalbos tarnyba, pateikite pagalbos užklausą ir būkite pasiruošę ESET specialistams nusiųsti failą **AppRemover.log**. Failas **AppRemover.log** yra aplanke **eset**. Norėdami patekti į šį aplanką, „Windows Explorer“ lange atverkite *%TEMP%*. Siekdama padėti išspręsti problemą, ESET techninės pagalbos tarnyba su jumis susisieks kaip įmanoma greičiau.

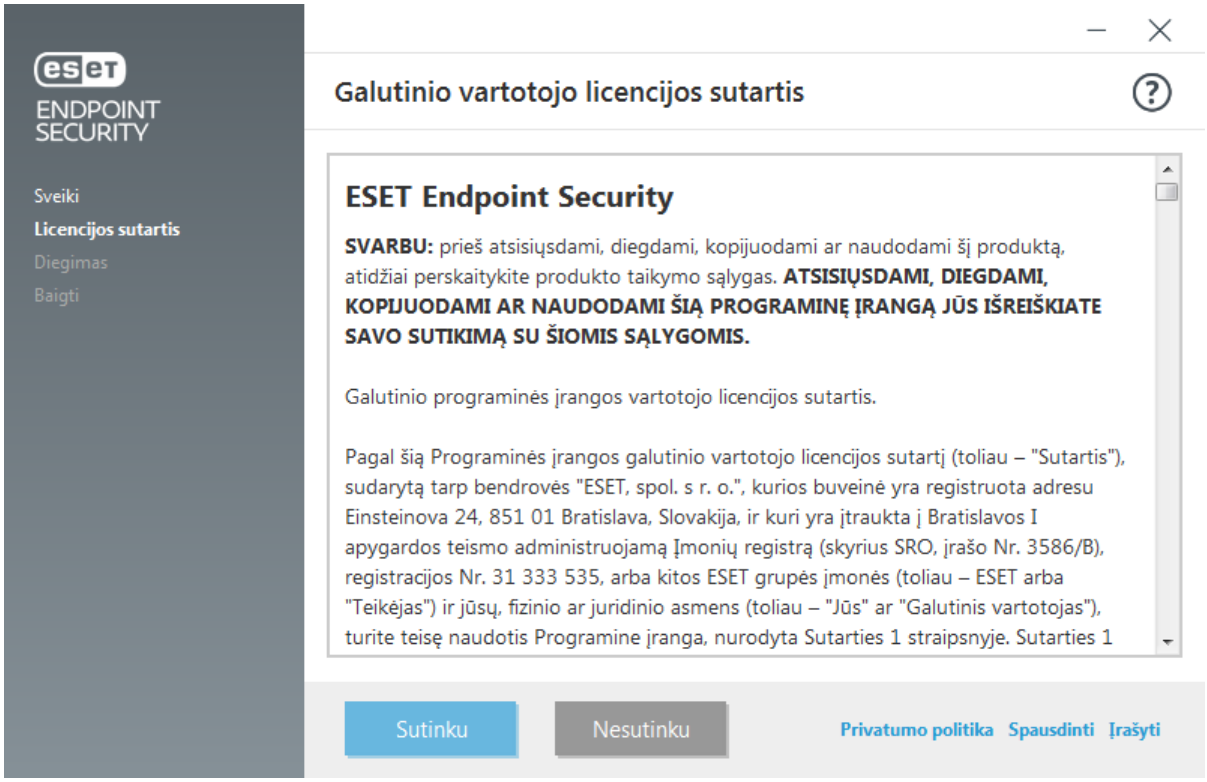
Diegimas (.exe)

Paleidus .exe diegimo programą, diegimo vediklis padės jums vykdyti diegimo procedūrą.

Įsitikinkite, kad kompiuteryje nėra įdiegta jokių kitų antivirusinių programų. Jeigu du arba daugiau antivirusinių sprendimų yra įdiegta viename kompiuteryje, jie gali konfliktuoti vienas su kitu. Rekomenduojame išdiegti visas kitas antivirusines programas savo sistemoje. Žiūrėkite mūsų žinių bazės straipsnį, kuriame rasite įprastinės antivirusinės programinės įrangos pašalinimo įrankių sąrašą (pateikiamas anglų ir keliomis kitomis kalbomis).



1. Perskaitykite galutinio naudotojo licencijos sutartį. Spustelėkite **Leisti viską ir tęsti**, jei norite konfigūruoti Galimų nepageidaujamų taikomųjų programų aptikimą ir įjungti ESET LiveGrid® atsiliepimų sistemą. ESET LiveGrid® padeda užtikrinti, kad ESET būtų nedelsiant ir nuolat informuojama apie naujus įsiskverbimus, o tai leidžia mums geriau apsaugoti savo klientus. Sistema leidžia pateikti naujas grėsmes ESET virusų laboratorijai, kurioje jos analizuojamos, apdorojamos ir įtraukiamos į aptikimo variklį. Spustelėkite **Tęsti**, kad patvirtintumėte, jog sutinkate su Galutinio naudotojo licencijos sutartimi. Galite įdiegti ESET Endpoint Security konkrečiame aplanke, spustelėdami **Keisti diegimo aplanką**.



2. Baigus diegti, būsite paraginti aktyvinti ESET Endpoint Security.

Keisti diegimo aplanką (.exe)

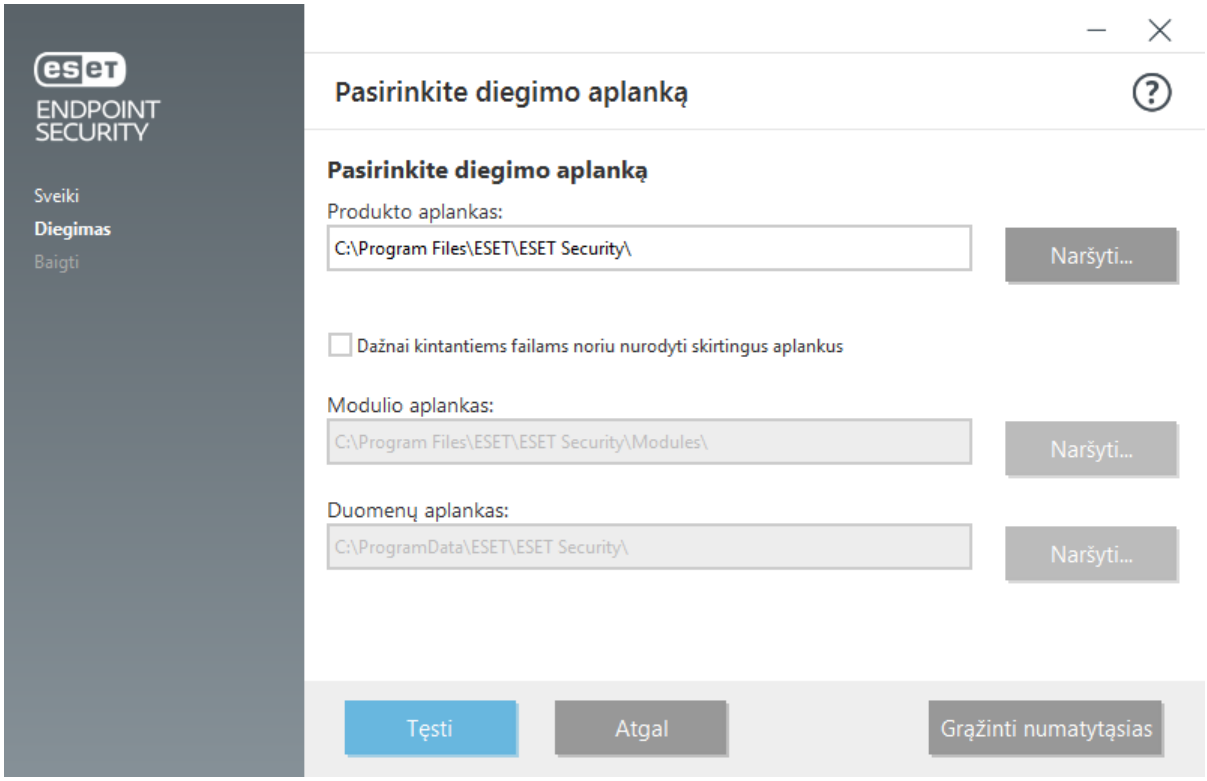
Pasirinkus galimai nepageidaujamų programų aptikimo funkciją ir spustelėjus „**Change installation folder**“ (keisti diegimo katalogą), bus paraginta pasirinkti produkto ESET Endpoint Security diegimo aplanką. Pagal numatytuosius nustatymus programa diegiama šiame kataloge:

C:\Program Files\ESET\ESET Security

Galite nurodyti vietą, skirtą programos moduliams ir duomenims. Pagal numatytuosius nustatymus jie (atitinkamai) diegiami šiuose aplankuose:

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

Spustelėkite „**Browse**“ (naršyti), jei norite šias vietas pakeisti (to daryti nerekomenduojama).



Spustelėkite **Atgal** ir tęskite diegimo procesą.

Diegimas (.msi)

Paleidus .msi diegimo programą, diegimo vediklis padės jums vykdyti diegimo procedūrą.

Verslo aplinkoje rekomenduojamas .msi diegimo programos paketas. Daugiausiai dėl to, kad juo galima diegti neprisijungus ir nuotoliniu būdu, naudojant įvairius įrankius, pvz., ESET PROTECT.

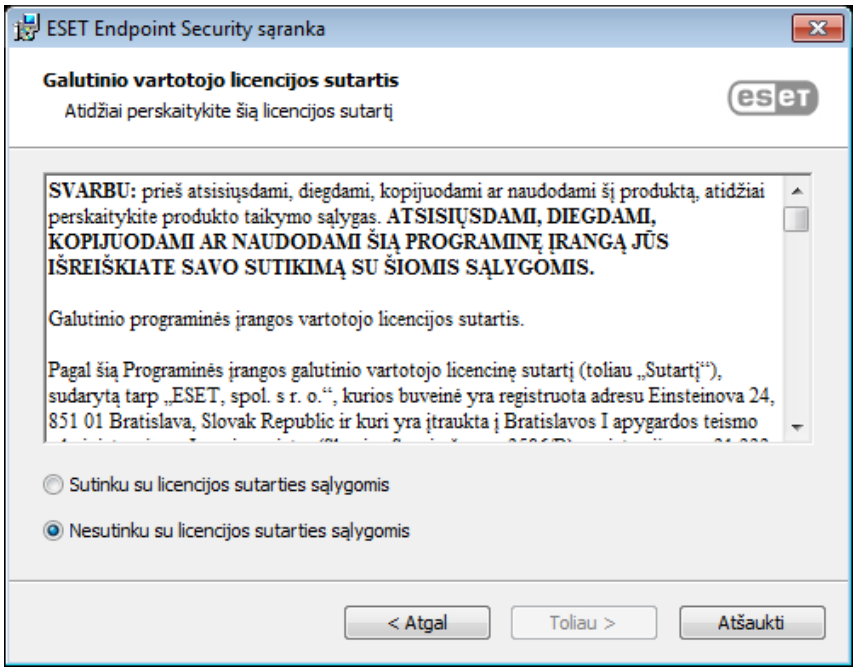
Įsitikinkite, kad kompiuteryje nėra įdiegta jokių kitų antivirusinių programų. Jeigu du arba daugiau antivirusinių sprendimų yra įdiegta viename kompiuteryje, jie gali konfliktuoti vienas su kitu. Rekomenduojame išdiegti visas kitas antivirusines programas savo sistemoje. Žiūrėkite mūsų žinių bazės straipsnį, kuriame rasite įprastinės antivirusinės programinės įrangos pašalinimo įrankių sąrašą (pateikiamas anglų ir keliomis kitomis kalbomis).

ESET Endpoint Security diegimo programa, sukurta ESET PROTECT 8.1 ir naujesnėmis versijomis, palaiko „Windows 10 Enterprise for Virtual Desktops“ ir „Windows 10“ kelių seansų režimą.

1. Pasirinkite pageidaujamą kalbą ir spustelėkite **Kitas**.

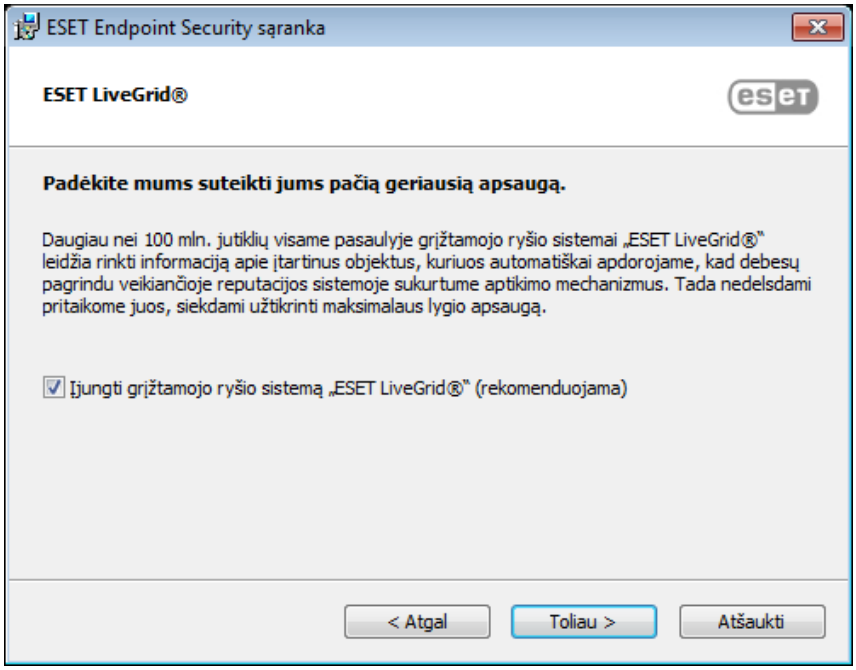


2. Perskaitykite galutinio vartotojo licencijos sutartį ir spustelėkite **Sutinku su licencinės sutarties sąlygomis**, kad patvirtintumėte, jog sutinkate su galutinio vartotojo licencijos sutartimi. Sutikę su sąlygomis, spustelėkite **Toliau**, kad tęstumėte diegimo procesą.



3. Jei norite, įjunkite ESET LiveGrid® atsiliepimų sistemą. ESET LiveGrid® padeda užtikrinti, kad ESET būtų nedelsiant ir nuolat informuojama apie naujus įsiskverbimus, o tai leidžia mums geriau apsaugoti savo

klientus. Sistema leidžia pateikti naujas grėsmes ESET virusų laboratorijai, kurioje jos analizuojamos, apdorojamos ir įtraukiamos į aptikimo variklį. Spustelėkite **Išplėstiniai nustatymai**, nei norite tęsti Išplėstinį diegimą (.msi).



5. Galutinis žingsnis – patvirtinti diegimą spustelint **Diegti**. Baigus diegti, būsite paraginti aktyvinti ESET Endpoint Security.

Išplėstinis diegimas (.msi)

Išplėstinio diegimo metu atsiranda galimybė tinkinti įvairius diegimo parametrus, kurie būna nepasiekiami vykdant tipinį diegimo procesą.

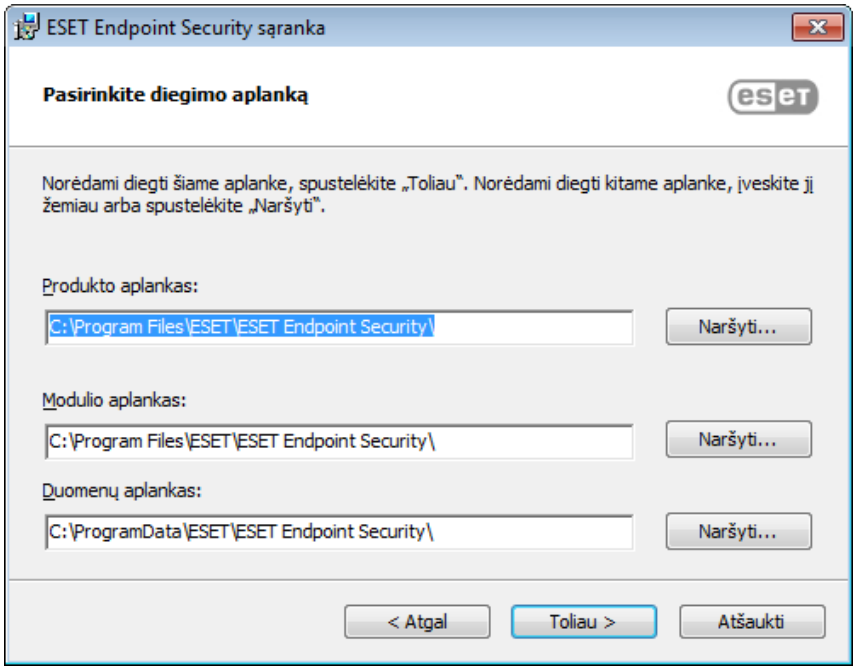
5. Pasirinkus galimas nepageidaujamas taikomąsias programas aptikimo funkciją ir spustelėjus **Išplėstiniai parametrai**, bus pateiktas siūlymas pasirinkti produkto ESET Endpoint Security diegimo aplanką. Pagal numatytuosius nustatymus programa diegiama šiame kataloge:

C:\Program Files\ESET\ESET Security

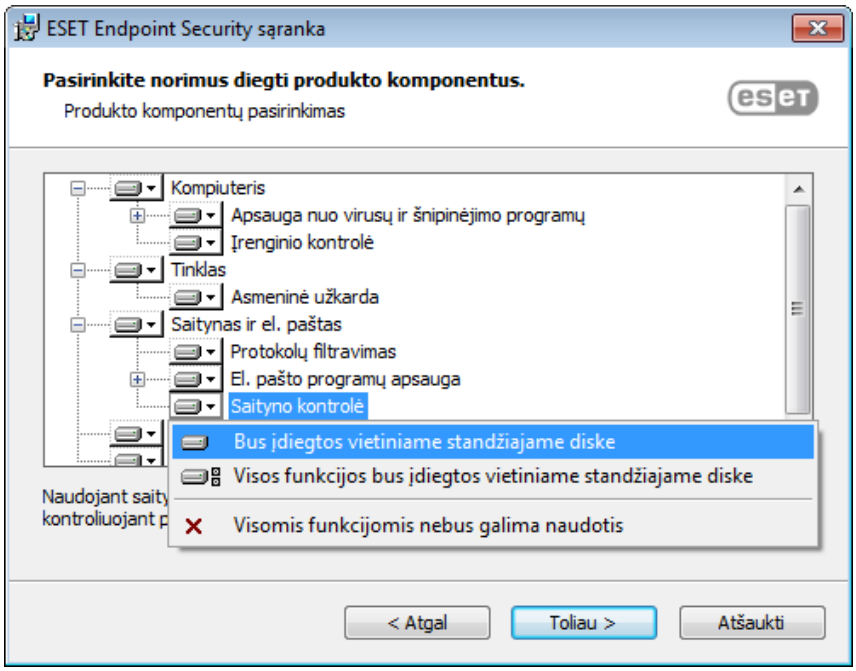
Galite nurodyti vietą, skirtą programos moduliams ir duomenims. Pagal numatytuosius nustatymus jie (atitinkamai) diegiami šiuose aplankuose:

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

Spustelėkite „**Browse**“ (naršyti), jei norite šias vietas pakeisti (to daryti nerekomenduojama).



6. Pasirinkite, kuriuos produkto komponentus įdiegti. Produkto komponentai, esantys skyriuje Kompiuteris: failų sistemos apsauga realiuoju laiku, kompiuterio nuskaitymas, dokumento apsauga ir įrenginio kontrolė. Atminkite: du pirmieji komponentai yra privalomi, kad jūsų saugumo sprendimas veiktų tinkamai. Skyriuje Tinklas yra parinktis įdiegti ESET užkardą, kuri stebi visą priimamą ir išsiunčiamą tinklo srautą ir taiko taisykles atskiriems tinklo ryšiams. Be to, užkarda saugo nuo atakų iš nuotolinių kompiuterių. Apsauga nuo atakos iš tinklo (IDS) analizuoja tinklo srauto turinį ir saugo nuo atakų iš tinklo. Blokuojamas bet koks žalingu laikomas turinys. Skyriuje Saitynas ir el. paštas esantys komponentai saugo jus naršant internete ir bendraujant el. paštu. Komponentas Naujinimo veidrodis gali būti naudojamas kitiems jūsų tinklo kompiuteriams atnaujinti. Nuotolinis stebėjimas ir valdymas (RMM) yra programinės įrangos sistemų priežiūros ir valdymo procesas, naudojant vietoje įdiegtą agentą, kurį gali pasiekti valdymo paslaugų teikėjas.



7. Galutinis žingsnis – patvirtinti diegimą spustelint **Diegti**.

Minimalus modulių diegimas

Siekiant sumažinti tinklo duomenų srautą, susijusį su diegimo priemonės dydžiu, ir sutaupyti išteklių, ESET pateikiama su minimalu modulių diegimu. Diegimo priemonėje yra tik pagrindiniai moduliai, o visi kiti moduliai bus atsisiųsti pradinio modulio naujinimo metu po produkto aktyvinimo. Pagrindinis privalumas – gerokai mažesnė diegimo priemonė ir ESET Endpoint Security atsisiunčia tik naujausius programos modulius, kai aktyvinate produktą.

Minimalaus modulių diegimo priemonėje yra šie moduliai:

- Įkelties programos
- Apsaugos nuo slaptųjų virusų palaikymo modulis
- Tiesioginio ryšio su debesimi modulis
- Vertimo palaikymo modulis
- Konfigūravimo modulis
- SSL modulis

Suaktyvinę produktą, matysite **apsaugos inicijavimo** būseną, kuri informuos apie inicijuojamas funkcijas.

Jei kyla problemų dėl modulių atsisiuntimo (pvz., tarpinio serverio nustatymų, tinklo nebuvimo ir pan.), rodoma įspėjamoji programos būsena **Reikia atkreipti dėmesį**. Pagrindiniame programos lange spustelėkite **Naujinti** > **Ieškoti naujinimų**, kad vėl pradėtumėte naujinimo procesą.

Po kelių nesėkmingų bandymų rodoma raudona programos būsena **Apsaugos nustatyti nepavyko**.

Jei kliento kompiuteriuose nėra interneto ryšio arba jie veikia neprisijungę ir jiems reikia atnaujinimų, norėdami atsisiųsti naujinimo failus iš ESET naujinimo serverių, naudokite šiuos metodus:
- Naujinimas iš veidrodinio atspindžio
- Veidrodžio įrankio naudojimas

Jei inicijavimo procesas nepavyksta ir vis tiek negalite atsisiųsti modulių, atsisiųskite visas MSI diegimo programas čia.

Diegimas naudojant komandinę eilutę

Galite diegti ESET Endpoint Security vietoje, naudodami komandinę eilutę arba diegti nuotoliniu būdu, naudodami kliento užduotį iš ESET PROTECT.

Palaikomi parametrai

APPDIR =<path>

- Path – galiojantis aplanko kelias
- Taikomosios programos diegimo aplankas.

APPDATADIR=<path>

- Path – galiojantis aplanko kelias
- Taikomosios programos duomenų diegimo aplankas.

MODULEDIR=<path>

- Path – galiojantis aplanko kelias
- Modulio diegimo aplankas.

ADDLOCAL=<list>

- Komponento diegimas – neprivalomų funkcijų, kurios diegiamos lokaliai, sąrašas.
- Naudojimas su ESET .msi paketais: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Daugiau informacijos apie **ADDLOCAL** ypatybę rasitehttp://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<list>

- Sąrašas ADDEXCLUDE yra kableliais atskirtas sąrašas su visų neįdiegtų funkcijų pavadinimais, pakeičiantis pasenusį REMOVE.
- Pasirinkus nediegti funkcijos, visas kelias (t.y., visos jos antrinės funkcijos) ir susijusios nematomos funkcijos turi būti aiškiai nurodytos sąraše.
- Naudojimas su ESET .msi paketais: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

ADDEXCLUDE negalima naudoti kartu su **ADDLOCAL**.

Žr. dokumentus, skirtus **msiexec** versijai, naudojamai atitinkamiems komandinės eilutės jungikliams.

Taisyklės

- **ADDLOCAL** sąrašas yra kableliais atskirtas visų funkcijų, kurios tui būti įdiegtos, vardų sąrašas.
- Kai pasirenkama diegiama funkcija, visas kelias (visos pirminės funkcijos) turi būti aiškiai įtrauktas į sąrašą.
- Žiūrėkite papildomas teisingo naudojimo taisykles.

Komponentai ir funkcijos

Komponentų diegimas naudojant ADDLOCAL/ADDEXCLUDE parametrus neveiks su ESET Endpoint Antivirus.

Funkcijos suskirstytos į 4 kategorijas:

- **Privaloma** – funkcija visada diegiama.
- **Pasirinktinė** – funkcijos galima atsisakyti ir nediegti.
- **Nematoma** – loginė funkcija, būtina, kad kitos funkcijos galėtų tinkamai veikti
- **Vietos rezervavimo ženklas** – funkcija, neturinti įtakos produktui, tačiau turi būti sąraše su papildomomis funkcijomis

ESET Endpoint Security funkcijų rinkinį sudaro:

Aprašymas	Funkcijos pavadinimas	Pirminė funkcija	Buvimas
Pagrindiniai programos komponentai	`Computer`		Vietos rezervavimo ženklas
Aptikimo modulis	`Antivirus`	`Computer`	Privalomas

Aprašymas	Funkcijos pavadinimas	Pirminė funkcija	Buvimas
Aptikimo modulis / kenkėjiškos programinės įrangos nuskaitymas	Scan	Computer	Privalomas
Aptikimo modulis / failų sistemos apsaugai realiuoju laiku	RealtimeProtection	Computer	Privalomas
Aptikimo modulis / kenkėjiškos programinės įrangos nuskaitymas / dokumentų apsauga	DocumentProtection	Antivirus	Pasirenkama
Įrenginio kontrolė	DeviceControl	Computer	Pasirenkama
Tinklo apsauga	Network		Vietos rezervavimo ženklas
Tinklo apsauga / užkarda	Firewall	Network	Pasirenkama
Tinklo apsauga / tinklo apsauga nuo atakų / ...	IdsAndBotnetProtection	Network	Pasirenkama
Saugi naršyklė	OnlinePaymentProtection	WebAndEmail	Pasirenkama
Saitynas ir el. paštas	WebAndEmail		Vietos rezervavimo ženklas
Žiniatinklis ir el. paštas / protokolų filtravimas	ProtocolFiltering	WebAndEmail	Nematoma
Saitynas ir el. paštas / prieigos prie saityno apsauga	WebAccessProtection	WebAndEmail	Pasirenkama
Saitynas ir el. paštas / el. pašto programų apsauga	EmailClientProtection	WebAndEmail	Pasirenkama
Žiniatinklis ir el. paštas / el. pašto kliento apsauga / el. pašto klientai	MailPlugins	EmailClientProtection	Nematoma
Saitynas ir el. paštas / el. pašto programų apsauga / apsauga nuo brukalo	Antispam	EmailClientProtection	Pasirenkama
Saitynas ir el. paštas / saityno kontrolė	WebControl	WebAndEmail	Pasirenkama
Įrankiai / ESET RMM	Rmm		Pasirenkama
Naujinimas / profiliai / naujinimo veidrodinis atspindys	UpdateMirror		Pasirenkama
„ESET Inspect“ papildinys	EnterpriseInspector		Nematoma

Grupės funkcijų rinkinys:

Aprašymas	Funkcijos pavadinimas	Funkcijos buvimas
Visos privalomos funkcijos	_Base	Nematoma
Visos galimos funkcijos	ALL	Nematoma

Papildomos taisyklės

- Jei kuri nors **WebAndEmail** funkcija pasirenkama diegti, į sąrašą turi būti įtraukta ir nematoma **ProtocolFiltering** funkcija.
- Visų funkcijų pavadinimų didžiosios ir mažosios raidės yra skiriamos, pavyzdžiui UpdateMirror nėra tas pats, kas UPDATEMIRROR.

Konfigūracijos ypatybių sąrašas

Ypatybė	Vertė:	Funkcija
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – išjungta 1 – įjungta	PUA aptikimas
CFG_LIVEGRID_ENABLED=	Žr. toliau	Žr. „LiveGrid“ ypatybę toliau
FIRSTSCAN_ENABLE=	0 – išjungta 1 – įjungta	Suplanuokite ir vykdykite Kompiuterio nuskaitymas po įdiegimo
CFG_PROXY_ENABLED=	0 – išjungta 1 – įjungta	Įgaliotojo serverio parametrai
CFG_PROXY_ADDRESS=	<ip>	Tarpinio serverio IP adresas
CFG_PROXY_PORT=	<port>	Tarpinio serverio prievado numeris
CFG_PROXY_USERNAME=	<username>	Atpažinimo vartotojo vardas
CFG_PROXY_PASSWORD=	<password>	Atpažinimo slaptažodis
ACTIVATION_DATA=	Žr. toliau	Produkto aktyvinimas, licencijos raktas arba autonominis licencijos failas
ACTIVATION_DLG_SUPPRESS=	0 – išjungta 1 – įjungta	Kai nustatyta „1“, nerodyti produkto aktyvinimo lango po pirmojo paleidimo
ADMINCFG=	<path>	Kelias į eksportuotą XML konfigūraciją (numatytoji vertė *cfg.xml*)

Konfigūravimo ypatybės tik ESET Endpoint Security

CFG_EPFW_MODE=	0 – automatinė (numatytoji) 1 – interaktyvi 2 – grįsta politika 3 – mokomoji	Užkarda filtravimo režimas
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Mokomojo režimo pabaigos data kaip „Unix“ laiko žyma

LiveGrid® ypatybė

Diegiant ESET Endpoint Security su CFG_LIVEGRID_ENABLED produkto elgesys po įdiegimo bus:

Funkcija	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
„ESET LiveGrid®“ reputacijos sistema	Įjungta	Įjungta
Atgalinio ryšio sistema „ESET LiveGrid®“	Išjungta	Įjungta
Pateikti anoniminę statistiką	Išjungta	Įjungta

Ypatybė ACTIVATION_DATA

Formatas	Būdas
`ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`	Aktyvinimas naudojant ESET licencijos raktą (turi būti aktyvus interneto ryšys)
`ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf`	Aktyvinimas naudojant autonominį licencijos failą

Kalbos ypatybės

ESET Endpoint Security kalba (būtina nurodyti abi ypatybes).

Ypatybė	Vertė:
`PRODUCT_LANG=`	LCID dešimtainis skaičius (lokalės ID), pvz., 1033 anglų k. (JAV), žr. kalbų kodų sąrašą.
`PRODUCT_LANG_CODE=`	LCID eilutė (kalbos kultūros pavadinimas) mažosiomis raidėmis, pvz., en-us anglų k. (JAV), žr. kalbos kodų sąrašą.

Paleidimo iš naujo ypatybės

Nurodykite šiuos parametrus, kad iš naujo paleistumėte kompiuterį po diegimo:

Ypatybė	Vertė:	Funkcija
`REBOOT_WHEN_NEEDED=`	0 – išjungta 1 – įjungta	Jei įjungta, po diegimo kompiuteris bus paleistas iš naujo.
`REBOOT_CANCELABLE=`	0 – išjungta 1 – įjungta	Jei įjungta, naudotojas gali atšaukti kompiuterio paleidimą iš naujo.
`REBOOT_POSTPONE=`	reikšmė sekundėmis	Didžiausias laikas sekundėmis, kad naudotojas galėtų atidėti kompiuterio paleidimą iš naujo.

REBOOT_CANCELABLE ir REBOOT_POSTPONE yra pasiekiami tik tuo atveju, jei įjungta REBOOT_WHEN_NEEDED.

Diegimo naudojant komandinę eilutę pavyzdžiai

Prieš diegdami būtinai perskaitykite Galutinio Naudotojo licencijos sutartį yra pasirūpinkite administratoriaus teisėmis.

Išskirkite **NetworkProtection** dalį iš diegimo (taip pat reikia nurodyti visas antrines funkcijas):
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

Jei norite, kad ESET Endpoint Security būtų automatiškai sukonfigūruota po diegimo, galite nurodyti pagrindinius konfigūravimo parametrus diegimo komandoje.
Diekite ESET Endpoint Security su įjungta ESET LiveGrid®:
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

Įdiekite į kitą diegimo katalogą, o ne į numatytąjį.
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

Įdiekite ir aktyvinkite ESET Endpoint Security naudodami savo ESET licencijos raktą.
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

Tylusis diegimas naudojant išsamų registravimą (praverčia trikčių diagnostikai) ir RMM tik su privalomais komponentais:
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

Priverstinis tylusis diegimas su nurodyta kalba.
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

Komandinės eilutės parinktys po diegimo

- ESET CMD – importuoti .xml konfigūravimo failą arba įjungti / išjungti apsaugos funkciją
- Komandinės eilutės skaitytuvas – paleiskite kompiuterio nuskaitymą iš komandinės eilutės

Diegimas naudojant GPO arba SCCM

Be diegimo ESET Endpoint Security tiesiogiai kliento darbo vietoje, taip pat galite diegti naudodami valdymo įrankius, pvz., grupinės politikos objektą (GPO), programinės įrangos centro konfigūravimo tvarkytuvę (SCCM), Symantec Altiris arba Puppet.

Valdomas (rekomenduojama)

Valdomam kompiuteriui pirmiausia įdiegiame ESET Management agentą, tada diegiame ESET Endpoint Security per ESET PROTECT. ESET PROTECT reikia diegti tinkle.

1. Atsisiųskite atskirą diegimo programą ESET Management agentui.
2. Paruoškite GPO/SCCM nuotolinio diegimo scenarijų.
3. Įdiekite ESET Management agentą, naudodami GPO arba SCCM.
4. Įsitikinkite, kad kliento kompiuteriai jau įtraukti į ESET PROTECT.
5. Įdiekite ir aktyvinkite ESET Endpoint Security savo kliento kompiuteriuose.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Įdiekite ESET valdymo agentą per SCCM arba GPO
- „ESET Management Agent“ visuotinis diegimas naudojant grupinės politikos objektą (GPO)

Nevaldomas

Nevaldomiems kompiuteriams galite diegti ESET Endpoint Security tiesiai kliento darbo vietose. Tai nerekomenduojama, nes negalėsite stebėti ir taikyti politikų visiems savo ESET įrenginių produktams darbo stotyse.

Pagal numatytuosius nustatymus ESET Endpoint Security neaktyvinama po diegimo, todėl ji neveikia.

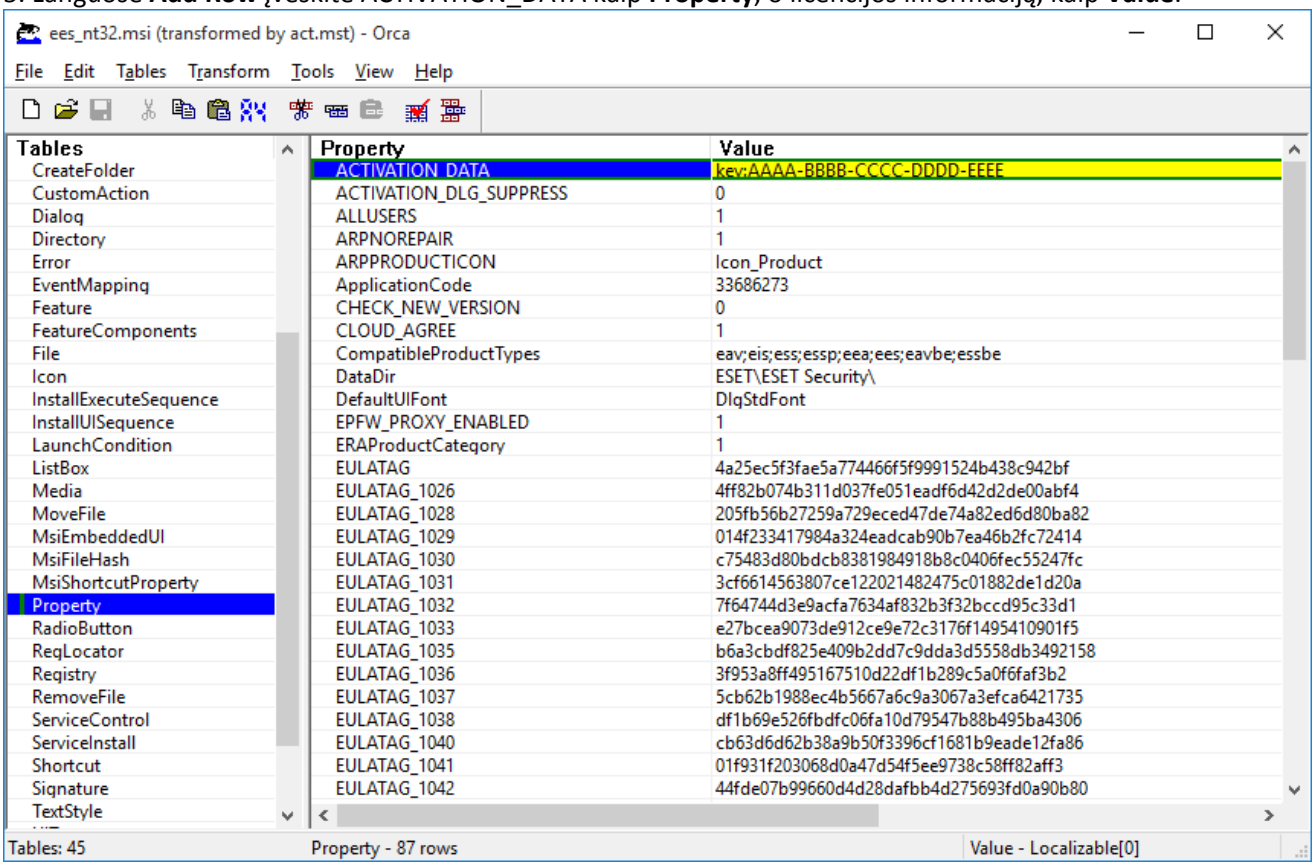
1 būdas (programinės įrangos diegimas)

1. Atsisiųskite .msi diegimo programą, skirtą ESET Endpoint Security.
2. Sukurkite .mst transformavimo paketą iš .msi failo (pvz., naudodami Orca .msi redagavimo programą), kad

įtrauktumėte produkto aktyvinimo ypatybę (žr. ACTIVATION_DATA dalyje Diegimas naudojant komandinę eilutę).

Rodyti .mst kūrimo „Orca“ aplinkoje veiksmus

1. Atidaryti Orca.
2. Įkelkite .msi diegimo programą spustelėdami **File** > **Open**.
3. Spustelėkite **Transform** > **New Transform**.
4. Spustelėkite **Property** dalyje **Tables** ir meniu **Tables** > **Add row**.
5. Languose **Add Row** įveskite ACTIVATION_DATA kaip **Property**, o licencijos informaciją, kaip **Value**.



6. Spustelėkite **Transformuoti** > **Generuoti transformaciją**, kad įrašytumėte .mst failą.

1. Pasirenkama: norėdami importuoti savo tinkintą ESET Endpoint Security .xml konfigūracijos failą (pvz., kad įgalintumėte RMM arba konfigūruotumėte tarpinio serverio parametrus), perkelkite cfg.xml failą į tą pačią vietą, kur yra .msi diegimo programa.
2. Įdiekite .msi diegimo programą su .mst failu nuotoliniu būdu, naudodami vieną iš šių būdų – GPO (naudodami Programinės įrangos diegimą) arba SCCM.

2 būdas (naudojant suplanuotą užduotį)

1. Atsisiųskite .msi diegimo programą, skirtą ESET Endpoint Security.
2. Paruoškite Diegimo naudojant komandinę eilutę scenarijų ir įtraukite į jį produkto aktyvinimo ypatybę (žr. ACTIVATION_DATA).
3. Suteikite prieigą prie .msi diegimo programos ir .cmd scenarijaus tinkle visoms darbo vietoms.
4. Pasirenkama: norėdami importuoti savo tinkintą ESET Endpoint Security .xml konfigūracijos failą (pvz., kad įgalintumėte RMM arba konfigūruotumėte tarpinio serverio parametrus), perkelkite cfg.xml failą į tą pačią vietą, kur yra .msi diegimo programa.
5. Pritaikykite paruoštą diegimo naudojant komandinę eilutę naudodami GPO arba SCCM.

    - GPO naudokite Grupinės politikos nuostatos > Grupinės politikos suplanuotos užduotys >

Skubi užduotis

Jei nenorite naudoti ESET PROTECT nuotoliniam savo ESET įrenginių produktų valdymui, ESET Endpoint Security turi ESET priedą RMM suteikiantį galimybę prižiūrėti ir kontroliuoti programinė įrangos sistemas, naudodami vietoje įdiegtą agentą, kurį gali pasiekti valdymo paslaugų teikėjas.
• Daugiau informacijos rasite

Naujinimas į naujesnę versiją

Naujos ESET Endpoint Security versijos yra išleidžiamos įvedus patobulinimus arba išsprendus problemas, kurių negalima išspręsti automatiškai atnaujinant programos modulius.

Atnaujinti į naujesnę versiją galima keliais būdais:

1. Automatiškai, naudojant ESET PROTECT arba ESET PROTECT Cloud. ESET Endpoint Security 9 versijos negali valdyti ESET Remote Administrator.
2. Automatiškai, naudojant GPO arba SCCM.
3. Automatiškai atliekant programos naujinimą.
   Kadangi programos naujinimai yra pateikiami visiems vartotojams ir gali turėti įtakos tam tikroms sistemų konfigūracijoms, jie išleidžiami atlikus ilgalaikius tikrinimus, kurie užtikrina programos veikimą visose galimose sistemos konfigūracijose. Jei norite išplėtoti programą į naujesnę versiją iš karto po jos išleidimo, taikykite vieną iš toliau pateiktų metodų.
   Įsitikinkite, kad įjungėte **Naujinimo režimą** dalyje **Išplėstinis nustatymas** (F5) > **Naujinimas** > **Profiliai** > **Produkto naujinimai**.
4. Rankiniu būdu atsisiunčiant ir įdiegiant naujesnę versiją vietoj ankstesnės.

Rekomenduojami naujinimo scenarijai

Aš valdau arba noriu valdyti savo ESET produktus nuotoliniu būdu

Jei valdote daugiau nei 10 „ESET Endpoint“ produktų, apsvarstykite tvarkyti atnaujinimus naudodami ESET PROTECT, ESET PROTECT Cloud.

Skaitykite šiuos dokumentus:

- ESET PROTECT | Atnaujinti ESET programinę įrangą per kliento užduotį
- ESET PROTECT | Mažų ir vidutinio dydžio įmonių vadovas, kaip valdyti iki 250 „Windows“ ESET įrenginio produktų
- Įvadas į ESET PROTECT Cloud

Versijų naujinimas rankiniu būdu kliento darbo vietoje

Nediekite 9 versijos iš 4.x versijos, taip pat, jei turite senesnę / neveikiančią ESET Endpoint Security 5.x ar 6.x versiją.

Jei ketinate patys naujinti versijas atskirose kliento darbo vietose:

1. Patikrinkite, ar jūsų operacinė sistema yra palaikoma Windows Vista ir Windows XP nepalaikoma versijoje.

2. Atsisiųskite ir įdiekite naujesnę versiją nei ankstesnė.

Jei norite kuo labiau padidinti sėkmingo atnaujinimo į naujausią 9.x versiją tikimybę, atnaujinkite iš vienos iš šių ESET Endpoint Security versijų:
• 5.0.2272.x
• 6.5.2132.x
• 2044 m. 7.3.x
Kitu atveju iš pradžių išdiekite ESET Endpoint Security. Papildomos informacijos apie ESET Endpoint Security versijos naujinimą kliento darbo vietoje ieškokite šiame ESET žinių bazės straipsnyje.

Saugos ir stabilumo atnaujinimai

ESET Endpoint Security Atnaujinimas yra svarbiausia visiškos apsaugos nuo kenkėjiškų kodų išlaikymo dalis. Kiekviena nauja ESET Endpoint Security versija pasižymi patobulinimais ir ištaisytomis klaidomis. Labai rekomenduojame periodiškai atnaujinti ESET Endpoint Security, kad būtumėte apsaugoti nuo saugos pažeidžiamumo ir grėsmių. ESET Endpoint Security, kaip ir bet kurie kiti ESET produktai, tinka konkrečiam produkto gyvavimo ciklo etapui.

Skaityti išsamiau apie:
Gyvavimo pabaigos politika (produktai įmonėms)
Produkto naujinimai
Skubūs saugos ir stabilumo taisymai
Daugiau informacijos apie ESET Endpoint Security pakeitimus, skaitykite ESET žinių bazės straipsnyje.

Automatiniai naujinimai užtikrina maksimalią jūsų produkto saugą ir stabilumą. Saugos ir stabilumo naujinimų išjungti negalima.

Dažniausios diegimo problemos

Jei diegiant kyla problemų, peržiūrėkite mūsų sudarytą dažniausių diegimo klaidų ir sprendimų sąrašą, kuriame galbūt rasite savo problemos sprendimą.

Suaktyvinti nepavyko

Jei nepavyko aktyvinti ESET Endpoint Security, labiausiai tikėtini scenarijai yra:

- Licencijos raktas jau naudojamas
- Neteisingas licencijos raktas. Produkto aktyvinimo formos klaida
- Trūksta aktyvinant reikalingos papildomos informacijos arba ji negaliojanti
- Ryšys su aktyvinimo duomenų baze nutrūko. Bandykite aktyvinti dar kartą po 15 minučių
- Nėra ryšio su ESET aktyvinimo serveriais arba ryšys išjungtas

Įsitikinkite, kad įvedėte tinkamą Licencijos raktą arba prisegėte tinkamą Autonominę licenciją ir bandykite aktyvinti dar kartą.

Jei negalite aktyvinti mūsų sutikimo paketas jums padės išspręsti dažniausius aktyvinimo ir licencijavimo klausimus, klaidas, problemas (pateikiama anglų ir keliomis kitomis kalbomis).

- Paleisti ESET produkto aktyvinimo trikčių diagnostiką

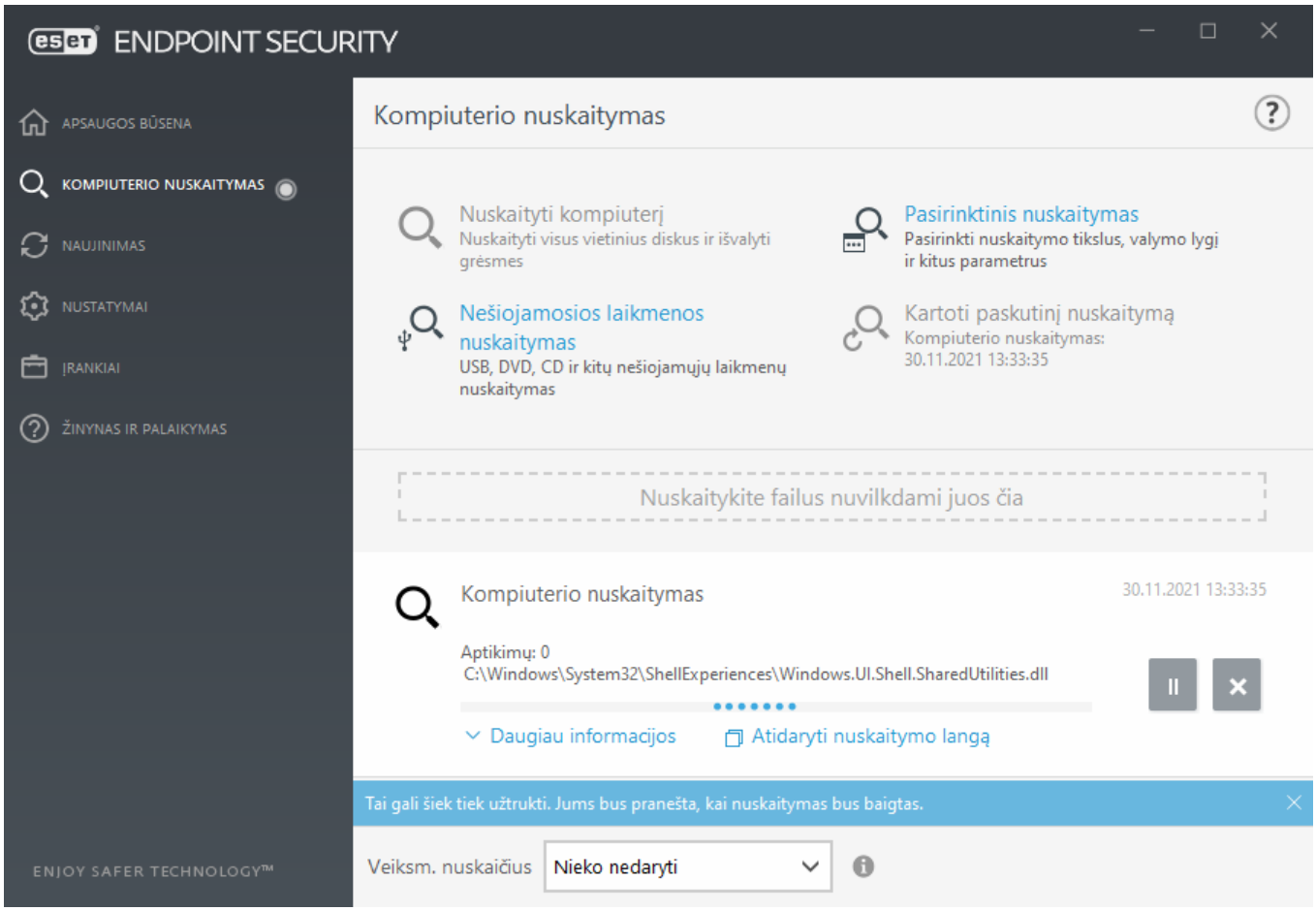
Produkto aktyvinimas

Baigus diegti jums bus pasiūlyta suaktyvinti savo produktą.

Pasirinkite vieną iš galimų metodų, kad suaktyvintumėte ESET Endpoint Security. Žr. Kaip suaktyvinti ESET Endpoint Security, kur rasite daugiau informacijos.

Kompiuterio nuskaitymas

Rekomenduojame reguliariai vykdyti kompiuterio nuskaitymus arba suplanuoti reguliarų nuskaitymą, kad būtų ieškoma grėsmių. Pagrindiniame programos lange spustelėkite **Kompiuterio nuskaitymas**, tada spustelėkite **Nuskaityti jūsų kompiuterį**. Daugiau informacijos apie kompiuterio nuskaitymus rasite skyriuje Kompiuterio nuskaitymas.



Pradedančiojo vadovas

Šiame skyriuje pateikiama bendra ESET Endpoint Security apžvalga ir pagrindiniai parametrai.

Vartotojo sąsaja

Pagrindinis ESET Endpoint Security programos langas yra padalytas į du pagrindinius skyrius. Dešinėje esantis pagrindinis langas rodo informaciją, kuri atitinka kairėje esančiame pagrindiniame meniu pasirinktą parinktį.

Čia pateikiami pagrindinio meniu parinkčių aprašai:

Apsaugos būsena – pateikia informacijos apie ESET Endpoint Security apsaugos būseną.

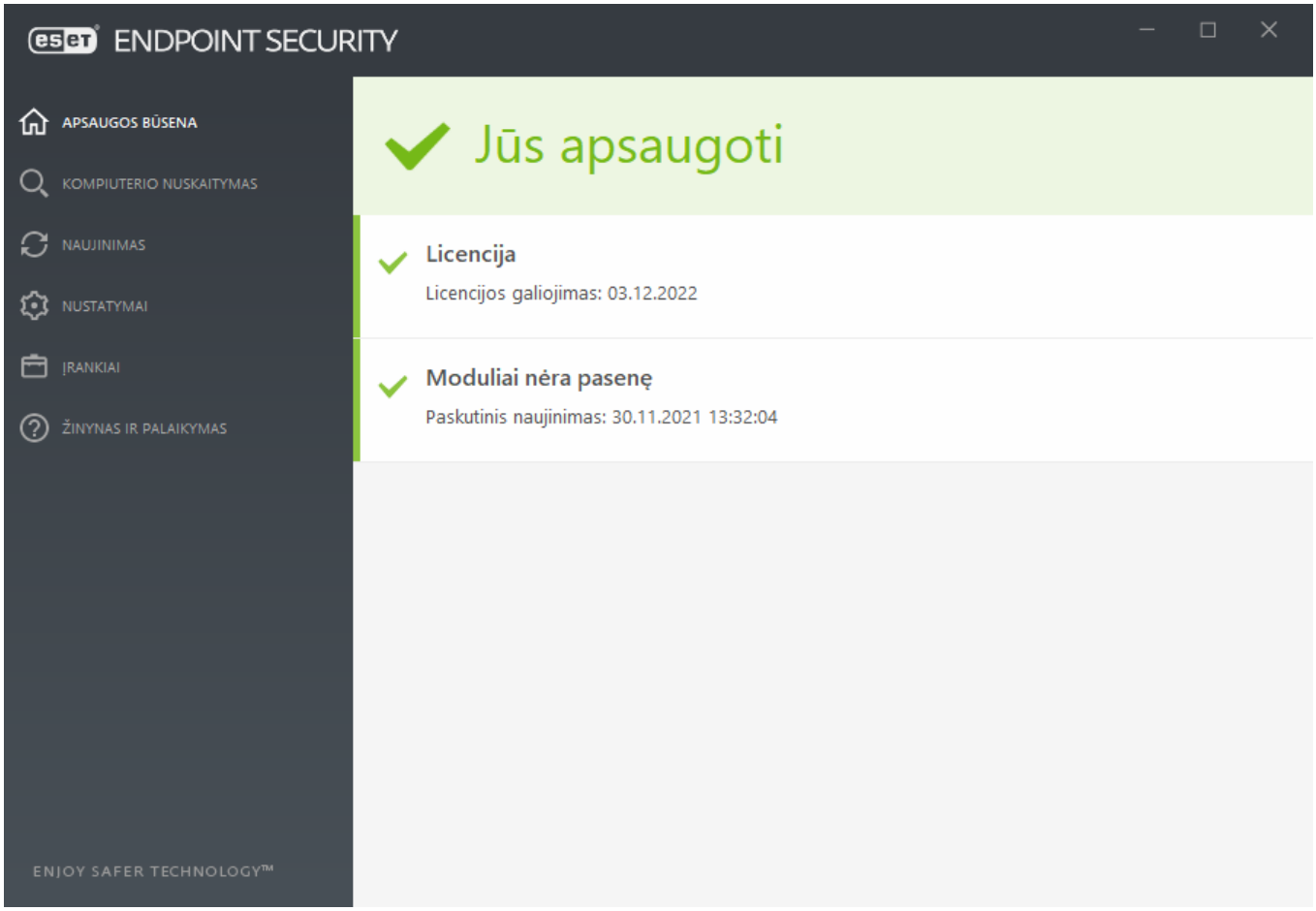
Kompiuterio nuskaitymas – šis pasirinkimas leidžia konfigūruoti ir paleisti kompiuterio nuskaitymo procesą, sukurti pasirinktinį nuskaitymą arba nešiojamosios laikmenos nuskaitymą. Taip pat galima pakartoti paskutinį vykdytą nuskaitymą.

Naujinimas – rodo informaciją apie aptikimo modulį ir suteikia galimybę rankiniu būdu tikrinti, ar yra naujinimų.

Nustatymai – nurodykite šią parinktį, kad galėtumėte pakoreguoti kompiuterio, tinklo arba saityno ir el. pašto saugumo parametrus.

Įrankiai – suteikia prieigą prie žurnalo failų, apsaugos statistikos, veiklos stebėjimo, veikiančių procesų, planuoklės, karantino, tinklo ryšių, ESET SysInspector ir ESET SysRescue, kad galėtumėte sukurti pagalbos CD. Be to, galima pateikti mėginį analizei.

Žinynas ir palaikymas – suteikia prieigą prie žinyno failų, ESET žinių bazės ir ESET bendrovės interneto svetainės. Be to, čia taip pat pateikiami saitai, skirti atverti techninės pagalbos užklausą, palaikymo įrankius ir informaciją apie produkto suaktyvinimą.

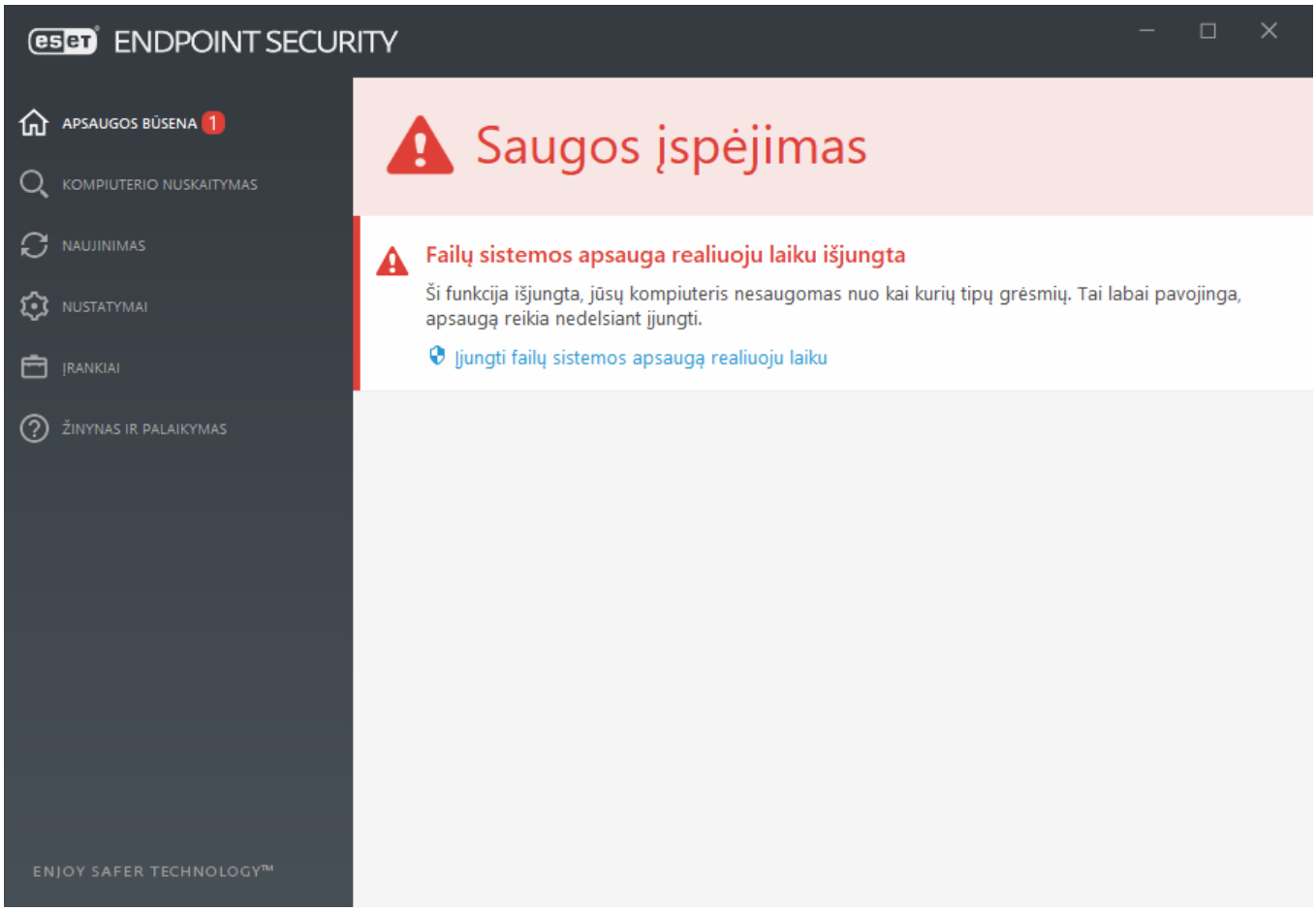


Ekrane **Apsaugos būsena** pateikiama informacijos apie jūsų kompiuterio saugumą ir esamą apsaugos lygį. Žalia **maksimalios apsaugos** būsena rodo, kad užtikrinama maksimali apsauga.

Būsenos lange papildomai pateikiama sparčiųjų saitų į dažnai naudojamas ESET Endpoint Security funkcijas bei informacijos apie paskutinį naujinimą.

Ką daryti, jeigu programa neveikia tinkamai?

Prie visų veikiančių programos modulių rodoma rodoma žalia varnelė. Jei į atitinkamą modulį reikia atkreipti dėmesį, prie jo rodomas raudonas šauktukas arba oranžinė pranešimo piktograma. Papildoma informacija apie modulį, įskaitant mūsų rekomendacijas apie tai, kaip atkurti jo veikimą, rodoma lango viršutinėje dalyje. Norėdami pakeisti modulio būseną, pagrindiniame meniu spustelėkite **Nustatymas** ir tada spustelėkite norimą modulį.



Raudona šauktuko (!) piktograma nurodo, kad maksimali jūsų kompiuterio apsauga nėra užtikrinta. Su tokiu pranešimu galite susidurti esant tokioms aplinkybėms:

- **Apsauga nuo virusų ir šnipinėjimo programų pristabdyta** – tam, kad vėl įjungtumėte apsaugą nuo virusų ir šnipinėjimo programų, spustelėkite **Paleisti visus apsaugos nuo virusų ir šnipinėjimo programų modulius** polangyje **Apsaugos būsena** arba **Įjungti apsaugą nuo virusų ir šnipinėjimo programų** polangyje **Nustatymas**, kuris yra pagrindiniame programos lange.
- Apsauga nuo virusų neveikia – inicijuoti virusų nuskaitymo programos nepavyko. Daugelis ESET Endpoint Security modulių tinkamai neveiks.
- **Apsauga nuo sukčiavimo apsimetant neveikia** – ši funkcija neveikia, nes neaktyvūs kiti būtini programos moduliai.
- **ESET užkarda išjungta** – apie šią problemą informuoja raudona piktograma ir saugumo pranešimas šalia elemento **Tinklas**. Tam, kad vėl įjungtumėte tinklo apsaugą, spustelėkite **Įjungti filtravimo režimą**.
- **Užkardos inicijuoti nepavyko** – asmeninė užkarda išjungta dėl sistemos integravimo problemų. Kuo greičiau paleiskite kompiuterį iš naujo.
- **Aptikimo modulis pasenęs** – ši klaida bus parodoma po keleto nesėkmingų bandymų atnaujinti aptikimo modulį (anksčiau vadintą virusų kodų duomenų baze). Rekomenduojame patikrinti naujinimo parametrus. Dažniausiai pasitaikanti šios klaidos priežastis yra neteisingai įvesti atpažinimo duomenys arba neteisingai

sukonfigūruoti ryšio parametrai.

- **Produktas nesuaktyvintas** arba **Licencijos galiojimas baigėsi** – apie tai praneša raudona apsaugos būsenos piktograma. Kai baigiasi licencijos galiojimas, programa negali atsinaujinti. Laikydamiesi perspėjimo lange pateikiamų instrukcijų atnaujinkite licenciją.
- **Pagrindinio kompiuterio apsaugos nuo įsilaužimo sistema (HIPS) išjungta** – ši problema nurodoma tada, kai HIPS išjungta naudojantis funkcija „Išplėstinis nustatymas“. Apsauga turi būti kuo greičiau įjungta spustelėjus **Įjungti HIPS**.
- **ESET LiveGrid® išjungta** – ši problema nurodoma tada, kai ESET LiveGrid® išjungta naudojantis išplėstiniu nustatymu.
- **Suplanuotų reguliarių naujinimų nėra** – ESET Endpoint Security netikrins, ar yra svarbių naujinių, jei nesuplanuosite naujinimo užduoties.
- **Apsauga nuo slaptųjų virusų išjungta** – tam, kad šią funkciją vėl įjungtumėte, spustelėkite **Įjungti apsaugą nuo slaptųjų virusų**.
- **Tinklo prieiga užblokuota** – rodoma, kai šios darbo vietos kliento užduotis **Izoliuoti kompiuterį nuo tinklo** paleidžiama iš ESET PROTECT. Dėl išsamesnės informacijos susisiekite su sistemos administratoriumi.
- **Failų sistemos apsauga realiuoju laiku pristabdyta** – apsaugą realiuoju laiku išjungė vartotojas. Jūsų kompiuteris neapsaugotas nuo grėsmių. Tam, kad šią funkciją vėl įjungtumėte, spustelėkite Įjungti apsaugą realiuoju laiku.

Oranžinė „i“ reiškia, kad jūsų ESET produktui reikia skirti dėmesio: reikia išspręsti nekritinę problemą. Galimos priežastys:

- **Išjungta saityno prieigos apsauga** – spustelėkite saugos pranešimą, kad iš naujo įjungtumėte saityno prieigos apsaugą, tada spustelėkite **Įjungti prieigos prie saityno apsaugą**.
- **Jūsų licencijos galiojimo laikas greitai baigsis** – apie tai praneša apsaugos būsenos piktograma su šauktuku. Kai jūsų licencijos galiojimas pasibaigia, programa nebegali atlikti naujinimų ir apsaugos būsenos piktograma pasidaro raudona.
- **Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą pristabdyta** – tam, kad šią funkciją vėl įjungtumėte, spustelėkite **Įjungti apsaugą nuo įtraukimo į užgrobtų kompiuterių tinklą**.
- **Apsauga nuo atakos iš tinklo (IDS) pristabdyta** – tam, kad šią funkciją vėl įjungtumėte, spustelėkite **Įjungti apsaugą nuo atakos iš tinklo (IDS)**.
- **Apsauga nuo brukalo pristabdyta** – tam, kad šią funkciją vėl įjungtumėte, spustelėkite **Įjungti apsaugą nuo brukalo**.
- **Saityno kontrolė pristabdyta** – tam, kad šią funkciją vėl įjungtumėte, spustelėkite **Įjungti saityno kontrolę**.
- **Aktyvus politikos nepaisymas** – politikos nustatytos konfigūracijos laikinai nepaisoma, galbūt tol, kol bus baigtas trikčių šalinimas. Nepaisyti politikos parametrų leidžiama tik įgaliotam vartotojui. Daugiau informacijos žr. Kaip naudoti nepaisymo režimą.
- **Įrenginio kontrolė pristabdyta** – tam, kad šią funkciją vėl įjungtumėte, spustelėkite **Įjungti įrenginio kontrolę**.

Norėdami pirmajame ESET Endpoint Security lange reguliuoti produktų būsenų matomumą, žr. Programos būsenos.

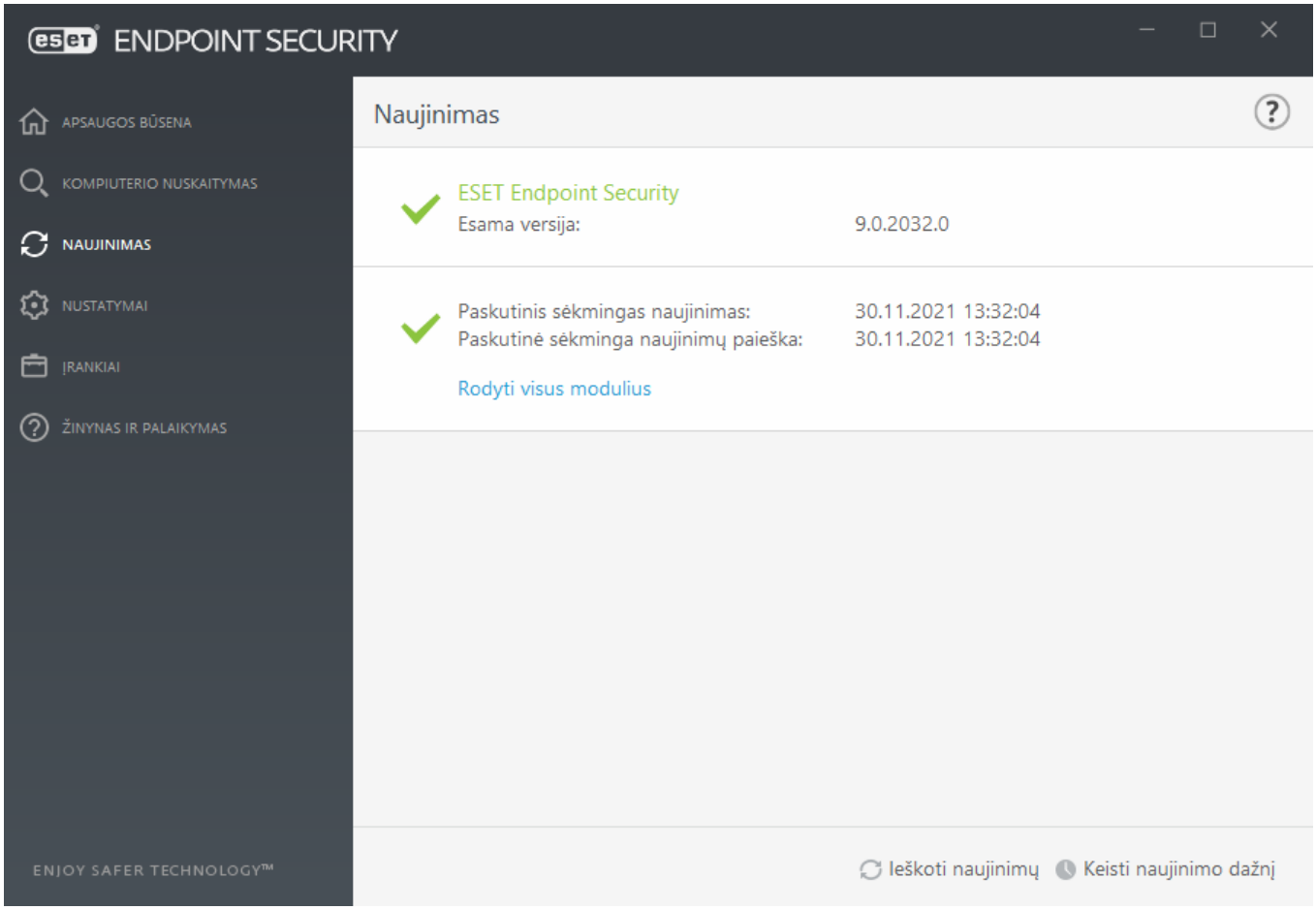
Jei nepavyksta išspręsti problemos naudojant siūlomus sprendimus, spustelėkite **Žinynas ir palaikymas**, kad galėtumėte pasinaudoti žinyno failais arba ieškoti ESET žinių bazėje. Jei vis dar reikia pagalbos, galite pateikti ESET techninės pagalbos prašymą. ESET techninės pagalbos tarnyba greitai atsakys į jūsų klausimus ir padės rasti sprendimą.

Jei būsena priklauso funkcijai, kurią ESET PROTECT politika blokuoja, nuorodos spustelėti neleidžiama.

Naujinimo nustatymai

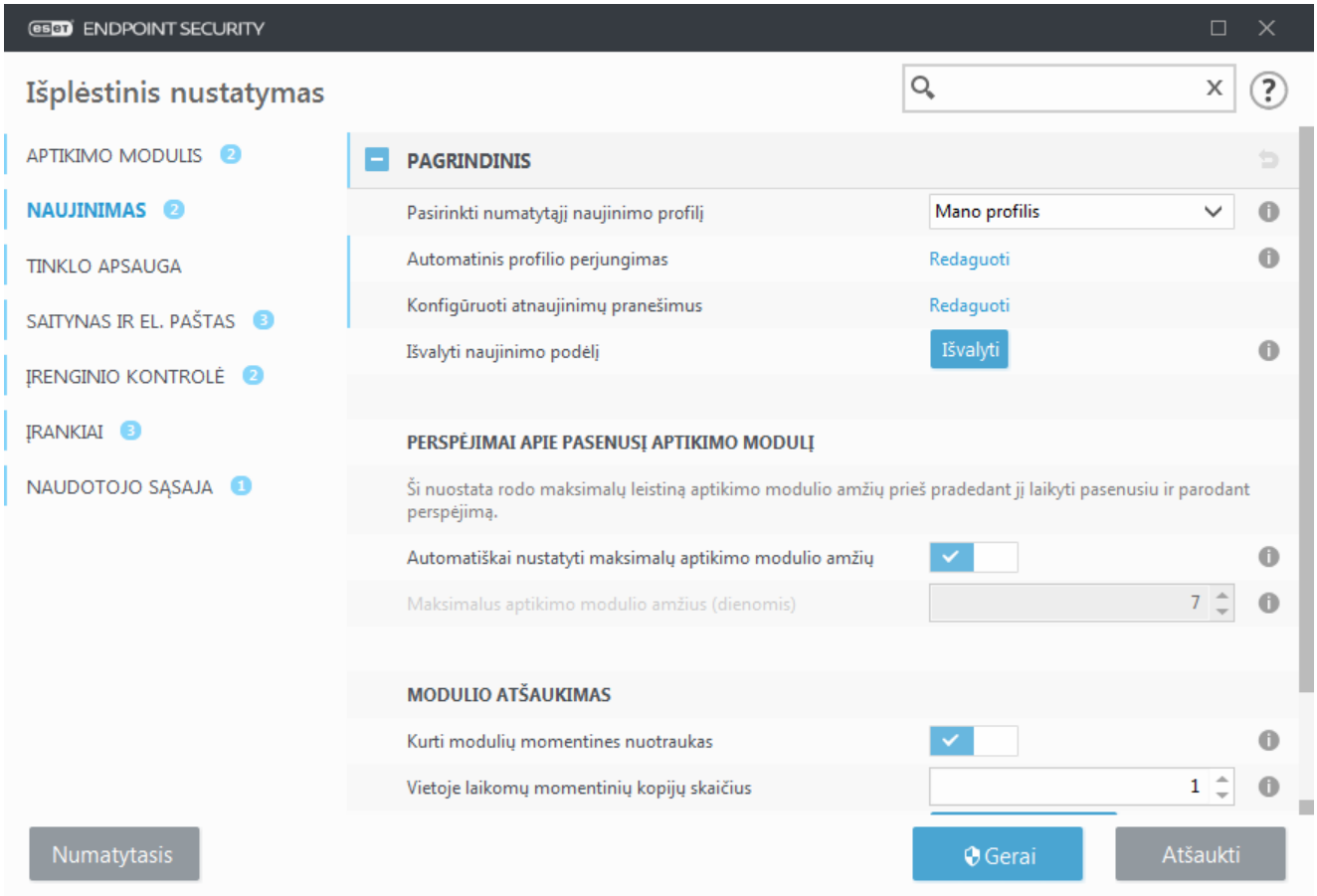
Modulių naujinimas yra svarbus norint palaikyti visišką apsaugą nuo kenkėjiškų kodų. Būtinai atkreipkite dėmesį į naujinimo konfigūraciją ir veikimą. Pagrindiniame meniu pasirinkite **Naujinimas** > **Tikrinti, ar yra naujinimų**, kad patikrintumėte, ar yra naujesnių modulio naujinimų.

Jei dar nesate įvedę **Licencijos rakto**, naujausių naujinimų negalėsite gauti ir būsite raginami suaktyvinti savo produktą.



Išplėstinio nustatymo lange (pagrindiniame meniu spustelėkite **Nustatymai** > **Išplėstiniai nustatymai arba** klaviatūroje paspauskite **F5**) pateikiama papildomų naujinimų parinkčių. Jei norite sukonfigūruoti išplėstines naujinimo parinktis, tokias kaip naujinimo režimas, įgaliotojo serverio prieiga, LAN ryšiai ir aptikimo modulio kopijos kūrimo nustatymai, nustatymo medyje Išplėstinis spustelėkite **Naujinimas**.

- Jei susiduriate su naujinimo problemomis, spustelėkite **Valyti**, kad išvalytumėte laikinųjų naujinimų podėlį.



- Parinktis **Pasirinkti automatiškai** dalyje **Profiliai** > **Naujinimai** > **Modulių naujinimai** įjungiama pagal numatytuosius nustatymus. Naudojant ESET naujinimo serverį naujinimams gauti, rekomenduojame nekeisti šio nustatymo.
- Jei nenorite, kad sėkmingo naujinimo sistemos dėklo pranešimas būtų rodomas ekrano apatiniame dešiniajame kampe, išplėskite **Profiliai** > **Naujinimai**, spustelėkite **Redaguoti** šalia **Pasirinkti gautus pranešimus apie atnaujinimą** ir atitinkamai pažymėkite pranešimo **Aptikimo modulis sėkmingai atnaujintas** žymės langelius.

Siekiant optimalaus veikimo, svarbu, kad programa būtų automatiškai atnaujinama. Tai galima atlikti, tik jei **Žinynas ir palaikymas** > **Aktyvinti produktą** įvedamas teisingas **Licencijos raktas**.

Jei įdiegę neįvedėte savo **licencijos rakto**, galite tai padaryti bet kada. Išsamesnės informacijos apie aktyvinimą ieškokite skyriuje Kaip suaktyvinti ESET Endpoint Security ir **licencijos duomenų** lange įveskite kredencialus, kuriuos gavote su ESET saugos produktu.

Zonų nustatymai

Kad jūsų kompiuteris būtų apsaugotas tinklo aplinkoje, būtina sukonfigūruoti patikimas zonas. Galite leisti kitiems naudotojams pasiekti savo kompiuterį sukonfigūruodami patikimą zoną, kurioje būtų leidžiama bendrinti. Spustelėkite **Išplėstinis nustatymas** (F5) > **Tinklo apsauga** > **Užkarda** > **Išplėstinis** > **Zonos**, kad pasiektumėte patikimų zonų parametrus.

Patikimos zonos aptikimo procedūra atliekama įdiegus ESET Endpoint Security ir visada, kai jūsų kompiuteris jungiasi prie naujo tinklo. Taigi, patikimos zonos apibrėžti paprastai nereikia. Pagal numatytuosius nustatymus aptikus naują zoną pateikiamas dialogo langas, kuris leidžia nustatyti šios zonos apsaugos lygį.



Neteisingai sukonfigūravus patikimą zoną jūsų kompiuterio saugai gali iškilti grėsmė.

Pagal numatytuosius nustatymus darbo vietoms iš patikimos zonos suteikiama prieiga prie bendrinamų failų ir spausdintuvų, leidžiamas gaunamas RPC ryšys ir nuotolinis darbalaukio bendrinimas.

Jei reikia daugiau informacijos apie šią funkciją, skaitykite šį ESET žinių bazės straipsnį:

- Aptiktas naujas tinklo ryšys ESET Endpoint Security

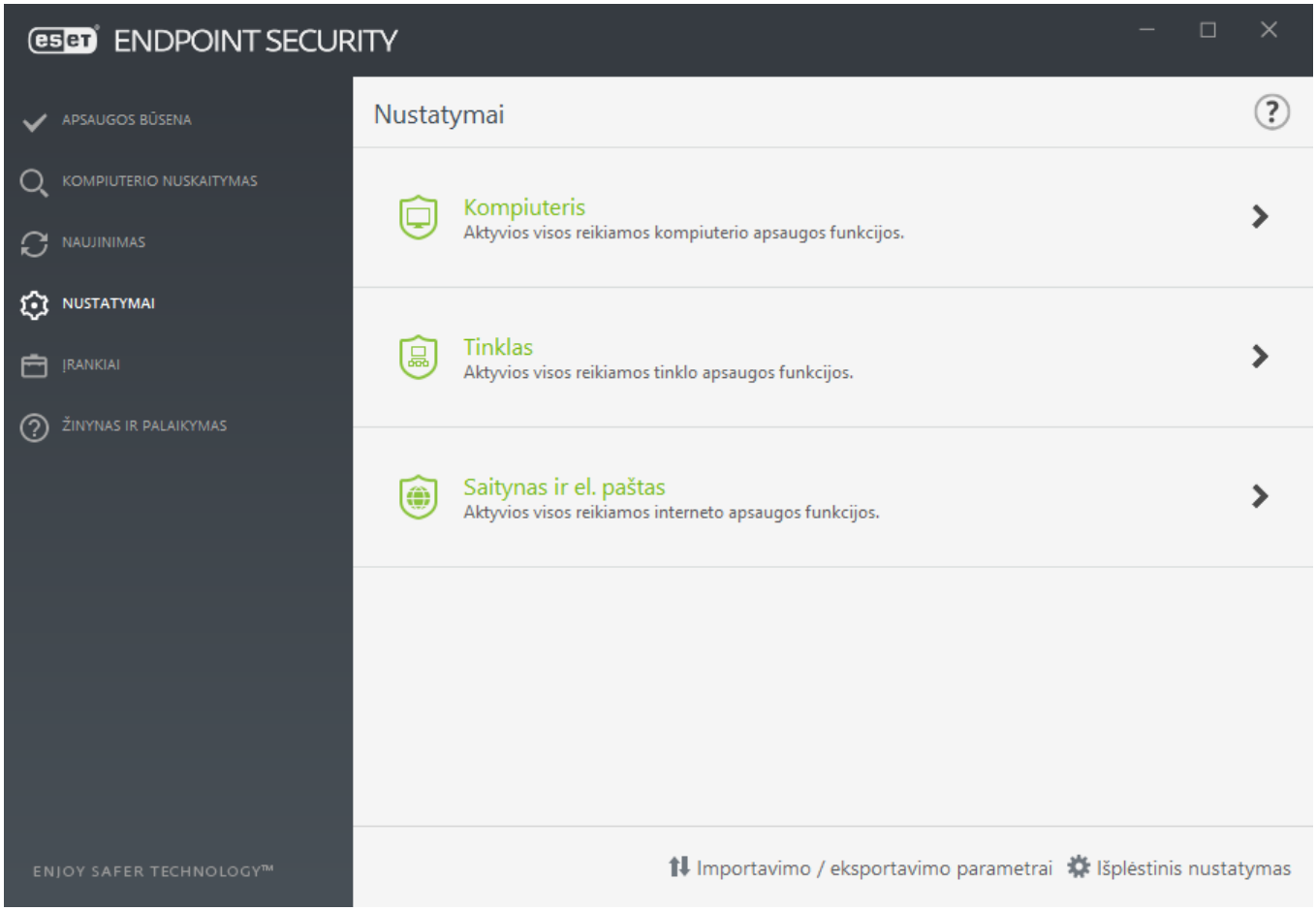
Saityno kontrolės įrankiai

Jei naudodami ESET Endpoint Security jau įjungėte saityno kontrolę, turite sukonfigūruoti ir reikiamoms vartotojų paskyroms skirtą saityno kontrolę, kad ši funkcija veiktų tinkamai. Žr. skyrių Saityno kontrolė, kur rasite instrukcijų, kaip klientų darbo stotims sukurti konkrečius apribojimus ir apsaugoti jas nuo galimai įžeidžiančio turinio.

Darbas su ESET Endpoint Security

ESET Endpoint Security nustatymų parinktys leidžia koreguoti jūsų kompiuterio, saityno, el. pašto ir tinklo apsaugos lygį.

Kai kuriate politiką iš ESET PROTECT saityno pulto, galite pasirinkti kiekvieno nustatymo vėliavėlę. Nustatymams su vėliavėle „Force“ (priversti), suteikiama pirmenybė ir jų negali perrašyti jokia vėliau pritaikyta politika (net jei ji taip pat pažymėta vėliavėle „Force“ (priversti). Taip užtikrinama, kad šis nustatymas nebus pakeistas (pvz., vartotojo arba vėliau pritaikytų politikų suliejimo metu). Daugiau informacijos rasite „ESET PROTECT“ internetinio žinyno skyriuje „Vėliavėlės“.



Meniu **Nustatymai** turi šiuos skyrius:

- **Kompiuteris**
- **Tinklas**
- **Saitynas ir el. paštas**

Dalyje Kompiuteris galima įjungti arba išjungti šiuos komponentus:

- **Failų sistemos apsauga realiuoju laiku** – visi failai atidarant, kuriant ar vykdant juos yra nuskaitomi tikrinant, ar nėra kenkėjiškų kodų.
- **Įrenginio kontrolė** – Atlieka automatinę įrenginių (CD / DVD / USB / ...) kontrolę. Šis modulis leidžia blokuoti arba koreguoti išplėstinius filtrus / teises ir pasirinkti, kaip vartotojas gali naudotis ir dirbti su nurodytais įrenginiais.
- **Host Intrusion Prevention System (HIPS)** – HIPS sistema stebi įvykius operacinėje sistemoje ir į juos reaguoja pagal pasirinktinių taisyklių rinkinį.
- **Išplėstinis atminties skaitytuvas** – veikia kartu su spragų išnaudojimo blokatoriumi ir sustiprina apsaugą nuo kenkimo programinės įrangos, kuri buvo sukurta siekiant išvengti apsaugos nuo kenkimo programinės įrangos aptikimo, pasitelkiant klaidinimo arba šifravimo priemones. Išplėstinis atminties skaitytuvas būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.
- **Įsilaužimų blokatorius** – sustiprina programas, į kurias įsilaužiama dažniausiai, pavyzdžiui, saityno naršykles, PDF skaitymo programas, el. pašto programas ir „MS Office“ komponentus. Įsilaužimų blokatorius būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.
- **Apsauga nuo „Ransomware“** – tai dar vienas apsaugos lygmuo, kuris veikia kaip HIPS funkcijos dalis. Jei norite, kad apsauga nuo „Ransomware“ veiktų tinkamai, turite įjungti ESET LiveGrid® reputacijos sistemą.

Skaitykite daugiau apie šio tipo apsaugą.

- **Pristatymo režimas** – tai funkcija, skirta vartotojams, kuriems reikalingas nepertraukiamas jų programinės įrangos veikimas, kai norima, kad netrukdytų iškylantieji langai ir būtų maksimaliai sumažinta procesoriaus apkrova. Įjungę Pristatymo režimą, gausite įspėjamąjį pranešimą (galimas saugumo pavojus), o pagrindinis programos langas pasidarys oranžinis.

Skyriuje **Tinklas** galite konfigūruoti Užkardą, apsaugą nuo atakos iš tinklo (IDS) ir Apsaugą nuo įtraukimo į užgrobtų kompiuterių tinklą.

Saityno ir el. pašto apsaugos nustatymas leidžia įjungti arba išjungti šias dalis:

- **Saugi naršyklė** – apsaugo jūsų jautrius duomenis, kai naršote internete (pavyzdžiui, finansiniai duomenys atliekant operacijas internetu).
- **Saityno kontrolė** – blokuoja tinklalapius, kuriuose gali būti galimai įžeidžiančios informacijos. Be to, sistemos administratoriai gali nurodyti prieigos pageidavimus 27 iš anksto apibrėžtoms tinklaviečių kategorijoms.
- **Prieigos prie saityno apsauga** – jeigu įjungta, visas srautas per HTTP arba HTTPS yra nuskaitomas ieškant kenkėjiškų programų.
- **El. pašto programos apsauga** – stebi ryšį, gaunamą naudojant POP3 ir IMAP protokolus.
- **Apsauga nuo brukalo** – nuskaito nepageidaujamus el. laiškus arba brukalą.
- **Apsauga nuo sukčiavimo apsimetant** – saugo nuo mėginimų gauti slaptažodžius, bankininkystės duomenis ar kitą slaptą informaciją sukuriant neteisėtas interneto svetaines, kurios apsimeta teisėtomis.

Norint laikinai išjungti atskirus modulius, reikia spustelėti žaliąjį jungiklį , esantį šalia pageidaujamo modulio. Atminkite, kad tai gali sumažinti jūsų kompiuterio apsaugos lygį.

Norint vėl įjungti išjungto saugumo komponento apsaugą, reikia spustelėti raudonąjį jungiklį ir komponentas vėl bus įjungtas.

Kai taikoma politika ESET PROTECT, prie atitinkamo komponento rodoma spynos piktograma . Politikos, kurią taiko ESET PROTECT, galima nepaisyti, jei gaunamas vietinio prisijungusio naudotojo (pvz., administratoriaus) įgaliojimas. Išsamesnės informacijos rasite ESET PROTECT internetiniame žinyne.

Visos taip išjungtos apsaugos priemonės bus vėl įjungtos paleidus kompiuterį iš naujo.

Kad pasiektumėte išsamius konkretaus saugumo komponento parametrus, spustelėkite krumpliaračio piktogramą šalia bet kurio komponento.

Nustatymo lango apačioje yra papildomos parinktys. Norėdami įkelti nustatymų parametrus iš *.xml* konfigūracijos failo arba įrašyti esamus nustatymų parametrus į konfigūracijos failą, naudokite parinktį **Parametrų importavimas / eksportavimas**. Žr. Parametrų importavimas / eksportavimas, kur rasite išsamesnės informacijos.

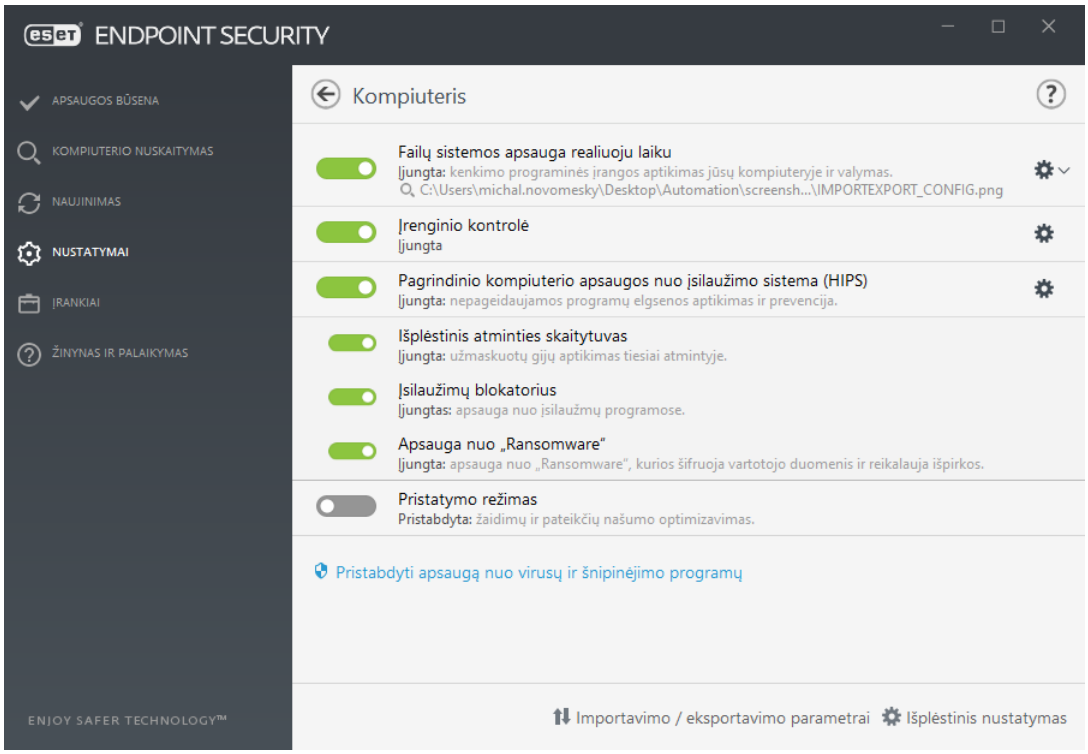
Jei norite pasirinkti išsamesnes parinktis, spustelėkite **Išplėstinis nustatymas** arba paspauskite **F5**.

Kompiuteris

Modulį **Kompiuteris** surasite skiltyje **Nustatymai** > **Kompiuteris**. Jame pateikiama ankstesniame skyriuje aprašytų apsaugos modulių apžvalga. Šiame skyriuje pasiekiami tokie parametrai:

Spustelėkite krumpliaračio piktogramą , esančią šalia punkto **Failų sistemos apsauga realiuoju laiku** ir

spustelėkite **Redaguoti išskyrimus**, kad atidarytumėte Išskyrimų nustatymų langą, kuriame galima neįtraukti failų ir aplankų į nuskaitymo procesą. Norėdami atidaryti **Failų sistemos apsaugos realiuoju laiku** išplėstinį nustatymą, spustelėkite **Konfigūruoti**.



Dalyje **Kompiuteris** galima įjungti arba išjungti šiuos komponentus:

- **Failų sistemos apsauga realiuoju laiku** – visi failai atidarant, kuriant ar vykdant juos kompiuteryje yra nuskaitomi tikrinant, ar nėra kenkėjiškų kodų.
- **Įrenginio kontrolė** – Atlieka automatinę įrenginių (CD / DVD / USB / ...) kontrolę. Šis modulis leidžia blokuoti arba koreguoti išplėstinius filtrus / teises ir pasirinkti, kaip vartotojas gali naudotis ir dirbti su nurodytais įrenginiais.
- **Host Intrusion Prevention System (HIPS)** – HIPS sistema stebi įvykius operacinėje sistemoje ir į juos reaguoja pagal pasirinktinių taisyklių rinkinį.
- **Išplėstinis atminties skaitytuvas** – veikia kartu su spragų išnaudojimo blokatoriumi ir sustiprina apsaugą nuo kenkimo programinės įrangos, kuri buvo sukurta siekiant išvengti apsaugos nuo kenkimo programinės įrangos aptikimo, pasitelkiant klaidinimo arba šifravimo priemones. Išplėstinis atminties skaitytuvas būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.
- **Įsilaužimų blokatorius** – sustiprina programas, į kurias įsilaužiama dažniausiai, pavyzdžiui, saityno naršykles, PDF skaitymo programas, el. pašto programas ir „MS Office" komponentus. Įsilaužimų blokatorius būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.
- **Apsauga nuo „Ransomware"** – tai dar vienas apsaugos lygmuo, kuris veikia kaip HIPS funkcijos dalis. Jei norite, kad apsauga nuo „Ransomware" veiktų tinkamai, turite įjungti ESET LiveGrid® reputacijos sistemą. Skaitykite daugiau apie šio tipo apsaugą.
- **Pristatymo režimas** – tai funkcija, skirta vartotojams, kuriems reikalingas nepertraukiamas jų programinės įrangos veikimas, kai norima, kad netrukdytų iškylantieji langai ir būtų maksimaliai sumažinta procesoriaus apkrova. Įjungę Pristatymo režimą, gausite įspėjamąjį pranešimą (galimas saugumo pavojus), o pagrindinis programos langas pasidarys oranžinis.

Pristabdyti apsaugą nuo virusų ir šnipinėjimo programų – kai tik laikinai išjungiate apsaugą nuo virusų iš šnipinėjimo programų, galite nurodyti laikotarpį, kurį norite, kad pasirinktas komponentas būtų išjungtas. Tai

atliekama per išskleidžiamąjį meniu, spustelint **Taikyti** ir išjungiant saugumo komponentą. Jei norite vėl įjungti apsaugą, spustelėkite **Įjungti apsaugą nuo virusų ir šnipinėjimo programų**.

Aptikimo modulis

Aptikimo modulis saugo nuo kenkėjiškų sistemos atakų, valdydamas failus, el. paštą ir interneto ryšį. Pavyzdžiui, jei aptinkamas objektas, klasifikuojamas kaip kenkėjiška programinė įranga, prasidės valymas. Aptikimo modulis gali pašalinti ją pirmiausiai užblokuodamas, tada valydamas, pašalindamas arba perkeldamas į karantiną.

Kad išsamiai sukonfigūruotumėte aptikimo modulio parametrus, spustelėkite **Išplėstiniai nustatymai** arba paspauskite **F5**.

Šiame skyriuje:

- Apsaugos realiuoju laiku ir naudojant mašininį mokymąsi kategorijos
- Kenkėjiškų programų nuskaitymai
- Pranešimų nustatymai
- Apsaugos nustatymai
- Geriausios praktikos

> Nuo 7.2 versijos aptikimo modulio dalyje nebėra įjungimo / išjungimo jungiklių, kaip 7.1 ir senesnėse versijose. Įjungimo / išjungimo mygtukai pakeisti keturiomis ribinėmis reikšmėmis – agresyvi, subalansuota, atsargi ir išjungta.

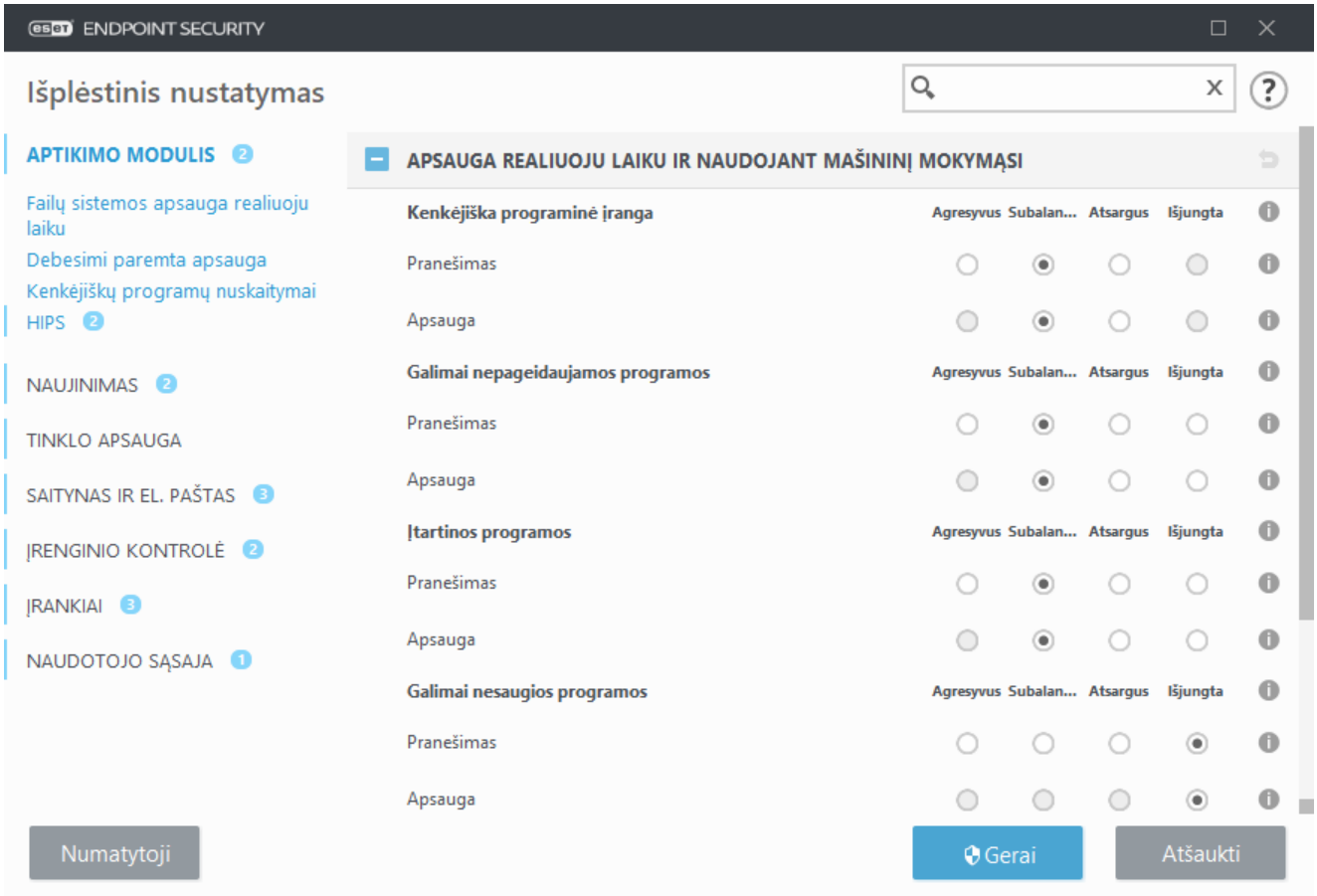
Apsaugos realiuoju laiku ir naudojant mašininį mokymąsi kategorijos

Apsauga realiuoju laiku ir naudojant mašininį mokymąsi visiems apsaugos moduliams (pvz., failų sistemos apsaugos realiuoju laiku, prieigos prie saityno apsauga, ...) leidžia konfigūruoti pranešimų ir apsaugos lygius toliau nurodytoms kategorijoms:

- **Kenkėjiška programinė įranga** – kompiuterinis virusas yra kenkėjiškas kodas, kuris yra pridedamas prie jūsų kompiuteryje esančių failų. Tačiau terminas „virusas“ dažnai naudojamas netinkamai. Tikslesnis terminas yra „kenkėjiška programinė įranga“. Kenkėjiškos programinės įrangos aptikimą vykdo aptikimo modulis kartu su mašininio mokymosi komponentu.
  Daugiau apie šiuos programų tipus skaitykite Terminų žodyne.

- **Galimas nepageidaujamas taikomąsias programas** – „Grayware“ arba potencialiai nepageidaujamos programos (PUA) yra plati programinės įrangos kategorija, kurios tikslas nėra vienareikšmiškai kenkėjiškas, kaip kitų tipų kenkėjiškos programinės įrangos, pvz., virusų ar Trojos arklių. Visgi ji gali įdiegti nepageidaujamą papildomą programinę įrangą, pakeisti skaitmeninio įrenginio veikimo būdą ar atlikti veiksmus, kurių naudotojas nepatvirtino arba nesitiki.
  Daugiau apie šiuos programų tipus skaitykite Terminų žodyne.
- **Galimai nesaugios programos**– yra teisėta komercinė programinė įranga, kuri gali būti netinkamai panaudota kenkimo tikslais. Galimai nesaugių programų (PUA) pavyzdžiais gali būti nuotolinės prieigos įrankiai, slaptažodžio iššifravimo ir klavišų registravimo programos (programos, įrašančios kiekvieną naudotojo klaviatūros klavišo paspaudimą).
  Daugiau apie šiuos programų tipus skaitykite Terminų žodyne.

- **Įtartinos programos** gali būti programos, suglaudintos pakavimo programomis arba apsaugos programomis. Šio tipo apsaugos programas yra dažnai naudojamos kenkėjiškos programinės įrangos kūrėjų, siekiant išvengti aptikimo.



Išplėstinis mašininis mokymasis dabar yra aptikimo modulio dalis, kaip išplėstinis apsaugos sluoksnis, kuriuo pagerinamas aptikimas, grindžiamas mašininiu mokymusi. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.

Kenkėjiškų programų nuskaitymai

Skaitytuvo nustatymus galima atskirai konfigūruoti nuskaitymui realiuoju laiku ir nuskaitymui pareikalavus. Pagal numatytuosius nustatymus, įgalinta nuostata **Naudoti apsaugą realiuoju laiku**. Kai jie įgalinti, susiję nuskaitymo pareikalavus nustatymai gaunami iš dalies **Apsauga realiuoju laiku ir naudojant mašininį mokymąsi**.

Pranešimų nustatymai

Aptikimo atveju (pvz, aptinkama grėsmė, klasifikuojama kaip kenkėjiška programinė įranga), informacija užfiksuojama aptikimų žurnale ir pateikiami darbalaukio pranešimai, jei sukonfigūruota ESET Endpoint Security.

Pranešimų ribinė reikšmė konfigūruojama kiekvienai kategorijai (vadinamai „KATEGORIJA“):

1. Kenkėjiška programinė įranga
2. Galimai nepageidaujamos programos
3. Galimai nesaugu
4. Įtartinos programos

Pranešimus teikia aptikimo modulis, įskaitant mašininio mokymosi komponentą. Galima nustatyti aukštesnę pranešimo ribinę reikšmę, nei dabartinė apsaugos ribinė reikšmė. Šie pranešimo nustatymai nedaro įtakos objektų blokavimui, valymui arba naikinimui.

Prieš keisdami KATEGORIJOS pranešimų ribinę reikšmę (arba lygį), perskaitykite toliau pateiktą informaciją:

Ribinė reikšmė	Paaiškinimas
Agresyvi	Sukonfigūruotas didžiausias pranešimo apie KATEGORIJĄ jautrumas. Pranešama apie daugiau aptikimų. Esant **agresyviai** nuostatai, objektai gali būti klaidingai identifikuojami kaip KATEGORIJA.
Subalansuota	Sukonfigūruotas subalansuotas pranešimas apie KATEGORIJĄ. Ši nuostata leidžia subalansuoti našumą ir aptikimo tikslumą bei klaidingai praneštų objektų skaičių.
Atsargi	Pranešimas apie KATEGORIJĄ sukonfigūruotas taip, kad sumažintų klaidingai nustatytų objektų kiekį išlaikant pakankamą apsaugos lygį. Apie objektus pranešama tik tada, kai tikimybė yra didelė ir kai atitinka KATEGORIJOS veikimo kriterijus.
Išjungta	Pranešimas apie KATEGORIJĄ neaktyvus, o šio tipo aptikimų nėra ieškoma, apie juos nepranešama ir jie nėra valomi. Todėl ši nuostata išjungia apsaugą nuo šio aptikimo tipo. Pranešimo apie kenkėjišką programinę įrangą išjungti negalima ir tai yra numatytoji reikšmė galimai nesaugioms programoms.

⊟ ESET Endpoint Security apsaugos modulių galimumas

Apsaugos modulio galimumas (įjungta arba išjungta) pasirinktai KATEGORIJOS ribinei reikšmei yra:

	Agresyvi	Subalansuota	Atsargi	Išjungta**
Išplėstinis mašininio mokymosi modulis*	✔ (agresyvus režimas)	✔ (atsargus režimas)	X	X
Aptikimo modulis	✔	✔	✔	X
Kiti apsaugos moduliai	✔	✔	✔	X

* Galima ESET Endpoint Security 7.2 ir naujesnėse versijose.
** Nerekomenduojama

⊟ Nustatykite programos versiją, programos modulio versijas ir kompiliavimo datas

1. Spustelėkite **Žinynas ir palaikymas** > **Apie ESET Endpoint Security**.
2. Ekrane **Apie** pirmoje teksto eilutėje rodomas jūsų ESET produkto versijos numeris.
3. Spustelėkite **Rodyti modulius**, kad pasiektumėte informaciją apie konkrečius modulius.

Svarbiausios pastabos

Kelios svarbiausios pastabos apie atitinkamų ribinių reikšmių nustatymą jūsų aplinkai:

- **Subalansuota** ribinė reikšmė rekomenduojama daugumai sąrankų.
- **Atsargi** ribinė reikšmė suteikia panašų apsaugos lygį, kaip ankstesnės ESET Endpoint Security versijos (7.1 ir senesnės). Tai rekomenduojama aplinkoms, kuriose prioritetas skiriamas apsaugos programinės įrangos klaidingai identifikuotų objektų skaičiaus sumažinimui.

- Kuo aukštesnė pranešimo ribinė reikšmė, tuo daugiau aptikimų, tačiau kartu didėja klaidingo objektų identifikavimo tikimybė.
- Neįmanoma užtikrinti 100 % aptikimų dažnio ir 0 % tikimybės išvengti nepavojingų objektų kategorizavimo kaip kenkėjiškos programinės įrangos.
- Naudokite naujausias ESET Endpoint Security ir jo modulių versijas, siekdami geriausios pusiausvyros tarp našumo bei aptikimo dažnių ir klaidingų pranešimų apie objektus.

Apsaugos nustatymai

Jei pranešama apie objektą, klasifikuotą kaip KATEGORIJA, programa užblokuoja objektą ir išvalo, panaikina arba perkelia jį į karantiną.

Prieš keisdami KATEGORIJOS apsaugos ribinę reikšmę (arba lygį), perskaitykite toliau pateiktą informaciją:

Ribinė reikšmė	Paaiškinimas
Agresyvi	Pranešimai apie agresyvaus (arba žemesnio) lygio aptikimus yra blokuojami ir pradedamas automatinis atkūrimas (t. y. valymas). Ši nuostata rekomenduojama, kai visi įrenginiai buvo nuskaityti taikant agresyvias nuostatas ir klaidingai pranešti objektai buvo pridėti prie aptikimo išimčių.
Subalansuota	Pranešimai apie subalansuoto (arba žemesnio) lygio aptikimus yra blokuojami ir pradedamas automatinis atkūrimas (t. y. valymas).
Atsargi	Pranešimai apie atsargaus lygio aptikimus yra blokuojami ir pradedamas automatinis atkūrimas (t. y. valymas).
Išjungta	Naudinga identifikuojant ir išskiriant klaidingai praneštus objektus. Apsaugos nuo kenkėjiškos programinės įrangos išjungti negalima ir tai yra numatytoji reikšmė galimai nesaugioms programoms.

⊟ ESET PROTECT politikos konvertavimo lentelė ESET Endpoint Security 7.1 ir senesnėms versijoms

Nuo ESET PROTECT skaitytuvo nuostatų politikos redaktoriuje nebėra kiekvienos KATEGORIJOS įjungimo / išjungimo jungiklių. Toliau pateiktoje lentelėje aprašomas apsaugos ribinės reikšmės konvertavimas į galutinę jungiklio būseną ESET Endpoint Security 7.1 ir senesnėse versijose.

KATEGORIJOS ribinės reikšmės būsena	Agresyvi	Subalansuota	Atsargi	Išjungta
Taikomas KATEGORIJOS jungiklis	✓	✓	✓	✗

Atnaujinant 7.1 ir senesnes versijas iki 7.2 ir naujesnių versijų, nauja ribinės reikšmės būsena bus:

Kategorijos jungiklis prieš atnaujinimą	✓	✗
Nauja KATEGORIJOS ribinė reikšmė po atnaujinimo	Subalansuota	Išjungta

---

Geriausios praktikos

NEVALDOMA (atskira kliento darbo vieta)

Palikite esamas numatytąsias rekomenduojamas reikšmes.

VALDOMA APLINKA

Šie nustatymai paprastai taikomi darbo vietoms, naudojant politiką.

1. Pradinis etapas

Šis etapas gali užtrukti iki savaitės.

- Visas **pranešimo** ribines reikšmes nustatykite ties **Subalansuota**.
  PASTABA: jei reikia, nustatykite **Agresyvi**.
- Kenkėjiškos programinės įrangos **apsaugą** nustatykite arba palikite **Subalansuota**.
- Kitų KATEGORIJŲ **apsaugą** nustatykite ties **Atsargi**.
  PASTABA: Šiame etape nerekomenduojama nustatyti **apsaugos** ribinę reikšmę ties **Agresyvi**, nes visi aptikimai bus atkurti, įskaitant klaidingai atpažintus.
- Aptikimų žurnale nustatykite klaidingai atpažintus objektus ir pirmiausiai įtraukite juos į aptikimo išimtis.

2. Pereinamasis etapas

- Kai kuriose darbo vietose vykdykite „Gamybos etapą“ kaip bandymą (ne visose tinklo darbo vietose).

3. Gamybos etapas

- Visas **apsaugos** ribines reikšmes nustatykite ties **Subalansuota**.
- Jei valdoma nuotoliniu būdu, ESET Endpoint Security naudokite atitinkamą apsaugos nuo virusų iš anksto nustatytą politiką.
- **Agresyvi** apsaugos ribinė reikšmė gali būti nustatyta, jei reikalingas didžiausias aptikimo dažnis ir priimtinas klaidingas objektų identifikavimas.
- Aptikimo žurnale arba ESET PROTECT ataskaitose patikrinkite galimus trūkstamus aptikimus.

Aptikimo modulio išplėstinės parinktys

Apsaugos nuo slaptųjų virusų technologija yra moderni sistema, leidžianti aptikti pavojingas programas, pvz., kenkimo prieigos programas, kurios sugeba pasislėpti nuo operacinės sistemos. Tai reiškia, kad jų neįmanoma aptikti naudojant įprastinius tikrinimo metodus.

Įjungti išplėstinį nuskaitymą per AMSI – „Microsoft“ apsaugos nuo kenkėjiškų programų nuskaitymo sąsajos įrankis leidžia programų kūrėjams pasinaudoti nauja apsauga nuo kenkėjiškų programų (tik „Windows 10, 11“).

Aptiktas įsiskverbimas

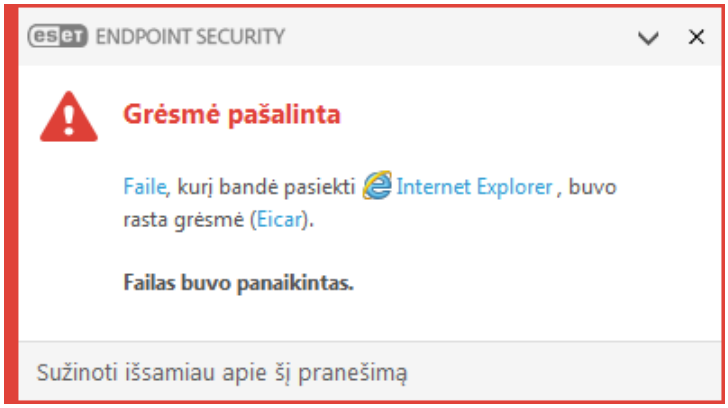
Įsiskverbimai gali patekti į sistemą per įvairius įsiskverbimo taškus: iš tinklalapių, bendrinamų aplankų, el. paštu arba iš nešiojamųjų įrenginių (USB, išorinių diskų, CD, DVD ir t. t.).

Standartinis veikimas

Bendras pavyzdys, kaip įsiskverbimus apdoroja ESET Endpoint Security, gali būti įsiskverbimų aptikimas, kai naudojama:

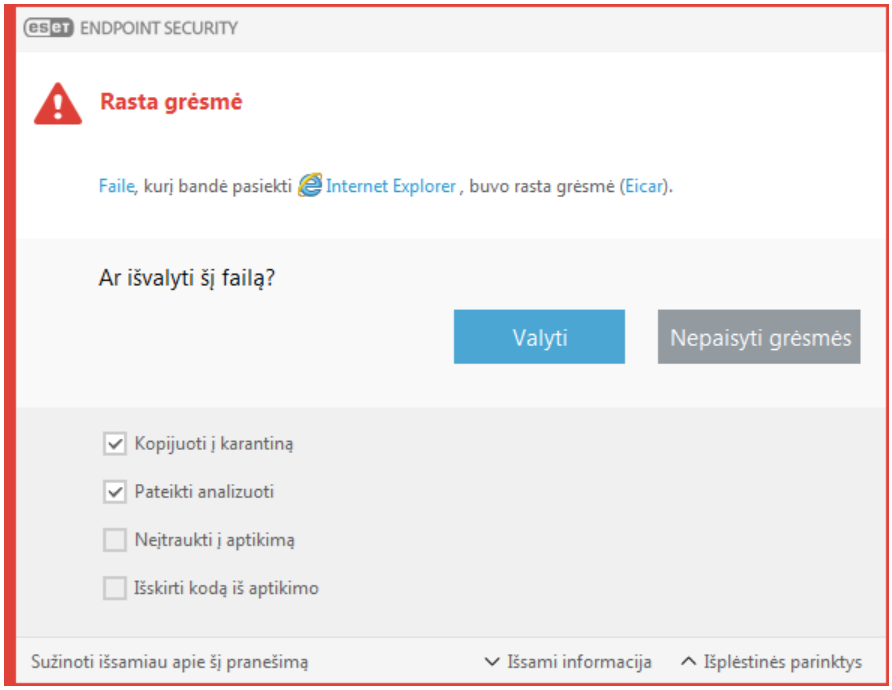
- Failų sistemos apsauga realiuoju laiku
- Prieigos prie saityno apsauga
- El. pašto programų apsauga
- Kompiuterio nuskaitymas pareikalavus

Kiekvienas jų naudoja standartinį valymo lygį ir bandys išvalyti failą bei perkelti jį į Karantiną arba nutraukti ryšį. Pranešimo langas rodomas informacinių pranešimų srityje, apatiniame dešiniajame lango kampe. Išsamią informaciją apie aptiktus / išvalytus objektus rasite dalyje Žurnalo failai. Daugiau informacijos apie valymo lygius ir veiksmus rasite skyriuje Valymas.



Valymas ir naikinimas

Jeigu nėra iš anksto nustatyto veiksmo, kurį turi vykdyti failų sistemos apsauga realiuoju laiku, jūsų paprašys pasirinkti parinktį perspėjimo lange. Paprastai siūlomos parinktys **Valyti**, **Naikinti** ir **Nieko nedaryti**. Pasirinkti **Nieko nedaryti** nerekomenduojama, nes taip užkrėsti failai liks neišvalyti. Išimtis gali būti, kai esate tikri, jog failas yra nekenksmingas ir buvo aptiktas klaidingai.



Naudokite valymą, jeigu failą atakavo virusas ir prie jo prijungė kenkėjišką kodą. Tokiu atveju pirmiausia bandykite išvalyti užkrėstą failą ir atkurti jo originalią būseną. Jeigu failą sudaro tik kenkėjiškas kodas, jis bus panaikintas.

Jei užkrėstas failas yra „užrakintas“ arba naudojamas sistemos proceso, jis bus panaikintas, tik kai atsilaisvins (paprastai paleidus sistemą iš naujo).

Atkūrimas iš karantino

Karantiną galima pasiekti ESET Endpoint Security pagrindiniame programos lange spustelėjus **Įrankiai** > **Karantinas**.

Karantinuotus failus taip pat galima atkurti į jų originalią vietą:

- Šiuo tikslu naudokite funkciją **Atkurti**, kuri pasiekiama kontekstiniame meniu, dešiniuoju pelės klavišu spustelėjus nurodytą karantinuotą failą.
- Jei failas pažymėtas kaip galima nepageidaujama taikomoji programa, aktyvinta parinktis **Atkurti ir neįtraukti į nuskaitymą**. Taip pat žr. skiltį Išimtys.
- Be to, kontekstiniame meniu siūloma parinktis **Atkurti į**, kuri leidžia atkurti failą į kitą vietą (ne į tą, iš kurios jis buvo pašalintas).
- Atkūrimo funkcija kai kuriais atvejais nepasiekiama, pvz., failams, esantiems tik skaitomoje tinklo dalyje.

Keletas grėsmių

Jei kurie nors užkrėsti failai nebuvo išvalyti nuskaitant kompiuterį (arba buvo parinkta parametro Valymo lygis vertė **Nevaloma**), bus pateiktas perspėjimo langas, kuriame raginama pasirinkti, ką daryti su šiais failais.

Failų naikinimas archyvuose

Numatytuoju valymo režimu visas archyvas bus panaikintas, tik jeigu jame visi failai yra užkrėsti ir nėra švarių. Kitaip tariant, archyvai nebus panaikinami, jeigu juose yra ir nekenksmingų švarių failų. Būkite atsargūs, kai atliekate nuskaitymą naudodami griežtą valymą – įjungtas griežtas valymas, neatsižvelgdamas į kitų archyvo failų būseną, archyvą panaikins, jeigu jame yra bent vienas užkrėstas failas.

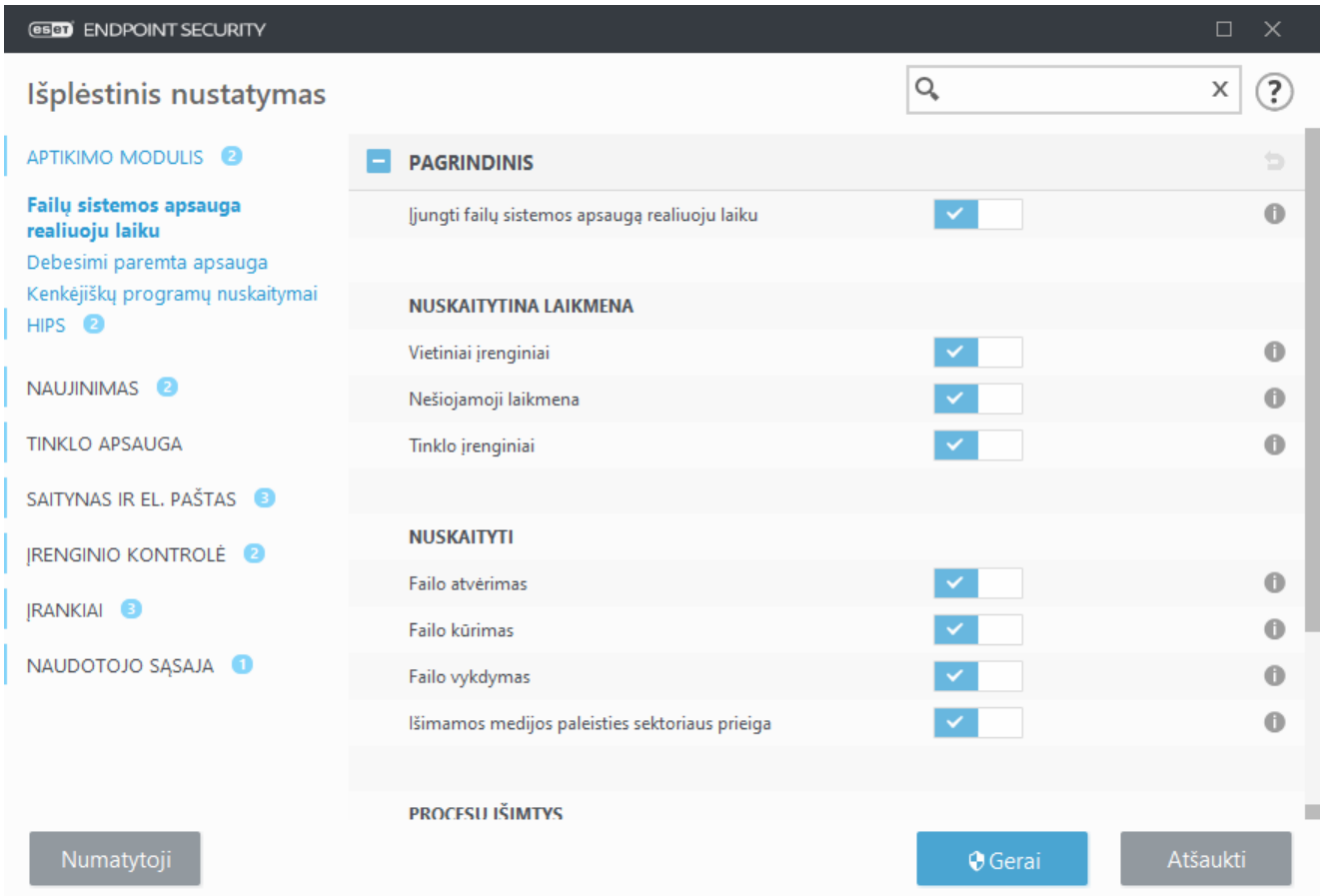
Jei kompiuteryje pastebite užsikrėtimo kenkimo programa ženklų, pvz., jis pradeda lėčiau veikti, dažnai užstringa ir pan., rekomenduojame atlikti šiuos veiksmus:

- Atidarykite ESET Endpoint Security ir spustelėkite „Kompiuterio nuskaitymas“
- Spustelėkite **Išmanusis nuskaitymas** (daugiau informacijos rasite skyriuje Kompiuterio nuskaitymas)
- Kai nuskaitymas bus baigtas, peržiūrėkite žurnalą, kuriame pateikiamas nuskaitytų, užkrėstų ir išvalytų failų skaičius

Jeigu norite nuskaityti tik tam tikrą disko dalį, spustelėkite **Pasirinktinis nuskaitymas** ir pasirinkite tikslus, kuriuos reikia nuskaityti ieškant virusų.

Failų sistemos apsauga realiuoju laiku

Failų sistemos apsauga realiuoju laiku tikrina, ar nėra kenkėjiško kodo, atidarant, kuriant arba paleidžiant visus sistemos failus.



Pagal numatytuosius nustatymus failų sistemos apsauga realiuoju laiku įjungiama paleidžiant sistemą ir atlieka nepertraukiamą nuskaitymą. Nerekomenduojame išjungti **Įjungti failų sistemos apsaugą realiuoju laiku** dalyje **Išplėstiniai nustatymai**, kuri yra skyriuje **Aptikimo modulis** > **Failų sistemos apsauga realiuoju laiku** > **Bazinis**.

Nuskaitoma laikmena

Pagal numatytuosius nustatymus visų tipų laikmenos nuskaitomos ieškant galimų grėsmių:

- **Vietiniai įrenginiai** – nuskaito visus sisteminius ir fiksuotus standžiuosius diskus (pvz.: *C:*\, *D:*\).

- **Nešiojamoji laikmena** – nuskaito CD/DVD, USB laikmenas, atminties korteles ir pan.
- **Tinklo diskų įrenginiai** – nuskaito visus susietus tinklo diskų įrenginius (pvz.: *H:*\ kaip *store04*) arba tiesioginės prieigos tinklo diskų įrenginius (pvz.: *store08*).

Rekomenduojame naudoti numatytuosius parametrus ir keisti juos tik tam tikrais atvejais, pvz., jei kurios nors laikmenos nuskaitymas labai sulėtina duomenų persiuntimą.

Nuskaitymas įjungtas

Pagal numatytuosius nustatymus visi failai yra nuskaitomi atidarant, sukuriant arba vykdant. Rekomenduojame palikti numatytuosius nustatymus, nes jie užtikrina geriausią jūsų kompiuterio apsaugos realiuoju laiku lygį:

- **Failo atidarymas** – nuskaitoma failą atidarant.
- **Failo kūrimas** – nuskaitoma kuriant arba modifikuojant failą.
- **Failo vykdymas** – nuskaitoma vykdant arba paleidžiant failą.
- **Nešiojamosios laikmenos paleidimo sektoriaus prieiga** – kai prie įrenginio prijungiama nešiojamoji laikmena su paleidimo sektoriumi, iškart nuskaitomas paleidimo sektorius. Ši parinktis neįjungia nešiojamosios laikmenos failų nuskaitymo. Nešiojamosios laikmenos failų nuskaitymą rasite **Nuskaitoma laikmena** > **Nešiojamoji laikmena**. Kad **Nešiojamosios laikmenos paleidimo sektoriaus prieiga** veiktų tinkamai, **Paleidimo sektoriai/UEFI** turi būti įjungta „ThreatSense“ parametruose.

Procesai, kuriems nuskaitymo metu bus taikomos išimtys –apie šio tipo išimtis daugiau skaitykite skyriuje Procesų išimtys.

Failų sistemos apsauga realiuoju laiku tikrina visų tipų laikmenas ir yra paleidžiama įvairių sistemos įvykių, pavyzdžiui, kai norima pasiekti failą. Naudojant „ThreatSense“ technologijos aptikimo metodus (kaip aprašyta skyriuje „ThreatSense“ modulio parametrų nustatymai), failų sistemos apsauga realiuoju laiku gali būti konfigūruota skirtingai elgtis su naujai sukurtais ir esamais failais. Pavyzdžiui, galite konfigūruoti failų sistemos apsaugą realiuoju laiku atidžiau stebėti naujai sukuriamus failus.

Kad būtų užtikrinta mažiausia įtaka sistemos našumui naudojant apsaugą realiuoju laiku, kartą nuskaityti failai pakartotinai nenuskaitomi (jeigu jie nebuvo pakeisti). Failai nuskaitomi dar kartą iškart po kiekvieno aptikimo modulio naujinimo. Šie veiksmai valdomi naudojant **Išmanųjį optimizavimą**. Jei funkcija **Išmanusis optimizavimas** išjungta, visi failai nuskaitomi kaskart juos pasiekiant. Jei norite pakeisti šį parametrą, paspauskite **F5**, kad atidarytumėte dalį Išplėstiniai nustatymai ir išskleiskite **Aptikimo modulis** > **Failų sistemos apsauga realiuoju laiku**. Spustelėkite **ThreatSense parametrai** > **Kita** ir pažymėkite arba panaikinkite žymėjimą prie **Įjungti išmanųjį optimizavimą**.

Apsaugos realiuoju laiku tikrinimas

Norėdami įsitikinti, kad apsauga realiuoju laiku veikia ir aptinka virusus, naudokite tikrinimo failą iš eicar.com. Šis tikrinimo failas yra nekenksmingas failas, kurį aptinka visos antivirusinės programos. Šis tikrinimo failas yra nekenksmingas failas, kurį aptinka visos antivirusinės programos. „European Institute for Computer Antivirus Research“), kad būtų galima patikrinti antivirusinių programų funkcionalumą.

Failą galima atsisiųsti čia http://www.eicar.org/download/eicar.com
Naršyklėje įvedę šį URL, turėtumėte pamatyti pranešimą, kad grėsmė pašalinta.

Kada keisti apsaugos realiuoju laiku konfigūraciją

Failų sistemos apsauga realiuoju laiku yra svarbiausias komponentas, užtikrinantis sistemos apsaugą. Visada būkite atidūs keisdami jos parametrus. Rekomenduojame keisti jos parametrus tik tam tikrais atvejais.

Įdiegus ESET Endpoint Security, visi parametrai optimizuojami, kad būtų užtikrinamas maksimalus vartotojo sistemos saugumo lygis. Norėdami atkurti numatytuosius parametrus, spustelėkite šalia kiekvieno lange esančio skirtuko (**Išplėstiniai nustatymai** > **Aptikimo modulis** > **Failų sistemos apsauga realiuoju laiku**).

Ką daryti, jeigu apsauga realiuoju laiku neveikia

Šiame skyriuje apibūdiname problemas, kurių gali kilti naudojant apsaugą realiuoju laiku, ir kaip jas spręsti.

Apsauga realiuoju laiku išjungta

Jei naudotojas netyčia išjungia apsaugą realiuoju laiku, turėtumėte iš naujo aktyvinti šią funkciją. Norėdami iš naujo aktyvinti apsaugą realiuoju laiku, pagrindiniame programos lange eikite **Nustatymas** ir spustelėkite **Kompiuterio apsauga** > **Failų sistemos apsauga realiuoju laiku**.

Jei apsauga realiuoju laiku nepaleidžiama paleidžiant sistemą, paprastai taip yra dėl to, kad išjungta parinktis **Paleisti failų sistemos apsaugą realiuoju laiku**. Jei norite pasitikrinti, ar ši parinktis įjungta, eikite į dalį **Išplėstiniai nustatymai** (**F5**) ir spustelėkite **Aptikimo modulis** > **Failų sistemos apsauga realiuoju laiku**.

Jeigu apsauga realiuoju laiku neaptinka ir neišvalo įsiskverbimų

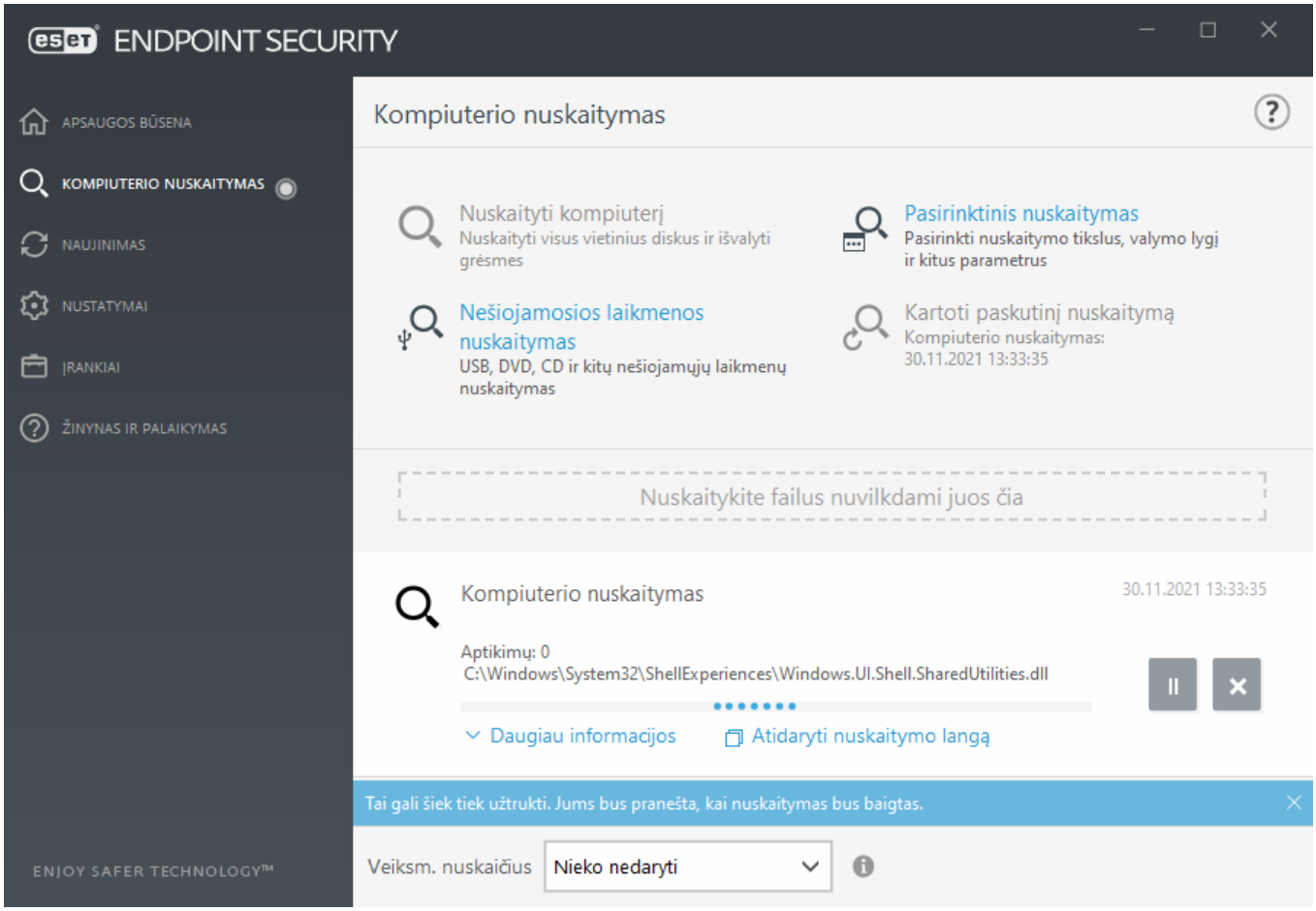
Įsitikinkite, kad kompiuteryje nėra įdiegta jokių kitų antivirusinių programų. Jei vienu metu yra įdiegtos dvi antivirusinės programos, jos gali būti nesuderinamos viena su kita. Rekomenduojame prieš įdiegiant ESET išdiegti visas kitas antivirusines programas savo sistemoje.

Apsauga realiuoju laiku nepaleidžiama

Jeigu apsauga realiuoju laiku nepaleidžiama paleidžiant sistemą (ir parinktis **Įjungti failų sistemos apsaugą realiuoju laiku** yra įjungta), gali būti, kad ji yra nesuderinama su kitomis programomis. Šiai problemai išspręsti kreipkitės į ESET techninės pagalbos tarnybą. Sukūrus „ESET SysInspector žurnalą“ ir pateikus jį ESET techninė pagalbos tarnybai išanalizuoti, galbūt bus galima išspręsti problemą. Daugiau sužinosite perskaitę šį ESET žinių bazės straipsnį.

Kompiuterio nuskaitymas

Nuskaitymo pareikalavus modulis yra svarbi ESET Endpoint Security dalis. Jis naudojamas failams ir katalogams jūsų kompiuteryje nuskaityti. Saugumui užtikrinti svarbu, kad kompiuteris būtų nuskaitomas ne tik tuomet, kai įtariamas užkratas, bet ir reguliariai, vykdant įprastines saugumo priemones. Rekomenduojame reguliariai (pvz., vieną kartą per mėnesį) vykdyti sistemos išsamaus nuskaitymo procedūras, kad surastumėte virusus, kurių neaptinka Failų sistemos apsauga realiuoju laiku. Taip gali nutikti, jei failų sistemos apsauga realiuoju laiku kažkuriuo metu buvo išjungta, jei paseno aptikimo modulis arba failas neaptiktas kaip virusas, įrašant jį į diską.



Yra du **kompiuterio nuskaitymo** tipai. **Nuskaityti jūsų kompiuterį** greitai nuskaito sistemą ir jam nereikia papildomai konfigūruoti nuskaitymo parametrų. **Pasirinktinis nuskaitymas** leidžia pasirinkti bet kurį iš anksto nustatytą nuskaitymo profilį bei apibrėžti konkrečius nuskaitymo tikslus.

Žiūrėkite Nuskaitymo eiga, kur pateikiama daugiau informacijos apie nuskaitymo procesą.

Nuskaityti jūsų kompiuterį

Išmanusis nuskaitymas suteikia galimybę greitai paleisti kompiuterio nuskaitymą ir išvalyti užkrėstus failus vartotojui neatliekant jokių veiksmų. Išmaniojo nuskaitymo privalumai yra paprastas naudojimas ir tai, kad jam nereikalinga išsami nuskaitymo konfigūracija. Išmanusis nuskaitymas tikrina visus failus vietiniuose įrenginiuose ir automatiškai išvalo arba panaikina aptiktus įsiskverbimus. Valymo lygis automatiškai nustatomas į numatytąjį. Išsamesnės informacijos apie valymo tipus rasite skyriuje Valymas.

Pasirinktinis nuskaitymas

Pasirinktinis nuskaitymas yra optimalus sprendimas, jei norite nurodyti nuskaitymo parametrus (pvz., nuskaitymo tikslus ir metodus). Pasirinktinio nuskaitymo privalumas – galimybė išsamiai konfigūruoti parametrus. Konfigūracijas galima įrašyti į vartotojo apibrėžtus nuskaitymo profilius. Tai gali būti naudinga, jei vėliau nuskaitymas pakartotinai vykdomas su tais pačiais parametrais.

Norėdami pasirinkti nuskaitymo tikslus, nurodykite **Kompiuterio nuskaitymas** > **Pasirinktinis nuskaitymas** ir parinktį iš išskleidžiamojo meniu **Nuskaitymo tikslai** arba konkrečius tikslus medžio struktūroje. Be to, nuskaitymo tikslas gali būti nurodytas įvedant aplanko kelią arba failą (-us), kurį (-iuos) norite įtraukti. Jei norite, kad būtų tik nuskaityta sistema neatliekant papildomų valymo veiksmų, pasirinkite **Nuskaityti nevalant**. Nuskaitymo metu vieną iš trijų valymo lygių galima pasirinkti spustelėjus **Nustatyti** > **„ThreatSense“ parametrai** > **Valymas**.

Kompiuterį nuskaityti pasirinktinio nuskaitymo būdu rekomenduojama patyrusiems vartotojams, turintiems antivirusinių programų naudojimo patirties.

Be to, failui ar aplankui nuskaityti rankiniu būdu galite naudoti funkciją **Nuvilkti ir nuskaityti** – tiesiog spustelėkite failą ar palanką ir laikydami nuspaudę pelės mygtuką perkelkite pelės žymeklį į pažymėtą sritį, tada mygtuką atleiskite. Tada programa perkeliama į pirmą planą.

Nešiojamosios laikmenos nuskaitymas

Panašus į **Nuskaityti jūsų kompiuterį** – greitai paleidžia šiuo metu prie kompiuterio prijungtos nešiojamosios laikmenos nuskaitymą (pavyzdžiui, CD / DVD / USB). Tai gali būti naudinga, kai prie kompiuterio prijungiate USB atmintuką ir norite nuskaityti jo turinį ieškodami kenkimo programinės įrangos ir kitų galimų grėsmių.

Šio tipo nuskaitymą galima paleisti ir spustelint **Pasirinktinis nuskaitymas**, tada išskleidžiamajame meniu **Nuskaitymo tikslai** nurodant **Nešiojamoji laikmena** ir spustelint **Nuskaityti**.

Kartoti paskutinį nuskaitymą

Galite greitai paleisti anksčiau atliktą nuskaitymą, kuriam bus naudojami tie patys parametrai.

Išskleidžiamajame meniu **Veiksmas nuskaičius** galite pasirinkti **Nieko nedaryti**, **Išjungti**, **Paleisti iš naujo**, **Jei reikia, paleisti iš naujo**, **Jei reikia, priversti paleisti iš naujo** arba **Priversti paleisti iš naujo**. Veiksmai **Miego režimas** arba **Sulaikytosios veiksenos režimas** pasiekiami atsižvelgiant į jūsų kompiuterio operacinės sistemos maitinimo ir miego režimo nustatymus arba jūsų stalinio / nešiojamojo kompiuterio galimybes. Pasirinktas veiksmas bus pradėtas užbaigus visus vykdomus nuskaitymus. Pasirinkus veiksmą **Išjungti**, išjungimo patvirtinimo dialogo lange bus rodoma 30 sekundžių atbulinė atskaita (spustelėkite **Atšaukti**, kad atšauktumėte pageidaujamo išjungimo veiksmą). Norėdami gauti daugiau informacijos žr. skiltį Išplėstinės nuskaitymo parinktys.

> Mes rekomenduojame atlikti kompiuterio nuskaitymą mažiausiai kartą per mėnesį. Nuskaitymas gali būti sukonfigūruotas kaip suplanuota užduotis, pasirenkant **Įrankiai** > **Planuoklė**. Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą?

Pasirinktinio nuskaitymo paleidimo priemonė

Jeigu norite nuskaityti tik konkrečią paskirties vietą, galite naudoti pasirinktinio nuskaitymo įrankį – spustelėkite **Kompiuterio nuskaitymas** > **Pasirinktinis nuskaitymas** ir nurodykite parinktį išskleidžiamajame meniu > **Nuskaitymo tikslai** arba pasirinkite konkrečias paskirties vietas aplankų struktūroje (medyje).

Nuskaitymo paskirties langas leidžia nustatyti, kurie objektai (atmintis, diskai, sektoriai, failai ir aplankai) turi būti nuskaitomi ieškant įsiskverbimų.

Išskleidžiamajame meniu **Nuskaitymo tikslai** galite pasirinkti iš anksto nustatytus nuskaitymo tikslus.

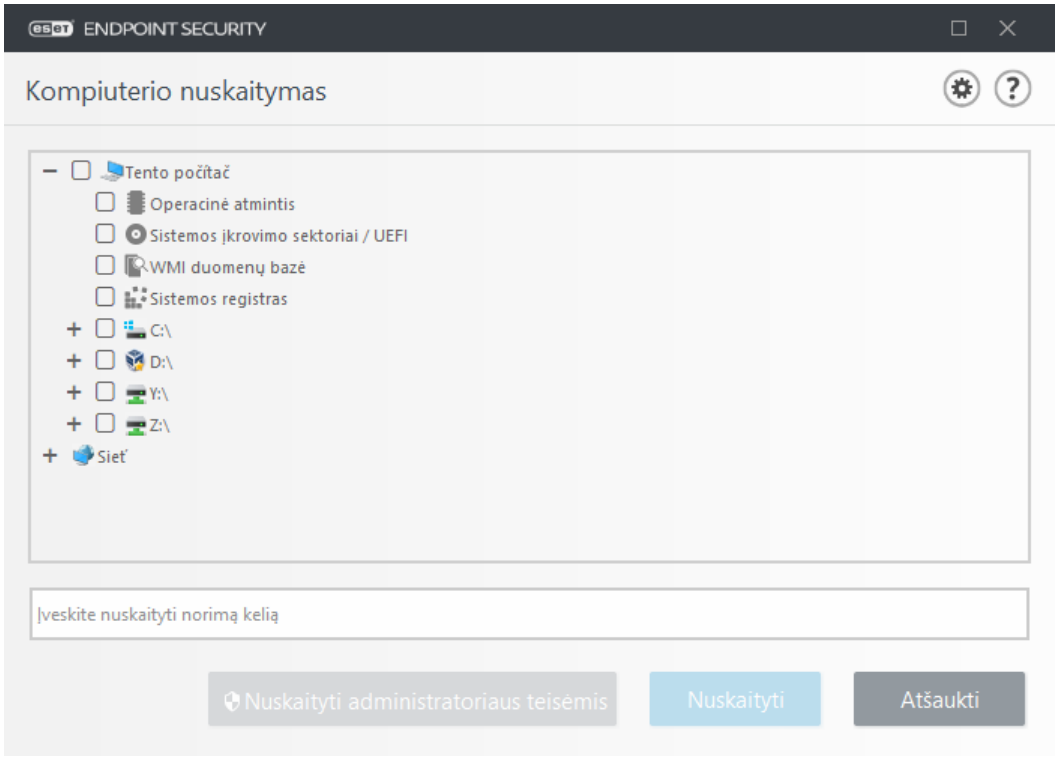
- **Pagal profilio parametrus** – pasirenkami paskirties tikslai, nustatyti pagal pasirinktą nuskaitymo profilį.
- **Nešiojamoji laikmena** – pasirenka diskelius, USB atminties įrenginius, CD/DVD.
- **Vietiniai įrenginiai** – pasirenka visus sistemos standžiuosius diskus.
- **Tinklo diskų įrenginiai** – pasirenka visus susietus tinklo diskus.

- **Tinkintaspasirinkimas** – atšaukia visus ankstesnius pasirinkimus.

Aplanko (medžio) struktūroje taip pat yra konkrečių tikslinių nuskaitymo objektų.

- **Operacinė atmintis** – nuskaito visus procesus ir duomenis, kuriuos šiuo metu naudoja operacinė atmintis.
- **Įkrovos sektoriai / UEFI** – nuskaito įkrovos sektorius ir UEFI, siekiant aptikti kenkėjišką programinę įrangą. Daugiau apie UEFI skaitytuvą skaitykite žodynėlėje.
- **WMI duomenų bazė** – nuskaito visą Windows Management Instrumentation WMI duomenų bazę, visus pavadinimus, visus klasės egzempliorius ir visas ypatybes. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis.
- **Sistemos registras** – nuskaito visą sistemos registrą, visus raktus ir antrinius raktus. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis. Valant aptiktus elementus, nuoroda lieka registre, kad įsitikintumėte, jog nebus prarasti svarbūs duomenys.

Norėdami greitai pereiti prie nuskaitymo paskirties vietos (failo ar aplanko), įveskite jo kelią į teksto lauką po medžio struktūra. Kelio pavadinime skiriamos didžiosios ir mažosios raidės. Norėdami įtraukti paskirties vietą į nuskaitymą, pažymėkite jos žymės langelį medžio struktūroje.



Užkrėsti elementai nebus automatiškai valomi. Nuskaitymas nevalant gali būti naudojamas norint atlikti esamos apsaugos būsenos apžvalgą. Be to, galite pasirinkti vieną iš trijų valymo lygių spustelėdami **Išplėstinis nustatymas** > **Aptikimo modulis** > **Nuskaitymas pareikalavus** > **ThreatSense parametrai** > **Valymas**. Jei norite, kad būtų tik nuskaityta sistema neatliekant papildomų valymo veiksmų, pasirinkite **Nuskaityti nevalant**. Nuskaitymo istorija išsaugoma nuskaitymo žurnale.

Kai pasirenkama **Nepaisyti išimčių**, bus nuskaitomi ir failai su išimtimis, kurie anksčiau nebuvo įtraukti į nuskaitymą.

Galite pasirinkti profilį iš išplečiamojo meniu **Nuskaitymo profilis**, kuris bus naudojamas nuskaitant pasirinktus tikslus. Numatytasis profilis yra **Išmanusis nuskaitymas**. Yra dar trys iš anksto nustatyti nuskaitymo profiliai, kurie vadinasi **Kontekstinio meniu nuskaitymas**, **Giluminis nuskaitymas** ir **Kompiuterio nuskaitymas**. Šie nuskaitymo profiliai naudoja skirtingus „ThreatSense“ parametrus. Pasiekiamos parinktys aprašytos dalyje **Išplėstinis**

nustatymai > **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymas** > **Nuskaitymas pareikalavus** > „ThreatSense“ parametrai.

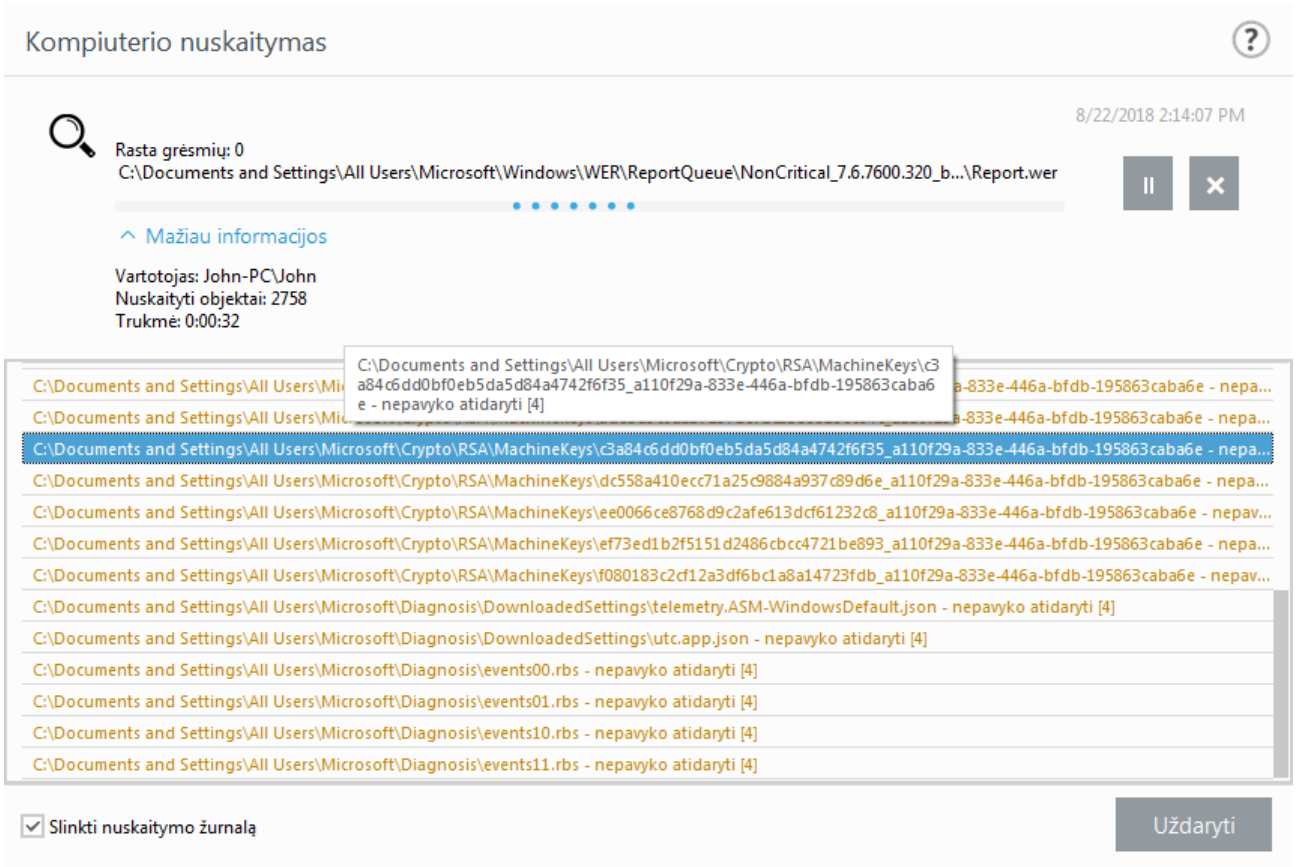
Spustelėkite **Nuskaityti**, kad būtų vykdomas nuskaitymas, naudojant jūsų nustatytus pasirinktinius parametrus.

Mygtuku **Nuskaityti administratoriaus teisėmis** galima vykdyti nuskaitymą iš administratoriaus paskyros. Spustelėkite jį, jeigu esamas vartotojas neturi pakankamų teisų pasiekti failams, kuriuos reikia nuskaityti. Atminkite, kad šis mygtukas nepasiekiamas, jeigu esamas vartotojas negali iškviesti UAC operacijų kaip administratorius.

Pasibaigus nuskaitymui kompiuterio nuskaitymo žurnalą galite peržiūrėti spustelėdami **Rodyti žurnalą**.

Nuskaitymo eiga

Nuskaitymo eigos lange rodoma esama nuskaitymo būsena ir informacija apie failų, kuriuose buvo rastas kenkėjiškas kodas, kiekį.



Įprasta, kad kai kurių failų, tokių kaip slaptažodžiu apsaugotų failų arba failų, kuriuos išskirtinai naudoja tik sistema (paprastai *pagefile.sys* ir tam tikrų žurnalo failų), negalima nuskaityti.

Nuskaitymo eiga – eigos juosta rodo jau nuskaitytų objektų būseną, palyginti su dar turimais nuskaityti objektais. Nuskaitymo eigos būsena apskaičiuojama pagal visą į nuskaitymą įtrauktų objektų skaičių.

Tikslas – šiuo metu nuskaitomo objekto pavadinimas ir jo vieta.

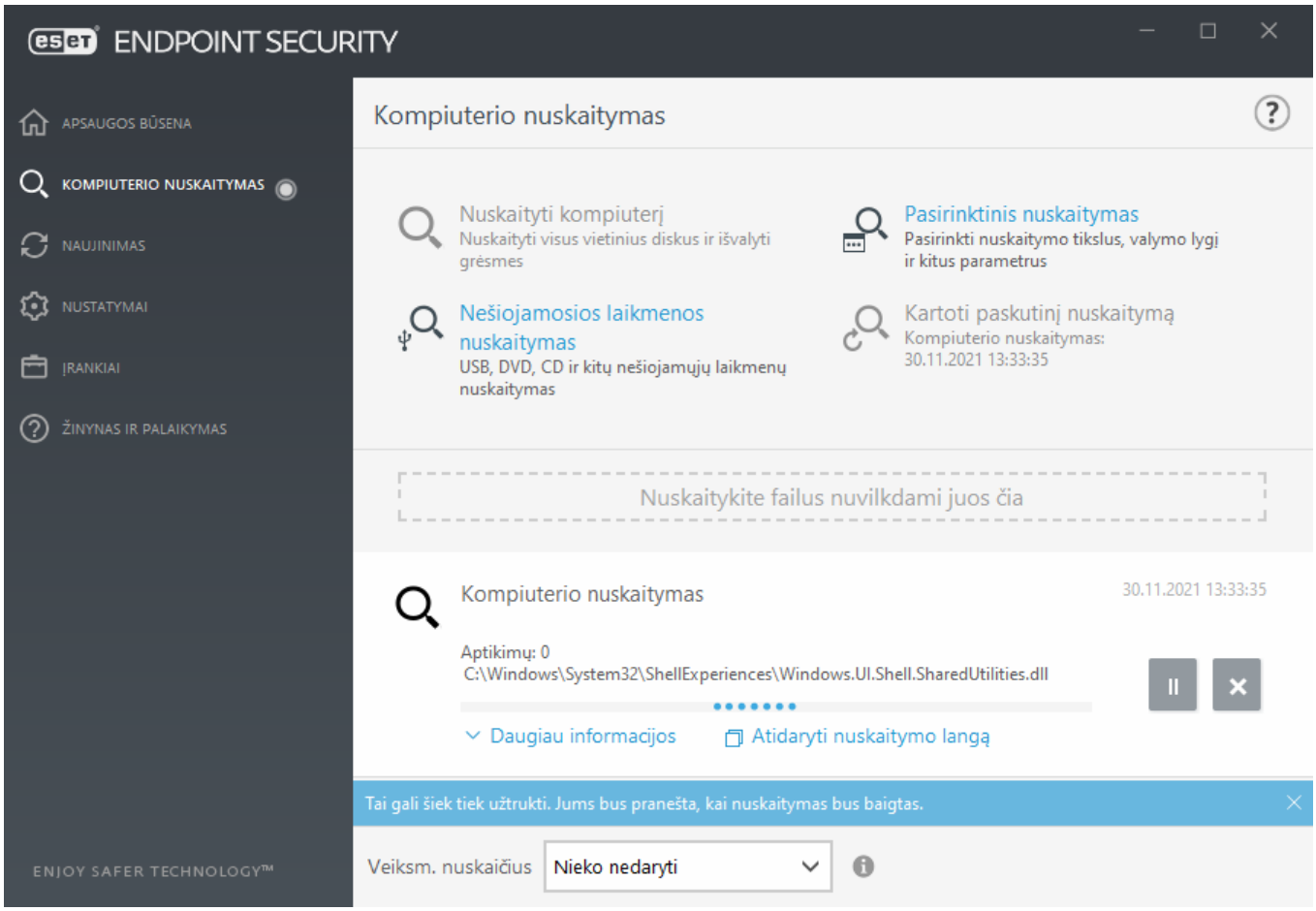
Rasta grėsmių – parodo visą nuskaitant rastų grėsmių skaičių.

Pristabdyti – pristabdo nuskaitymą.

Tęsti – ši parinktis matoma, kai nuskaitymo eiga buvo pristabdyta. Jei norite tęsti nuskaitymą, spustelėkite **Tęsti**.

Stabdyti – nutraukia nuskaitymą.

Slinkti nuskaitymo žurnalą – jeigu įjungta, pridėjus naujų įrašų nuskaitymo žurnalas bus automatiškai slenkamas žemyn, todėl bus matomi naujausi įrašai.



Kompiuterio nuskaitymo žurnalas

Kompiuterio nuskaitymo žurnale pateikiama bendroji informacija apie nuskaitymą, pvz.:

- Nuskaitymo data ir laikas
- Nuskaityta diskų, aplankų ir failų
- Nuskaitytų objektų skaičius
- Rastų grėsmių skaičius
- Įvykdymo laikas
- Bendras nuskaitymo laikas

Kenkėjiškų programų nuskaitymai

Dalis **Kenkėjiškų programų nuskaitymai** yra pasiekiama meniu Išplėstiniai nustatymai. Paspauskite mygtuką **F5** , spustelėkite **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** ir pasirodys parinktys pasirinkti nuskaitymo

parametrus. Šioje dalyje yra šios parinktys:

- **Pasirinktas profilis** – konkretus nustatymų rinkinys, kurį naudoja skaitytuvas pagal pareikalavimą. Kad sukurtumėte naują profilį, spustelėkite Redaguoti šalia Profilių sąrašo. Jei reikia daugiau informacijos, žr. Nuskaitymo profiliai.
- **Apsauga pareikalavus ir naudojant mašininį mokymąsi** – žr. Aptikimo modulis (7.2 ir naujesnės versijos).
- **Nuskaitymo paskirties vietos** – Jei norite nuskaityti tik konkrečią tikslinę vietą, galite spustelėti **Redaguoti** (šalia **Nuskaitymo paskirties vietos**) ir nurodyti parinktį išskleidžiamajame meniu arba pasirinkti konkrečias paskirties vietas aplankų (medžio) struktūroje. Jei reikia daugiau informacijos, žr. Nuskaitymo paskirties vietos.
- **ThreatSense** parametrai – šiame skyriuje galite rasti išplėstinių nustatymų parinktis, pvz., failų plėtiniai, kuriuos norite kontroliuoti, naudojami aptikimo metodai ir t. t. Spustelėkite, kad atidarytumėte kortelę su išplėstinėmis skaitytuvo parinktimis.

Nuskaitymas laukimo būsenoje

Galite įjungti laukimo būsenos skaitytuvą dalyje **Išplėstiniai nustatymai** dalyje **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Nuskaitymas laukimo būsenoje**.

Nuskaitymas laukimo būsenoje

Kad įjungtumėte šią funkciją, nustatykite jungiklį, esantį šalia **Įjungti laukimo būsenos nuskaitymą**, į padėtį **Įjungta**. Kai kompiuteris yra laukimo būsenos, tylusis kompiuterio nuskaitymas yra atliekamas visuose vietiniuose įrenginiuose.

Kaip numatyta, laukimo būsenos aptikimo skaitytuvas neveiks (nešiojamajam) kompiuteriui veikiant akumuliatoriaus energija. Šį parametrą galite apeiti, išplėstiniuose nustatymuose suaktyvinę jungiklį ties **Vykdyti, net jei kompiuteris veikia naudodamas akumuliatoriaus energiją**.

Išplėstiniuose nustatymuose įjunkite jungiklį **Įjungti registravimą**, kad kompiuterio nuskaitymo išvestis būtų registruojama Žurnalo failuose (pagrindiniame programos lange spustelėkite **Įrankiai** > **Žurnalo failai** ir išplečiamajame meniu **Žurnalas** pasirinkite **Kompiuterio nuskaitymas**).

Laukimo būsenos aptikimas

Išsamaus sąlygų, būtinų įjungti laukimo būsenos skaitytuvui, sąrašą žr. Laukimo būsenos aptikimo paleidimo sąlygos.

Spustelėkite ThreatSense modulio parametrų nustatymai, kad modifikuotumėte laukimo būsenos skaitytuvo nuskaitymo parametrus (pvz., aptikimo metodus).

Nuskaitymo profiliai

ESET Endpoint Security yra 4 iš anksto apibrėžti nuskaitymo profiliai:

- **Išmanusis nuskaitymas** – tai numatytasis išplėstinis nuskaitymo profilis. Išmaniojo nuskaitymo profilyje naudojama išmaniojo optimizavimo technologija, kuri neapima failų, kurie ankstesnio nuskaitymo metu

buvo rasti švarūs ir po šio nuskaitymo nebuvo pakeisti. Tai leidžia sutrumpinti nuskaitymo laiką ir daro mažiausią poveikį sistemos saugumui.
- **Kontekstinio meniu nuskaitymas** – pagal poreikį galite pradėti bet kurio failo nuskaitymą iš kontekstinio meniu. Kontekstinio meniu nuskaitymo profilis leidžia nustatyti nuskaitymo konfigūraciją, kuri bus naudojama paleidus nuskaitymą tokiu būdu.
- **Giluminis nuskaitymas** – giluminio nuskaitymo profilyje pagal numatytuosius parametrus išmanusis optimizavimas nenaudojamas, todėl naudojant šį profilį nuskaitomi visi failai.
- **Kompiuterio nuskaitymas** – numatytasis profilis, naudojamas įprastai nuskaitant kompiuterį.

Jūsų pasirinkti nuskaitymo parametrai gali būti išsaugoti, kad galėtumėte juos panaudoti nuskaitydami kitą kartą. Rekomenduojame susikurti skirtingus profilius (su skirtingais nuskaitymo tikslais, nuskaitymo metodais ir kitais parametrais) kiekvienam reguliariai atliekamam nuskaitymui.

Norėdami sukurti naują profilį, atidarykite išplėstinių nustatymų langą (F5) ir spustelėkite **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymas** > **Nuskaitymas pareikalavus** > **Profilių sąrašas**. **Profilių tvarkytuvės** lange yra **Pasirinkto profilio** išskleidžiamasis meniu, kuriame pateikti nuskaitymo profiliai ir naujo profilio kūrimo parinktis. Norėdami sukurti nuskaitymo profilį, kuris atitiktų jūsų poreikius, žiūrėkite skyrių ThreatSense modulio parametrų nustatymas, kuriame aprašytas kiekvienas nuskaitymo nustatymų parametras.

> Tarkime, norite sukurti savo nuskaitymo profilį ir jums iš dalies tinka **kompiuterio nuskaitymo** konfigūracija, tačiau nenorite nuskaityti momentinio pakavimo arba galimai nesaugių programų, be to, norite taikyti **griežto valymo**. Įveskite savo naujojo profilio pavadinimą į langą **Profilių tvarkytuvas** ir spustelėkite **Pridėti**. **Pasirinkto profilio** išskleidžiamajame meniu pasirinkite naująjį profilį ir pakeiskite likusius parametrus pagal savo reikalavimus, tada spustelėkite **Gerai**, kad naująjį profilį įrašytumėte.

Nuskaitymo tikslai

Nuskaitymo paskirties langas leidžia nustatyti, kurie objektai (atmintis, diskai, sektoriai, failai ir aplankai) turi būti nuskaitomi ieškant įsiskverbimų.

Išskleidžiamajame meniu **Nuskaitymo tikslai** galite pasirinkti iš anksto nustatytus nuskaitymo tikslus.

- **Pagal profilio parametrus** – pasirenkami paskirties tikslai, nustatyti pagal pasirinktą nuskaitymo profilį.
- **Nešiojamoji laikmena** – pasirenka diskelius, USB atminties įrenginius, CD/DVD.
- **Vietiniai įrenginiai** – pasirenka visus sistemos standžiuosius diskus.
- **Tinklo diskų įrenginiai** – pasirenka visus susietus tinklo diskus.
- **Tinkintaspasirinkimas** – atšaukia visus ankstesnius pasirinkimus.

Aplanko (medžio) struktūroje taip pat yra konkrečių tikslinių nuskaitymo objektų.

- **Operacinė atmintis** – nuskaito visus procesus ir duomenis, kuriuos šiuo metu naudoja operacinė atmintis.
- **Įkrovos sektoriai / UEFI** – nuskaito įkrovos sektorius ir UEFI, siekiant aptikti kenkėjišką programinę įrangą. Daugiau apie UEFI skaitytuvą skaitykite žodynėlėje.
- **WMI duomenų bazė** – nuskaito visą Windows Management Instrumentation WMI duomenų bazę, visus pavadinimus, visus klasės egzempliorius ir visas ypatybes. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis.
- **Sistemos registras** – nuskaito visą sistemos registrą, visus raktus ir antrinius raktus. Ieško nuorodų į užkrėstus failus arba kenkėjišką programinę įrangą, įdėtą kaip duomenis. Valant aptiktus elementus, nuoroda lieka registre, kad įsitikintumėte, jog nebus prarasti svarbūs duomenys.

Norėdami greitai pereiti prie nuskaitymo paskirties vietos (failo ar aplanko), įveskite jo kelią į teksto lauką po medžio struktūra. Kelio pavadinime skiriamos didžiosios ir mažosios raidės. Norėdami įtraukti paskirties vietą į nuskaitymą, pažymėkite jos žymės langelį medžio struktūroje.

Išplėstinės nuskaitymo parinktys

Šiame lange galite nurodyti suplanuotos kompiuterio nuskaitymo užduoties išplėstines parinktis. Išskleidžiamajame meniu galite nustatyti veiksmą, kuris bus atliekamas automatiškai pabaigus nuskaitymą:

- **Išjungti** – pasibaigus nuskaitymui kompiuteris išjungiamas.
- **Paleisti iš naujo** – užbaigus nuskaitymą uždaromos visos atidarytos programos, o kompiuteris paleidžiamas iš naujo.
- **Prireikus paleisti iš naujo** – uždaromos visos atidarytos programos ir, jei užbaigus nuskaitymą reikalaujama, kompiuteris paleidžiamas iš naujo.
- **Miego režimas** – įrašomas jūsų seansas ir įjungiamas kompiuterio energijos taupymo režimas, kurį išjungę galite greitai tęsti darbą.
- **Sulaikytosios veiksenos režimas** – visus RAM vykdomus procesus perkelia į specialų failą standžiajame diske. Kompiuteris išjungiamas, tačiau kitą kartą įjungę galite tęsti darbą nuo ten, kur baigėte.
- **Jokių veiksmų** – užbaigus nuskaitymą nebus atliekami jokie veiksmai.

> Atminkite, kad miego režimu veikiantis kompiuteris nėra išjungtas. Jame toliau veikia pagrindinės funkcijos ir vartojama elektros energija, jei kompiuteris veikia naudodamas akumuliatorių. Jei norite pailginti akumuliatoriaus veikimo laiką, pavyzdžiui, išvykę iš biuro, rekomenduojame naudoti sulaikytosios veiksenos režimą.

Pasirinkite **Veiksmo negali atšaukti vartotojas**, kad uždraustumėte neįgaliotiems vartotojams sustabdyti veiksmus, kurie atliekami užbaigus nuskaitymą.

Jei ribotų teisių vartotojui norite leisti nurodytam laikui pristabdyti kompiuterio nuskaitymą, pasirinkite parinktį **Vartotojas nuskaitymą gali pristabdyti (min.)**.

Taip pat žiūrėkite skyrių Nuskaitymo eiga.

Įrenginio kontrolė

ESET Endpoint Security atlieka automatinę įrenginių (CD / DVD / USB / ...) kontrolę. Šis modulis leidžia blokuoti arba koreguoti išplėstinius filtrus / teises ir pasirinkti, kaip vartotojas gali naudotis ir dirbti su nurodytais įrenginiais. Tai gali būti naudinga, jei kompiuterio administratorius nori neleisti naudotis įrenginiais, kuriuose yra nepageidaujamo turinio.

Palaikomi išoriniai įrenginiai:

- Disko atminties įrenginys (HDD, USB keičiamasis diskas)
- CD/DVD
- spausdintuvas USB
- FireWire kaupiklis
- „Bluetooth“ įrenginys
- Lustinių kortelių skaitytuvas
- Vaizdavimo įrenginys

- Modemas
- LPT/COM prievadas
- Nešiojamasis įrenginys (baterijomis maitinami įrenginiai, pvz., medijos leistuvai, išmanieji telefonai, „prijungti ir leisti“ įrenginiai ir kt.)
- Visi įrenginių tipai

Įrenginių kontrolės nustatymų parinktys gali būti keičiamos per **Išplėstiniai nustatymai** (F5) > **Įrenginio kontrolė**.

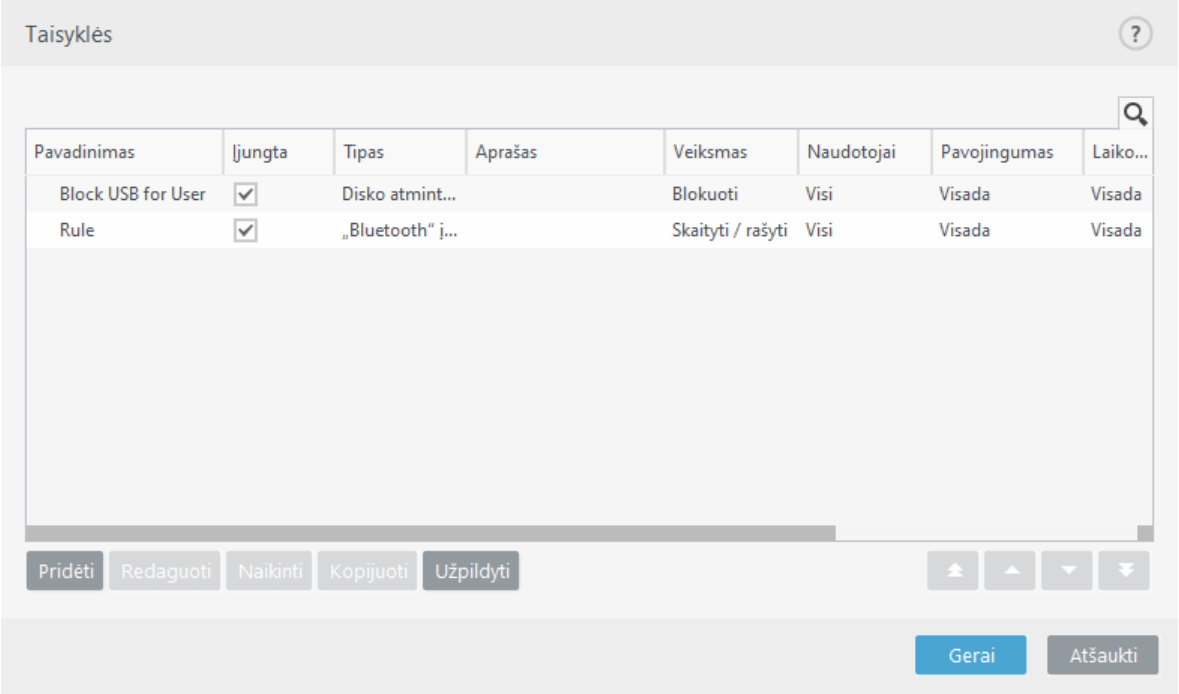
Įjungus jungiklį šalia punkto **Įjungti įrenginio kontrolę**, suaktyvinama ESET Endpoint Security įrenginio kontrolės funkcija. Kad šis pakeitimas įsigaliotų, turėsite iš naujo paleisti kompiuterį. Įjungus įrenginio kontrolę, parinktis **Taisyklės** taps aktyvi ir bus galima atidaryti langą Taisyklių rengyklė.

Jei bus prijungtas įrenginys, kurį blokuoja esama taisyklė, pasirodys pranešimo langas ir prieiga prie įrenginio suteikta nebus.

Įrenginio kontrolės taisyklių rengyklė

Lange **Įrenginio kontrolės taisyklių rengyklė** rodomos esančios taisyklės ir jame galima tiksliai kontroliuoti išorinius įrenginius, kuriuos vartotojai prijungia prie kompiuterio. Taip pat žr. Įrenginio valdymo taisyklių įtraukimas.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Įrenginių valdymo taisyklių įtraukimas ir modifikavimas naudojant ESET įrenginių produktus



Konkrečius įrenginius galima leisti arba blokuoti pagal jų vartotoją, vartotojų grupę ar bet kuriuos kelis papildomus parametrus, kuriuos galima nustatyti taisyklės konfigūracijoje. Taisyklių sąraše yra keletas taisyklės aprašymų, tokių kaip išorinio įrenginio pavadinimas, tipas, veiksmas, kurį reikia atlikti po to, kai išorinis įrenginys prijungiamas prie jūsų kompiuterio, ir žurnalo svarba.

Spustelėkite **Pridėti** arba **Redaguoti** norėdami tvarkyti taisyklę. Panaikinkite žymės langelio **Įjungta** žymėjimą šalia taisyklės, kad išjungtumėte ją, kol ją vėl norėsite naudoti. Pasirinkite vieną ar kelias taisykles ir spustelėkite **Naikinti**, kad taisyklę (-es) panaikintumėte visam laikui.

Kopijuoti – sukuriama nauja taisyklė su iš anksto nustatytomis parinktimis, naudojamomis kitoje pasirinktoje taisyklėje.

Spustelėkite parinktį **Susieti**, kad automatiškai susietumėte nešiojamosios laikmenos įrenginio parametrus, skirtus prie kompiuterio prijungtiems įrenginiams.

Taisyklės sąraše išdėstomos pagal prioritetus: kuo aukštesnis prioritetas, tuo arčiau viršaus yra taisyklė. Taisykles galite perkelti spustelėdami  **Viršus / aukštyn / žemyn / apačia**; jas galite perkelti po vieną arba grupėmis.

Įrenginio kontrolės žurnale registruojami visi įvykiai, kai buvo suaktyvinta įrenginio kontrolė. Žurnalo įrašai gali būti peržiūrimi iš pagrindinio ESET Endpoint Security programos lango, pasirinkus **Įrankiai** > **Žurnalo failai**.

Aptikti įrenginiai

Mygtukas **Pateikti** parodo visų šiuo metu prijungtų įrenginių apžvalgą su informacija apie įrenginio tipą, įrenginio tiekėją, modelį ir serijos numerį (jei toks yra).

Pasirinkite įrenginį iš aptiktų įrenginių sąrašo ir spustelėkite **Gerai**, kad įtrauktumėte įrenginio kontrolės taisyklę su iš anksto nustatyta informacija (visus nustatymus galima koreguoti).

Mažos galios (miego) režimu veikiantys įrenginiai pažymėti įspėjamąja piktograma . Norėdami įgalinti mygtuką **Gerai** ir įtraukti šio įrenginio taisyklę, atlikite šiuos veiksmus:

- Iš najujo prijunkite įrenginį.
- Naudokite įrenginį (pvz., „Windows“ paleiskite programą „Kamera“, kad pažadintumėte internetinę kamerą).

Įrenginių grupės

⚠ Prie kompiuterio prijungtas įrenginys gali kelti saugumo pavojų.

Įrenginių grupių langas yra padalytas į dvi dalis. Dešinėje lango pusėje yra įrenginių, kurie priklauso atitinkamai grupei, sąrašas, o kairėje – sukurtos grupės. Pasirinkite grupę su reikiamu įrenginių sąrašu, kad ji būtų parodyta dešiniajame polangyje.

Atidarę įrenginių grupių langą ir pasirinkę grupę galite į sąrašą pridėti įrenginių arba jų pašalinti. Kita būdas pridėti įrenginių prie grupės – importuoti juos iš failo. Arba galite spustelėti mygtuką **Surinkti**, kad visi prie kompiuterio prijungti įrenginiai būtų pateikti lange **Aptikti įrenginiai**. Spustelėdami **Gerai** sudarytame sąraše pasirinkite įrenginius, kuriuos norite pridėti prie grupės.

Valdymo elementai

Pridėti – galite pridėti grupę įrašydami jos pavadinimą, arba pridėti įrenginį prie esamos grupės (jei norite, galite nurodyti daugiau informacijos, pavyzdžiui, tiekėjo pavadinimą, modelį ir serijos numerį) – tai priklauso nuo to, kurioje lango dalyje spustelite mygtuką.

Redaguoti – jums leidžiama keisti pasirinktos grupės pavadinimą ar įrenginio parametrus (teikėją, modelį, serijos numerį).

Naikinti – atsižvelgiant į tai, kurioje lango dalyje spustelėjote mygtuką, panaikinama pasirinkta grupė ar įrenginys.

Importuoti – importuojamas įrenginių sąrašas iš tekstinio failo. Norint importuoti įrenginius iš tekstinio failo, reikalingas tinkamas formatavimas.

- Kiekvienas įrenginys pateikiamas naujoje eilutėje.
- **Tiekėjas ,** Modelis **ir Serijos numeris** turi būti pateikti kiekvienam įrenginiui ir atskirti kableliu.

Tekstinių failų turinio pavyzdys:

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

Eksportuoti – eksportuoja įrenginių sąrašą į failą.

Mygtukas **Pateikti** parodo visų šiuo metu prijungtų įrenginių apžvalgą su informacija apie įrenginio tipą, įrenginio tiekėją, modelį ir serijos numerį (jei toks yra).

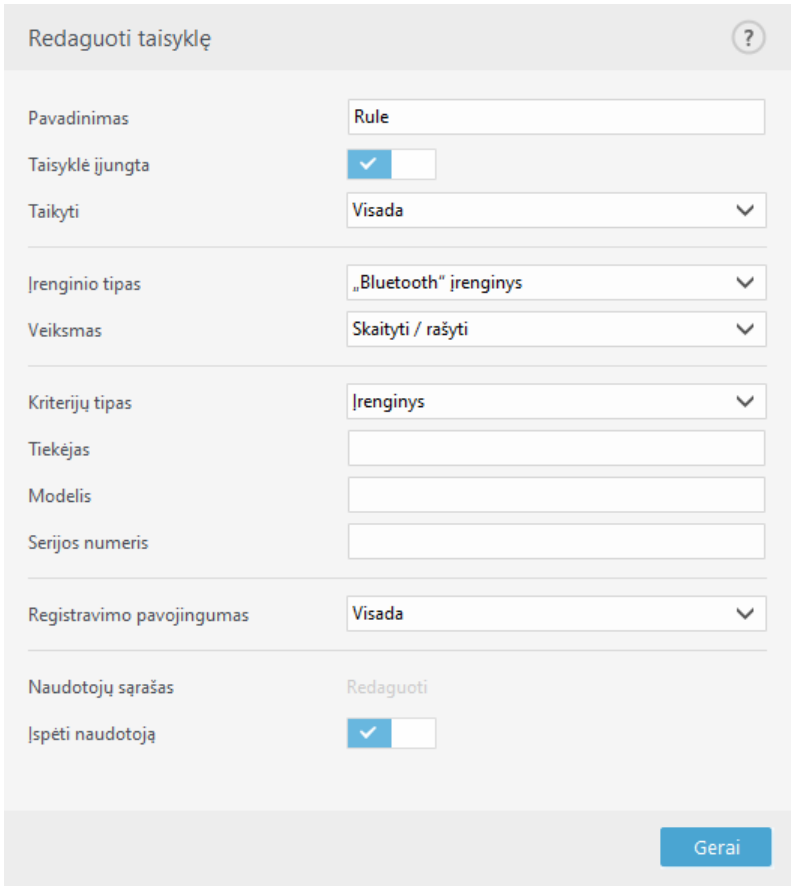
Baigę tinkinti, spustelėkite **Gerai**. Spustelėkite **Atšaukti**, jei langą **Įrenginių grupės** norite uždaryti neįrašę pakeitimų.

Galite sukurti įvairias įrenginių grupes, kurioms bus taikomos skirtingos taisyklės. Be to, galite sukurti tik vieną įrenginių grupę, kuriai bus taikoma taisyklė su veiksmu **Skaityti / rašyti** arba **Tik skaityti**. Taip užtikrinama, kad bus blokuojami įrenginių valdymo neatpažinti įrenginiai, kai juos prijungiate prie kompiuterio.

Atminkite, kad ne visos teisės (veiksmai) suteikiamos visų tipų įrenginiams. Jei naudojate atminties įrenginį, leidžiami visi keturi veiksmai. Ne atminties įrenginiuose leidžiami tik trys veiksmai (pavyzdžiui, veiksmas **Tik skaitomas** negali būti taikomas „Bluetooth“, todėl „Bluetooth“ įrenginys gali būti tik leidžiamas, užblokuotas arba dėl jo pateikiamas įspėjimas).

Įrenginio kontrolės taisyklių pridėjimas

Įrenginio kontrolės taisyklė apibrėžia veiksmą, kuris bus atliekamas, kai įrenginys, atitinkantis taisyklės kriterijų, bus prijungtas prie kompiuterio.



Kad būtų patogiau nustatyti, įveskite taisyklės aprašymą į lauką **Pavadinimas**. Spustelėkite jungiklį šalia **Taisyklė įjungta**, kad išjungtumėte arba įjungtumėte šią taisyklę. Tai gali būti naudinga, jei nenorite taisyklės panaikinti visam laikui.

Taikyti per – leidžia tam tikru laiku taikyti sukurtą taisyklę. Iš išskleidžiamojo meniu pasirinkite sukurtą laiko intervalą. Žr. daugiau informacijos apie laiko intervalus.

Įrenginio tipas

Iš išskleidžiamojo meniu pasirinkite išorinio įrenginio tipą (diskų atminties įrenginys / nešiojamasis įrenginys „Bluetooth“ / „FireWire“ / ...). Įrenginių tipų informacija gaunama iš operacinės sistemos, o jei įrenginys prijungtas prie kompiuterio, ją galima peržiūrėti sistemos įrenginių tvarkytuvėje. Atminties įrenginiai gali būti išoriniai diskai arba įprasti atminties kortelių skaitytuvai, prijungti per USB arba „FireWire“. Lustinių kortelių skaitytuvai – tai visi skaitytuvai, nuskaitantys lustines korteles su lustu, pvz., SIM arba atpažinimo korteles. Vaizdo įrenginių pavyzdžiai yra skaitytuvai arba kameros. Kadangi šie įrenginiai pateikia informaciją tik apie savo veiksmus, o ne apie vartotojus, juos galima užblokuoti tik visuotinai.

> Vartotojų sąrašo funkcija neveikia su modemo įrenginio tipu. Taisyklė bus taikoma visiems vartotojams, o dabartinis vartotojų sąrašas bus panaikintas.

Veiksmas

Prieiga prie ne atminties įrenginių gali būti leidžiama arba blokuojama. Tuo tarpu atminties įrenginių taisyklės leidžia pasirinkti vieną šių teisių parametrų:

- **Skaityti / rašyti** – bus leidžiama visa prieiga prie įrenginio.
- **Blokuoti** – prieiga prie įrenginio bus blokuojama.

- **Tik skaitomas** – bus leidžiama įrenginį tik skaityti.
- **Įspėti** – kaskart prijungus įrenginį, vartotojui pranešama, ar jis leidžiamas / blokuojamas, ir sukuriamas žurnalo įrašas. Įrenginiai neįsimenami, o kitą kartą prijungus tą patį įrenginį vis tiek parodomas pranešimas.

Atminkite, kad ne visos teisės (veiksmai) suteikiamos visų tipų įrenginiams. Jei naudojate atminties įrenginį, leidžiami visi keturi veiksmai. Ne atminties įrenginiuose leidžiami tik trys veiksmai (pavyzdžiui, veiksmas **Tik skaitomas** negali būti taikomas „Bluetooth“, todėl „Bluetooth“ įrenginys gali būti tik leidžiamas, užblokuotas arba dėl jo pateikiamas įspėjimas).

Kriterijų tipas

Pasirinkite **Įrenginių grupė** arba **Įrenginys**.

Toliau pateikiami papildomi parametrai, kurie gali būti naudojami taisyklėms pakoreguoti ir pritaikyti jas įrenginiams. Visiems parametrams yra svarbios didžiosios ar mažosios raidės:

- **Tiekėjas** – filtruokite pagal tiekėjo pavadinimą arba ID.
- **Modelis** – duotas įrenginio pavadinimas.
- **Serijos numeris** – išoriniai įrenginiai dažniausiai turi savo serijos numerį. CD / DVD tai yra duotos laikmenos, o ne CD įrenginio serijos numeris.

Jei šie parametrai nenustatomi, taisyklė ieškodama atitikmenų šios taisyklės nepaisys. Filtravimo parametrai visuose teksto laukuose skiria didžiąsias ir mažąsias raides ir nepalaiko pakaitos simbolių (*, ?).

Jei norite peržiūrėti informaciją apie įrenginį, sukurkite šio tipo įrenginiui taisyklę, prijunkite įrenginį prie kompiuterio, tada patikrinkite išsamią įrenginio informaciją, kuri pateikiama Įrenginių valdymo žurnale.

Registravimo svarbumas

- **Visada** – registruojami visi įvykiai.
- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą.
- **Informacija** – įrašo informacinius pranešimus, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – įrašo kritines klaidas bei įspėjimo pranešimus ir siunčia juos į ERA Server.
- **Nėra** – žurnalai nekuriami.

Taisyklės gali būti ribojamos tam tikriems vartotojams arba vartotojų grupėms įtraukiant juos į **Vartotojų sąrašą**:

- **Pridėti** – atidaro **objekto tipus: Vartotojų arba grupių** dialogo langas leidžia pasirinkti norimus vartotojus.
- **Šalinti** – šalina pasirinktą vartotoją iš filtro.

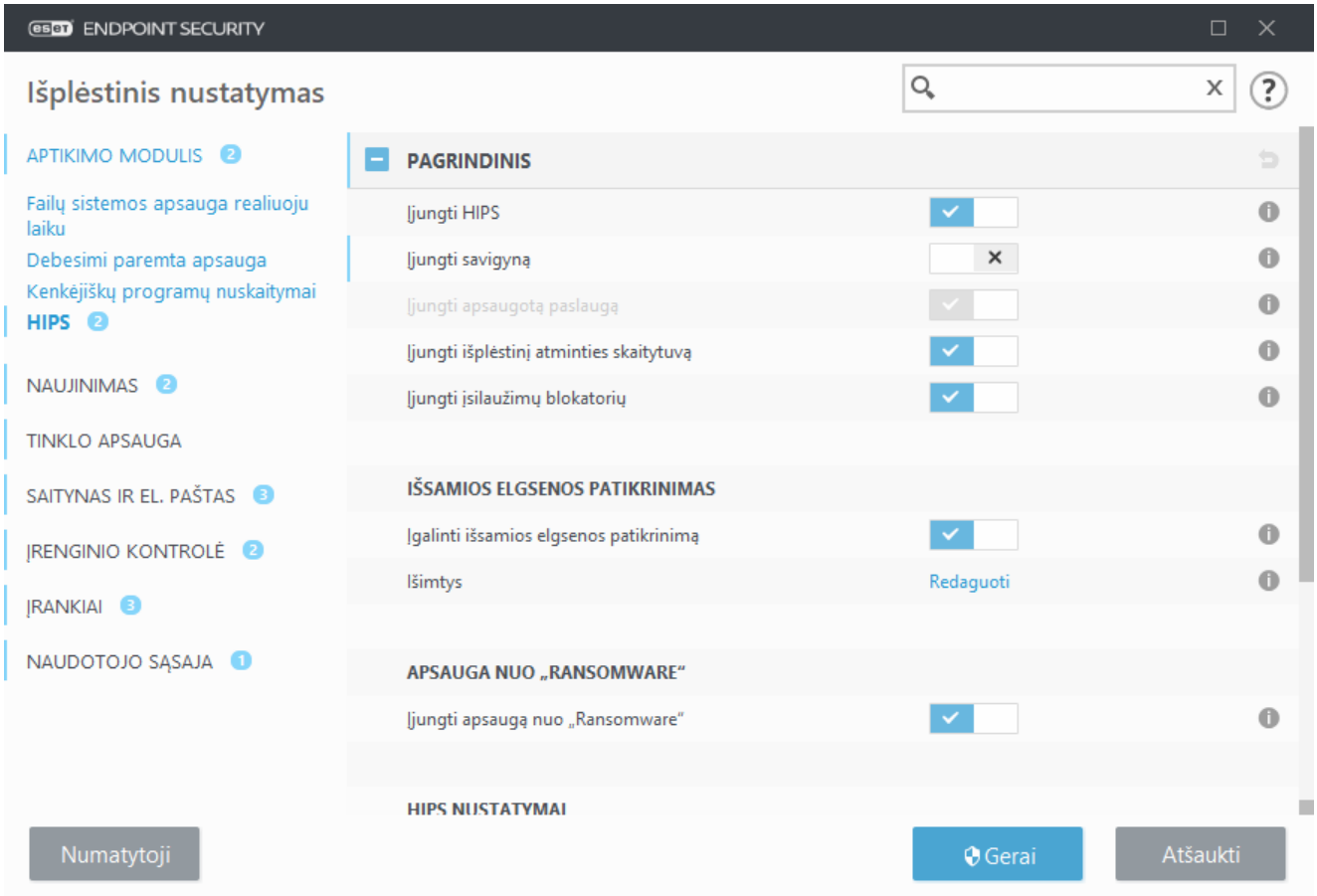
Ne visi įrenginiai gali būti filtruojami pagal vartotojo taisykles (pvz., vaizdo įrenginiai nepateikia informacijos apie vartotojus, tik apie veiksmus).

Pagrindinio kompiuterio apsaugos nuo įsilaužimo sistema (HIPS)

HIPS parametrų keitimus gali atlikti tik patyręs vartotojas. Netinkamai sukonfigūravus HIPS parametrus gali būti paveiktas sistemos veikimo stabilumas.

Pagrindinio kompiuterio apsaugos nuo įsilaužimo sistema (HIPS) saugo jūsų sistemą nuo kenkimo programinės įrangos ir nepageidaujamų veiksmų, bandančių neigiamai paveikti jūsų kompiuterį. HIPS naudoja išplėstinę veikimo analizę, suderintą su tinklo filtravimo aptikimo galimybėmis, kad būtų galima stebėti vykdomus procesus, failus ir registrų raktus. HIPS veikia atskirai nuo failų sistemos apsaugos realiuoju laiku ir nėra užkarda; ji tik stebi operacinėje sistemoje vykdomus procesus.

HIPS parametrus galima rasti čia: **Išplėstiniai nustatymai** (F5) > **Aptikimo modulis** > **HIPS** > **Bendra**. HIPS būsena (įjungta / išjungta) rodoma ESET Endpoint Security pagrindiniame programos lange (**Nustatymas** > **Kompiuteris**).



Pagrindinis

Įjungti HIPS – programoje ESET Endpoint Security HIPS yra įjungta pagal numatytuosius nustatymus. Išjungus HIPS išjungiamos visos kitos HIPS funkcijos, pvz., Įsilaužimų blokatorius.

Įjungti savigyną – ESET Endpoint Security yra integruota **Savigynos** technologija (HIPS funkcijos dalis), kuri neleidžia kenkėjiškai programinei įrangai sugadinti arba išjungti jūsų apsaugos nuo virusų ir šnipinėjimo programų. Savigynos technologija saugo svarbiausią sistemą ir ESET procesus, registrų raktus ir failus nuo sugadinimo. ESET Management Agentas saugomas ir įdiegus.

Įjungti apsaugotą paslaugą – įjungia ESET tarnybos (ekrn.exe) apsaugą. Ją įjungus tarnyba paleidžiama kaip apsaugotas „Windows“ procesas apsaugai nuo kenkėjiškos programinės įrangos. Ši parinktis pasiekiama Windows 8.1 ir Windows 10.

Įjungti išplėstinį atminties skaitytuvą – veikia kartu su spragų išnaudojimo blokatoriumi ir sustiprina apsaugą nuo

kenkimo programinės įrangos, kuri buvo sukurta siekiant išvengti apsaugos nuo kenkimo programinės įrangos aptikimo, pasitelkiant klaidinimo arba šifravimo priemones. Išplėstinis atminties skaitytuvas būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.

Įjungti įsilaužimų blokatorių – sustiprina programas, į kurias įsilaužiama dažniausiai, pavyzdžiui, saityno naršykles, PDF skaitymo programas, el. pašto programas ir „MS Office“ komponentus. Įsilaužimų blokatorius būna įjungtas pagal numatytąją parinktį. Daugiau apie šio tipo apsaugą skaitykite terminų žodyne.

Išsamios elgsenos patikrinimas

Įgalinti išsamios elgsenos patikrinimą – kitas apsaugos lygis, naudojamas kaip HIPS funkcija. Šis HIPS plėtinys analizuoja visų kompiuteryje veikiančių programų elgseną ir įspėja jus, jei proceso elgsena yra kenkėjiška.

HIPS išskyrimai iš išsamaus elgsenos patikrinimo leidžia į nuskaitymą neįtraukti procesų. Kad visi procesai būtų nuskaityti ieškant galimų grėsmių, išimtis rekomenduojame kurti tik kai tai visiškai būtina.

Apsauga nuo išpirkos reikalaujančių programų

Įjungti apsaugą nuo „Ransomware“ – tai dar vienas apsaugos lygmuo, kuris veikia kaip HIPS funkcijos dalis. Jei norite, kad apsauga nuo „Ransomware“ veiktų tinkamai, turite įjungti ESET LiveGrid® reputacijos sistemą. Skaitykite daugiau apie šio tipo apsaugą.

Įjungti audito režimą – visi apsaugos nuo „Ransomware“ aptikimai automatiškai neblokuojami, bet registruojami su įspėjimo kategorija ir siunčiami į valdymo konsolę su žyme AUDITO REŽIMAS. Administratorius gali išskirti aptikimą, kad jis daugiau nebebūtų aptinkamas arba palikti jį įjungtą, todėl išjungus audito režimą jis bus užblokuotas ir pašalintas. Audito režimo įjungimas / išjungimas taip pat registruojamas ESET Endpoint Security. Ši parinktis pasiekiama tik ESET PROTECT politikos konfigūracijos redagavimo programoje.

HIPS nustatymai

Filtravimo režimas gali būti atliekamas vienu iš toliau nurodytų režimų:

Filtravimo režimas	Aprašymas
Automatinis režimas	operacijos yra leidžiamos, išskyrus blokuojamas iš anksto nustatytomis taisyklėmis, kurios apsaugo jūsų sistemą.
Išmanusis režimas	Vartotojas informuojamas tik apie labai įtartinus įvykius.
Interaktyvusis režimas	Vartotojas bus raginamas patvirtinti operacijas.
Politika pagrįstas režimas	blokuoja visas operacijas, kurios nėra apibrėžtos konkrečia ją leidžiančia taisykle.
Mokymosi režimas	Operacijos įjungiamos ir taisyklė sukuriama po kiekvienos operacijos. Šiuo režimu sukurtas taisykles galima peržiūrėti **HIPS taisyklių** rengyklėje, tačiau jų prioritetas yra mažesnis nei rankiniu būdu arba automatiniu režimu sukurtų taisyklių prioritetas. **Filtravimo režimo** išskleidžiamajame meniu pasirinkus **mokymosi režimą** atsiranda nustatymas **Mokymosi režimas bus išjungtas**. Pasirinkite laikotarpį, kuriam norite įjungti mokymosi režimą (ilgiausia trukmė yra 14 d.). Kai nurodytas laikotarpis pasibaigia, jūsų prašoma pakeisti taisykles, sukurtas HIPS veikiant mokymosi režimu. Galite pasirinkti ir kitą filtravimo režimą arba atidėti šį pasirinkimą ir toliau naudoti mokymosi režimą.

Režimas įjungiamas pasibaigus mokymosi režimo laikui – pasirinkite filtravimo režimą, kuris bus naudojamas

pasibaigus mokymosi režimo laikui. Pasibaigus, parinktis **Teirautis naudotojo** prašo administratoriaus teisių, kad galėtų atlikti HIPS filtravimo režimo pakeitimą.

HIPS sistema stebi įvykius operacinėje sistemoje ir atitinkamai reaguoja, atsižvelgdama į taisykles, kurios yra panašios į užkardos naudojamas taisykles. Spustelėkite **Redaguoti** šalia **taisyklių**, kad būtų atidaryta **HIPS taisyklės HIPS** rengyklė. HIPS taisyklių lange galite pasirinkti, pridėti, redaguoti arba šalinti taisykles. Daugiau informacijos apie taisyklių kūrimą ir HIPS operacijas rasite skyriuje HIPS taisyklės redagavimas.

HIPS interaktyvusis langas

HIPS pranešimo lange galite sukurti taisyklę, paremtą naujais veiksmais, kuriuos aptinka HIPS, ir tada apibrėžti sąlygas, kuriomis leidžiamas arba uždraudžiamas šis veiksmas.

Pranešimo lange sukurtos taisyklės laikomos prilygstančiomis taisyklėms, sukurtoms rankiniu būdu. Taisyklė, sukurta pranešimo lange, gali būti ne tokia konkreti kaip šį dialogo langą suaktyvinusi taisyklė. Tai reiškia, kad, sukūrus taisyklę dialogo lange, tokia pati operacija gali suaktyvinti tą patį langą. Jei reikia daugiau informacijos, žr. HIPS taisyklių pirmenybė.

Jei numatytasis taisyklės veiksmas yra **Kaskart klausti**, kaskart susidarius taisyklės taikymo sąlygoms pasirodys dialogo langas. Galite pasirinkti **Uždrausti** arba **Leisti** operaciją. Jei per skirtą laiką nepasirinksite veiksmo, naujas veiksmas bus pasirinktas pagal taisykles.

Parinktis **Prisiminti, kol programa baigs darbą** leidžia naudoti veiksmą (**Leisti / drausti**) tol, kol bus pakeistos taisyklės ar filtravimo režimas, bus atnaujintas HIPS modulis ar sistema bus paleista iš naujo. Atlikus bet kuriuos iš šių trijų veiksmų laikinosios taisyklės bus panaikintos.

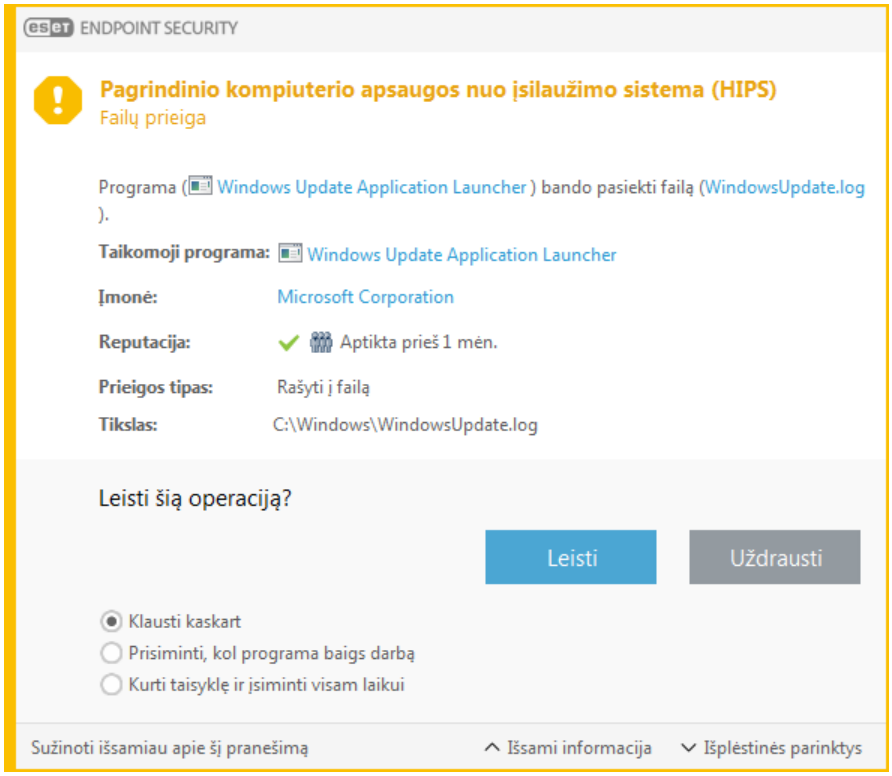
Parinktis **Kurti taisyklę ir įsiminti visam laikui** sukurs naują HIPS taisyklę, kurią vėliau galima pakeisti dalyje HIPS taisyklių tvarkymas (būtinos administratoriaus teisės).

Apačioje spustelėkite **Išsami informacija**, kad pamatytumėte kuri programa aktyvina operaciją, kokia failo reputacija arba kokią operaciją prašoma leisti arba drausti.

Išsamesnius taisyklės parametrų nustatymus pasieksite spustelėję **Išplėstinės parinktys**. Tolesnės parinktys pasiekiamos pasirinkus **Kurti taisyklę ir įsiminti visam laikui**:

- **Sukurti taisyklę, galiojančią tik šiai programai** – jei išvalote šį žymės langelį, taisyklė bus sukurta visoms šaltinio programoms.
- **Tik šiai operacijai** – pasirinkite taisyklės failą / programą / registro operaciją (-as). Žr. visų HIPS operacijų aprašus.
- **Tik šiam tikslui** – pasirinkite taisyklės failą / programą / registro tikslą (-us).

Norėdami, kad pranešimai nebebūtų rodomi, pakeiskite filtravimo režimą į **Automatinis režimas** dalyje **Išplėstiniai nustatymai** (F5) > **Aptikimo modulis** > **HIPS** > **Bendra**.



Aptiktas potencialus „Ransomware“ viruso elgesys

Šis interaktyvusis langas pasirodys, kai bus aptiktas „Ransomware“ viruso elgesys. Galite pasirinkti **Uždrausti** arba **Leisti** operaciją.

Spustelėkite **Išsami informacija** ir peržiūrėkite konkrečius aptikimo parametrus. Šiame dialogo lange galite **pateikti failą analizei** ar **neįtraukti į aptikimą**.

kad apsauga nuo „Ransomware“ viruso veiktų tinkamai, būtina įjungti ESET LiveGrid®.

HIPS taisyklių tvarkymas

Vartotojo apibrėžtų ir automatiškai įtrauktų taisyklių iš HIPS sistemos sąrašas. Daugiau informacijos apie taisyklių kūrimą ir HIPS operacijas galima rasti skyriuje HIPS taisyklių nustatymai. Taip pat žr. Bendrieji HIPS principai.

Stulpeliai

Taisyklė – vartotojo pasirinktas arba automatiškai sukurtas taisyklės pavadinimas.

Įjungta – išjunkite šią parinktį, jei taisyklę norite išlaikyti sąraše, bet nenorite jos naudoti.
Veiksmas – taisykle apibrėžiamas veiksmas – **Leisti**, **Blokuoti** arba **Klausti** – kuris turi būti atliekamas esant tinkamoms sąlygoms.

Šaltiniai – taisyklė bus naudojama, tik jei įvykis suaktyvinamas šios (šių) taikomosios (-ųjų) programos (-ų).

Paskirtis – taisyklė bus naudojama tik tada, jei operacija yra susijusi su konkrečiu failu, programa ar registro įrašu.

Registravimo svarbumas – jei suaktyvinsite šią parinktį, informacija apie šią taisyklę bus įrašyta į HIPS žurnalą.

Pranešti – suaktyvinus veiksmą apatiniame dešiniajame kampe pasirodys mažas iškylantysis pranešimas.

Valdymo elementai

Pridėti – sukuriama nauja taisyklė.

Redaguoti – leidžia redaguoti pasirinktus įrašus.

Šalinti – pašalinami pasirinkti įrašai.

HIPS taisyklių pirmenybė

HIPS taisyklių pirmenybės lygio negalima reguliuoti mygtukais aukštyn / žemyn (kaip Užkardos taisyklių, kurias galima vykdyti iš viršaus į apačią).

- Visos sukurtos taisyklės yra lygiavertės
- Kuo konkretesnė taisyklė, tuo didesnė pirmenybė (pvz., konkrečios programos taisyklė turi didesnę pirmenybę, nei taisyklė visoms programoms)
- HIPS turi didesnės pirmenybės vidinių taisyklių, kurios nėra jums pasiekiamos (pvz., negalite apeiti savigynos taisyklių)
- Jūsų sukurtos taisyklės, dėl kurių gali užstrigti operacinė sistema, nebus taikomos (jų pirmenybė bus mažiausia).

HIPS taisyklės parametrai

Pirmiausia žr. HIPS taisyklių tvarkymas.

Taisyklės pavadinimas – vartotojo pasirinktas arba automatiškai sukurtas taisyklės pavadinimas.

Veiksmas – nurodomas veiksmas – Leisti, Blokuoti arba Klausti – kuris turi būti atliekamas, kai tenkinamos nustatytos sąlygos.

Susijusios operacijos – turite pasirinkti operacijų tipą, kuriam bus taikoma taisyklė. Taisyklė bus naudojama tik šio tipo operacijoms ir pasirinktam tikslui.

Įjungta – išjunkite šį jungiklį, jei taisyklę norite išlaikyti sąraše, bet nenorite jos taikyti.

Registravimo svarbumas – jei suaktyvinsite šią parinktį, informacija apie šią taisyklę bus įrašyta į HIPS žurnalą.

Pranešti vartotojui – mažas iškylantysis langas parodomas apatiniame dešiniajame kampe, jei paleidžiamas įvykis.

Taisyklė sudaryta iš dalių, kurios apibūdina sąlygas, įjungiančias šią taisyklę:

Šaltinio programos– taisyklė bus naudojama, tik jei įvykį paleidžia ši (šios) programa (-os). Išskleidžiamajame

meniu pasirinkite **Konkrečios programos** ir spustelėkite **Pridėti**, kad pridėtumėte naujų failų ar aplankų, arba išskleidžiamajame meniu galite pasirinkti **Visos programos** ir pridėti visas programas.

Tiksliniai failai – taisyklė bus naudojama, tik jei operacija bus susijusi su šiuo tikslu. Išskleidžiamajame meniu pasirinkite **Konkretūs failai** ir spustelėkite **Pridėti**, kad pridėtumėte naujų failų ar aplankų, arba išskleidžiamajame meniu galite pasirinkti **Visi failai** ir pridėti visus failus.

Programos– taisyklė bus naudojama, tik jei operacija bus susijusi su šiuo tikslu. Išskleidžiamajame meniu pasirinkite **Konkrečios programos** ir spustelėkite **Pridėti**, kad pridėtumėte naujų failų ar aplankų, arba išskleidžiamajame meniu galite pasirinkti **Visos programos** ir pridėti visas programas.

Registro įrašai– taisyklė bus naudojama, tik jei operacija bus susijusi su šiuo tikslu. Išskleidžiamajame meniu pasirinkite **Konkretūs įrašai** ir spustelėkite **Pridėti**, kad pridėtumėte naujų failų ar aplankų, arba išskleidžiamajame meniu galite pasirinkti **Visi įrašai** ir pridėti visus įrašus.

> **i** Kai kurių tam tikrų taisyklių iš anksto HIPS nustatytų operacijų negalima užblokuoti, todėl jos yra leidžiamos pagal numatytuosius nustatymus. Be to, ne visos sistemos operacijos yra stebimos HIPS. HIPS stebi operacijas, kurios gali būti laikomos nesaugiomis.

> **i** Nurodant kelią, C:\example paveikia veiksmus su pačiu aplanku, o C:\example*.* paveikia failus aplanke.

Programų operacijos

- **Derinti kitą programą** – derinimo modulis prijungiamas prie proceso. Derinant taikomąją programą galima peržiūrėti ir pakeisti daugelį jos veikimo detalių ir prieiti prie jos duomenų.
- **Sustabdyti kitų programų įvykiai** – šaltinio programa bando perimti įvykius, nukreiptus į konkrečią programą (pavyzdžiui, klaviatūros paspaudimų registravimo programa bando įrašyti naršyklės įvykius).
- **Nutraukti / laikinai sustabdyti kitą taikomąją programą** – laikinai sustabdo, tęsia arba nutraukia procesą (galima prieiga tiesiai iš „Process Explorer“ arba iš procesų polangio).
- **Pradėti naują taikomąją programą** – naujų programų arba procesų paleidimas.
- **Modifikuoti kitos programos būseną** – šaltinio programa bando rašyti į tikslo programos atmintį arba vykdyti kodą jos vardu. Ši funkcija gali būti naudinga norint apsaugoti svarbią programą konfigūruojant ją kaip tikslo programą taisyklėje, blokuojančioje šios operacijos naudojimą.

> **i** Neįmanoma pertraukti procesų operacijų 64 bitų „Windows XP“ versijoje.

Registrų operacijos

- **Modifikuoti paleidimo parametrus** – visi parametrų, nurodančių, kurios programos bus vykdomos paleidžiant „Windows“, keitimai. Jie gali būti aptikti, pavyzdžiui, ieškant Run rakto „Windows“ registre.
- **Naikinti iš registro** – registro rakto arba jo reikšmės naikinimas.
- **Pervardyti registro raktą** – registrų raktų pervardijimas.
- **Keisti registrą** – kuriamos naujos registro rakto reikšmės, keičiamos esamos reikšmės, duomenys perkeliami į duomenų bazės medį arba nustatomos vartotojo ar grupės teisės registro raktams.

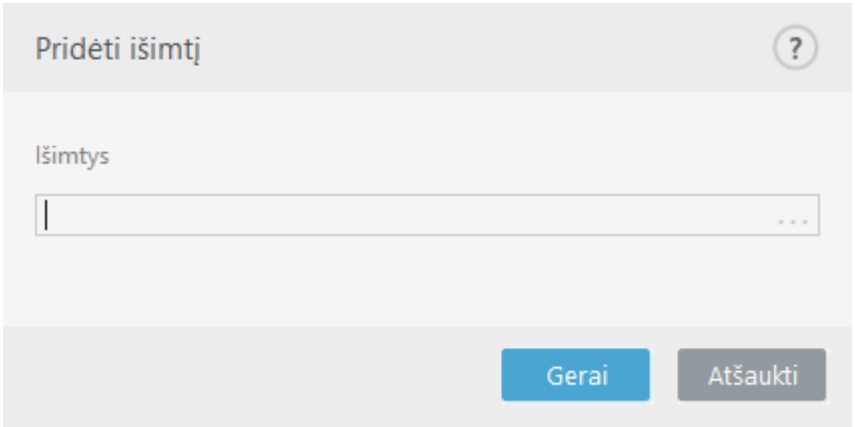
Pakaitos simbolių naudojimas taisyklėse
Žvaigždutė taisyklėse gali būti naudojama tik tam tikram raktui pakeisti, pavyzdžiui, „HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start“. Kiti pakaitos simbolių naudojimo būdai nepalaikomi.

Taisyklių, skirtų „HKEY_CURRENT_USER“ raktui, kūrimas
Šis raktas yra tik nuoroda į atitinkamą „HKEY_USERS“ dalinį raktą, skirtą vartotojui, identifikuotam pagal SID (saugų identifikatorių). Norėdami sukurti taisyklę tik dabartiniam vartotojui, užuot naudojęsi keliu į „HKEY_CURRENT_USER“, naudokitės keliu, vedančiu į „HKEY_USERS\%SID%“. Kaip SID galite naudoti žvaigždutę, kad taisyklė būtų taikoma visiems vartotojams.

Jei sukursite labai bendrą taisyklę, bus parodytas įspėjimas apie šio tipo taisyklę.

Šiame pavyzdyje parodysime, kaip uždrausti nepageidaujamus konkrečios programos veiksmus:

1. Pavadinkite taisyklę ir pasirinkite **Blokuoti** (arba **Klausti**, jei norite pasirinkti vėliau) išskleidžiamajame meniu **Veiksmas**.
2. Įjunkite jungiklį **Pranešti vartotojui**, kad pranešimas būtų rodomas kaskart pritaikius taisyklę.
3. Pasirinkite bent vieną operaciją dalyje **Aktualios operacijos**, kurioms bus taikoma taisyklė.
4. Spustelėkite **Kitas**.
5. Lango **Šaltinio programos** išskleidžiamajame meniu pasirinkite **Konkrečios programos**, kad naują taisyklę pritaikytumėte visoms programoms, kurios bandys atlikti kurią nors iš pasirinktų programų operacijų.
6. Spustelėkite **Pridėti** ir **...**, kad pasirinktumėte konkrečios programos kelią, ir paspauskite **Gerai**. Jei norite, įtraukite daugiau programų.
   Pavyzdžiui: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Pasirinkite operaciją **Rašyti į failą**.
8. Išskleidžiamajame meniu pasirinkite **Visi failai**. Taip užblokuosite ankstesniu veiksmu pasirinktos programos (-ų) bandymus įrašyti į failus.
9. Spustelėkite **Baigti**, kad naują taisyklę įrašytumėte.



HIPS išplėstinis nustatymai

Šios parinktys naudingos derinant ir analizuojant programos veikimą:

Tvarkyklės, kurias leidžiama įkelti visada – pasirinktas tvarkykles įkelti leidžiama visada, neatsižvelgiant į sukonfigūruotą filtravimo režimą, nebent naudotojo taisyklė aiškiai tai užblokuotų.

Registruoti visas užblokuotas operacijas – visos užblokuotos operacijos bus įrašytos į HIPS žurnalą. Naudokite šią funkciją tik šalinant triktis arba paprašius ESET techninio palaikymo tarnybai, nes ji gali generuoti didžiulį žurnalo

failą ir sulėtinti kompiuterį.

Pranešti, kai įvyksta pakeitimai paleidimo programose – rodo darbalaukio pranešimą kaskart, kai taikomoji programa įtraukiama arba pašalinama iš sistemos paleidimo.

Tvarkyklės, kurias leidžiama įkelti visada

Jei jos nėra aiškiai blokuojamos pagal vartotojo nustatytą taisyklę, šiame sąraše pateikiamas tvarkykles leidžiama įkelti visada, nesvarbu, koks naudojamas HIPS filtravimo režimas.

Pridėti – pridedama nauja tvarkyklė.

Redaguoti – redaguojama pasirinkta tvarkyklė.

Šalinti – tvarkyklė pašalinama iš sąrašo.

Nustatyti iš naujo – iš naujo įkeliamas sistemos tvarkyklių rinkinys.

Spustelėkite **Nustatyti iš naujo**, kad nebūtų įtrauktos rankiniu būdu jūsų pridėtos tvarkyklės. Tai gali būti naudinga, jei esate pridėję kelias tvarkykles ir negalite jų panaikinti iš sąrašo rankiniu būdu.

Pristatymo režimas

Pristatymo režimas yra funkcija, skirta vartotojams, kuriems reikalingas nepertraukiamas jų programinės įrangos naudojimas, kai norima, kad netrukdytų iškylantieji langai ir nebūtų papildomai apkraunamas procesorius. Pristatymo režimas taip pat gali būti naudojamas per pristatymus, kurie neturi būti pertraukiami antivirusinės programos veiksmų. Įjungus šį režimą, išjungiami visi iškylantieji langai ir nevykdomos planinės užduotys. Sistemos apsauga ir toliau veikia foniniu režimu, tačiau jai nereikia jokių vartotojo veiksmų.

Spustelėkite **Nustatymai** > **Kompiuteris** ir tada spustelėkite jungiklį, esantį šalia **Pristatymo režimas, kad rankiniu būdu įjungtumėte pristatymo režimą.** Skiltyje **Išplėstiniai nustatymai** (F5) spustelėkite **Įrankiai** > **Pristatymo režimas**, tada spustelėkite jungiklį šalia **Įjungti pristatymo režimą automatiškai, kai programos vykdomos viso ekrano režimu, kad ESET Endpoint Security automatiškai pereitų į pristatymo režimą, kai vykdomos viso ekrano režimu veikiančios programos**. Įjungus pristatymo režimą, iškyla galima saugumo pavojus, todėl apsaugos būsenos piktograma užduočių juostoje įspėja apie galimą pavojų ir tampa oranžinė. Be to, matysite šį įspėjimą pagrindiniame programos lange, kur **Pristatymo režimas įjungtas** švies oranžine spalva.

Įjungus punktą **Automatiškai įjungti pristatymo režimą, kai programos vykdomos visame ekrane**, pristatymo režimas įsijungs, kai tik paleisite programą, veikiančią viso ekrano režimu, ir automatiškai išsijungs užvėrus tokią programą. Tai labai naudinga, kai norite paleisti pristatymo režimą iškart, kai paleidžiate žaidimą, atidarote visame ekrane veikiančią programą arba pradedate pristatymą.

Galite papildomai pasirinkti variantą **Išjungti pristatymo režimą automatiškai po**, kad nustatytumėte, po kiek minučių pristatymo režimas bus automatiškai išjungtas.

Jeigu užkarda veikia interaktyviuoju režimu ir įjungtas pristatymo režimas, gali iškilti problemų jungiantis prie interneto. Tai gali sukelti nepatogumų, jeigu paleidžiate žaidimą, kuris jungiamas prie interneto. Paprastai jūsų būtų prašoma patvirtinti šį veiksmą (jeigu nebuvo nustatyta ryšio taisyklių arba išimčių), tačiau vartotojo veiksmai pristatymo režimu neleidžiami. Tai galite išspręsti apibrėždami taisyklę kiekvienai taikomajai programai, kuri gali būti nesuderinama su šiais veiksmais, arba užkardoje naudoti kitą filtravimo režimą. Atminkite: jei pristatymo režimas įjungtas ir jūs einate į rizikingą tinklalapį arba naudojate programą, kuri gali kelti saugumo pavojų, ji gali būti blokuojama, tačiau jūs nematysite jokio paaiškinimo arba įspėjimo, nes vartotojo veiksmai neleidžiami.

Nuskaitymas paleidžiant

Pagal numatytąją parinktį automatinė failų patikra paleidimo metu bus atliekama paleidus sistemą arba atnaujinus modulius. Šis nuskaitymas priklauso nuo Planuoklės konfigūracijos ir užduočių.

Nuskaitymo paleidžiant parinktys yra **Sistemos failų patikros paleidžiant** planuoklės užduoties dalis. Norėdami pakeisti nuskaitymo paleidžiant parametrus, eikite į **Įrankiai** > **Planuoklė**, spustelėkite **Automatinė failų patikra paleidžiant**, tada spustelėkite **Redaguoti**. Atliekant paskutinį veiksmą pasirodys langas Automatinė paleidimo failo patikra (daugiau informacijos rasite kitame skyriuje).

Norėdami rasti išsamias instrukcijas apie planuoklės užduoties kūrimą ir tvarkymą, žiūrėkite Naujų užduočių kūrimas.

Automatinė paleidimo failo patikra

Kurdami suplanuotą sistemos paleidimo failo patikros užduotį toliau pateikiamus parametrus galite pakeisti įvairiai:

Išskleidžiamajame meniu **Nuskaitymo tikslas** pasitelkus slaptą modernų algoritmą nurodomas nuskaitymo išsamumas failams, kurie vykdomi paleidžiant sistemą. Failai išdėstomi mažėjimo tvarka pagal šiuos kriterijus:

- **Visi registruotieji failai** (daugiausia nuskaitytų failų)
- **Retai naudojami failai**
- **Įprastai naudojami failai**
- **Dažnai naudojami failai**
- **Tik dažniausiai naudojami failai** (nuskaitoma mažiausiai failų)

Įtraukiamos ir dvi konkrečios grupės:

- **Failai, paleidžiami prieš prisijungiant vartotojui** – failai iš tokių vietų, kurias galima pasiekti vartotojui neprisijungus (tai beveik visos paleidimo vietos, pavyzdžiui, paslaugos, naršyklės pagalbos objektai, „winlogon“ pranešimai, „Windows“ planuoklės įrašai, žinomi dll ir pan.).
- **Failai, paleidžiami vartotojui prisijungus** – failai iš tokių vietų, kurias galima pasiekti tik vartotojui prisijungus (tai failai, kuriuos paleidžia konkretus vartotojas, paprastai šie failai yra saugomi *HKEY_CURRENT_USER**SOFTWARE**Microsoft**Windows**CurrentVersion**Run*).

Failų, kuriuos reikia nuskaityti, sąrašai yra fiksuoti kiekvienai anksčiau minėtai grupei.

Nuskaitymo prioritetas – prioriteto lygis, naudojamas nustatant, kada prasidės skenavimas:

- **Kai laisva** – užduotis bus atliekama, tik kai sistema veiks laukimo režimu,
- **Žemiausias** – esant pačiai mažiausiai sistemos apkrovai,
- **Žemesnis** – esant mažai sistemos apkrovai,
- **Įprastas** – esant vidutinei sistemos apkrovai.

Dokumentų apsauga

Dokumentų apsaugos funkcija prieš atidarant nuskaito „Microsoft Office“ dokumentus, kaip ir „Internet Explorer“ automatiškai atsisiųstus failus, pavyzdžiui, „Microsoft ActiveX“ elementus. Dokumentų apsauga pateikia papildomą apsaugos lygmenį šalia failų sistemos apsaugos realiuoju laiku ir gali būti išjungta, siekiant pagerinti efektyvumą sistemose, kuriose neapdorojamas didelis „Microsoft Office“ dokumentų kiekis.

Norėdami suaktyvinti dokumentų apsaugą, atidarykite langą **Išplėstiniai nustatymai** (spauskite **F5**) > **Aptikimo modulis** > **Kenkėjiškos programinės įrangos nuskaitymai** > **Dokumentų apsauga** ir spustelėkite jungiklį šalia punkto **Įjungti dokumentų apsaugą**.

> Šią funkciją suaktyvina programos, kurios naudoja „Microsoft Antivirus API“ (pvz., „Microsoft Office 2000“ ir naujesnės versijos arba „Microsoft Internet Explorer 5.0“ ir naujesnės versijos).

Išimtys

Išimtys leidžia neįtraukti objektų į aptikimo modulį. Kad būtų nuskaityti visi objektai, išimtis rekomenduojame kurti tik kai tai visiškai būtina. Atskiri atvejai, kai gali reikėti neįtraukti tam tikro objekto: didelės duomenų bazės įrašai, kurie lėtina kompiuterio darbą nuskaitant, ar programinė įranga, kuri konfliktuoja su nuskaitymo procesu.

Našumo išimtys leidžia neįtraukti failų ir aplankų į nuskaitymą. Našumo išimtys yra naudingos neįtraukiant žaidimų į failų lygmens nuskaitymą arba jei sukeliamas nenormalus sistemos veikimas arba didinant našumą.

Aptikimo išimtys leidžia neįtraukti objektų į valymą, naudojant aptikimo pavadinimą, kelią arba maišą. Aptikimo išimtys nepašalina failams ir aplankams taikomo nuskaitymo, tai atlieka našumo išimtys. Aptikimo išimtys taikomos objektams tik kai juos aptinka aptikimo modulis ir išimčių sąraše yra atitinkama taisyklė.

Išimtys 7.1 ir senesnėse versijose sujungia našumo išimtis ir aptikimo išimtis.

Nesupainiokite jų su kitų tipų išimtimis:

- Proceso išimtys – į nuskaitymą neįtraukiamos visos failų operacijos, priskiriamos neįtrauktos programos procesams (gali būti būtina, norint pagerinti atsarginių kopijų kūrimo greitį ir paslaugų prieinamumą).
- Neįtraukti failų plėtiniai
- HIPS išimtys
- Debesimi paremtos apsaugos išimčių filtras

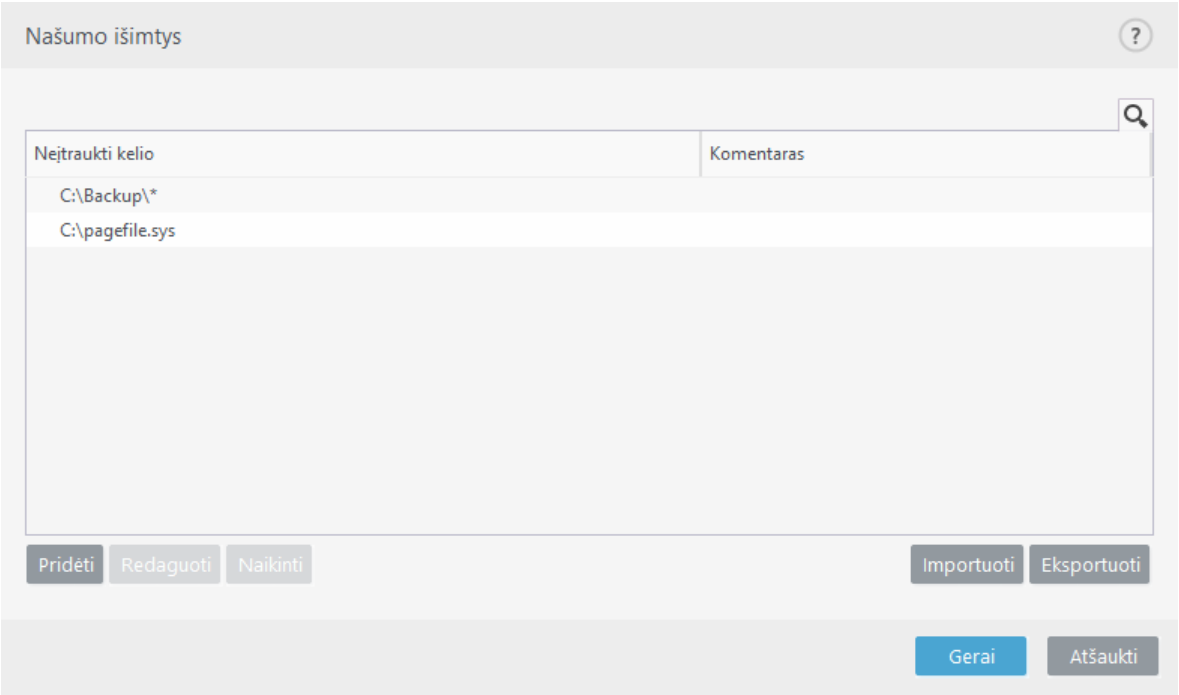
Našumo išimtys

Našumo išimtys leidžia neįtraukti failų ir aplankų į nuskaitymą.

Kad visi objektai būtų nuskaityti ieškant grėsmių, išimtis rekomenduojame kurti tik kai tai visiškai būtina. Vis dėlto yra situacijų, kai reikia neįtraukti tam tikro objekto, pavyzdžiui, didelių duomenų bazės įrašų, kurie lėtintų kompiuterio darbą nuskaitant, ar programinės įrangos, kuri nesuderinama su nuskaitymu.

Galite įtraukti failus ir aplanką į nuskaitymo išimčių sąrašą dalyje **Išplėstinis nustatymai** (F5) > **Aptikimo modulis** > **Išimtys** > **Našumo išimtys** > **Redaguoti**.

Norėdami nejtraukti objekto (kelio, failo arba aplanko) į nuskaitymą, spustelėkite **Pridėti** ir įveskite taikytiną kelią į arba pasirinkite jį medžio struktūroje.



Jei failas atitinka nuskaitymo išimties kriterijus, jame esančios grėsmės **failų sistemos apsaugos realiuoju laiku** modulis ar **kompiuterio nuskaitymo** modulis neaptiks.

Valdymo elementai

- **Pridėti** – pridėkite naują įrašą, kad išskirtumėte objektus, kurių nereikia nuskaityti.
- **Redaguoti** – leidžia redaguoti pasirinktus įrašus.
- **Šalinti** – pašalinami pasirinkti įrašai (paspauskite CTRL ir spustelėkite norėdami pasirinkti kelis įrašus).
- **Importuot / eksportuoti** – veikimo išskyrimų importavimas ir eksportavimas yra naudingas, jeigu reikia padaryti dabartinių išskyrimų atsarginę kopiją, kurią galėtumėte naudoti vėliau. Be to, nustatymų eksportavimo parinktis yra patogi naudotojams nevaldomosiose aplinkose, kurie nori pageidautiną konfigūraciją naudoti keliose sistemose – jie gali lengvai importuoti .txt failą ir perkelti šiuos nustatymus.
  Rodo importuojamo / eksportuojamo failo formato pavyzdį

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManagement.PerformanceExclusions","columns":["Path","Description"]}

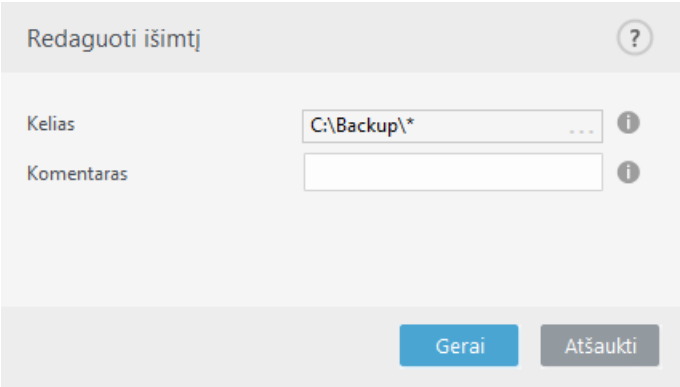
C:\Backup\*,custom comment

C:\pagefile.sys
```

Pridėti arba redaguoti našumo išimtis

Šis dialogo langas neįtraukia konkretaus kelio (failo arba katalogo) šiame kompiuteryje.

Norėdami pasirinkti tinkamą kelią, spustelėkite **...** lauke **Kelias**. Jei įvedate ranka, daugiau išimčių formatų pavyzdžių žr. toliau.



Galite naudoti pakaitos simbolius norėdami neįtraukti failų grupės. Klaustukas (*?*) reiškia vieną simbolį, o žvaigždutė (***) reiškia eilutę iš nulio ar daugiau simbolių.

- Norėdami neįtraukti visų aplanke esančių failų ir antrinių aplankų, įveskite kelią į aplanką ir naudokite kaukę ***.
- Norėdami neįtraukti tik „doc“ failų, naudokite kaukę **.doc*.
- Jei vykdomojo failo pavadinimas turi konkretų simbolių skaičių (su skirtingais simboliais) ir žinote tik pirmąjį simbolį (pavyzdžiui, „D“), naudokite šį formatą:
D????.exe (klaustukai pakeičia trūkstamus / nežinomus simbolius)

✓ Pavyzdžiai:
- *C:\Tools** – Kelias turi baigtis kairiniu brūkšniu (\) ir žvaigždute (*), kad būtų nurodyta, jog tai aplankas ir visas aplanko turinys (failai ir antriniai aplankai) nebus įtrauktas.
- *C:\Tools*.** – Toks pat elgesys kaip ir *C:\Tools**
- *C:\Tools* – *Tools* aplankui nebus taikoma išimtis. Skaitytuvui *Tools* gali atrodyti ir kaip failo pavadinimas.
- *C:\Tools*.dat* – tai neįtrauks .dat failų, esančių *Tools* aplanke.
- *C:\Tools\sg.dat* – neįtrauks šio konkretaus failo, į kurį veda konkretus kelias.

Galite naudoti sistemos kintamuosius kaip *%PROGRAMFILES%* norėdami nustatyti nuskaitymo išskyrimus.
• Jei norite neįtraukti aplanko Programiniai failai naudodami šį sistemos kintamąjį, naudokite kelią *%PROGRAMFILES%** (nepamirškite kelio gale pridėti įžambaus kairinio brūkšnio ir žvaigždutės) pridedami jį į išskyrimus.
• Jei norite neįtraukti visų pakatalogio *%PROGRAMFILES%* failų ir aplankų, naudokite kelią *%PROGRAMFILES%\Excluded_Directory**

Išskleiskite palaikomų sistemos kintamųjų sąrašą

Toliau pateikti kintamieji gali būti naudojami kelio išskyrimo formate:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Nuo naudotojų priklausantys sistemos kintamieji (pavyzdžiui, *%TEMP%* arba *%USERPROFILE%*) arba aplinkos kintamieji (pavyzdžiui, *%PATH%*) nepalaikomi.

Pakaitos simbolių naudojimas kelio viduryje (pvz., *C:\Tools*\Data\file.dat*) gali veikti, bet nėra oficialiai palaikomas veiklos išskyrimų atveju. Norėdami gauti daugiau informacijos, žr. toliau pateiktą Žinių bazės straipsnį.
Nėra jokių pakaitos simbolių naudojimo kelio viduryje apribojimų, kai naudojate aptikimo išimtis.

Išskyrimų tvarka:
• Išskyrimų pirmenybės lygio negalima reguliuoti mygtukais aukštyn / žemyn (kaip Užkardos taisyklių, kurias galima vykdyti iš viršaus į apačią).
• Kai pirma taikoma taisyklė yra suderinta skaitytuvo, antra taikoma taisyklė nebus vertinama.
• Kuo mažiau taisyklių, tuo geresnis nuskaitymų rezultatas.
• Venkite kurti jau esamas taisykles.

Kelio išskyrimo formatas

Galite naudoti pakaitos simbolius norėdami neįtraukti failų grupės. Klaustukas (*?*) reiškia vieną simbolį, o žvaigždutė (***) reiškia eilutę iš nulio ar daugiau simbolių.

• Norėdami neįtraukti visų aplanke esančių failų ir antrinių aplankų, įveskite kelią į aplanką ir naudokite kaukę **.*
• Norėdami neįtraukti tik „doc“ failų, naudokite kaukę **.doc*.
• Jei vykdomojo failo pavadinimas turi konkretų simbolių skaičių (su skirtingais simboliais) ir žinote tik pirmąjį simbolį (pavyzdžiui, „D“), naudokite šį formatą:
D????.exe (klaustukai pakeičia trūkstamus / nežinomus simbolius)
Pavyzdžiai:
• *C:\Tools** – Kelias turi baigtis kairiniu brūkšniu (\) ir žvaigždute (*), kad būtų nurodyta, jog tai aplankas ir visas aplanko turinys (failai ir antriniai aplankai) nebus įtrauktas.
• *C:\Tools*.** – Toks pat elgesys kaip ir *C:\Tools**
• *C:\Tools* – *Tools* aplankui nebus taikoma išimtis. Skaitytuvui *Tools* gali atrodyti ir kaip failo pavadinimas.
• *C:\Tools*.dat* – tai neįtrauks .dat failų, esančių *Tools* aplanke.
• *C:\Tools\sg.dat* – neįtrauks šio konkretaus failo, į kurį veda konkretus kelias.

Galite naudoti sistemos kintamuosius kaip *%PROGRAMFILES%* norėdami nustatyti nuskaitymo išskyrimus.
• Jei norite neįtraukti aplanko Programiniai failai naudodami šį sistemos kintamąjį, naudokite kelią *%PROGRAMFILES%** (nepamirškite kelio gale pridėti įžambaus kairinio brūkšnio ir žvaigždutės) pridedami jį į išskyrimus.
• Jei norite neįtraukti visų pakatalogio *%PROGRAMFILES%* failų ir aplankų, naudokite kelią *%PROGRAMFILES%\Excluded_Directory**

Išskleiskite palaikomų sistemos kintamųjų sąrašą

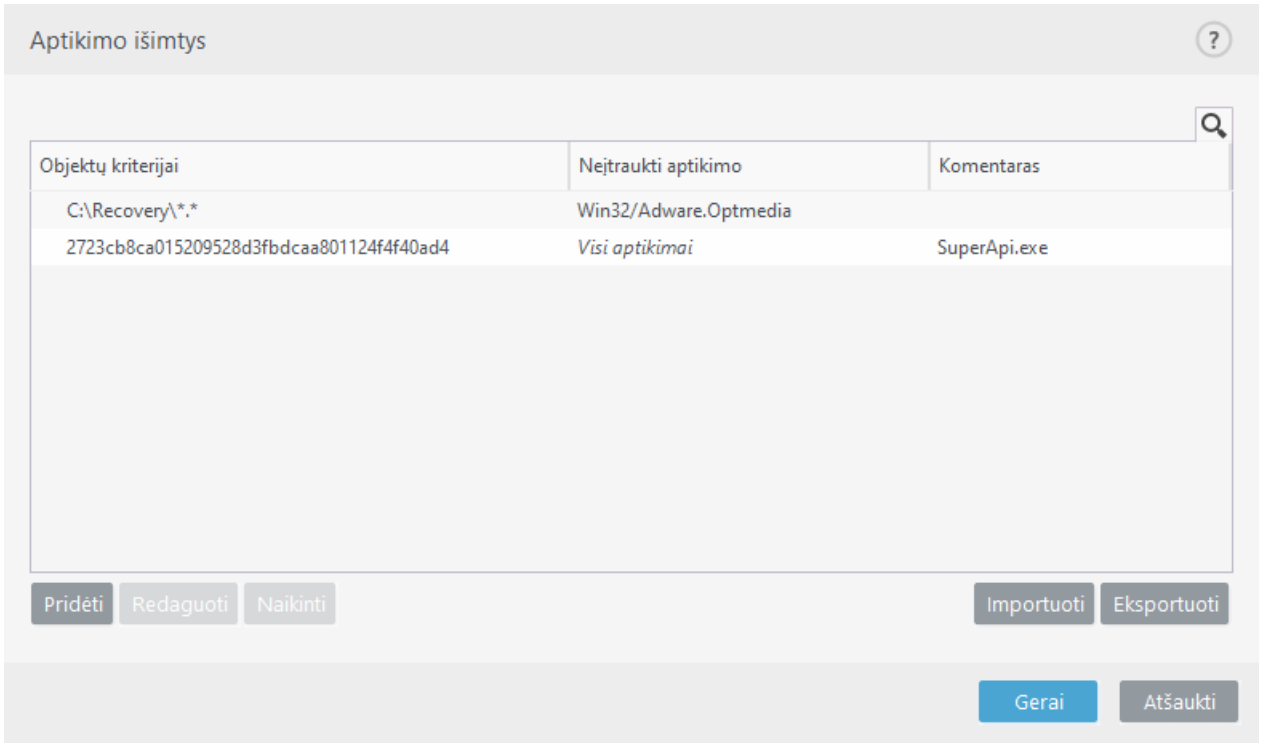
Toliau pateikti kintamieji gali būti naudojami kelio išskyrimo formate:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Nuo naudotojų priklausantys sistemos kintamieji (pavyzdžiui, *%TEMP%* arba *%USERPROFILE%*) arba aplinkos kintamieji (pavyzdžiui, *%PATH%*) nepalaikomi.

Aptikimo išimtys

Aptikimo išimtys leidžia neįtraukti objektų į valymą, filtruojant aptikimo pavadinimą, objekto kelią arba maišą.

Aptikimo išimtys nepašalina failams ir aplankams taikomo nuskaitymo, tai atlieka Našumo išimtys. Aptikimo išimtys taikomos objektams tik kai juos aptinka aptikimo modulis ir išimčių sąraše yra atitinkama taisyklė. Pavyzdžiui, (žr. toliau pateiktos iliustracijos pirmą eilutę), kai objektas aptinkamas kaip Win32/Adware.Optmedia ir aptiktas failas yra *C:\Recovery\file.exe*. Antroje eilutėje kiekvienam failui su tinkama SHA-1 maiša visada bus taikoma išimtis, nepaisant aptikimo pavadinimo.



Norint užtikrinti visų grėsmių aptikimą, rekomenduojame kurti aptikimo išimtis tik kai tai būtina.

Norėdami įtraukti failus ir aplankus į išimčių sąrašą, pasirinkite **Išplėstinis nustatymai** (F5) > **Aptikimo modulis** > **Išimtys** > **Aptikimo išimtys** > **Redaguoti**.

Kad objektas būtų neįtraukiamas (pagal aptikimo pavadinimą arba maišą) į valymą, spustelėkite **Pridėti**.

Potencialiai nepageidaujamoms programoms ir potencialiai nesaugioms programoms taip pat galima sukurti išskyrimą pagal aptikimo pavadinimą:

- Įspėjimo lange, kuriame pranešama apie aptikimą (spustelėkite **Rodyti išplėstines parinktis,** tada pasirinkite **Neįtraukti į aptikimą**).
- Žurnalo failų kontekstiniame meniu, naudojant Aptikimo išimčių kūrimo vedlį.
- Spustelėję **Įrankiai** > **Karantinas**, dešiniuoju mygtuku spustelėję karantinuotą failą ir kontekstiniame meniu pasirinkę **Atkurti ir neįtraukti į nuskaitymą**.

Aptikimo išimčių kriterijai objektams

- **Kelias** – riboti aptikimo išimtį nurodytam keliui (arba bet kokiam).
- **Aptikimo pavadinimas** – jei šalia neįtraukto failo yra aptikimo pavadinimas, tai reiškia, kad failas neįtraukiamas tik nurodytam aptikimui, o ne visiškai. Jei vėliau šis failas bus užkrėstas kitomis kenkėjiškomis programomis, jis bus aptiktas.
- **Maiša** – neįtraukia failo pagal konkrečią maišą SHA-1, nepaisant failo tipo, vietos, pavadinimo ar jo plėtinio.

Valdymo elementai

- **Pridėti** – pridėkite naują įrašą, kad išskirtumėte objektus, kurių nereikia valyti.
- **Redaguoti** – leidžia redaguoti pasirinktus įrašus.
- **Šalinti** – pašalinami pasirinkti įrašai (paspauskite CTRL ir spustelėkite norėdami pasirinkti kelis įrašus).
- **Importuot / eksportuoti** – aptiktų išskyrimų importavimas ir eksportavimas yra naudingas, jeigu reikia padaryti dabartinių išskyrimų atsarginę kopiją, kurią galėtumėte naudoti vėliau. Be to, nustatymų eksportavimo parinktis yra patogi naudotojams nevaldomosiose aplinkose, kurie nori pageidautiną konfigūraciją naudoti keliose sistemose – jie gali lengvai importuoti .txt failą ir perkelti šiuos nustatymus.
  Rodo importuojamo / eksportuojamo failo formato pavyzdį

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManageme
nt.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileH
ash"]}

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

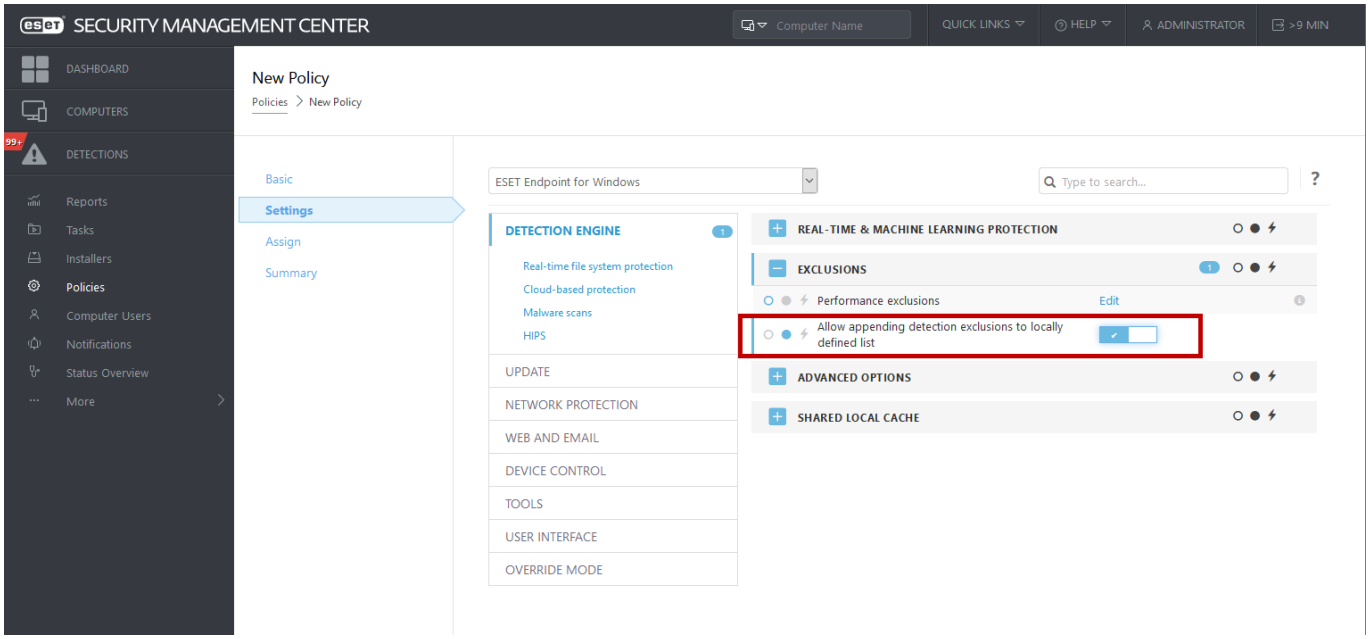
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Aptikimo išimčių nustatymas ESET PROTECT

Į ESET PROTECT 8.0 įeina naujas aptikimo išimčių valdymo vedlys – kurkite aptikimo išimtis ir taikykite jas daugiau kompiuterių / grupių.

Aptikimo išimčių galima nepaisyti ESET PROTECT

Kai yra vietinis aptikimo išimčių sąrašas, administratorius turi taikyti politiką su **Leisti pridėti aptikimo išskyrimus prie vietinio apibrėžto sąrašo**. Po to aptikimo išimčių papildymas ESET PROTECT veiks taip, kaip numatyta.

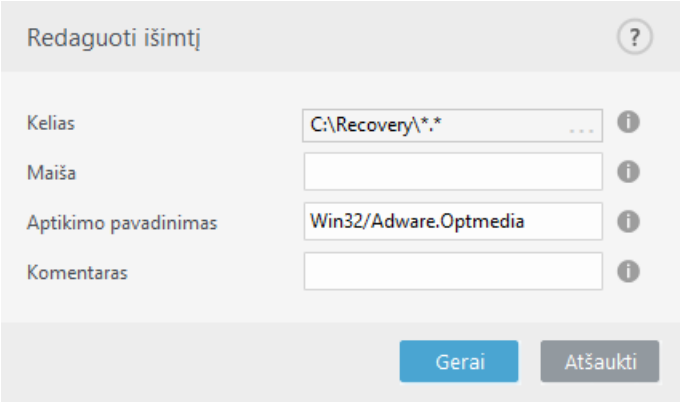


Pridėti arba redaguoti aptikimo išimtį

Neįtraukti aptikimo

Turi būti pateiktas teisingas ESET aptikimo pavadinimas. Norėdami sužinoti teisingą aptikimo pavadinimą, žr. sritį Žurnalo failai ir tada išskleidžiamame žurnalo failų meniu pasirinkite **Aptikimai**. Tai yra naudinga, kai ESET Endpoint Security aptinkamas klaidingai teigiamas pavyzdys. Tikrų grėsmių išskyrimai yra labai pavojingi, pagalvokite apie tai, kad turėtumėte neįtraukti tik paveiktų failų / katalogų, lauke **Kelio kaukė** spustelėdami **...**, ir (arba) tik laikinai. Išimtys apima ir galimas nepageidaujamas taikomąsias programas, galimas nesaugias taikomąsias programas ir įtartinas programas.

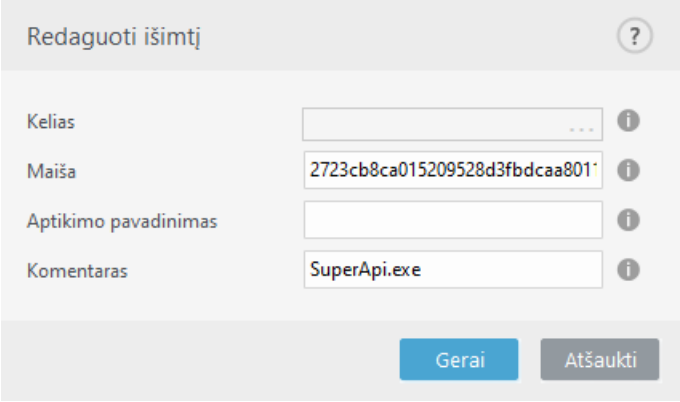
Taip pat skaitykite Kelio išskyrimo formatas.



Žr. Aptikimo išimčių pavyzdys toliau.

Išskirti maišą

Neįtraukia failo pagal konkrečią maišą SHA-1, nepaisant failo tipo, vietos, pavadinimo ar jo plėtinio.



Norėdami pašalinti konkretų aptikimą pagal jo pavadinimą, įveskite teisingą aptikimo pavadinimą: *Win32/Adware.Optmedia*
Taip pat galite naudoti toliau nurodytus formatus, kai pašalinate aptikimą iš ESET Endpoint Security perspėjimo lango:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Valdymo elementai

- **Pridėti** – neįtraukia objektų į aptikimą.
- **Redaguoti** – leidžia redaguoti pasirinktus įrašus.
- **Šalinti** – pašalinami pasirinkti įrašai (paspauskite CTRL ir spustelėkite norėdami pasirinkti kelis įrašus).

Aptikimo išimčių kūrimo vedlys vedlį

Aptikimo išimtį taip pat galima sukurti kontekstiniame meniu Žurnalo failai (netaikoma kenkėjiškos programinės įrangos aptikimui):

1. Pagrindiniame programos lange spustelėkite **Įrankiai** > **Žurnalo failai**.
2. Dešiniuoju pelės mygtuku spustelėkite aptikimą **Aptikimų žurnale**.
3. Spustelėkite **Kurti išimtį**.

Norėdami išskirti vieną arba daugiau aptikimų pagal **Išimčių kriterijus**, spustelėkite **Keisti kriterijus**:

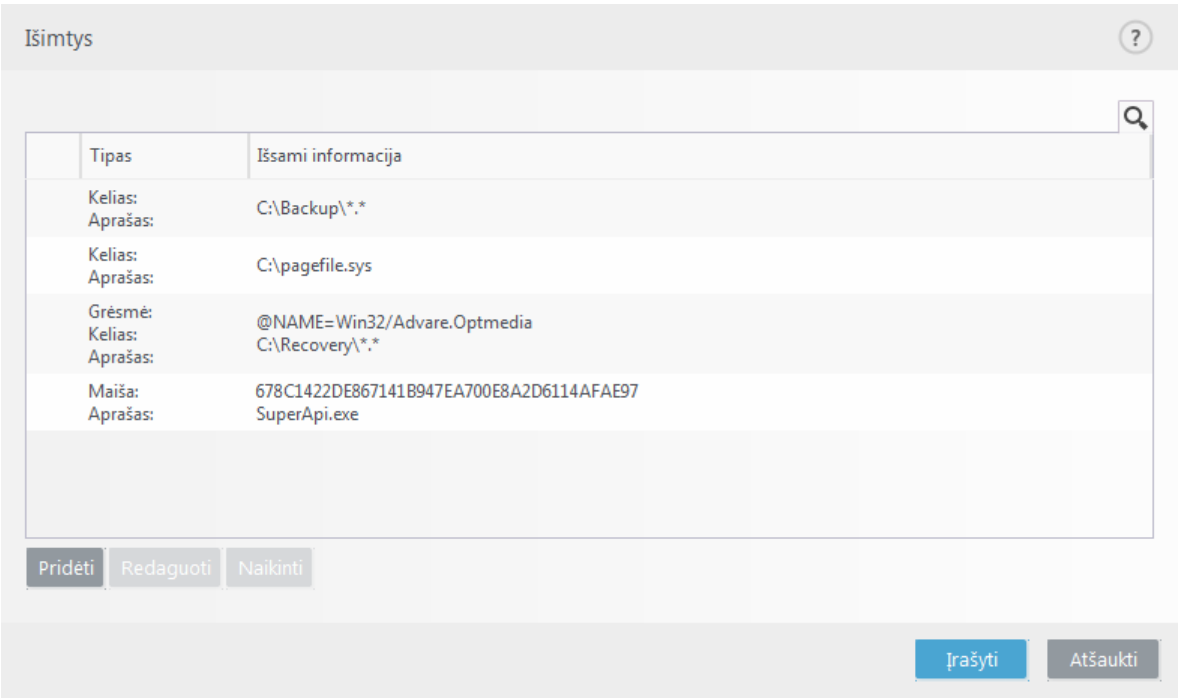
- **Tikslūs failai** – išskirti kiekvieną failą pagal jo SHA-1 maišą.
- **Aptikimas** – išskirti kiekvieną failą pagal jo aptikimo pavadinimą.
- **Kelias ir aptikimas** – išskirti kiekvieną failą pagal jo aptikimo pavadinimą ir kelią, įskaitant failo pavadinimą (pvz., *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Rekomenduojama parinktis yra iš anksto pasirinkta pagal aptikimo tipą.

Pasirinktinai galite pridėti **Komentarą**, prieš spustelėdami **Kurti išimtį**.

Išimtys (7.1 ir senesnis)

Išimtys 7.1 ir senesnėse versijose sujungia Našumo išimtis ir Aptikimo išimtis.



Procesų išimtys

Procesų išimčių funkcija suteikia galimybę neįtraukti programos procesų į failų sistemos apsaugą realiuoju laiku. Kad būtų sparčiau kuriamos atsarginės kopijos, pagerintas procesų patikimumas ir paslaugų pasiekiamumas, atsarginių kopijų kūrimo metu naudojamos kai kurios technikos, kurios sukelia konfliktus su failų lygmens apsauga nuo kenkėjiškų programų. Su panašiomis problemomis galima susidurti bandant realiuoju laiku perkelti virtualiuosius kompiuterius. Vienintelis veiksmingas būdas išvengti šių situacijų yra išjungti apsaugos nuo kenkėjiškų programų programinę įrangą. Sukuriant konkrečių procesų išimtis (pavyzdžiui, išsprendžiančias atsarginės kopijos kūrimo problemas), nepaisoma visų su neįtrauktais procesais susijusių failų operacijų ir jos laikomos saugiomis, taip sumažinant trukdžius atsarginės kopijos kūrimo procesui. Rekomenduojame išimtis kurti atsargiai – į išimčių sąrašą įtrauktas atsarginių kopijų kūrimo įrankis gali pasiekti užkrėstus failus ir sukelti pavojaus

signalą. Būtent todėl išplėstiniai leidimai leidžiami tik apsaugos realiuoju laiku moduliui.

Procesų išimtys padeda sumažinti galimų konfliktų riziką ir padidina išimtinių programų našumą, o tai padidina bendrą operacinės sistemos našumą ir stabilumą. Proceso / programos išimtis yra jos vykdomojo failo (*.exe*) įtraukimas į išskyrimų sąrašą.

Galite įtraukti vykdomuosius failus į išimtinių procesų sąrašą dalyje **Išplėstiniai nustatymai** (F5) > **Aptikimo modulis** > **Failų sistemos apsauga realiuoju laiku** > **Procesų išimtys**.

Ši funkcija buvo sukurta atsarginių kopijų kūrimo įrankių išimtims kurti. Neįtraukiant atsarginių kopijų kūrimo įrankio proceso į nuskaitymą ne tik užtikrinamas sistemos stabilumas, bet it nekenkiama atsarginių kopijų kūrimo našumui, nes vykdomas atsarginių kopijų kūrimas nestabdomas.

Spustelėkite **Redaguoti**, kad atidarytumėte valdymo langą **Procesų išimtys**, kuriame galite Pridėti išimtis ir ieškoti vykdomųjų failų (pvz., *Backup-tool.exe*), kurie nebus įtraukti į nuskaitymą.
Kai tik *.exe* failas įtraukiamas į išimtis, šio proceso veiklos nebestebi ESET Endpoint Security ir nebenuskaitomos jokios šio proceso vykdomos failų operacijos.

Jei pasirinkdami vykdomąjį proceso failą nesinaudojate naršymo funkcija, turite patys įvesti visą vykdomojo failo kelią. Antraip išimtis bus sukurta netinkamai ir HIPS gali pranešti apie klaidas.

Taip pat galite **Redaguoti** esamus procesus arba **Naikinti** juos išimčių sąraše.

Į šias išimtis neatsižvelgia saityno prieigos apsauga, todėl į išimčių sąrašą įtraukus saityno naršyklės vykdomąjį failą, atsisiųsti failai vistiek nuskaitomi. Taip apsaugoma nuo įsibrovimo. Tai tik pavyzdinis scenarijus ir mes nerekomenduojame kurti saityno naršyklių išimčių.

Pridėti arba redaguoti procesų išskyrimus

Šiame dialogo lange leidžiama **pridėti** procesus, neįtraukus į aptikimo modulį. Procesų išimtys padeda sumažinti galimų konfliktų riziką ir padidina išimtinių programų našumą, o tai padidina bendrą operacinės sistemos našumą ir stabilumą. Proceso / programos išimtis yra jos vykdomojo failo (*.exe*) įtraukimas į išskyrimų sąrašą.

Pasirinkite išskirtos programos failo kelią spustelėdami ... (pvz., *C:\Program Files\Firefox\Firefox.exe*). NEĮVESKITE programos pavadinimo.
Kai tik *.exe* failas įtraukiamas į išimtis, šio proceso veiklos nebestebi ESET Endpoint Security ir nebenuskaitomos jokios šio proceso vykdomos failų operacijos.

Jei pasirinkdami vykdomąjį proceso failą nesinaudojate naršymo funkcija, turite patys įvesti visą vykdomojo failo kelią. Antraip išimtis bus sukurta netinkamai ir HIPS gali pranešti apie klaidas.

Taip pat galite **Redaguoti** esamus procesus arba **Naikinti** juos išimčių sąraše.

HIPS išimtys

Išskyrimai leidžia neįtraukti procesų iš HIPS išsamaus elgsenos patikrinimo.

Norėdami neįtraukti objekto, spustelėkite **Pridėti** ir įveskite kelią į objektą arba pasirinkite jį medžio struktūroje. Taip pat galite **redaguoti** arba **šalinti** pasirinktus įrašus.

Skaitykite skyrių Išskyrimai.

„ThreatSense“ parametrai

„ThreatSense“ sudaro įvairūs sudėtiniai grėsmių aptikimo metodai. Ši technologija yra iniciatyvi, o tai reiškia, kad ji užtikrina apsaugą, vos tik pradeda plisti nauja grėsmė. Joje kartu naudojama kodų analizė, kodų imitavimas, bendrieji kodai ir virusų kodai, kurie darniai veikia ir gerokai padidina sistemos saugumą. Nuskaitymo modulis gali vienu metu kontroliuoti keletą duomenų srautų – tai padidina efektyvumą ir aptikimo greitį. Be to, „ThreatSense“ technologija sėkmingai panaikina kenkėjiškas prieigos programas.

„ThreatSense“ modulio nustatymų parinktys leidžia nurodyti keletą nuskaitymo parametrų:

- failų, kurie turi būti nuskaityti, tipai ir plėtiniai;
- įvairių aptikimo metodų derinys;
- valymo lygiai ir t. t.

Norėdami patekti į nustatymo langą, išplėstinio nustatymo lange spustelėkite **„ThreatSense“ parametrai** , kad būtų parodyti moduliai, kuriems naudojama ThreatSense technologija (žr. toliau). Skirtingiems saugumo scenarijams gali reikėti skirtingų konfigūracijų. Atsižvelgiant į tai, „ThreatSense“ yra atskirai konfigūruojama šiems apsaugos moduliams:

- Failų sistemos apsauga realiuoju laiku
- Laukimo būsenos nuskaitymas
- Nuskaitymas paleidžiant
- Dokumentų apsauga
- El. pašto programų apsauga
- Prieigos prie saityno apsauga
- Kompiuterio nuskaitymas

„ThreatSense“ parametrai yra optimizuoti kiekvienam moduliui ir jų keitimas gali labai paveikti sistemos veikimą. Pavyzdžiui, pakeitus parametrus, kad visada būtų nuskaitomos momentinio pakavimo programos, arba įjungus išplėstinę euristiką failų sistemos apsaugos realiuoju laiku modulyje, sistemos darbas gali sulėtėti (paprastai naudojant šiuos metodus nuskaitomi tik naujai sukurti failai). Rekomenduojame palikti numatytuosius „ThreatSense“ parametrus nepakeistus visuose moduliuose, išskyrus kompiuterio nuskaitymą.

Nuskaitytini objektai

Šiame skyriuje galite nurodyti, kurie kompiuterio komponentai ir failai bus nuskaityti ieškant įsiskverbimų.

Operacinė atmintis – nuskaitomos grėsmės, kurios atakuoja sistemos operacinę atmintį.

Paleidimo sektorius / UEFI – nuskaitomi sistemos įkrovimo sektoriai tikrinant, ar nėra kenkėjiškos programinės įrangos pagrindiniame sistemos įkrovimo įraše. Daugiau apie UEFI skaitykite terminų žodyne.

El. laiškų failai – programa palaiko šiuos plėtinius: DBX („Outlook Express“) ir EML.

Archyvai – programa palaiko šiuos plėtinius: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE ir daugelį kitų.

Išsiskleidžiantieji archyvai – išsiskleidžiantieji archyvai (SFX) yra archyvai, kurie gali išsiskleisti patys.

Momentiniai pakuotuvai – įvykdytos momentinio išpakavimo programos (skirtingai nei standartinių tipų archyvai) vėl suglaudinamos atmintyje. Be standartinių statinių pakavimo programų (UPX, yoda, ASPack, FSG ir

t. t.), naudodamas kodų imitavimo principą skaitytuvas gali atpažinti kelis papildomus pakuotuvų tipus.

Nuskaitymo parinktys

Pasirinkite metodus, kurie bus naudojami nuskaitant sistemą ir ieškant įsiskverbimų. Galimos šios parinktys:

Euristika – euristika yra algoritmas, analizuojantis programų (kenkimo programinės įrangos) veiklą. Pagrindinis šios technologijos privalumas yra gebėjimas identifikuoti kenkimo programinę įrangą, kurios nebuvo ankstesnėje aptikimo modulio versijoje arba ji nebuvo žinoma. Trūkumas yra klaidingų pavojaus pranešimų (labai maža) tikimybė.

Išplėstinė euristika / DNA kodai – išplėstinė euristika yra unikalus ESET sukurtas algoritmas, optimizuotas aptikti kompiuterio kirminus bei Trojos arklius ir yra parašytas aukšto lygio programavimo kalbomis. Naudojant išplėstinę euristiką, gerokai padidėja ESET produktų grėsmių aptikimo galimybės. Kodai gali patikimai aptikti ir identifikuoti virusus. Naudojant automatinę naujinimo sistemą, nauji kodai tampa pasiekiami per kelias valandas nuo grėsmės atskleidimo. Kodų trūkumas yra tai, kad jie aptinka tik jiems žinomus virusus (arba šiek tiek modifikuotas jų versijas).

Valymas

Valymo nustatymai apibrėžia ESET Endpoint Security veiksmus valant objektus.

Išimtys

Plėtinys yra tašku atskirta failo pavadinimo dalis. Plėtinys apibrėžia failo tipą ir turinį. Šis „ThreatSense“ parametrų nustatymo skyrius leidžia apibrėžti failų tipus, kuriuos reikia nuskaityti.

Kita

Konfigūruojant „ThreatSense“ modulio kompiuterio užsakomojo nuskaitymo parametrų nustatymus, papildomai pasiekiamos ir šios parinktys, pateikiamos skyriuje **Kita**:

Nuskaityti kintamuosius duomenų srautus (ADS) – NTFS failų sistemos naudojami kintamieji duomenų srautai yra failų ir aplankų ryšiai, kurie nematomi įprastoms nuskaitymo priemonėms. Daugelis įsiskverbimų bando išvengti aptikimo apsimesdami kintamaisiais duomenų srautais.

Vykdyti mažo prioriteto foninius nuskaitymus – kiekviena nuskaitymo seka naudoja tam tikrą kiekį sistemos išteklių. Jeigu dirbate su programomis, kurios intensyviai naudoja sistemos išteklius, galite suaktyvinti mažo prioriteto foninį nuskaitymą ir taupyti išteklius savo programoms.

Registruoti visus objektus – nuskaitymo žurnale bus rodomi visi nuskaityti failai išsiskleidžiančiuosiuose archyvuose, net neužkrėsti (gali būti generuojama daug nuskaitymo žurnalo duomenų ir padidės nuskaitymo žurnalo failo dydis).

Įjungti išmanųjį optimizavimą – įjungus išmanųjį optimizavimą, naudojami optimaliausi parametrai, leidžiantys užtikrinti efektyviausią nuskaitymo lygį ir kartu palaikyti didžiausią nuskaitymo greitį. Įvairūs apsaugos moduliai išmaniai atlieka nuskaitymą, naudodami įvairius nuskaitymo metodus ir taikydami juos konkretiems failų tipams. Jei išmanusis optimizavimas išjungtas, atliekant nuskaitymą taikomi tik vartotojo apibrėžti parametrai tam tikrų modulių ThreatSense šerdyje.

Saugoti paskutinį prieigos laiką – nurodykite šią parinktį, norėdami išlaikyti nuskaitytų failų originalius prieigos laikus, o ne naujinti juos (pavyzdžiui, naudojant su duomenų atsarginio kopijavimo sistemomis).

Ribos

Ribų skyriuje galima nurodyti maksimalius nuskaitomų objektų dydžius ir archyvų įdėties lygius:

Objekto parametrai

Maksimalus objekto dydis – apibrėžia maksimalų nuskaitomų objektų dydį. Antivirusinės programos modulis nuskaitys tik mažesnius nei nurodytas dydis objektus. Šią parinktį turėtų keisti tik patyrę vartotojai, kurie gali turėti tam tikrų priežasčių neįtraukti didelių objektų į nuskaitymą. Numatytoji reikšmė: neribota.

Maksimali objekto nuskaitymo trukmė (sek.) – apibrėžia maksimalią objekto failų (pvz., esančių RAR / ZIP archyve arba el. laiške su keliais priedais) nuskaitymo trukmę. Šis nustatymas netaikomas pavieniams failams. Jei įvesta naudotojo apibrėžta vertė ir tas laikas praėjo, nuskaitymas bus sustabdytas kuo greičiau, neatsižvelgiant į tai, ar kiekvieno failo nuskaitymas objekte yra užbaigtas. Archyvo su dideliais failais atveju nuskaitymas bus sustabdytas išskleidus failą iš archyvo (pvz., kai naudotojo apibrėžtas kintamasis yra 3 sekundės, bet failo išskleidimas užtrunka 5 sekundes). Praėjus nurodytam laikui, likę archyvo failai nebus nuskaitomi. Norėdami apriboti nuskaitymo trukmę, taip pat ir didesnių archyvų atveju, naudokite parinktis **Maksimalus objekto dydis** ir **Maksimalus failo archyve dydis** (nerekomenduojama dėl galimos rizikos saugai). Numatytoji reikšmė: neribota.

Archyvo nuskaitymo nustatymai

Archyvo įdėties lygis – nurodo maksimalų archyvų nuskaitymo gylį. Numatytoji vertė: 10.

Maksimalus failo archyve dydis – ši parinktis leidžia nurodyti, kokio maksimalaus dydžio (kai jie išskleidžiami) archyve esantys failai bus nuskaitomi. Maksimali reikšmė: 3 GB.

Mes nerekomenduojame keisti numatytųjų verčių: dirbant įprastai, jų keisti nėra priežasties.

Valymo lygiai

Norėdami pasiekti pageidaujamo apsaugos modulio išvalymo lygio nustatymus, išplėskite **„ThreatSense“ parametrus** (pavyzdžiui, **Failų sistemos apsaugos realiuoju laiku**) ir spustelėkite **Valymas**.

Apsauga realiuoju laiku ir kiti apsaugos moduliai turi tolesnius atkūrimo (t. y. išvalymo) lygius.

Atkūrimas programoje ESET Endpoint Security 9

Valymo lygis	Aprašymas
Visada valyti objektą	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais retais atvejais (pvz., esant sisteminiams failams), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje. **Visada valyti objektą** yra rekomenduojama numatytoji nuostata valdomoje aplinkoje..
Jei saugu, valyti objektą, priešingu atveju palikti	Valant objektus, bandoma atkurti aptikimą be jokių galutinio naudotojo atliekamų veiksmų. Kai kuriais atvejais (pvz., esant sisteminiams failams arba archyvams, kuriuose yra ir švarūs, ir užkrėsti failai), jei aptikimo negalima atkurti, nurodytas objektas paliekamas pradinėje vietoje.

Valymo lygis	Aprašymas
Jei saugu, valyti objektą, priešingu atveju paklausti	Valant objektus, bandoma atkurti aptikimą. Kai kuriais atvejais, jei negalima atlikti jokių veiksmų, galutiniam naudotojui rodomas interaktyvus įspėjimas ir jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Daugeliu atveju ši nuostata yra rekomenduojama.
Visada klausti galutinio naudotojo	Valant objektus, galutiniam naudotojui rodomas interaktyvus langas, kuriame jis turi pasirinkti atkūrimo veiksmą (pvz., šalinti arba nepaisyti). Šis lygis skirtas labiau patyrusiems naudotojams, kurie žino, kokį veiksmą atlikti aptikimo atveju.



Failų plėtiniai, kurie nebus nuskaitomi

Plėtinys yra tašku atskirta failo pavadinimo dalis. Plėtinys apibrėžia failo tipą ir turinį. Šis „ThreatSense“ parametrų nustatymo skyrius leidžia apibrėžti failų tipus, kuriuos reikia nuskaityti.

Nesupainiokite jų su kitų tipų Išimtimis.

Pagal numatytąją parinktį nuskaitomi visi failai. Bet kurį plėtinį galima įtraukti į failų, kurie nebus nuskaitomi, sąrašą.

Neįtraukti failų kartais būtina, jeigu nuskaitant tam tikro tipo failus blogai veikia programa, kuri naudoja failus su tam tikro tipo plėtiniais. Pavyzdžiui, gali tekti neįtraukti `.edb`, `.eml` ir `.tmp` plėtinių, kai naudojami „Microsoft Exchange“ serveriai.

Norėdami įtraukti plėtinį į sąrašą, spustelėkite **Pridėti**. Įveskite plėtinį į tuščią laukelį (pvz., `tmp`) ir spustelėkite **Gerai**. Kai pasirinksite **Įvesti kelias vertes**, galėsite įtraukti kelis failų plėtinius, atskirtus eilutėmis, kableliais arba kabliataškiais (pvz., išskleidžiamajame meniu kaip skirtuką pasirinkite **Kabliataškis** ir įveskite `edb;eml;tmp`).
Galite naudoti specialų simbolį „?“ (klaustuką). Klaustukas reiškia bet kurį simbolį (pvz., `?db`).

Kad „Windows“ operacinėje sistemoje būtų matomas tikslus failo plėtinys (jei yra), turite nuimti parinkties **Slėpti žinomų tipų failų plėtinius** žymėjimą pasirinkę **Valdymo skydas** > **Aplanko parinktys** > **Rodymas** (skirtuke) ir taikyti šį pakeitimą.

Papildomi „ThreatSense“ parametrai

Papildomi ThreatSense naujai sukurtų ir pakeistų failų parametrai – naujai sukurtų arba pakeistų failų užkrėtimo tikimybė yra santykinai didesnė nei jau esančių failų. Todėl programa tikrina šiuos failus su papildomais nuskaitymo parametrais. Be įprastų kodu paremtų nuskaitymo metodų, papildomai naudojama išplėstinė euristika, kuri gali aptikti naujas grėsmes dar neišleidus aptikimo modulio naujinimo. Be naujai sukurtų failų, nuskaitomi išsiskleidžiantieji failai (.sfx) ir momentinio išpakavimo programos (viduje suglaudinti vykdomieji failai). Pagal numatytuosius nustatymus archyvai yra nuskaitomi iki 10-to įdėjimo lygio ir yra tikrinami neatsižvelgiant į jų realų dydį. Norėdami pakeisti archyvo nuskaitymo parametrus, išaktyvinkite punktą **Numatytieji archyvo nuskaitymo parametrai**.

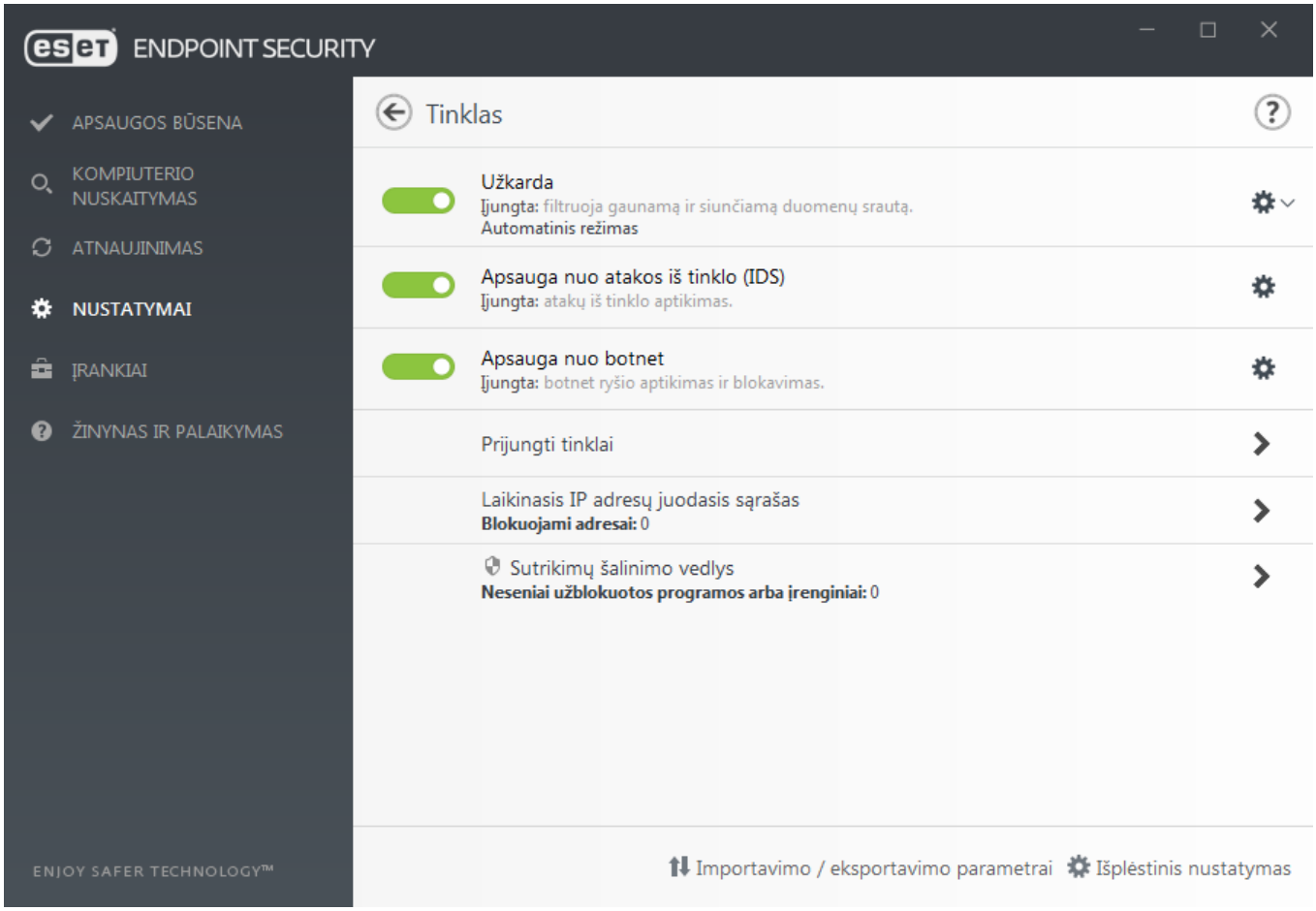
Jei norite daugiau sužinoti apie Momentinio pakavimo programas, Išsiskleidžiančius archyvus ir Išplėstinę euristiką, žr. ThreatSense modulio parametrų nustatymas.

Papildomi ThreatSense vykdomųjų failų parametrai – pagal numatytuosius nustatymus išplėstinė euristika naudojama ir tada, kai failai vykdomi. Įjungus funkciją, primygtinai rekomenduojame palikti punktus Išmanusis optimizavimas ir ESET LiveGrid® įjungtus, kad būtų minimaliai paveiktas sistemos našumas.

Tinklas

Dalyje **Tinklas** galima greitai pasiekti šiuos komponentus arba parametrus **išplėstiniame nustatyme**:

- **Užkarda** – čia galite nustatyti ESET užkardos filtravimo režimą. Išsamesnius parametrus galite pasiekti spustelėdami krumpliaračio piktogramą ⚙ > **Konfigūruoti** (šalia parinkties **Užkarda**) arba paspauskite **F5**, kad būtų atidarytas **išplėstinis nustatymas**.
- **Apsauga nuo atakos iš tinklo (IDS)** – analizuoja tinklo duomenų srauto turinį ir saugo nuo atakų iš tinklo. Blokuojamas visas duomenų srautas, kuri laikomas žalingu. ESET Endpoint Security informuos jus, kai prisijungsite prie neapsaugoto belaidžio tinklo arba silpnai apsaugoto tinklo.
- **Apsauga nuo įtraukimo į užgrobtų kompiuterių tinklą** – sistemoje greitai ir tiksliai aptinka kenkimo programinę įrangą. Apsaugą nuo įtraukimo į užgrobtų kompiuterių tinklą galite išjungti pasirinktam laikotarpiui spustelėdami  (nerekomenduojama).
- „**Connected networks**“ (prijungti tinklai) – rodo tinklus, prie kurių prijungti tinklo adapteriai. Spustelėkite krumpliaračio piktogramą ⚙, kad pasirinktumėte tinklo, prie kurio esate prisijungę, apsaugos tipą. Norėdami peržiūrėti kiekvieną tinklo adapterį ir jam priskirtą užkardos profilį bei patikimą zoną, spustelėkite **Prijungti tinklai** > **Tinklo adapteriai**. Išsamesnės informacijos skaitykite čia: Tinklo adapteriai.
- **Laikinas IP adresų juodasis sąrašas** – peržiūrėkite sąrašą IP adresų, kurie buvo aptikti kaip atakų šaltiniai ir pridėti prie juodojo sąrašo, kad kuriam laikui būtų uždrausti ryšiai. Jei reikia daugiau informacijos, spustelėkite šią parinktį ir paspauskite F1.
- **Trikčių šalinimo vediklis** – padeda išspręsti jungiamumo problemas, kurias sukelia ESET užkarda. Išsamesnės informacijos skaitykite čia: Trikčių šalinimo vediklis.



Spustelėkite krumpliaračio piktogramą , esančią šalia **Užkardos**, kad pasiektumėte tokius parametrus:

- **Konfigūruoti** – atveria išplėstinių nustatymų užkardos langą, kuriame galima apibrėžti, kaip užkarda tvarkys tinklo ryšį.
- **Blokuoti visą srautą** – užkarda užblokuos visus gaunamus ir siunčiamus ryšius. Naudokite šią parinktį tik tada, jei įtariate kritinį saugumo pavojų, dėl kurio sistemą būtina atjungti nuo tinklo. Jei norite atkurti įprastinį užkardos darbą, kai tinklo srauto filtravimas vykdomas režimu **Blokuoti visą srautą**, spustelėkite **Stabdyti viso srauto blokavimą**.
- **Pristabdyti užkardą (leisti visus duomenų srautus)** – yra priešinga parinktis viso tinklo duomenų srauto blokavimo parinkčiai. Pasirinkus visos užkardos filtravimo parinktys bus išjungtos ir visi gaunami ir siunčiami ryšiai bus leidžiami. Spustelėkite **Įjungti užkardą**, kad vėl įjungtumėte užkardą, kol veikia šis tinklo srauto filtravimo režimas.
- **Automatinis režimas** – (kai įjungtas kitas filtravimo režimas) – spustelėkite norėdami pakeisti filtravimo režimą į automatinį (su vartotojo apibrėžtomis taisyklėmis).
- **Interaktyvusis režimas** – (kai įjungtas kitas filtravimo režimas) – spustelėkite norėdami pakeisti filtravimo režimą į interaktyvųjį.

Užkarda

Užkarda valdo visą tinklo srautą į sistemą ir iš jos. Tai atliekama leidžiant arba draudžiant atskirus tinklo ryšius, remiantis nurodytomis filtravimo taisyklėmis. Ji užtikrina apsaugą nuo atakų iš nuotolinių kompiuterių ir gali užblokuoti galimai pavojingas tarnybas.

Pagrindinis

Įjungti užkarda

rekomenduojame šią funkciją palikti įjungtą, kad būtų užtikrintas sistemos saugumas. Įjungus šią užkardą tinklo srautas nuskaitomas abiem kryptimis.

Įvertinti ir „Windows“ užkardos taisykles

Veikiant automatiniam režimui bus leidžiamas ir gaunamas srautas, kuris yra leidžiamas pagal „Windows“ užkardos taisykles, nebent jis tiesiogiai blokuojamas pagal ESET taisykles.

„Windows“ užkardos taisyklės, sukonfigūruotos naudojant grupės strategiją (GPO), nevertinamos.

Filtravimo režimas

Užkardos veikimas pasikeičia pagal filtravimo režimą. Be to, filtravimo režimai lemia, kiek reikia vartotojo veiksmų.

Galite pasirinkti toliau pateikiamus ESET Endpoint Security užkardos filtravimo režimus:

Filtravimo režimas	Aprašymas
Automatinis režimas	Numatytasis režimas. Šis režimas tinka vartotojams, kurie nori lengvai ir patogiai naudotis užkarda nenustatinėdami taisyklių. **Automatiniu režimu** galima kurti pasirinktines, vartotojo apibrėžtas taisykles, tačiau jos neprivalomos. Automatinis režimas leidžia išsiųsti visą konkrečios sistemos srautą ir blokuoja didžiąją dalį atsiunčiamo srauto (išskyrus srautą iš patikimos zonos, kuris apibrėžiamas IDS ir išplėstinėse parinktyse / leidžiamose paslaugose bei reaguoja į pastaruoju metu išsiųstą srautą).
Interaktyvusis režimas	leidžia sukurti pasirinktinę konfigūraciją savo užkardai. Kai aptinkamas ryšys ir nėra šiam ryšiui taikomos taisyklės, parodomas dialogo langas, kuriame pranešama apie nežinomą ryšį. Dialogo langas suteikia galimybę leisti arba uždrausti ryšį, ir šis sprendimas leisti arba drausti gali būti įrašytas kaip nauja užkardos taisyklė. Jeigu pasirinksite sukurti naują taisyklę, visi vėlesni šio tipo ryšiai pagal tokią taisyklę bus leidžiami arba blokuojami.
Politika pagrįstas režimas	blokuoja visus ryšius, kurie nėra apibrėžti konkrečios juos leidžiančios taisyklės. Šis režimas leidžia patyrusiems vartotojams apibrėžti taisykles, kurios leidžia tik norimus ir saugius ryšius. Visus kitus nenurodytus ryšius užkarda blokuos.
Mokymosi režimas	Automatiškai sukuriamos ir išsaugomos taisyklės; šis režimas itin naudingas pirminės užkardos konfigūracijos etape, tačiau jo nereikėtų palikti įjungto ilgam. Nereikalingi jokie vartotojo veiksmai, nes ESET Endpoint Security įrašo taisykles pagal iš anksto nustatytus parametrus. Mokymosi režimas turėtų būti naudojamas tik iki tol, kol sukuriamos visos reikiamų ryšių taisyklės, kad būtų išvengta saugumo pavojų.

Profilius galima naudoti siekiant pritinkinti ESET Endpoint Security užkardos elgseną, atskiroms situacijoms nurodant skirtingus taisyklių rinkinius.

Papildoma

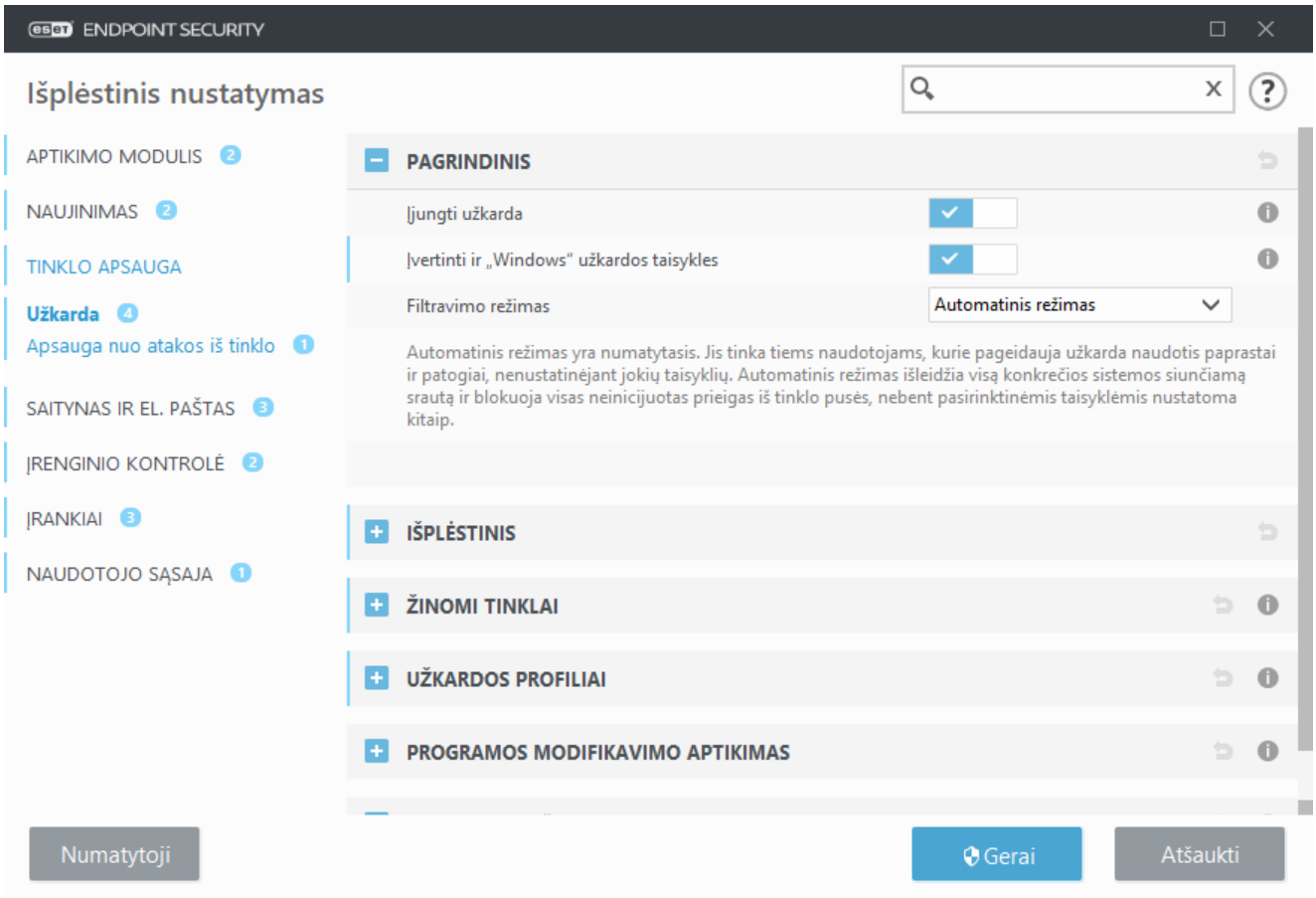
Taisyklės

Taisyklių nustatymas leidžia peržiūrėti visas taisykles, taikomas srautui, kurį patikimoje zonoje ir internete

generuoja atskiros programos.

Zonos

Zona nurodo tinklo adresų, kurie sudaro vieną loginę grupę, rinkinį.



Užgrobtų kompiuterių tinklui („Botnet“) surengus ataką prieš jūsų kompiuterį, galite sukurti IDS taisyklę. Išimtis gali būti pakeista dalyje **Išplėstiniai nustatymai** (F5) > **Tinklo apsauga** > **Apsauga nuo atakos iš tinklo** > **IDS taisyklės** spustelėję **Redaguoti**.

Mokymosi režimas

Mokymosi režimas automatiškai sukuria ir įrašo po taisyklę kiekvienam ryšiui, kuris buvo užmegztas sistemoje. Nereikalingi jokie vartotojo veiksmai, nes ESET Endpoint Security įrašo taisykles pagal iš anksto nustatytus parametrus.

Šis režimas gali kelti jūsų sistemai pavojų, todėl rekomenduojamas tik pradiniam užkardos konfigūravimui.

Pasirinkite **Mokymosi režimas** iš išskleidžiamojo meniu **Išplėstiniai nustatymai** (F5) > **Užkarda** > **Bendra** > **Filtravimo režimas,** kad aktyvintumėte **Mokymosi režimo parinktis**. Šiame skyriuje yra tokie elementai:

mokymosi režimu užkarda nefiltruoja ryšio. Leidžiami visi siunčiami ir gaunami ryšiai. Šiuo režimu jūsų kompiuteris nėra visiškai apsaugotas užkardos.

Režimas, nustatytas pasibaigus mokymosi režimui – nustatykite, kurį filtravimo režimą ESET Endpoint Security asmeninė užkarda vėl įjungs pasibaigus mokymosi režimo laikui. Skaitykite daugiau apie filtravimo režimus. Pasibaigus, parinktis Teirautis naudotojo prašo administratoriaus teisių, kad galėtų atlikti užkardos filtravimo

režimo pakeitimą.

Ryšio tipas – kiekvienam ryšio tipui parinkite specifinius taisyklių kūrimo parametrus. Yra keturi ryšio tipai:

- **Gaunamas srautas iš patikimos zonos** – gaunamo ryšio pavyzdys patikimoje zonoje būtų nuotolinis kompiuteris iš patikimos zonos, bandantis užmegzti ryšį su vietine taikomąja programa, vykdoma jūsų kompiuteryje.

- **Siunčiamas srautas į patikimą zoną** – vietinė taikomoji programa, bandanti užmegzti ryšį su kitu kompiuteriu, esančiu vietiniame tinkle arba tinkle patikimoje zonoje.

- **Gaunamas interneto duomenų srautas** – nuotolinis kompiuteris, bandantis susisiekti su kompiuteryje veikiančia taikomąja programa.

- **Siunčiamas interneto duomenų srautas** – vietinė taikomoji programa bando užmegzti ryšį su kitu kompiuteriu.

Kiekviename skyriuje galima apibrėžti parametrus, kurie bus pridedami prie naujai kuriamų taisyklių:

Pridėti vietinį prievadą – įtraukia tinklo ryšio vietinio prievado numerį. Siunčiamiems ryšiams paprastai generuojami atsitiktiniai numeriai. Dėl šios priežasties rekomenduojame įjungti šią parinktį tik gaunamiems ryšiams.

Pridėti taikomąją programą – įtraukia vietinės taikomosios programos pavadinimą. Ši parinktis tinka programos lygio taisyklėms ateityje (taisyklėms, kurios apibrėžia visos programos ryšį). Pavyzdžiui, galite leisti ryšį tik žiniatinklio naršyklei arba el. pašto programai.

Pridėti nuotolinį prievadą – įtraukia tinklo ryšio nuotolinio prievado numerį. Pavyzdžiui, galite leisti arba uždrausti konkrečias paslaugas, susijusias su standartiniu prievado numeriu (HTTP – 80, POP3 – 110 ir t. t.).

Pridėti nuotolinį IP adresą / patikimą zoną – nuotolinis IP adresas arba zona gali būti naudojami kaip parametrai naujoms taisyklėms, nustatančioms visus tinklo ryšius tarp vietinės sistemos ir to nuotolinio adreso / zonos. Ši parinktis tinka, jeigu norite nustatyti konkretaus kompiuterio arba tinklo kompiuterių grupės veiksmus.

Maksimalus skirtingų taisyklių taikomajai programai skaičius – jeigu taikomoji programa palaiko ryšius per skirtingus prievadus, su įvairiais IP adresais ir t. t., užkarda mokymosi režimu sukuria atitinkamą skaičių taisyklių šiai programai. Ši parinktis leidžia riboti taisyklių, kurios gali būti sukurtos vienai taikomajai programai, skaičių.

Tinklo apsauga nuo atakų

Įjungti apsaugą nuo atakos iš tinklo (IDS) – Analizuoja tinklo srauto turinį ir saugo nuo atakų iš tinklo. Blokuojamas bet koks žalingu laikomas turinys.

Įjungti apsaugą nuo įtraukimo į užgrobtų kompiuterių tinklą – aptinka ir užblokuoja ryšį su kenkti skirtais komandų ir valdymo centrais, vadovaujantis simptomais, pasireiškiančiais kompiuterį užkrėtus ir botui mėginant užmegzti ryšį. Daugiau apie apsaugą nuo įtraukimo į užgrobtų kompiuterių tinklą skaitykite terminų žodyne.

IDS taisyklės – Ši parinktis jums leis sukonfigūruoti išplėstines filtravimo parinktis, kad aptiktumėte įvairių tipų atakas ir spragų išnaudojimus, kurie gali būti panaudoti pakenkti jūsų kompiuteriui.

Apsauga nuo grubios jėgos atakų

Apsauga nuo grubios jėgos atakų blokuoja RDP ir SMB tarnybų slaptažodžių spėliojimo atakas. Apsauga nuo grubios jėgos atakų yra būdas atrasti tikslinį slaptažodį, sistemingai bandant visus raidžių, skaičių ir simbolių derinius. Norėdami konfigūruoti apsaugą nuo grubios jėgos atakų, pagrindiniame programos lange spustelėkite **Sąranka** > **Išplėstinis nustatymas** (F5) > **Tinklo apsauga** > **Tinklo apsauga nuo atakų** > **Apsauga nuo grubios jėgos atakų**.

Įjungti apsaugą nuo grubios jėgos atakų – ESET Endpoint Security tikrina tinklo srauto turinį ir blokuoja slaptažodžių spėliojimo atakų bandymus.

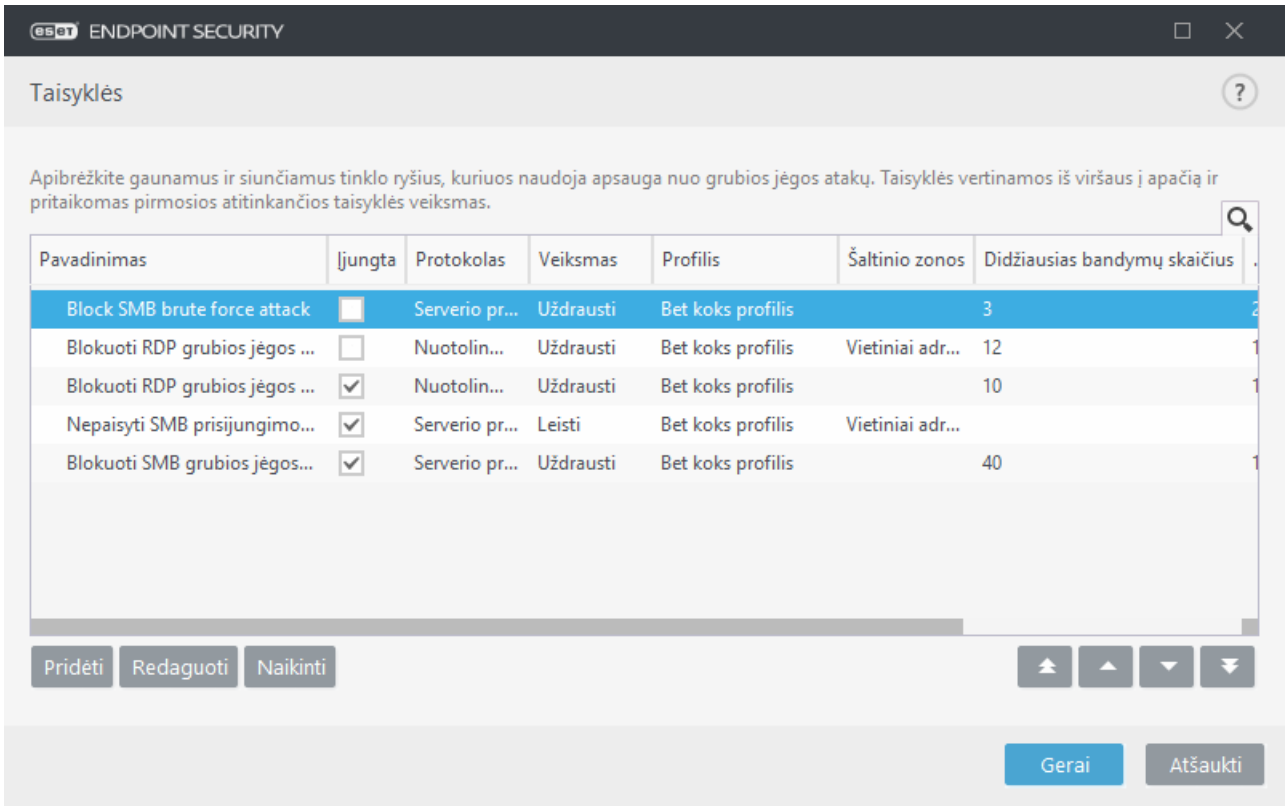
Taisyklės – leidžia kurti, redaguoti ir peržiūrėti gaunamų ir siunčiamų tinklo ryšių taisykles. Daugiau informacijos rasite skyriuje Taisyklės.

Išimtys – neįtrauktų aptikimų, apibrėžtų IP adresu arba programos keliu, sąrašas. Išimtis galite kurti ir redaguoti savo ESET PROTECT konsolėje. Daugiau informacijos rasite skyriuje Išimtys.

Taisyklės

Apsaugos nuo grubios jėgos atakų taisyklės leidžia kurti, redaguoti ir peržiūrėti gaunamų ir siunčiamų tinklo ryšių taisykles. Iš anksto apibrėžtų taisyklių negalima redaguoti arba naikinti.

Apsaugos nuo grubios jėgos atakų taisyklių valdymas

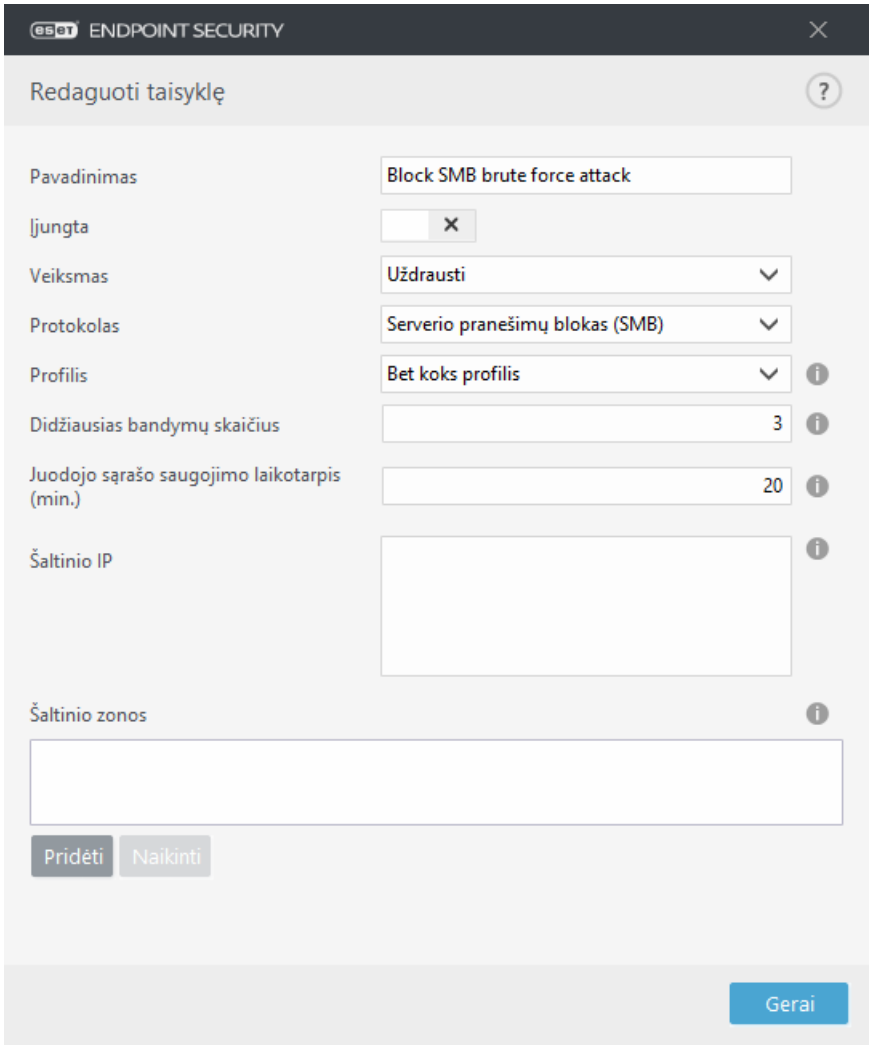


- **Pridėti** – spustelėkite, jei norite kurti naują apsaugos nuo grubios jėgos atakų taisyklę.
- **Redaguoti** – spustelėkite, jei norite redaguoti esamą apsaugos nuo grubios jėgos atakų taisyklę.
- **Naikinti** – pasirinkite ir spustelėkite, jei norite pašalinti išimtį iš IDS taisyklių sąrašo.

- **Į viršų / aukštyn / žemyn / į apačią** – suteikia galimybę nustatyti taisyklių pirmumo lygį.

> Siekiant užtikrinti didžiausią įmanomą apsaugą, taikoma blokavimo taisyklė su mažiausia **didžiausio bandymų skaičiaus** reikšme, net jei taisyklė yra žemiau taisyklių sąraše, kai kelios blokavimo taisyklės atitinka aptikimo sąlygas.

Taisyklių rengyklė



Pavadinimas – taisyklės pavadinimas.

Įjungta – išjunkite slankiklį, jei taisyklę norite išlaikyti sąraše, bet nenorite jos taikyti.

Veiksmas – pasirinkite, ar **Drausti** arba **Leisti** ryšį, jei taisyklės parametrai įvykdyti.

Protokolas – ryšio protokolas, kurį tikrins ši taisyklė.

Profilis – tam tikriems profiliams galima nustatyti ir taikyti pasirinktines taisykles.

Didžiausias bandymų skaičius – Didžiausias leidžiamų bandymų pakartotinai atakuoti skaičius, kol IP adresas bus užblokuotas ir įtrauktas į juodąjį sąrašą.

Juodojo sąrašo saugojimo laikotarpis (min.) – nustato adreso buvimo juodajame sąraše pabaigos datą.

Šaltinio IP – IP adresų / diapazonų / potinklių sąrašas. Kelis adresus reikia atskirti kableliais.

Šaltinio zonos – leidžia pridėti iš anksto nustatytą arba sukurtą zoną su IP adresų diapazonu spustelint **Pridėti**.

Išimtys

Grubios jėgos išimtys gali būti naudojamos norint nerodyti grubios jėgos aptikimo pagal konkrečius kriterijus. Šios išimtys kuriamos iš ESET PROTECT pagal grubios jėgos aptikimą.

Stulpeliai

- **Aptikimas** – aptikimo tipas.
- **Programa** – pasirinkite išskirtos programos failo kelią spustelėdami ... (pvz., *C:\Program Files\Firefox\Firefox.exe*). NEĮVESKITE programos pavadinimo.
- **Nuotolinis IP** – nuotolinių IPv4 arba IPv6 adresų / ribų / potinklių sąrašas. Kelis adresus reikia atskirti kableliais.

Išimčių valdymas

Išimtys bus rodomos, jei administratorius sukurs grubios jėgos išimtis ESET PROTECT tinkle valdomoje konsolėje. Išimtyse gali būti tik leidimo taisyklių ir jos turi būti įvertintos prieš IDS taisykles.

Išplėstinės filtravimo parinktys

Užkardos ir Apsaugos nuo atakų iš tinklo dalys suteikia galimybę konfigūruoti išplėstines filtravimo parinktis, kad aptiktumėte įvairių tipų atakas ir pažeidžiamumus, kuriuos galima išnaudoti prieš jūsų kompiuterį.

Kai kuriais atvejais negausite grėsmės pranešimo apie užblokuotus ryšius. Žr. skyrių Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo, kur rasite instrukcijų, kaip peržiūrėti visus užblokuotus ryšius užkardos žurnale.

Konkrečių parinkčių pasiekiamumas dalyje **Išplėstinis nustatymas** (F5) > **Tinklo apsauga** > **Užkarda** ir **Išplėstinis nustatymas** (F5) > **Tinklo apsauga** > **Tinklo apsauga nuo atakų** gali skirtis, atsižvelgiant į jūsų užkardos modulio tipą arba versiją bei jūsų operacinės sistemos versiją.

Leidžiamos paslaugos

Šios grupės parametrai skirti supaprastinti prieigos prie kompiuterio tarnybų iš patikimos zonos konfigūravimą. Daugelis jų įjungia / išjungia iš anksto apibrėžtas užkardos taisykles.

- **Leisti bendrai naudoti failus ir spausdintuvus patikimoje zonoje** – leidžia patikimoje zonoje esantiems nuotoliniams kompiuteriams pasinaudoti jūsų bendrinamais failais ir spausdintuvais.
- **Leisti UPNP sistemos paslaugoms patikimoje zonoje** – leidžia gaunamas ir siunčiamas UPnP protokolų užklausas sistemos paslaugoms. UPnP (universalus savaiminis diegimas, taip pat žinomas kaip „Microsoft“ tinklo radimas) yra naudojamas „Windows Vista“ ir naujesnėse operacinėse sistemose.
- **Leisti gaunamus RPC ryšius patikimoje zonoje** – leidžia TCP ryšius iš patikimos zonos, suteikiant prieigą prie „MS RPC Portmapper“ ir RPC / DCOM tarnybų.
- **Leisti nuotolinį darbalaukį patikimoje zonoje** – įjungia ryšius „Microsoft“ nuotolinio darbalaukio protokolu

(RDP) ir leidžia patikimoje zonoje esantiems kompiuteriams pasiekti jūsų kompiuterį RDP naudojančia programa (pvz., nuotolinio prisijungimo prie darbalaukio programa). Taip pat žr. kaip leisti RDP ryšį už patikimo zonos ribų.

- **Įjungti registravimą į daugiaadresio perdavimo grupes per IGMP** – leidžia priimti / siųsti IGMP ir priimamus UDP daugiaadresius srautus, pvz., vaizdo įrašų srautus, generuojamus IGMP protokolą (interneto grupinių adresų valdymo protokolas – angl. „Internet Group Management Protocol“) naudojančių programų.
- **Leisti susietų jungčių ryšį** – pasirinkite šią parinktį, kad nenutrūktų susietos jungtys. Naudojant susietą tinklą, virtualus įrenginys prijungiamas prie tinklo naudojant pagrindinio kompiuterio eterneto adapterį. Jei naudojate susietą tinklą, virtualus įrenginys gali pasiekti kitus tinklo įrenginius ir atvirkščiai, tarsi tai būtų fizinis kompiuteris tinkle.

- **Leisti automatinį saityno paslaugų radimą (WSD) sistemos paslaugoms patikimoje zonoje** – leidžia per užkardą iš patikimų zonų priimti saityno paslaugų radimo užklausas. WSD protokolas yra naudojamas rasti paslaugas vietiniame tinkle.
- **Leisti daugiaadresio perdavimo adresų nustatymą patikimoje zonoje (LLMNR)** – LLMNR (vietinio saito daugiaadresio pavadinimo vertimas) yra DNS paketų protokolas, kuris leidžia tiek IPv4, tiek IPv6 pagrindiniams kompiuteriams atlikti pagrindinių kompiuterių vardų vertimą tame pačiame vietiniame saite, nereikalaujant DNS serverio arba DNS kliento konfigūravimo. Ši parinktis leidžia per užkardą iš patikimos zonos priimti daugiaadreses DNS užklausas.
- **„Windows HomeGroup“ palaikymas** – įjungia „HomeGroup“ palaikymą „Windows 7“ ir naujesnėse operacinėse sistemose. „HomeGroup“ gali bendrinti failus ir spausdintuvus namų tinkle. Norėdami konfigūruoti namų grupę, eikite į **Pradėti** > **Valdymo skydas** > **Tinklas ir internetas** > **Namų grupė**.

Įsilaužimo aptikimas

- **Protokolo SMB** – aptinka ir užblokuota įvairias SMB protokolo saugumo problemas, pvz.:

- **Apgaulingo serverio iškvietimo atakos atpažinimo aptikimas** – saugo nuo atakos, atpažinimo metu naudojančios apgaulingą iškvietimą siekiant gauti vartotojo kredencialus.

- **IDS vengimo atidarant įvardytąjį kanalą aptikimas** – aptinka žinomus vengimo metodus, naudojamus atidarant MSRPC įvardytuosius kanalus.

- **CVE aptikimas** (bendras pažeidžiamumas ir atskleidimas) – įdiegti įvairių atakų, formų, saugos skylių ir išnaudojimų SMB protokole aptikimo metodai. Jei reikia išsamesnės informacijos apie CVE identifikatorius (CVEs), žr. CVE interneto svetainę cve.mitre.org.

- **Protokolo RPC** – aptinka ir užblokuoja įvairius CVE nuotolinių procedūrų iškvietimo sistemoje, sukurtoje paskirstytųjų skaičiavimų aplinkai (DCE).
- **RDP protokolas** – aptinka ir užblokuoja įvairius RDP protokole (žr. pirmiau).
- **ARP nuodijimo atakos aptikimas** – aptinka ARP nuodijimo atakas, sukeltas tarpininko atakų, arba tinklo komutatoriaus šnipinėjimą. ARP (adresų nustatymo protokolas) yra naudojamas tinklo programų ir įrenginių eterneto adresui nustatyti.
- **TCP/UDP prievadų nuskaitymo atakos aptikimas** – aptinka atakas, atliekamas prievadų nuskaitymo programine įranga – programomis, sukurtomis tikrinti atviriems pagrindinio kompiuterio prievadams siunčiant klientų užklausas įvairiais prievadų adresais, siekiant aptikti aktyvius prievadus ir išnaudoti tarnybos saugumo spragas. Išsamiau apie šio tipo atakas skaitykite terminų žodyne.
- **Blokuoti nesaugius adresus aptikus ataką** – IP adresai, kurie buvo aptikti kaip atakų šaltiniai, pridedami prie juodojo sąrašo ir kuriam laikui uždraudžiamas ryšys.
- **Rodyti pranešimą aptikus ataką** – įjungia sistemos dėklo pranešimą apatiniame dešiniajame lango kampe.

- **Rodyti pranešimus ir apie atakas panaudojant saugumo spragas** – perspėja jus apie aptiktas atakas

panaudojant saugumo spragas arba grėsmių bandymus tokiu būdu patekti į sistemą.

Paketo tikrinimas

- **Leisti įeinantį ryšį su administratoriaus bendrinimais SMB protokolu** – administratoriaus bendrinimai yra numatytieji tinklo bendrinimai, bendrinantys standžiojo disko skaidinius (*C$*, *D$*, ...) sistemoje kartu su sisteminiu aplanku (*ADMIN$*). Išjungus įeinantį ryšį prie administratoriaus bendrinimų turi sumažėti daugelis saugos pavojų. Pavyzdžiui, kirminas „Conficker“ vykdo žodyno atakas, siekdamas prisijungti prie administratoriaus bendrinimų.

- **Uždrausti senus (nepalaikomus) SMB dialektus** – draudžia SMB seansus, naudojančius seną SMB dialektą, kurio nepalaiko IDS. Šiuolaikinės „Windows“ operacinės sistemos palaiko senus SMB dialektus, kad būtų suderinamos su senomis operacinėmis sistemomis, pvz., „Windows 95“. Užpuolikas gali panaudoti seną dialektą SMB seansui, kad išvengtų duomenų srauto tikrinimo. Uždrauskite senus SMB dialektus, jei kompiuteriui nereikia bendrinti failų (ar naudoti SMB ryšį apskritai) su seną „Windows“ versiją turinčiu kompiuteriu.
- **Uždrausti SMB seansus be išplėstinės apsaugos** – SMB seanso pradžios metu galima naudoti išplėstinę apsaugą, siekiant užtikrinti saugesnį atpažinimo mechanizmą nei atpažinimas LAN tvarkytuvo iškvietimu / atsakymu (LM). LM schema laikoma silpna ir jos naudoti nerekomenduojama.
- **Uždrausti atidaryti SMB protokolu vykdomuosius failus iš serverio, kuris nėra patikimoje zonoje** – nutraukia ryšį, kai bandote atidaryti vykdomąjį failą (.exe, .dll, ...) iš bendrinamo aplanko serveryje, kuris nepriklauso patikimai zonai asmeninėje užkardoje. Atminkite: vykdomųjų failų kopijavimas iš patikimų šaltinių gali būti teisėtas, tačiau šis aptikimo būdas turėtų sumažinti pavojų nepageidaujamai atidaryti kenkimo serveryje esantį failą (pvz., atidaryti failą spustelint bendrinamo kenkimo vykdomojo failo saitą).
- **Uždrausti NTLM atpažinimą SMB protokole prisijungiant prie serverio, esančio arba nesančio patikimoje zonoje** – NTLM (abiejų versijų) atpažinimo schemas naudojantys protokolai yra pažeidžiami kredencialų persiuntimo atakomis (SMB protokolo atveju jos vadinamos „SMB relay“ atakomis). Uždraudžiant NTLM atpažinimą serveriams ne iš patikimos zonos turi sumažinti kredencialų persiuntimo atakos grėsmę iš kenkėjiškų serverių už patikimos zonos. Analogiškai NTLM atpažinimą galima uždrausti ir serveriams patikimoje zonoje.

- **Leisti ryšį su saugumo paskyrų tvarkytuvo tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-SAMR].

- **Leisti ryšį su vietinių saugumo institucijų tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-LSAD] ir [MS-LSAT].

- **Leisti ryšį su nuotolinio registravimo tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-RRP].

- **Leisti ryšį su tarnybų valdymo tvarkytuvo tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-SCMR].

- **Leisti ryšį su serverio tarnyba** – papildomos informacijos apie šią tarnybą rasite [MS-SRVS].
- **Leisti ryšį su kitomis tarnybomis** – kitos MSRPC tarnybos. MSRPC yra „Microsoft“ būdas įdiegti DCE RPC mechanizmą. Be to, MSRPC dėl transportavimo gali naudoti įvardytuosius kanalus, perkeltus į SMB (tinklo failų bendrinimo) protokolą (ncacn_np transport). MSRPC paslaugos suteikia sąsajas nuotoliniu būdu pasiekti ir valdyti „Windows“ sistemoms. Buvo aptiktos kelios „Windows“ MSRPC sistemos saugumo spragos, kurias išnaudojo plintantys virusai (kirminai „Conficker“, „Sasser“…). Išjunkite nebūtiną ryšį su MSRPC tarnybomis daugeliui saugumo pavojų (tokių kaip nuotolinis kodo vykdymas ar tarnybų gedimo atakos) sumažinti.

IDS taisyklės

Tam tikrais atvejais Įsilaužimo aptikimo tarnyba (IDS) gali nustatyti maršrutų parinktuvų ir kitų tarptautinių tinklų įrenginių ryšį kaip galimą ataką. Pavyzdžiui, kad būtų apeita IDS, galite pridėti žinomą saugų adresą prie adresų, neįtrauktų į IDS sritį.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Kurkite kliento darbo vietų IDS taisykles programoje ESET Endpoint Security
- Kurkite IDS taisykles kliento darbo vietoms programoje ESET PROTECT

Stulpeliai

- **Aptikimas** – aptikimo tipas.
- **Programa** – pasirinkite išskirtos programos failo kelią spustelėdami ... (pvz., *C:\Program Files\Firefox\Firefox.exe*). NEĮVESKITE programos pavadinimo.
- **Nuotolinis IP** – nuotolinių IPv4 arba IPv6 adresų / ribų / potinklių sąrašas. Kelis adresus reikia atskirti kableliais.
- **Blokuoti** – kiekvienas sistemos procesas turi savo numatytąją elgseną ir priskirtą veiksmą (blokuoti arba leisti). Norint apeiti ESET Endpoint Security numatytąją elgseną, pasirinkite ją blokuoti arba leisti, pasinaudojant išskleidžiamuoju meniu.
- **Pranešti** – Pasirinkite Taip, kad rodytumėte Darbalaukio pranešimus savo kompiuteryje. Pasirinkite Ne, jei nepageidaujate kompiuterio pranešimų. Galimos parinktys yra Numatytoji/Taip/Ne.
- **Žurnalas** – Pasirinkite **Taip**, kad fiksuotumėte įvykius ESET Endpoint Security žurnalo failuose. Pasirinkite **Ne**, jei nepageidaujate fiksuoti įvykių. Galimos parinktys yra **Numatytoji**/**Taip**/**Ne**.

Skirtukas „Išimtys“ bus rodomas, jei administratorius sukurs IDS išimtis ESET PROTECT tinkle valdomoje konsolėje. IDS išimtyse gali būti tik leidimo taisyklių ir jos turi būti įvertintos prieš IDS taisykles.

IDS taisyklių valdymas

- **Pridėti** – spustelėkite, kad sukurtumėte naują IDS taisyklę.
- **Redaguoti** – spustelėkite, norėdami redaguoti esamą IDS taisyklę.
- **Naikinti** – pasirinkite ir spustelėkite, jei norite pašalinti išimtį iš IDS taisyklių sąrašo.
-  **Į viršų / aukštyn / žemyn / į apačią** – leidžia nustatyti taisyklių pirmumo lygį (išimtys vertinamos iš viršaus žemyn).

Norite rodyti pranešimą ir fiksuoti visus įvykius:
1. Spustelėkite **Įtraukti**, kad įtrauktumėte naują IDS taisyklę.
2. Pasirinkite konkretų įspėjimą išskleidžiamajame meniu **Aptikimas**.
3. Spustelėkite **...** ir pasirinkite programos, kuriai norite taikyti pranešimą, failo kelią.
4. Palikite parinktį **Numatytoji** išskleidžiamajame meniu **Blokuoti**. Taip bus naudojamas numatytasis veiksmas, kurį taiko ESET Endpoint Security.
5. Išskleidžiamuosiuose meniu **Pranešti** ir **Žurnalas** pasirinkite **Taip**.
6. Įrašykite pranešimą spustelėdami **Gerai**.

Norite pašalinti pasikartojančius pranešimus apie aptikimų tipą, kurio nelaikote grėsme:
1. Spustelėkite **Įtraukti**, kad įtrauktumėte naują IDS išimtį.
2. Pasirinkite konkretų įspėjimą išskleidžiamajame meniu **Aptikimas**, pvz., **SMB seansas be saugumo plėtinių TCP prievadų nuskaitymo ataka**.
3. Išskleidžiamajame krypčių meniu pasirinkite **Įvestis**, jei įspėjimas skelbiamas dėl įeinančiojo ryšio.
4. Išskleidžiamajame meniu **Pranešti** pasirinkite **Ne**.
5. Išskleidžiamajame meniu **Žurnalas** pasirinkite **Taip**.
6. Palikite **Programa** tuščią.
7. Jei ryšys ateina ne iš konkretaus IP adreso, palikite **Nuotoliniai IP adresai** tuščią.
8. Įrašykite pranešimą spustelėdami **Gerai**.

Užblokuota įtartina grėsmė

Taip gali nutikti, pavyzdžiui, jei kompiuteryje įdiegta programa bando perduoti kenkimo duomenis į kitą tinklo kompiuterį, panaudojamos saugumo spragos arba kas nors bando nuskaityti jūsų tinklo prievadus.

Grėsmė – grėsmės pavadinimas.

Šaltinis – šaltinio tinklo adresas.

Tikslas – tikslinis tinklo adresas.

Stabdyti blokavimą – galimai grėsmei sukuriama IDS taisyklė su parametrais, kuriuos pritaikius ryšys leidžiamas.

Blokuoti toliau – aptikta grėsmė užblokuojama. Jei norite sukurti IDS taisyklę su parametrais, kuriuos pritaikius šios grėsmės ryšys būtų blokuojamas, pasirinkite **Daugiau nebepranešti**.

Pranešimo lange pateikiama informacija priklauso nuo aptiktos grėsmės tipo.
Daugiau informacijos apie grėsmes ir kitas susijusias sąvokas rasite skyriuose Nuotolinių atakų tipai arba Aptikimų tipai.

Tinklo apsaugos trikčių šalinimas

Trikčių diagnostikos vedlys padeda išspręsti ryšio problemas, kurias sukelia ESET užkarda. Išskleidžiamajame meniu pasirinkite laikotarpį, kurį ryšys buvo blokuojamas. Pastaruoju metu užblokuotų ryšių sąraše nurodomas programos ar įrenginio tipas, reputacija bei bendras programų ir įrenginių, kurie buvo užblokuoti per šį laikotarpį, skaičius. Jei reikia išsamesnės informacijos apie užblokuotus ryšius, spustelėkite **Išsami informacija**. Tada reikės atblokuoti programą ar įrenginį, dėl kurio kyla ryšio problemų.

Kai spustelėsite **Atblokuoti**, anksčiau užblokuoti ryšiai taps leidžiami. Jei problemų su programa kils ir toliau arba įrenginys neveiks kaip turėtų, spustelėkite **Programa vis tiek neveikia** ir visi anksčiau šiam įrenginiui užblokuoti ryšiai taps leidžiami. Jei problema išlieka, paleiskite kompiuterį iš naujo.

Spustelėkite **Rodyti pakeitimus**, kad peržiūrėtumėte vedlio sukurtas taisykles. Be to, vedlio sukurtas taisykles galite peržiūrėti ir eidami **Išplėstiniai nustatymai** > **Tinklo apsauga** > **Užkarda** > **Bendra** > **Taisyklės**.

Spustelėkite **Atblokuoti kitą, kad išspręstumėte kito įrenginio ar programos ryšio problemas**.

Prijungti tinklai

Prijungto tinklo dalis yra pasiekiama pagrindiniame programos ESET Endpoint Security lange spustelėjus **Nustatymai** > **Tinklas** > **Prijungti tinklai**.

Pateikiami tinklai, prie kurių prisijungę tinklo adapteriai. Spustelėję po tinklo pavadinimu esančią nuorodą būsite paraginti pasirinkti tinklo, prie kurio esate prisijungę per tinklo adapterį, apsaugos tipą (griežtą ar leidžiamą). Spustelėkite krumpliaratį (⚙), jei norite pakeisti šį pasirinkimą **„Išplėstiniame nustatyme“**. Šiuo nustatymu apibrėžiama, kaip jūsų kompiuteris bus pasiekiamas kitiems tinklo kompiuteriams.

Galite prisijungti prie trijų rūšių tinklo vietų:

- **Nepatikimas tinklas** – šios rūšies tinklo vieta skirta viešosioms vietoms ir nėra patikima. Jūsų įrenginys nebus matomas tinkle ir negalėsite matyti jokių kitų įrenginių tinkle. Tinklo aptikimas pagal numatytuosius nustatymus išjungtas viešuosiuose tinkluose.
- **Patikimas tinklas** – priešingai nei viešojo tinklo atveju, išteklius galite bendrinti su kitais LAN kompiuteriais privačiame tinkle. Pasirinkite **Namų arba biuro tinklas**, jei žinote įrenginius tinkle ir jais pasitikite.
- **Domenų tinklas** – jūsų tinklo administratorius valdo šios rūšies tinklo vietą ir negalite pasirinkti arba keisti šios rūšies tinklo. Domeno tinklo rūšies vieta aptinkama, kai vietinis kompiuteris priklauso Active Directory Domain Services. Vietinis kompiuteris gali autentifikuoti to domeno valdymą per vieną iš jo tinklo ryšių.

Tinklo vietos pasirinkimas gali padėti užtikrinti, kad kompiuterio saugos lygis visada būtų tinkamas.

Apatiniame dešiniajame lango kampe spustelėję **Tinklo adapteriai** galite peržiūrėti kiekvieną tinklo adapterį ir jam priskirtą užkardos profilį bei patikimą zoną. Išsamesnės informacijos skaitykite čia: Tinklo adapteriai.

> Kai pasirenkate **Naudoti „Windows“ nustatymą**, langas nerodomas, o tinklas, prie kurio prisijungiate, automatiškai pažymimas pagal „Windows“ nustatymus. Tokiu būdu iš naujų tinklų tampa pasiekiamos kai kurios funkcijos (pvz., failų bendrinimo ir nuotolinio darbalaukio).

Žinomi tinklai

Jei naudojate kompiuterį, kuriuo dažnai jungiatės prie viešųjų tinklų arba už jūsų įprasto darbo tinklo ribų esančių tinklų, rekomenduojame tikrinti naujų tinklų patikimumą. Apibrėžus tinklą, ESET Endpoint Security gali atpažinti patikimus (namų / biuro) tinklus, naudodamas įvairius tinklo parametrus, sukonfigūruotus skyriuje **Tinklo identifikacija**. Kompiuteriai dažnai jungiasi prie tinklų, kurių IP adresai panašūs į patikimo tinklo adresus. Tokiais atvejais ESET Endpoint Security gali priskirti nežinomą tinklą prie patikimų (namų / biuro). Siekiant išvengti tokios situacijos, rekomenduojama naudoti **Tinklo autentiškumo patvirtinimo** funkciją.

Kai tinklo adapteris prisijungia prie tinklo arba perkonfigūruojami jo tinklo parametrai, ESET Endpoint Security žinomų tinklų sąraše ieško įrašo, kuris atitiktų naująjį tinklą. Jei **Tinklo identifikacija** ir **Tinklo autentiškumo patvirtinimas** (pasirenkama) sutampa, tinklas šioje sąsajoje pažymimas kaip prijungtas. Kai neaptinkamas joks žinomas tinklas, tinklo identifikavimo konfigūracija sukuria naują tinklo ryšį, kuriuo bus identifikuojamas tinklas kitą kartą prie jo jungiantis. Pagal numatytuosius parametrus naujam tinklo ryšiui naudojamas apsaugos tipas **Viešasis tinklas**. Dialogo lange **Aptiktas naujas tinklo ryšys** jūsų bus paprašyta pasirinkti apsaugos tipą **Nepatikimas tinklas**, **Patikimas tinklas** arba **Naudoti „Windows“ parametrą**. Jei tinklo adapteris prijungiamas prie žinomo tinklo, o tas tinklas yra pažymėtas kaip **Patikimas tinklas**, vietiniai adapterio potinkliai pridedami prie patikimos zonos.

Naujų tinklų apsaugos tipas – pasirinkite vieną iš šių parinkčių: Naudoti „Windows“ nuostatą, Klausti vartotojo arba Žymėti kaip viešą pagal numatytuosius nustatymus, naudojamus naujiems tinklams.

> Kai pasirenkate **Naudoti „Windows“ parametrą,** dialogo langas nebus parodytas, o tinklas, prie kurio prisijungiate, bus automatiškai pažymėtas pagal „Windows“ parametrus. Tokiu būdu iš naujų tinklų tampa pasiekiamos kai kurios funkcijos (pvz., failų bendrinimo ir nuotolinio darbalaukio).

Žinomus tinklus galima sukonfigūruoti rankiniu būdu, lange Žinomų tinklų rengyklė.

Žinomų tinklų rengyklė

Žinomus tinklus galima konfigūruoti rankiniu būdu, pasirenkant **Išplėstiniai nustatymai** > **Tinklo apsauga** > **Pagrindinis** > **Žinomi tinklai** ir spustelėjus **Redaguoti** šalia **Žinomi tinklai**.

Stulpeliai

Pavadinimas – žinomo tinklo pavadinimas.

Apsaugos tipas – parodo, kaip nustatytas tinklas: **Patikimas tinklas**, **Nepatikimas tinklas** arba **Naudoti „Windows“ nustatymą**.

Užkardos profilis – pasirinkite profilį iš išskleidžiamojo meniu **Rodyti profilyje naudojamas taisykles**, kad būtų rodomas profilių taisyklių filtras.

Naujinimo profilis – suteikia galimybę pritaikyti sukurtą atnaujinimo profilį, kai prisijungiama prie šio tinklo.

Valdymo elementai

Pridėti – sukuria naują žinomą tinklą.

Redaguoti – spustelėkite, norėdami redaguoti esamą žinomą tinklą.

Naikinti – pasirinkite tinklą ir spustelėkite **Naikinti**, kad pašalintumėte jį iš žinomų tinklų sąrašo.

 **Į viršų / aukštyn / žemyn / į apačią** – leidžia nustatyti žinomų tinklų pirmumo lygį (tinklai vertinami iš viršaus žemyn).

Tinklo konfigūracijos parametrai yra suskaidyti į šias korteles:

Tinklas

Čia galite nustatyti **Tinklo pavadinimą** ir pasirinkti tinklo **Apsaugos tipą** („Nepatikimas tinklas“, „Patikimas tinklas“ arba „Naudoti „Windows“ parametrą“). Pasinaudokite išskleidžiamuoju meniu **Užkardos profilis** ir pasirinkite šiam tinklui tinkamą profilį. Jei tinkle naudojamas apsaugos tipas **Patikimas tinklas**, visi tiesiogiai prijungti tinklo potinkliai yra laikomi patikimais. Pavyzdžiui, jei prie šio tinklo prijungtas tinklo adapteris, kurio IP adresas yra 192.168.1.5, o potinklio kaukė yra 255.255.255.0, tuomet prie adapterio patikimosios zonos bus pridėtas potinklis 192.168.1.0/24. Jei adapteris turi daugiau adresų / potinklių, visi jie bus patikimi neatsižvelgiant į žinomo **Tinklo identifikacijos** konfigūraciją.

Be to, adresai, pridėti prie **Papildomų patikimų adresų** sąrašo, visada pridedami prie adapterių, prijungtų prie šio tinklo, patikimos zonos (neatsižvelgiant į tinklo apsaugos tipą).

Įspėti apie silpną „WiFi“ šifravimą – ESET Endpoint Security praneš jums, kai prisijungsite prie neapsaugoto belaidžio tinklo arba tinklo su silpna apsauga.

Užkardos profilis – pasirinkite užkardos profilį, kuris bus naudojamas prisijungus prie šio tinklo.

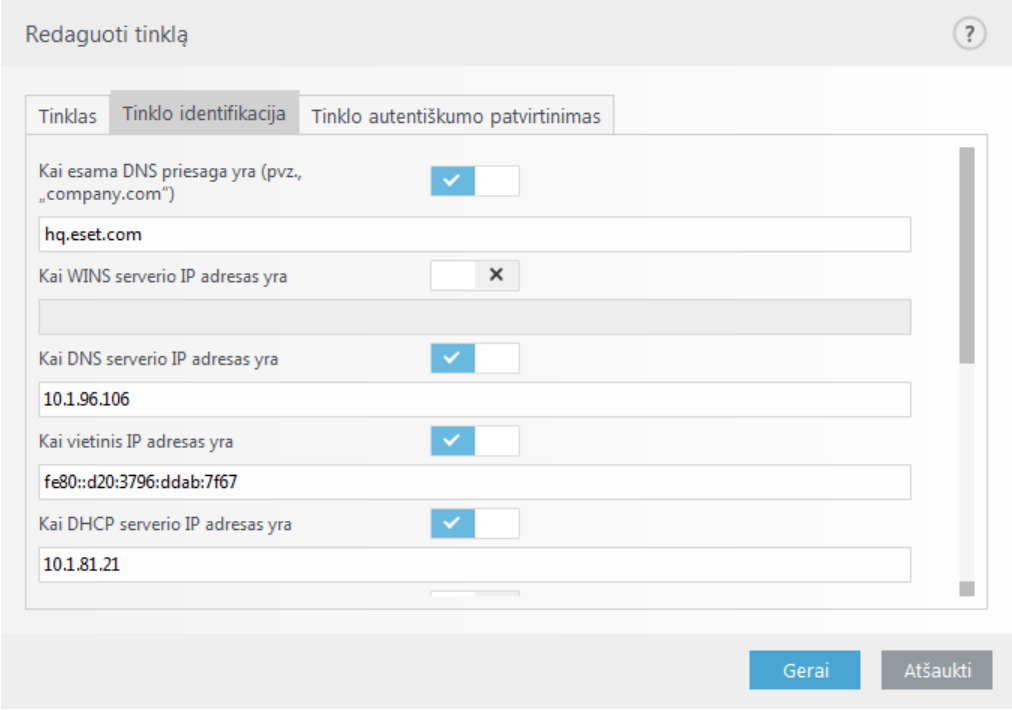
Naujinimo profilis – pasirinkite naujinimo profilį, kuris bus naudojamas prisijungus prie šio tinklo.

Kad prijungtų tinklų sąraše tinklas būtų pažymėtas kaip prijungtas, turi būti patenkintos toliau nurodytos sąlygos:

- **Tinklo identifikacija** – visi įvesti parametrai turi sutapti su aktyviojo ryšio parametrais.
- **Tinklo autentiškumo patvirtinimas** – pasirinkus autentiškumo patvirtinimo serverį, „ESET Authentication Server“ turi sėkmingai patvirtinti autentiškumą.

Tinklo identifikavimas

Tinklo identifikavimas atliekamas pagal vietinio tinklo adapterio parametrus. Visi pasirinkti parametrai palyginami su faktiniais aktyvaus tinklo ryšių parametrais. Leidžiami IPv4 ir IPv6 adresai.



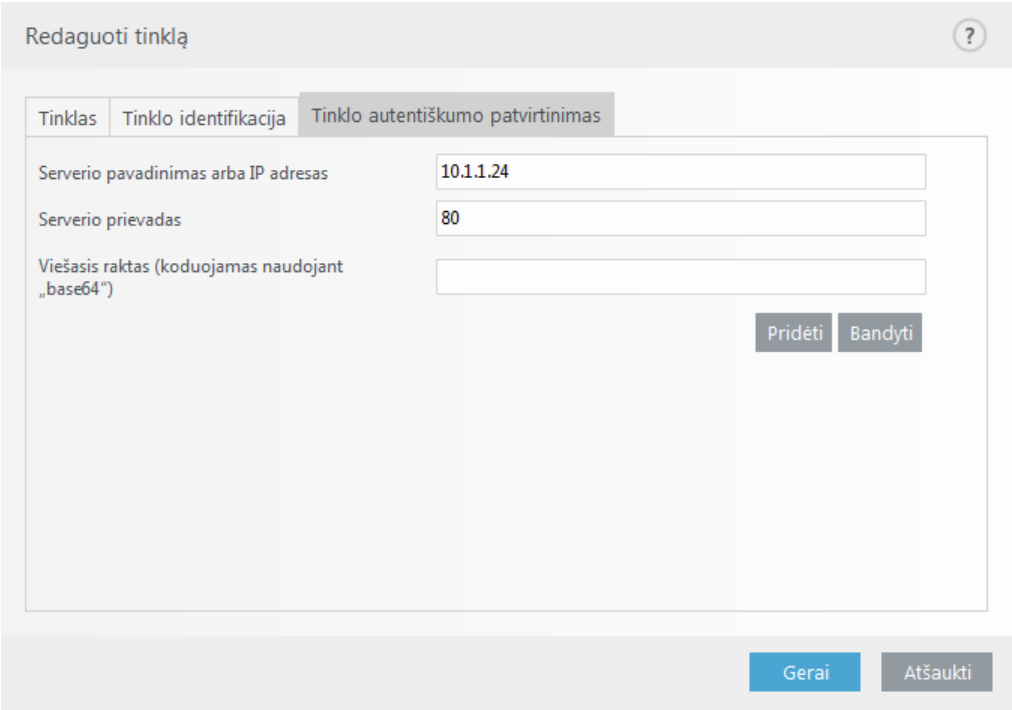
Tinklo autentiškumo patvirtinimas

Tinklo autentiškumo patvirtinimo funkcija ieško konkretaus serverio tinkle ir to serverio autentiškumui patvirtinti naudoja asimetrinio šifravimo būdą (RSA). Tinklo, kurio autentiškumas tvirtinamas, pavadinimas turi sutapti su zonos pavadinimu, nustatytu autentiškumo patvirtinimo serverio parametruose. Pavadinime skiriamos didžiosios ir mažosios raidės. Nurodykite serverio pavadinimą, serverio klausymo prievadą ir viešąjį raktą, kuris atitinka privatų serverio raktą (žr. Tinklo autentiškumo patvirtinimas – Serverio konfigūravimas). Serverio pavadinimą galima įvesti taip: IP adresas, DNS arba „NetBios“ pavadinimas. Po jo gali būti pateiktas kelias, nurodantis rakto vietą serveryje (pvz., serverio_pavadinimas_/1katalogas/2katalogas/autentiškumo patvirtinimas). Galite nurodyti alternatyvius naudotinus serverius, įtraukdami juos į kelią ir atskirdami kabliataškiais.

Atsisiųskite „ESET Authentication Server“

Viešasis raktas gali būti importuojamas naudojant bet kurį iš šių failų tipų:

- PEM šifruotas viešasis raktas („.pem“): šis raktas gali būti sugeneruotas naudojant „ESET Authentication Server“ (žr. skyrių Tinklo autentiškumo patvirtinimas – Serverio konfigūravimas).
- Šifruotas viešasis raktas
- Viešojo rakto sertifikatas („.crt“)



Spustelėkite **Bandyti** , kad išbandytumėte savo parametrus. Jei autentiškumas patvirtinamas sėkmingai, pasirodo pranešimas Serverio autentiškumas patvirtintas sėkmingai. Jei atpažinimas nėra tinkamai sukonfigūruotas, bus parodytas vienas iš šių klaidos pranešimų:

Serverio atpažinimas nesėkmingas. Negalioja arba nesutampa parašas.
Serverio parašas neatitinka įvesto viešojo rakto.

Serverio atpažinimas nesėkmingas. Nesutampa tinklo pavadinimas.
Sukonfigūruoto tinklo pavadinimas neatitinka autentiškumo patvirtinimo serverio zonos pavadinimo.
Peržvelkite abu pavadinimus ir užtikrinkite, kad jie būtų identiški.

Serverio atpažinimas nesėkmingas. Negauta atsakymo iš serverio arba gautas negaliojantis atsakymas.
Atsakymo negaunama, jei serveris neveikia arba yra nepasiekiamas. Negaliojantis atsakymas gali būti gautas, jei nurodytu adresu veikia kitas HTTP serveris.

Įvestas negaliojantis viešasis raktas.
Patikrinkite, ar jūsų įvestas viešasis raktas nėra sugadintas.

Tinklo autentiškumo patvirtinimas – serverio konfigūravimas

Atpažinimo procesą gali vykdyti bet kuris kompiuteris / serveris, prijungtas prie tinklo, kurį reikia atpažinti. „ESET Authentication Server“ programa turi būti įdiegta kompiuteryje / serveryje, kuris būtų visada pasiekiamas prireikus atlikti atpažinimą, kai tik klientas bando jungtis prie tinklo. „ESET Authentication Server“ programos diegimo failą galima atsisiųsti iš ESET svetainės.

Įdiegus „ESET Authentication Server“ programą, pasirodys dialogo langas (programą galite pasiekti spustelėję **Pradėti** > **Programos** > **ESET** > **ESET Authentication Server**).

Norėdami konfigūruoti autentiškumo patvirtinimo serverį, įveskite autentiškumo patvirtinimo tinklo pavadinimą, serverio klausymo prievadą (numatytasis yra 80) ir vietą, kur bus saugoma viešojo ir privačiojo raktų pora. Tada generuokite viešąjį ir privatųjį raktus, kurie bus naudojami atpažįstant. Privatusis raktas liks serveryje, o viešasis raktas turi būti importuotas į kliento pusės tinklo autentiškumo patvirtinimo skyrių, kai nustatomas tinklas užkardos nustatymuose.

Užkardos profiliai

„**Global default profile**“ (visuotinis numatytasis profilis) – jei iš tinklo ir adapterio konfigūracijos negaunama profilio, naudojamas visuotinis numatytasis profilis.

„**List of profiles**“ (profilių sąrašas) – profilius galima naudoti „ESET Endpoint Security“ užkardos elgsenai valdyti. Kurdami arba redaguodami užkardos taisyklę, galite priskirti ją konkrečiam profiliui arba taikyti kiekvienam profiliui. Kai tinklo sąsajoje aktyvus konkretus profilis, jam taikomos tik visuotinės taisyklės (taisyklės, nepriskirtos konkrečiam profiliui) ir taisyklės, kurios priskirtos tam profiliui. Kad galėtumėte paprastai keisti užkardos elgseną, galite sukurti įvairius profilius su skirtingomis taisyklėmis, priskirtomis tinklo adapteriams arba tinklams.

„**Profiles assigned to network adapters**“ (profiliai, priskirti tinklo adapteriams) – tinklo adapterį galima nustatyti taip, kad būtų naudojamas profilis, sukonfigūruotas konkrečiam tinklui, kai jis prisijungs prie to tinklo.

Tai atliekama skiltyje „**Advanced setup**“ (išplėstiniai nustatymai) (F5) > „**Firewall**“ (užkarda) > „**Known networks**“ (žinomi tinklai). Sąraše **Žinomi tinklai** pasirinkite tinklą ir spustelėkite **Redaguoti**, kad išskleidžiamajame meniu **Užkardos profilis** priskirtumėte užkardos profilį konkrečiam tinklui. Jei tas tinklas neturi priskirto profilio, tuomet bus naudojamas adapterio numatytasis profilis. Jei adapteris nustatytas nenaudoti tinklo profilio, bus naudojamas jo numatytasis profilis, nepaisant tinklo, prie kurio jis prisijungs. Jei nėra tinklo ar adapterio konfigūracijos profilio, naudojamas visuotinis numatytasis profilis. Norėdami priskirti profilį tinklo adapteriui, pasirinkite tinklo adapterį, spustelėkite „**Edit**“ (redaguoti) šalia „**Profiles assigned to network adapters**“ (profiliai, priskirti tinklo adapteriams), pasirinkite profilį išskleidžiamajame meniu „**Default firewall profile**“ (numatytasis užkardos profilis) ir tada spustelėkite „**OK**“ (gerai).

Kai užkarda persijungia į kitą profilį, apatiniame dešiniajame kampe, prie sistemos laikrodžio, pateikiamas pranešimas.

Profiliai, priskirti tinklo adapteriams

Perjungiant profilius galima operatyviai atlikti daug užkardos elgsenos pakeitimų. Galima nustatyti tinkintas taisykles ir pritaikyti jas konkretiems profiliams. Į sąrašą **Tinklo adapteriai** automatiškai įtraukiami visų kompiuteryje esančių tinklo adapterių įrašai.

Stulpeliai

Pavadinimas – tinklo adapterio pavadinimas.

Numatytasis užkardos profilis – numatytasis profilis naudojamas, kai tinklas, prie kurio prisijungėte, neturi sukonfigūruoto profilio arba jūsų tinklo adapteris nustatytas nenaudoti tinklo profilio.

„**Prefer network's profile**“ (pageidauti tinklo profilio) – tinklo adapteris gali naudoti užkardos profilį,

sukonfigūruotą prijungtam žinomam tinklui. Jei tas tinklas sukonfigūruoto profilio neturi arba tinklo adapteris nustatytas nenaudoti tinklo profilio, naudojamas adapterio numatytasis profilis.

Valdymo elementai

Pridėti – pridedamas naujas tinklo adapteris.

Redaguoti – leidžiama redaguoti esamą tinklo adapterį.

Šalinti – pasirinkite tinklo adapterį ir spustelėkite Šalinti, jei tinklo adapterį norite pašalinti iš sąrašo.

Gerai / atšaukti – spustelėkite **Gerai**, jei norite įrašyti pakeitimus, arba spustelėkite **Atšaukti**, kad užvertumėte neatlikę pakeitimų.

Programos modifikavimo aptikimas

Jei ryšį bando užmegzti modifikuotos programos, kurioms yra nustatyta užkardos taisyklė, programos modifikavimo aptikimo funkcija ima rodyti pranešimus. Tai naudinga siekiant išvengti piktnaudžiavimo kai kurioms programoms sukonfigūruotomis taisyklėmis, kai tai bando daryti kita programa, laikinai arba nuolatos pakeisdama originalios programos vykdomąjį failą kitos programos vykdomuoju failu arba kenkimo tikslais modifikuodama originalios programos vykdomąjį failą.

Atminkite, kad šia savybe nesiekiama bendrai aptikti programų modifikavimo atvejų. Šiuo atveju tikslas – išvengti piktnaudžiavimo esamomis užkardos taisyklėmis ir stebimos tik tos programos, kurioms yra nustatytos konkrečios užkardos taisyklės.

Įjungti programos keitimų aptikimą – jeigu pasirinkta, sistema stebės, ar nekeičiamos programos (naujinimai, užkrėtimai, kitos modifikacijos). Kai modifikuota taikomoji programa bandys užmegzti ryšį, užkarda jums apie tai praneš.

Leisti modifikuoti pasirašytas (patikimas) programas – nepranešti, jei programa prieš ir po modifikavimo išlaiko tą patį galiojantį skaitmeninį parašą.

Netikrinamų programų sąrašas – šiame lange galima pridėti arba pašalinti atskiras programas, kurias galima modifikuoti neparodant pranešimų.

Į modifikavimo aptikimo procesą neįtrauktos programos

ESET Endpoint Security užkarda aptinka pokyčius tose programose, kurioms yra sukurtos taisyklės (žr. Programų modifikavimo aptikimas).

Tam tikrais atvejais galite nenorėti taikyti šios funkcijos kai kurioms programoms ir galite norėti jų neįtraukti į užkardos vykdomas patikras.

Pridėti – atidaromas langas ir jame galima pasirinkti programą, kurią norite pridėti prie sąrašo programų, neįtrauktų į modifikavimo aptikimo procesą. Galima rinktis iš sąrašo veikiančių programų su atviru tinklo ryšiu, kurioms taikoma užkardos taisyklė, arba pridėti konkrečią programą.

Redaguoti – atidaromas langas ir jame galima pakeisti vietą programos, kuri priklauso sąrašui programų,

neįtrauktų į modifikavimo aptikimo procesą. Galima rinktis iš sąrašo veikiančių programų su atviru tinklo ryšiu, kurioms taikoma užkardos taisyklė, arba pakeisti vietą rankiniu būdu.

Šalinti – šalina į modifikavimo aptikimo procesą neįtrauktų programų sąrašo įrašus.

Taisyklių konfigūravimas ir naudojimas

Taisyklės – tai sąlygų rinkinys, naudojamas tikrinti visus šioms sąlygoms priskirtus tinklo ryšius ir veiksmus. Naudodamiesi užkardos taisyklėmis galite nurodyti veiksmą, kurį reikia atlikti užmezgus įvairius tinklo ryšius. Kad pasiektumėte taisyklių filtravimo nustatymus, atverkite **Išplėstiniai nustatymai** (F5) > **Tinklo apsauga** > **Užkarda** > **Išplėstinis**. Kai kurios iš anksto apibrėžtos taisyklės yra siejamos su **leidžiamų paslaugų** žymimaisiais langeliais (Leidžiamos paslaugos ir išplėstinės parinktys) ir jų negalima išjungti tiesiogiai: vietoj to šiuo tikslu galima naudoti tuos susijusius žymimuosius langelius.

Priešingai nei ankstesnėje ESET Endpoint Security versijoje, taisyklės yra vertinamos iš viršaus žemyn. Kiekvienam vertinamam tinklo ryšiui naudojamas pirmosios atitinkančios taisyklės veiksmas. Tai – svarbus elgsenos pakeitimas lyginant su ankstesne versija, kurioje taisyklių prioritetai buvo suteikiami automatiškai ir konkretesnės taisyklės gaudavo aukštesnius prioritetus nei bendresnio pobūdžio taisyklės.

Ryšius galima skirstyti į gaunamus ir siunčiamus ryšius. Gaunami ryšiai yra inicijuojami nuotolinio kompiuterio, bandančio užmegzti ryšį su vietine sistema. Siunčiami ryšiai veikia atvirkščiai – vietinė sistema kreipiasi į nuotolinį kompiuterį.

Jeigu aptinkamas naujas nežinomas ryšys, atsargiai apsvarstykite, ar leisti jį, ar uždrausti. Neprašyti, nesaugūs arba nežinomi ryšiai kelia riziką sistemos saugai. Jeigu toks ryšys užmezgamas, rekomenduojame atkreipti ypatingą dėmesį nuotolinio kompiuterio ir taikomosios programos bandymą prisijungti prie jūsų kompiuterio. Daugelis įsiskverbimų bando gauti ir išsiųsti asmeninius duomenis arba atsisiųsti kitas kenkėjiškas programas į pagrindinius kompiuterius. Užkarda leidžia aptikti ir nutraukti tokius ryšius.

Užkardos taisyklių sąrašas

Užkardos taisyklių sąrašą rasite **Išplėstiniai nustatymai (F5)** > **Tinklo apsauga** > **Užkarda** > **Pagrindinis** ir spustelėję **Redaguoti** šalia **Taisyklės**.

Stulpeliai

Pavadinimas – taisyklės pavadinimas.

Įjungta – parodo, ar taisyklė įjungta, ar išjungta. Norint suaktyvinti taisyklę, reikia pažymėti atitinkamą žymimąjį langelį.

Protokolas – protokolas, kuriam taikoma ši taisyklė.

Profilis – čia rodomas užkardos profilis, kuriam taikoma ši taisyklė.

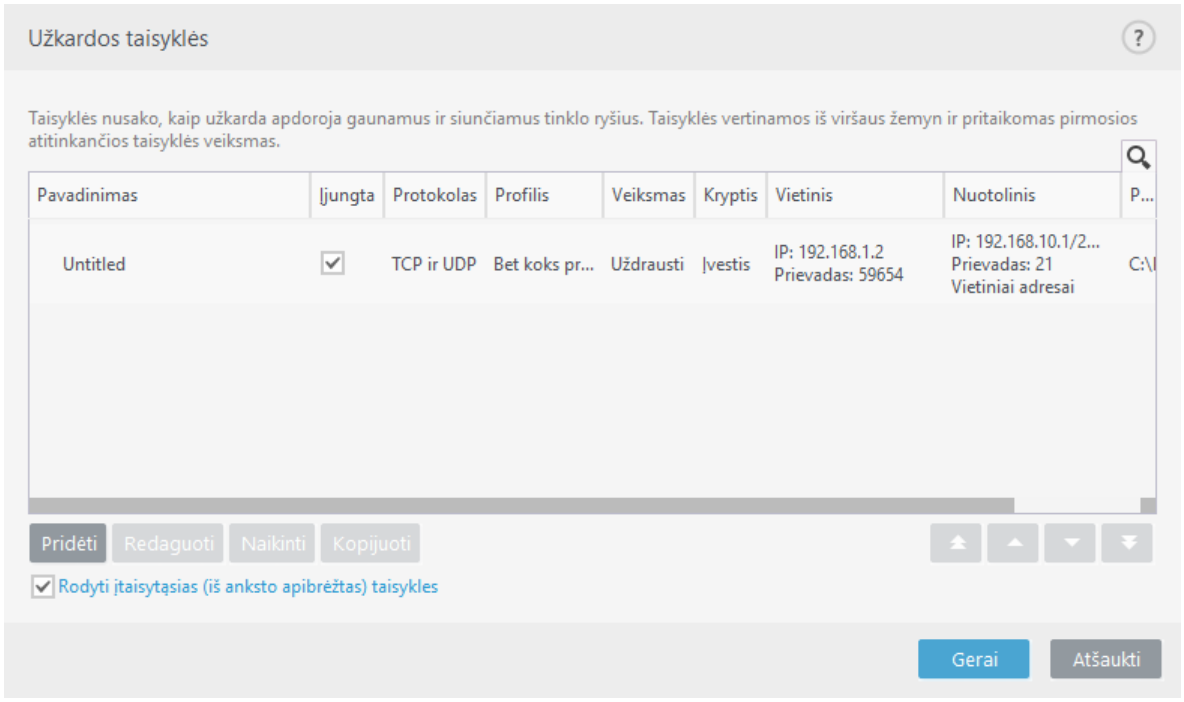
Veiksmas – pateikiama ryšio būsena (blokuoti / leisti / klausti).

Kryptis – ryšio kryptis (įeinantis / išeinantis / abi).

Vietinis – vietinio kompiuterio nuotolinis Ipv4 arba Ipv6 adresas / diapazonas / potinklis ir prievadas.

Nuotolinis – nuotolinio kompiuterio nuotolinis Ipv4 arba Ipv6 adresas / diapazonas / potinklis ir prievadas.

Programa – programa, kuriai taikoma taisyklė.



Valdymo elementai

Pridėti – sukuriama nauja taisyklė.

Redaguoti – redaguokite esamą taisyklę.

Pašalinti – pašalinkite esamą taisyklę.

Kopijuoti – sukurkite pasirinktos taisyklės kopiją.

Rodyti įtaisytąsias (iš anksto apibrėžtas) taisykles – taisyklės, iš anksto apibrėžtos ESET Endpoint Security, kurios leidžia arba draudžia konkrečius ryšius. Šias taisykles galite išjungti, tačiau iš anksto nustatytos taisyklės panaikinti negalima.

Į viršų / aukštyn / žemyn / į apačią – suteikia galimybę nustatyti taisyklių pirmumo lygį (taisyklės vykdomos iš viršaus žemyn).

Spustelėkite paieškos piktogramą viršutiniame dešiniajame kampe ir ieškokite taisyklės pagal pavadinimą, protokolą ar prievadą.

Užkardos taisyklių įtraukimas arba redagavimas

Gali reikėti redaguoti arba pridėti užkardos taisykles, kai pasikeičia tinklo nustatymai (pvz., pasikeitė nuotolinės pusės tinklo adresas arba prievado numeris), kad būtų užtikrintas tinkamas programos, kuriai taikoma taisyklė, veikimas.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Užkardos taisyklių ESET Endpoint Security kūrimas arba redagavimas
- Užkardos taisyklių kūrimas arba redagavimas klientų darbo vietose ESET PROTECT

Viršutinėje lango dalyje yra trys skirtukai:

- **Bendroji informacija** – nurodykite taisyklės pavadinimą, ryšio kryptį, veiksmą (**Leisti**, **Drausti**, **Klausti**), protokolą ir profilį, kuriam taisyklė bus taikoma.
- **Vietinis** – rodo informaciją apie ryšio vietinę pusę, kurioje pateikiamas vietinio prievado numeris arba prievadų intervalas ir ryšį palaikančios taikomosios programos pavadinimas. Čia galite pridėti iš anksto nustatytą arba sukurtą zoną su IP adresų diapazonu spustelėdami **„Pridėti“**.
- **Nuotolinis** – šiame skirtuke yra informacija apie nuotolinį prievadą (prievadų intervalą). Čia galite sudaryti nuotolinių IP adresų ar zonų, skirtų tam tikrai taisyklei, sąrašą. Čia galite pridėti iš anksto nustatytą arba sukurtą zoną su IP adresų diapazonu spustelėdami **„Pridėti“**.

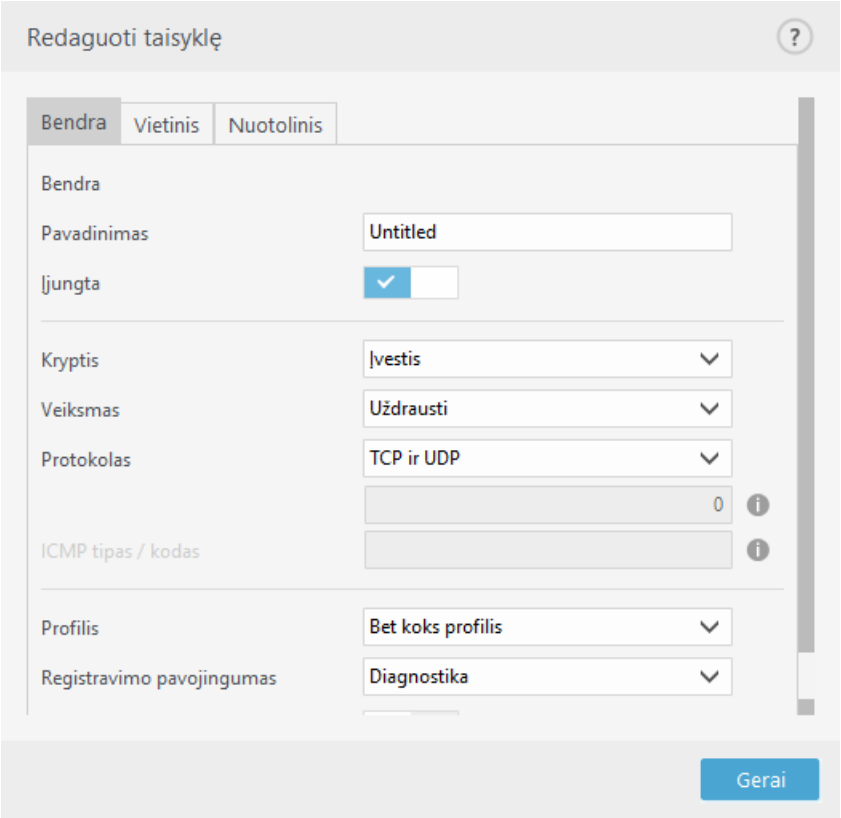
Kurdami naują taisyklę, lauke **Pavadinimas** turite įvesti taisyklės pavadinimą. Išskleidžiamajame meniu **Kryptis** pasirinkite kryptį, kuria taisyklė bus taikoma, ir veiksmą, kuris bus vykdomas, kai ryšiui bus pritaikyta taisyklė iš išskleidžiamojo meniu **Veiksmas**.

Protokolas pateikia taisyklei naudojamą ryšio protokolą. Išskleidžiamajame meniu nurodykite, kuris protokolas bus taikomas konkrečioje taisyklėje.

ICMP tipas / kodas atitinka ICMP pranešimą, kuris identifikuojamas skaičiumi (pvz., 0 atitinka „Aido atsakymas“).

Pagal numatytąją parinktį nurodžius **Bet koks profilis**, įjungiamos visos taisyklės. Kitas būdas: išskleidžiamajame meniu **Profiliai** nurodykite pasirinktinį užkardos profilį.

Jei įjungsite parinktį **Registravimo svarbumas**, su taisykle susijusi veikla bus registruojama žurnale. Parinktis **Įspėti naudotoją** rodo pranešimą, kai taisyklė yra taikoma.



Užkardos žurnalus su veiksmu **Atmesti** ir registravimo rimtumo **įspėjimą** gali rinkti ESET PROTECT.

Sukuriame naują taisyklę, kad interneto naršyklė Firefox galėtų prisijungti prie Internetas / vietinio tinklo svetainių.
1. Skirtuke **Bendroji informacija** įjunkite siunčiamą ryšį, naudojantį TCP ir UDP protokolus.
2. Spragtelėkite skirtuką **Vietinis** .
3. Pasirinkite jūsų naudojamos žiniatinklio naršyklės failo kelią spustelėdami **...** (pvz., *C:\Program Files\Firefox\Firefox.exe*). NEĮVESKITE programos pavadinimo.
4. Kortelėje **Nuotolinis** įjunkite prievado numerius 80 ir 443, jeigu norite leisti tik standartinius interneto naršymo veiksmus.

Iš anksto nustatytose taisyklėse pakeitimai ribojami.

Užkardos taisyklės – vietinis

Įveskite vietinės programos pavadinimą ir vietinį prievadą (prievadus), kuriam bus taikoma taisyklė.

Prievadas – vietinio prievado numeris (-iai). Jeigu numeriai nepateikiami, taisyklė bus taikoma visiems prievadams. Pridėkite vieną ryšio prievadą arba jų intervalą.

IP – leidžia pridėti nuotolinį adresą / adresus, adresų intervalą arba potinklį, kuriame bus taikoma taisyklė. Jei reikšmė nepateikiama, taisyklė bus taikoma visiems ryšiams.

Zonos – pridėtų zonų sąrašas.

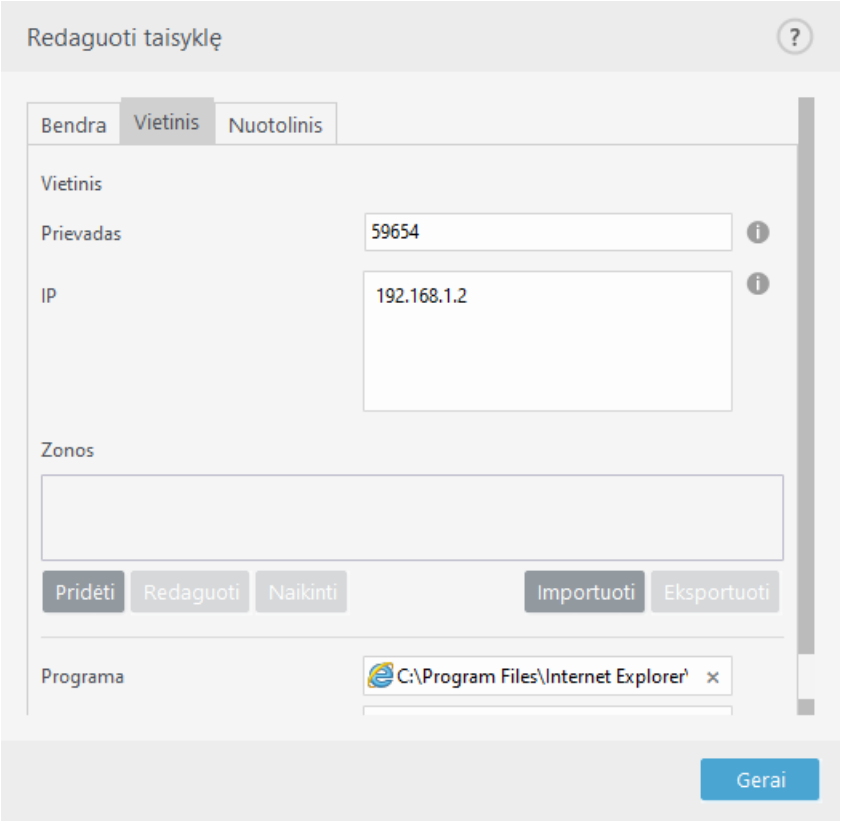
Pridėti – išskleidžiamajame meniu pasirinkite ir pridėkite sukurtą zoną. Zonai sukurti naudokite kortelę Zonos nustatymai.

Šalinti – pašalinamos zonos iš sąrašo.

Taikomoji programa – taikomosios programos, kuriai taikoma taisyklė, pavadinimas. Pridėkite programos, kuriai bus taikoma taisyklė, vietą.

Paslauga – išskleidžiamajame meniu parodomos sistemos paslaugos.

Naudodamiesi išskleidžiamuoju meniu galbūt veidrodiniam atspindžiui norėsite sukurti taisyklę, kuri naujinimus teiks per 2221 prievadą ryšiui naudodama EHttpSrv *tarnybą* .



Užkardos taisyklės – nuotolinis

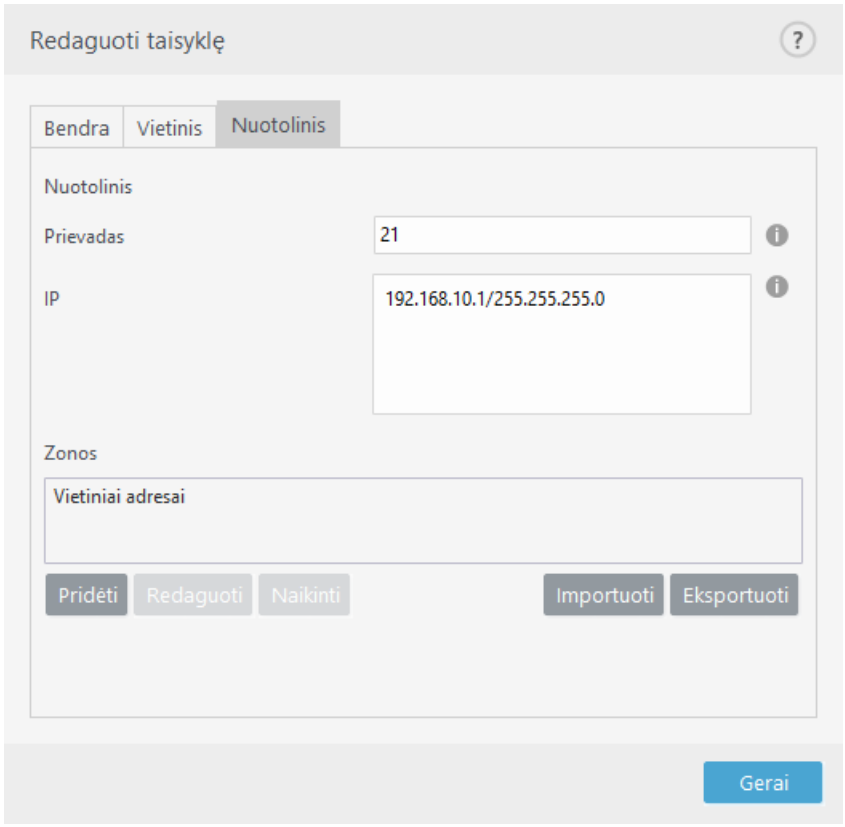
Prievadas – nuotolinio prievado numeris (-iai). Jeigu numeriai nepateikiami, taisyklė bus taikoma visiems prievadams. Pridėkite vieną ryšio prievadą arba jų intervalą.

IP – leidžia pridėti nuotolinį adresą, adresų intervalą arba potinklį. Adresas, intervalas / potinklis arba nuotolinė zona, kuriems taikoma taisyklė. Jeigu reikšmė nepateikiama, taisyklė bus taikoma visiems ryšiams.

Zonos – pridėtų zonų sąrašas.

Pridėti – pridėkite zoną, pasirinkdami ją išskleidžiamajame meniu. Zonai sukurti naudokite kortelę Zonos nustatymai.

Šalinti – pašalinamos zonos iš sąrašo.



Laikinas IP adresų juodasis sąrašas

Norėdami peržiūrėti IP adresus, kurie buvo aptikti kaip atakų šaltiniai, pridedami prie juodojo sąrašo, kad kuriam laikui būtų uždraustas ryšys, programoje ESET Endpoint Security eikite į **Nustatymai** > **Tinklas** > **Laikinasis IP adresų juodasis sąrašas**. Laikinai užblokuoti IP adresai blokuojami 1 valandą.

Stulpeliai

IP adresas – rodo užblokuotą IP adresą.

Blokavimo pagrindas – rodo atakos tipą, kuriam buvo sutrukdyta pasiekti adresą (pavyzdžiui, TCP prievadų nuskaitymo ataka).

Skirtasis laikas – rodo datą ir laiką, kada adresas bus pašalintas iš juodojo sąrašo.

Valdymo elementai

Šalinti – spustelėkite norėdami pašalinti adresą iš juodojo sąrašo nesibaigus skirtajam laikui.

Šalinti visus – spustelėkite norėdami nedelsiant pašalinti visus adresus iš juodojo sąrašo.

Add exception – spustelėkite norėdami pridėti užkardos išimtį prie IDS filtravimo.

Patikima zona

tai tinklo adresų grupė, iš kurios naudojant numatytuosius parametrus užkarda leidžia priimti tam tikrą srautą. Tam tikrų patikimos zonos funkcijų, pvz., failų bendrinimo ir nuotolinės prieigos prie darbalaukio, parametrus apibrėžia IDS ir išplėstinės parinktys.

Faktinė patikima zona apskaičiuojama dinamiškai ir atskirai kiekvienam tinklo adapteriui pagal tai, prie kurio tinklo kompiuteris šiuo metu yra prijungtas. Adresai, Zonų rengyklėje laikomi vidiniais patikimos zonos adresais, visada traktuojami kaip patikimi. Jei tinklo adapteris prisijungia prie žinomo tinklo, tame tinkle sukonfigūruoti **Papildomi patikimi adresai** yra pridedami prie adapterio patikimos zonos. Jei tinklas yra namų / biuro apsaugos tipo, visi tiesiogiai prijungti potinkliai yra įtraukiami į patikimą zoną. Faktinę kiekvieno tinklo adapterio patikimą zoną galima pamatyti lange **Nustatymas**, kurį rasite eidami **Tinklas** > **Tinklo adapteriai**.

Zonų konfigūravimas

Zona atitinka tinklo adresų rinkinį, kurie sudaro vieną loginę IP adresų grupę, kad būtų patogiau, kai keliose taisyklėse reikia pakartotinai naudoti tuos pačius adresus. Kiekvienam grupės adresui yra priskirtos analogiškos taisyklės, centralizuotai apibrėžtos visai grupei. Vienas iš tokios grupės pavyzdžių yra **Patikima zona**. Patikimą zoną sudaro grupė tinklo adresų, kurie jokiu būdu nėra blokuojami užkardos. Šias zonas galite konfigūruoti eidami į **Išplėstiniai nustatymai** > **Tinklo apsauga** > **Pagrindinis** > **Zonos** ir spustelėdami **Redaguoti** šalia **Zonos**. Jei norite pridėti naują zoną, spustelėkite **Pridėti**, įveskite zonos **Pavadinimą**, **Aprašą** ir pridėkite nuotolinio IP adresą lauke **Nuotolinio kompiuterio adresas (IPv4/IPv6, diapazonas, kaukė)**. Taip pat žr. Užkardos zonos.

Užkardos zonos

Jei reikia daugiau informacijos apie zonas, skaitykite skyrių Zonų konfigūravimas.

Stulpeliai

Pavadinimas – nuotolinių kompiuterių grupės pavadinimas.

IP adresai – nuotoliniai IP adresai, kurie priklauso šiai zonai.

Valdymo elementai

Pridėdami arba **redaguodami** zoną galite naudotis šiais laukais:

Pavadinimas – nuotolinių kompiuterių grupės pavadinimas.

Aprašas – bendras grupės aprašas.

Nuotolinio kompiuterio adresas (IPv4, IPv6, intervalas, kaukė) – leidžia pridėti nuotolinį adresą, adresų intervalą arba potinklį.

Šalinti – zona pašalinama iš sąrašo.

Atminkite, kad iš anksto nustatytų zonų negalima pašalinti.

Užkardos žurnalas

ESET Endpoint Security Užkarda įrašo visus svarbius įvykius į žurnalo failą, kurį galima peržiūrėti tiesiai iš pagrindinio meniu. Spustelėkite **Įrankiai** > **Žurnalo failai**, tada pasirinkite **Tinklo apsauga** išskleidžiamajame meniu **Žurnalas**. Jei norite įjungti šį užkardos registravimą, eikite į **Išplėstinis nustatymas** > **Įrankiai** > **Žurnalo failai** ir minimalų registravimo daugiažodiškumą nustatykite kaip **Diagnostika**. Visi uždrausti ryšiai bus užregistruoti.

Žurnalo failus galima naudoti klaidoms aptikti ir įsiskverbimams į jūsų sistemą atskleisti. ESET užkardos žurnaluose yra šie duomenys:

- **Laikas** – įvykio data ir laikas.
- **Įvykis** – įvykio pavadinimas.
- **Šaltinis** – šaltinio tinklo adresas.
- **Tikslas** – tikslinis tinklo adresas.
- **Protokolas** – tinklo ryšio protokolas.
- **Taisyklė / kirmino pavadinimas** – taikoma taisyklė arba kirmino pavadinimas (jei atpažintas).
- **Programa** – susijusi programa.
- **Naudotojas** – naudotojo, prisijungusio įsiskverbimo aptikimo metu, vardas.

Išsami šių duomenų analizė gali padėti aptikti bandymus kėsintis į sistemos saugą. Daugelis kitų veiksnių rodo galimą saugumo pavojų ir leidžia sumažinti jo poveikį. Galimų grėsmių indikatorių pavyzdžiai: dažni ryšiai iš nežinomų vietų, daug bandymų užmegzti ryšius ir ryšius bandančios užmegzti nežinomos programos arba naudojami neįprasti prievadų numeriai.

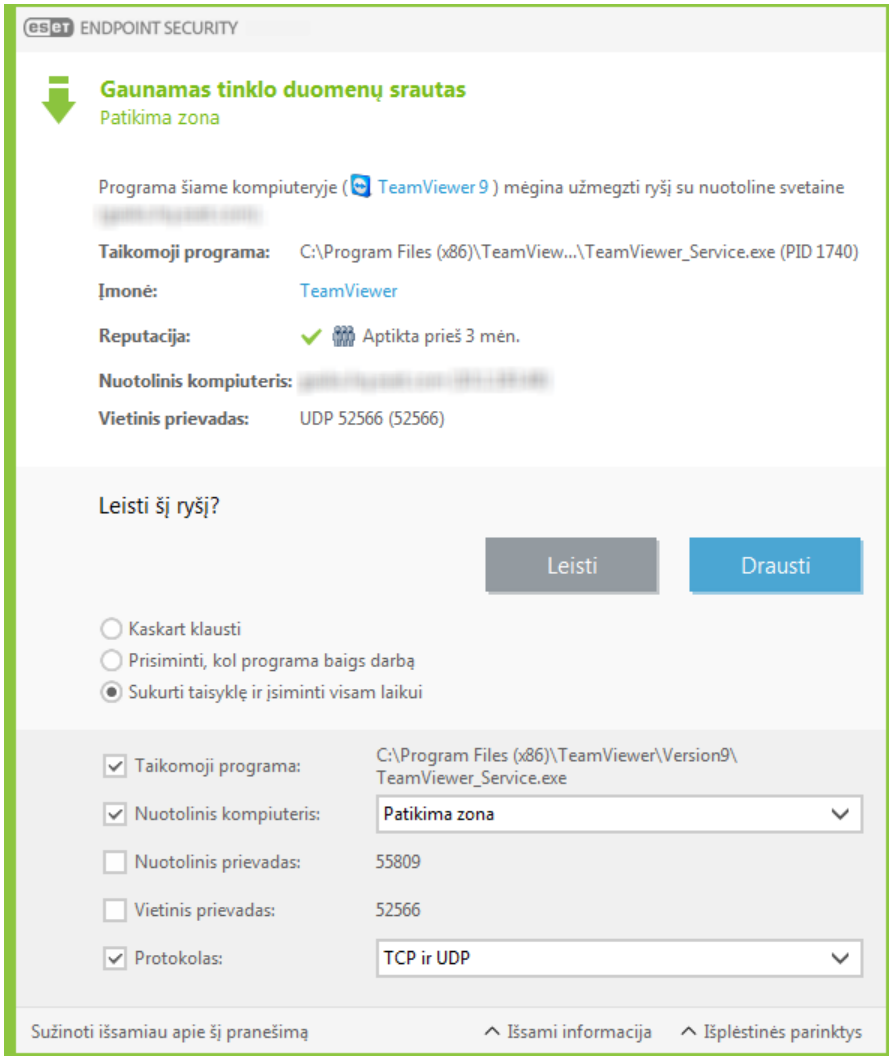
> Pranešimas apie saugumo pažeidžiamumą registruojamas net ir tuo atveju, jei konkretus pažeidžiamumas jau pašalintas, nes aptinkamas naudojimo bandymas ir jis blokuojamas tinklo lygmeniu prieš faktiškai naudojant.

Ryšio nustatymas – aptikimas

Užkarda aptinka kiekvieną naujai sukurtą tinklo ryšį. Aktyvusis užkardos režimas nustato, kokie veiksmai atliekami su nauju ryšiu. Jei aktyvinamas **Automatinis režimas** arba **Politika pagrįstas režimas**, užkarda atliks iš anksto nustatytus veiksmus nesikišant vartotojui.

Sąveikusis režimas rodo informacinį langą, kuriame pranešama apie naujo tinklo ryšio aptikimą ir pateikiama išsami informacija apie šį sujungimą. Galite leisti ryšį arba jo atsisakyti (blokuoti). Jeigu pakartotinai leisite tą patį ryšį dialogo lange, rekomenduojame sukurti naują taisyklę šiam ryšiui. Tam pasirinkite **Įsiminti veiksmą (sukurti taisyklę)** ir įrašykite šį veiksmą kaip naują užkardos taisyklę. Jeigu užkarda vėliau atpažins tą patį ryšį, ji taikys esamą taisyklę be vartotojo veiksmų.

Parinkus **Laikinai įsiminti proceso veiksmą**, veiksmas (**Leisti** / **Uždrausti**) naudojamas, kol programa paleidžiama iš naujo, pakeičiamos taisyklės arba filtravimo režimai, atnaujinamas užkardos modulis arba sistema paleidžiama iš naujo. Atlikus bet kuriuos iš šių veiksmų, laikinos taisyklės bus panaikintos.



Būkite atsargūs kurdami naujas taisykles ir leiskite tik tikrai saugius sujungimus. Jei visi ryšiai yra leidžiami, užkarda netenka prasmės. Tai svarbūs ryšių parametrai:

- **Nuotolinė pusė** – leiskite ryšius tik su patikimais ir žinomais adresais.
- **Vietinė taikomoji programa** – nepatariama leisti nežinomų programų ir procesų vykdomų ryšių.
- **Prievado numeris** – ryšys su bendraisiais prievadais (pvz., saityno srautas – prievado numeris 80) įprastomis aplinkybėmis turi būti leidžiamas.

Kad galėtų plisti, kompiuterio įsiskverbimai dažnai naudoja internetą ir paslėptus ryšius, kad užkrėstų nuotolines sistemas. Jeigu taisyklės yra tinkamai sukonfigūruotos, užkarda tampa naudingu įrankiu apsisaugant nuo įvairių kenkėjiškų kodų atakų.

ESET užkardos problemų sprendimas

Jei patiriate jungiamumo problemų, kai įdiegta ESET Endpoint Security, yra keli būdai nustatyti, ar ESET užkarda yra jų priežastis. Be to, ESET užkarda gali padėti sukurti naujas taisykles ar išimtis jungiamumo problemoms spręsti.

Žr. toliau pateiktą temą, kurioje rasite priemonių, padedančių spręsti ESET užkardos problemas:

- Trikčių šalinimo vedlys
- Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo
- Išimčių kūrimas iš užkardos pranešimų

- Tinklo apsaugos išplėstinį registravimą
- Problemų sprendimas naudojant protokolų filtravimą

Trikčių šalinimo vedlys

Trikčių šalinimo vedlys tyliai stebi visus blokuojamus ryšius ir padeda jums atlikti trikčių šalinimo procedūrą, kad išspręstų užkardos problemas, kurias sukelia konkrečios programos ar įrenginiai. Vėliau vedlys pasiūlo naują taikytiną taisyklių rinkinį (jei jį patvirtinate). **Trikčių šalinimo vedlį** rasite pagrindiniame meniu, pasirinkdami **Nustatymai** > **Tinklas**.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Užkardos išimties įtraukimas naudojant trikčių diagnostikos vedlį

Registravimas ir taisyklių arba išimčių kūrimas iš žurnalo

Pagal numatytąją parinktį ESET užkarda neregistruoja visų užblokuotų ryšių. Jei norite peržiūrėti užkardos užblokuotus elementus, įjunkite tinklo apsaugos išplėstinį registravimą skiltyje „**Diagnostics**“ (diagnostika), esančioje „**Advanced setup**“ (išplėstiniai nustatymai), nuėjus į „**Tools**“ (įrankiai) > **„Diagnostics“** (diagnostika). Jei žurnale pastebėsite ką nors, ko nenorite, kad jūsų užkarda blokuotų, galite sukurti taisyklę arba IDS taisyklę, dešiniuoju pelės klavišu spustelėdami tą elementą ir pasirinkdami „**Don't block similar events in the future**“ (neblokuoti panašių įvykių ateityje). Atminkite, kad visų užblokuotų ryšių žurnale gali būti tūkstančiai punktų, tarp kurių bus sunku surasti konkretų ryšį. Išsprendę problemą, galite išjungti registravimo funkciją.

Papildomos informacijos apie žurnalą rasite čia: Žurnalo failai.

Naudokite registravimo funkciją, kad pamatytumėte tvarką, pagal kurią užkarda blokuoja konkrečius ryšius. Be to, taisyklių kūrimo iš žurnalo funkcija leis sukurti taisykles, kurios darys tiksliai tai, ko jūs norėsite.

Sukurti taisyklę iš žurnalo

Naujoji ESET Endpoint Security versija leidžia sukurti taisyklę iš žurnalo. Pagrindiniame meniu spustelėkite **Įrankiai** > **Žurnalo failai**. Išskleidžiamajame meniu pasirinkite **Tinklo apsauga**, dešiniuoju pelės klavišu spustelėkite pageidaujamą žurnalo įrašą ir iš kontekstinio meniu pasirinkite **Ateityje neblokuoti panašių įvykių**. Pranešimo lange bus parodyta jūsų naujoji taisyklė.

Kad būtų galima iš žurnalo sukurti naujas taisykles, ESET Endpoint Security turi būti sukonfigūruota tokiais parametrais:

- nustatykite minimalų registravimo daugiažodiškumo lygį **Diagnostika**, pasirinkdami **Išplėstiniai nustatymai** (F5) > **Įrankiai** > **Žurnalo failai**,
- įjunkite parinktį **Rodyti pranešimus ir apie gaunamas atakas prieš saugumo spragas**, esančią **Išplėstiniai nustatymai** (F5) > **Tinklo apsauga** > **Apsauga nuo tinklo atakos** > **Išplėstinės parinktys** > **Įsilaužimo aptikimas**.

Išimčių kūrimas iš užkardos pranešimų

ESET užkardai aptikus kenkimo veiklą tinkle, pateikiamas įvykį apibūdinantis pranešimo langas. Šiame pranešime yra saitas, kurį paspaudus galima sužinoti išsamiau apie įvykį ir pageidaujant nustatyti jam išimtį.

> Jei tinklo programa ar įrenginys tinkamai neįgyvendina tinklo standartų, jis gali sužadinti pasikartojančius užkardos IDS pranešimus. Galite sukurti išimtį tiesiogiai iš pranešimo, kad ESET užkarda nebeaptiktų šios programos ar įrenginio.

Tinklo apsaugos išplėstinį registravimą

Šia funkcija siekiama vesti sudėtingesnius žurnalo failus ESET techninei pagalbai teikti. Šią funkciją naudokite tik to paprašius ESET techninės pagalbos tarnybai, nes ji gali sukurti didžiulį žurnalo failą ir sulėtinti jūsų kompiuterio darbą.

1. Pereikite prie **Išplėstinis nustatymai** > **Įrankiai** > **Diagnostika** ir įjunkite **Įjungti tinklo apsaugos išplėstinį registravimą**.
2. Pamėginkite atkurti problemą, su kuria susiduriate.
3. Išjunkite tinklo apsaugos išplėstinį registravimą.
4. Tinklo apsaugos išplėstinio registravimo sukurtą PCAP žurnalo failą rasite tame pačiame aplanke, kuriame generuojamos diagnostinės atminties išklotinės: *C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics*

Problemų sprendimas naudojant protokolų filtravimą

Jei kyla problemų su naršykle ar el. pašto programa, pirmiausia reikia išsiaiškinti, ar už jas neatsakinga protokolų filtravimo funkcija. Kad tai padarytumėte, pamėginkite išplėstiniuose nustatymuose laikinai išjungti programos protokolų filtravimo funkciją (nepamirškite baigę jos vėl įjungti, nes kitaip jūsų naršyklė ir el. pašto programa liks neapsaugotos). Jei išjungus problema dingsta, peržvelkite toliau pateiktą dažniausiai pasitaikančių problemų sąrašą su jų sprendimais:

Naujinimo arba saugaus ryšio problemos

Jei jūsų programa praneša, kad negali atsinaujinti arba ryšio kanalas nesaugus:

- Jei įjungta SSL protokolo filtravimo funkcija, pabandykite ją laikinai išjungti. Jei tai padeda, galite ir toliau naudoti SSL filtravimo funkciją ir leisti veikti naujinimo funkcijai, neįtraukdami probleminių ryšių: Perjunkite SSL protokolo filtravimo režimą į interaktyvųjį. Paleiskite naujinimo procesą iš naujo. Turi pasirodyti dialogo langas, informuojantis apie šifruojamą tinklo srautą. Užtikrinkite, kad programa atitiktų tą, kurios triktį šalinate, o sertifikatas būtų atsiunčiamas iš serverio, kuris tiekia jai naujinimus. Tada pasirinkite įsiminti veiksmą su šiuo sertifikatu ir spustelėkite „Nepaisyti“. Jei daugiau nerodoma susijusių dialogo langų, galite perjungti filtravimo režimą atgal į automatinį ir problema turėtų būti išspręsta.
- Jei konkreti programa nėra naršyklė arba el. pašto programa, galite jos visai neįtraukti į protokolų filtravimą (jei tai padarysite su naršykle ar el. pašto programa, kompiuteris taps pažeidžiamas). Visos programos, kurių ryšiai buvo filtruojami praeityje, turi jau būti įtrauktos į jums pateiktą sąrašą, kai buvo pridedama išimtis, tad rankiniu būdu jų įtraukti turbūt nereikės.

Jūsų tinkle veikiančio įrenginio pasiekimo problema

Jei negalite naudotis savo tinkle esančio įrenginio funkcijomis (pvz., atverti internetinės kameros tinklalapį ar leisti vaizdo įrašą namų medijos leistuvu), pamėginkite pridėti jo IPv4 ir IPv6 adresus į neįtrauktų adresų sąrašą.

Problemos su konkrečia interneto svetaine

Galite neįtraukti konkrečių interneto svetainių į protokolų filtravimą, naudodami URL adresų tvarkymo funkciją. Pavyzdžiui, jei negalite pasiekti https://www.gmail.com/intl/en/mail/help/about.html, pamėginkite pridėti *gmail.com* į neįtrauktų adresų sąrašą.

Klaida „Vis dar vykdomos kai kurios programos, galinčios importuoti šakninį sertifikatą“

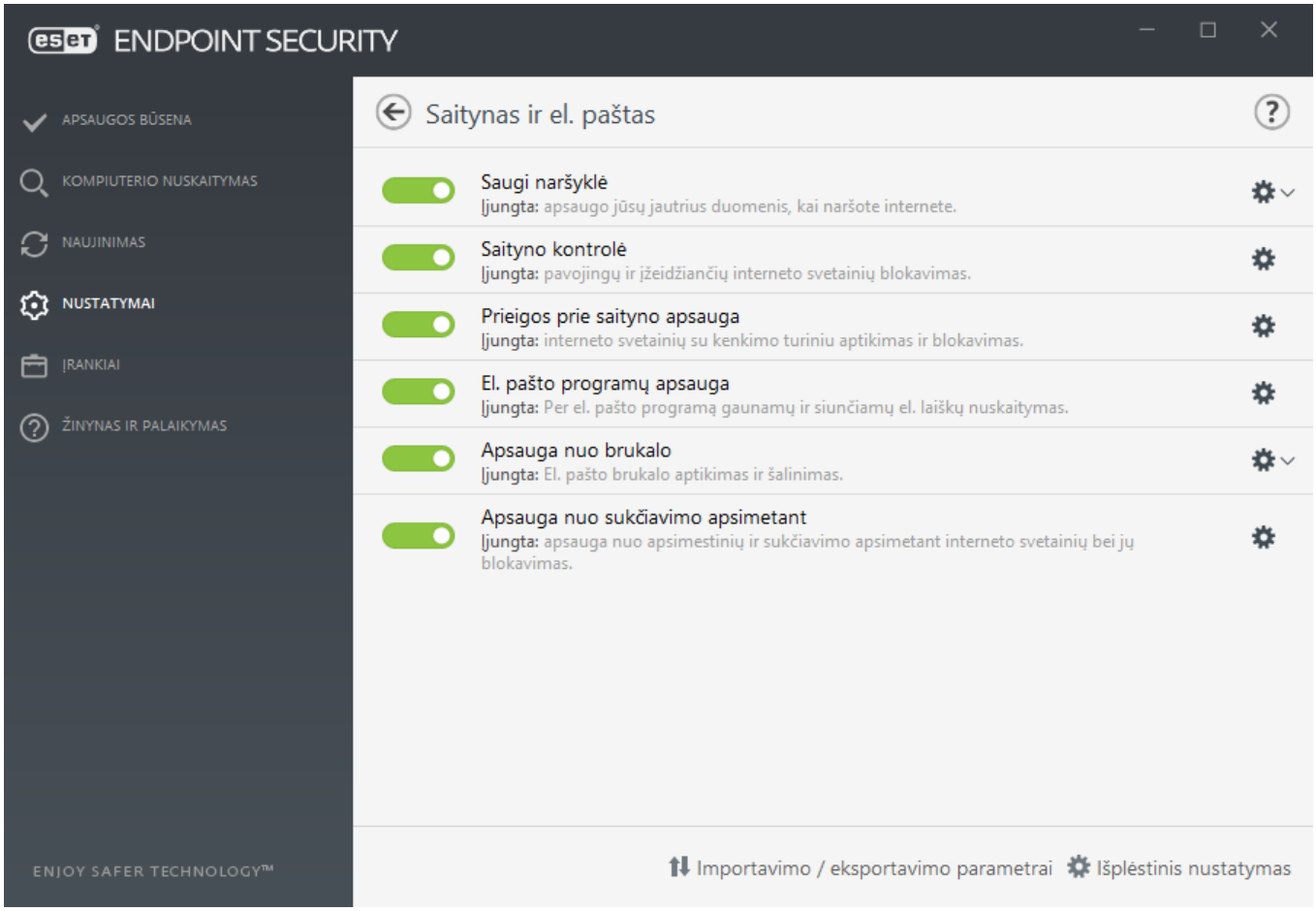
Jums įjungus SSL protokolų filtravimą, ESET Endpoint Security pasirūpina, kad įdiegtos programos pasikliautų būdu, kuriuo ji filtruoja SSL protokolą, importuodama sertifikatą į jų sertifikatų saugyklą. Kai kurioms programoms to padaryti neįmanoma, kol jos veikia. Tai taikoma „Firefox“ ir „Opera“. Įsitikinkite, kad nė viena iš jų neveikia (geriausias būdas tai padaryti – atverti užduočių tvarkytuvą ir patikrinti, ar jo kortelėje „Procesai“ nėra veikiančių failų „firefox.exe“ arba „opera.exe“), tada spustelėkite „Kartoti“.

Nepatikimo leidėjo arba negaliojančio sertifikato klaida

Tai dažniausiai reiškia, kad įvyko pirmiau nurodyto aprašyto importo proceso triktis. Pirmiausia įsitikinkite, kad neveikia nė viena iš paminėtų programų. Tada išjunkite SSL protokolų filtravimo funkciją ir po to vėl ją įjunkite. Taip pakartotinai įvykdysite importo procedūrą.

Saitynas ir el. paštas

Saityno ir el. pašto konfigūraciją rasite skiltyje **Nustatymai** > **Saitynas ir el. paštas**. Čia galite pasiekti išsamesnius programos parametrus.



Saugi naršyklė – Apsaugo jūsų jautrius duomenis, kai naršote internete.

Modulis Saityno kontrolė leidžia sukonfigūruoti parametrus, kurie administratoriams suteikia automatinių įrankių, padedančių apsaugoti kompiuterius ir nustatyti interneto naršymo apribojimus. Saityno kontrolės funkcijos paskirtis – uždrausti prieigą prie puslapių su netinkamu ar žalingu turiniu. Žr. Saityno kontrolė, kur rasite daugiau informacijos.

Galimybė jungtis prie interneto yra standartinė asmeninių kompiuterių funkcija. Deja, internetas tapo pagrindine kenkėjiško kodo platinimo terpe. Dėl to itin svarbu atidžiai įvertinti savo **prieigos prie saityno apsaugos** parametrus.

El. pašto programos apsauga kontroliuoja el. pašto ryšius, priimamus naudojant POP3(S) ir IMAP(S) protokolus. Naudodama jūsų el. pašto programos papildinį, ESET Endpoint Security užtikrina visų ryšių iš el. pašto programos kontrolę.

Apsauga nuo brukalo filtruoja nepageidaujamus el. laiškus.

Spustelėjus krumpliaračio piktogramą , šalia punkto Apsauga nuo brukalo pateikiamos tokios parinktys:

Konfigūruoti – atveria išplėstinius el. pašto programos apsaugos nuo brukalo parametrus.

Naudotojo adresų sąrašas – atveria dialogo langą, kuriame galite pridėti, redaguoti arba naikinti el. pašto adresus, kurie laikomi saugiais ar nesaugiais. Pagal čia nustatytas taisykles, el. laiškai iš šių adresų bus nenuskaitomi arba bus laikomi brukalu. Spustelėkite Naudotojo išimčių sąrašas, kad atvertumėte dialogo langą, kuriame galite pridėti, redaguoti arba pašalinti el. laiškų adresus, kurie gali būti apgaulingi ir naudojami brukalui siųsti. El. laiškai, gauti iš adresų, kurie nurodyti išimčių sąraše, visada bus nuskaitomi ieškant brukalo.

Apsauga nuo sukčiavimo apsimetant – tai dar vienas apsaugos sluoksnis, siūlantis padidintą apsaugą nuo

neteisėtų interneto svetainių, kurios mėgina išgauti slaptažodžius ir kitą slaptą informaciją. Apsaugą nuo sukčiavimo apsimetant rasite skiltiesSaitynas ir el. paštas polangyje Nustatymai. Žr. Apsauga nuo sukčiavimo apsimetant, kur rasite papildomos informacijos.

Saityno / el. pašto / apsaugos nuo sukčiavimo apsimetant/ apsaugą apsaugos modulį galite laikinai išjungti spustelėję .

Protokolų filtravimas

Programų protokolų apsaugą nuo virusų užtikrina „ThreatSense“ nuskaitymo modulis, kuriame sklandžiai integruotos visos pažangiausios kenkėjiškos programinės įrangos nuskaitymo metodikos. Protokolų filtravimas vykdomas automatiškai, nesvarbu, kokia interneto naršyklė ar el. pašto programa naudojama. Jei norite keisti užšifruotus (SSL) parametrus, eikite į **Išplėstinis nustatymas** (F5) > **Saitynas ir el. paštas** > **SSL/TLS**.

Įjungti programos protokolo turinio filtravimą – gali būti naudojamas protokolo filtravimui išjungti. Atminkite, kad nuo jo priklauso daugelis ESET Endpoint Security komponentų (prieigos prie saityno apsauga, el. pašto protokolų apsauga, apsauga nuo sukčiavimo apsimetant, saityno kontrolė), kurie be jo neveiks.

Neįtrauktos programos – leidžia į protokolų filtravimą neįtraukti konkrečių nuotolinių adresų. Naudinga, kai protokolų filtravimo funkcija kelia suderinamumo problemų.

Neįtraukti IP adresai – leidžia į protokolų filtravimą neįtraukti konkrečių programų. Naudinga, kai protokolų filtravimo funkcija kelia suderinamumo problemų.

IPv4 adresai ir kaukė:
• *192.168.0.10* – prideda atskiro kompiuterio IP adresą, kuriam bus taikoma taisyklė.
• *192.168.0.1–192.168.0.99* – įveda pradinį ir galutinį IP adresus, kad būtų nurodytas IP diapazonas (keleto kompiuterių), kuriam bus taikoma taisyklė.
• Potinklis, pavyzdžiui, kompiuterių grupė), kurį apibrėžė IP adresas ir kaukė. Pavyzdžiui, *255.255.255.0* yra tinklo kaukė prefiksui *192.168.1.0/24*, tai atitinka *192.168.1.1*–192.168.1.254 adresų diapazoną.
IPv6 adresai ir kaukė:
• *2001:718:1c01:16:214:22ff:fec9:ca5* – įtraukia atskiro kompiuterio IPv6 adresą, kuriam bus taikoma taisyklė
• *2002:c0a8:6301:1::1/64* – IPv6 adresas su 64 bitų prefikso ilgiu, tai reiškia *2002:c0a8:6301:0001:0000:0000:0000:0000 to 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

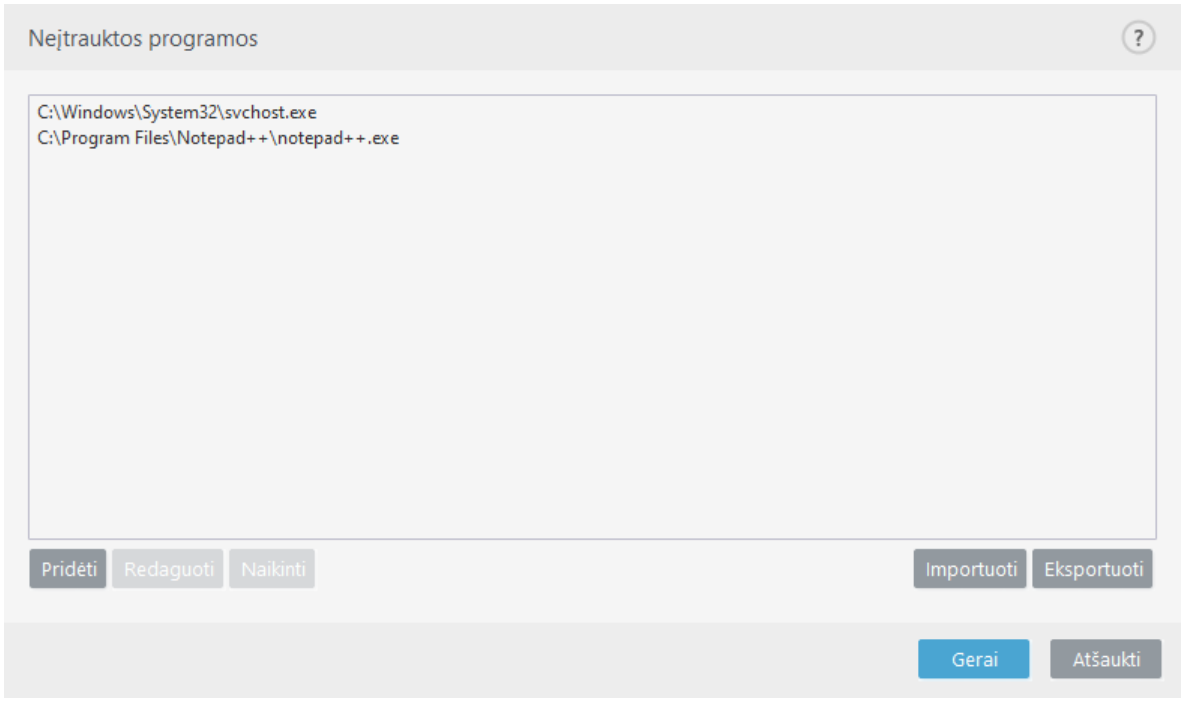
Neįtrauktos programos

Norėdami neįtraukti tam tikrų tinklinių programų į protokolų filtravimą, pridėkite jas į šį sąrašą. Pasirinktų programų HTTP/POP3/IMAP ryšys nebus tikrinamas ieškant grėsmių. Rekomenduojame šį metodą naudoti tik tais atvejais, kai esant įjungtam protokolui programos neveikia tinkamai.

Programos ir tarnybos, jau paveiktos protokolų filtravimo, bus automatiškai pateiktos spustelėjus **Pridėti**.

Redaguoti – suredaguokite pasirinktus sąrašo įrašus.

Šalinti – šalina pasirinktus įrašus iš sąrašo.



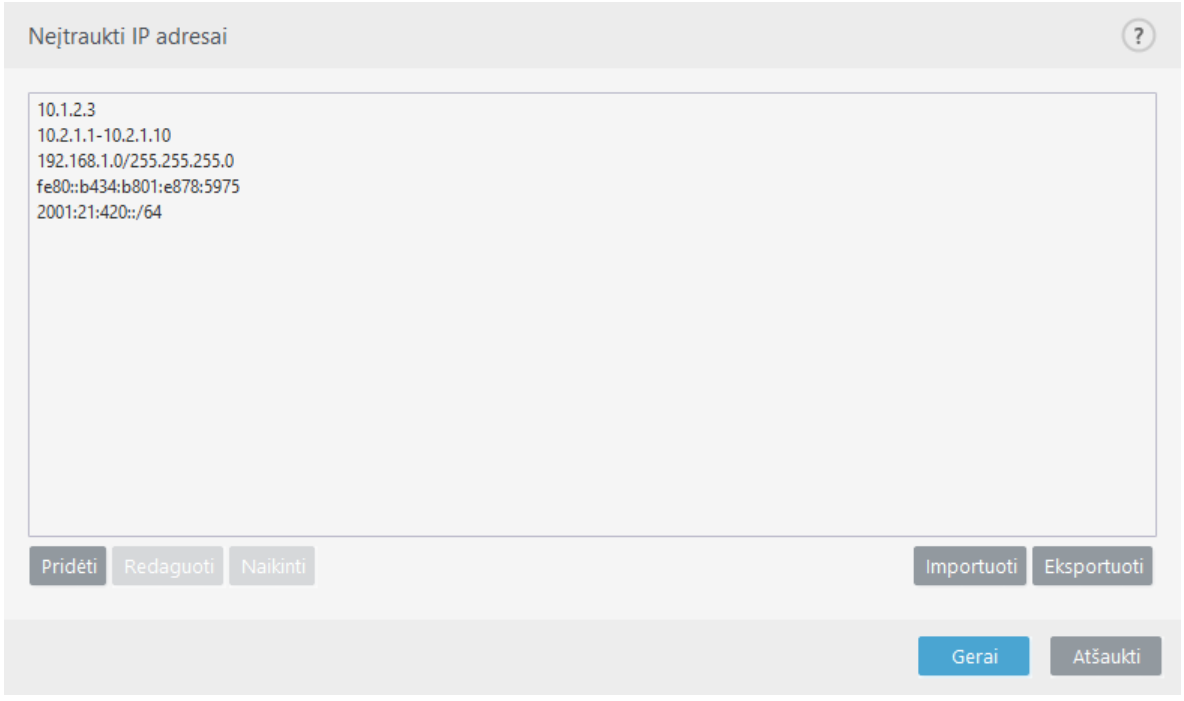
Nejtraukti IP adresai

Šiame sąraše esantys IP adresai bus nejtraukti į protokolo turinio filtravimo procesą. HTTP / POP3 / IMAP ryšys į pasirinktus adresus ir iš jų nebus tikrinamas ieškant grėsmių. Rekomenduojame naudoti šias parinktis tik adresams, kurie žinomi kaip patikimi.

Pridėti – spustelėkite, kad pridėtumėte IP adresą / adresų intervalą / nuotolinio taško potinklį, kuriam taikoma taisyklė.

Redaguoti – suredaguokite pasirinktus sąrašo įrašus.

Šalinti – šalina pasirinktus įrašus iš sąrašo.



SSL/TLS

ESET Endpoint Security gali ieškoti grėsmių ryšiuose, kuriuose naudojamas SSL protokolas. Galite rinktis įvairius nuskaitymo režimus SSL apsaugotiems ryšiams ištirti, naudodami patikimus sertifikatus, nežinomus sertifikatus arba sertifikatus, kurie yra neįtraukti į SSL apsaugotų ryšių tikrinimo procesą.

Įjungti SSL/TLS protokolo filtravimą – Protokolo filtravimas yra įjungtas pagal numatytuosius nustatymus. Galite išjungti SSL/TLS protokolų filtravimą dalyje **Išplėstinis nustatymas** > **Saitynas ir el. paštas** > **SSL/TLS** arba politikoje. Jei protokolo filtravimo funkcija išjungta, programa ryšių per SSL nenuskaito.

SSL/TLS protokolų filtravimo režimas siūlo tokias parinktis:

Filtravimo režimas	Aprašymas
Automatinis režimas	Numatytasis režimas nuskaitys tik reikiamas programas, pavyzdžiui, saityno naršykles ir el. pašto programas. Jį apeiti galima pasirenkant programas, kurių ryšiai bus nuskaitomi.
Interaktyvusis režimas	Jei įvesite naują SSL- apsaugotą svetainę (su nežinomu sertifikatu), bus parodytas veiksmo pasirinkimo dialogo langas. Šis režimas leidžia sukurti SSL sertifikatų / programų, kurie nebus nuskaitomi, sąrašą.
Politikos režimas	Nurodykite šią parinktį norėdami nuskaityti visus SSL apsaugotus ryšius, išskyrus sertifikatų apsaugotus ryšius, kurie yra neįtraukti į tikrinimą. Jeigu užmezgamas naujas ryšys, naudojantis nežinomą pasirašytą sertifikatą, jums apie tai nebus pranešta ir ryšys bus automatiškai filtruojamas. Kai prisijungsite prie serverio su nepatikimu sertifikatu, kuris buvo pažymėtas kaip patikimas (jis yra patikimų sertifikatų sąraše), ryšys su šiuo serveriu bus leidžiamas, o šio ryšio kanalo turinys bus filtruojamas.

Naudodamiesi **Filtruojamų SSL/TLS taikomųjų programų sąrašu** galite tinkinti ESET Endpoint Security veikimą konkrečiose programose

Žinomų sertifikatų sąrašas leidžia tinkinti ESET Endpoint Security elgseną su konkrečiais SSL sertifikatais.

Pašalinti ryšius su patikimais domenais – kai įjungta, ryšiai su patikimais domenais nebus tikrinami. Domeno patikimumas nustatomas pagal integruotąjį baltąjį sąrašą.

Blokuoti šifruotąjį ryšį, naudojantį pasenusį protokolą SSL v2 – ryšys, naudojantis ankstesnę SSL protokolo versiją, bus automatiškai blokuojamas.

> Adresai nebus filtruojami, jei įjungtas nustatymas „**Exclude communication with trusted domains**“ (neįtraukti ryšių su patikimais domenais) ir domenas laikomas patikimu.

Šakninis sertifikatas

Šakninis sertifikatas – kad SSL ryšys veiktų tinkamai jūsų naršyklėse / el. pašto programose, svarbu, kad ESET šakninis sertifikatas būtų įtrauktas į žinomų šakninių sertifikatų (leidėjų) sąrašą. Parinktis **Įtraukti šakninį sertifikatą į žinomas naršykles** turi būti įjungta. Nurodykite šią parinktį, kad automatiškai įtrauktumėte ESET šakninį sertifikatą į žinomas naršykles (pavyzdžiui, „Opera“ ir „Firefox“). Naršyklėse, naudojančiose sistemos sertifikavimo saugyklą, sertifikatas yra pridedamas automatiškai (pvz., „Internet Explorer“).

Norėdami taikyti sertifikatą nepalaikomoms naršyklėms, spustelėkite **Peržiūrėti sertifikatą** > **Išsami informacija** > **Kopijuoti į failą** ir rankiniu būdu importuokite jį į naršyklę.

Sertifikato galiojimas

Veiksmai, jei sertifikato patikimumo negalima nustatyti – kai kuriais atvejais svetainės sertifikato negalima patikrinti naudojant patikimų šakninių sertifikavimo tarnybų (TRCA) saugyklą (pvz., nebegaliojantis sertifikatas, nepatikimas sertifikatas, sertifikatas negalioja konkrečiam domenui arba parašas, kurį galima išanalizuoti, bet sertifikatas nepasirašomas teisingai). Teisėtose svetainėse visada bus naudojami patikimi sertifikatai. Jei jie jo nepateikia, tai gali reikšti, kad atakuojanti programa iššifruoja jūsų ryšį arba svetainė patiria techninių sunkumų.

Jei punktas **Klausti apie sertifikato galiojimą** yra pažymėtas (pagal numatytąją parinktį), naudotojas raginamas pasirinkti, kokį veiksmą vykdyti, kai užmezgamas šifruotasis ryšys. Bus rodomas veiksmo pasirinkimo dialogas, kuriame galite nuspręsti pažymėti sertifikatą kaip patikimą arba neįtrauktą. Jeigu sertifikato nėra TRCA sąraše, langas yra raudonas. Jeigu sertifikatas yra TRCA sąraše, langas bus žalias.

Galite pasirinkti parinktį **Blokuoti sertifikatą naudojantį ryšį**, jeigu norite visada nutraukti šifruotąjį ryšį su svetaine, naudojančia nepatikimą sertifikatą.

Veiksmai dėl sugadintų sertifikatų – sugadintas sertifikatas reiškia, kad sertifikate naudojamas formatas, kurio neatpažino ESET Endpoint Security arba kuris buvo gautas sugadintas (pvz., perrašytas atsitiktiniais duomenimis). Tokiu atveju rekomenduojame palikti punktą **Blokuoti sertifikatą naudojantį ryšį** pažymėtą. Jei pažymėtas punktas **Klausti apie sertifikato galiojimą**, naudotojas raginamas pasirinkti, kokį veiksmą vykdyti, kai užmezgamas šifruotasis ryšys.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Sertifikatų pranešimai ESET produktuose
- „Šifruotas tinklo srautas: nepatikimas sertifikatas“ – Lankantis tinklalapiuose rodomas pranešimas

Sertifikatai

Kad SSL ryšys veiktų tinkamai jūsų naršyklėse / el. pašto programose, svarbu, kad ESET šakninis sertifikatas būtų įtrauktas į žinomų šakninių sertifikatų (leidėjų) sąrašą. Parinktis **Įtraukti šakninį sertifikatą į žinomas naršykles** turi būti įjungta. Pasirinkite šią parinktį, kad automatiškai įtrauktumėte ESET šakninį sertifikatą į žinomas naršykles (pavyzdžiui, „Opera“ ir „Firefox“). Naršyklėms, naudojančioms sistemos sertifikavimo saugyklą, sertifikatas yra pridedamas automatiškai (pvz., „Internet Explorer“). Norėdami taikyti sertifikatą nepalaikomoms naršyklėms, spustelėkite **Peržiūrėti sertifikatą** > **Išsami informacija** > **Kopijuoti į failą**, tada rankiniu būdu importuokite jį į naršyklę.

Kai kuriais atvejais sertifikato negalima patvirtinti naudojant patikimos šakninio sertifikavimo tarnybos saugyklą (pvz., „VeriSign“). Tai reiškia, kad sertifikatas yra kažkieno paties pasirašytas (pvz., žiniatinklio serverio arba mažos verslo įmonės administratoriaus) ir laikyti šį sertifikatą patikimu ne visada rizikinga. Daug didelių verslo įmonių (pavyzdžiui, bankai) naudoja TRCA pasirašytą sertifikatą. Jeigu parinktis **Klausti apie sertifikato galiojimą** yra pasirinkta (pasirinkta kaip numatytoji), vartotojas raginamas pasirinkti, kokį veiksmą vykdyti, kai užmezgamas šifruotasis ryšys. Bus rodomas veiksmo pasirinkimo dialogas, kuriame galite nuspręsti pažymėti sertifikatą kaip patikimą arba neįtrauktą. Jeigu sertifikato nėra TRCA sąraše, langas yra raudonas. Jeigu sertifikatas yra TRCA sąraše, langas bus žalias.

Galite pasirinkti parinktį **Blokuoti sertifikatą naudojantį ryšį**, jeigu norite visada nutraukti šifruotąjį ryšį su svetaine, naudojančia nepatikrintą sertifikatą.

Jeigu sertifikatas negaliojantis arba sugadintas, tai reiškia, kad sertifikato galiojimas baigėsi arba jis buvo neteisingai vartotojo pasirašytas. Šiuo atveju rekomenduojame blokuoti ryšį, naudojantį šį sertifikatą.

Šifruotas tinklo srautas

Jei jūsų sistema sukonfigūruota naudoti SSL protokolų nuskaitymo procedūrą, toliau nurodytais dviem atvejais pasirodys dialogo langas, raginantis pasirinkti veiksmą:

Pirmiausia, jei svetainėje naudojamas nepatikrinamas arba negaliojantis sertifikatas, o ESET Endpoint Security yra sukonfigūruotas tokiais atvejais klausti naudotojo (pagal numatytuosius parametrus atsakymas yra „Taip“ dėl nepatikrinamų sertifikatų ir „Ne“ dėl negaliojančių sertifikatų), dialogo lange jūsų bus paklausta, ar tokį ryšį **Leisti**, ar **Blokuoti**. Jei sertifikatas nerandamas Trusted Root Certification Authorities store (TRCA), jis laikomas nepatikimu.

Antra, jei **SSL protokolų filtravimo režimas** yra nustatytas kaip **Interaktyvusis režimas**, dialogo lange, pateikiamame prie kiekvienos svetainės, jūsų bus paklausta, ar srautą **Nuskaityti**, ar **Ignoruoti**. Kai kurios programos tikrina, ar jų SSL srautas nėra kieno nors modifikuotas ar tikrintas: tokiais atvejais ESET Endpoint Security turi **Ignoruoti** tą srautą, kad programa ir toliau veiktų normaliai.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Sertifikatų pranešimai ESET produktuose
- „Šifruotas tinklo srautas: nepatikimas sertifikatas“ – Lankantis tinklalapiuose rodomas pranešimas

Abiem atvejais vartotojas gali nurodyti įsiminti pasirinktą veiksmą. Įrašyti veiksmai yra laikomi Žinomų sertifikatų sąraše.

Žinomų sertifikatų sąrašas

Žinomų sertifikatų sąrašą galima naudoti norint pritaikyti ESET Endpoint Security veikimo būdą prie konkrečių SSL sertifikatų ir įsiminti veiksmus, pasirinktus, kai dalyje **SSL protokolų filtravimo režimas** pasirinkta **Interaktyvusis režimas**. Sąrašą galima peržiūrėti ir suredaguoti per **Išplėstinis nustatymai** (F5) > **Saitynas ir el. paštas** > **SSL/TLS** > **Žinomų sertifikatų sąrašas**.

Lango **Žinomų sertifikatų sąrašas** sudėtinės dalys:

Stulpeliai

Pavadinimas – sertifikato pavadinimas.

Sertifikato išdavėjas – sertifikato kūrėjo pavadinimas.

Sertifikato tema – temos laukas identifikuoja įmonę, susijusią su viešuoju raktu, laikomu temos viešojo rakto lauke.

Prieiga – kaip **Prieigos veiksmą** pasirinkite **Leisti arba Blokuoti**, kad leistumėte / užblokuotumėte šio sertifikato saugomą ryšį neatsižvelgiant į jo patikimumą. Pasirinkite **Automatinis**, kad leistumėte naudoti patikimus sertifikatus ir būtų klausiama dėl nepatikimų. Pasirinkite **Klausti**, kad vartotojo būtų visada klausiama, ką daryti.

Nuskaityti – kaip **Nuskaitymo veiksmą** pasirinkite **Nuskaityti** arba **Ignoruoti**, kad šiuo sertifikatu saugomą ryšį nuskaitytumėte arba ignoruotumėte. Pasirinkite **Automatinis**, kad būtų nuskaitoma automatiniu režimu ir būtų klausiama interaktyviuoju režimu. Pasirinkite **Klausti**, kad vartotojo būtų visada klausiama, ką daryti.

Valdymo elementai

Įtraukti – sertifikatą galima įkelti rankiniu būdu, kaip failą su plėtiniu *.cer*, *.crt* arba *.pem*. Spustelėkite **Failas**, kad įkeltumėte vietinį sertifikatą, arba spustelėkite **URL**, jei pageidaujate nurodyti sertifikato vietą internete.

Redaguoti – pasirinkite sertifikatą, kurį norite konfigūruoti, ir spustelėkite **Redaguoti**.

Naikinti – pasirinkite sertifikatą, kurį norite panaikinti, ir spustelėkite **Šalinti**.

Gerai / atšaukti – spustelėkite **Gerai**, jei norite įrašyti pakeitimus arba **Atšaukti**, jei norite išeiti neįrašę.

Filtruojamų SSL/TLS taikomųjų programų sąrašas

Naudodamiesi **Filtruojamų SSL/TLS taikomųjų programų sąrašu** galite tinkinti ESET Endpoint Security veikimą konkrečiose programose ir veiksmams įsiminti, jei **SSL/TLS protokolų filtravimo režimas** pasirenkate **Interaktyvusis režimas**. Sąrašą galite peržiūrėti ir redaguoti eidami į **Išplėstinis nustatymas** (F5) > **Saitynas ir el. paštas** > **SSL/TLS** > **Filtruojamų SSL/TLS programų sąrašas**.

Langą **SSL/TLS filtruojamų programų sąrašas** sudaro:

Stulpeliai

Programa – pasirinkite vykdomąjį failą iš katalogo medžio, spustelėkite parinktį **...** arba įveskite kelią rankiniu būdu.

Nuskaitymo veiksmas – pasirinkite **Nuskaityti** arba **Nepaisyti**. Pasirinkite **Automatinis**, kad būtų nuskaitoma automatiniu režimu ir būtų klausiama interaktyviuoju režimu. Pasirinkite **Klausti**, kad vartotojo būtų visada klausiama, ką daryti.

Valdymo elementai

Pridėti – pridėkite filtruojamą programą.

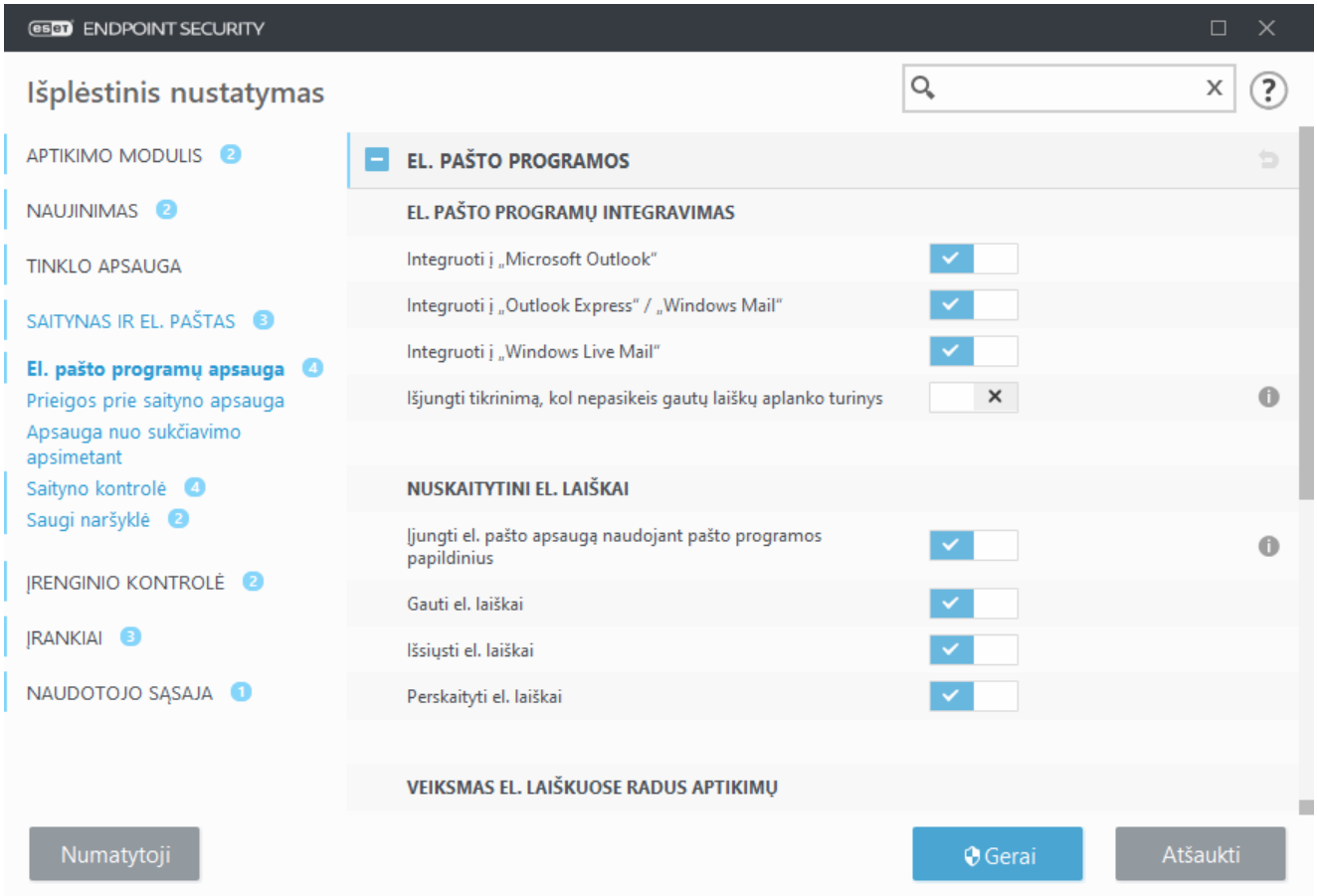
Redaguoti – pasirinkite sertifikatą, kurį norite konfigūruoti, ir spustelėkite **Redaguoti**.

Naikinti – pasirinkite sertifikatą, kurį norite panaikinti, ir spustelėkite **Šalinti**.

Gerai / atšaukti – spustelėkite **Gerai**, jei norite įrašyti pakeitimus, arba spustelėkite **Atšaukti**, jei norite išeiti neįrašydami.

El. pašto programų apsauga

ESET Endpoint Security Integravimas el. pašto programoje padidina aktyvios apsaugos nuo kenkimo kodų lygį el. laiškuose. Jeigu jūsų el. pašto programa yra palaikoma, integravimą galima įjungti programoje ESET Endpoint Security. Integravus į el. pašto programą ESET Endpoint Security įrankių juosta įterpiama tiesiai į šią programą, kad būtų efektyviau saugomas el. paštas. Integravimo parametrus rasite čia: **Išplėstinis nustatymai** (F5) > **Saitynas ir el. paštas** > **El. pašto programos apsauga** > **El. pašto programos**.



Nuskaitytini el. laiškai

Įjungti el. pašto apsaugą naudojant pašto programos papildinius – kai išjungta, apsauga naudojant el. pašto kliento papildinius yra išjungta.

Gauti el. laiškai – kai įjungta, tikrinami gauti el. laiškai.

Išsiųsti el. laiškai – kai įjungta, tikrinami išsiųsti el. laiškai.

Perskaityti el. laiškai – kai įjungta, tikrinami perskaityti el. laiškai.

> Rekomenduojame laikyti **Įjungti el. pašto apsaugą naudojant pašto programos papildinius** įjungtą.Net jei integracija neįjungta ar neveikia, el. pašto ryšį vis tiek saugo Protokolo filtravimas (IMAP/IMAPS ir POP3/POP3S).

Veiksmai radus užkrėstą el. laišką

Nieko nedaryti – jeigu įjungta, programa identifikuos užkrėstus priedus, tačiau paliks el. laiškus neatlikdama jokių veiksmų.

Naikinti el. laišką – programa praneš vartotojui apie įsiskverbimą (-us) ir panaikins laišką.

***Perkelti el. laiškus į panaikintų elementų aplanką** – užkrėsti el. laiškai bus automatiškai perkeliami į Panaikintų elementų aplanką.

Perkelti el. laiškus į aplanką (numatytasis veiksmas) – užkrėsti el. laiškai bus automatiškai perkeliami į nurodytą aplanką.

Aplankas – nurodykite pasirinktinį aplanką, į kurį pageidaujate perkelti aptiktus užkrėstus el. laiškus.

Kartoti nuskaitymą atlikus naujinimą – kai įjungta, užkrėsti el. laiškai pakartotinai nuskaitomi atlikus aptikimo modulio atnaujinimą.

Priimti nuskaitymo rezultatus iš kitų modulių – el. pašto apsaugos moduliui, užuot atlikus pakartotinį nuskaitymą, leidžiama naudoti nuskaitymo rezultatus iš kitų apsaugos modulių.

El. pašto protokolai

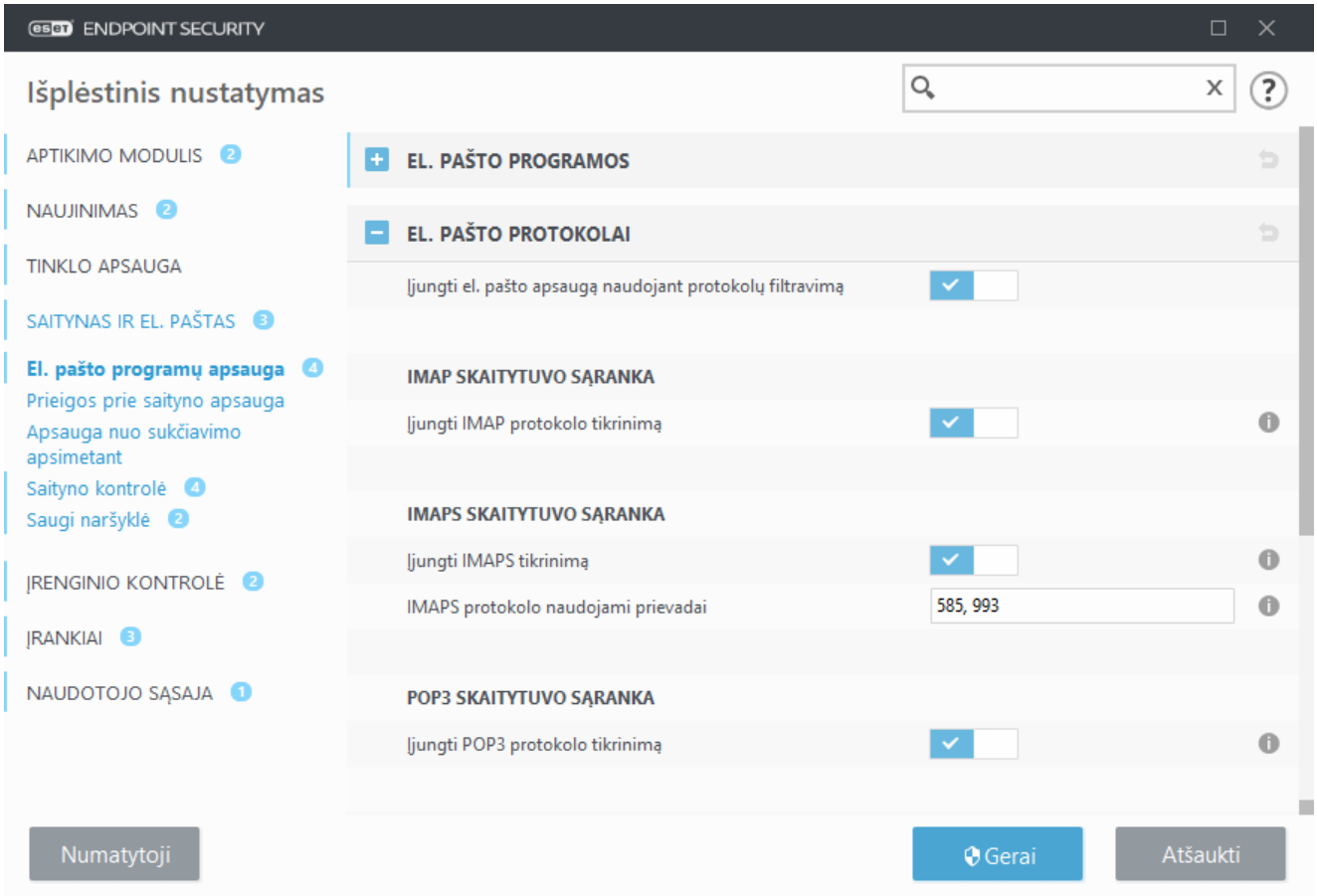
IMAP ir POP3 yra populiariausi protokolai, naudojami el. pašto ryšiams priimti el. pašto programoje. Interneto pranešimų prieigos protokolas (IMAP) yra dar vienas el. pašto interneto protokolas. IMAP turi kai kurių privalumų prieš POP3, pavyzdžiui, keletas klientų gali vienu metu prisijungti prie tos pačios pašto dėžutės ir tvarkyti laiško būsenos informaciją (pvz., ar pranešimas buvo perskaitytas, atsakytas arba panaikintas). Apsaugos modulis, atliekantis šią kontrolę, automatiškai inicijuojamas paleisties metu ir tada yra aktyvus atmintyje.

ESET Endpoint Security užtikrina šių protokolų apsaugą neatsižvelgiant į naudojamą el. pašto klientą ir nereikalaujant el. pašto kliento perkonfigūravimo. Pagal numatytuosius nustatymus, visas ryšys, einantis per POP3 ir IMAP protokolus, yra nuskenuojamas nepaisant numatytųjų POP3 / IMAP prievadų skaičių.
MAPI protokolas nenuskaitytas. Tačiau ryšį su Microsoft Exchange serveriu gali nuskaityti integracijos modulis el. pašto kliente, pavyzdžiui, „Microsoft Outlook“.

Rekomenduojame, kad parinktis **Įjungti el. pašto apsaugą naudojant protokolų filtravimą** būtų įjungta.Norėdami konfigūruoti IMAP/IMAPS ir POP3/POP3S protokolų tikrinimą, eikite į Išplėstinis nustatymai > **Saitynas ir el. paštas** > **El. pašto programų apsauga** > **El. pašto protokolai**.

ESET Endpoint Security papildomai dera su IMAPS (585, 993) ir POP3S (995) protokolų nuskaitymo funkcija. Šie protokolai informacijai tarp serverio ir kliento siųsti naudoja šifruotą kanalą. ESET Endpoint Security tikrina ryšius naudodama SSL (saugaus lizdo lygmens) ir TLS (transportavimo lygmens saugumo) protokolus. Programa nuskaito srautą tik per prievadus, kurie nustatyti parinktyje **IMAPS/POP3S protokolo naudojami prievadai**, nesvarbu, kokią operacinės sistemos versiją naudojate. Kitus ryšio prievadus galima pridėti, jei reikia. Kelių prievadų numerius reikia atskirti kableliais.

Šifruotas ryšys bus nuskaitytas pagal numatytuosius nustatymus. Norėdami peržiūrėti skaitytuvo nustatymus, išplėstinių nustatymų skyriuje eikite į SSL/TLS, spustelėkite **Saitynas ir el. paštas** > **SSL/TLS** ir įjunkite parinktį **Įjungti SSL/TLS protokolų filtravimą**.



El. laiškų žymos

Šios funkcijos parinktys pasiekiamos **Išplėstiniuose nustatymuose, per Saitynas ir el. paštas** > **El. pašto programos apsauga** > **Perspėjimai ir pranešimai**.

Patikrinus el. laišką, pranešimas su nuskaitymo rezultatais gali būti prijungiamas prie laiško. Galite nuspręsti **Prijungti gairės pranešimus prie gautų ir perskaitytų el. laiškų** arba **Prijungti gairės pranešimus prie išsiųstų el. laiškų**. Atminkite, kad retais atvejais gairių pranešimai probleminiuose HTML pranešimuose gali būti praleisti arba suklastoti kenkimo programinės įrangos. Gairės pranešimai gali būti pridėti prie gautų ir perskaitytų el. laiškų, prie išsiųstų el. laiškų arba prie abiejų. Galimos šios parinktys:

- **Niekada** – gairės pranešimai nebus pridedami.
- **Aptikus** – tik kenkėjiškas programas turintys laiškai bus pažymėti kaip patikrinti (numatytoji parinktis).
- **Visiems nuskaitytiems el. laiškams** – programa prijungs pranešimus prie visų nuskaitytų el. laiškų.

Naujinti išsiųsto el. laiško temą – išjunkite šią funkciją, jei nenorite, kad el. pašto apsauga įtrauktų įspėjimą apie virusus į užkrėsto el. laiško temą. Ši funkcija leidžia paprastai, pagal temą filtruoti užkrėstus el. laiškus (jeigu tai palaiko jūsų el. pašto programa). Be to, tai padidina patikimumo lygį gavėjui ir, jeigu aptinkamas įsiskverbimas, pateikiama vertinga informacija apie šio el. laiško ar siuntėjo grėsmės lygį.

Tekstas pridėtas prie užkrėsto el. laiško temos – redaguokite šį šabloną, jeigu norite pakeisti užkrėsto el. laiško temos prefikso formatą. Ši funkcija pakeis pranešimo temą „Sveiki“ tokiu formatu: „[aptikimas %APTIKIMO PAVADINIMAS%] Sveiki“. Kintamasis %DETECTIONNAME% nurodo aptikimą.

Integravimas su el. pašto programomis

Šiuo metu palaikomos el. pašto programos yra „Microsoft Outlook“, „Outlook Express“, „Windows Mail“ ir „Windows Live Mail“. El. pašto apsauga veikia kaip šių programų papildinys. Pagrindinis papildinio privalumas yra tas, kad jis nepriklauso nuo naudojamo protokolo. Kai el. pašto programa gauna šifruotą laišką, jis iššifruojamas ir siunčiamas į virusų skaitytuvą. Visą palaikomų el. pašto programų ir jų versijų sąrašą rasite šiame ESET žinių bazės straipsnyje.

Specialios nuostatos

Priedų tvarkymo optimizavimas – jei optimizavimas išjungtas, visi priedai nuskaitomi iš karto. Išjungus, el. pašto programa gali veikti lėčiau.

Išplėstinis el. pašto programų tvarkymas – jei dirbdami el. pašto programa pastebite, kad sistema sulėtėjo, išjunkite šią parinktį.

„Microsoft Outlook“ įrankių juosta

„Microsoft Outlook“ apsauga veikia kaip papildinio modulis. Įdiegus ESET Endpoint Security, ši įrankių juosta su antivirusinės programos/apsaugos nuo brukalo parinktimis įtraukiama į „Microsoft Outlook“:

Brukalas – pažymi pasirinktus laiškus kaip brukalą. Pažymėjus laiško „kontroliniai kodai“ siunčiami į centrinį serverį, kaupiantį brukalo kodus. Jeigu serveris gauna daugiau panašių „kontrolinių kodų“ iš keleto vartotojų, pranešimas ateityje bus klasifikuojamas kaip brukalas.

Ne brukalas – pažymi pasirinktus laiškus kaip ne brukalą.

Brukalo adresas (juodasis sąrašas, brukalo adresų sąrašas) – įtraukia naują siuntėjo adresą į juodąjį sąrašą. Visi laiškai, gauti iš šio sąrašo, bus automatiškai klasifikuojami kaip brukalas.

Saugokitės apsimetinėjimo – siuntėjo adreso klastojimo el. laiškuose, siekiant suklaidinti el. laiško gavėjus, kad jie perskaitytų laišką ir atsakytų į jį.

Patikimas adresas (baltasis sąrašas, patikimų adresų sąrašas) – įtraukia naują siuntėjo adresą į baltąjį sąrašą. Visi laiškai, gauti iš baltojo sąrašo adresų, niekada automatiškai nebus klasifikuojami kaip brukalas.

ESET Endpoint Security – spustelėjus piktogramą, atidaro ESET Endpoint Security pagrindinį programos langą.

Nuskaityti iš naujo laiškus – leidžia paleisti el. pašto tikrinimą rankiniu būdu. Galite nurodyti laiškus, kurie bus tikrinami, ir galite aktyvinti pakartotinį gautų el. laiškų nuskaitymą. Jeigu norite rasti daugiau informacijos, žiūrėkite El. pašto programos apsauga.

Skaitytuvo nustatymai – rodo el. pašto programos apsaugos nustatymų parinktis.

Apsaugos nuo brukalo nustatymai – rodo apsaugos nuo brukalo nustatymo parinktis.

Adresų knygos – atidaro apsaugos nuo brukalo langą, kuriame galite rasti neįtrauktų, patikimų ir brukalo adresų sąrašus.

„Outlook Express“ ir „Windows Mail“ įrankių juosta

Apsauga programose „Outlook Express“ ir „Windows Mail“ veikia kaip papildinio modulis. Įdiegus ESET Endpoint Security, ši įrankių juosta su antivirusinės programos/apsaugos nuo brukalo parinktimis yra įtraukiama į „Outlook Express“ arba „Windows Mail“:

Brukalas – pažymi pasirinktus laiškus kaip brukalą. Pažymėjus laiško „kontroliniai kodai“ siunčiami į centrinį serverį, kaupiantį brukalo kodus. Jeigu serveris gauna daugiau panašių „kontrolinių kodų“ iš keleto vartotojų, pranešimas ateityje bus klasifikuojamas kaip brukalas.

Ne brukalas – pažymi pasirinktus laiškus kaip ne brukalą.

Brukalo adresas – įtraukia naują siuntėjo adresą į juodąjį sąrašą. Visi laiškai, gauti iš šio sąrašo, bus automatiškai klasifikuojami kaip brukalas.

Saugokitės apsimetinėjimo – siuntėjo adreso klastojimo el. laiškuose, siekiant suklaidinti el. laiško gavėjus, kad jie perskaitytų laišką ir atsakytų į jį.

Patikimas adresas – įtraukia naują siuntėjo adresą į baltąjį sąrašą. Visi laiškai, gauti iš baltojo sąrašo adresų, niekada automatiškai nebus klasifikuojami kaip brukalas.

ESET Endpoint Security – spustelėjus piktogramą, atidaro ESET Endpoint Security pagrindinį programos langą.

Nuskaityti iš naujo laiškus – leidžia paleisti el. pašto tikrinimą rankiniu būdu. Galite nurodyti laiškus, kurie bus tikrinami, ir galite aktyvinti pakartotinį gautų el. laiškų nuskaitymą. Jeigu norite rasti daugiau informacijos, žiūrėkite El. pašto programos apsauga.

Skaitytuvo nustatymai – rodo el. pašto programos apsaugos nustatymų parinktis.

Apsaugos nuo brukalo nustatymai – rodo apsaugos nuo brukalo nustatymo parinktis.

Vartotojo sąsaja

Tinkinti išvaizdą – įrankių juostos išvaizdą jūsų el. pašto programoje galima keisti. Atsisakykite parinkties, jei norite tinkinti išvaizdą neatsižvelgdami į el. pašto programos parametrus.

Rodyti tekstą – rodo piktogramų aprašus.

Tekstas į dešinę – parinkčių aprašai perkeliami iš apačios į piktogramos dešinę.

Didelės piktogramos – rodo dideles meniu parinkčių piktogramas.

Patvirtinimo dialogas

Šis pranešimas leidžia įsitikinti, kad vartotojas tikrai nori atlikti pasirinktą veiksmą. Tai padeda išvengti galimų klaidų.

Kita vertus, dialogas siūlo galimybę atsisakyti patvirtinimų.

Nuskaityti iš naujo laiškus

ESET Endpoint Security įrankių juosta, integruota į el. pašto programas, leidžia vartotojams nurodyti keletą el. laiškų tikrinimo parinkčių. Parinktis **Nuskaityti iš naujo laiškus** siūlo du nuskaitymo režimus:

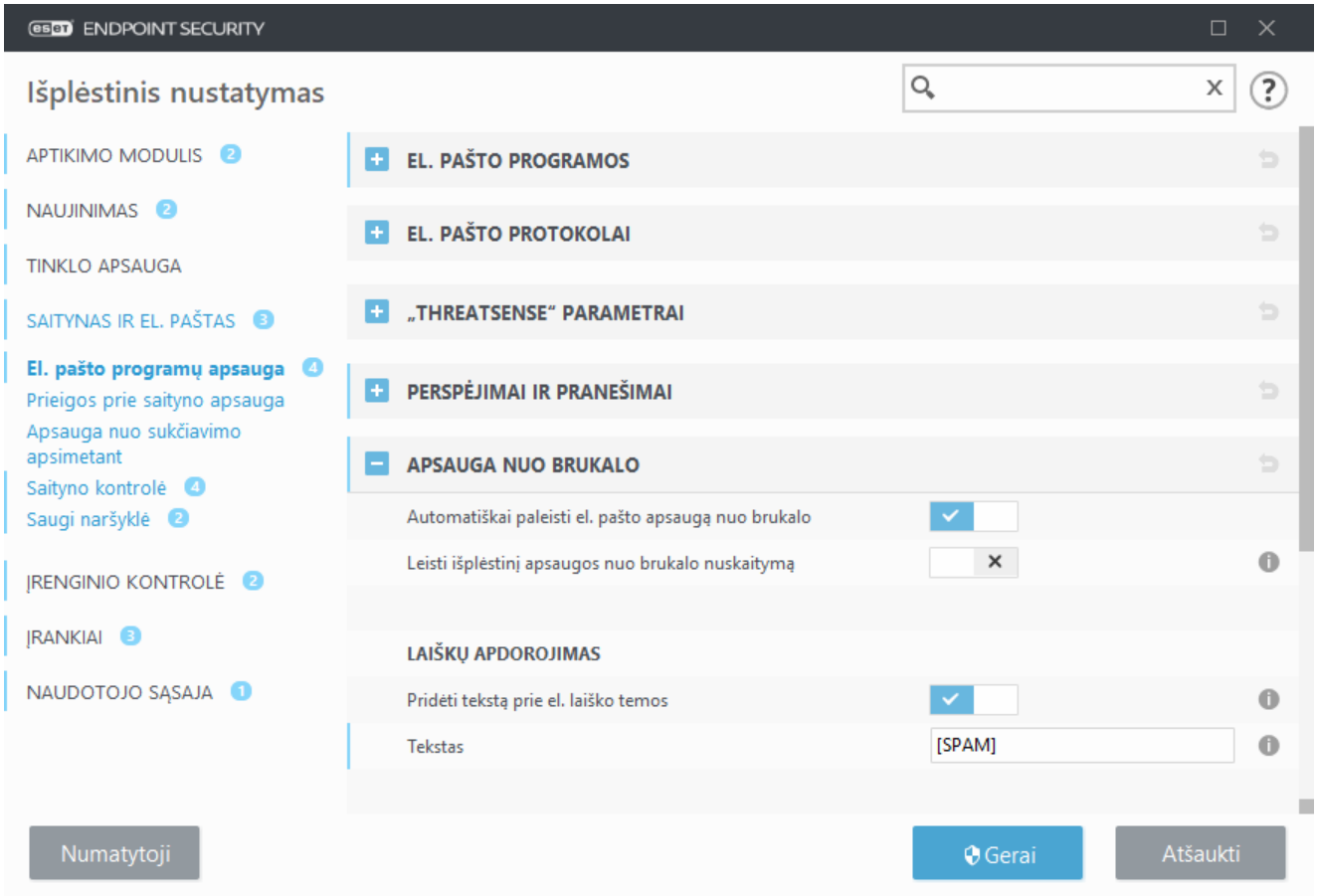
Visus laiškus esamame aplanke – nuskaito laiškus šiuo metu rodomame aplanke.

Tik pasirinktus laiškus – nuskaito tik vartotojo pažymėtus laiškus.

Žymės langelis **Nuskaityti iš naujo jau nuskaitytus laiškus** suteikia vartotojui galimybę paleisti dar kartą nuskaityti laiškus, kurie buvo nuskaityti anksčiau.

Apsauga nuo brukalo

Nepageidaujami el. laiškai, vadinami brukalu, patenka į didžiausių elektroninio ryšio problemų kategoriją. Brukalas užima iki 50 procentų visų el. pašto ryšių. Apsauga nuo brukalo yra skirta apsaugoti nuo šios problemos. Suderindamas keletą el. pašto saugos principų, apsaugos nuo brukalo modulis užtikrina puikų filtravimą, kad jūsų pašto dėžutė išliktų švari.



Vienas svarbus principas aptinkant brukalą yra galimybė atpažinti nepageidaujamą el. paštą remiantis iš anksto nustatytais patikimais adresais (baltasis sąrašas) ir brukalo adresais (juodasis sąrašas). Visi adresai iš jūsų kontaktų sąrašo automatiškai įtraukiami į baltąjį sąrašą kaip ir visi kiti adresai, kuriuos pažymite kaip saugius.

Pagrindinis metodas, naudojamas brukalui aptikti, yra el. laiškų ypatybių nuskaitymas. Gauti laiškai yra nuskaitomi remiantis pagrindiniais apsaugos nuo brukalo kriterijais (laiško apibrėžtys, statistinė euristika, atpažinimo algoritmai ir kiti unikalūs metodai) ir gauta indekso reikšmė nusako, ar laiškas yra brukalas, ar ne.

Pradėti el. pašto programos apsaugą nuo brukalo automatiškai – įjungus apsaugą nuo brukalo bus automatiškai aktyvinama paleidžiant sistemą.

Leisti išplėstinį apsaugos nuo brukalo nuskaitymą – bus periodiškai atsisiunčiami papildomi apsaugos nuo brukalo duomenys, padidinantys apsaugos nuo brukalo galimybes ir užtikrinantys geresnius rezultatus.

ESET Endpoint Security apsauga nuo brukalo leidžia nustatyti įvairius parametrus darbui su pašto sąrašais. Yra šios parinktys:

Laiškų apdorojimas

Pridėti tekstą prie el. pašto temos – leidžia įtraukti pasirinktinę prefikso eilutę į laiško, kuris buvo klasifikuotas kaip brukalas, temos eilutę. Numatytoji reikšmė yra „[SPAM]“ (brukalas).

Perkelti laiškus į brukalo aplanką – įjungus brukalo laiškai bus perkeliami į numatytąjį nepageidaujamų el. laiškų aplanką, laiškai identifikuoti kaip ne brukalas bus perkelti į gautų laiškų aplanką. Dešiniuoju pelės klavišu spustelėdami el. laišką ir kontekstiniame meniu pasirinkdami ESET Endpoint Security galite pasirinkti taikytinas parinktis.

Naudoti aplanką – nurodykite pasirinktinį aplanką, į kurį pageidaujate perkelti aptiktus užkrėstus el. laiškus.

Pažymėti brukalo laiškus kaip perskaitytus – įjunkite šią parinktį, jeigu norite automatiškai pažymėti brukalą kaip perskaitytą. Tai padės patogiau atkreipti dėmesį į „švarius“ laiškus.

Pažymėti perklasifikuotus pranešimus kaip neskaitytus – laiškai, kurie iš pradžių buvo klasifikuoti kaip brukalas, tačiau vėliau pažymėti kaip „švarūs“, bus rodomi kaip neskaityti.

Brukalo rezultatų registravimas – ESET Endpoint Security apsaugos nuo brukalo modulis priskiria brukalo tikimybę kiekvienam nuskaitytam laiškui. Laiškas bus įrašytas į apsaugos nuo brukalo žurnalą (**ESET Endpoint Security** > **Įrankiai** > **Žurnalo failai** > **Apsauga nuo brukalo**).

- **Nėra** – apsaugos nuo brukalo nuskaitymo nustatytas tikimybės lygis nėra registruojamas.
- **Perskirstyta ir pažymėta kaip brukalas** – pasirinkite šią parinktį, jei norite užregistruoti laiškų, pažymėtų kaip BRUKALAS, brukalo tikimybės lygį.
- **Viskas** – visi laiškai bus įrašyti į žurnalą nurodant brukalo tikimybės lygį.

Nepageidaujamų laiškų aplanke spustelėję laišką galite pasirinkti **Perskirstyti pasirinktus laiškus ir nepriskirti brukalui**, kad laiškas būtų perkeltas į gautų laiškų aplanką. Gautų laiškų aplanke spustelėję laišką, kurį laikote brukalu, pasirinkite **Perskirstyti laiškus ir priskirti brukalui**, kad laiškas būtų perkeltas į nepageidaujamų laiškų aplanką. Galite pasirinkti kelis laiškus, kad vienu metu su jais visais atliktumėte tą patį veiksmą.

ESET Endpoint Security palaiko apsaugą nuo brukalo programose „Microsoft Outlook“, „Outlook Express“, „Windows Mail“ ir „Windows Live Mail“.

Apsaugos nuo brukalo adresų knygelės

Apsaugos nuo brukalo funkcija programoje ESET Endpoint Security leidžia konfigūruoti įvairius adresų sąrašų parametrus.

Adresų knygos

Leisti vartotojo adresų sąrašą – įjunkite šią parinktį norėdami aktyvinti vartotojo sukurtą adresų knygą jo paties el. pašto programoje.

Leisti visuotinius adresų sąrašus – įjunkite šią parinktį norėdami aktyvinti visuotinės adresų knygos bendrinimą visiems darbo vietos naudotojams, el. pašto sistemos katalogų paslaugą. Global Address List) pateikiama informacija, skirta visiems el. pašto vartotojams, paskirstymo grupėms ir ištekliams.

Vartotojo baltasis sąrašas – adresatų sąrašas, kuriame galima pridėti, redaguoti arba panaikinti saugiais laikomus adresus, iš kurių vartotojas pageidauja gauti laiškus.

Vartotojo juodasis sąrašas – adresatų sąrašas, kuriame galima pridėti, redaguoti arba panaikinti nesaugiais laikomus adresus, iš kurių vartotojas nepageidauja gauti laiškų.

Vartotojo išimčių sąrašas – šiame adresatų sąraše paprastai būna galimai apgaulingi el. pašto adresai, iš kurių siunčiamas brukalas. Taip pat žr. Išimčių sąrašas.

Visuotinis baltasis sąrašas / juodasis sąrašas / išimčių sąrašas – šie sąrašai naudojami visuotinėms apsaugos nuo brukalo politikoms taikyti visiems naudotojams, kurie naudojasi ESET Endpoint Security šioje darbo vietoje. Kai ESET Endpoint Security valdomas nuotoliniu būdu, ESET PROTECT / ECA politika bus taikoma visoms priskirtoms darbo vietoms.

Automatiškai įtraukti į vartotojo baltąjį sąrašą

Pridėti adresus iš adresų knygos – pridėkite adresus iš savo adresatų sąrašo prie Baltojo sąrašo.

Pridėti siunčiamų laiškų gavėjų adresus – pridėkite išsiųstų laiškų gavėjų adresus prie baltojo sąrašo.

Pridėti adresus iš laiškų, kurie buvo perklasifikuoti kaip NE brukalas – pridėkite prie baltojo sąrašo siuntėjų adresus iš laiškų, kurie buvo perklasifikuoti kaip NE brukalas.

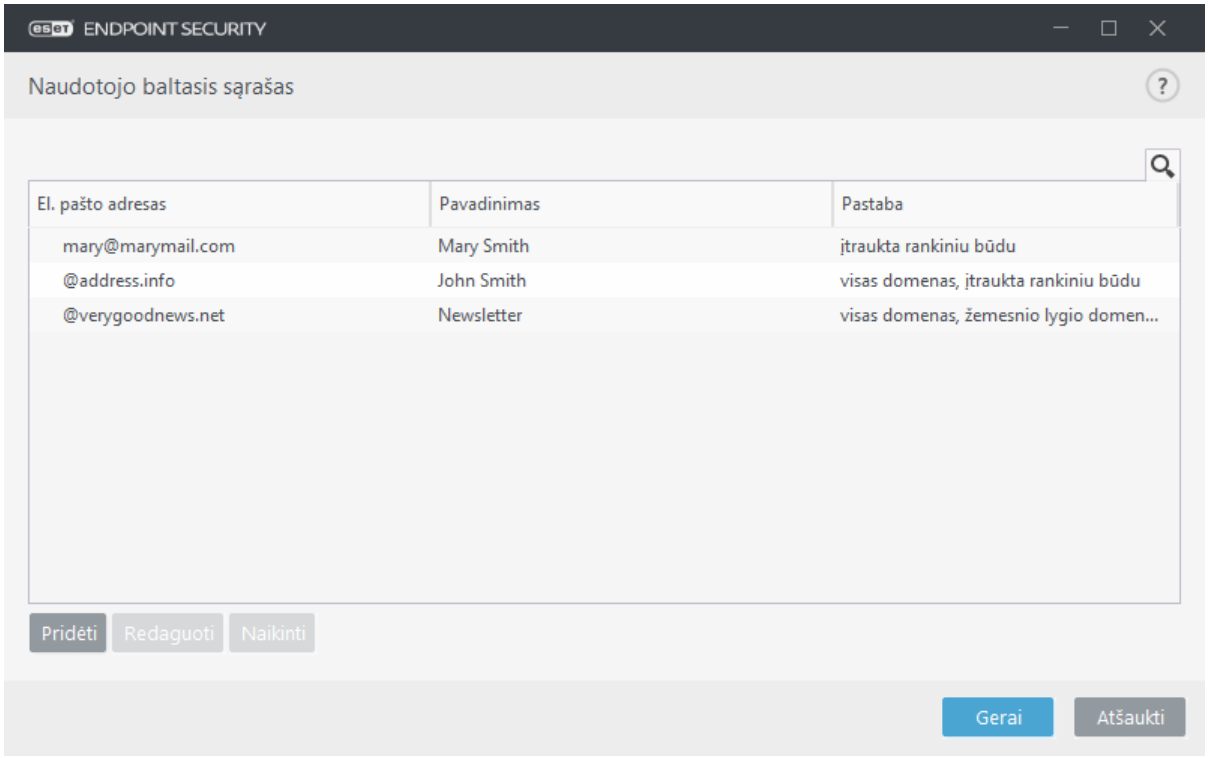
Įtraukti į vartotojo išimčių sąrašą automatiškai

Pridėti adresus iš savo paskyrų – pridėkite prie Išimčių sąrašo savo adresus iš esamų el. pašto programos paskyrų.

Juodasis sąrašas / baltasis sąrašas / išimčių sąrašas

Kad užtikrintų apsaugą nuo nepageidaujamų el. laiškų, ESET Endpoint Security leidžia klasifikuoti el. pašto adresus specializuotuose sąrašuose. Baltajame sąraše yra el. pašto adresai, kurie laikomi saugiais. Laiškai iš vartotojų, esančių Baltajame sąraše, visada patenka į gaunamų laiškų aplanką. Juodajame sąraše yra el. laiškų, kurie klasifikuojami kaip brukalas, adresai ir visi laiškai iš juodajame sąraše esančių siuntėjų yra atitinkamai pažymimi. Išimčių sąraše yra el. pašto adresai, kurie visada tikrinami, ar nesiunčiamas brukalas, tačiau čia gali būti ir nepageidaujamų el. laiškų, kurių iš pradžių nepavyko identifikuoti kaip brukalo, adresų.

Visus sąrašus galima redaguoti iš ESET Endpoint Security pagrindinio programos lango, pasirenkant **Išplėstiniai nustatymai** > **Saitynas ir el. paštas** > **El. pašto programos apsauga** > **Apsaugos nuo brukalo adresų knygelės** ir pasinaudojant mygtukais **„Pridėti“**, **„Redaguoti“** bei **„Šalinti“**, esančiais kiekvieno sąrašo dialogo lange, arba per **Nustatymai** > **Saitynas ir el. paštas**, pirma spustelėjus krumpliaračio piktogramą šalia **Apsauga nuo brukalo**.



Pagal numatytuosius nustatymus ESET Endpoint Security įtraukia visus adresus iš palaikomos el. pašto programos adresų knygos į baltąjį sąrašą. Juodasis sąrašas pagal numatytuosius nustatymus yra tuščias. Išimčių sąraše pagal numatytuosius nustatymus yra tik paties vartotojo el. pašto adresai.

Juodojo sąrašo / baltojo sąrašo / išimčių adresų pridėjimas

Šiame lange galima pridėti arba redaguoti įrašus baltajame arba juodajame sąraše. Atidarykite ESET Endpoint Security pagrindinį programos langą dalyje **Išplėstinis nustatymas** > **Saitynas ir el. paštas** > **El. pašto programų apsauga** > **Apsaugos nuo brukalo adresų knygelės**.

El. pašto adresas – pridėti ar redaguoti skirtas el. pašto adresas.

Pavadinimas – įrašo pavadinimas.

Visas domenas – pasirinkite šią parinktį, kad įrašas būtų taikomas visam kontakto domenui (ne tik adresams, nurodytiems El. pašto adresų lauke, bet ir visiems el. pašto adresams domene *address.info*).

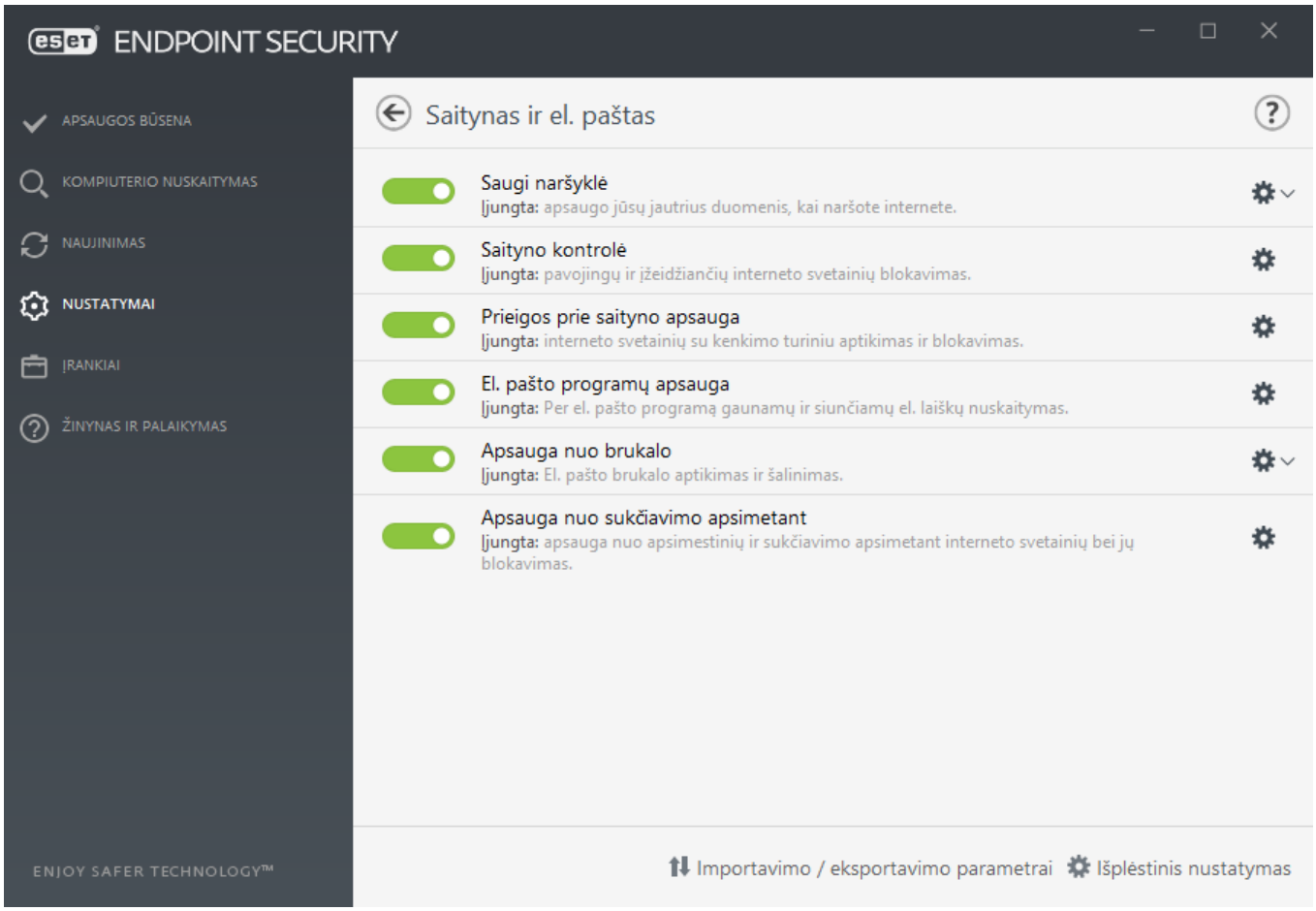
Žemesnio lygio domenai – pasirinkite šią parinktį, kad įrašas būtų taikomas kontakto žemesnio lygio domenams (*address.info* nurodo domeną, o *my.address.info* – padomenį).

Prieigos prie saityno apsauga

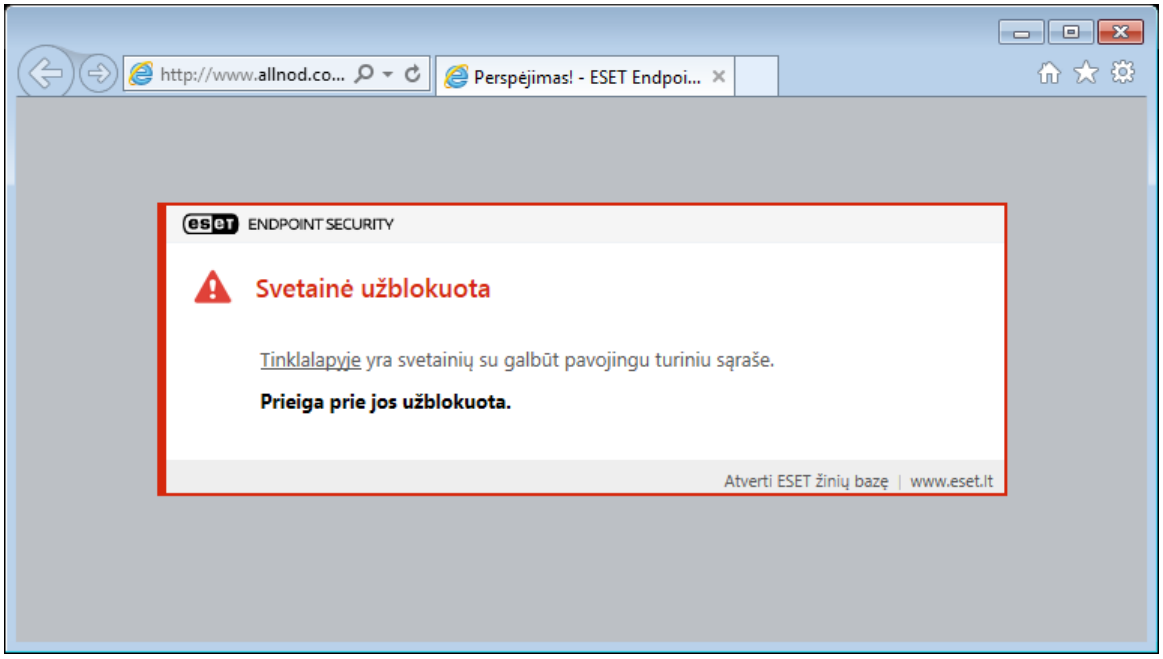
Galimybė jungtis prie interneto yra standartinė asmeninio kompiuterio funkcija. Deja, internetas taip pat tapo pagrindine kenkėjiško kodo persiuntimo terpe. Prieigos prie saityno apsauga veikia stebėdama ryšį tarp interneto naršyklės ir nuotolinių serverių ir vykdo HTTP (hiperteksto perdavimo protokolas) bei HTTPS (šifruotasis ryšys) taisykles.

Prieiga prie tinklalapių, kuriuose, mūsų žiniomis, yra kenkimo turinio, yra užblokuojama prieš tokį turinį atsisiunčiant. Visus kitus tinklalapius nuskaito atitinkamas nuskaitymo modulis „ThreatSense“, kai jie yra įkeliami. Jei aptinkama kenkimo turinio, tokie tinklalapiai užblokuojami. Prieigos prie saityno apsauga siūlo du apsaugos lygius: blokavimo naudojant juodąjį sąrašą ir blokavimo pagal turinį.

Mes primygtinai rekomenduojame, kad prieigos prie saityno apsauga būtų įjungta. Šią parinktį galima pasirinkti iš pagrindinio ESET Endpoint Security lango einant į **Nustatymai** > **Interneto apsauga** > **Prieigos prie saityno apsauga**.



Prieigos prie saityno apsauga naršyklėje rodys toliau nurodytą pranešimą, kai svetainė užblokuota:

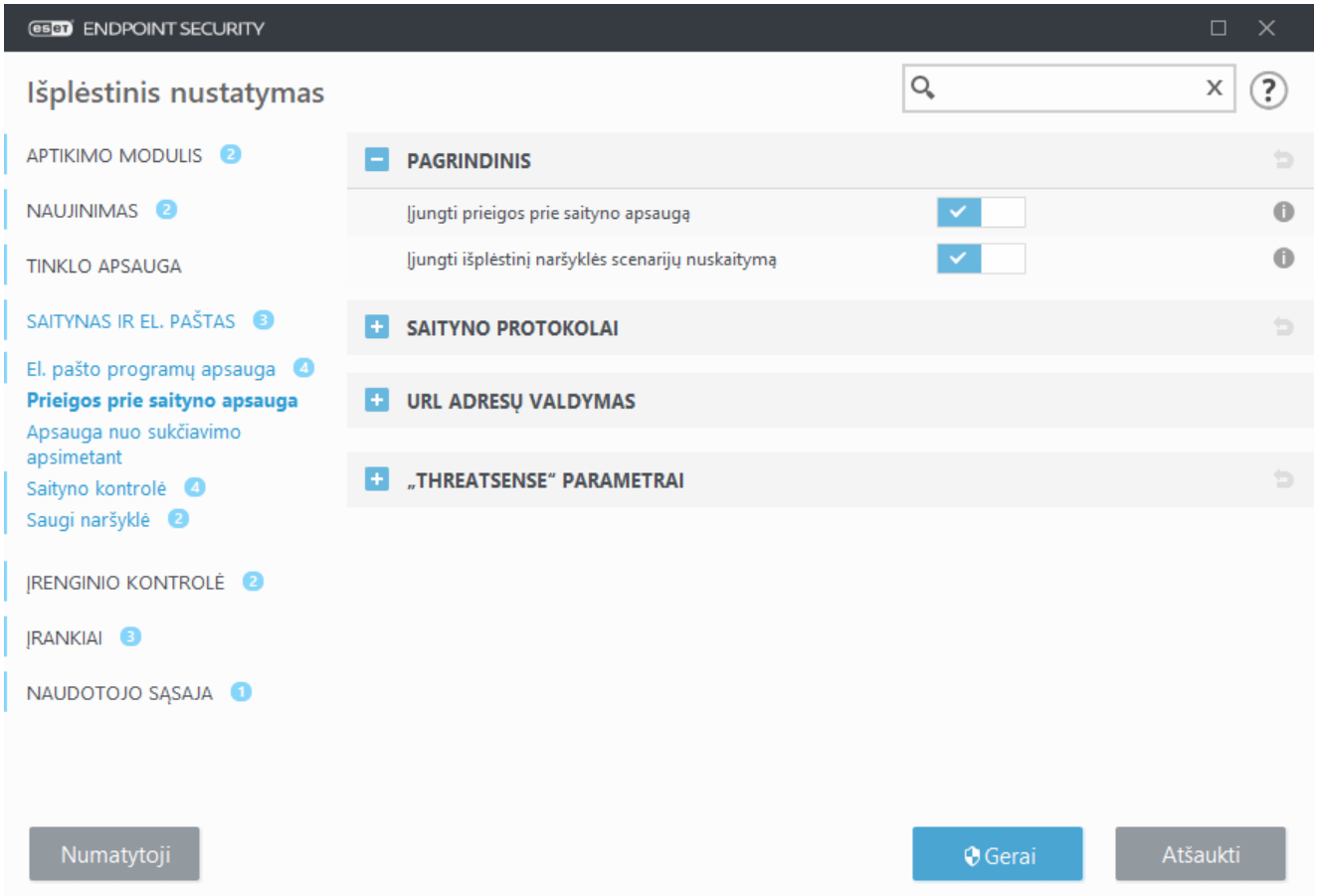


Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Atblokuokite saugią svetainę atskiroje darbo vietoje ESET Endpoint Security

---

Per **Išplėstiniai nustatymai** (F5) > **Saitynas ir el. paštas** > **Prieigos prie saityno apsauga** pasiekiamos tokios parinktys:

- **Bazinis** – šios funkcijos įjungimas arba išjungimas išplėstiniuose nustatymuose.
- **Saityno protokolai** – leidžia sukonfigūruoti šių standartinių protokolų, kuriuos naudoja daugelis interneto naršyklių, stebėjimo procedūras.
- **URL adresų valdymas** – leidžia nurodyti, kuriuos URL adresus blokuoti, leisti arba kurių netikrinti.
- **„ThreatSense“ parametrai** – išplėstinis virusų nuskaitymo programos nustatymas – leidžia sukonfigūruoti parametrus, pvz., nuskaitytinus objektų tipus (el. laiškus, archyvus ir pan.), prieigos prie saityno apsaugos aptikimo metodus ir pan.



Prieigos prie saityno apsaugos išplėstinis nustatymas

Per **Išplėstiniai nustatymai** (F5) > **Saitynas ir el. paštas** > **Prieigos prie saityno apsauga** > **Bazinis** pasiekiamos tokios parinktys:

Įjungti prieigos prie saityno apsaugą – kai ši parinktis išjungta, prieigos prie saityno apsauga ir apsauga nuo sukčiavimo apsimetant nebus paleista.

Įjungti išplėstinį naršyklės scenarijų nuskaitymą – kai ši parinktis įjungta, visos „JavaScript“ programos, kurias paleidžia interneto naršyklės, bus tikrinamos aptikimo moduliu.

Mes primygtinai rekomenduojame, kad prieigos prie saityno apsauga būtų palikta įjungta.

Saityno protokolai

Pagal numatytąją parinktį ESET Endpoint Security yra sukonfigūruota stebėti HTTP protokolą, kurį naudoja daugelis interneto naršyklių.

HTTP nuskaitymo programos nustatymai

HTTP srautas, siunčiamas per visus prievadus, yra visada stebimas.

HTTPS nuskaitymo programos nustatymai

ESET Endpoint Security taip pat palaiko HTTPS protokolo tikrinimą. HTTPS ryšys naudoja šifruotą kanalą informacijai tarp serverio ir kliento siųsti. ESET Endpoint Security tikrina ryšius naudodama SSL (saugaus lizdo lygmens) ir TLS (transportavimo lygmens saugos) protokolus. Programa nuskaito srautą tik per prievadus (443, 0-65535), kurie nustatyti parinktyje **HTTPS protokolo naudojami prievadai**, nesvarbu, kokią operacinės sistemos versiją naudojate.

Šifruotas ryšys bus nuskaitytas pagal numatytuosius nustatymus. Norėdami peržiūrėti skaitytuvo nustatymus, išplėstinių nustatymų skyriuje eikite į SSL/TLS, spustelėkite **Saitynas ir el. paštas** > **SSL/TLS** ir įjunkite parinktį **Įjungti SSL/TLS protokolų filtravimą**.

URL adresų valdymas

URL adresų valdymo skyrius leidžia nurodyti, kuriuos HTTP adresus blokuoti, leisti arba kurių neįtraukti į turinio nuskaitymą.

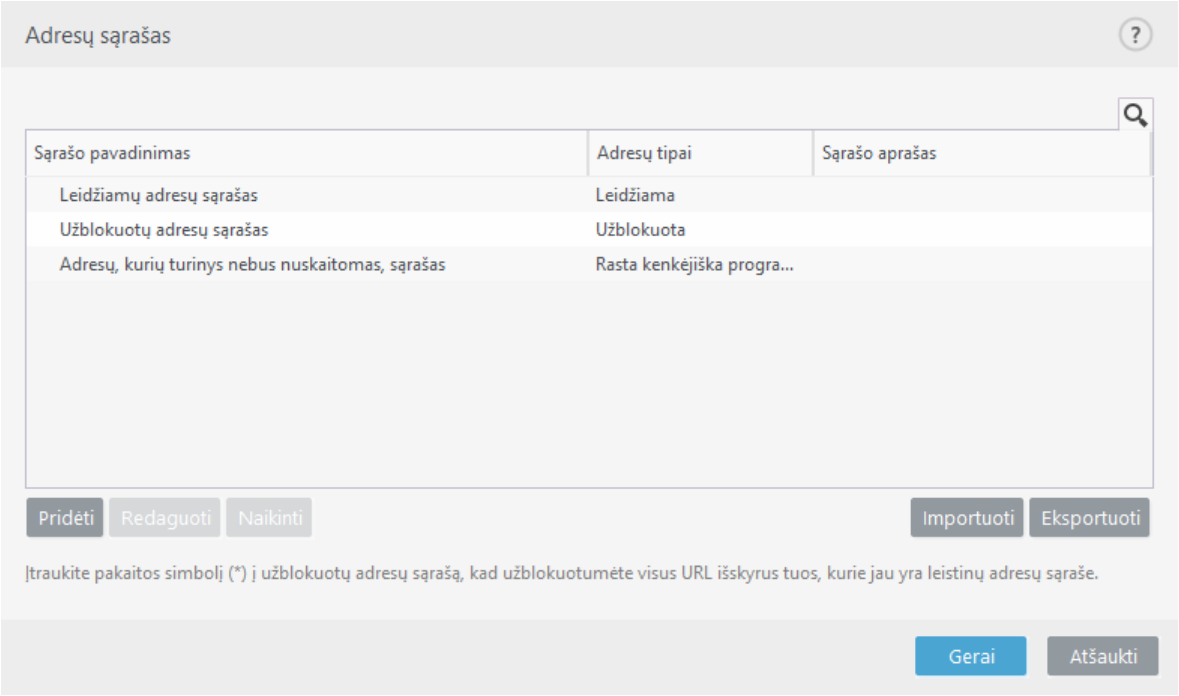
Įjungti SSL/TLS protokolo filtravimą būtina įjungti, jei norite filtruoti HTTPS adresus kartu su HTTP svetainėmis. Kitaip bus pridėti tik jūsų aplankytų HTTPS svetainių domenai, o visas URL – ne.

Blokuojamų adresų sąrašas nebus pasiekiamas svetainėse, jei jos bus įtrauktos ir į **Leidžiamų adresų sąrašą**. **Adresų, kurie nebus įtraukiami į turinio tikrinimą, sąrašas** nėra nuskaitomas ieškant kenkėjiško kodo.

Jei norite užblokuoti visus HTTP adresus, išskyrus esančius aktyviame **Leidžiamųjų adresų sąraše**, pridėkite * prie aktyvaus **Blokuojamųjų adresų sąrašo**.

Sąrašuose galima naudoti specialiuosius simbolius „*“ (žvaigždutes) ir „?“ (klaustukus). Žvaigždutė pakeičia bet kokią simbolių eilutę, o klaustukas – bet kokį simbolį. Reikia būti itin atidiems nurodant neįtrauktus adresus, nes šiame sąraše turi būti tik patikimi ir saugūs adresai. Be to, būtina užtikrinti, kad šiame sąraše būtų tinkamai naudojami simboliai „*“ ir „?“. Žr. Pridėti HTTP adresą / domeno kaukę, kur aprašoma, kaip gali būti saugiai sutapdintas visas domenas su visais padomeniais. Jei norite suaktyvinti sąrašą, pasirinkite **Sąrašas aktyvus**. Jei norite gauti pranešimą, kai patenkate į adresą iš esamo sąrašo, pasirinkite **Pranešti, kai naudojama**.

> Adresai nebus filtruojami, jei įjungtas nustatymai **Saitynas ir el. paštas** > **SSL/TLS** > **Neįtraukti ryšių su patikimais domenais** ir domenas laikomas patikimu.



Valdymo elementai

Pridėti – šalia iš anksto apibrėžtų sukuria naują sąrašą. Tai gali būti naudinga, jei norite logiškai išskaidyti atskiras adresų grupes. Pavyzdžiui, viename blokuojamųjų adresų sąraše gali būti adresai iš tam tikro išorinio viešo juodojo sąrašo, o kitame – jūsų sudarytas juodasis sąrašas: taip bus lengviau atnaujinti išorinį sąrašą išlaikant savąjį nepakeistą.

Redaguoti – modifikuoja esamus sąrašus. Šią parinktį galite naudoti norėdami įtraukti adresų arba jų pašalinti.

Naikinti – panaikinami esami sąrašai. Galima naudoti tik sąrašuose, sukurtuose naudojant parinktį **Pridėti**, bet ne su numatytaisiais sąrašais.

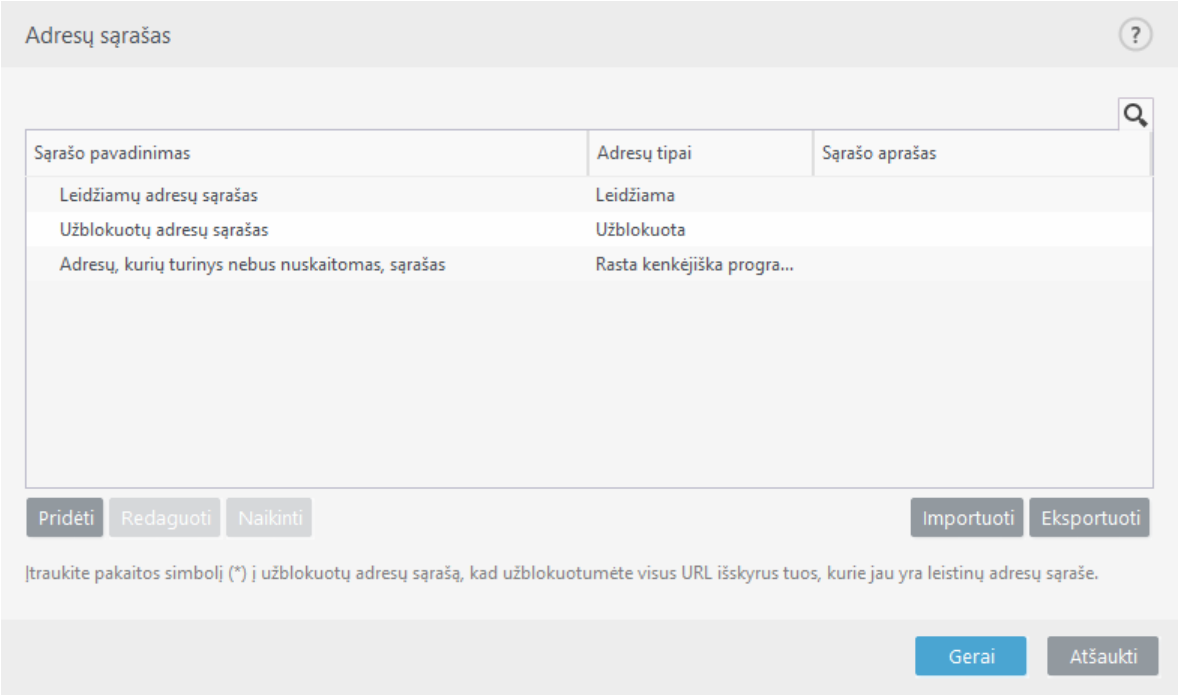
URL adresų sąrašas

Šiame skyriuje galite sudaryti sąrašus iš HTTP adresų, kurie bus blokuojami, leidžiami arba netikrinami.

Pagal numatytuosius nustatymus galimi trys sąrašai:

- **Adresų, kurių turinys nebus tikrinamas, sąrašas** – jokie į šį sąrašą įtraukti adresai nebus tikrinami ieškant kenkėjiško kodo.
- **Leidžiamų adresų sąrašas** – jei įjungta parinktis Leisti prieigą tik prie leidžiamų adresų sąraše nurodytų HTTP adresų, o blokuojamų adresų sąraše yra „*“ (tinka viskas), vartotojui bus suteikta prieiga tik prie šiame sąraše nurodytų adresų. Šiame sąraše adresai yra leidžiami, net jei jie įtraukti į blokuojamų adresų sąrašą.
- **Užblokuotų adresų sąrašas** – vartotojui nebus leidžiama prieiga prie adresų, nurodytų šiame sąraše, nebent šie adresai yra įtraukti ir į leidžiamų adresų sąrašą.

Spustelėkite **Pridėti**, norėdami sukurti naują sąrašą. Norėdami panaikinti pasirinktus sąrašus, spustelėkite **Šalinti**.



Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Atblokuokite saugią svetainę atskiroje darbo vietoje ESET Endpoint Security

Daugiau informacijos žr. URL adresų valdymas.

Kurti naują sąrašą

Šis dialogo langas leidžia konfigūruoti naują URL adresų / kaukių, kurie bus blokuojami, leidžiami arba neįtraukti į tikrinimą, sąrašą.

Galite konfigūruoti šias parinktis:

Adresų sąrašo tipas – galimi trys sąrašo tipai:

- **Rasta kenkėjiška programinė įranga ignoruojama** – ieškant kenkėjiško kodo jokie į šį sąrašą įtraukti adresai nebus tikrinami.
- **Blokuojama** - prieiga prie šiame sąraše nurodytų adresų bus blokuojama.
- **Leidžiama** – bus leidžiama pasiekti šiame sąraše nurodytus adresus. Šiame sąraše nurodyti adresai yra leidžiami, net jei sutampa su blokuojamų adresų sąraše esančiais adresais.

Sąrašo pavadinimas – nurodykite sąrašo pavadinimą. Šis laukas bus nepasiekiamas redaguojant vieną iš sąrašų, nustatytų iš anksto.

Sąrašo aprašas – įveskite trumpą sąrašo aprašymą (nebūtina). Nepasiekiama redaguojant vieną iš sąrašų, nustatytų iš anksto.

Norint suaktyvinti sąrašą, reikia pasirinkti punktą **Sąrašas aktyvus**, esantį šalia to sąrašo. Jei norite, kad jums būtų pranešta, kai prisijungiant prie svetainių naudojamas konkretus sąrašas, pasirinkite **Pranešti, kai teikiama paraiška**. Pavyzdžiui, jei interneto svetainė yra blokuojama arba leidžiama, nes yra įtraukta į blokuojamų arba leidžiamų adresų sąrašą, gausite pranešimą. Pranešime bus pateiktas pavadinimas sąrašo.

Registravimo svarba – išskleidžiamajame meniu pasirinkite registravimo svarbą. Įrašus su įspėjimų

daugiažodiškumu gali rinkti ESET PROTECT.

Informacijos ir įspėjimo registravimo daugiažodiškumas galimas tik taisyklėms, kuriose yra bent du komponentai be pakaitos simbolių domene. Pavyzdžiui:
- *.domain.com/*
- *www.domain.com/*

Valdymo elementai

Pridėti – pridėkite prie sąrašo naują URL adresą (kelias vertes atskirkite skyrikliais).

Redaguoti – modifikuoja sąraše esamą adresą. Pasiekiama tik adresams, sukurtiems naudojant funkciją **Pridėti**.

Šalinti – panaikina iš sąrašo jame esančius adresus. Pasiekiama tik adresams, sukurtiems naudojant funkciją **Pridėti**.

Importuoti – importuokite failą su URL adresais (atskirkite reikšmes eilučių skirtukais, pvz., „*.txt“ faile, naudojančiame koduotę UTF-8).

Daugiau informacijos ieškokite skyriuje Kaip pridėti URL kaukę.

Kaip pridėti URL kaukę

Peržiūrėkite instrukcijas šiame dialoge prieš įvesdami norimą adresą / domeno kaukę.

ESET Endpoint Security leidžia vartotojui blokuoti prieigą prie nurodytos svetainės ir neleisti interneto naršyklei rodyti jų turinio. Be to, ji leidžia vartotojui nurodyti adresus, kurie turi būti netikrinami. Jeigu nuotolinio serverio visas pavadinimas yra nežinomas arba vartotojas nori nurodyti visą nuotolinių serverių grupę, tokiai grupei identifikuoti gali būti naudojami vadinamieji šablonai. Kaukėje naudojami simboliai „?“ ir „*“:

- naudokite „?“ norėdami pakeisti simbolį
- naudokite „*“ norėdami pakeisti teksto eilutę.

Pavyzdžiui, *.c?m taikoma visiems adresams, kuriuose paskutinė dalis prasideda raide c, baigiasi raide m, o tarp jų yra nežinomas simbolis (.com, .cam ir t. t.)

Pavyzdžiui, kaukė *x? žymi visus adresus, kuriuose priešpaskutinis simbolis yra „x“. Siekdami viso domeno atitikties, įveskite jį tokiu formatu: **.domain.com/**. Protokolo priešdėlio *http://*, *https://* kaukėje nurodyti nebūtina. Jei jis praleidžiamas, kaukė atitinka bet kurį protokolą. Priekyje esanti seka „*.“ apdorojama ypatingai, jei yra naudojama domeno vardo pradžioje. Pirmiausia šiuo atveju pakaitos simbolis „*“ neatitinka pasvirojo brūkšnio („/“). Tuo siekiama išvengti kaukės apėjimo, pvz., kaukė **.domain.com* neatitiks *http://anydomain.com/anypath#.domain.com* (tokia priesaga gali būti pridedama prie bet kokio URL nepaveikiant atsisiuntimo). Be to, antrasis „*.“ šiuo ypatinguoju atveju taip pat atitinka tuščią eilutę. Tuo siekiama leisti naudojant vieną kaukę sutapdinti visą domeną, įskaitant padomenius. Pavyzdžiui, kaukė **.domain.com* taip pat atitinka *http://domain.com*. Naudoti kaukę **domain.com* būtų neteisinga, nes ji taip pat atitiktų ir *http://anotherdomain.com*.

Informacijos ir įspėjimo registravimo daugiažodiškumas galimas tik taisyklėms, kuriose yra bent du komponentai be pakaitos simbolių domene. Pavyzdžiui:
- *.domain.com/*
- *www.domain.com/*

Apsauga nuo sukčiavimo apsimetant

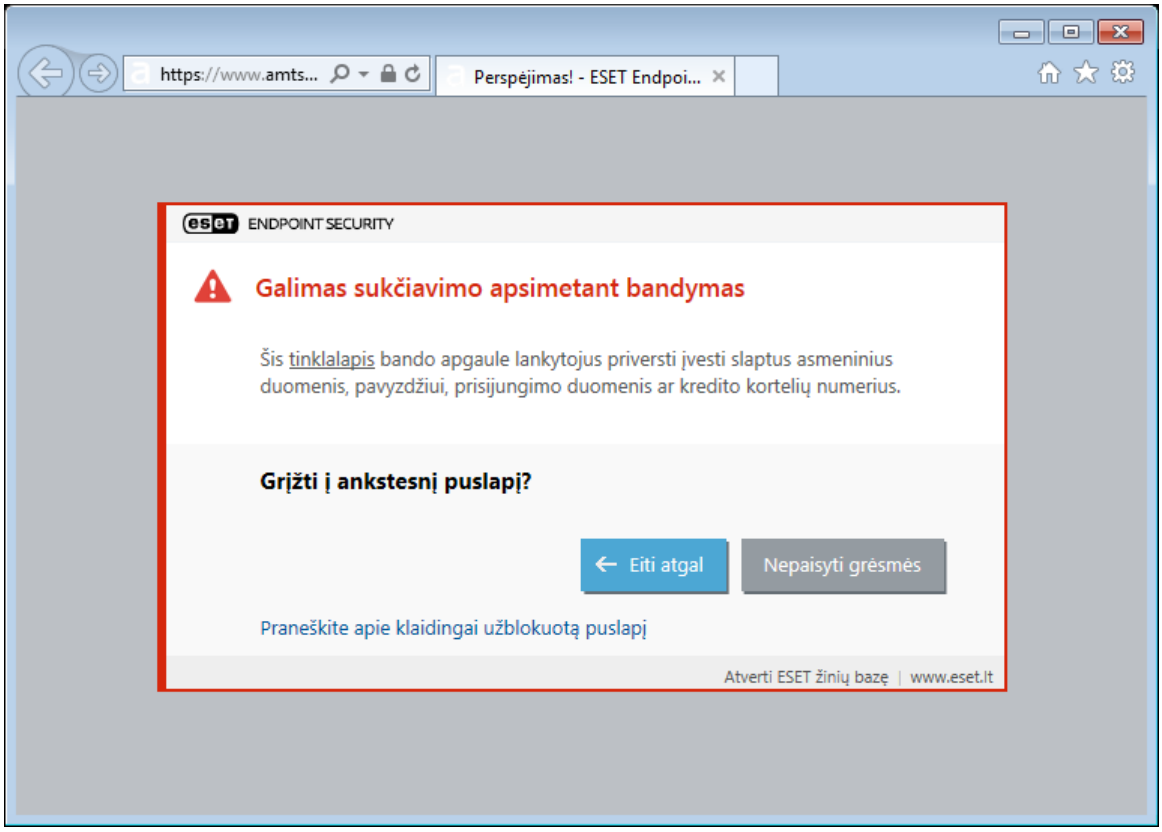
Sukčiavimas apsimetant yra nusikalstama veikla, kurioje naudojama socialinė inžinerija (manipuliavimas naudotojais, siekiant gauti konfidencialią informaciją). Sukčiavimas apsimetant naudojamas norint pasiekti neskelbtinus duomenis, pvz., banko sąskaitų numerius, PIN kodus ir kt. Daugiau informacijos rasite terminų žodyne. ESET Endpoint Security yra apsaugos nuo sukčiavimo apsimetant funkcija, kuri blokuoja tinklalapius, platinančius šio tipo turinį.

Apsauga nuo sukčiavimo apsimetant įgalinta pagal numatytuosius nustatymus. Šį nustatymą galima pasiekti pagrindiniame programos lange > **Išplėstinis nustatymas** (F5) > **Saitynas ir el. paštas** > **Apsauga nuo sukčiavimo apsimetant**.

Apsilankę mūsų žinių bazės straipsnyje rasite daugiau informacijos apie ESET Endpoint Security apsaugą nuo sukčiavimo apsimetant.

Prieiga prie apsimestinės svetainės

Kai pasiekiate atpažintą sukčiavimo apsimetant svetainę, jūsų saityno naršyklėje bus rodomas šis dialogo langas. Jei svetainėje vis tiek norėsite apsilankyti, spustelėkite **Nepaisyti grėsmės** (nerekomenduojama).



Galimos sukčiavimo apsimetant svetainės, kurios buvo įtrauktos į baltąjį sąrašą, pagal numatytuosius nustatymus nustos galioti po keleto valandų. Kad leistumėte naudoti interneto svetainę nuolat, naudokite URL adresų valdymo įrankį. Dalyje **Išplėstinis nustatymai** (F5) išplėskite **Saitynas ir el. paštas** > **Prieigos prie saityno apsauga** > **URL adresų valdymas** > **Adresų sąrašas**, spustelėkite **Redaguoti**, tada įtraukite į sąrašą svetainę, kurią norite redaguoti.

Pranešimas apie sukčiavimo apsimetant svetaines

Naudodami saitą Pranešti galite pranešti apie apsimestinę / kenkėjišką svetainę ir pateikti ją ESET, kad būtų atlikta analizė.

Prieš pateikdami svetainę ESET įsitikinkite, kad ji atitinka vieną ar daugiau iš šių kriterijų:
• svetainė visiškai nebuvo aptikta,
• svetainė klaidingai aptikta kaip grėsmė. Šiuo atveju galite pranešti apie klaidingą sukčiavimo apsimetant svetainę.

Arba galite pateikti svetainę el. paštu. Siųskite el. laišką adresu samples@eset.com. Būtinai nurodykite aprašomąją temą ir pridėkite kuo daugiau informacijos apie svetainę (pvz., svetainę, iš kurios čia patekote, kaip sužinojote apie šią svetainę ir pan.).

Saugios naršyklės išplėstinis nustatymas

Šis nustatymas yra prieinamas srityje **Išplėstiniai nustatymai** (F5) > **Saitynas ir el. paštas** > **Saugi naršyklė**.

Pagrindinis

Įjungti saugią naršyklę – įjungus, suaktyvinamas apsaugotų svetainių sąrašas, iš kurio galite atidaryti langą Apsaugotos svetainės.

Interneto svetainės peradresavimas

Įjungti apsaugotų svetainių nukreipimą – jei įjungta, svetainės iš apsaugotų svetainių sąrašo ir vidinio internetinės bankininkystės sąrašo bus nukreiptos į saugią naršyklę.

Apsaugotos svetainės – sąrašas su svetainėmis, kurioms galite pasirinkti atidarymui naudojamą naršyklę (įprastą arba apsaugotą). Naršyklės rėmelyje bus rodomas ESET logotipas, kuris reiškia, kad veikia saugus naršymas.

Saugi internetinė bankininkystė ir mokėjimo puslapiai – išjungta pagal numatytuosius nustatymus. Be saugomų svetainių sąrašo, ESET vidinio sąrašo svetainės bus nukreiptos į ESET apsaugotą naršyklę. ESET identifikuotos svetainės reguliariai atnaujinamos.

Apsaugota naršyklė

Išplėsta atminties apsauga – jei įjungta, saugios naršyklės atmintis bus apsaugota nuo kitų procesų vykdomo tikrinimo.

Klaviatūros apsauga – jei įjungta, saugioje naršyklėje klaviatūra įvesta informacija bus paslėpta nuo kitų programų. Tai padidina apsaugą nuo registravimo programų.

Naršyklės žalias rėmelis – Jei išjungta, žalias rėmelis aplink naršyklės langą ir susijęs pranešimas naršyklėje bus

trumpai rodomas naršyklės paleidimo metu, o tada išnyks. Žalias rėmelis reiškia, kad jūsų naršyklė yra visiškai apsaugota.

Konfigūruoti saugios naršyklės interaktyvius įspėjimus – leidžia atidaryti langą Interaktyvūs įspėjimai.

> Kai kuriais atvejais interaktyvus įspėjimas rodomas tik tada, kai nepavyksta tinkamai paleisti saugios naršyklės. Daugiau informacijos ieškokite skyriuje Interaktyvūs įspėjimai.

Apsaugotos svetainės

ESET Endpoint Security yra integruotas sąrašas su iš anksto nustatytomis svetainėmis, kurioms bus atidaroma apsaugota naršyklė. Pridėti svetainių ar redaguoti svetainių sąrašą galite produkto konfigūracijoje.

Sąrašą **Apsaugotos svetainės** galima peržiūrėti ir redaguoti srityje **Išplėstiniai nustatymai** (F5) > **Saitynas ir el. paštas** > **Saugi naršyklė** > **Bendra** > **Apsaugotos svetainės** > **Redaguoti**.

Langą sudaro:

Stulpeliai

Svetainė – apsaugota svetainė.

Apsaugota naršyklė – veikiant apsaugotam naršymui aplink naršyklės rėmelį bus rodomas ESET logotipas.

Įprasta naršyklė – pasirinkite šią parinktį, jei norite tęsti savo numatytojoje žiniatinklio naršyklėje (pvz., banko operaciją).

Valdymo elementai

Pridėti – prie žinomų svetainių sąrašo galite pridėti svetainę.

Redaguoti – leidžia redaguoti pasirinktus įrašus.

Šalinti – pašalinami pasirinkti įrašai.

Naršyklės pranešimas

Apsaugota naršyklė informuoja apie dabartinę būseną naršyklės pranešimu ir naršyklės rėmelio spalva.

Naršyklės pranešimai rodomi dešinėje pusėje esančiame skirtuke.



Norėdami išplėsti pranešimą naršyklėje, spustelėkite ESET piktogramą . Norėdami sumažinti pranešimą, spustelėkite pranešimo tekstą. Norėdami atmesti pranešimą, spustelėkite uždarymo piktogramą .

Naršyklės pranešimai

Pranešimo tipas	Būsena
Informacinis pranešimas ir žalia naršyklės rėmelis	Užtikrinama maksimali apsauga ir pagal numatytuosius nustatymus sumažinamas naršyklės pranešimas.
Įspėjimas ir oranžinis naršyklės rėmelis	Apsaugota naršyklė reikalauja jūsų dėmesio dėl nekritinės problemos. Norėdami gauti daugiau informacijos apie problemą ar sprendimą, vadovaukitės naršyklės pranešime pateiktomis instrukcijomis.
Saugos įspėjimas ir raudonas naršyklės rėmelis	Naršyklė nėra apsaugota ESET banko mokėjimų apsauga. Paleiskite naršyklę iš naujo, kad įsitikintumėte, jog apsauga yra aktyvi. Norėdami išspręsti konfliktą dėl į naršyklę įkeltų failų, kreipkitės į ESET techninę pagalbą vadovaudamiesi mūsų žinių bazės straipsnyje pateiktomis instrukcijomis.

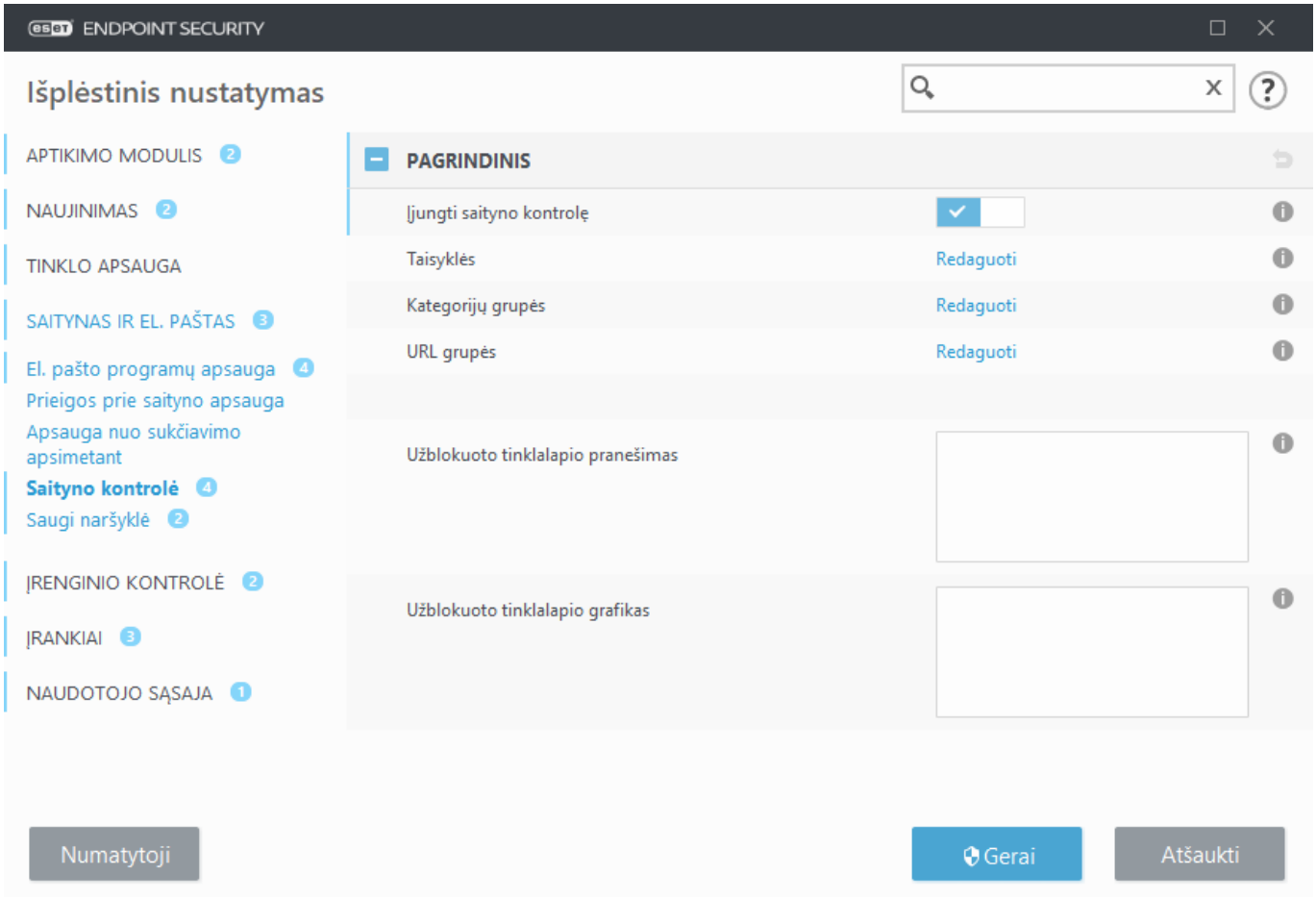
Saityno kontrolė

Saityno kontrolės skyriuje galima konfigūruoti parametrus, kurie apsaugo jūsų įmonę nuo teisinės atsakomybės rizikos. Saityno kontrolė gali reguliuoti prieigą prie interneto svetainių, kurios pažeidžia intelektinės nuosavybės teises. Tikslas – neleisti darbuotojams pasiekti puslapių su netinkamu arba žalingu turiniu arba puslapių, kurie gali turėti neigiamos įtakos našumui.

Saityno kontrolė leidžia blokuoti interneto puslapius, kuriuose gali būti galimai įžeidžiančios žalingos informacijos. Be to, darbdaviai arba sistemos administratoriai gali uždrausti prieigą prie daugiau nei 27 iš anksto nustatytų svetainių kategorijų ir daugiau nei 140 subkategorijų.

Pagal numatytuosius nustatymus saityno kontrolė išjungta. Norint įjungti saityno kontrolę:

1. Paspauskite **F5** ir atverkite **Išplėstinis nustatymas**, tada išskleiskite **Saitynas ir el. paštas** > **Saityno kontrolė**.
2. Pasirinkite **Įjungti saityno kontrolę**, kad aktyvintumėte saityno kontrolę ESET Endpoint Security.
3. Norėdami konfigūruoti prieigą prie konkrečių tinklalapių, spustelėkite **Redaguoti** šalia **Taisyklės**, kad galėtumėte pasiekti langą Saityno kontrolės taisyklių rengyklė .

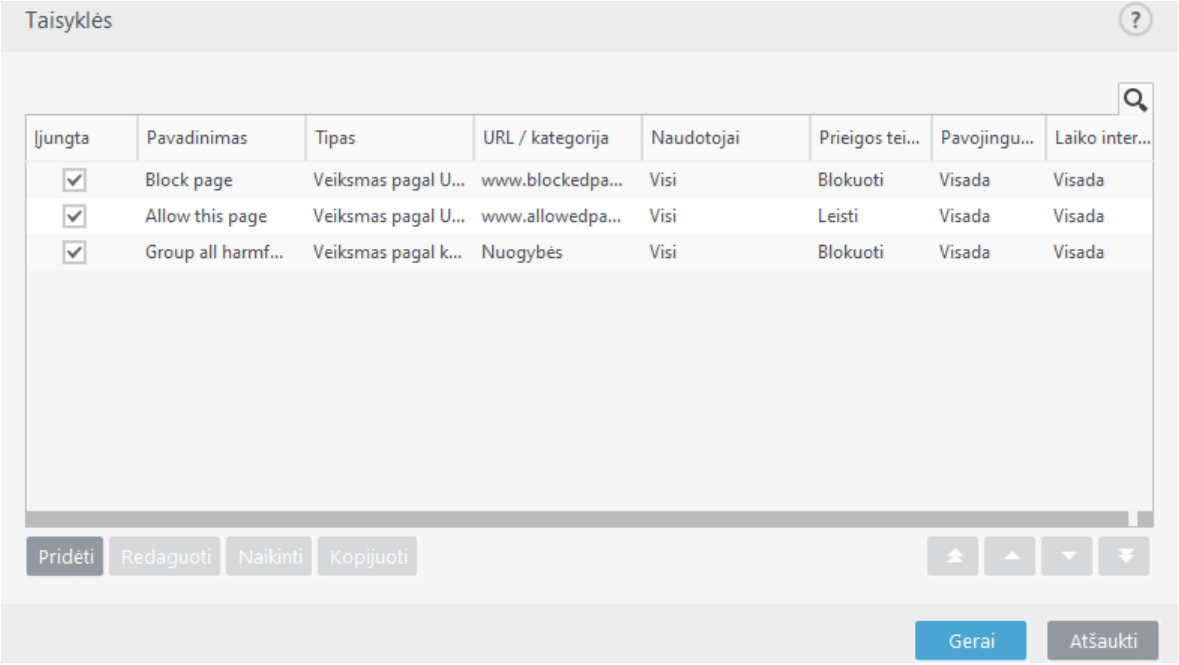


Laukuose **Užblokuoto tinklalapio pranešimas** ir **Užblokuoto tinklalapio grafika** galite lengvai pasirinkti pranešimą, kuris bus rodomas užblokavus svetainę.

Jei pageidaujate blokuoti visus tinklalapius, išskyrus tam tikrus, naudokite URL adresų valdymas.

Saityno kontrolės taisyklės

Lange **Taisyklių rengyklė** rodomos esamos taisyklės pagal URL adresus ir kategorijas.



Taisyklių sąrašas turi keletą taisyklių aprašymų, tokių kaip pavadinimas, blokavimo tipas, veiksmas, kurį reikia atlikti pritaikius saityno kontrolės taisyklę, ir žurnalo svarba.

Spustelėkite **Pridėti** arba **Redaguoti** norėdami tvarkyti taisyklę. Jei norite sukurti naują taisyklę su iš anksto nustatytomis parinktimis, naudojamomis kitai pasirinktai taisyklei, spustelėkite **Kopijuoti**. Paspausdami **Ctrl** ir spustelėdami galite pasirinkti kelias taisykles ir panaikinti visas pasirinktas taisykles. Žymės langelis **Įjungta** išjungia ar įjungia šią taisyklę. Tai gali būti naudinga, jei nenorite panaikinti taisyklės visam laikui, kadangi ją gali reikėti panaudoti ateityje.

Taisyklės yra rūšiuojamos pagal jų svarbą, didesnės svarbos taisykles pateikiant viršuje. Norėdami pakeisti taisyklės svarbą, pasirinkite taisyklę ir spragtelėkite rodyklės mygtuką, kad padidintumėte arba sumažintumėte taisyklės svarbą. Spustelėkite dvigubą rodyklę, kad perkeltumėte taisyklę į sąrašo viršų arba apačią.

Skaitykite daugiau informacijos apie taisyklių kūrimą.

Saityno kontrolės taisyklių pridėjimas

Saityno kontrolės taisyklių lange galima rankiniu būdu sukurti arba keisti esamas saityno kontrolės filtravimo taisykles.

Pavadinimas

Kad būtų patogiau nustatyti, įveskite taisyklės aprašymą į lauką **Pavadinimas**.

Įjungta

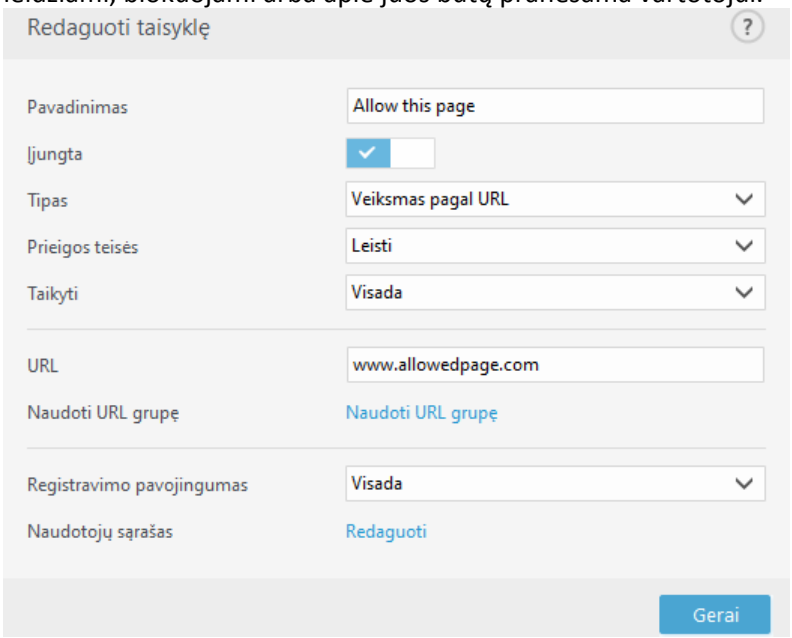
Spustelėkite jungiklį **Įjungta**, kad išjungtumėte arba įjungtumėte šią taisyklę. Tai gali būti naudinga, jei taisyklės nenorite panaikinti visam laikui.

Veiksmas

Pasirinkite **Veiksmas pagal URL** arba **Veiksmas pagal kategoriją**:

Veiksmas pagal URL

jei norite nustatyti taisykles, kuriomis kontroliuojama prieiga prie konkrečios svetainės, lauke **URL** įveskite URL.
Specialiųjų simbolių * (žvaigždutės) ir ? (klaustuko) negalima naudoti URL adreso sąraše. Kurdami URL grupę, kurioje yra svetainė su keliais aukščiausio lygio domenais (TLD), kiekvieną TLD turėsite pridėti atskirai. Kai prie grupės pridedate domeną, visas šio domeno ir visų padomenių turinys (pvz., *sub.examplepage.com*) bus blokuojamas arba leidžiamas, atsižvelgiant į jūsų pasirinktą veiksmą pagal URL.
URL arba **Naudoti URL grupę** – naudojamas URL saitas arba URL grupė, kad aptikus šiuos URL jie būtų leidžiami, blokuojami arba apie juos būtų pranešama vartotojui.



Veiksmas pagal kategoriją

Jei pasirinksite šią parinktį, išskleidžiamajame meniu nustatykite savo veiksmo kategoriją.
URL kategorija arba **Naudoti grupę** – naudoja svetainės kategoriją arba kategorijas Kategorijų grupė, kad aptikus šias grupes, jos būtų leidžiamos, blokuojamos arba apie jas būtų pranešama vartotojui.

Prieigos teisės

- **Leisti** – bus suteikta prieiga prie URL adreso / kategorijos.
- **Įspėti** – vartotojas bus įspėjamas apie URL adresą / kategoriją.
- **Visada įspėti** – vartotojas bus įspėjamas apie URL adresą / kategoriją. Svetainėje galite apsilankyti, tačiau apie tai bus pranešta administratoriui.
- **Blokuoti** – bus blokuojamas URL adresas / kategorija.

Taikyti

Suteikia galimybę tam tikru laiku taikyti sukurtą taisyklę. Iš išskleidžiamojo meniu pasirinkite sukurtą laiko intervalą.

- Daugiau informacijos apie Laiko intervalai

Registravimo pavojingumas

- **Visada** – registruoja visus internetinius ryšius.
- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą.
- **Informacija** – įrašo informacinius pranešimus, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimas** – įrašo kritines klaidas ir įspėjimo pranešimus.
- **Nėra** – žurnalai nekuriami.

> Registravimo svarbą galima sukonfigūruoti atskirtai kiekvienam sąrašui. Žurnalus, kurių būsena yra **Įspėjimas**, gali sukurti ESET PROTECT.

Vartotojų sąrašas

- **Pridėti** – atveria dialogo langą **Pasirinkti vartotojus arba grupes**, kuriame galima pasirinkti pageidaujamus vartotojus. Jei vartotojas nenurodomas, taisyklė taikoma visiems vartotojams.
- **Šalinti** – šalina pasirinktą vartotoją iš filtro.

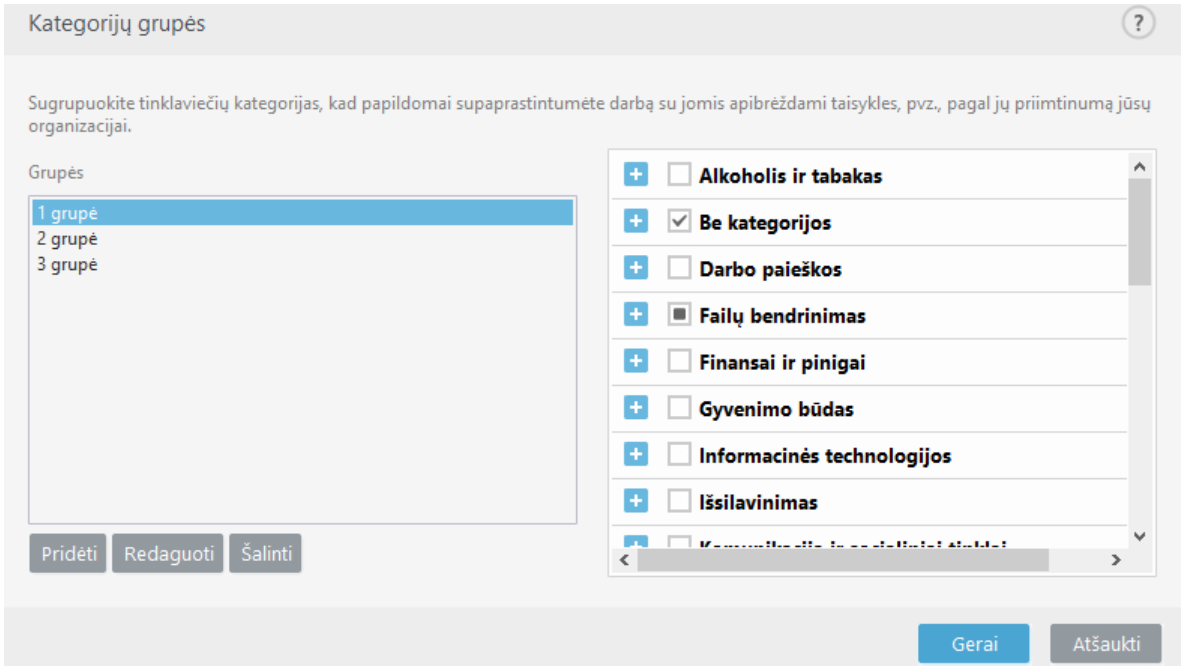
Kategorijų grupės

Kategorijų grupių langas yra padalytas į dvi dalis. Kairėje lango pusėje yra kategorijų grupių sąrašas.

- **Pridėti** – spustelėkite, kad sukurtumėte naują kategorijų grupę.
- **Redaguoti** – spustelėkite, jei norite redaguoti esamą kategorijų grupę.
- **Šalinti** – pasirinkite ir spustelėkite, jei norite pašalinti esamą kategorijų grupę iš kategorijų grupių sąrašo.

Dešinėje lango pusėje yra kategorijų ir pakategorių sąrašas. Kategorijų sąraše pasirinkite kategoriją, kad būtų parodytos pakategorės. Kiekvienoje grupėje yra suaugusiųjų ir (arba) bendruoju požiūriu netinkamų pakategorių ir kategorijų, kurios yra laikomos bendruoju požiūriu priimtinomis. Atvėrus kategorijų grupių langą ir spustelėjus pirmąją grupę, galima prie atitinkamų grupių sąrašo pridėti arba iš jo pašalinti kategorijas / pakategores (pvz., „Smurtas“ ar „Ginklai“). Tinklalapius su netinkamu turiniu galima užblokuoti arba sukūrus taisyklę su iš anksto apibrėžtais veiksmais galima informuoti naudotojus.

Pažymėkite langelį, kad pridėtumėte arba pašalintumėte subkategoriją iš konkrečios grupės.



Čia pateikiami kurie kategorijų pavyzdžiai, kurie vartotojams gali būti nepažįstami:

Įvairūs – paprastai asmeniniai (vietiniai) IP adresai, pvz., intraneto, 192.168.0.0/16 ir pan. Kai gausite klaidos kodą Nr. 403 arba 404, interneto svetainė taip pat atitiks šią kategoriją.

Neišspręsta – šiai kategorijai priklauso tinklalapiai, kurie yra neišspręsti dėl klaidos jungiantis prie saityno kontrolės duomenų bazės modulio.

Be kategorijos – nežinomi tinklalapiai, kurių dar nėra saityno kontrolės duomenų bazėje.

Įgaliotieji serveriai – tokie tinklalapiai kaip anonimiškumą užtikrinantys, nukreipiantieji ar viešieji įgaliotieji serveriai, gali būti naudojami norint (anonimiškai) pasiekti tinklalapius, kuriuos paprastai draudžia saityno kontrolės filtras.

Failų bendrinimas – šiuose tinklalapiuose yra daug duomenų, tokių kaip nuotraukos, vaizdo įrašai arba el. knygos. Kyla pavojus, kad šiose interneto svetainėse gali būti galimai įžeidžiančio arba suaugusiesiems skirto turinio.

> Subkategorija gali priklausyti bet kuriai grupei. Kai kurios subkategorijos nėra įtrauktos į iš anksto nustatytas grupes (pvz., „Žaidimai“). Kad galėtumėte pritaikyti norimą subkategoriją naudodami saityno kontrolės filtrą, įtraukite ją į norimą grupę.

URL grupės

URL grupės leidžia sukurti grupę su keliais URL saitais, kuriems norite sukurti taisyklę (leisti / drausti konkrečias tinklavietes).

Naujos URL grupės kūrimas

Norėdami sukurti naują URL grupę, spustelėkite **Įtraukti** ir įveskite naujos URL grupės pavadinimą.

Naudoti URL grupę gali būti pravartu, kai administratorius nori sukurti taisyklę daugiau žiniatinklio puslapių

(blokuojamų arba leidžiamų, atsižvelgiant į pasirinkimą).

Įtraukti URL adresus į URL grupė sąrašą – rankiniu būdu

Norėdami įtraukti naujus URL adresus į sąrašą, pasirinkite URL ir spustelėkite **Įtraukti** lango apačioje.

Specialiųjų simbolių * (žvaigždutės) ir ? (klaustuko) negalima naudoti URL adreso sąraše.

Nebūtina įvesti viso domeno vardo su http:// arba https://.

Jei įtraukiate į grupę domeną, visas domene ir padomeniuose esantis turinys (pvz., *sub.examplepage.com*) bus užblokuotas arba leidžiamas, atsižvelgiant į pasirenkamus veiksmus pagal URL.

Jei dvi taisyklės prieštarauja viena kitai, t. y. pirmoji taisyklė blokuoja domeną, o antroji leidžia tą patį domeną, konkretus domenas arba IP adresas vis vien bus užblokuotas. Jei reikia daugiau informacijos apie taisyklių kūrimą, žr. Veiksmai pagal URL.

Įtraukti URL adresus į URL grupių sąrašą – importuoti naudojant .txt failą

Spustelėkite **Importuoti**, kad importuotumėte failą su URL adresų sąrašu (atskiros reikšmės atskirtos eilute, pvz., .txt failas su UTF-8 koduote). Specialiųjų simbolių * (žvaigždutės) ir ? (klaustuko) negalima naudoti URL adreso sąraše.

URL grupių naudojimas saityno kontrolei

Jei norite nustatyti veiksmą konkrečiai URL grupei, atidarykite Saityno kontrolės taisyklių redagavimo programą, pasirinkite savo URL grupę išskleidžiamajame meniu, koreguokite parametrus ir spustelėkite **Gerai**.

> Blokuoti arba leisti konkrečius tinklalapius gali būti tiksliau, nei blokuoti arba leisti visą tinklalapių kategoriją. Būkite atsargūs keisdami šiuos parametrus ir įtraukdami kategoriją / tinklalapį į sąrašą.

Užblokuoto tinklalapio pranešimo tinkinimas

Laukuose **Užblokuoto tinklalapio pranešimas** ir **Užblokuoto tinklalapio grafika** galite lengvai pasirinkti pranešimą, kuris bus rodomas užblokavus svetainę.

Tai yra numatytoji naršyklės pranešimo žinutė ir dizainas, kai naudotojas bando atidaryti blokuojamą svetainę:

Naudojimas

Leidžia blokuoti svetainių kategoriją „Ginklai“.

Užblokuoto tinklalapio pranešimo pavyzdys:

```
Tinklalapis %URL_OR_CATEGORY% buvo užblokuotas, nes jo turinys laikomas netinkamu a
rba žalingu.
Dėl išsamesnės informacijos susisiekite su administratoriumi.
```

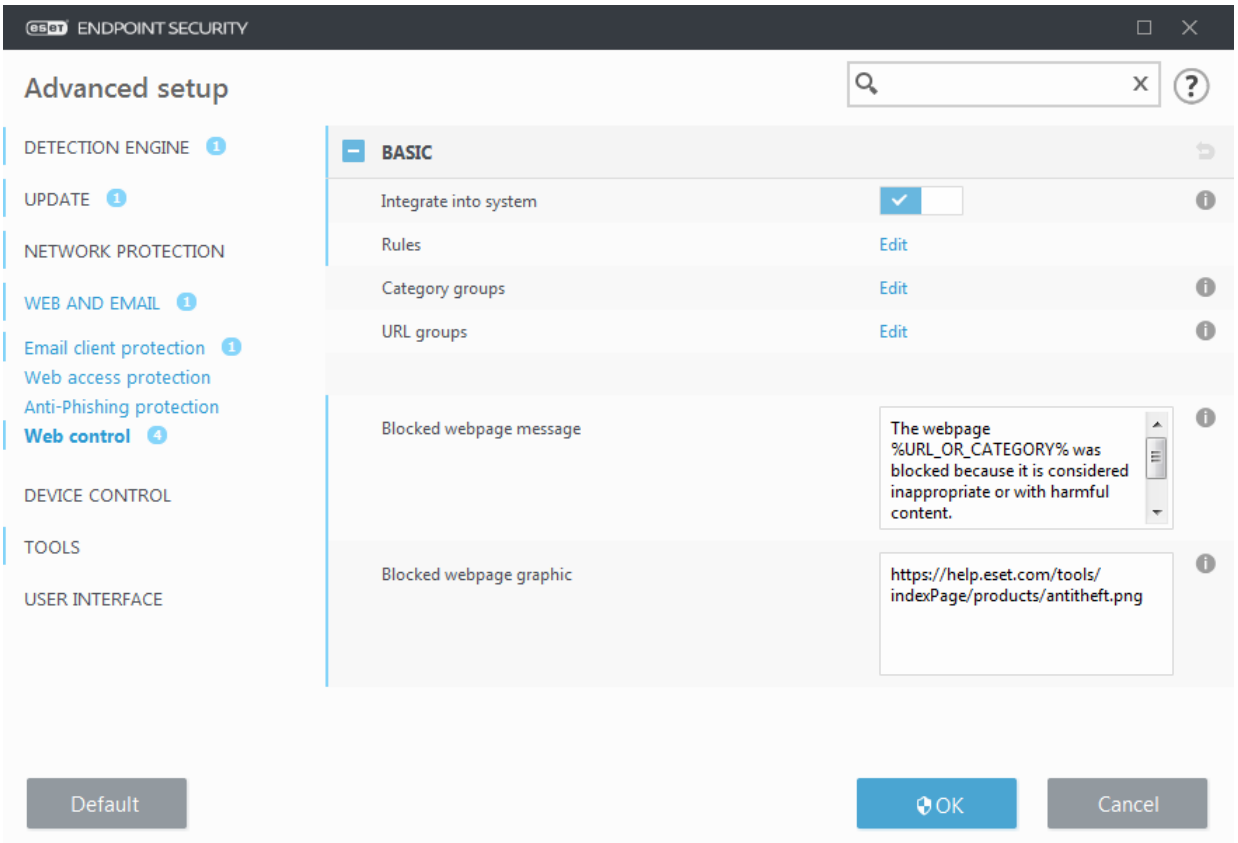
Kintamasis	Aprašymas
%CATEGORY%	Užblokuota saityno kontrolės kategorija.
%URL_OR_CATEGORY%	Užblokuota saityno kontrolės svetainė arba kategorija (priklauso nuo saityno kontrolės blokavimo taisyklės).
%STR_GOBACK%	Mygtuko „Eiti atgal“ reikšmė.
%product_name%	ESET produkto pavadinimas (ESET Endpoint Security)
%product_version%	ESET produkto versija.

Užblokuoto tinklalapio grafikos pavyzdys:

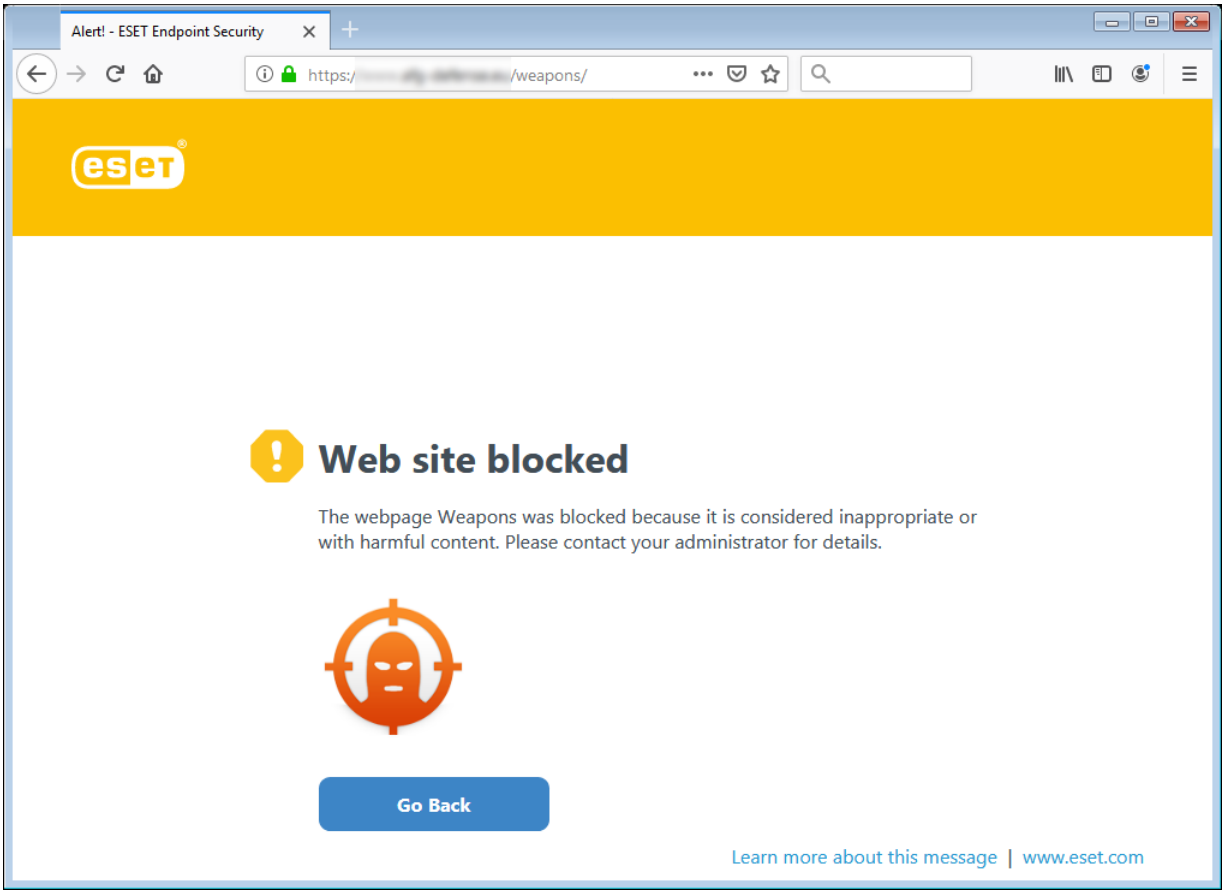
```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

Vaizdo dydis (plotis / aukštis) keičiamas automatiškai, jei yra per didelis.

ESET Endpoint Security konfigūracija atrodys taip:



Pasirinktinis naršyklės pranešimas naudotojui bandant pasiekti užblokuotą svetainę atrodys taip:



Programos naujinimas

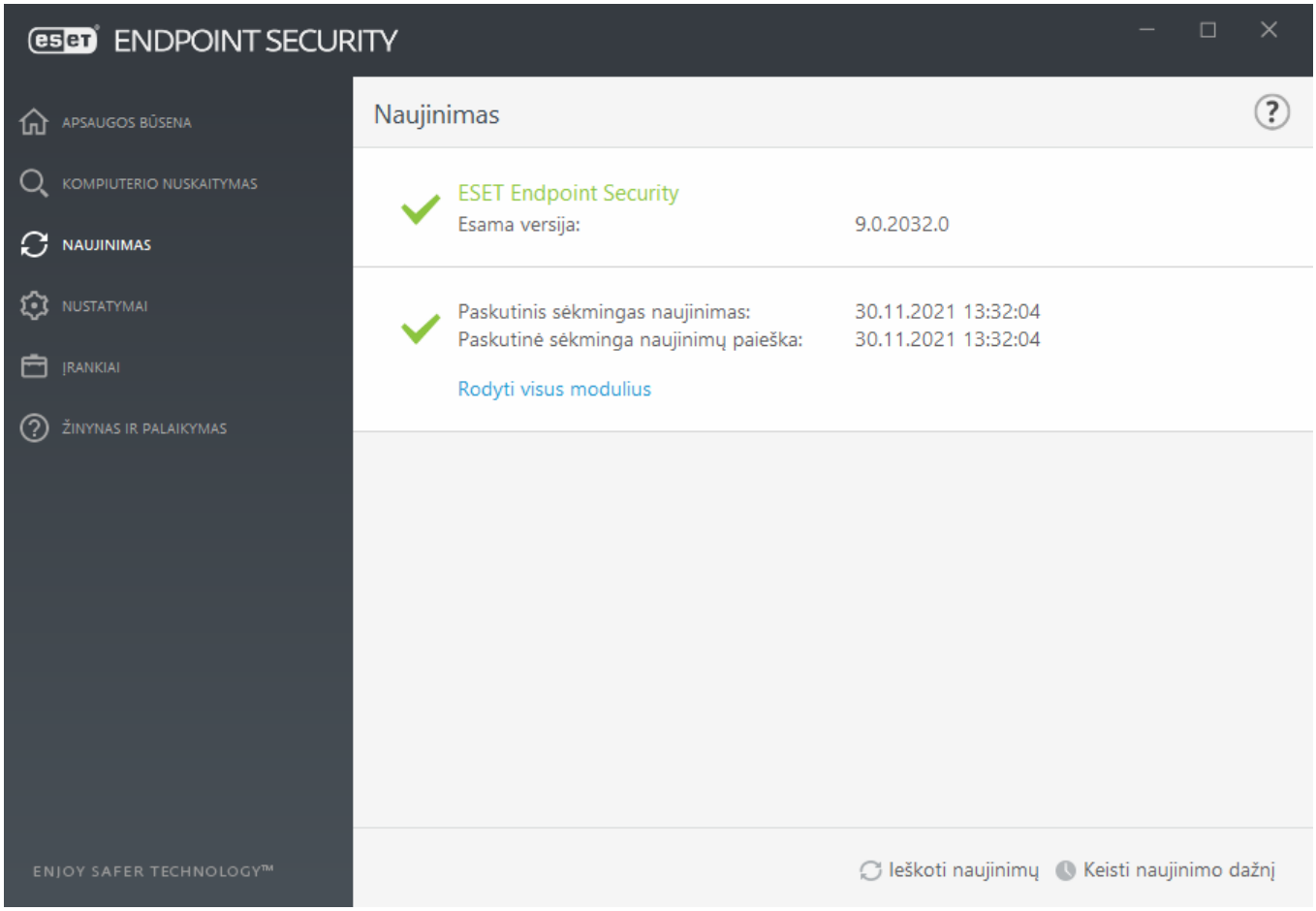
Reguliariai naujinti ESET Endpoint Security yra geriausias būdas palaikyti maksimalų saugumo lygį jūsų kompiuteryje. Naujinimo modulis užtikrina, kad programa visada bus atnaujinta, dviem būdais – naujindamas virusų aptikimo modulį ir sistemos komponentus. Pagal numatytuosius nustatymus aktyvinus programą naujinamai diegiami automatiškai.

Spustelėję **Naujinimas** pagrindiniame programos lange, galite rasti esamą naujinimo būseną, įskaitant paskutinio sėkmingo naujinimo datą ir laiką ir ar reikalingas naujinimas. Taip pat galite spustelėti saitą **Rodyti viskus modulius**, kad atsidarytų įdiegtų modulių sąrašas, ir patikrinti versiją bei paskutinį modulio naujinimą.

Be to, yra galimybė rankiniu būdu paleisti naujinimo procesą – **Tikrinti naujinimus**. Atnaujinti aptikimo modulį ir programos komponentus yra svarbu, kad būtų palaikoma visiška apsauga nuo kenkėjiškų kodų. Atkreipkite dėmesį į jų konfigūraciją ir veikimą. Jei diegdami neįvedėte savo licencijos duomenų, naujindami licencijos raktą galite įvesti spustelėję **Aktyvinti produktą**, kad prisijungtumėte prie ESET naujinimo serverių.

Jeigu ESET Endpoint Security suaktyvinate naudodamiesi autonominiu licencijos failu be vartotojo vardo ir slaptažodžio, tada bandote atnaujinti, raudonai rodomas pranešimas **Modulių naujinimas nepavyko** informuoja, kad siųstis naujinius galite tik veidrodinio serverio.

Licencijos raktą gaunate iš ESET įsigydami ESET Endpoint Security.



Esama versija – ESET Endpoint Security kompiliacijos numeris.

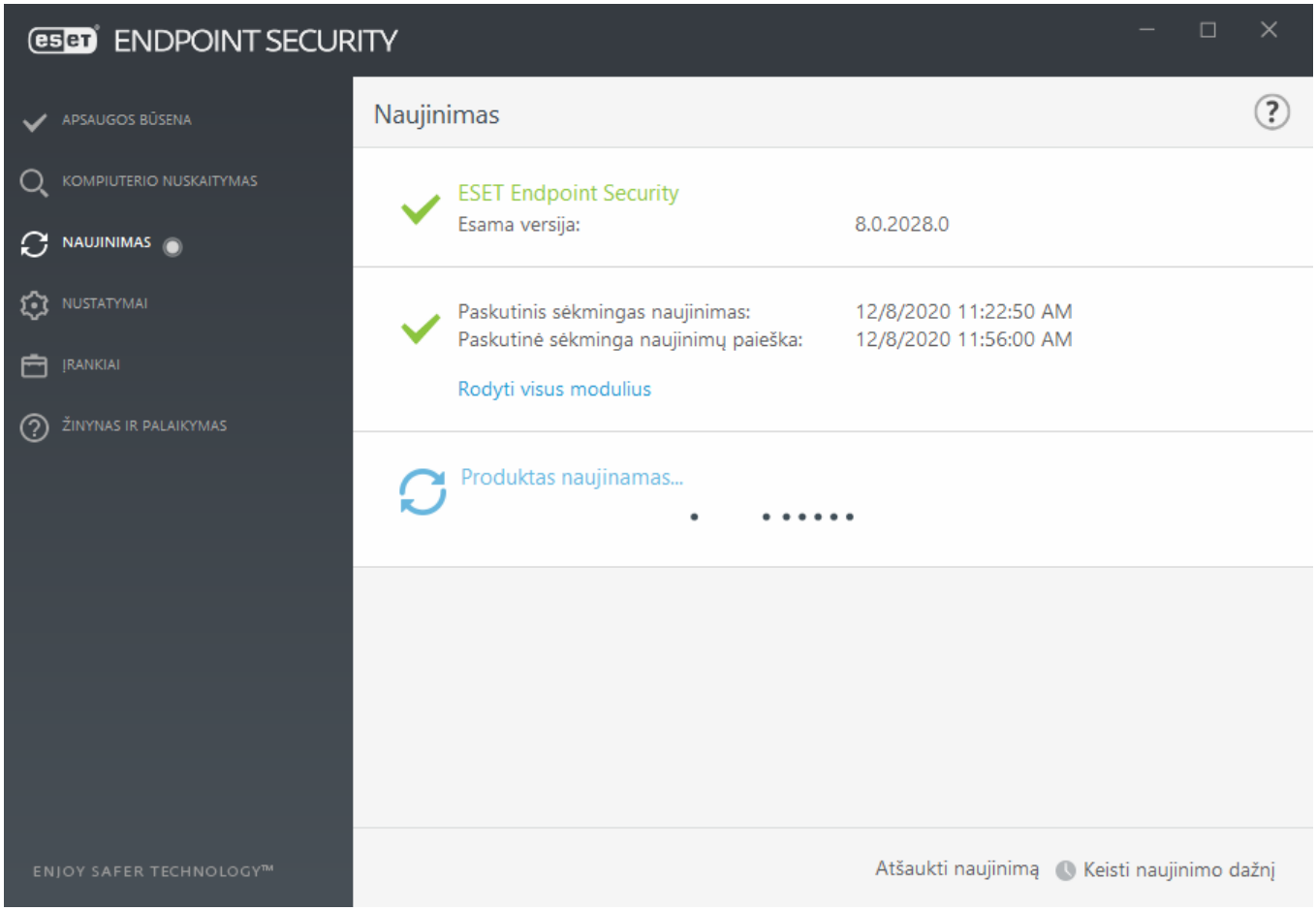
Paskutinis sėkmingas naujinimas – paskutinio sėkmingo naujinimo data ir laikas. Ji turi nurodyti naujausią datą, kuri užtikrina, jog aptikimo modulis nepasenęs.

Paskutinis sėkmingas naujinimų tikrinimas – paskutinio sėkmingo bandymo atnaujinti data ir laikas.

Rodyti visus modulius – spustelėkite saitą, kad atsidarytų įdiegtų modulių sąrašas, ir patikrinti versiją bei paskutinį modulio naujinimą.

Naujinimo procesas

Spustelėjus **Ieškoti naujinimų**, pradedamas atsisiuntimo procesas. Bus rodoma atsisiuntimo eigos juosta ir likęs atsisiuntimo laikas. Jei norite nutraukti naujinimą, spustelėkite **Atšaukti naujinimą**.

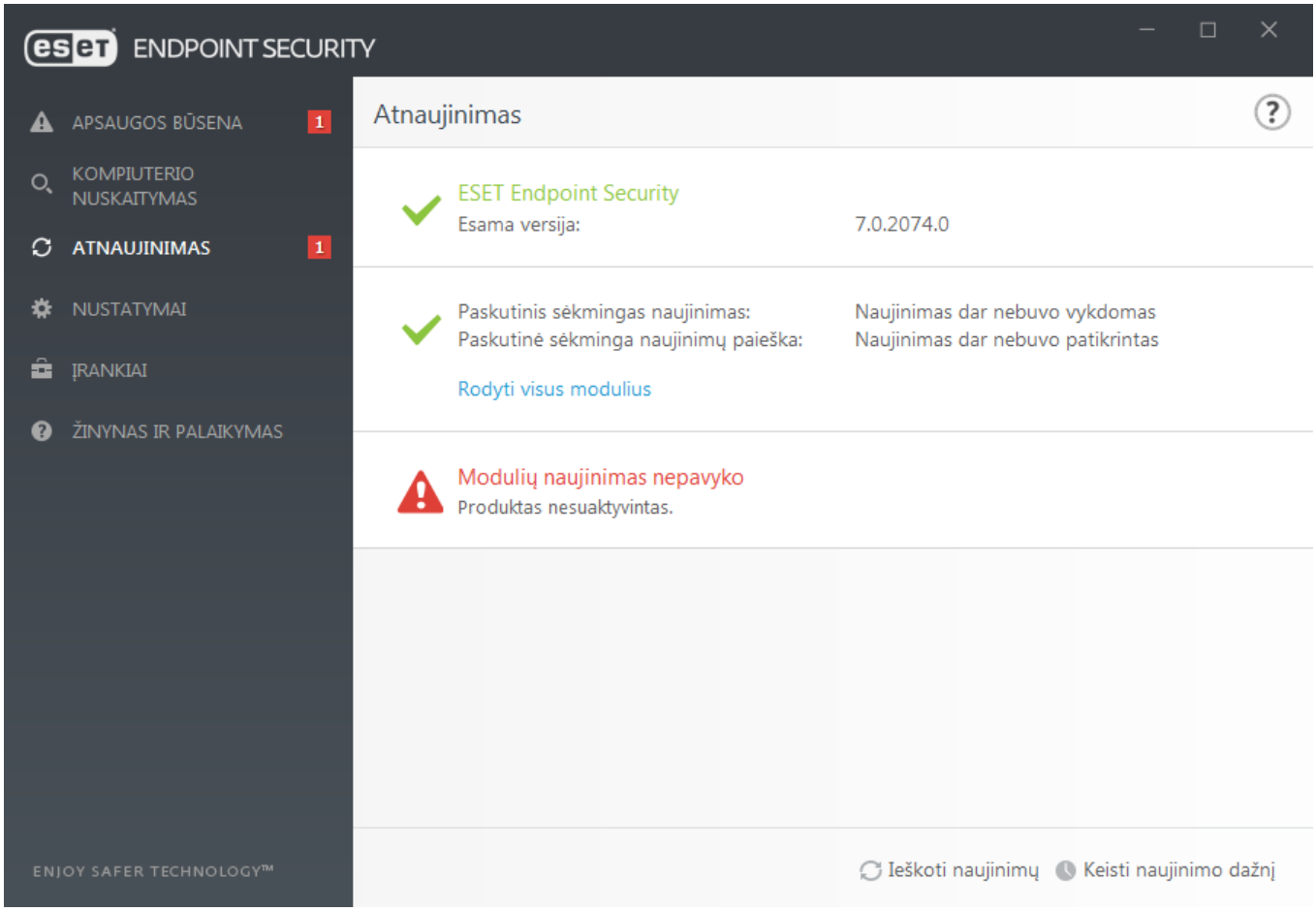


Įprastomis aplinkybėmis moduliai atnaujinami keletą kartų per dieną. Jeigu ne, programa yra pasenusi ir labiau pažeidžiama užkrato. Atnaujinkite modulius, kai tik bus įmanoma.

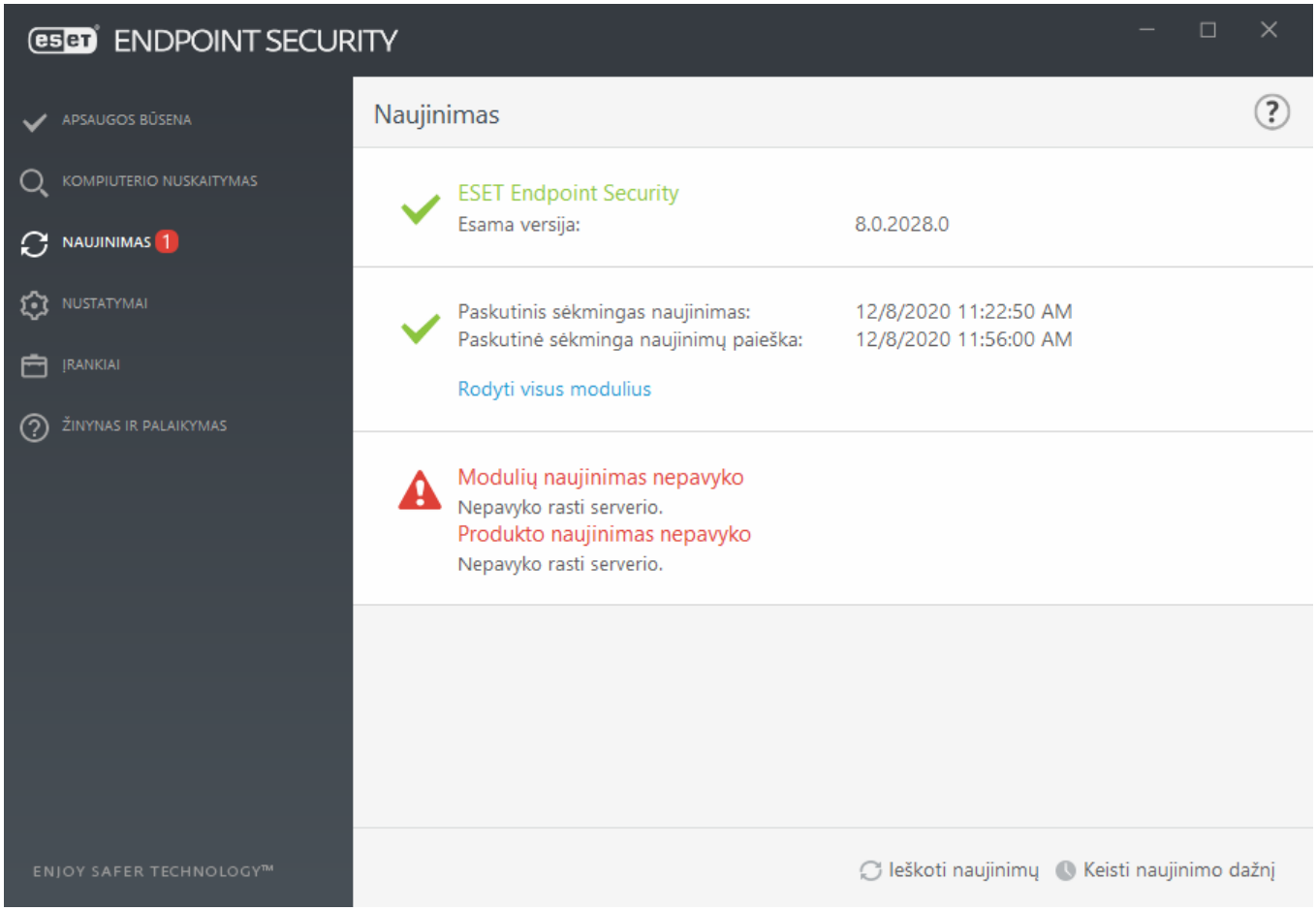
Aptikimo modulis pasenęs – ši klaida bus parodoma po keleto nesėkmingų bandymų atnaujinti modulius. Rekomenduojame patikrinti naujinimo parametrus. Dažniausiai pasitaikanti šios klaidos priežastis yra neteisingai įvesti atpažinimo duomenys arba neteisingai sukonfigūruoti ryšio parametrai.

Ankstesnis pranešimas yra susijęs su šiais dviem pranešimais (**Modulių naujinimas nepavyko**) apie nesėkmingus naujinimus:

1. **Negaliojanti licencija** – licencijos raktas neteisingai įvestas atliekant naujinimo nustatymą. Rekomenduojame patikrinti atpažinimo duomenis. Išplėstinio nustatymo lange (pagrindiniame meniu spustelėkite **Nustatymai**, tada – **Išplėstinis nustatymas** arba klaviatūroje paspauskite F5) pateikiama papildomų naujinimų parinkčių. Jei norite įvesti naują licencijos raktą, pagrindiniame meniu spustelėkite **Žinynas ir palaikymas** > **Keisti licenciją**.



2. **Įvyko klaida atsisiunčiant naujinimo failus** – galima šios klaidos priežastis yra neteisingi interneto ryšio parametrai. Rekomenduojame patikrinti savo interneto ryšį (atidarant bet kokią svetainę savo žiniatinklio naršyklėje). Jeigu svetainė neatsidaro, gali būti, kad nėra interneto ryšio arba yra jūsų kompiuterio prisijungimo problemų. Susisiekite su savo interneto paslaugų teikėju (ISP), jeigu nėra aktyvaus interneto ryšio.



Papildomos informacijos rasite šiame ESET žinių bazės straipsnyje.

Naujinimo nustatymai

Naujinimo nustatymų parinktys pasiekiamos **Išplėstinių nustatymų** medyje (F5) spustelėjus **Naujinimas**. Šiame skyriuje nurodoma naujinimo šaltinio informacija, tokia kaip naudojami naujinimo serveriai ir šių serverių autentiškumo patvirtinimo duomenys.

Kad naujinimai būtu atsisiunčiami tinkamai, labai svarbu teisingai įvesti visus naujinimo parametrus. Jei naudojate užkardą, įsitikinkite, kad jūsų ESET programai leidžiama jungtis prie interneto (t. y. leidžiamas HTTPS ryšys).

Pagrindinis

Šiuo metu naudojamas naujinimo profilis rodomas išskleidžiamajame meniu**Pasirinkti numatytąjį naujinimo profilį**.

Norėdami sukurti naują profilį, žr. skyrių Profilių

Automatinis profilio perjungimas – priskirkite naujinimo profilį pagal žinomus tinklus užkardoje. Automatinis profilio perjungimas leidžia pakeisti profilį specifiniam tinklui pagal planuoklės nustatymą. Daugiau informacijos žr. žinyno puslapiuose

Konfigūruoti atnaujinimų pranešimus – spustelėkite Redaguoti, jei norite pasirinkti, kokie programų pranešimai būtų rodomi. Galite pasirinkti, ar pranešimus Rodyti darbalaukyje ir (arba) Siųsti el. paštu.

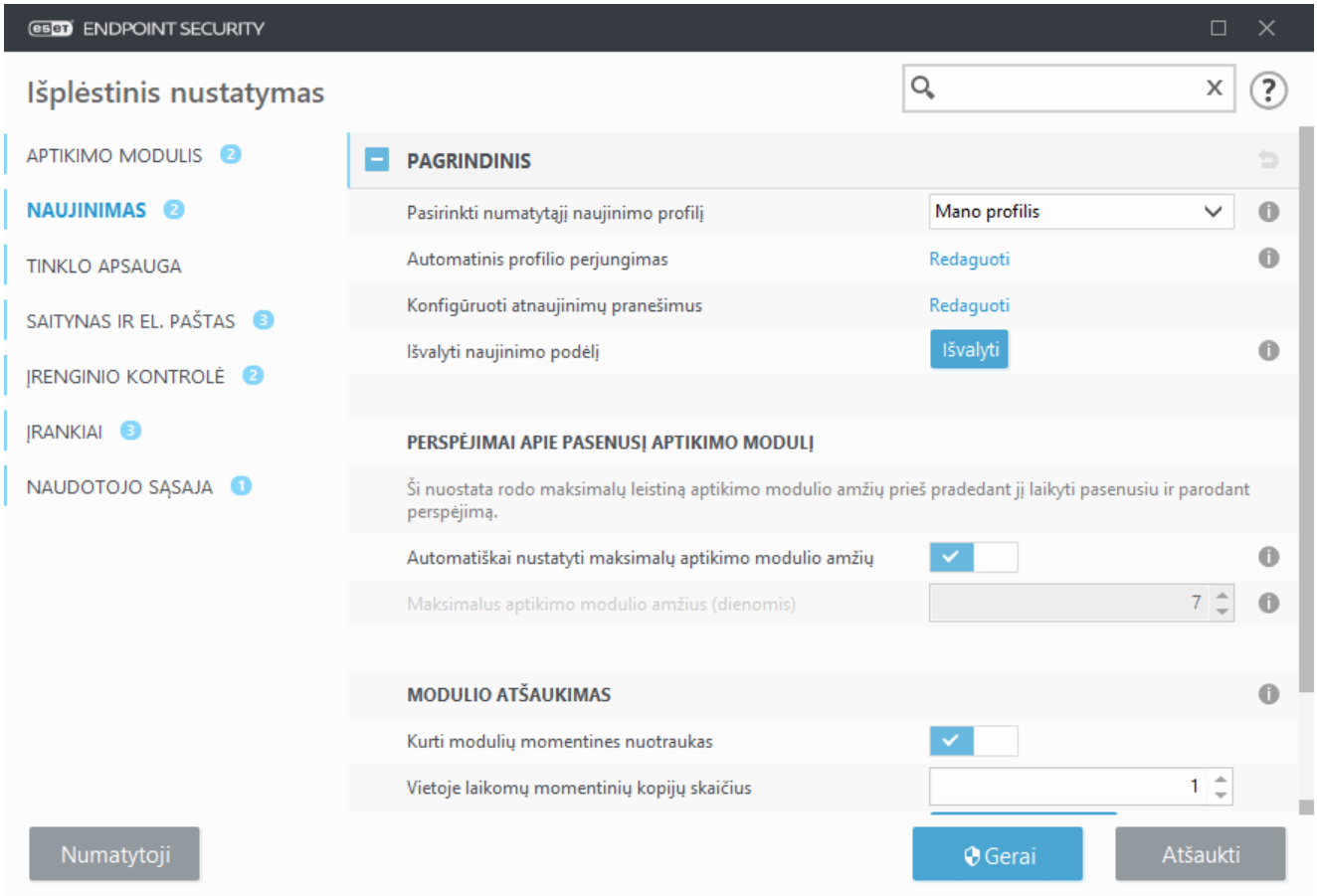
Jei mėgindami atsisiųsti modulius patiriate sunkumų, spustelėkite **Išvalyti** šalia **Išvalyti naujinimo podėlį**, kad išvalytumėte laikinuosius naujinimo failus / podėlį.

Įspėjimai apie pasenusį aptikimo modulį

Automatiškai nustatyti didžiausią aptikimo modulio amžių – galite nustatyti ilgiausią trukmę (dienomis), kuriai pasibaigus bus nurodoma, kad aptikimo modulis pasenęs. Numatytoji **didžiausio aptikimo modulio amžiaus (dienomis)** reikšmė yra 7.

Modulio atšaukimas

Jei įtariate, kad naujas aptikimo modulio ir (arba) programos modulio naujinimas gali būti nestabilus arba sugadintas, galite atšaukti keitimus į ankstesnę versiją ir išjungti visus pasirinkto laikotarpio naujinimus.



Profiliai

Naujinimų profiliai gali būti sukurti įvairioms naujinimų konfigūracijoms ir užduotims. Kurti naujinimų profilius yra labai naudinga mobiliųjų vartotojams, kuriems reikalingas alternatyvus profilis, atitinkantis nuolat besikeičiančias interneto ryšio ypatybes.

Išskleidžiamajame meniu **Pasirinkti redaguojamą profilį** rodomas šiuo metu pasirinktas profilis, kuris pagal numatytuosius nustatymus nustatomas kaip **Mano profilis**.

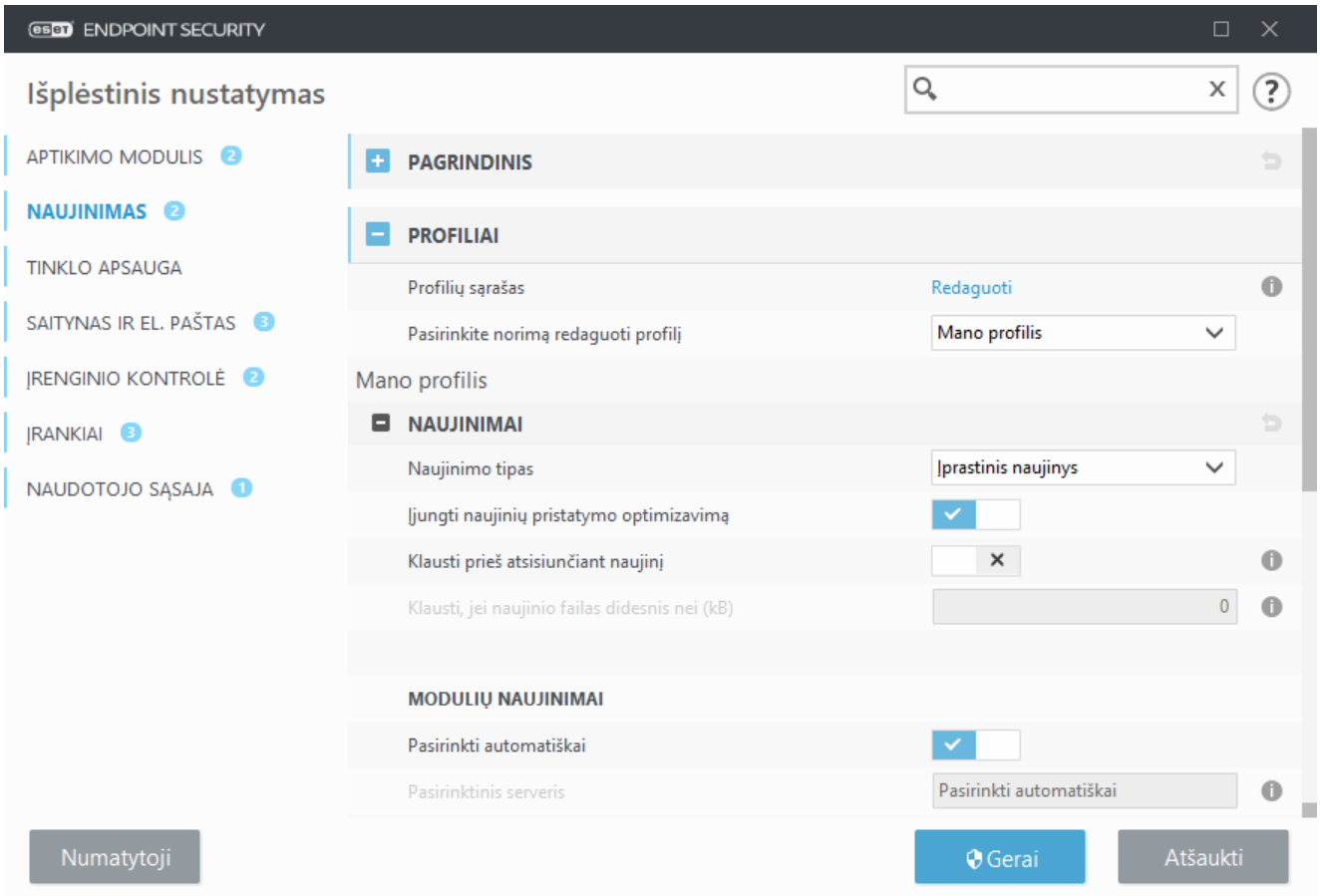
Jei norite sukurti naują profilį, šalia **Profilių sąrašas** spustelėkite **Redaguoti**, įveskite savo **Profilio pavadinimą** ir spustelėkite **Pridėti**.

Naujinimai

Pagal numatytuosius nustatymus nustatyta parinkties Naujinimo tipas vertė yra Reguliarus naujinimas, kad naujinimo failai būtų automatiškai atsisiunčiami iš ESET serverio, kai tinklo srautas mažiausias. Išankstinio leidimo naujinimai (parinktis Išankstinio leidimo naujinimas) yra naujinimai, kuriems atliktas vidinis tikrinimas ir kurie bus greitai pateikti viešai. Įjungę išankstinio leidimo naujinimus galite pasinaudoti jų privalumais, gavę prieigą prie naujausių aptikimo metodų ir taisymų. Tačiau išankstinio leidimo naujinimai gali būti nepakankamai stabilūs visą laiką ir NETURĖTŲ būti naudojami gamybos serveriuose ir kompiuteriuose, kur reikalingas maksimalus prieinamumas ir stabilumas. Uždelstas naujinimas suteikia galimybę naujinti iš specialių naujinimo serverių, teikiančių naujas virusų duomenų bazių versijas su X valandų delsa, t. y. duomenų bazės patikrintos realioje aplinkoje ir dėl to laikomos stabiliomis.

Įjungti naujinių pristatymo optimizavimą – kai įgalinta, atnaujinimo failus galima atsisiųsti iš CDN (turinio teikimo tinklo). Išjungus šį nustatymą atsisiuntimai gali būti pertraukiami ir sulėtėti, kai specialių ESET naujinimo serverių apkrovos per didelės. Išjungti naudinga, kai užkarda leidžia prieigą tik prie ESET naujinimo serverių IP adresų arba kai ryšio su CDN paslaugos neveikia.

Klausti prieš atsisiunčiant naujinimą – programoje bus rodomas pranešimas, kuriame galėsite patvirtinti arba atsisakyti naujinimų failų atsisiuntimo. Jeigu naujinimo failo dydis yra didesnis nei nurodytas lauke Klausti, jeigu naujinimo failas yra didesnis negu (kB), programa rodys patvirtinimo dialogo langą. Jei naujinimo failo dydis yra nustatytas į 0 kB, programa visada rodys patvirtinimo dialogo langą.



Modulių naujinimai

Parinktis **Pasirinkti automatiškai** yra įjungta pagal numatytuosius nustatymus. **Pasirinktinis serveris** yra vieta, kur laikomi naujinimai. Jei naudojate ESET serverį, rekomenduojame palikti įjungtą numatytąją parinktį.

Įjungti dažnesnius aptikimo parašų naujinimus – aptikimo parašai bus naujinami trumpesniais intervalais. Šio

parametro išjungimas gali neigiamai paveikti aptikimo spartą.

Leisti naujinti modulius iš keičiamosios laikmenos – galite naujinti iš nešiojamosios laikmenos, kurioje yra sukurtas veidrodinis atspindys. Pasirinkus Automatinis, naujinimas vyks foniniu režimu. Jeigu norite rodyti naujinimo dialogus, pasirinkite Visada klausti.

Kai naudojate vietinį HTTP serverį, dar vadinamą veidrodžiu, naujinimo serveris turi būti nustatytas taip: *http://kompiuterio_pavadinimas_arba_jo_IP_adresas:2221*

Kai naudojamas vietinis HTTP serveris su SSL, naujinimo serveris turi būti nustatytas taip: *https://kompiuterio_pavadinimas_arba_jo_IP_adresas:2221*

Kai naudojamas vietinis bendrinamas aplankas, naujinimo serveris turi būti nustatytas taip: *\kompiuterio_pavadinimas_arba_jo_IP_adresas\bendrinamas_aplankas*

> HTTP serverio prievado numeris, nurodytas pateiktuose pavyzdžiuose, priklauso nuo to, kokio prievado klausosi jūsų HTTP/HTTPS serveris.

Produkto naujinimai

Žr. Produkto naujinimai.

Ryšio parinktys

Žr. Ryšio parinktys.

Naujinimo veidrodinis atspindys

Žr. Naujinimo veidrodinis atspindys.

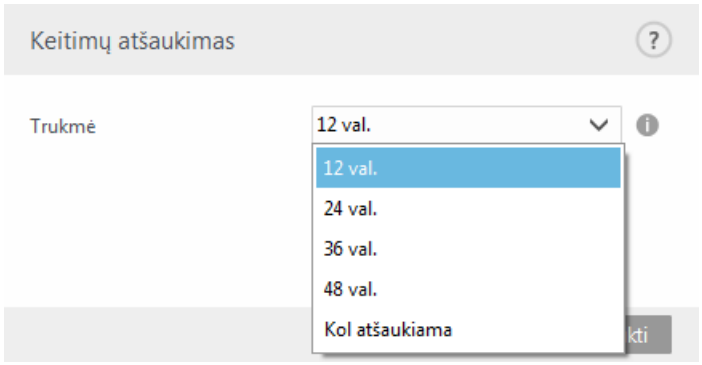
Naujinimo atšaukimas

Jei įtariate, kad naujas aptikimo modulio naujinimas arba programos moduliai gali būti nestabilūs arba sugadinti, galite atšaukti keitimus į ankstesnę versiją ir laikinai išjungti naujinimus. Arba galite įjungti anksčiau išjungtus naujinimus, jeigu atidėjote juos neapibrėžtam laikui.

ESET Endpoint Security įrašo aptikimo modulio ir programos modulių, naudojamų su keitimų atšaukimo funkcija, momentines kopijas. Norėdami sukurti virusų duomenų bazės momentines kopijas, **įjunkite modulių momentines kopijas.** Įgalinus **modulių momentinių kopijų kūrimą,** pirmojo naujinimo metu sukuriama pirmoji momentinė kopija. Kita sukuriama po 48 valandų. Lauke **Vietoje saugomų momentinių kopijų skaičius** apibrėžiamas išsaugotų aptikimo modulio momentinių kopijų skaičius.

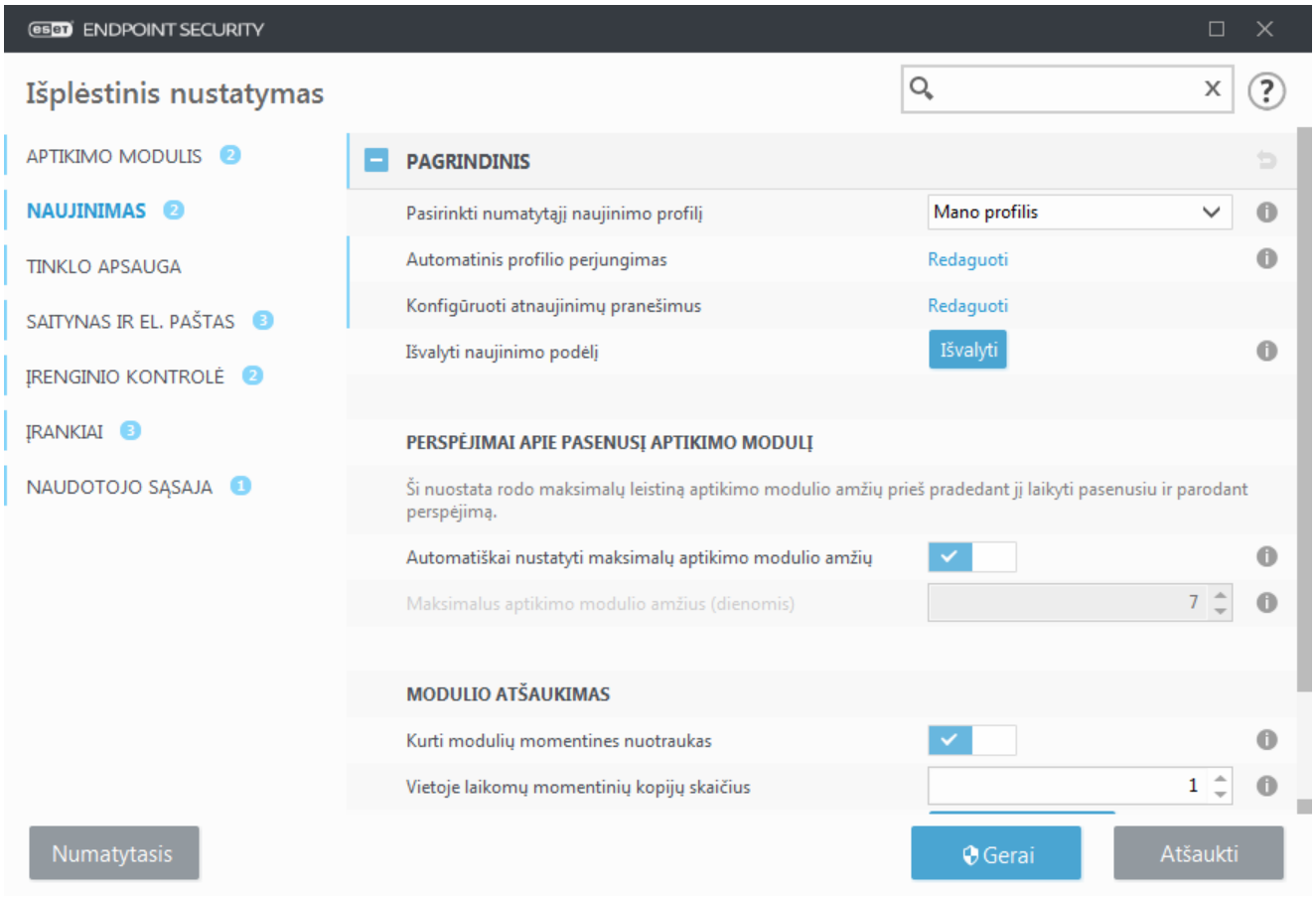
> Pasiekus maksimalų momentinių kopijų kiekį (pvz., tris), seniausia momentinė kopija kas 48 valandas pakeičiama nauja momentinė kopija. ESET Endpoint Security grąžina aptikimo modulio ir programos modulio naujinimo versijas į seniausią momentinę kopiją.

Jei spustelėsite **Grąžinimas** (**Išplėstinė sąranka** (F5) > **Naujinimas** > **Bendra** > **Modulio atšaukimas**), turėsite pasirinkti laiko intervalą iš išskleidžiamojo meniu **Trukmė**.



Pasirinkite **Kol bus atšaukta**, norėdami atidėti reguliarius naujinimus neribotam laikui, kol atkursite naujinimų funkcionavimą rankiniu būdu. Kadangi iškyla galima saugos rizika, mes nerekomenduojame pasirinkti šios parinkties.

Atlikus keitimų atšaukimą, mygtukas **Atšaukti keitimus** pasikeičia į **Leisti naujinimus**. Naujinimai neleidžiami laikotarpiu, kuris buvo pasirinktas iš išskleidžiamojo meniu **Laikinai sustabdyti naujinimai**. Aptikimo modulio versija pakeista į seniausią galimą versiją ir saugoma kaip momentinė kopija vietinio kompiuterio failų sistemoje.



Tarkime, 22700 yra naujausias aptikimo modulio versijos numeris, o 22698 ir 22696 saugomos kaip aptikimo modulio momentinės kopijos. Atminkite, kad 22697 nepasiekiamas. Šiame pavyzdyje kompiuteris buvo išjungtas 22697 naujinimo metu, o naujesnis naujinimas buvo prieinamas prieš atsisiunčiant 22697. Jei lauko vertė **vietoje saugomos momentinės kopijos** yra du ir spustelite **Atšaukti keitimus**, aptikimo modulis (įskaitant programos modulius) atkuriamas į versijos numerį 22696. Šis procesas gali šiek tiek užtrukti. Patikrinkite, ar aptikimo modulio versija sumažinta ekrane Naujinimas.

Produkto naujinimai

Dalyje **Produkto naujinimai** yra parinktys, susijusios su produkto naujinimais. Programa leidžia iš anksto nustatyti jos veiksmus, kai atsiranda naujų produkto naujinimų.

Produkto naujinimai įdiegia naujų funkcijų arba atlieka ankstesnėse versijose buvusių funkcijų pakeitimus. Tai gali būti atliekama automatiškai vartotojui neatliekant jokių veiksmų arba galite pasirinkti, kad jums apie tai praneštų. Įdiegus produkto naujinimus, gali tekti paleisti kompiuterį iš naujo.

Automatiniai atnaujinimai – pristabdžius automatinius konkrečių atnaujinimo profilių atnaujinimus, laikinai išjungiami automatiniai produktų naujiniai, kai prie interneto jungiamasi naudojant kitus tinklus arba apskaičiuotų duomenų ryšius. Palikite šį nustatymą įjungtą, kad galėtumėte nuolat naudotis naujausiomis funkcijomis ir būti kuo geriau apsaugoti. Daugiau informacijos apie automatinius naujinimus ieškokite DUK apie automatinius naujinimus.

Pagal numatytuosius nustatymus produkto naujinimai siunčiami iš ESET saugyklų serverių. Dideliuose arba neprijungtose aplinkose eismą galima išskirstyti, kad būtų galima kaupti viduje produkto failus.

Programos komponentų naujinimo pasirinktinio serverio nurodymas

1. Nurodykite produkto naujinimų kelią lauke **Pasirinktinis serveris**.
Tai gali būti HTTP(S) nuoroda, SMB tinklo bendrinimo kelias, kelias į vietinį diską arba nešiojamąją laikmeną. Tinklo diskų įrenginiams naudokite UNC kelią, o ne susietą disko raidę.
2. Jei nereikia, palikite **Naudotojo vardas** ir **Slaptažodis** neužpildytą.
Jei reikia, čia nustatykite atitinkamus kredencialus, skirtus HTTP autentifikavimui pasirinktiniame žiniatinklio serveryje.
3. Patvirtinkite keitimus ir patikrinkite produkto naujinimus naudodami standartinį ESET Endpoint Security naujinimą.

Tinkamiausios parinkties pasirinkimas priklauso nuo darbo vietos, kurioje šie parametrai bus taikomi. Atsiminkite, kad yra skirtumas tarp darbo vietų ir serverių – pvz., automatiškai paleidus iš naujo serverį po produkto naujinimo, jūsų įmonė gali patirti didelę žalą.

Ryšio parinktys

Norėdami pasiekti duotojo naujinimo profilio įgaliotojo serverio nustatymų parinktis, **Išplėstinių nustatymų** medyje (F5) spustelėkite **Naujinimas**, tada spustelėkite **Profiliai** > **Naujinimai** > **Ryšio parinktys**.

Įgaliotasis serveris

Spustelėkite išskleidžiamąjį meniu **Įgaliotojo serverio režimas** ir nurodykite vieną iš šių trijų parinkčių:

- Nenaudoti įgaliotojo serverio
- Jungtis per įgaliotąjį serverį
- Naudoti visuotinius įgaliotojo serverio parametrus

Pasirinkus **Naudoti visuotinius įgaliotojo serverio parametrus** bus naudojamos įgaliotojo serverio konfigūracijos parinktys, jau nurodytos išplėstinio nustatymo medžio šakoje **Įrankiai** > **Įgaliotasis serveris**.

Pasirinkite **Nenaudoti įgaliotojo serverio** ir nurodykite, kad įgaliotasis serveris nebus naudojamas naujinant ESET

Endpoint Security.

Parinktį **Jungtis per įgaliotąjį serverį** reikia pasirinkti, jeigu:

- Kitas įgaliotasis serveris nei nurodytas Įrankiai > **Įgaliotasis serveris** naudojamas naujinant ESET Endpoint Security. Esant šiai konfigūracijai naujo įgaliojo serverio informaciją reikia nurodyti įvedant **Įgaliotojo serverio** adresą, ryšio **Prievadą** (pagal numatytuosius nustatymus – 3128) ir **Vartotojo vardą** bei **Slaptažodį** (jei reikia).
- Įgaliotojo serverio parametrai nėra nustatyti visuotinai, tačiau ESET Endpoint Security jungsis prie įgaliotojo serverio atliekant naujinimus.
- Jūsų kompiuteris yra prijungtas prie interneto per įgaliotąjį serverį. Parametrai paimami iš naršyklė, kai diegiama programa, tačiau jei jie pakeičiami (pvz., jei pakeičiate interneto paslaugų teikėją), patikrinkite, ar šiame lange išvardyti įgaliotojo serverio parametrai yra teisingi. Kitaip programa negalės prisijungti prie naujinimo serverių.

Numatytasis įgaliotojo serverio nustatymas yra **Naudoti visuotinius įgaliotojo serverio parametrus**.

Jei įgaliotasis serveris nepasiekiamas, naudoti tiesioginį prisijungimą – jei įgaliotasis serveris nepasiekiamas, atliekant naujinimą jis bus apeinamas.

„Windows“ bendrinimai

Naujinant iš vietinio serverio su „Windows NT“ operacinės sistemos versija, pagal numatytuosius nustatymus kiekvienam tinklo ryšiui reikia pritaikyti autentiškumo patvirtinimo procedūrą.

Jei norite sukonfigūruoti tokią paskyrą, išskleidžiamajame meniu pasirinkite **Jungtis prie LAN kaip**:

- **Sistemos paskyra (numatytoji)**,
- **Esamas vartotojas**,
- **Nurodytas vartotojas**.

Pasirinkite **Sistemos paskyra (numatytoji)**, jei norite autentiškumui patvirtinti naudoti sistemos paskyrą. Paprastai atpažinimo procesas nevykdomas, jeigu nėra pateikta atpažinimo duomenų pagrindiniame naujinimo nustatymo skyriuje.

Kad programa vykdytų atpažinimą naudodama šiuo metu prisijungusio vartotojo paskyrą, pasirinkite **Esamas vartotojas**. Šio sprendimo trūkumas yra tai, kad programa negali prisijungti prie naujinimo serverio, jeigu šiuo metu vartotojas nėra prisijungęs.

Pasirinkite **Nurodytas vartotojas**, jeigu norite, kad programa atpažindama naudotų konkretaus vartotojo paskyrą. Naudokite šį metodą, jeigu numatytosios sistemos paskyros prisijungimas nepavyko. Atsiminkite, kad nurodyto vartotojo paskyra turi turėti prieigą prie naujinimo failų katalogo vietiniame serveryje. Kitaip programa negalės užmegzti ryšio ir atsisiųsti naujinimų.

Parametrai **Vartotojo vardas** ir **Slaptažodis** yra nebūtini.

⚠ pasirinkus **Esamas vartotojas** arba **Nurodytas vartotojas**, gali įvykti klaida keičiant programos tapatumą į norimą vartotoją. Mes rekomenduojame įvesti LAN atpažinimo duomenis pagrindiniame naujinimo nustatymo skyriuje. Šiame naujinimo nustatymo skyriuje atpažinimo duomenys turi būti įvesti taip: *domeno_pavadinimas**vartotojas* (jeigu tai darbo grupė, įveskite *darbo_grupės_pavadinimas**pavadinimas*) ir slaptažodis. Kai naujinama iš vietinio serverio HTTP versijos, atpažinimas nereikalingas.

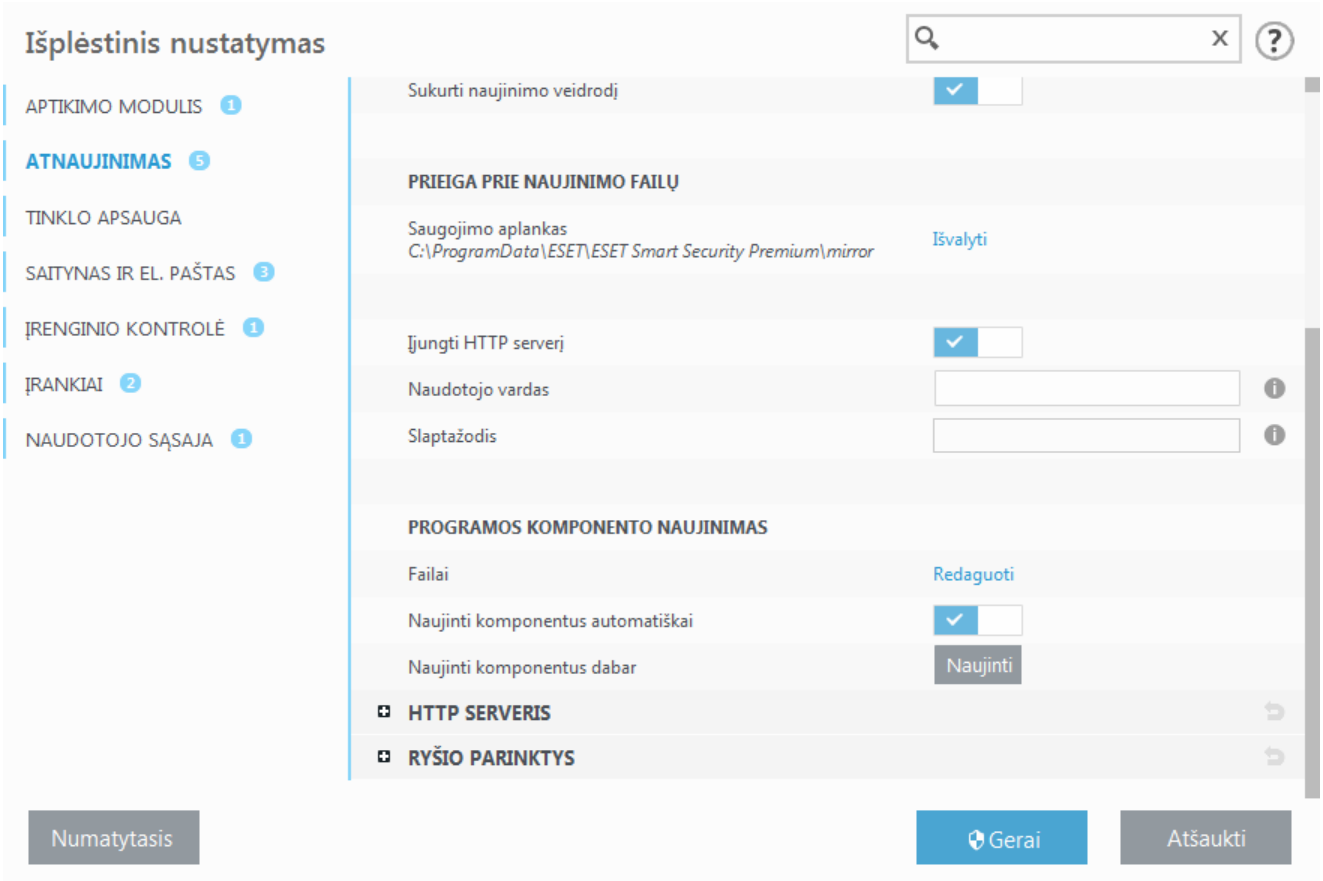
Pasirinkite atnaujinus **Atsijungti** nuo serverio, kad priverstinai atsijungtumėte, jeigu ryšys su serveriu lieka aktyvus net atsisiuntus naujinimus.

Naujinimo veidrodinis atspindys

ESET Endpoint Security leidžia sukurti naujinimų failų kopijas, kurias bus galima naudoti kitoms tinkle esančioms darbo vietoms naujinti. Veidrodinio atspindžio naudojimas – naujinimo failų kopija LAN aplinkoje yra patogi, nes naujinimo failų nereikia nuolatos atsisiuntinėti iš tiekėjo serverio naudojant darbo vietą. Naujinimai centralizuotai atsisiunčiami į vietinį serverio veidrodinį atspindį, tada paskirstomi visoms darbo vietoms, todėl išvengiama tinklo srauto perkrovos pavojaus. Naujinant klientų darbo vietas iš veidrodinio atspindžio, optimizuojamas tinklo apkrovos pasiskirstymas ir sumažinamas interneto srautas.

> Siekiant sumažinti interneto srautą tinkluose, kuriuose ESET PROTECT naudojama valdyti daugelį klientų, rekomenduojame naudoti „Apache“ HTTP tarpinį serverį, o ne konfigūruoti klientą kaip veidrodį. „Apache“ HTTP tarpinį serverį galima įdiegti su ESET PROTECT naudojant „viskas viename“ diegimo programą arba kaip atskirą komponentą. Daugiau informacijos ir skirtumų tarp „Apache“ HTTP tarpinio serverio, veidrodžio įrankio ir tiesioginio ryšio ieškokite mūsų ESET PROTECT internetinio žinyno puslapyje.

Vietinio serverio veidrodinio atspindžio konfigūracijos parinktys pasiekiamos išplėstiniuose nustatymuose dalyje **Naujinimas**. Jei norite pasiekti šį skirsnį, paspauskite **F5**, kad būtų atidarytas meniu Išplėstiniai nustatymai, tada spustelėkite **Naujinimas** > **Profiliai ir išplėskite Naujinti veidrodinį atspindį**.



Jei norite sukurti veidrodinį atspindį kliento darbo vietoje, įjunkite **Kurti naujinimo veidrodinį atspindį**. Įjungus šią parinktį, suaktyvinamos kitos veidrodinio atspindžio konfigūracijos parinktys, pvz., naujinimo failų pasiekimo būdas ir kelias į veidrodinio atspindžio failus.

Prieiga prie naujinimo failų

Įjungti HTTP serverį – jeigu įjungta, naujinimo failus galima pasiekti per HTTP, o kredencialų pateikti nereikės.

Serverio veidrodinio atspindžio prieigos metodai išsamiai aprašomi skyriuje Naujinimas iš veidrodinio atspindžio. Yra du baziniai būdai veidrodiniam atspindžiui pasiekti – aplankas su naujinimo failais gali būti pateiktas kaip bendrinamas tinklo aplankas arba klientai gali pasiekti veidrodinį atspindį, esantį HTTP serveryje.

Aplankas, skirtas veidrodinio atspindžio naujinimo failams saugoti, yra apibrėžtas skyriuje **Aplankas veidrodinio atspindžio failams saugoti**. Jei norite pasirinkti kitą aplanką, spustelėkite **Išvalyti**, kad panaikintumėte iš anksto nustatytą aplanką *C:\ProgramData\ESET\ESET Endpoint Security\mirror* ir spustelėkite **Redaguoti**, kad kompiuteryje susirastumėte vietinį arba bendrinamą tinklo aplanką. Jei reikalinga tam tikro aplanko autorizacija, į laukus **Vartotojo vardas** ir **Slaptažodis** reikia įvesti autentiškumo patvirtinimo duomenis. Jeigu pasirinktas paskirties aplankas yra tinklo diske, kuriame įdiegta operacinė sistema „Windows NT“ / 2000 / XP, nurodytas vartotojo vardas ir slaptažodis turi turėti teisę rašyti į pasirinktą aplanką. Vartotojo vardas ir slaptažodis turi būti įvesti formatu *Domenas/Vartotojas* arba *Darbo_grupė/Vartotojas*. Nepamirškite pateikti atitinkamų slaptažodžių.

Veidrodžio HTTP serveris ir SSL

Skirtuko **Veidrodis** skyriuje **HTTP serveris** galite nurodyti **serverio prievadą,** kuriame klausysis HTTP serveris, taip pat HTTP serverio naudojamą **autentifikavimo** tipą. Pagal numatytuosius nustatymus serverio prievadas nustatytas kaip **2221**.

Autentiškumo patvirtinimas – apibrėžia autentiškumo patvirtinimo būdą, naudojamą prieigai prie naujinimo failų. Galimos šios parinktys: **Nėra**, **Bazinis** ir **NTLM**. Pasirinkite **Bazinis**, norėdami naudoti „base64“ koduotę su baziniu autentiškumo patvirtinimo būdu per vartotojo vardą ir slaptažodį. Parinktis **NTLM** skirta koduoti naudojant saugų kodavimo metodą. Čia patvirtinamas vartotojo, sukurto darbo vietoje, kurioje bendrinami naujinimo failai, autentiškumas. Numatytasis nustatymas yra **Nėra**, kuris suteikia prieigą prie naujinimo failų nereikalaujant pateikti atpažinimo duomenų.

Autentifikavimo duomenys, pvz., **Vartotojo vardas** ir **Slaptažodis**, skirti tik prieigai prie veidrodžio HTTP serverio. Užpildykite šiuos laukus tik tuo atveju, jei vartotojo vardas ir slaptažodis yra būtini.

Prijunkite savo **Sertifikato grandinės failą** arba sugeneruokite vartotojo pasirašomą sertifikatą, jeigu norite paleisti HTTP serverį su HTTPS (SSL) palaikymu. Galimi tokie **sertifikatų tipai**: ASN, PEM ir PFX. Siekiant užtikrinti papildomą saugumą, naujinimo failams atsisiųsti galima naudoti HTTPS protokolą. Naudojant šį protokolą, beveik neįmanoma atsekti duomenų persiuntimo ir prisijungimo kredencialų. Parinktis **Privataus rakto tipas** pagal numatytuosius nustatymus yra nustatyta kaip **Integruota** (todėl parinktis **Privataus rakto failas** pagal numatytuosius nustatymus yra išjungta). Vadinasi, privatus raktas yra pasirinkto sertifikatų grandinės failo dalis.

Savarankiškai pasirašyti HTTPS veidrodžio sertifikatai
Jei naudojate HTTPS veidrodžio serverį, turite importuoti jo sertifikatą į patikimą šakninę saugyklą visuose kliento įrenginiuose. Žr. Patikimo šakninio sertifikato diegimas sistemoje „Windows“.

Naujinimas iš veidrodinio atspindžio

Yra du pagrindiniai būdai, kuriuos naudodami galite sukurti veidrodinį atspindį – iš esmės saugyklą, iš kurios klientai gali atsisiųsti naujinimo failus. Aplankas su naujinimo failais gali būti pateikiamas kaip bendrinamas tinklo

aplankas arba HTTP serveris.

Prieiga prie veidrodinio atspindžio naudojant vidinį HTTP serverį

Ši konfigūracija yra numatytoji, nurodyta iš anksto nustatytoje programos konfigūracijoje. Kad galėtumėte pasiekti veidrodinį atspindį per HTTP serverį, eikite į „**Advanced setup**“ (išplėstiniai nustatymai) > „**Update**“ (naujinti) > „**Profiles**“ (profiliai) > „**Naujinimo veidrodis**“ (veidrodinis atspindys) ir pasirinkite „**Create update mirror**“ (sukurti naujinimo veidrodinį atspindį).

Skirtuko **Veidrodis** skyriuje **HTTP serveris** galite nurodyti **serverio prievadą,** kuriame klausysis HTTP serveris, taip pat HTTP serverio naudojamą **autentifikavimo** tipą. Pagal numatytuosius nustatymus serverio prievadas nustatytas kaip **2221**.

Autentiškumo patvirtinimas – apibrėžia autentiškumo patvirtinimo būdą, naudojamą prieigai prie naujinimo failų. Galimos šios parinktys: **Nėra**, **Bazinis** ir **NTLM**. Pasirinkite **Bazinis**, norėdami naudoti „base64“ koduotę su baziniu autentiškumo patvirtinimo būdu per vartotojo vardą ir slaptažodį. Parinktis **NTLM** skirta koduoti naudojant saugų kodavimo metodą. Čia patvirtinamas vartotojo, sukurto darbo vietoje, kurioje bendrinami naujinimo failai, autentiškumas. Numatytasis nustatymas yra **Nėra**, kuris suteikia prieigą prie naujinimo failų nereikalaujant pateikti atpažinimo duomenų.

jeigu norite leisti prieigą prie naujinimo failų per HTTP serverį, veidrodinio atspindžio aplankas turi būti tame pačiame kompiuteryje, kaip ir jį sukūręs ESET Endpoint Security egzempliorius.

Po kelių nesėkmingų bandymų atnaujinti iš veidrodžio pagrindinio meniu naujinimo polangyje pasirodys klaidos pranešimas **Netinkamas vartotojo vardas ir (arba) slaptažodis**. Rekomenduojame eiti į **Išplėstinis nustatymas** > **Naujinimas** > **Profiliai** > **Naujinimo veidrodis** ir patikrinti vartotojo vardą bei slaptažodį. Dažniausiai pasitaikanti šios klaidos priežastis yra neteisingai įvesti atpažinimo duomenys.

Sukonfigūravus veidrodžio serverį, galima klientų kompiuteriuose pridėti naują naujinimo serverį. Tam atlikite šiuos veiksmus:

- **Eikite į Išplėstinis nustatymas** (F5) ir spustelėkite **Naujinimas** > **Profiliai** > **Naujinimai** > **Modulių naujinimai**.
- Išjunkite **Pasirinkti automatiškai** ir lauke **Naujinimo serveris** pridėkite naują serverį naudodami vieną iš šių formatų:
  http://jūsų_serverio_IP_adresas:2221
  https://jūsų_serverio_IP_adresas:2221 (jei naudojamas SSL)

Prieiga prie veidrodinio atspindžio per sistemos bendrinimus

Pirmiausia vietiniame arba tinklo įrenginyje reikia sukurti bendrinimo aplanką. Kurdami aplanką veidrodiniam atspindžiui, turite suteikti „rašymo“ prieigą vartotojui, kuris įrašys naujinimo failus į aplanką, ir „skaitymo“ prieigą visiems vartotojams, kurie vykdys ESET Endpoint Security naujinimus iš veidrodinio atspindžio aplanko.

Tai atliekama skirtuke **Išplėstiniai nustatymai** > **Naujinimas** > **Profiliai** > **Naujinimo veidrodis** išjungiant punktą **Įjungti HTTP serverį**. Ši parinktis yra įjungta pagal numatytuosius nustatymus programos diegimo pakete.

Jeigu bendrinimo aplankas yra kitame tinklo kompiuteryje, turite įvesti autentiškumo patvirtinimo duomenis, leidžiančius prieigą prie kito kompiuterio. Norėdami įvesti autentiškumo patvirtinimo duomenis, atverkite ESET Endpoint Security **Išplėstiniai nustatymai** (**F5**) ir spustelėkite **Naujinimas** > **Profiliai** > **Naujinimai** > **Ryšio parinktys** > **„Windows“ bendrinimai** > **Jungtis prie LAN kaip**. Naudojamas toks pat parametras kaip ir naujinant: žr.

aprašymą skyriuje Jungtis prie LAN kaip.

Norint atidaryti veidrodinio atspindžio aplanką, tai turi būti padaryta toje pačioje paskyroje, kuri naudojama prisijungiant prie kompiuterio, kuriame sukurtas veidrodinis atspindys. Jei kompiuteris yra domene, turėtų būti naudojamas vartotojo vardas „domenas\vartotojas“. Jei kompiuteris ne domene, turėtų būti naudojama „jūsų_serverio_IP_adresas\vartotojas“ arba „pagrindiniokompiuteriopavadinimas\vartotojas“.

Baigę konfigūruoti veidrodį, klientų kompiuteriuose naujinimo serveriu nustatykite *UNC**PATH*, atlikdami toliau nurodytus veiksmus:

1. Atidarykite ESET Endpoint Security **Išplėstiniai nustatymai** ir spustelėkite **Naujinimas** > **Profiliai** > **Naujiniai**.
2. Išjunkite **Pasirinkti automatiškai** šalia **Modulių naujinimai** ir pridėkite naują serverį prie lauko **Naujinimo serveris**, laikydamiesi formato *UNC**PATH*.

Kad naujinimai tinkamai veiktų, kelias į veidrodinio atspindžio aplanką turi būti nurodytas kaip UNC kelias. Naujinimai iš susietų įrenginių gali neveikti.

Veidrodinio atspindžio kūrimas, naudojant Veidrodžių įrankį
Veidrodžių įrankis sukuria aplankų struktūrą, kuri atlieka kitas funkcijas nei „Endpoint“ veidrodinis atspindys. Kiekviename aplanke yra naujinimo failai grupei produktų. Turite nurodyti visą kelią iki tinkamo aplanko produkto, kuris naudoja veidrodinį atspindį naujinimo nustatymuose.
Pavyzdžiui, norėdami naujinti ESET PROTECT iš veidrodinio atspindžio, nustatykite Naujinimo serveris į (pagal jūsų HTTP serverio pagrindinę vietą):
`http://your_server_address/mirror/eset_upd/era6`

Paskutinis skyrius valdo programos komponentus (PCU). Pagal numatytuosius nustatymus atsisiųsti programos komponentai būna paruošti kopijuoti į vietinį veidrodinį atspindį. Jei suaktyvinate parinktį **Produkto naujinimai**, visiškai nereikia spustelėti **Naujinti**, nes failai į vietinį veidrodinį atspindį nukopijuojami automatiškai, kai tik tampa prieinami. Žiūrėkite Naujinimo režimas norėdami rasti daugiau informacijos apie produkto naujinimus.

Veidrodžio naujinimo trikčių šalinimas

Daugeliu atvejų problemas naujinant veidrodžio serverį sukelia viena arba kelios priežastys: netinkamos veidrodinio atspindžio aplanko parinkčių specifikacijos, netinkami veidrodinio atspindžio aplanko autentiškumo patvirtinimo duomenys, netinkama vietinių darbo vietų, bandančių atsisiųsti naujinimo failus iš veidrodinio atspindžio, konfigūracija arba kelios iš pirmiau paminėtų priežasčių. Toliau apžvelgiamos dažniausiai pasitaikančios problemos, kurių gali kilti naujinant iš veidrodinio atspindžio:

ESET Endpoint Security praneša apie klaidas jungiantis prie veidrodžio serverio – greičiausiai įvyko dėl netinkamų naujinimo serverio (tinklo kelio į veidrodinio atspindžio aplanką), iš kurio vietinės darbo vietos atsisiunčia naujinimus, specifikacijų. Norėdami patikrinti aplanką, spustelėkite „Windows“ meniu **Pradėti**, spustelėkite **Vykdyti**, įveskite aplanko pavadinimą ir spustelėkite **Gerai**. Turi būti rodomas aplanko turinys.

ESET Endpoint Security reikalauja vartotojo vardo ir slaptažodžio – greičiausiai įvyko dėl netinkamų autentiškumo patvirtinimo duomenų (vartotojo vardo ir slaptažodžio) naujinimo skyriuje. Vartotojo vardas ir slaptažodis yra reikalingi siekiant suteikti prieigą prie naujinimo serverio, iš kurio programa pati atsinaujina. Įsitikinkite, kad autentiškumo patvirtinimo duomenys yra teisingi ir įvesti teisingu formatu. Pavyzdžiui, Domenas/Vardas arba Darbo_grupė/Vardas ir atitinkami slaptažodžiai. Jei veidrodžio serveris yra pasiekiamas „Visiems“, atminkite, kad tai nereiškia, jog kiekvienam vartotojui suteikiama prieiga. „Visiems“ nereiškia visų neįgaliotų vartotojų, tai tiesiog reiškia, kad aplankas yra pasiekiamas visiems domeno vartotojams. Todėl, jeigu aplankas yra pasiekiamas „Visiems“, domeno vartotojo vardas ir slaptažodis vis tiek bus reikalingi, kad

patektumėte į naujinimo nustatymų skyrių.

ESET Endpoint Security praneša apie klaidą jungiantis prie veidrodžio serverio – ryšys su prievadu, skirtu jungtis prie veidrodžio HTTP versijos, yra užblokuotas.

„**ESET Endpoint Security“ praneša apie klaidą atsisiunčiant naujinimo failus** – ji greičiausiai įvyko dėl netinkamų naujinimo serverio (tinklo kelio į veidrodinio atspindžio aplanką), iš kurio vietinės darbo vietos atsisiunčia naujinimus, specifikacijų.

Kaip sukurti naujinimo užduotis

Naujinimus galima paleisti rankiniu būdu spustelėjus **Ieškoti naujinimų** pradiniame lange, kuris parodomas pagrindiniame meniu spustelėjus **Naujinimas**.

Naujinimus galima vykdyti ir kaip suplanuotas užduotis. Norėdami konfigūruoti suplanuotą užduotį, spustelėkite **Įrankiai** > **Planuoklė**. Pagal numatytuosius nustatymus programoje ESET Endpoint Security yra suaktyvintos šios užduotys:

- **Reguliarus automatinis naujinimas**
- **Automatinis naujinimas prisijungus telefono ryšiu**
- **Automatinis naujinimas prisiregistravus vartotojui**

Kiekvieną naujinimo užduotį galima pakeisti pagal savo poreikius. Šalia numatytųjų naujinimo užduočių galite kurti naujas naujinimo užduotis su vartotojo apibrėžta konfigūracija. Daugiau informacijos apie naujinimo užduočių kūrimą ir konfigūravimą rasite skyriuje Planuoklė.

Įrankiai

Įrankių meniu pateikiami moduliai, palengvinantys programos administravimą ir siūlantys papildomas parinktis patyrusiems vartotojams.

Šiame meniu yra tokie įrankiai:

- Žurnalo failai
- Vykdomi procesai (jei ESET LiveGrid® yra įjungtas produkte ESET Endpoint Security)
- Saugumo ataskaita (nevaldomiesiems įrenginiams)
- Tinklo ryšiai (jei Užkarda įjungta ESET Endpoint Security)
- Saugi naršyklė (išjungta pagal ESET Endpoint Security numatytuosius nustatymus)
- ESET SysInspector
- Planuoklė
- „ESET SysRescue Live“ – Nukreipia jus į „ESET SysRescue Live“ svetainę, kurioje galima atsisiųsti „ESET SysRescue Live“ .iso CD/DVD atvaizdą.
- Pavyzdžio pateikimas siekiant atlikti analizę – suteikia galimybę pateikti įtartiną failą analizuoti ESET virusų laboratorijai (gali būti nepasiekiama atsižvelgiant į ESET LiveGrid® konfigūraciją).
- Karantinas



Žurnalo failai

Žurnalų failuose pateikiama informacija apie visus svarbius programos įvykius ir aptiktų grėsmių apžvalga. Žurnalai yra esminis sistemos analizės, grėsmių aptikimo ir trikčių šalinimo įrankis. Registravimas aktyviai atliekamas foniniu režimu, be vartotojo veiksmų. Informacija įrašoma remiantis esamais žurnalas daugiažodiškumo parametrais. Teksto pranešimus ir žurnalus galima peržiūrėti tiesiogiai ESET Endpoint Security aplinkoje. Be to, žurnalų failus galima archyvuoti.

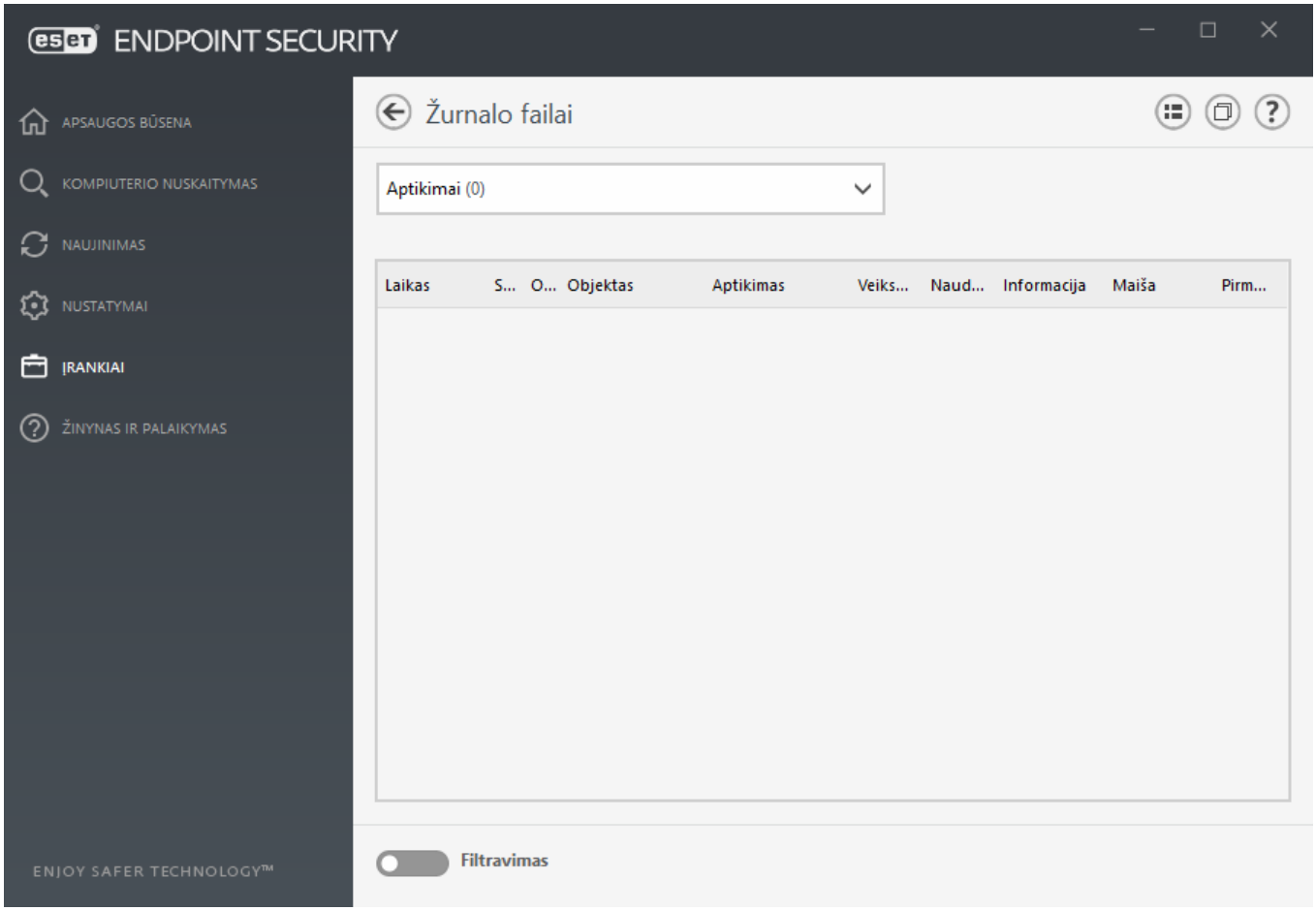
Žurnalo failus galima pasiekti programos lange spustelėjus **Įrankiai** > **Žurnalo failai**. Pasirinkite norimą žurnalo tipą iš išskleidžiamojo meniu **Žurnalas**. Galimi šie žurnalai:

- **Aptikimai** – šiame žurnale pateikiama išsami informacija apie aptikimus ir įsiskverbimus, kuriuos aptiko ESET Endpoint Security moduliai. Informaciją sudaro aptikimo laikas, aptikimo pavadinimas, vieta, atliktas veiksmas ir vartotojo, kuris buvo prisijungęs, kai įsiskverbimas buvo aptiktas, vardas. Dukart spustelėkite žurnalo įrašą, kad atskirame lange būtų rodoma išsami jo informacija. Neišvalyti įsiskverbimai visada pažymimi raudonu tekstu šviesiai raudoname fone, išvalyti įsiskverbimai pažymimi geltonu tekstu baltame fone. Neišvalytos PUA arba neišvalytos galimai nesaugios programos pažymimos geltonu tekstu baltame fone.
- **Įvykiai** – visi svarbūs veiksmai, kuriuos atliko ESET Endpoint Security, įrašomi įvykių žurnaluose. Įvykių žurnale pateikiama informacija apie įvykius ir klaidas, kurios įvyko programoje. Jis skirtas padėti sistemos administratoriams ir vartotojams spręsti problemas. Dažnai čia esanti informacija gali padėti rasti programoje iškilusios problemos sprendimą.
- **Kompiuterio nuskaitymas** – šiame lange pateikiami visi nuskaitymo rezultatai. Kiekviena eilutė atitinka vieną kompiuterio tikrinimą. Dukart spustelėję bet kurį įrašą, galite peržiūrėti atitinkamo nuskaitymo išsamią informaciją.

- **Užblokuoti failai** – failų, kurie buvo užblokuoti ir yra nepasiekiami prisijungus prie ESET Enterprise Inspector, įrašai. Protokole nurodyta priežastis ir pirminis modulis, kuris užblokavo failą, o taip pat programa ir naudotojas, kuris vykdė failą. Daugiau informacijos rasite ESET Enterprise Inspector internetiniame naudotojo vadove.
- **Nusiųsti failai** – sudaro įrašai failų, kurie buvo nusiųsti ESET LiveGrid® arba ESET LiveGuard analizei.
- **Audito žurnalai** – kiekvieną žurnalą sudaro informacija apie datą ir laiką, kada buvo atliktas pakeitimas, pakeitimo tipas, aprašas, šaltinis ir naudotojas. Jei reikia papildomos informacijos, žr. Audito žurnalai.
- **HIPS** – jį sudaro konkrečių taisyklių, kurios buvo nurodytos registruoti, įrašai. Protokole nurodyta programa, kuri iškvietė operaciją, rezultatas (ar taisyklė buvo leidžiama, ar draudžiama) ir sukurtos taisyklės pavadinimas.
- **Tinklo apsauga** – Užkardos žurnale pateikiamos aptiktos nuotolinės atakos, kurias aptiko Apsauga nuo atakos iš tinklo arba Užkarda. Čia jūs rasite informacijos apie visas atakas, vykdytas prieš jūsų kompiuterį. Skiltyje Įvykis pateikiamos aptiktos atakos. Skiltyje Šaltinis pateikiama daugiau informacijos apie įsilaužėlį. Skiltyje Protokolas nurodomas ryšio protokolas, kuris buvo naudojamas atakuojant. Tinklo apsaugos žurnalo analizė gali padėti laiku aptikti įsiskverbimų į sistemą bandymus ir užkirsti kelią neįgaliotai prieigai prie jūsų sistemos. Daugiau informacijos apie tam tikras tinklo atakas rasite skyriuje IDS ir išplėstinės parinktys.

- **Filtruojamos svetainės** – Šis sąrašas naudingas pageidaujant peržiūrėti sąrašą interneto svetainių, kurias užblokavo prieigos prie saityno apsauga arba saityno kontrolė. Šiuose žurnaluose galite matyti laiką, URL, vartotoją ir programą, kuri užmezgė ryšį su tam tikra interneto svetaine.

- **Apsauga nuo brukalo** – ją sudaro įrašai, susiję su el. laiškais, kurie buvo pažymėti kaip brukalas.
- **Saityno kontrolė** – rodo užblokuotus arba leidžiamus URL adresus ir pateikia išsamios informacijos apie tai, kaip jie skirstomi į kategorijas. Stulpelyje Atliktas veiksmas nurodyta, kaip buvo pritaikytos filtravimo taisyklės.
- **Įrenginio kontrolė** – turi įrašus apie nešiojamąsias laikmenas arba įrenginius, kurie buvo prijungti prie kompiuterio. Į žurnalo failą bus įrašyti tik įrenginiai su įrenginio kontrolės taisykle. Jeigu taisyklė neatitinka prijungto įrenginio, žurnalo įrašas apie prijungtą įrenginį nebus sukurtas. Be to, čia galite peržiūrėti tokią išsamią informaciją kaip įrenginio tipas, serijos numeris, tiekėjo pavadinimas ir laikmenos dydis (jei yra).



Pasirinkite žurnalo turinį ir paspauskite `Ctrl + C` **, kad nukopijuotumėte jį į iškarpinę**. Laikydami `Ctrl + Shift` pasirinkite kelis elementus.

Spustelėkite **Filtravimas**, kad būtų atidarytas langas Žurnalo filtravimas, kuriame galima apibrėžti filtravimo kriterijus.

Dešiniuoju pelės mygtuku spustelėkite įrašą, kad būtų atidarytas kontekstinis meniu. Galimos šios parinktys kontekstiniame meniu:

- **Rodyti** – naujame lange pateikia išsamesnės informacijos apie pasirinktą žurnalą.
- **Filtruoti tuos pačius įrašus** – suaktyvinę šį filtrą, matysite tik to paties tipo įrašus (diagnostika, įspėjimai...).
- **Filtruoti** – spustelėję šią parinktį, lange Žurnalo filtravimas galėsite apibrėžti konkrečių žurnalo įrašų filtravimo kriterijus.
- **Įjungti filtrą** – suaktyvina filtro parametrus.
- **Išjungti filtrą** – panaikina visus filtro nustatymus (kaip aprašyta anksčiau).
- **Kopijuoti / kopijuoti viską** – kopijuoja informaciją apie visus įrašus lange.
- **Naikinti / naikinti viską** – panaikina pasirinktą (-us) įrašą (-us) arba visus rodomus įrašus – šiam veiksmui reikalingos administratoriaus teisės.
- **Eksportuoti** – eksportuoja informaciją apie įrašą (-us) XML formatu.
- **Eksportuoti viską** – informacija apie visus įrašus eksportuojama XML formatu.
- **Rasti / Rasti kitą / Rasti ankstesnį** – spustelėję šią parinktį, lange „Žurnalo filtravimas“ galėsite apibrėžti filtravimo kriterijus, kad būtų pažymėtas konkretus įrašas.
- **Kurti išimtį** – sukurti naują aptikimo išimtį, naudojant vedlį (negalima kenkėjiškos programinės įrangos aptikimui).

Žurnalo filtravimas

Spustelėkite **Filtravimas** dalyje **Įrankiai** > **Žurnalo failai** filtravimo kriterijams apibrėžti.

Žurnalo filtravimo funkcija padės rasti ieškomos informacijos, ypač, kai turite daugybę įrašų. Ji padeda susiaurinti žurnalo įrašų paiešką, pvz., jei ieškote konkretaus tipo įvykio, būsenos arba laikotarpio. Galite filtruoti žurnalo įrašus nurodydami konkrečias paieškos parinktis, kad lange žurnalo failai būtų rodomi tik aktualūs įrašai (atsižvelgiant į paieškos parinktis).

Įveskite ieškomą raktažodį į laukelį **Rasti tekstą**. Paieškai susiaurinti naudokite išskleidžiamąjį meniu **Ieškoti stulpeliuose**. Pasirinkite bent vieną įrašą išskleidžiamajame meniu **Įrašų žurnalų tipai**. Nurodykite **Laikotarpį** kurio rezultatus norite matyti. Taip pat galite naudoti kitas paieškos parinktis, pvz., **Ieškoti tik viso žodžio** arba **Skirti didžiąsias ir mažąsias raides**.

Rasti tekstą

Įveskite eilutę (žodį arba žodžio dalį). Bus rodomi tik įrašai, kuriuose yra ši eilutė. Kiti įrašai nebus rodomi.

Ieškoti stulpeliuose

Pasirinkite, kuriuos stulpelius įtraukti į paiešką. Galite pažymėti vieną ar daugiau stulpelių, kad jie būtų naudojami paieškoje.

Įrašų tipai

Pasirinkite vieną arba daugiau žurnalų įrašų tipų iš išskleidžiamojo meniu:

- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau paminėtus įrašus.
- **Informacija** – įrašo informacinius pranešimus, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – įrašo kritines klaidas ir įspėjimo pranešimus.
- **Klaidos** – įrašomos klaidos, pvz., „Klaida atsiunčiant failą“, ir kritinės klaidos.
- **Kritinės** – registruoja tik kritines klaidas (klaida paleidžiant apsaugą nuo virusų

Laikotarpis

apibrėžkite laikotarpį, kurio rezultatus norite peržiūrėti:

- **Nenurodytas** (numatytasis) – neieškoma konkretaus laikotarpio, ieškoma visame žurnale.
- **Paskutinė diena**
- **Paskutinė savaitė**
- **Paskutinis mėnuo**
- **Laikotarpis** – galite nurodyti konkretų laikotarpį (Nuo: ir Iki:), kad filtruotumėte tik konkretaus laikotarpio įrašus.

Ieškoti tik viso žodžio

Jei norite ieškoti viso žodžio, pasirinkite šį žymės langelį, kad būtų parodyti tikslesni rezultatai.

Skirti didžiąsias ir mažąsias raides

Įjunkite šią parinktį, jei jums svarbu skirti didžiąsias ir mažąsias raides filtruojant. Kai sukonfigūruosite savo filtravimo / paieškos parinktis, spustelėkite **Gerai**, kad būtų rodomi filtruojami žurnalo įrašai arba Rasti, kad pradėtumėte paiešką. Žurnalo failų ieškoma nuo viršaus į apačią, pradedant nuo dabartinės vietos (paryškinto įrašo). Paieška sustoja, kai randamas pirmasis atitinkamas įrašas. Paspauskite **F3**, kad ieškotumėte kito įrašo arba spustelėkite dešiniuoju pelės mygtuku ir pasirinkite **Rasti**, kad patikslintumėte paieškos parinktis.

Prisijungimo konfigūracija

ESET Endpoint Security Registravimo konfigūravimas galimas pagrindiniame programos lange. Spustelėkite **Nustatymai** > **Išplėstiniai nustatymai** > **Įrankiai** > **Žurnalo failai**. Žurnalų skyrius yra skirtas apibrėžti, kaip bus tvarkomi žurnalo įrašai. Programa automatiškai naikina senesnius žurnalo įrašus, kad būtų taupoma vieta diske. Galite žurnalo failams nurodyti šias parinktis:

Minimalus registravimo daugiažodiškumas – nurodo minimalų įvykių daugiažodiškumo lygį, kai jie registruojami:

- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau paminėtus įrašus.
- **Informacija** – įrašo informacinius pranešimus, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – įrašo kritines klaidas ir įspėjimo pranešimus.
- **Klaidos** – įrašomos klaidos, pvz., „Klaida atsiunčiant failą“, ir kritinės klaidos.
- **Kritinės** – registruoja tik kritines klaidas (klaida paleidžiant apsaugą nuo virusų, integruotą užkardą ir t. t.).

Kai pasirinktas daugiažodiškumo lygis „**Diagnostinis**“, užregistruojami visi užblokuoti ryšiai.

Žurnalo įrašai, senesni nei lauke **Naikinti senesnius nei (dienų) įrašus** nurodytas dienų skaičius, bus automatiškai panaikinti.

Optimizuoti žurnalo failus automatiškai – įjungus šį punktą, žurnalo failai bus automatiškai defragmentuojami, jei procentinė vertė bus didesnė nei lauke **Jeigu nenaudojamų įrašų skaičius viršija (%)** nurodyta vertė.

Jei norite pradėti žurnalo failų defragmentavimą, spustelėkite **Optimizuoti**. Tušti žurnalo įrašai pašalinami, kad padidėtų našumas ir žurnalo apdorojimo sparta. Šis darbo paspartėjimas ypač akivaizdus, jei žurnaluose yra daug įrašų.

Parinktis **Įjungti teksto protokolą** suteikia galimybę žurnalus saugoti kitu failo formatu (atskirai nuo žurnalo failų):

- **Tikslinis aplankas** – čia galima pasirinkti aplanką, kuriame bus laikomi žurnalo failai (taikoma tik tekstui / CSV). Nukopijuoti kelią arba pasirinkti kitą aplanką galite spustelėję **Išvalyti**. Kiekvienas žurnalo skyrius turi savo failą su iš anksto apibrėžtu failo pavadinimu (pvz., jei žurnalams saugoti naudojate paprasto teksto failų formatą, *virlog.txt* skirtas žurnalo failų skyriui **Aptiktos grėsmės**).
- **Tipas** – jei pasirinkote failų formatą **Tekstas**, žurnalai bus saugomi teksto faile, o duomenys bus atskiriami tabuliacijos ženklais. Tai pat taikoma kableliais atskiriamų duomenų **CSV** failo formatui. Jei pasirinksite **Įvykis**, žurnalai bus saugomi „Windows“ įvykių žurnale (jį galima peržiūrėti naudojant įvykių žiūryklę arba valdymo skydą), o ne faile.
- **Naikinti visus žurnalo failus** – ištrina visus saugomus žurnalus, šiuo metu pasirinktus išskleidžiamajame meniu **Tipas**. Sėkmingai panaikinus žurnalus bus parodytas pranešimas.

Įjungti konfigūracijos pakeitimų sekimą audito žurnaluose – praneša apie kiekvieną konfigūracijos keitimą. Daugiau informacijos žr. Audito žurnalai.

> Kad būtų galima greičiau išspręsti problemas, ESET kartais jūsų gali paprašyti pateikti kompiuteryje saugomus žurnalus. ESET Log Collector priemonė leidžia paprastai surinkti reikiamą informaciją. Papildomos informacijos apie ESET Log Collector priemonę rasite ESET žinių bazės straipsnyje.

Audito žurnalai

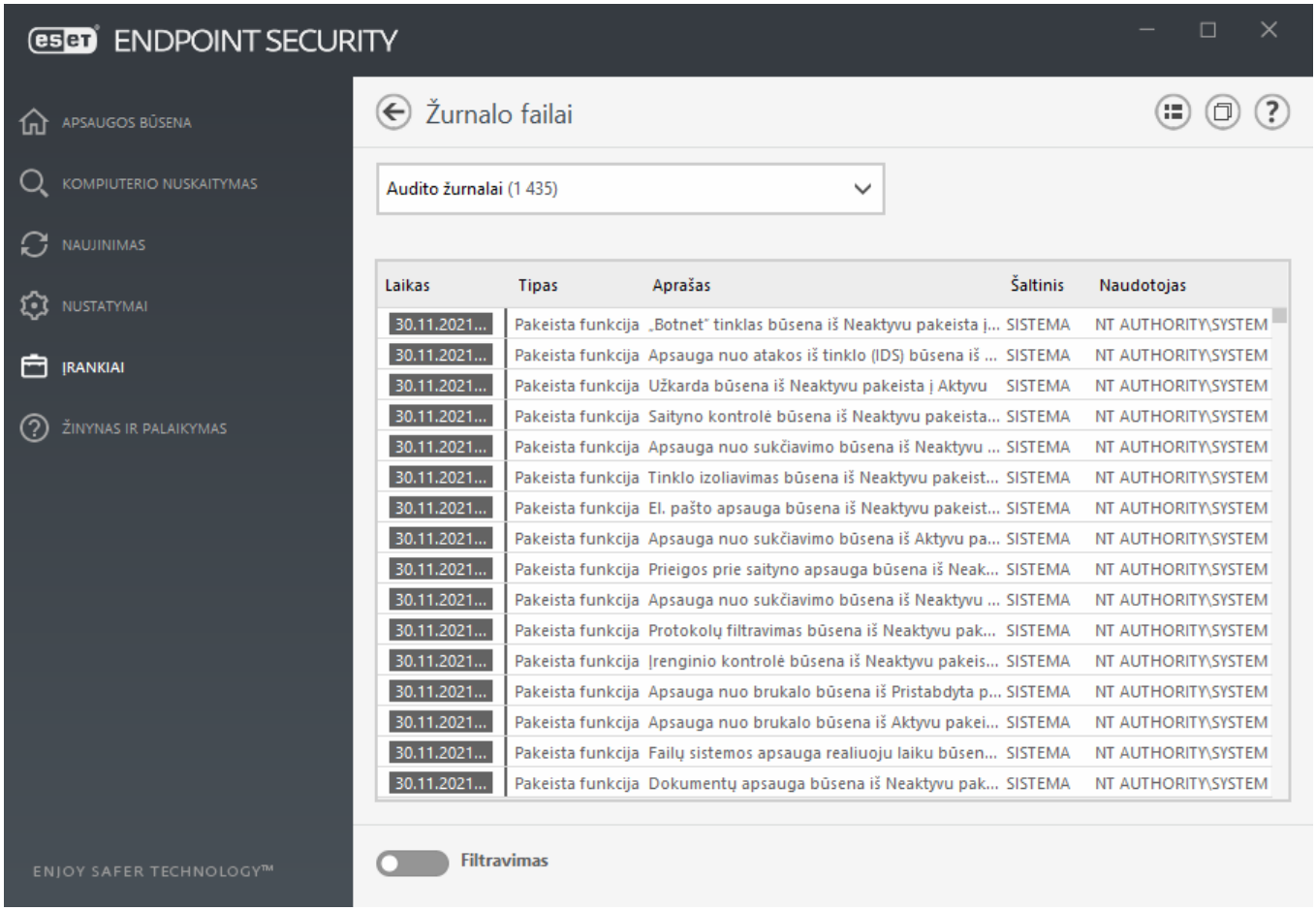
Įmonių aplinkoje, paprastai yra daug naudotojų, kurie turi teises, suteikiančias galimybę konfigūruoti įrenginius. Kadangi produkto konfigūracijos modifikavimas gali dramatiškai pakeisti produkto veikimą, svarbu, kad administratoriai norėtų atsekti naudotojų atliktus pakeitimus, kad administratoriai galėtų greitai nustatyti, išspręsti ir užkirsti kelią tokioms pat arba panašioms problemoms ateityje.

Audito žurnalas – tai naujo tipo registravimas, pasirodęs ESET Endpoint Security versijoje 7.1 ir kilmės nustatymo problemos sprendimas. Audito žurnale sekami konfigūracijos arba apsaugos būsenos pakeitimai ir įrašomos momentinės kopijos ateičiai.

Norėdami pamatyti **Audito žurnalą**, pagrindiniame meniu spustelėkite **Įrankiai** ir spustelėkite **Žurnalo failai** bei išskleidžiamajame meniu pasirinkite **Audito žurnalai**.

Audito žurnale pateikiama informacija apie:

- Laikas – kada buvo atliktas keitimas
- Tipas – kokio tipo nustatymas arba funkcija buvo pakeista
- Aprašas – kas tiksliai buvo pakeista ir kuri parametro dalis buvo pakeista kartu su pakeistų nustatymų skaičiumi
- Šaltinis – kur yra pakeitimų šaltinis
- Naudotojas – kas atliko pakeitimus



Dešiniuoju pelės mygtuku spustelėkite bet kurį audito žurnalo **Pakeisti nustatymai** tipą žurnalo failų lange ir pasirinkite **Rodyti pakeitimus**kontekstiniame meniu, kad būtų rodoma išsami informacija apie atliktus pakeitimus. Be to, galite atkurti nustatymų pakeitimus, spustelėdami **Atkurti** kontekstiniame meniu (negalima naudoti produktui valdomam ESET PROTECT). Jei kontekstiniame meniu pasirinkote **Panaikinti visus**, bus sukurtas žurnalas su informacija apie šį veiksmą.

Jei įjungtas nustatymas **Automatiškai optimizuoti žurnalo failus** dalyje **išplėstinis nustatymas** > **Įrankiai** > **Žurnalo failai>**, audito žurnalai bus automatiškai defragmentuojami kaip kiti žurnalai.

Jei įjungtas nustatymas **Automatiškai naikinti įrašus, senesnius nei (dienų)** dalyje **Išplėstinis nustatymas** > **Įrankiai** > **Žurnalo failai**, senesni nei nurodyto dienų skaičiaus failai bus automatiškai naikinami.

Planuoklė

planuoklė tvarko ir paleidžia planuotas užduotis su iš anksto nustatyta konfigūracija ir ypatybėmis.

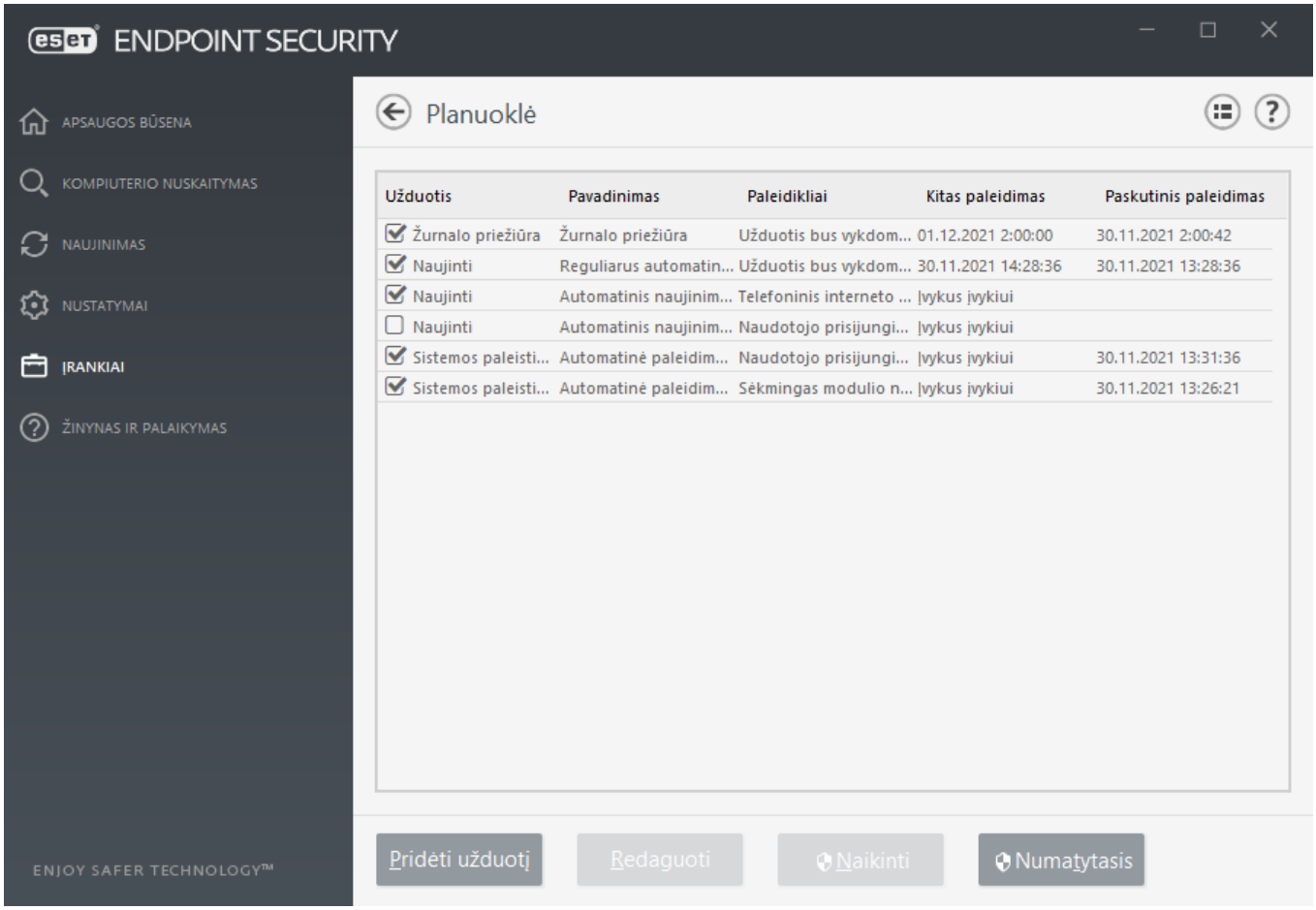
Planuoklę galima pasiekti iš ESET Endpoint Security pagrindinio programos lango spustelėjus **Įrankiai** > **Planuoklė**. **Planuoklėje** yra visų planuotų užduočių ir konfigūracijos ypatybių sąrašas – iš anksto nustatyta data, laikas ir naudojamas nuskaitymo profilis.

Planuoklė skirta planuoti šias užduotis: aptikimo modulio naujinimas, nuskaitymo užduotis, sistemos paleidimo failo patikra ir žurnalo priežiūra. Galite pridėti arba panaikinti užduotis tiesiog pagrindiniame planuoklės lange (spustelėkite **Pridėti užduotį...** arba **Naikinti** apačioje). Dešiniuoju pelės klavišu spustelėkite bet kur planuoklės lange, kad galėtumėte atlikti šiuos veiksmus: rodyti išsamią informaciją, atlikti užduotį iškart, pridėti naują užduotį ir panaikinti esamą. Naudodami žymės langelius kiekvieno įrašo pradžioje galite aktyvinti / deaktyvinti užduotis.

Pagal numatytuosius nustatymus **planuoklėje** rodomos šios suplanuotos užduotys:

- **Žurnalo priežiūra**
- **Reguliarus automatinis naujinimas**
- **Automatinis naujinimas prisijungus telefono ryšiu**
- **Automatinis naujinimas prisiregistravus vartotojui**
- **Automatinė paleidimo failo patikra** (prisiregistravus vartotojui)
- **Automatinė paleidimo failo patikra** (sėkmingai atnaujinus modulį)

Norėdami redaguoti esamos suplanuotos užduoties konfigūraciją (tiek numatytąją, tiek apibrėžtą vartotojo), spustelėkite dešiniuoju pelės klavišu užduotį ir **Redaguoti** arba pasirinkite užduotį, kurią norite keisti, ir spustelėkite mygtuką **Redaguoti**.



Pridėti naują užduotį

1. Spustelėkite **Pridėti užduotį** lango apačioje.
2. Įveskite užduoties pavadinimą.
3. Pasirinkite norimą užduotį iš išskleidžiamojo meniu:

- **Vykdyti išorinę taikomąją programą** – leidžia planuoti išorinės taikomosios programos vykdymą.
- **Žurnalo priežiūra** – žurnalo failuose taip pat gali būti panaikintų įrašų likučių. Ši užduotis reguliariai optimizuoja įrašus žurnalo failuose, kad darbas būtų efektyvus.
- **Sistemos paleidimo failo patikra** – tikrina failus, kurie leidžiami vykdyti paleidžiant sistemą arba registruojantis.
- **Sukurti kompiuterio būsenos momentinę kopiją** – sukuria ESET SysInspector kompiuterio momentinę kopiją – surenka išsamią informaciją apie sistemos dalis (pvz., tvarkykles, programas) ir įvertina kiekvienos

dalies rizikos lygį.

- **Kompiuterio nuskaitymas pareikalavus** – atlieka kompiuterio failų ir katalogų nuskaitymą.
- **Naujinimas** – suplanuoja naujinimo užduotį, skirtą atnaujinti aptikimo modulį ir programos modulius.

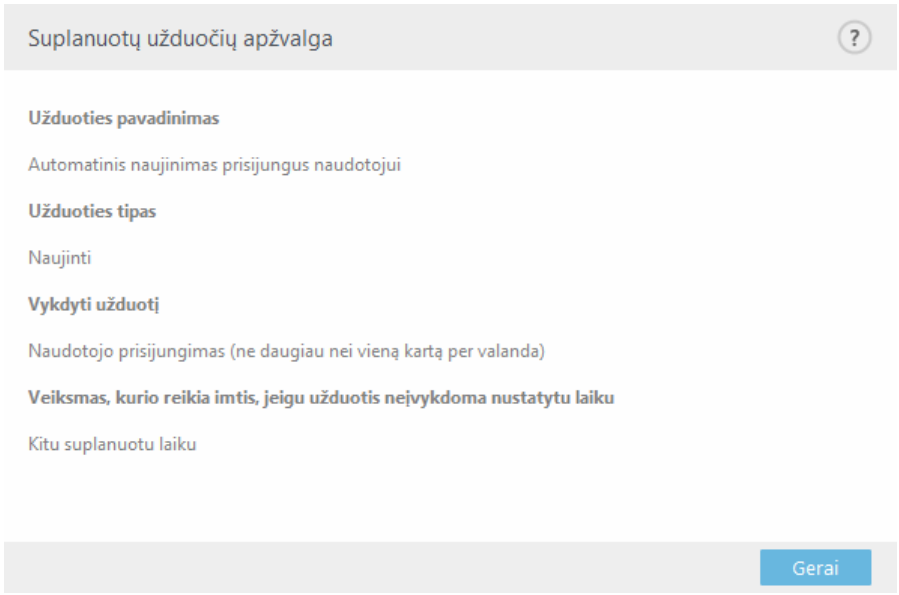
4. Įjunkite jungiklį **Įjungta**, jei norite suaktyvinti užduotį (tai galite padaryti vėliau, pažymėdami langelį ar nuimdami jo žymą planinių užduočių sąraše), spustelėkite **Toliau** ir nurodykite vieną iš laiko parinkčių:

- **Vieną kartą** – užduotis bus atlikta iš anksto nustatyta data ir laiku.
- **Pakartotinai** – užduotis bus atliekama nurodytais intervalais.
- **Kasdien** – užduotis bus pakartotinai vykdoma kasdien nurodytu laiku.
- **Kas savaitę** – užduotis bus vykdoma pasirinktą dieną ir laiku.
- **Įvykus įvykiui** – užduotis bus vykdoma įvykus nurodytam įvykiui.

5. **Nurodykite Praleisti užduotį, kai naudojama akumuliatoriaus energija**, kad maksimaliai apribotumėte energijos sąnaudas, kai nešiojamasis kompiuteris veikia maitinamas akumuliatoriaus. Užduotis bus vykdoma laukuose **Užduoties vykdymas** nurodytą datą ir laiku. Jeigu užduotis negali būti atlikta iš anksto nustatytu laiku, galite nurodyti, kada ji bus vėl vykdoma:

- **Kitu suplanuotu laiku**
- **Kaip įmanoma greičiau**
- **Iškart, jei nuo paskutinio vykdymo praėjo daugiau laiko nei nurodyta reikšme** (intervalą galima nustatyti naudojantis slinkimo laukeliu **Nuo paskutinio vykdymo praėjo**)

Galite peržiūrėti planinę užduotį, spustelėdami dešiniuoju pelės klavišu ir pasirinkdami **Rodyti užduoties informaciją**.



ESET SysInspector

ESET SysInspector yra programa, kuri nuodugniai tikrina jūsų kompiuterį, surenka išsamią informaciją apie sistemos komponentus (tvarkykles ir programas, tinklo ryšius ar svarbius registrų įrašus) ir įvertina kiekvieno komponento rizikos lygį. Ši informacija gali padėti nustatyti įtartino sistemos veikimo priežastis dėl programinės įrangos ar aparatūros nesuderinamumo arba užsikrėtus kenkėjiška programa. Taip pat žr. ESET SysInspector internetinį naudotojo vadovą.

„SysInspector“ langas rodo šią informaciją apie sukurtus žurnalus:

- **Laikas** – žurnalo sukūrimo laikas.
- **Komentaras** – trumpas komentaras.
- **Vartotojas** – vartotojo, sukūrusio žurnalą, vardas.
- **Būsena** – žurnalo kūrimo būsena.

Galimi šie veiksmai:

- **Rodyti** – atidaromas sukurtas žurnalas. Be to, galite dešiniuoju pelės klavišu spustelėti reikiamą žurnalo failą ir kontekstiniame meniu pasirinkti **Rodyti**.
- **Kurti** – sukuriamas naujas žurnalas. Prieš bandydami atidaryti žurnalą palaukite, kol ESET SysInspector užbaigs darbą (žurnalo būsena bus rodoma kaip „**Sukurta**“).
- **Naikinti** – iš sąrašo pašalinamas pasirinktas žurnalas (-ai).

Kai pasirenkamas vienas ar keli žurnalo failai, kontekstiniame meniu pateikiami tokie elementai:

- **Rodyti** – atidaro pasirinktą žurnalą ESET SysInspector lange (ta pati funkcija, kaip dukart spustelėjus žurnalą).
- **Kurti** – sukuriamas naujas žurnalas. Prieš bandydami atidaryti žurnalą palaukite, kol ESET SysInspector užbaigs darbą (žurnalo būsena bus rodoma kaip „**Sukurta**“).
- **Naikinti** – panaikina pasirinktą žurnalą.
- **Naikinti viską** – panaikina visus žurnalus.
- **Eksportuoti** – eksportuoja žurnalą į .xml failą arba zip formatu suglaudintą .xml.

Debesimi paremta apsauga

ESET LiveGrid® (pagal ESET ThreatSense.Net išplėstinę ankstyvojo įspėjimo sistemą) naudoja duomenis, kuriuos ESET pateikia vartotojai iš viso pasaulio ir siunčia juos į ESET tyrimų laboratoriją. Pateikdama įtartinus pavyzdžius ir metaduomenis iš pasaulio ESET LiveGrid® suteikia mums galimybę greitai prisitaikyti prie klientų poreikių ir padeda ESET reaguoti į naujausias grėsmes.

Yra trys parinktys:

1 pasirinkimas: įjungti ESET LiveGrid® reputacijos sistemą

ESET LiveGrid® reputacijos sistema teikia debesų technologija pagrįstą baltąjį ir juodąjį sąrašą.

Patikrinkite Vykdomų procesų ir failų reputaciją tiesiog naudodamiesi programos sąsaja arba kontekstiniu meniu su papildoma informacija, gauta iš ESET LiveGrid®.

2 pasirinkimas: įjungti ESET LiveGrid® atsiliepimų sistemą

Be ESET LiveGrid® sistemos, ESET LiveGrid® surinks informaciją apie naujai aptiktas grėsmes, susijusias su jūsų kompiuteriu. Ši informacija gali turėti failo, kuriame atsirado grėsmė, pavyzdį arba kopiją, kelią į šį failą, failo pavadinimą, datą ir laiką, procesą, kurio metu grėsmė atsirado jūsų kompiuteryje, ir informaciją apie jūsų kompiuterio operacinę sistemą.

Pagal numatytuosius nustatymus ESET Endpoint Security yra sukonfigūruotas, siekiant ESET virusų laboratorijai pateikti įtartinus failus, kad būtų atlikta išsami jų analizė. Failai su tam tikrais plėtiniais, pavyzdžiui, *.doc* ar *.xls*, niekada neįtraukiami. Taip pat galite pridėti kitų plėtinių, jei yra konkrečių failų, kurių jūs ar jūsų organizacija

nenori siųsti.

3 pasirinkimas: pasirinkti neįjungti ESET LiveGrid®

Neprarasite jokių programinės įrangos funkcijų, tačiau atskirais atvejais ESET Endpoint Security gali sparčiau reaguoti į naujas grėsmes nei aptikimo modulio naujinimas, kai įjungta „ESET LiveGrid®“.

> Išsamiau apie šių ESET LiveGrid® skaitykite terminų žodyne.
> Žr. mūsų iliustruotas instrukcijas anglų kalba ir kai kuriomis kitomis kalbomis, kaip įjungti arba išjungti ESET LiveGrid® programoje ESET Endpoint Security.

Debesimi paremta konfigūracija išplėstiniame nustatyme

Norėdami pasiekti ESET LiveGrid® nustatymus, paspauskite **F5**, kad įjungtumėte išplėstinį nustatymą ir išplėskite **Aptikimo modulis** > **Debesies pagrindo apsauga**.

Įjungti ESET LiveGrid® reputacijos sistemą (rekomenduojama) – ESET LiveGrid® reputacijos sistema pagerina ESET apsaugos nuo kenkimo programinės įrangos sprendimų efektyvumą, nes nuskaitytų failų duomenis palygina su debesies saugykloje esančiais duomenų bazės įrašais baltajame ir juodajame sąrašuose.

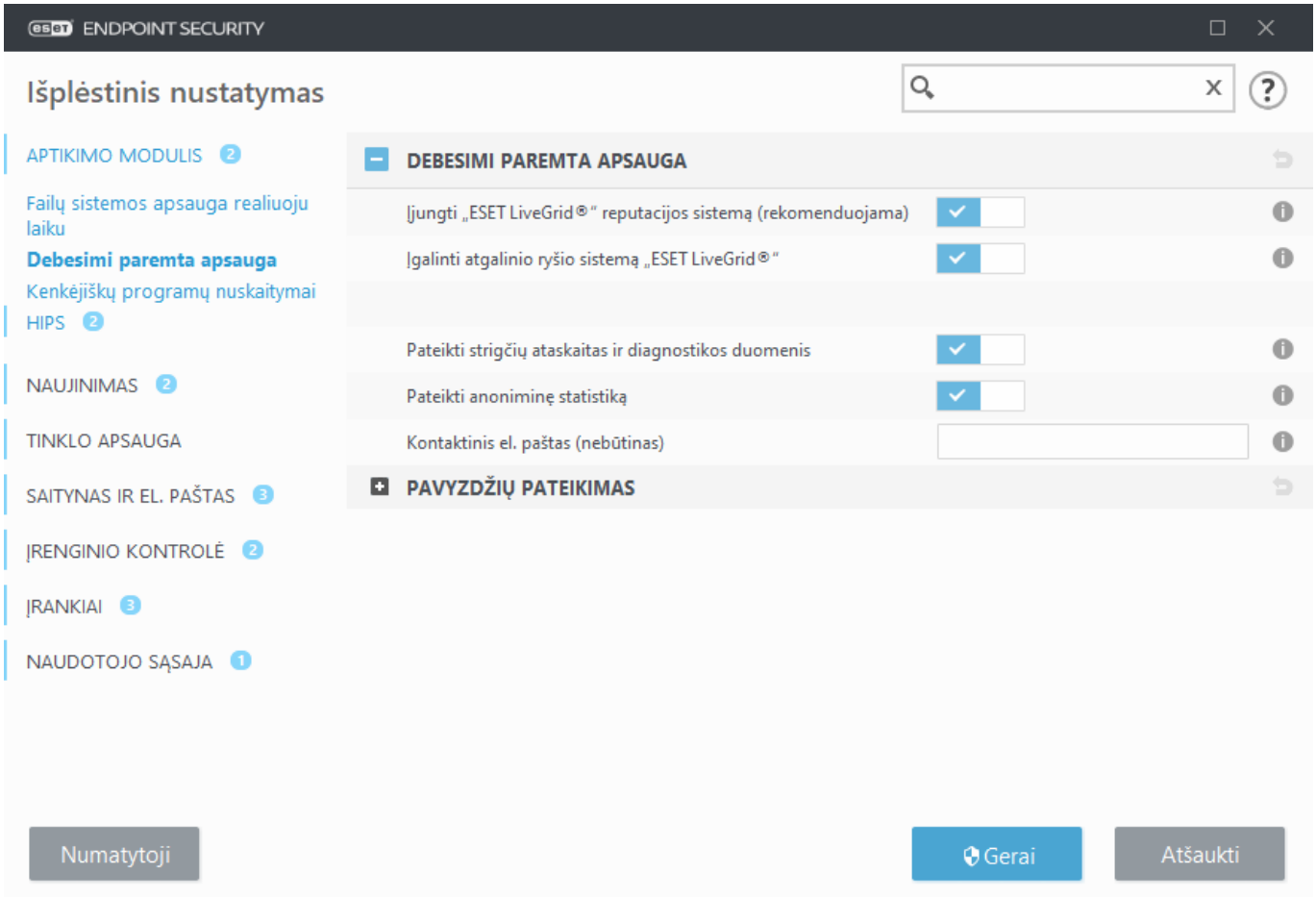
Įjungti ESET LiveGrid® atsiliepimų sistemą – siunčia atitinkamus pateikimo duomenis (aprašytus toliau esančiame skyriuje **Pavyzdžių pateikimas**) kartu su strigčių ataskaitomis ir statistiniais duomenimis į ESET tyrimo laboratoriją tolesnei analizei.

Įjungti ESET LiveGuard (nematoma ESET Endpoint Security) – ESET LiveGuard yra mokama paslauga, kurią teikia ESET. Jos tikslas yra pridėti apsaugos sluoksnį, specialiai sukurtą siekiant sumažinti naujas grėsmes. Įtartini failai yra automatiškai pateikiami į ESET debesį. Debesyje juos išanalizuoja mūsų pažangūs kenkėjiškų programinių įrangų aptikimo moduliai. Naudotojas, pateikęs pavyzdį, gaus elgsenos ataskaitą, kurioje pateikiama išanalizuoti pavyzdžio elgsena.

Pateikti strigčių ataskaitas ir diagnostinius duomenis – pateikti ESET LiveGrid® susijusius diagnostinius duomenis, pavyzdžiui, strigčių ataskaitas ir modulių atminties išklotines. Rekomenduojame laikyti įjungtą, nes tai padeda ESET diagnozuoti problemas, gerinti produktus ir užtikrinti geresnę galutinio naudotojo apsaugą.

Pateikti anoniminius statistinius duomenis – leiskite ESET rinkti informaciją apie naujai aptiktas grėsmes, pvz., grėsmės pavadinimą, aptikimo datą ir laiką, aptikimo metodą ir susijusius metaduomenis, produkto versiją ir konfigūraciją, įskaitant informaciją apie jūsų sistemą.

Kontaktinis el. paštas (nebūtinas) – jūsų kontaktinis el. pašto adresas gali būti įtrauktas su visais įtartinais failais ir gali būti naudojamas su jumis susisiekti, jeigu analizuojant reikės papildomos informacijos. Atsiminkite, kad negausite atsakymo iš ESET, jei neprireiks daugiau informacijos.



Pavyzdžių pateikimas

Rankinis pavyzdžių pateikimas – Leidžia rankiniu būdu pateikti pavyzdžius ESET iš kontekstinio meniu, pasirinkus Karantinas arba Įrankiai > Pateikti pavyzdį analizei.

Automatinis aptiktų pavyzdžių pateikimas

Pasirinkite kokius pavyzdžius pateikti ESET analizei, kad būtų pagerintas grėsmių aptikimas ateityje. Galimos šios parinktys:

- **Visi aptikti pavyzdžiai** – visi objektai, kuriuos aptiko aptikimo modulis (įskaitant galimas nepageidaujamas taikomąsias programas, kai įjungti skaitytuvo nustatymai).
- **Visi pavyzdžiai, išskyrus dokumentus** – visi aptikti pavyzdžiai, išskyrus **Dokumentai** (žr. toliau).
- **Nepateikti** – aptikti objektai nebus siunčiami ESET.

Automatinis įtartinų mėginių pateikimas

Šie pavyzdžiui taip pat bus siunčiami ESET, jei aptikimo modulis jų neaptiko. Pavyzdžiui, pavyzdžiai, kurių vos neaptiko, arba vienas iš ESET Endpoint Security aptikimo modulių laiko šiuos pavyzdžius įtartinais arba įtartinai elgiantis.

- **Vykdomieji failai** – įeina tokie failai kaip .exe, .dll, .sys
- **Archyvai** – įeina failų tipai, tokie kaip .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Scenarijai** – įeina failų tipai, tokie kaip .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Kita** – įeina failų tipai, tokie kaip .jar, .reg, .msi, .sfw, .lnk.
- **Galimi brukalo el. laiškai** – tai leis siųsti galimas brukalo dalis ar visus el. laiškus su priedais tolesnei ESET

analizei. Šios parinkties įgalinimas gerina visuotinį brukalų aptikimą, įskaitant efektyvesnį jūsų gaunamo brukalo aptikimą.

- **Dokumentai** – sudaro Microsoft Office arba PDF dokumentai su arba be aktyvaus turinio.
  Išplėsti visų įtrauktų dokumentų failų tipų sąrašą

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

Išimtys

Išimties filtras leidžia į pateikimo sąrašą neįtraukti tam tikrų failų ar aplankų (pvz., gali būti naudinga neįtraukti failų su konfidencialia informacija, tarkime, dokumentų ar skaičiuoklių). Sąraše esantys failai niekada nebus siunčiami analizuoti į ESET laboratoriją, net jei juose bus įtartino kodo. Dažniausiai naudojami failų tipai neįtraukti pagal numatytuosius nustatymus (.doc, ir t. t.). Jeigu norite, galite įtraukti į nesiunčiamų failų sąrašą.

Norėdami neįtraukti failų, atsisiųstų iš download.domain.com, eikite **Išplėstinis nustatymas** > **Debesimi pagrįsta apsauga** > **Pavyzdžių pateikimas** > **Išskyrimai** ir įtraukite išskyrimą *download.domain.com*.

ESET LiveGuard

Norėdami įjungti ESET LiveGuard paslaugą kliento įrenginyje naudodami ESET PROTECT tinkle valdomą konsolę, žr. ESET Endpoint Security ESET LiveGuard konfigūracija.

Jei anksčiau naudojote ESET LiveGrid® ir ją išjungėte, gali būti likę paruoštų siųsti duomenų paketų. Tokie paketai bus išsiųsti į ESET net ir išaktyvinus funkciją. Išsiuntus visą dabartinę informaciją, daugiau paketų kuriama nebus.

Debesimi paremtos apsaugos išimčių filtras

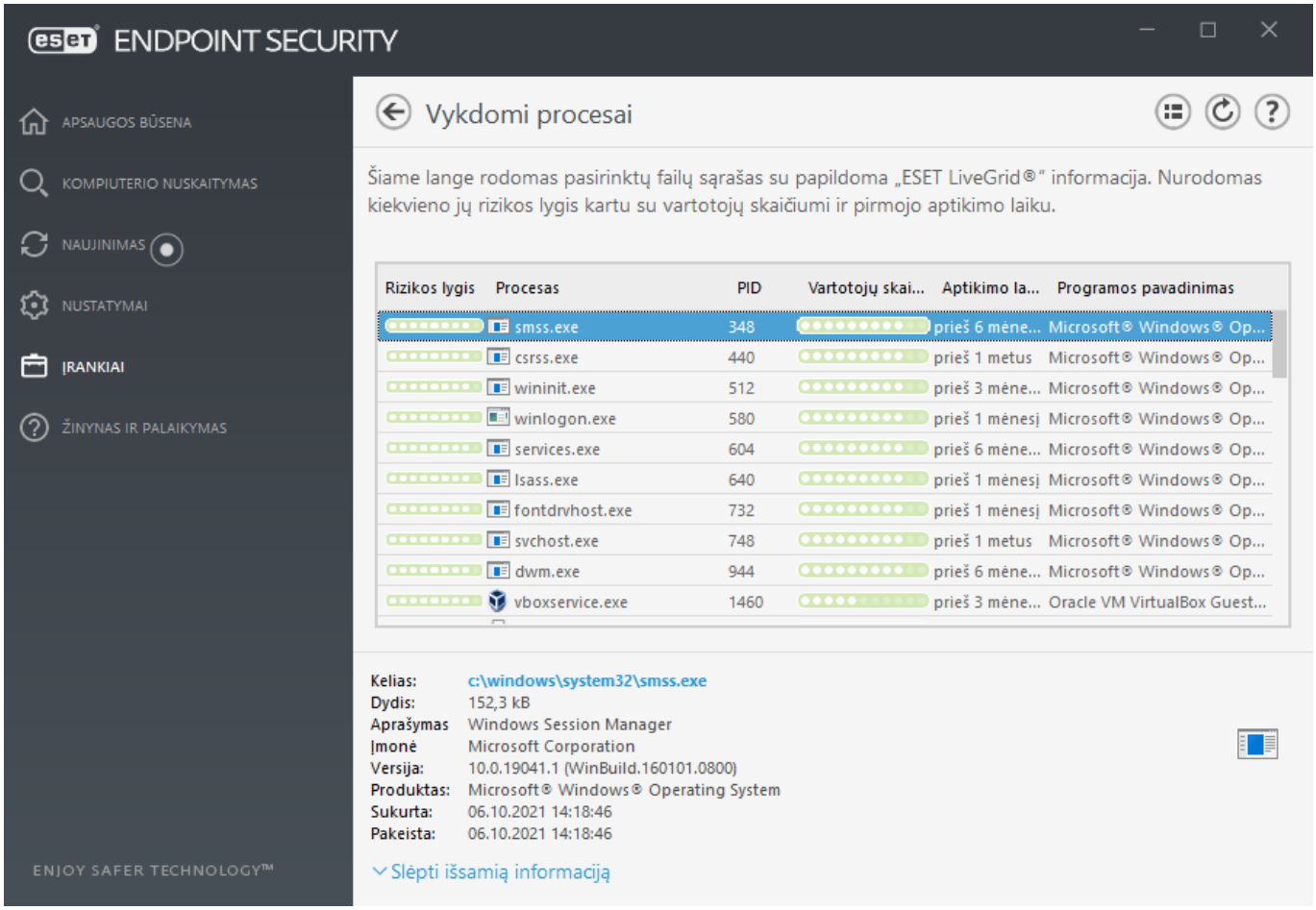
Išimčių filtras leidžia atsisakyti pateikti kai kuriuos failus ar aplankus kaip pavyzdžius. Sąraše esantys failai niekada nebus siunčiami analizuoti į ESET laboratoriją, net jei juose bus įtartino kodo. Dažniausi failų tipai (pvz., .doc ir pan.) neįtraukiami pagal numatytuosius nustatymus.

Ši funkcija praverčia, kai reikia neįtraukti failų, kuriuose gali būti konfidencialios informacijos, pvz., dokumentų arba skaičiuoklių.

Norėdami neįtraukti failų, atsisiųstų iš download.domain.com, eikite **Išplėstinis nustatymas** > **Debesimi pagrįsta apsauga** > **Pavyzdžių pateikimas** > **Išskyrimai** ir įtraukite išskyrimą *download.domain.com*.

Vykdomi procesai

Vykdomi procesai jūsų kompiuteryje rodo vykdomas programas arba procesus ir iškart bei nuolat informuoja ESET apie naujus įsiskverbimus. ESET Endpoint Security suteikia išsamios informacijos apie vykdomus procesus, kad įjungta technologija ESET LiveGrid® saugotų vartotojus.



Reputation (reputacija) – daugeliu atvejų „ESET Endpoint Security" ir „ESET LiveGrid®" technologija priskiria rizikos lygius objektams (failams, procesams, registrų raktams ir t. t.) naudodama euristikos taisyklių sekas, kurios tikrina kiekvieno objekto charakteristikas ir įvertina jų kenkėjiškos veiklos galimybę. Remiantis šia euristika, objektams priskiriami reputacijos lygiai nuo 9 (geriausia reputacija, žalia) iki 0 (blogiausia reputacija, raudona).

Procesas – šiuo metu jūsų kompiuteryje vykdomos programos arba proceso atvaizdo pavadinimas. Norėdami matyti visus savo kompiuteryje vykdomus procesus galite naudoti ir „Windows" užduočių tvarkytuvą. Galite atidaryti užduočių tvarkytuvą, dešiniuoju pelės klavišu spustelėdami tuščią sritį užduočių juostoje ir tada spustelėdami užduočių tvarkytuvą arba klaviatūroje paspausdami **Ctrl**+**Shift**+**Esc**.

PID – tai ID procesų, veikiančių „Windows" operacinėse sistemose.

Žinomos programos, pažymėtos žalia spalva, tikrai yra švarios (įtrauktos į baltąjį sąrašą) ir bus neįtrauktos į nuskaitymo sąrašą, nes tai padidins nuskaitymo greitį atliekant kompiuterio nuskaitymą pareikalavus arba vykdant failų sistemos apsaugą realiuoju laiku jūsų kompiuteryje.

Vartotojų skaičius – vartotojų, naudojančių duotą taikomąją programą, skaičius. Šią informaciją renka ESET LiveGrid® technologija.

Atskleidimo laikas – laikotarpis, praėjęs nuo tada, kai taikomąją programą aptiko ESET LiveGrid® technologija.

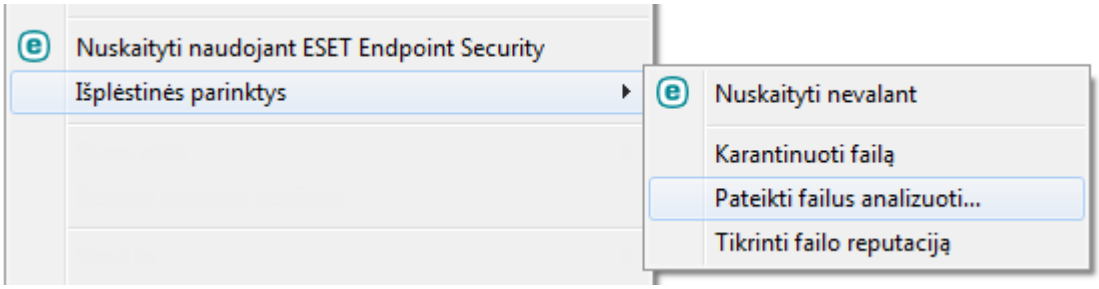
Kai taikomoji programa yra pažymėta nežinomu (oranžinė spalva) saugos lygiu, ji nebūtinai yra kenkėjiška. Paprastai tai naujesnė taikomoji programa. Jeigu nesate tikri dėl failo, galite pasinaudoti funkcija pateikti failą analizuoti ir nusiųsti failą ESET virusų laboratorijai. Jeigu failas pasirodys esantis kenkėjiška programa, jo aptikimas bus įtrauktas į vieną būsimų aptikimo modulio naujinimų.

Programos pavadinimas – duotas programos arba proceso pavadinimas.

Spustelėjus duotą taikomąją programą apačioje, lango apačioje pasirodys ši informacija:

- **Kelias** – programos vieta jūsų kompiuteryje.
- **Dydis** – failo dydis kB (kilobaitais) arba MB (megabaitais).
- **Aprašymas** – failo charakteristikos pagal aprašą operacinėje sistemoje.
- **Įmonės** – tiekėjo arba programos proceso pavadinimas.
- **Versija** – programos leidėjo informacija.
- **Produktas** – programos pavadinimas ir (arba) įmonės pavadinimas.
- **Sukurta** – programos sukūrimo data ir laikas.
- **Modifikavimo data** – programos paskutinio modifikavimo data ir laikas.

Galima patikrinti ir failų, kurie neveikia kaip vykdomosios programos / procesai, reputaciją – pažymėkite failus, kuriuos norite tikrinti, spustelėkite juos dešiniuoju pelės mygtuku ir iš kontekstinio meniu pasirinkite **Išplėstinės parinktys** > **Tikrinti failo reputaciją naudojant ESET LiveGrid®**.



Saugumo ataskaita

Ši funkcija leidžia peržiūrėti šių kategorijų statistiką:

Užblokuoti tinklalapiai – rodo užblokuotų tinklalapių skaičių (į juodąjį sąrašą įtrauktus PUA, sukčiavimo apsimetant, maršrutizatoriaus, į kurį įsibrauta, URL, IP arba sertifikatą).

Aptikta užkrėstų el. pašto objektų – rodo užkrėstų el. pašto objektų, kurie buvo aptikti, skaičių.

Tinklalapiai, užblokuoti naudojant paslaugą „saityno kontrolė“ – rodo užblokuotų tinklalapių, naudojant paslaugą „saityno kontrolė“, skaičių.

Aptikta PUA – rodo galimai nepageidaujamų programų (PUA) skaičių.

Aptikta el. pašto brukalo – rodo aptiktų el. pašto brukalų skaičių.

Patikrinta dokumentų – rodo nuskaitytų dokumentų objektų skaičių.

Patikrinta programų – rodo nuskaitytų vykdomųjų objektų skaičių.

Patikrinta kitų objektų – rodo kitų nuskaitytų objektų skaičių.

Patikrinta tinklalapių objektų – rodo nuskaitytų tinklalapių objektų skaičių.

Nuskaityta el. pašto objektų – rodo nuskaitytų el. pašto objektų skaičių.

Šių kategorijų tvarka yra pagrįsta skaitine verte nuo didžiausios iki mažiausios. Kategorijos su nuline verte nėra rodomos. Paspauskite „**Rodyti daugiau**“, kad būtų išplėstos ir rodomos paslėptos kategorijos.

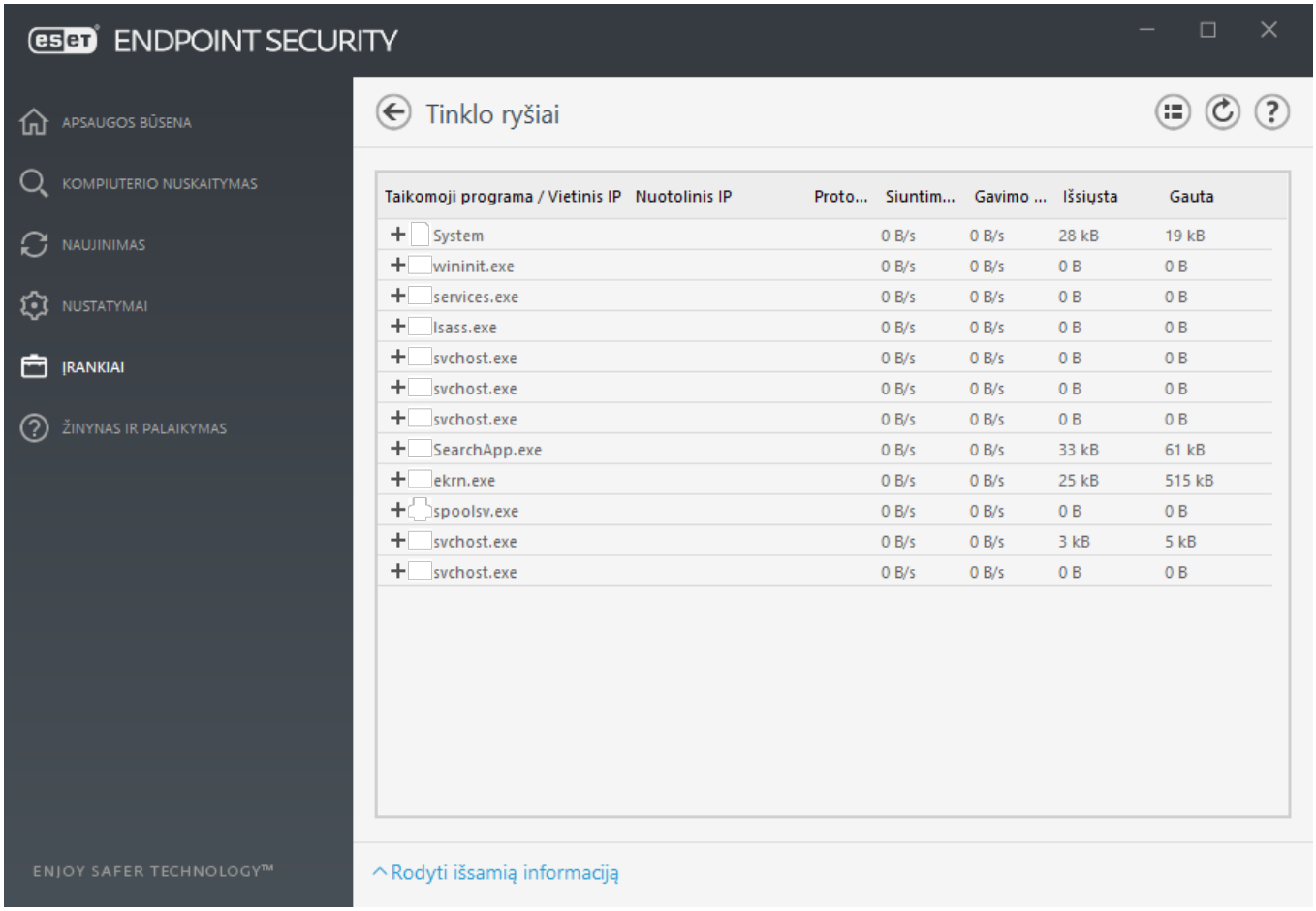
Paspauskite krumpliaračio piktogramą viršutiniame dešiniajame kampe ir galėsite **Įjungti / išjungti saugumo ataskaitos pranešimus** arba pasirinkti, ar rodyti paskutinių 30 dienų duomenis ar nuo to laiko, kai produktas buvo suaktyvintas. Jei ESET Endpoint Security buvo įdiegtas mažiau nei prieš 30 dienų, galima pasirinkti tik tą dienų skaičių, kuris praėjo nuo įdiegimo. 30 dienų laikotarpis nustatytas kaip numatytasis nustatymas.



Įjungus funkciją **Iš naujo nustatyti duomenis**, bus išvalyta visa statistika ir iš saugumo ataskaitos pašalinti visi joje esantys duomenys. Šį veiksmą reikia patvirtinti, išskyrus, jei atsisakysite parinkties **Klausti prieš atkuriant statistiką** (**Išplėstinis nustatymas** > **Pranešimai** > **Interaktyvūs įspėjimai** > **Patvirtinimo pranešimai**).

Tinklo ryšiai

Tinklo ryšių skyriuje galite matyti aktyvių ir laukiamų ryšių sąrašą. Tai padeda kontroliuoti visų programų palaikomus siunčiamus ryšius.



Pirmoje eilutėje rodomas programos pavadinimas ir jos duomenų perdavimo greitis. Norėdami matyti programos atliktų ryšių sąrašą (ir išsamesnės informacijos), spustelėkite **+**.

Stulpeliai

Programa / vietinis IP – programos pavadinimas, vietiniai IP adresai ir ryšio prievadai.

Nuotolinis IP – konkretaus nuotolinio kompiuterio IP adresas ir prievado numeris.

Protokolas – naudojamas siuntimo protokolas.

Siuntimo greitis / gavimo greitis – esamas siunčiamų ir gaunamų duomenų greitis.

Išsiųsta / gauta – duomenų kiekis, apsikeistas ryšio metu.

Rodyti išsamią informaciją – nurodykite šią parinktį, kad būtų pateikta išsamios informacijos apie pasirinktą ryšį.

Tinklo ryšių ekrane pasirinkite programą arba IP adresą ir dešiniuoju pelės klavišu spustelėkite jį, kad būtų pateiktas kontekstinis meniu su tokia struktūra:

Pasirinkti pagrindinio kompiuterio pavadinimus – jeigu įmanoma, visi tinklo adresai rodomi DNS formatu, o ne skaitiniu IP adreso formatu.

Rodyti tik TCP ryšius – sąraše rodomi tik tie ryšiai, kurie priklauso TCP protokolo programų paketui.

Rodyti klausomus ryšius – nurodžius šią parinktį, pateikiami tik tie ryšiai, kuriems ryšys šiuo metu nėra užmegztas, tačiau sistema yra atidariusi prievadą ir laukia ryšio.

Rodyti ryšius kompiuteryje – nurodykite šią parinktį, kad būtų rodomi tik tie ryšiai, kurių nuotolinė pusė yra

vietinė sistema – vadinamieji vietinio pagrindinio kompiuterio ryšiai.

Spustelėkite dešiniuoju pelės klavišu ryšį, norėdami matyti papildomas parinktis:

Uždrausti ryšį jungčiai – nutraukia užmegztą ryšį. Ši parinktis pasiekiama tik spustelėjus aktyvią jungtį.

Atnaujinti greitį – pasirinkite, kokiu dažnumu atnaujinti aktyvius ryšius.

Atnaujinti dabar – iš naujo įkelia Tinklo ryšių langą.

Šios parinktys pasiekiamos tik spustelėjus programą arba procesą, o ne aktyvią jungtį:

Laikinai uždrausti proceso ryšį – atmeta esamus duotosios programos ryšius. Jeigu užmezgamas naujas ryšys, užkarda naudoja iš anksto nustatytą taisyklę. Parametrų aprašą galima rasti skyriuje Taisyklės ir zonos.

Laikinai leisti proceso ryšį – leidžia esamus duotosios programos ryšius. Jeigu užmezgamas naujas ryšys, užkarda naudoja iš anksto nustatytą taisyklę. Parametrų aprašą galima rasti skyriuje Taisyklės ir zonos.

ESET SysRescue Live

„ESET SysRescue Live“ yra nemokama priemonė, suteikianti galimybę sukurti įkraunantį CD/DVD arba USB laikmeną. Galite įkrauti užkrėstą kompiuterį iš saugios laikmenos, kad rastumėte kenkėjiškas programas ir išvalytumėte užkrėstus failus.

Pagrindinis „ESET SysRescue Live“ privalumas yra tas, kad sprendimas veikia nepriklausomai nuo pagrindinio kompiuterio operacinės sistemos, bet turi tiesioginę prieigą prie disko bei failų sistemos. Tai suteikia galimybę pašalinti grėsmes, kurių paprastai neįmanoma pašalinti (pvz., kai veikia operacinė sistema, ir t. t.).

- „ESET SysRescue Live“ Interneto žinynas

Pavyzdžių pateikimas analizuoti

Jeigu radote įtartiną failą savo kompiuteryje arba įtartiną svetainę internete, galite pateikti jį analizuoti ESET tyrimų laboratorijai (gali būti neprieinama atsižvelgiant į ESET LiveGrid® konfigūraciją).

Pateikite tik šiuos reikalavimus atitinkančius pavyzdžius:
• Pavyzdžio visiškai neaptinka jūsų ESET produktas
• Pavyzdys klaidingai aptiktas kaip grėsmė
• Nepriimame jūsų asmeninių failų (kad pati ESET patikrintų, ar juose nėra kenkėjiškų programų ESET) kaip pavyzdžių (ESET tyrimų laboratorija netikrina vartotojų failų pagal pageidavimą)
• Aiškiai aprašykite temą ir pateikti kuo daugiau informacijos apie šį failą (pavyzdžiui, ekrano kopiją arba svetainę, iš kurios jis atsisiųstas)

Pateikdami pavyzdį galite nusiųsti failą arba svetainę ESET analizei vienu iš šių būdų:

1. Naudojant pavyzdžio pateikimo formą, kuri yra dalyje **Įrankiai** > **Pavyzdžio pateikimas siekiant atlikti analizę**.
2. Arba galite pateikti failą el. paštu. Jeigu pasirenkate šį būdą, supakuokite failą (-us) WinRAR/ZIP programa, apsaugokite archyvą slaptažodžiu „infected“ (užkrėstas) ir siųskite jį adresu samples@eset.com.
3. Norėdami pranešti apie brukalą, klaidingai aptiktą brukalą arba svetaines, kurioms saityno kontrolės modulis priskyrė klaidingą kategorijąžr. ESET žinių bazės straipsnį.

Kai atidarytas **Pasirinkti mėginį analizei**, pasirinkite aprašą iš išskleidžiamojo meniu **Pavyzdžio pateikimo priežastis**, kuris geriausiai atitinka jūsų pranešimą:

- Įtartinas failas
- Įtartina svetainė **(svetainė, užkrėsta bet kokia kenkėjiška programa)**,
- Klaidingai teigiamas failas (failas, kuris buvo aptiktas kaip užkrėstas, bet nėra užkrėstas),
- Klaidingai teigiama svetainė
- Kita

Failas / svetainė – kelias į failą arba svetainę, kurį norite pateikti.

Kontaktinis el. paštas – šis kontaktinis el. pašto adresas yra siunčiamas kartu su įtartinais failais į ESET ir gali būti naudojamas norint susisiekti su jumis, jeigu analizei reikalinga papildoma informacija. Įvesti kontaktinį el. pašto adresą nebūtina. Norėdami palikti tuščią, pasirinkite **Pateikti anonimiškai**.

> Jūs negausite atsakymo iš ESET, jeigu nereikės daugiau informacijos. Kasdien mūsų serveriai gauna dešimtis tūkstančių failų, todėl neįmanoma atsakyti visiems juos pateikusiems.
> Jeigu pavyzdys pasirodys esantis kenkėjiška programa arba svetainė, jo aptikimas bus įtrauktas į būsimą ESET naujinimą.

Pasirinkti pavyzdį analizei – įtartinas failas

Pastebėti užkrėtimo kenkėjiška programa ženklai ir požymiai – įveskite savo kompiuteryje pastebėto įtartino failo veikimo aprašymą.

Failo kilmė (URL adresas arba tiekėjas) – įveskite failo kilmę (šaltinį) ir nurodykite, kaip jūs susidūrėte su šiuo failu.

Pastabos ir papildoma informacija – čia galite įvesti papildomą informaciją arba aprašymą, kuris padėtų apdoroti arba identifikuoti įtartiną failą.

> Pirmasis parametras – **Pastebėti užkrėtimo kenkimo programine įranga ženklai ir požymiai** – yra būtinas, tačiau pateikdami papildomos informacijos labai padėsite mūsų laboratorijoms identifikuoti ir apdoroti pavyzdžius.

Pasirinkti pavyzdį analizei – įtartinas svetainė

Pasirinkite vieną iš šių parinkčių išskleidžiamajame meniu **Kas negerai su šia svetaine?**:

- **Užkrėsta** – svetainė, kurioje yra įvairiai platinamų virusų arba kenkėjiškų programų.
- **Sukčiavimas apsimetant** – dažnai naudojamas norint gauti prieigą prie slaptų duomenų, tokių kaip banko sąskaitų numeriai, PIN kodai ir t. t. Išsamiau apie šio tipo atakas skaitykite terminų žodyne.
- **Apsimestinė svetainė** – apgaulinga svetainė, kuri siekia greito pelno.
- Pasirinkite **Kita**, jei minėtos parinktys netinka svetainei, kurią ketinate pateikti.

Pastabos ir papildoma informacija – čia galite įvesti papildomą informaciją arba aprašymą, kuris padėtų analizuojant įtartiną svetainę.

Pasirinkti pavyzdį analizei – klaidingai aptiktas failas

Mes prašome pateikti failus, kurie buvo aptikti kaip užkrėsti, bet nėra užkrėsti, kad galėtume patobulinti apsaugos nuo virusų ir šnipinėjimo programų modulį ir geriau apsaugotume kitus. Klaidingai teigiami (KT) rezultatai gali būti gaunami, kai failo dalis sutampa su tokia pat dalimi aptikimo modulyje.

Programos pavadinimas ir versija – programos pavadinimas ir jos versija (pavyzdžiui, numeris, alternatyvusis vardas arba kodo pavadinimas).

Failo kilmė (URL adresas arba tiekėjas) – įveskite failo kilmę (šaltinį) ir nurodykite, kaip jūs susidūrėte su šiuo failu.

Programos paskirtis – bendras programos aprašas, jos tipas (pvz., naršyklė, medijos leistuvas...) ir jos funkcionalumas.

Pastabos ir papildoma informacija – čia galite pridėti papildomos informacijos arba aprašymą, kuris padėtų apdorojant įtartiną failą.

> Pirmieji trys parametrai yra būtini, kad būtų galima nustatyti teisėtas programas ir atskirti jas nuo kenkėjiško kodo. Pateikdami papildomos informacijos, jūs labai padėsite mūsų laboratorijoms identifikuojant ir apdorojant pavyzdžius.

Pasirinkti pavyzdį analizei – klaidingai aptikta svetainė

Mes prašome pateikti svetaines, kurios aptinkamos kaip užkrėstos arba apgaulingos, bet tokios nėra. Klaidingai teigiami (KT) rezultatai gali būti gaunami, kai failo dalis sutampa su tokia pat dalimi aptikimo modulyje. Prašome pateikti šią svetainę, kad galėtume pagerinti apsaugos nuo virusų ir šnipinėjimo programų modulį ir geriau apsaugoti kitus.

Pastabos ir papildoma informacija – čia galite pridėti papildomos informacijos arba aprašymą, kuris padėtų tvarkant įtartiną svetainę.

Pasirinkti pavyzdį analizei – kitas

Naudokite šią formą, jeigu failas negali būti priskirtas **įtartinų failų** arba **klaidingai teigiamų** kategorijai.

Failo pateikimo priežastis – įveskite išsamų aprašymą ir failo siuntimo priežastį.

Karantinas

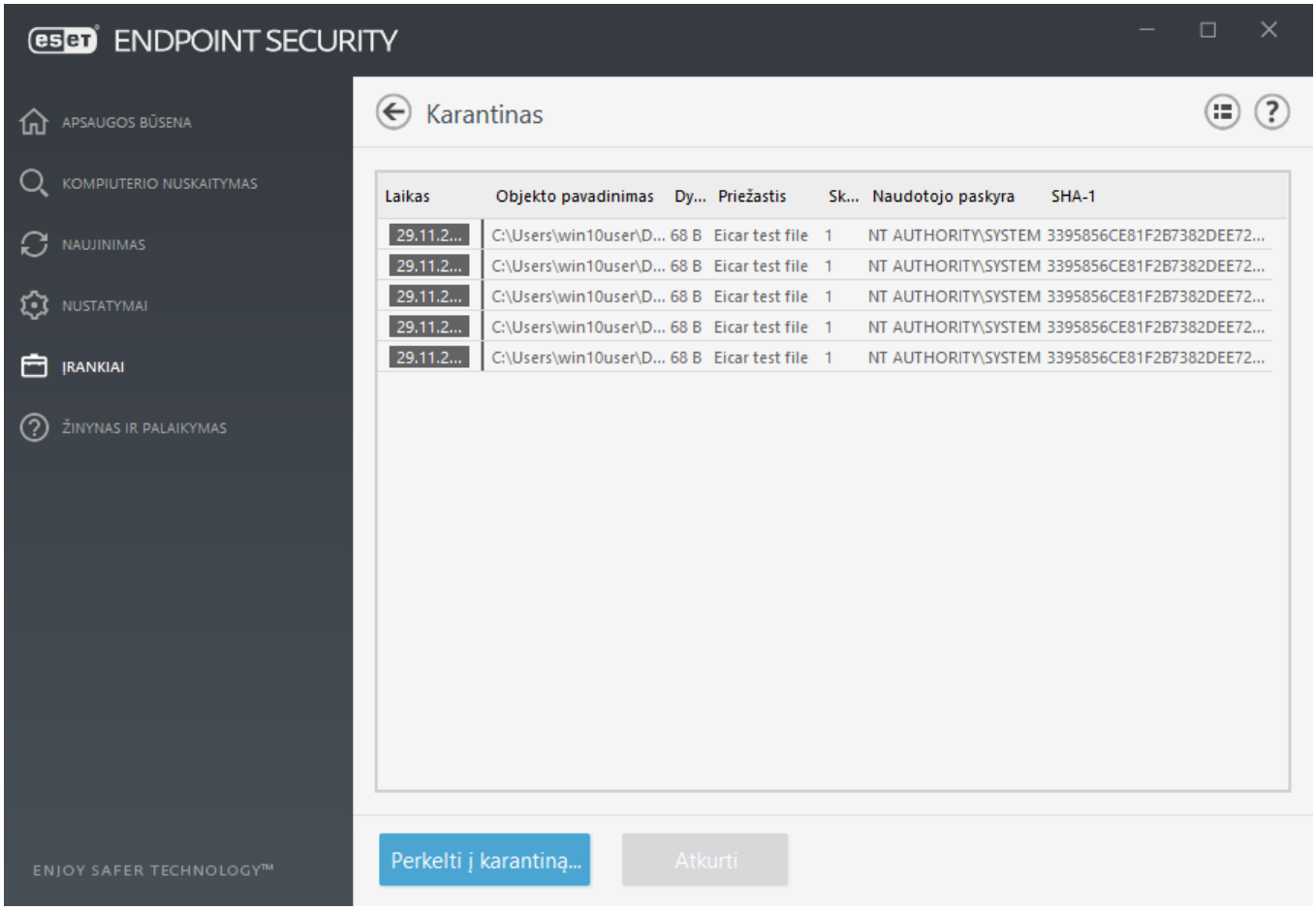
Pagrindinė karantino funkcija – saugiai saugoti objektus, apie kuriuos pranešta (pvz., kenkėjišką programinę įrangą, užkrėstus failus arba galimas nepageidaujamas taikomąsias programas).

Karantiną galima pasiekti ESET Endpoint Security pagrindiniame programos lange spustelėjus **Įrankiai** > **Karantinas**.

Karantino aplanke laikomus failus galima peržiūrėti lentelėje, kurioje rodoma:

- karantinavimo data ir laikas,
- kelias į originalią failo vietą,
- failo dydis baitais,
- priežastis (pvz., objektą pridėjo naudotojas),
- aptikimų skaičius (pvz., pasikartojantys to paties failo aptikimai arba archyvas, kuriame yra keli įsiskverbimai).

- Valdau kliento darbo stočių karantiną nuotoliniu būdu



Failų karantinavimas

ESET Endpoint Security automatiškai karantinuoja pašalintus failus (jei neatšaukėte šios parinkties įspėjimų lange).

Papildomus failus reikėtų karantinuoti, jeigu:

a. jų negalima išvalyti,
b. nesaugu arba nepatartina jų pašalinti,
c. juos klaidingai aptiko ESET Endpoint Security,
d. failai įtartinai atrodo, tačiau jų neaptinka skaitytuvas.

Norėdami karantinuoti failą, galite rinktis iš šių galimybių:

a. failui karantinuoti rankiniu būdu galite naudoti funkciją „Nuvilkti“ – tiesiog spustelėkite failą ir laikydami nuspaudę pelės mygtuką perkelkite pelės žymeklį į pažymėtą sritį, tada mygtuką atleiskite. Tada programa perkeliama į pirmą planą.
b. Spustelėkite **Perkelti į karantiną** pagrindiniame programos lange.
c. Tam galima naudoti ir kontekstinį meniu – spustelėkite dešiniuoju pelės klavišu langą **Karantinas** ir

pasirinkite **Karantinuoti**.

Atkūrimas iš karantino

Karantinuotus failus taip pat galima atkurti į jų originalią vietą:

- Šiuo tikslu naudokite funkciją **Atkurti**, kuri pasiekiama kontekstiniame meniu, dešiniuoju pelės klavišu spustelėjus nurodytą karantinuotą failą.
- Jei failas pažymėtas kaip galima nepageidaujama taikomoji programa, aktyvinta parinktis **Atkurti ir neįtraukti į nuskaitymą**. Taip pat žr. skiltį Išimtys.
- Be to, kontekstiniame meniu siūloma parinktis **Atkurti į**, kuri leidžia atkurti failą į kitą vietą (ne į tą, iš kurios jis buvo pašalintas).
- Atkūrimo funkcija kai kuriais atvejais nepasiekiama, pvz., failams, esantiems tik skaitomoje tinklo dalyje.

Pašalinimas iš karantino

Spustelėkite dešiniuoju pelės klavišu pateiktą elementą ir pasirinkite **Naikinti iš karantino** arba pasirinkite norimą naikinti elementą ir klaviatūroje paspauskite klavišą **Delete**. Galite pasirinkti kelis failus ir panaikinti juos vienu kartu. Panaikinti elementai bus visam laikui pašalinti iš jūsų įrenginio ir karantino.

Failų pateikimas iš karantino

Jeigu karantinavote įtartiną failą, kurio neaptiko programa, arba jeigu failas buvo neteisingai nustatytas kaip užkrėstas (pvz., atliekant kodo euristikos analizę) ir todėl izoliuotas karantinui, nusiųskite pavyzdį išanalizuoti ESET tyrimų laboratorijai. Norėdami pateikti failą, spustelėkite jį dešiniuoju pelės klavišu ir pasirinkite **Pateikti analizuoti** iš kontekstinio meniu.

Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
- Valdyti karantiną ESET PROTECT
- Mano ESET produktas pranešė apie aptikimą. Ką man daryti?

Įgaliotojo serverio nustatymas

Dideliuose LAN tinkluose jūsų kompiuterio ryšiui su internetu gali tarpininkauti įgaliotasis serveris. Naudojant tokią konfigūraciją reikia nustatyti toliau pateikiamus parametrus. Kitaip programa negalės automatiškai atsinaujinti. Programoje ESET Endpoint Security įgaliotąjį serverį nustatyti galima dviejose skirtingose išplėstinio nustatymo medžio vietose.

Pirmiausia įgaliotojo serverio parametrus galima konfigūruoti pasirinkus **Išplėstinis nustatymai** iš **Įrankiai** > **Įgaliotasis serveris**. Nurodžius įgaliotąjį serverį šiame lygmenyje, nustatomi visuotiniai įgaliotojo serverio parametrai visai programai ESET Endpoint Security. Čia nustatytus parametrus naudos visi moduliai, kuriems reikia jungtis prie interneto.

Jei norite nurodyti šio lygmens įgaliotojo serverio parametrus, pasirinkite **Naudoti įgaliotąjį serverį**, tada įveskite įgaliotojo serverio adresą į lauką **Įgaliotasis serveris** kartu su įgaliotojo serverio **Prievado** numeriu.

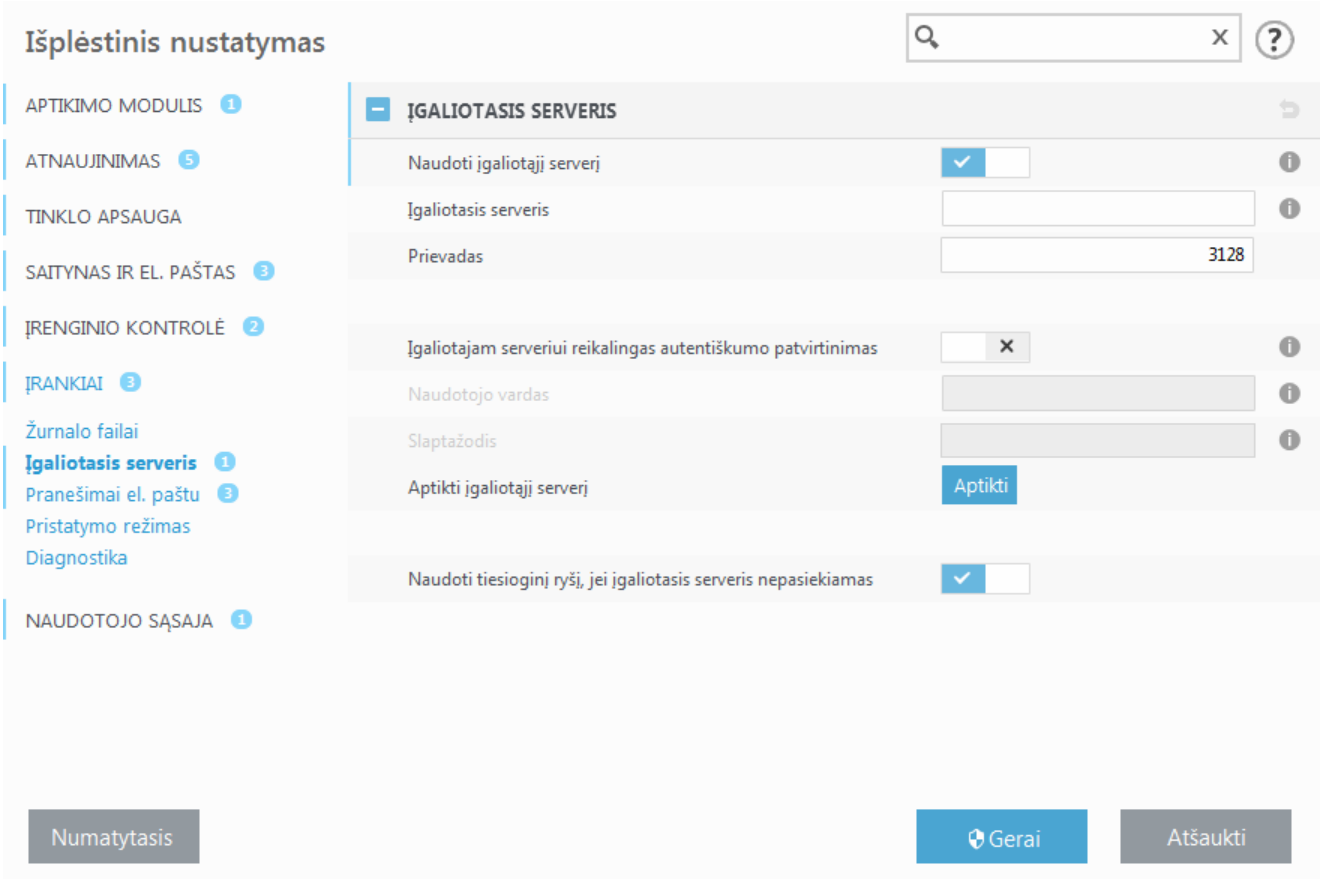
Jeigu ryšiui su įgaliotuoju serveriu reikalingas atpažinimas, pasirinkite **Įgaliotajam serveriui reikalingas atpažinimas** ir į atitinkamus laukus **Naudotojo vardas** bei **Slaptažodis** įveskite reikiamą informaciją. Spustelėkite **Aptikti įgaliotąjį serverį**, kad būtų automatiškai aptikti ir susieti įgaliotojo serverio nustatymai. Bus nukopijuoti

operacinėje sistemoje nurodyti parametrai. Norėdami rasti įgaliotojo serverio nustatymus operacinėje sistemoje, paspauskite sparčiuosius klavišus **Windows + I** ir spustelėkite **Tinklas ir internetas** > **Įgaliotasis serveris**.

Įgaliotojo serverio parametruose vartotojo vardą ir slaptažodį turite įvesti rankiniu būdu.

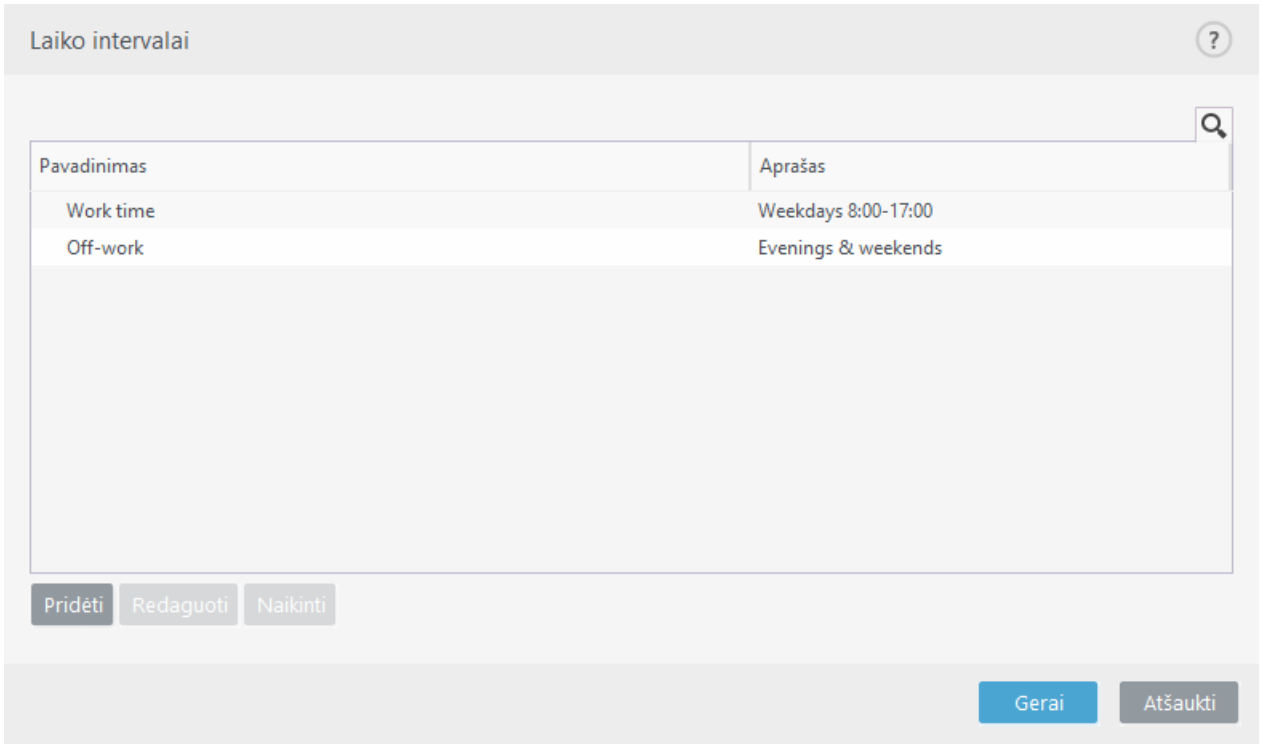
Naudoti tiesioginį ryšį, jei įgaliotasis serveris nepasiekiamas – jei ESET Endpoint Security yra sukonfigūruotas, kad prisijungtų naudojant įgaliotąjį serverį, o šis serveris yra nepasiekiamas, ESET Endpoint Security nepaisys įgaliotojo serverio ir jungsis prie ESET serverių tiesiogiai.

Įgaliotojo serverio parametrus galima parinkti ir išplėstinio naujinimo nustatymuose (**Išplėstinis nustatymas** > **Naujinimas** > **Profiliai** > **Naujinimai** > **Ryšio parinktys** pasirenkant išskleidžiamojo meniu **Įgaliotojo serverio režimas** punktą **Jungtis per įgaliotąjį serverį**). Šis parametras taikomas duotam naujinimo profiliui ir yra rekomenduojamas nešiojamiesiems kompiuteriams, kurie dažnai gauna aptikimo modulio naujinimų iš nuotolinių vietų. Daugiau informacijos apie šį parametrą rasite skyriuje Išplėstinis naujinimo nustatymai.



Laiko intervalai

Laiko intervalai gali būti sukurti ir vėliau priskirti taisyklėms, skirtoms „**Device control**“ (įrenginio kontrolė) ir „**Web control**“ (saityno kontrolė). Nustatymą „**Time slots**“ (laiko intervalai) galima rasti skiltyje „**Advanced setup**“ (išplėstiniai nustatymai) > „**Tools**“ (įrankiai). Taip galima nustatyti dažniausiai naudojamus laiko intervalus (pvz., darbo laiką, savaitgalį ir t. t.) ir juos lengvai pakartotinai panaudoti, iš naujo neapibrėžiant kiekvienai taisyklei skirtų laiko intervalų. Laiko intervalas taikomas bet kuriam atitinkamam taisyklės tipui, kuris palaiko laiko kontrolę.



Norėdami sukurti laiko intervalą, atlikite toliau nurodytus veiksmus.

1. Spustelėkite „**Edit**“ (redaguoti) > „**Add**“ (pridėti).
2. Įveskite laiko intervalo pavadinimą bei **aprašymą** ir spustelėkite „**Add**“ (pridėti).
3. Nurodykite laiko intervalo dieną ir pradžios bei pabaigos laiką arba pasirinkite „**All day**“ (visa diena).
4. Spustelėdami **Gerai** patvirtinkite pasirinkimą.

Vieną laiko intervalą galima apibrėžti vienu ar keliais laiko diapazonais, atsižvelgiant į dienas ir laiką. Sukūrus laiko intervalą, jis bus rodomas išskleidžiamajame meniu „**Apply during**“ (taikyti per), esančiame įrenginio kontrolės taisyklių rengyklės lange arba saityno kontrolės taisyklių rengyklės lange.

„Microsoft Windows“ naujinimas

„Windows“ naujinimo funkcija yra svarbus komponentas apsaugant vartotojus nuo kenkėjiškų programų. Todėl labai svarbu, kad įdiegtumėte „Microsoft Windows“ naujinimus, kai tik jie atsiranda. ESET Endpoint Security įspėja jus apie trūkstamus naujinimus, atsižvelgiant į jūsų nurodytą lygį. Galimi šie lygiai:

- **Naujinimų nėra** – nebus siūloma atsisiųsti jokių sisteminių naujinimų.
- **Pasirinktiniai naujinimai** – bus siūloma atsisiųsti naujinimus, pažymėtus kaip žemo prioriteto ir aukštesnius.
- **Rekomenduojami naujinimai** – bus siūloma atsisiųsti naujinimus, pažymėtus kaip įprastus ir aukštesnius.
- **Svarbūs naujinimai** – bus siūloma atsisiųsti naujinimus, pažymėtus kaip svarbius ir aukštesnius.
- **Kritiniai naujinimai** – bus siūloma atsisiųsti tik kritinius naujinimus.

Spustelėkite **Gerai**, kad būtų įrašyti keitimai. Sistemos naujinimų langas bus rodomas atlikus naujinimo serverio būsenos patikrinimą. Atitinkamai sistemos naujinimo informacija gali būti ne iškart pasiekiama išsaugojus pakeitimus.

Licencijos intervalų patikra

ESET Endpoint Security reikia automatiškai prisijungti prie ESET serverių. Norėdami pakeisti šį nustatymą, eikite į **Išplėstinis nustatymas (F5)** > **Įrankiai** > **Licencija**. Pagal numatytuosius nustatymus **Intervalų patikra** nustatyta **Automatinis** ir ESET licencijų serveris tikrina produktą keletą kartų per valandą. Jei padidėja tinklo duomenų srautas, pakeiskite nustatymus į **Ribotas**, kad numažintumėte perkrovą. Pasirinkus **Ribotas**, ESET Endpoint Security tikrina licenciją tik kartą per dieną arba paleidus kompiuterį iš naujo.

Nustačius **Intervalo patikra** į **Ribotas**, visi licencijos pakeitimai, atlikti per ESET Business Account /ESET MSP Administrator, gali būti pritaikyti ESET Endpoint Security nustatymams per vieną dieną.

Vartotojo sąsaja

Skyriuje **Vartotojo sąsaja** galima konfigūruoti programos grafinės vartotojo sąsajos savybes (GUI).

Naudodami įrankį Vartotojo sąsajos elementai, galite koreguoti programos išvaizdą ir naudojamus efektus.

Jeigu norite užtikrinti maksimalų savo saugumo programinės įrangos saugumą, galite neleisti jokių neįgaliotų keitimų, naudodami Prieigos nustatymo įrankį.

Konfigūruodami Perspėjimus ir pranešimų langus ir Pranešimus galite pakeisti aptikimų įspėjimų ir sistemos pranešimų veikimo pobūdį. Juos galite pritaikyti pagal savo poreikius.

Jei pasirinksite nerodyti kai kurių pranešimų, jie bus rodomi **Vartotojo sąsajos elementai** > **Programų būsenos**. Čia galite pasitikrinti jų būseną arba išjungti šiuos pranešimus.

Dešiniuoju pelės klavišu spustelėjus pasirinktą objektą, rodomos Integravimo į kontekstinį meniu priemonės. Naudokite šį įrankį, jeigu norite integruoti ESET Endpoint Security valdymo elementus į kontekstinį meniu.

Pristatymo režimas yra naudingas vartotojams, kurie nori dirbti su programa nepertraukiami iškylančiųjų langų, planinių užduočių ir bet kokių komponentų, kurie gali apkrauti procesorių bei RAM.

Taip pat žr. Kaip sumažinti ESET Endpoint Security naudotojo sąsają (naudinga valdomose aplinkose).

Naudotojo sąsajos elementai

Vartotojo sąsajos konfigūracijos parinktys programoje ESET Endpoint Security leidžia koreguoti darbinę aplinką pagal savo poreikius. Šios konfigūracijos parinktys yra pasiekiamos per **Vartotojo sąsaja** > **Vartotojo sąsajos elementai**, ESET Endpoint Security išplėstiniuose nustatymuose.

Skyriuje **Vartotojo sąsajos elementai** galima nustatyti darbinę aplinką. Išskleidžiamajame meniu **Paleidimo režimas** galite pasirinkti tokius grafinės vartotojo sąsajos (GUI) paleidimo režimus:

Visa – rodoma visa grafinė vartotojo sąsaja.

Minimali – GUI veikia, tačiau vartotojui rodomi tik pranešimai.

Rankinė – GUI nebuvo paleista automatiškai prisijungiant. Ją rankiniu būdu gali paleisti bet kuris naudotojas.

Tylioji – GUI neveikia ir nerodoma nei pranešimų, nei perspėjimų. Šis režimas naudingas valdomose aplinkose tais atvejais, kai reikia sumažinti naudojamus sistemos išteklius. Tylųjį režimą gali įjungti tik administratorius.

> Kai pasirenkamas minimalios GUI paleidimo režimas, o kompiuteris paleidžiamas iš naujo, pranešimai bus rodomi, o grafinė sąsaja – ne. Jei norite išjungti visos grafinės vartotojo sąsajos režimą, naudodami pradžios meniu parinktį **Visos programos** > **ESET** > ESET Endpoint Security paleiskite GUI administratorius teisėmis arba tai galite padaryti per ESET PROTECT naudodami politika.

Jeigu norite deaktyvinti ESET Endpoint Security prisistatymo langą, panaikinkite žymėjimą nuo parinkties **Rodyti prisistatymo langą paleidžiant kompiuterį**.

Jei norite, kad ESET Endpoint Security pagrotų garsą, kai nuskaitymo metu įvyksta kas nors svarbaus, pvz., kai aptinkama grėsmė arba baigiamas nuskaitymas, pasirinkite **Naudoti garso signalą**.

Integruoti į kontekstinį meniu – integruoti ESET Endpoint Security valdymo elementus į kontekstinį meniu.

Būsenos

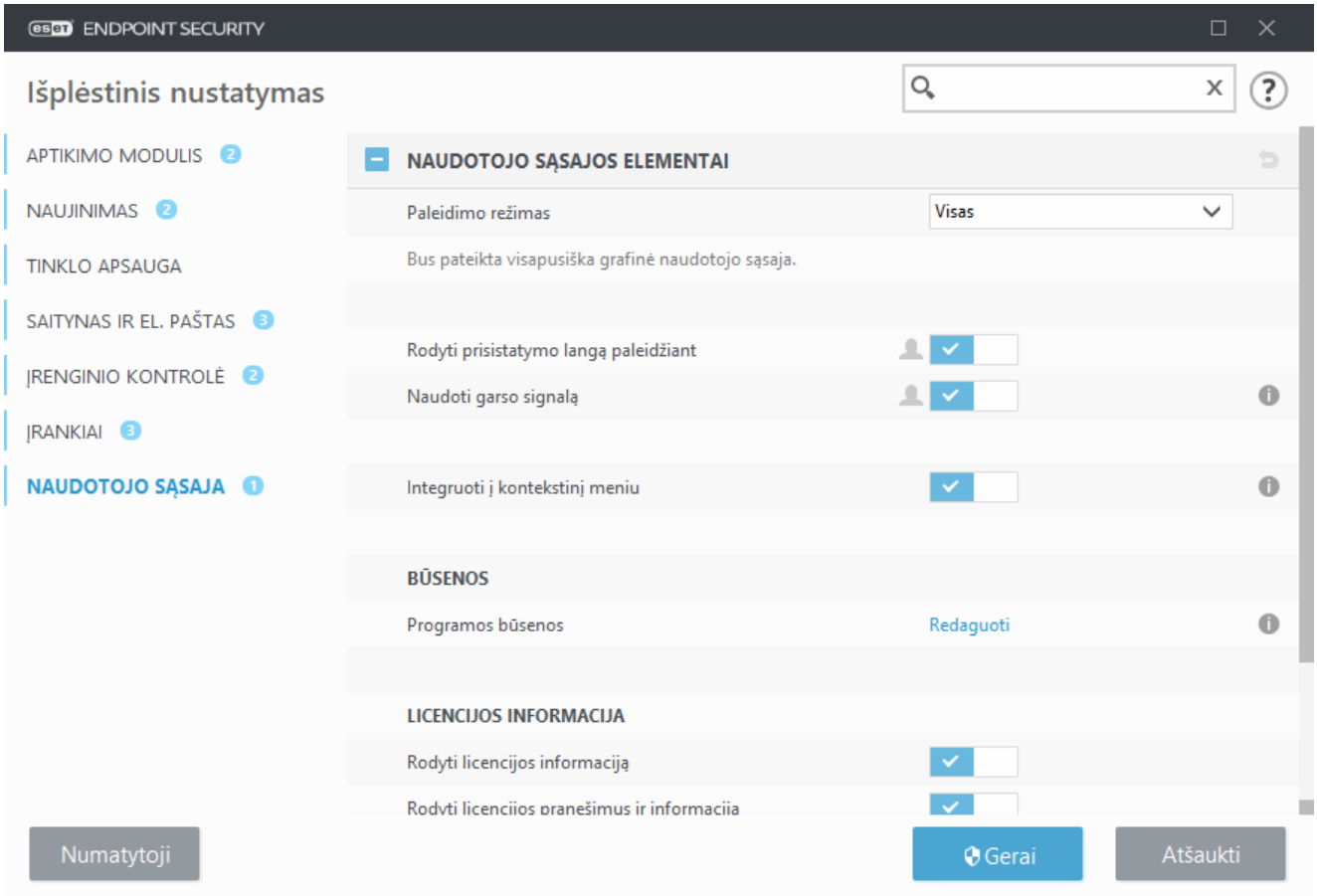
Programų būsenos – spustelėkite mygtuką **Redaguoti**, kad galėtumėte tvarkyti (išjungti) būsenas, rodomas pagrindinio meniu polangyje **Apsaugos būsena**.

Licencijos informacija

Rodyti licencijos informaciją – kai išjungta, licencijos galiojimo data languose **Apsaugos būsena** ir **Žinynas ir palaikymas** nebus rodoma.

Rodyti licencijos pranešimus ir informaciją – kai išjungta, pranešimai ir perspėjimai bus rodomi tik kai baigsis licencijos galiojimas.

> Licencijos informacijos nustatymai taikomi, tačiau nėra pasiekiami ESET Endpoint Security aktyvintam pagal MSP licenciją.



Prieigos nustatymas

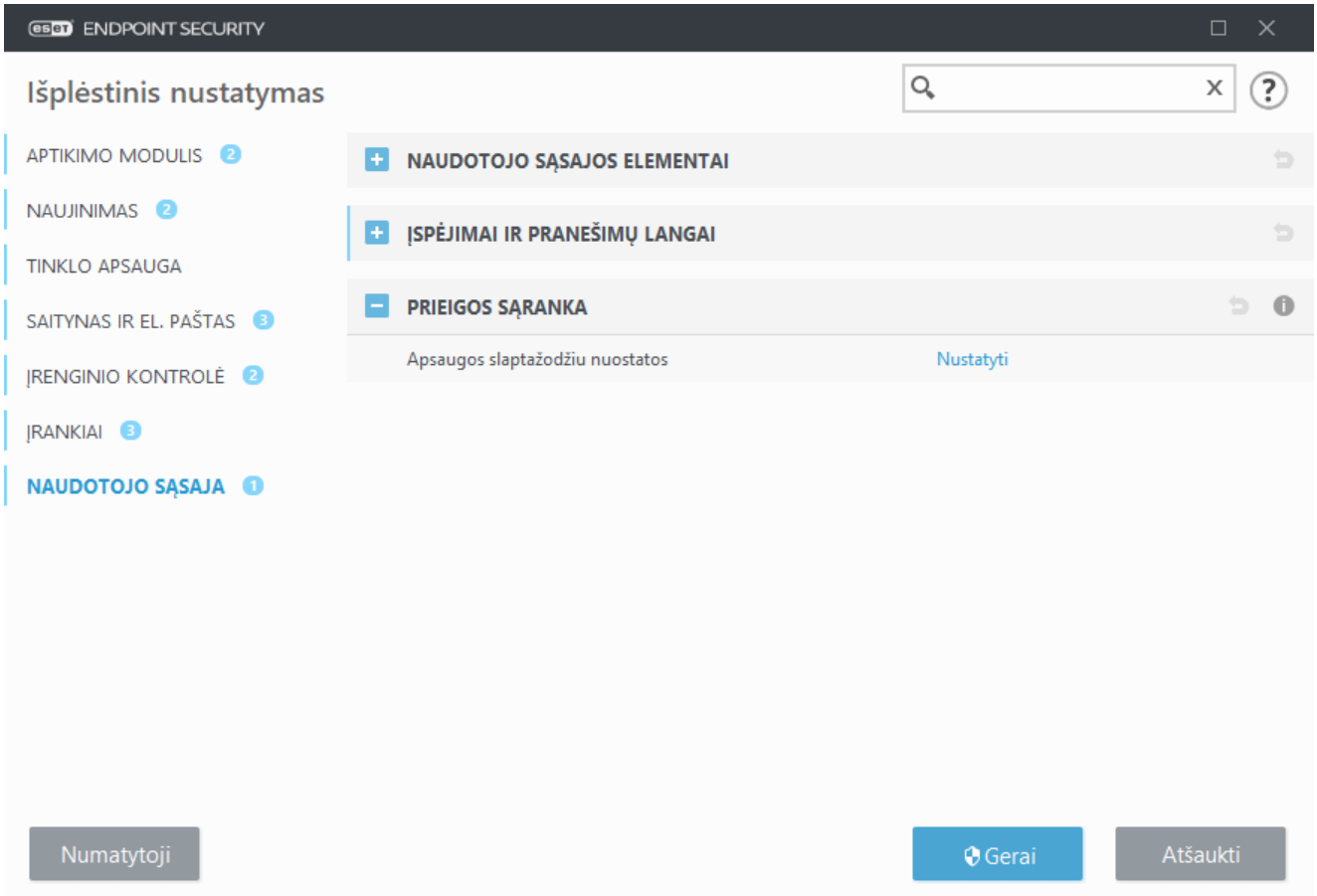
Kad būtų užtikrinta maksimali jūsų sistemos apsauga, ESET Endpoint Security turi būti tinkamai sukonfigūruota. Dėl bet kokių nekvalifikuotų keitimų galite prarasti svarbius duomenis. Kad išvengtumėte neįgaliotų keitimų, ESET Endpoint Security nustatymų parametrus galite apsaugoti slaptažodžiu.

Valdomos aplinkos

Administratorius gali sukurti politiką, skirtą slaptažodžiu apsaugoti prijungtuose kliento kompiuteriuose esančio ESET Endpoint Security nustatymus. Norėdami sukurti naują politiką, žr. Slaptažodžiu apsaugoti nustatymai.

Nevaldomas

Konfigūracijos nustatymai apsaugai slaptažodžiu yra **Išplėstinis nustatymas** (**F5**) dalyje **Naudotojo sąsaja** > **Prieigos nustatymas**.



Slaptažodžio apsaugos parametrai – pasirinkite slaptažodžio parametrus. Spustelėkite, kad atvertumėte slaptažodžio nustatymų langą.

Jei norite nustatyti ar pakeisti slaptažodį, kad apsaugotumėte nustatymo parametrus, spustelėkite **Nustatyti**.

Išplėstinio nustatymo slaptažodis

Kad apsaugotumėte ESET Endpoint Security nustatymų parametrus ir išvengtumėte neleistino modifikavimo, turi būti nustatytas naujas slaptažodis.

Valdomos aplinkos

Administratorius gali sukurti politiką, skirtą slaptažodžiu apsaugoti prijungtuose kliento kompiuteriuose esančio ESET Endpoint Security nustatymus. Norėdami sukurti naują politiką, žr. Slaptažodžiu apsaugoti nustatymai.

Nevaldomas

Prireikus pakeisti esamą slaptažodį:

1. įveskite senąjį slaptažodį į lauką **Senas slaptažodis**.
2. Įveskite naująjį slaptažodį į laukus **Naujas slaptažodis** ir **Patvirtinti slaptažodį**.
3. Spustelėkite **Gerai**.

Šis slaptažodis vėliau bus reikalingas kaskart modifikuojant ESET Endpoint Security.

Jei pamiršote slaptažodį, galima atkurti prieigą prie išplėstinio nustatymo.

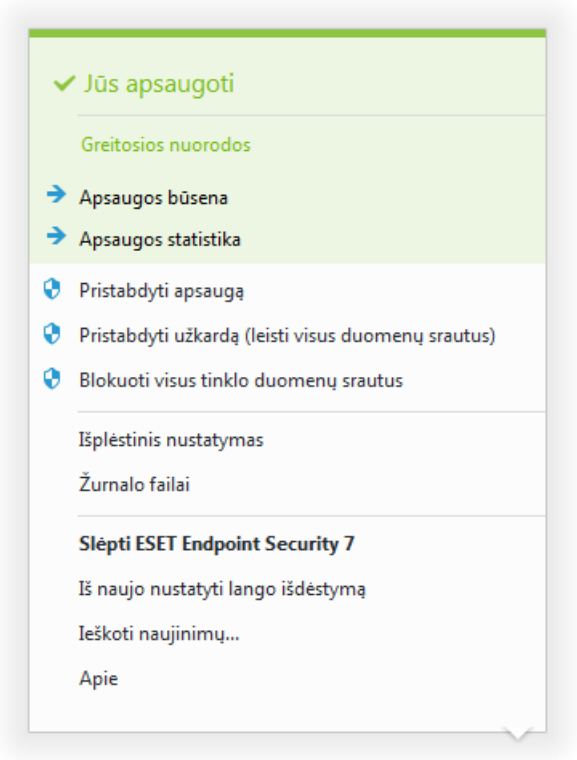
- Atkurkite naudodami būdą „Slaptažodžio atkūrimas“ (7.1 ir naujesnė versija)
- Atkurkite naudodami ESET atrakinimo įrankį (7.0 ir senesnė versija)

Skaitykite daugiau informacijos, jei pamiršote savo ESET išduotą licencijos raktą, iki kada galioja licencija arba kitą ESET Endpoint Security licencijos informaciją.

Sistemos dėklo piktograma

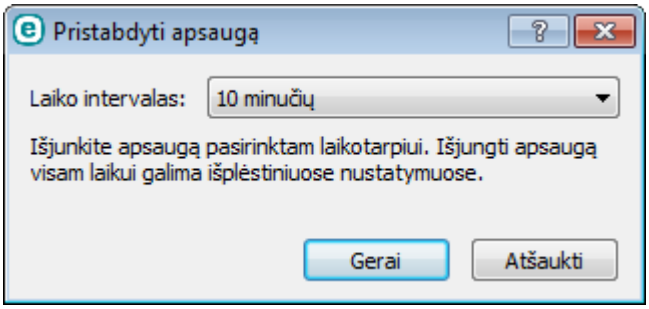
Kai kurias svarbiausias nustatymų parinktis ir funkcijas galima pasiekti dešiniuoju pelės klavišu spustelint sistemos dėklo piktogramą .

Norėdami pasiekti sistemos dėklo piktogramos meniu, įsitikinkite, kad vartotojo sąsajos elementų pradžios režimas nustatytas kaip Visas.



Pristabdyti apsaugą – pateikia patvirtinimo dialogo langą, kuris išjungia Aptikimo modulį, saugantį nuo atakų, kontroliuojančią failus, saityno ir el. pašto ryšį.

Išskleidžiamasis meniu **Laiko intervalas** nurodo laikotarpį, kuriam bus išjungta apsauga.



Pristabdyti užkardą (leisti visus duomenų srautus) – perjungia užkardą į neaktyvią būseną. Žr. Tinklas, kur rasite daugiau informacijos.

Blokuoti visą tinklo srautą – užkarda blokuos visą siunčiamą / gaunamą tinklo ir interneto srautą. Vėl įjungti galite spustelėję **Stabdyti visų tinklo duomenų srautų blokavimą**.

Išplėstiniai nustatymai – nurodykite šią parinktį, kad patektumėte į **Išplėstinių nustatymų** medį. Išplėstinius nustatymus pasieksite ir spustelėdami klavišą F5 arba pasirinkdami **Nustatymai** > **Išplėstiniai nustatymai**.

Žurnalų failai – žurnalų failuose pateikiama informacijos apie visus svarbius programos įvykius ir aptikimų apžvalga.

Atidaryti ESET Endpoint Security – atidaromas pagrindinis ESET Endpoint Security programos langas iš sistemos dėklo piktogramos.

Iš naujo nustatyti langų išdėstymą – atstato ESET Endpoint Security lango numatytąjį dydį ir vietą ekrane.

Ieškoti naujinimų – paleidžia programos naujinimo modulius, kad būtų užtikrinamas jūsų apsaugos nuo kenkėjiškų kodų lygis.

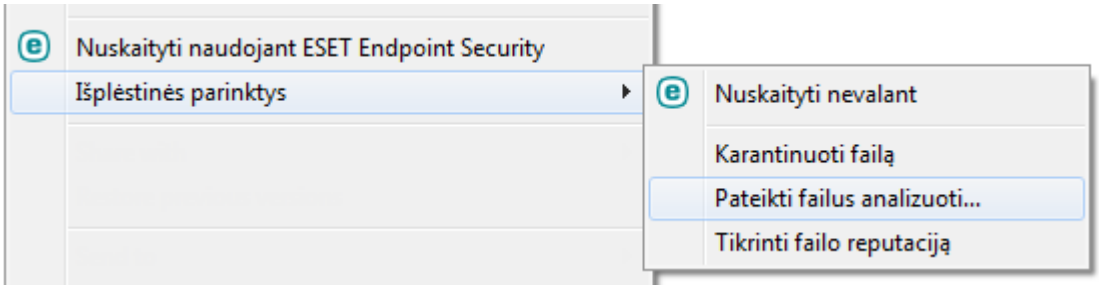
Apie – pateikia informacijos apie sistemą, išsamios informacijos apie įdiegtą ESET Endpoint Security versiją ir programos modulius bei jūsų licencijos galiojimo terminą. Informacijos apie savo operacinę sistemą ir sistemos išteklius rasite puslapio apačioje.

Kontekstinis meniu

Kontekstinis meniu parodomas dešiniuoju pelės klavišu spustelėjus objektą (failą). Meniu išdėstomi visi veiksmai, kuriuos galima atlikti su objektu.

Galima integruoti ESET Endpoint Security valdymo elementus į kontekstinį meniu. Šios funkcijos nustatymų parinktis rasite išplėstinių nustatymų medyje: **Vartotojo sąsaja** > **Vartotojo sąsajos elementai**.

Integruoti į kontekstinį meniu – integruoti ESET Endpoint Security valdymo elementus į kontekstinį meniu.



Žinynas ir palaikymas

ESET Endpoint Security turi sutrikimų šalinimo įrankius ir palaikymo informaciją, kuri padės jums sprendžiant problemos, su kuriomis galite susidurti.

Įdiegtas produktas

- **Apie ESET Endpoint Security** – rodo informaciją apie jūsų ESET Endpoint Security kopiją.
- **Produkto trikčių diagnostika** – spustelėkite šią nuorodą, kad rastumėte dažniausiai pasitaikančių problemų sprendimus.
- **Licencijos trikčių diagnostika** – spustelėkite šią nuorodą, kad rastumėte aktyvinimo arba licencijos keitimo problemų sprendimus.
- **Keisti licenciją** – spustelėkite, kad būtų atidarytas aktyvinimo langas, kuriame galėsite suaktyvinti savo produktą.

 **Žinyno puslapis** – spustelėkite šią nuorodą norėdami patekti į ESET Endpoint Security žinyno puslapius.

 **Techninė pagalba**

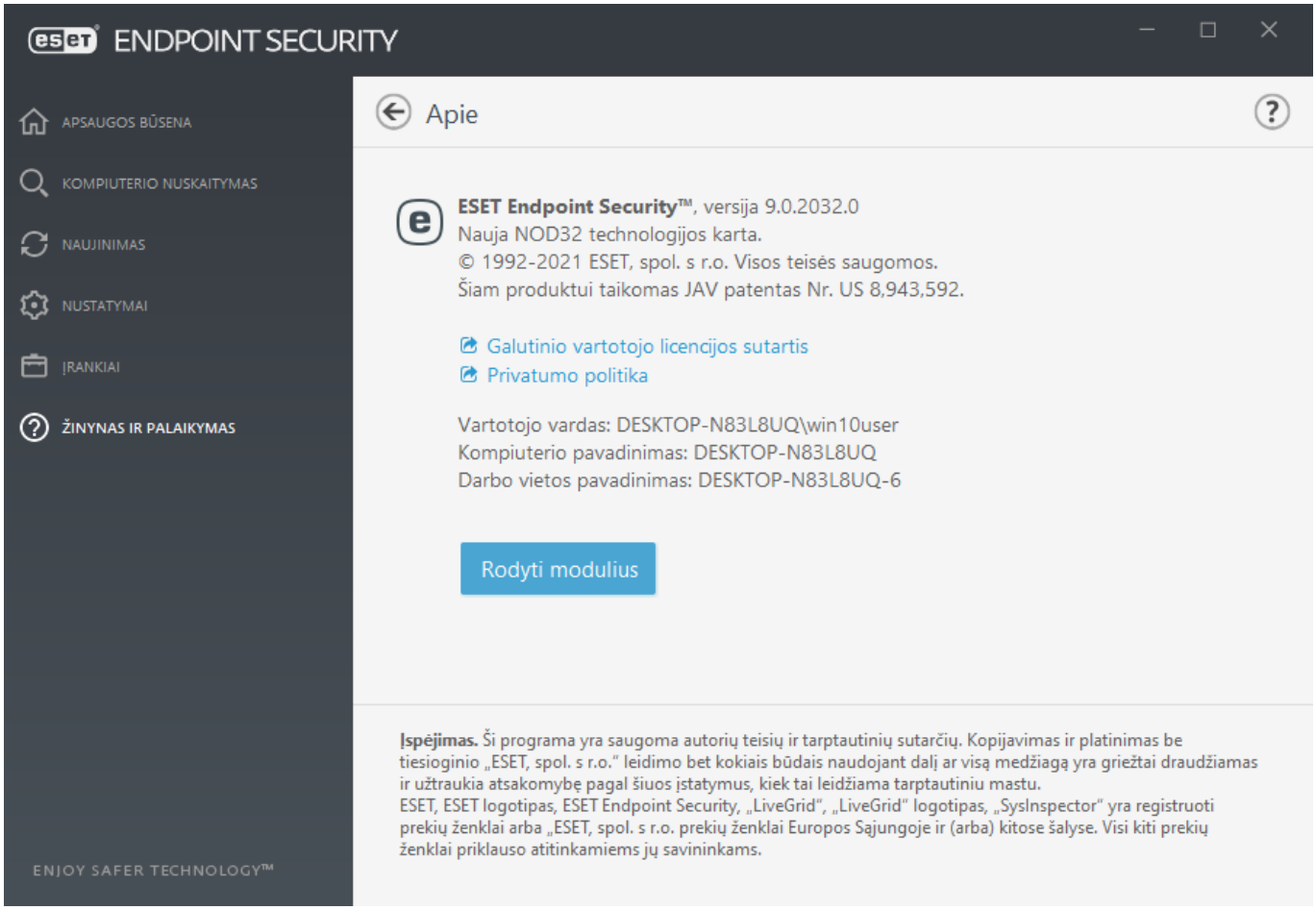
- **Prašyti pagalbos** – jei nepavyksta rasti savo problemos sprendimo, galite naudoti šią formą, esančią ESET svetainėje, kad galėtumėte greitai susisiekti su techninės pagalbos skyriumi. Atsižvelgiant į jūsų nustatymus, prieš pildant saityno formą rodomas sistemos konfigūracijos duomenų pateikimo langas.
- **Išsami informacija apie techninę pagalbą** – kai prašoma, galite nukopijuoti ir nusiųsti informaciją ESET techninės pagalbos tarnybai (pvz., produkto pavadinimą, produkto versiją, operacinę sistemą ir procesoriaus tipą).
- **ESET Log Collector** – saitai į ESET žinių bazės straipsnį, iš kurio galima atsisiųstiESET Log Collector – programą, kuri iš kompiuterio automatiškai renka informaciją ir žurnalus, kad padėtų greičiau spręsti kylančias problemas. Jei pageidaujate daugiau informacijos, žr. ESET Log Collector internetinį vartotojo vadovą.
- Spustelėkite Įjungti išplėstinį registravimą, kad sukurtumėte išplėstinius visų galimų funkcijų žurnalus ir padėtumėte kūrėjams nustatyti ir išspręsti problemas. Nustatytas Diagnostinis minimalaus registravimo daugiažodiškumo lygis. Išplėstinis registravimas bus išjungtas po dviejų valandų, nebent jį sustabdytumėte paspausdami Stabdyti išplėstinį registravimą. Kai visi žurnalai sukurti, pranešimų lange pateikta tiesioginė prieiga prie diagnostikos aplanko, kuriame yra sukurti žurnalai.

 **Žinių bazė** – ESET žinių bazėje yra pateikiami atsakymai į dažniausiai užduodamus klausimus ir rekomenduojami įvairių problemų sprendimai. Reguliariai ESET techninių specialistų naujinama žinių bazė yra galingiausias įrankis sprendžiant įvairiausias problemas.

Apie ESET Endpoint Security

Šiame lange pateikiama išsami informacija apie įdiegtą ESET Endpoint Security versiją, jūsų operacinę sistemą ir sistemos išteklius.

Jei norite peržiūrėti informaciją apie įdiegtų programų modulių ir jų versijų sąrašą, spustelėkite **Rodyti modulius**. Informaciją apie modulius galite nukopijuoti į mainų sritį spustelėdami **Kopijuoti**. Tai gali būti naudinga diagnozuojant sutrikimus arba kreipiantis į techninę pagalbą.



Sistemos konfigūracijos duomenų pateikimas

Kad pagalbą galėtų suteikti kuo greičiau ir tiksliau, ESET reikalauja informacijos apie ESET Endpoint Security konfigūraciją, išsamios sistemos informacijos ir vykdomų procesų („ESET SysInspector" žurnalo failas) bei registro duomenų. ESET šiuos duomenis naudos tik norėdama suteikti klientui techninę pagalbą.

Pateikiant saityno formą jūsų sistemos konfigūracijos duomenys pateikiami ESET. Jei norite šį veiksmą įsiminti ir toliau taikyti šiam procesui, pasirinkite **Visada pateikti šią informaciją**. Jei formą norite pateikti nesiųsdami jokių duomenų, spustelėkite **Neteikti duomenų** ir kreipkitės į ESET techninės pagalbos tarnybą naudodamiesi interneto pagalbos forma.

Šį nustatymą sukonfigūruoti galite ir eidami **Išplėstinis nustatymai** > **Įrankiai** > **Diagnostika** > **Techninė pagalba**.

Jei nusprendžiate pateikti sistemos duomenis, būtina užpildyti ir pateikti saityno formą, kitaip nebus sukurta jūsų kortelė, o sistemos duomenys bus prarasti.

Techninė pagalba

Susisiekti su technine pagalba

Prašyti pagalbos – jei nepavyksta rasti savo problemos sprendimo, galite naudoti ir šią formą, esančią ESET svetainėje, kad galėtumėte greitai susisiekti su ESET techninės pagalbos skyriumi. Atsižvelgiant į jūsų nustatymus, prieš pildant saityno formą rodomas sistemos konfigūracijos duomenų pateikimo langas.

Gaukite informacijos apie techninę pagalbą

Išsami informacija apie techninę pagalbą – kai prašoma, galite nukopijuoti ir nusiųsti informaciją ESET techninės pagalbos tarnybai (pvz., išsamią licencijos informaciją, produkto pavadinimą, produkto versiją, operacinę sistemą ir kompiuterio informaciją).

ESET Log Collector – saitai į ESET žinių bazės straipsnį, iš kurio galima atsisiųstiESET Log Collector – programą, kuri iš kompiuterio automatiškai renka informaciją ir žurnalus, kad padėtų greičiau spręsti kylančias problemas. Jei pageidaujate daugiau informacijos, žr. ESET Log Collector internetinį vartotojo vadovą.

Spustelėkite **Įjungti išplėstinį registravimą**, kad sukurtumėte išplėstinius visų galimų funkcijų žurnalus ir padėtumėte kūrėjams nustatyti ir išspręsti problemas. Nustatytas **Diagnostinis** minimalaus registravimo daugiažodiškumo lygis. Išplėstinis registravimas bus išjungtas po dviejų valandų, nebent jį sustabdytumėte paspausdami **Stabdyti išplėstinį registravimą**. Kai visi žurnalai sukurti, pranešimų lange pateikta tiesioginė prieiga prie diagnostikos aplanko, kuriame yra sukurti žurnalai.

Pranešimai

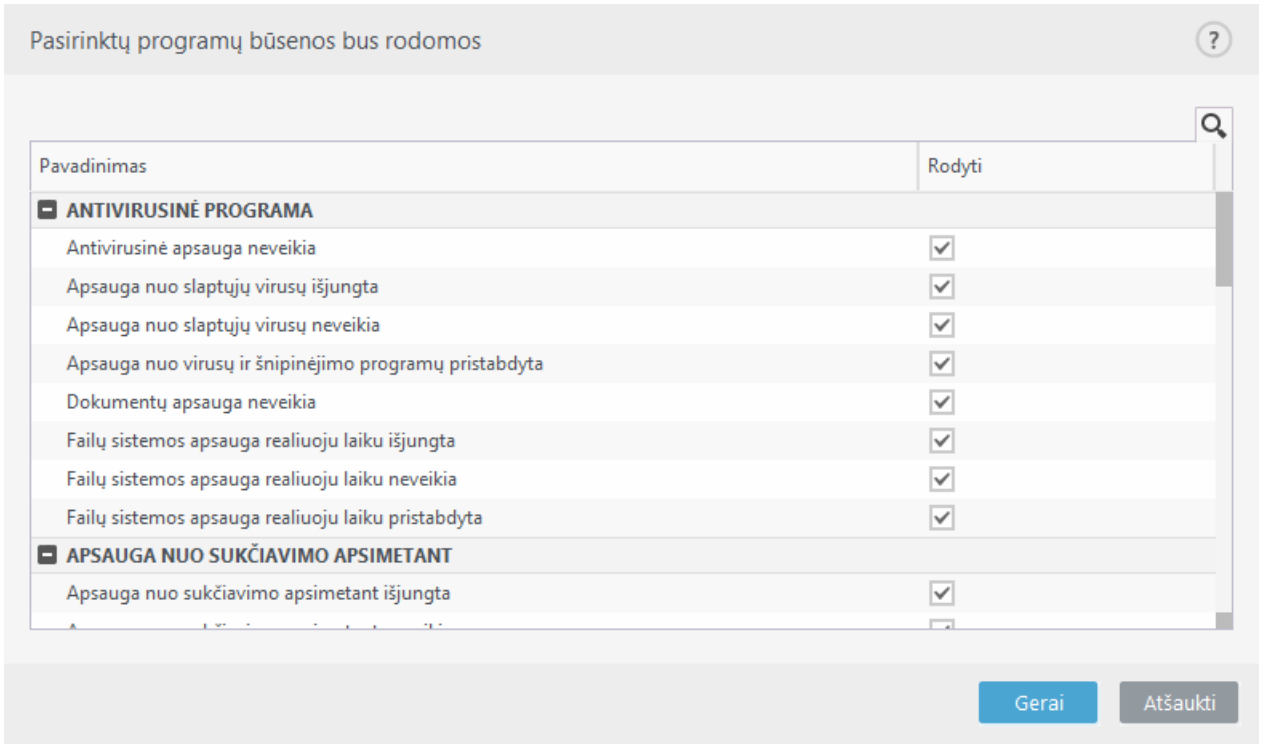
Norėdami tvarkyti ESET Endpoint Security pranešimus, atidarykite **Išplėstiniai nustatymai** (F5) > **Pranešimai**. Galite konfigūruoti šių tipų pranešimus:

- Programos būsenos – spustelėkite **Redaguoti**, kad pasirinktumėte, kurios programos būsenos bus rodomos pagrindinio programos lango pagrindiniame puslapyje.
- Darbalaukio pranešimai – maži iššokantys langai šalia sistemos užduočių juostos.
- Pranešimų tinkinimas – įtraukite pasirinktinį pranešimą, pvz., darbalaukio pranešimą.
- Interaktyvūs įspėjimai – įspėjimo langai ir pranešimų laukeliai, kuriuose reikalinga naudotojo sąveika.
- Peradresavimas (pranešimai el. paštu)– el. pašto pranešimai siunčiami nurodytu el. pašto adresu.

Programos būsenos

Norėdami konfigūruoti, kurios programos būsenos bus rodomos (pvz., kai pristabdysite apsaugą nuo virusų ir šnipinėjimo programų arba įjungsite žaidėjo režimą), atidarykite **Išplėstinis nustatymas** (F5) > **Pranešimai** ir spustelėkite **Redaguoti**, kad pasirinktumėte, kurios programos būsenos bus rodomos pagrindinio programos lango pagrindiniame skyriuje.

Programos būsena bus rodoma ir tada, jei jūsų produktas nesuaktyvintas arba baigė galioti jūsų licencija. Šį nustatymą galima pakeisti naudojantis ESET PROTECT politikomis.



Darbalaukio pranešimai

Darbalaukio pranešimas pateikiamas nedideliame iššokančiame lange šalia sistemos užduočių juostos. Pagal numatytuosius nustatymus jis rodomas 10 sekundžių, tada lėtai išnyksta. Tai yra pagrindinis ESET Endpoint Security bendravimo su naudotoju būdas, kuriuo pranešama apie sėkmingus produktų atnaujinimus, naujus įrenginius, virusų nuskaitymo užduotis arba naują grėsmę.

Rodyti pranešimus darbalaukyje – rekomenduojame palikti šią parinktį, kad produktas galėtų informuoti jus apie naujus įvykius.

Darbalaukio pranešimai – spustelėkite **Redaguoti**, kad įjungtumėte arba išjungtumėte konkrečius Darbalaukio pranešimus.

Nerodyti pranešimų, kai programos veikia viso ekrano režimu – nerodyti visų neinteraktyvių pranešimų, kai programos veikia viso ekrano režimu.

Laiko baigtis (sek.) – nustatykite pranešimo matomumo trukmę. Reikšmė turi būti nuo 3 iki 30 sekundžių.

Skaidrumas – nustatykite pranešimo skaidrumo procentą. Palaikomas intervalas yra nuo 0 (neskaidrus) iki 80 (labai skaidrus).

Minimalus rodomų įvykių daugiažodiškumas – nustatykite rodomą pradinį pranešimo svarbos lygį. Išplečiamajame meniu pasirinkite vieną iš šių parinkčių:

- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau paminėtus įrašus.
- **Informacija** – įrašo informacinius pranešimus, pvz., neįprastus tinklo įvykius, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – registruoja kritines klaidas ir įspėjamuosius pranešimus (apsauga nuo slaptųjų virusų veikia netinkamai arba nepavyko atnaujinti).
- **Klaidos** – registruojamos klaidos (nepaleista dokumento apsauga) ir kritinės klaidos.

- **Kritiniai** – registruoja tik kritines klaidas (klaida paleidžiant apsaugą nuo virusų arba sistema užkrėsta).

Kelių naudotojų sistemose rodyti pranešimus šio naudotojo ekrane – leidžia pasirinktoms paskyroms gauti darbalaukio pranešimus. Pavyzdžiui, jei nenaudojate administratoriaus paskyros, įveskite visą paskyros pavadinimą ir bus rodomi nurodytos paskyros darbalaukio pranešimai. Darbalaukio pranešimus gali gauti tik viena naudotojo paskyra.

Leisti daugiausia dėmesio ekrane skirti pranešimams – daugiausia dėmesio ekrane bus skiriama pranešimams ir jie bus pasiekiami spustelėjus klavišus Alt+Tab.

Dialogo langas - darbalaukio pranešimai

Norėdami pakoreguoti darbalaukio pranešimų matomumą (rodoma ekrano apatinėje dešinėje dalyje), atidarykite **Išplėstinis nustatymas** (F5) > **Pranešimai** > **Darbalaukio pranešimai**. Spustelėkite **Redaguoti** šalia **Darbalaukio pranešimai** ir pasirinkite atitinkamą **Rodyti darbalaukyje** žymės langelį.

Jei norite nustatyti pranešimus **Failai išanalizuoti** ir **Failai neišanalizuoti**, kai naudojate ESET LiveGuard, Aktyvioji apsauga turi būti nustatyta kaip **Blokuoti vykdymą, kol bus gautas analizės rezultatas**.

Pranešimų tinkinimas

Šiame lange galite tinkinti pranešimų tekstą.

Numatytasis pranešimo tekstas – pranešimo apačioje bus rodomas numatytasis tekstas.

Aptikimai

Įjunkite **Neuždaryti automatiškai pranešimų apie kenkėjiškas programas,** jei norite, kad pranešimai apie kenkėjiškas programas liktų ekrane tol, kol bus uždaryti rankiniu būdu.

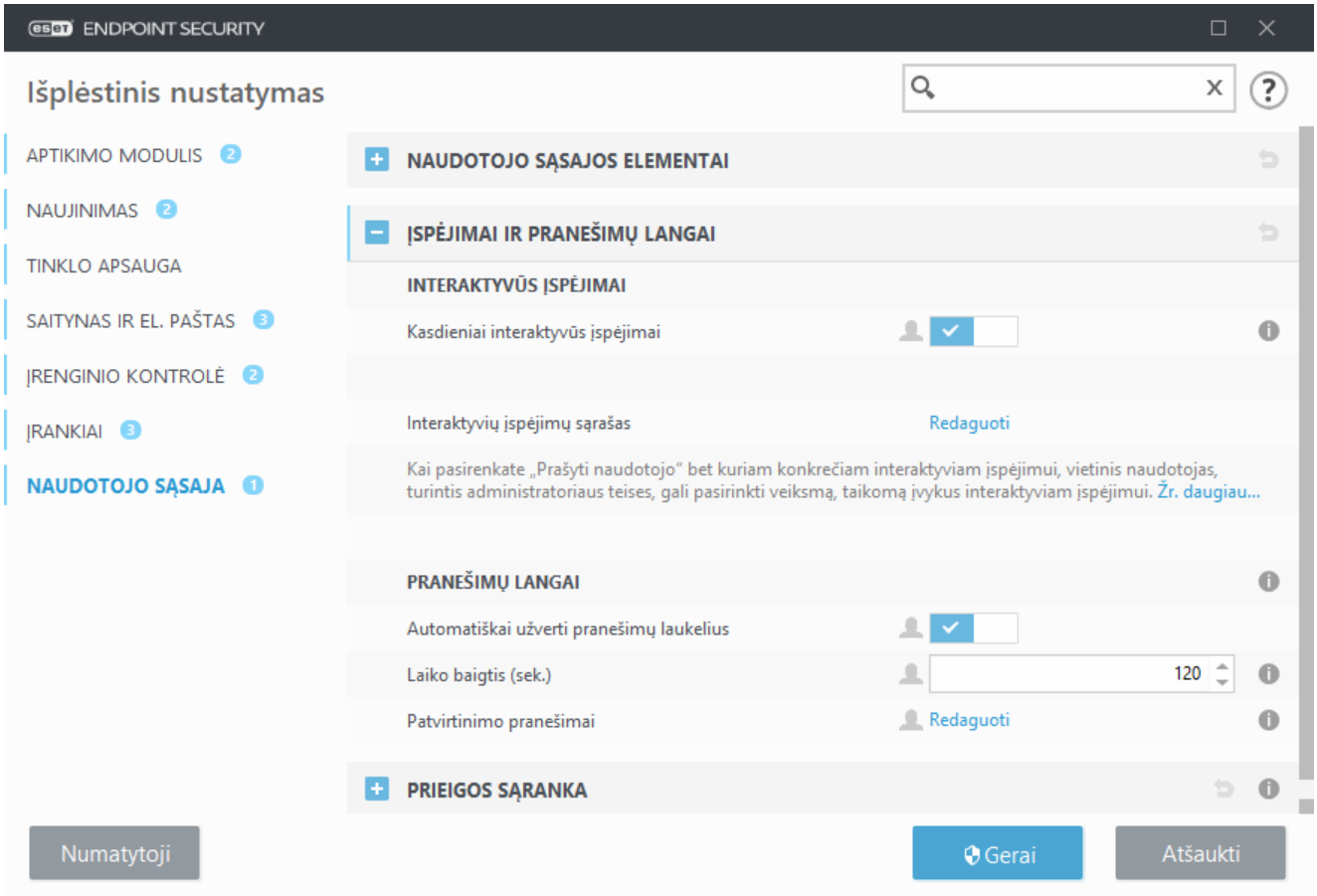
Išjunkite **Naudoti numatytąjį tekstą** ir lauke **Aptikimo pranešimo tekstas** įveskite savo pačių tekstą, jei norite, kad būtų rodomas tinkintas pranešimo tekstas.

Interaktyvūs įspėjimai

Ieškote informacijos apie bendruosius perspėjimus ir pranešimus?
- Rasta grėsmė
- Adresas užblokuotas.
- Produktas nesuaktyvintas
- Prieinamas naujinimas
- Naujinimo informacija netinkama
- Pranešimo „Modulių naujinimas nepavyko“ trikčių šalinimas
- „Failas sugadintas“ arba „Nepavyko pervadinti failo“
- Interneto svetainės sertifikatas atšauktas
- Užblokuota tinklo grėsmė
- Failas užblokuotas dėl analizės

Skyriaus **Interaktyvieji įspėjimai** dalyje **Pranešimai** galima konfigūruoti, kaip ESET Endpoint Security apdoroja

aptikimus, kurių atveju naudotojas turi priimti sprendimą (pvz., aptikus galimą apsimestinę svetainę).



Interaktyvūs įspėjimai

Interaktyvūs įspėjimo langai rodomi radus aptikimo funkciją arba jei naudotojas turi atlikti veiksmų.

Kasdieniai interaktyvūs įspėjimai

- Nevaldomiems naudotojams rekomenduojame palikti šios parinkties numatytąjį nustatymą (įjungta).
- Valdomiems naudotojams palikite šį nustatymą įjungtą ir pasirinkite iš anksto nustatytą veiksmą naudotojams Interaktyvių įspėjimų sąraše.

Išjungus **Rodyti interaktyvius perspėjimus** bus slepiami visi perspėjimų langai ir naršyklės dialogo langai. Bus automatiškai pasirinktas iš anksto nustatytas numatytasis veiksmas (pvz., „galima sukčiavimo apsimetant svetainė“ bus užblokuota).

Pranešimų langai

Norėdami po tam tikro laiko automatiškai uždaryti iškylančiuosius langus, nurodykite parinktį **Uždaryti pranešimų langus automatiškai**. Jeigu perspėjimo langai neuždaromi rankiniu būdu, jie bus automatiškai uždaryti pasibaigus nurodytam laikui.

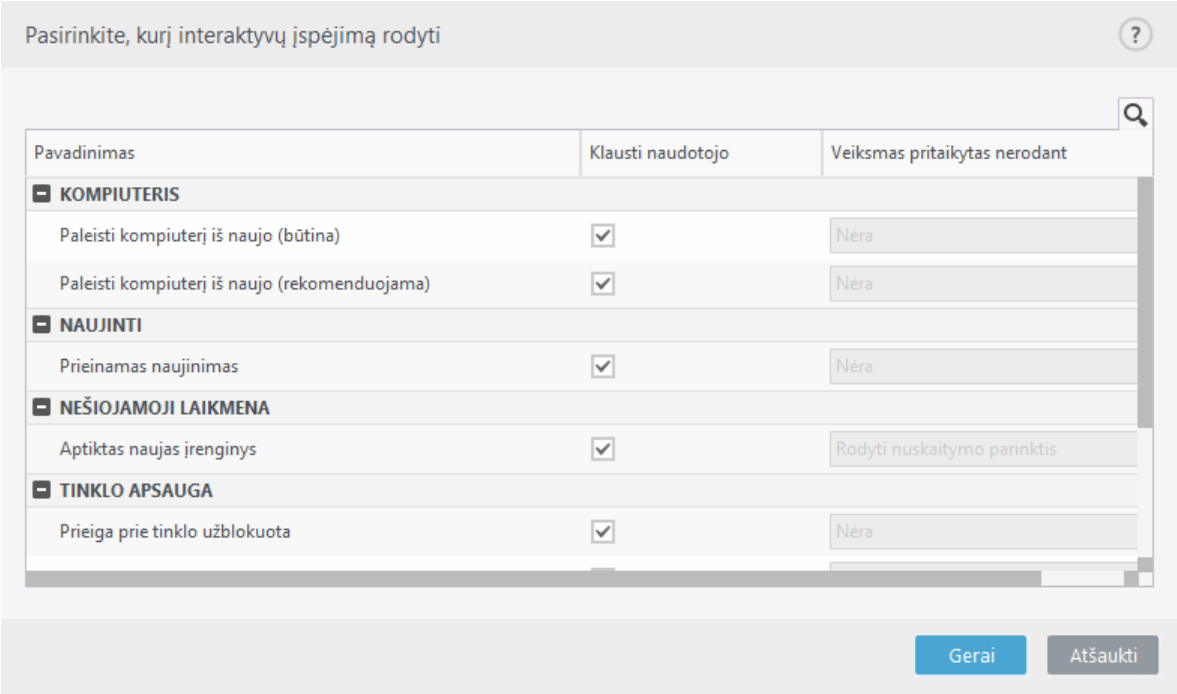
Patvirtinimo pranešimai – parodomas sąrašas su patvirtinimo pranešimais, kuriuos galima pasirinkti rodyti arba nerodyti.

Interaktyvių įspėjimų sąrašas

Šiame skyriuje aprašomi keli interaktyvūs perspėjimo langai, kuriuos ESET Endpoint Security rodys prieš atliekant bet kokį veiksmą.

Norėdami reguliuoti konfigūruojamų interaktyviųjų įspėjimų veikimą, eikite į **Pranešimai** > **Interaktyvieji įspėjimai** ESET Endpoint Security išplėstinio nustatymo medyje ir spustelėkite **Redaguoti**.

> Naudinga valdomose aplinkose, kuriose administratorius gali pašalinti visus pasirinkimus **Klausti naudotojo** ir pasirinkti iš anksto nustatytą veiksmą, taikomą, kai rodomi interaktyvių perspėjimų langai.
> Taip pat žr. programos būsenas produkte.



Informacijos apie konkretaus interaktyvaus įspėjimo langą ieškokite kituose žinyno skyriuose:

Nešiojamoji laikmena

- Aptiktas naujas įrenginys

Saugi naršyklė

- Leisti toliau naudoti numatytąją naršyklę

Tinklo apsauga

- Tinklo prieiga užblokuota rodoma, kai šios darbo vietos kliento užduotis **Izoliuoti kompiuterį nuo tinklo** paleidžiama iš ESET PROTECT.
- Tinklo ryšiai užblokuoti
- Užblokuota tinklo grėsmė

Žiniatinklio naršyklės įspėjimai

- Rastas galimai nepageidaujamas turinys
- Svetainė užblokuota dėl sukčiavimo apsimetant

Kompiuteris

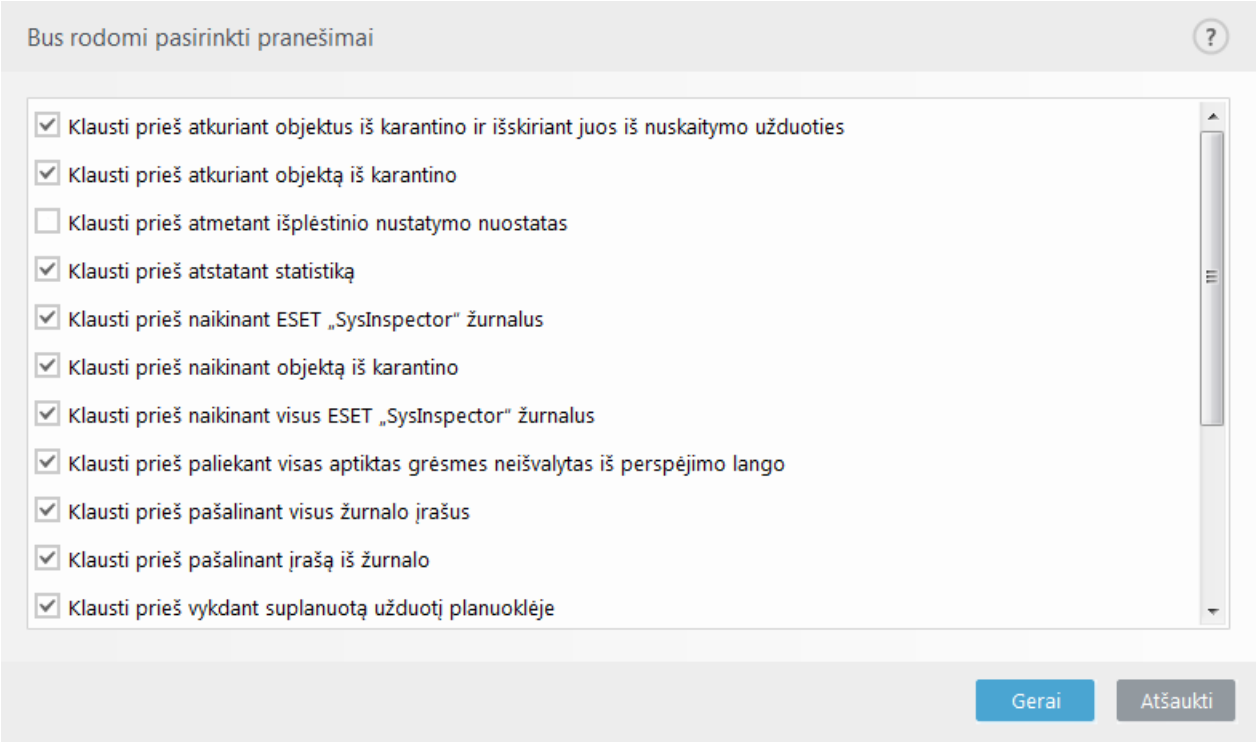
Šie perspėjimai pakeis naudotojo sąsają į oranžinę:

- Paleisti kompiuterį iš naujo (būtina)
- Paleisti kompiuterį iš naujo (rekomenduojama)

Interaktyviuose įspėjimuose nėra aptikimo modulio, HIPS arba užkardos interaktyvių langų, nes jų veikimą galima konfigūruoti atskirai konkrečioje funkcijoje.

Patvirtinimo pranešimai

Norėdami koreguoti patvirtinimo pranešimus, eikite į **Naudotojo sąsają** > **Įspėjimai ir pranešimų langai** > **Patvirtinimo pranešimai** ESET Endpoint Security išplėstinio nustatymo medyje ir spustelėkite **Redaguoti**.



Šiame dialogo lange pateikiami patvirtinimo pranešimai, kuriuos ESET Endpoint Security rodys prieš atliekant bet kokį veiksmą. Pažymėkite laukelį šalia kiekvieno patvirtinimo pranešimo arba nuimkite žymas, kad juos įjungtumėte arba išjungtumėte.

Sužinokite daugiau apie konkrečią funkciją, susijusią su patvirtinimo pranešimais:

- Klauskite prieš ištrindami ESET SysInspector žurnalus
- Klauskite prieš ištrindami visus ESET SysInspector žurnalus
- Klausti prieš naikinant objektą iš karantino
- Klausti prieš atmetant išplėstinio nustatymo nuostatas
- Klausti prieš paliekant visas aptiktas grėsmes neišvalytas iš perspėjimo lango
- Klausti prieš pašalinant įrašą iš žurnalo
- Klausti prieš šalinant suplanuotą užduotį iš planuoklės
- Klausti prieš pašalinant visus žurnalo įrašus
- Klausti prieš atstatant statistiką
- Klausti prieš atkuriant objektą iš karantino

- Klausti prieš atkuriant objektus iš karantino ir išskiriant juos iš nuskaitymo užduoties
- Klausti prieš vykdant suplanuotą užduotį planuoklėje
- Rodyti apsaugos nuo brukalo apdorojimo rezultatų pranešimus
- Rodyti apsaugos nuo brukalo apdorojimo rezultatų pranešimus el. pašto programose
- Rodyti el. pašto klientų „Outlook Express“ ir „Windows Mail“ produkto patvirtinimo dialogo langus
- Rodyti „Windows Live Mail“ produkto patvirtinimo dialogo langus
- Rodyti el. pašto kliento „Outlook“ produkto patvirtinimo dialogo langus

Išplėstinių nustatymų nesuderinamumo klaida

Ši klaida gali įvykti, jei kuris nors komponentas (pvz., HIPS arba užkarda) ir vartotojas vienu metu sukuria taisyklę interaktyviuoju ar mokymosi režimu.

Jei norite kurti savo taisykles, rekomenduojame filtravimo režimą perjungti į numatytąjį **automatinį režimą**. Skaitykite daugiau apie ESET užkardos mokymosi režimą. Skaitykite daugiau apie HIPS ir HIPS filtravimo režimus.

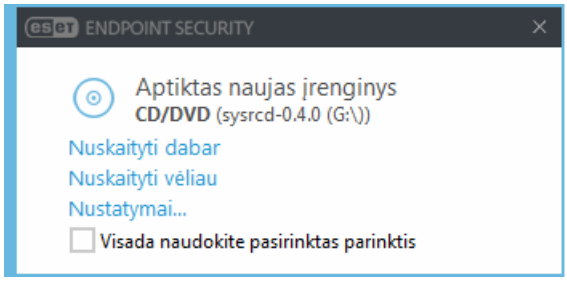
Leisti toliau naudoti numatytąją naršyklę

Konkretus interaktyvus įspėjimas rodomas tik tada, kai nepavyksta tinkamai paleisti saugios naršyklės.

Nešiojamoji laikmena

ESET Endpoint Security atlieka automatinį nešiojamosios laikmenos (CD / DVD / USB / ...) nuskaitymą, kai ji įdedama į kompiuterį. Tai gali būti naudinga, jeigu kompiuterio administratorius nenori, kad naudotojai naudotų nešiojamąsias laikmenas su nepageidaujamu turiniu.

Kai prijungiama nešiojamoji laikmena, **Rodyti nuskaitymo parinktis** nustatoma ESET Endpoint Security ir parodomas toks dialogo langas:



Šio dialogo parinktys:

- **Nuskaityti dabar** – galite paleisti nešiojamosios laikmenos nuskaitymą.
- **Nenuskaityti** – jokie veiksmai nebus atliekami.

Be to, ESET Endpoint Security yra įrenginio kontrolės funkcija, kurioje galite apibrėžti išorinių įrenginių taisykles tam tikrame kompiuteryje. Daugiau informacijos apie įrenginio kontrolę galima rasti skyriuje Įrenginių kontrolė.

Norėdami pasiekti nešiojamosios laikmenos nuskaitymo nustatymus, atidarykite Išplėstiniai nustatymai (**F5**) > **Naudotojo sąsaja** > **Įspėjimai ir pranešimų langai** > **Interaktyvūs įspėjimai** > **Interaktyvių įspėjimų sąrašas** >

Redaguoti > **Naujo įrenginio aptikimas**.

Jei nepasirinkta **Klausti naudotojo**, pasirinkite veiksmą, kurį norite atlikti, įdėdami nešiojamąją laikmeną į kompiuterį:

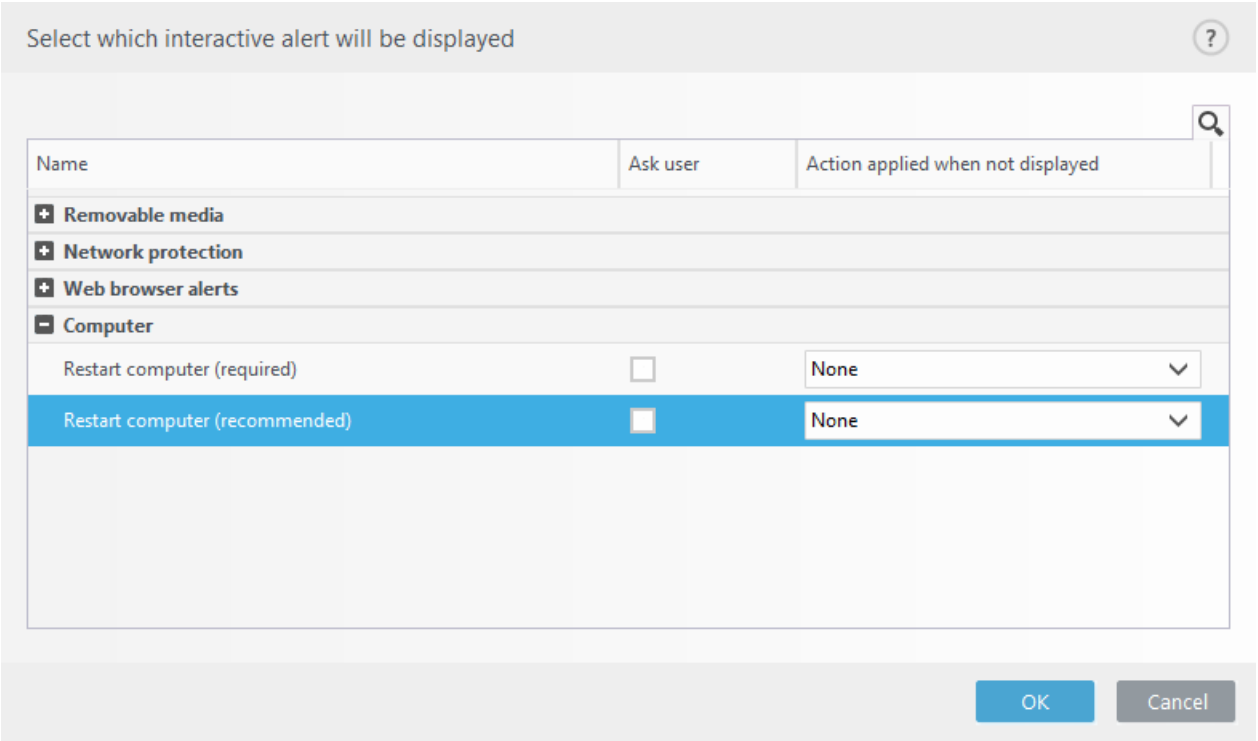
- **Nenuskaityti** – jokie veiksmai nebus atliekami, o langas **Aptiktas naujas įrenginys** nebus atidarytas.
- **Automatinis įrenginio nuskaitymas** – bus atliktas kompiuterio, į kurį įdėta nešiojamoji laikmena, nuskaitymas.
- **Priverstinis įrenginio nuskaitymas** – bus atliktas kompiuterio, į kurį įdėta nešiojamoji laikmena, nuskaitymas ir jo nebus galima atšaukti.
- **Rodyti nuskaitymo parinktis** – atidaro nustatymų skyrių **Interaktyvūs įspėjimai**.

Reikia iš naujo paleisti kompiuterį

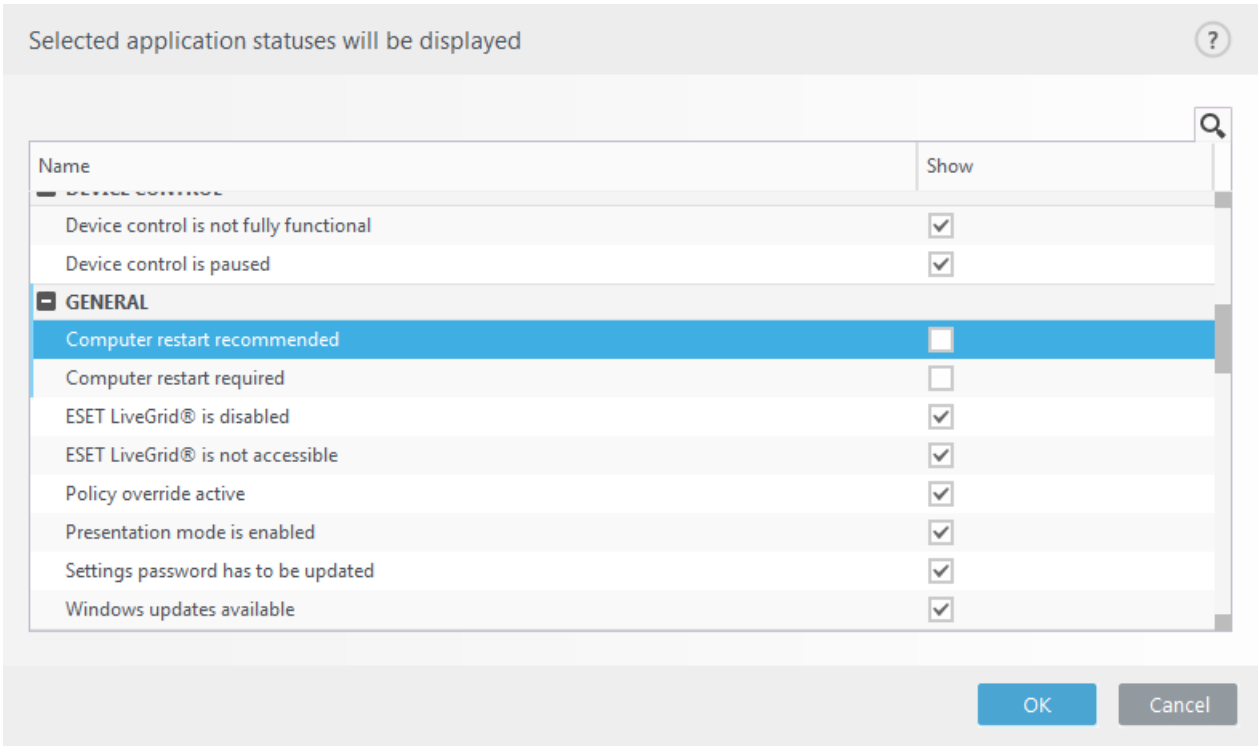
Jei įrenginiai gauna raudonus perspėjimus „Reikia iš naujo paleisti kompiuterį“, galite išjungti perspėjimų rodymą.

Norėdami išjungti perspėjimą „Reikia iš naujo paleisti kompiuterį“ ir „Rekomenduojama iš naujo paleisti kompiuterį“, atlikite toliau nurodytus veiksmus:

1. Paspauskite klavišą **F5**, kad atidarytumėte Išplėstinis nustatymas ir išskleiskite skyrių **Perspėjimai ir pranešimų langai**.
2. Spustelėkite **Redaguoti** šalia **Interaktyvių įspėjimų sąrašas**. Skyriuje **Kompiuteris** pašalinkite žymėjimus langeliuose šalia **Paleisti Paleisti kompiuterį iš naujo (būtina)** ir **Paleisti kompiuterį iš naujo (rekomenduojama)**.



3. Spustelėkite **Gerai**, kad išsaugotumėte pakeitimus abiejuose atidarytuose languose.
4. Pranešimai nebebus rodomi įrenginyje.
5. (pasirenkama) Norėdami išjungti programos būseną ESET Endpoint Security pagrindiniame programos lange, lange Programos būsenų langas pašalinkite žymėjimą langeliuose šalia **Reikia iš naujo paleisti kompiuterį** ir **Rekomenduojama iš naujo paleisti kompiuterį**.

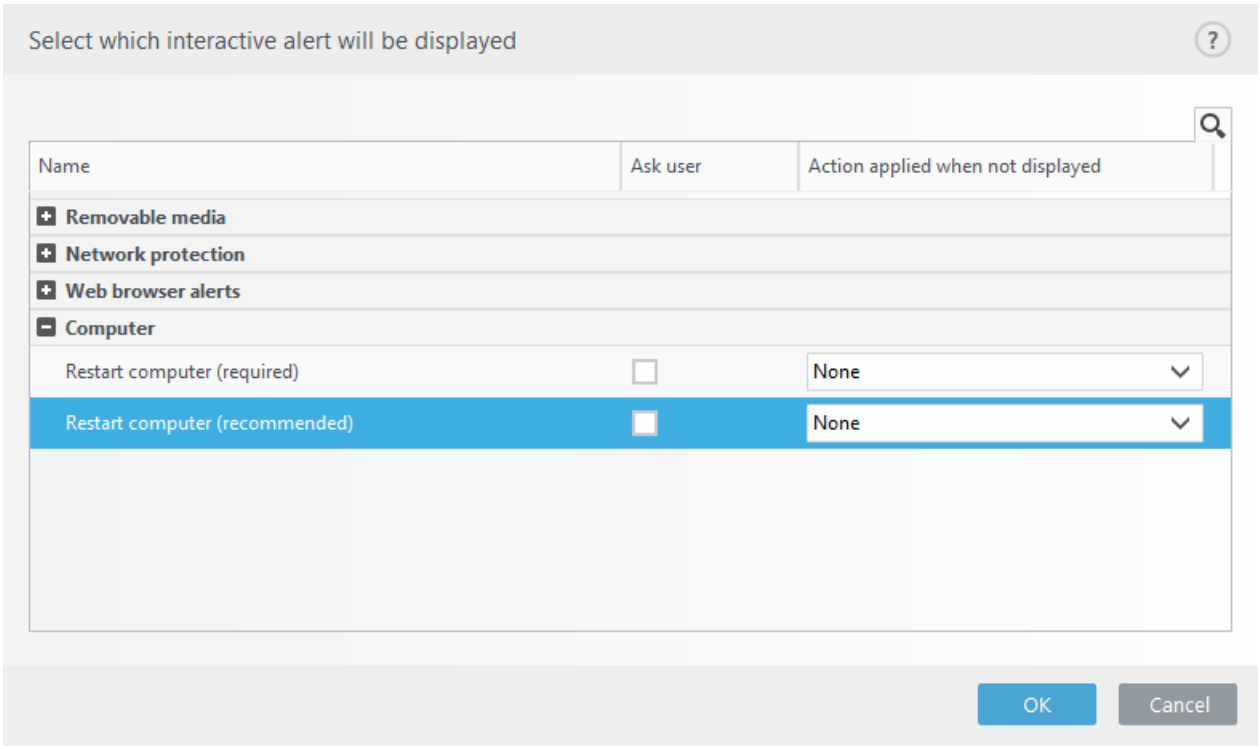


Rekomenduojama iš naujo paleisti kompiuterį

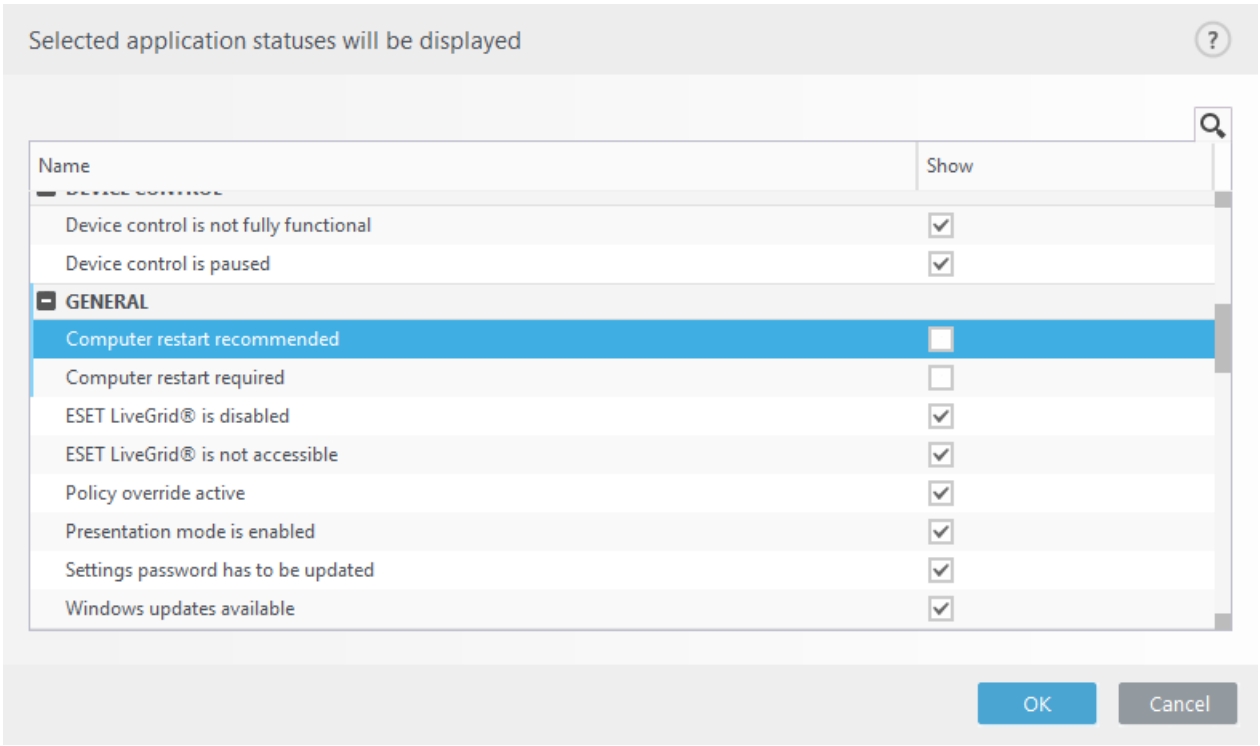
Jei įrenginiai gauna geltonus perspėjimus „Rekomenduojama iš naujo paleisti kompiuterį“, galite išjungti perspėjimų rodymą.

Norėdami išjungti perspėjimą „Reikia iš naujo paleisti kompiuterį“ ir „Rekomenduojama iš naujo paleisti kompiuterį“, atlikite toliau nurodytus veiksmus:

1. Paspauskite klavišą **F5**, kad atidarytumėte Išplėstinis nustatymas ir išskleiskite skyrių **Perspėjimai ir pranešimų langai**.
2. Spustelėkite **Redaguoti** šalia **Interaktyvių įspėjimų sąrašas**. Skyriuje **Kompiuteris** pašalinkite žymėjimus langeliuose šalia **Paleisti Paleisti kompiuterį iš naujo (būtina)** ir **Paleisti kompiuterį iš naujo (rekomenduojama)**.



3. Spustelėkite **Gerai**, kad išsaugotumėte pakeitimus abiejuose atidarytuose languose.
4. Pranešimai nebebus rodomi įrenginyje.
5. (pasirenkama) Norėdami išjungti programos būseną ESET Endpoint Security pagrindiniame programos lange, lange Programos būsenų langas pašalinkite žymėjimą langeliuose šalia **Reikia iš naujo paleisti kompiuterį** ir **Rekomenduojama iš naujo paleisti kompiuterį**.

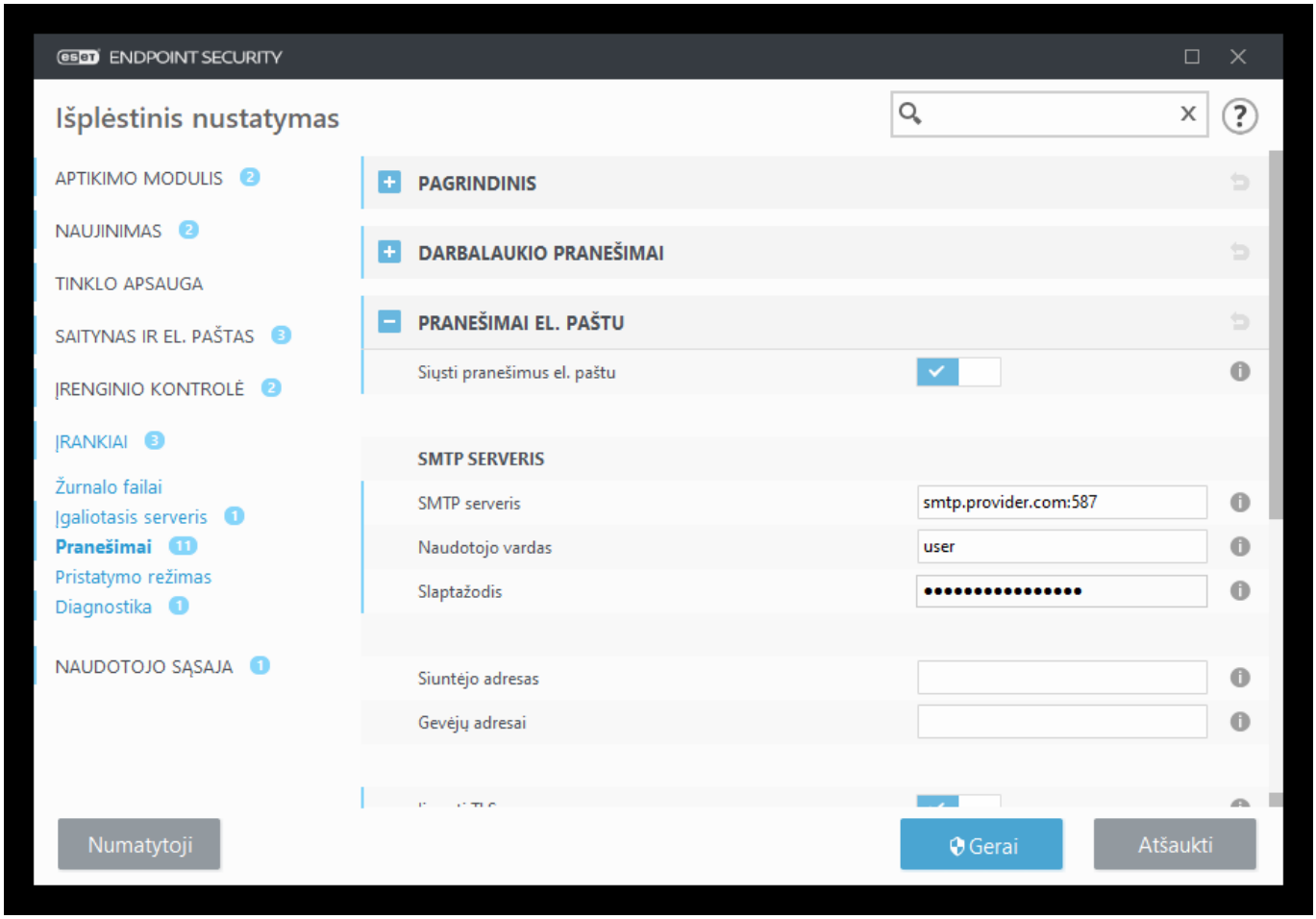


Peradresavimas

ESET Endpoint Security gali automatiškai siųsti pranešimų el. laiškus, jei įvyksta įvykis su pasirinktu daugiažodžio lygiu. Skyriuje **Išplėstinis nustatymas** > **Pranešimai** > **Persiuntimas** > **Persiųsti į el. paštą** įgalinkite **Persiųsti**

pranešimus el. paštu, kad suaktyvintumėte el. pašto pranešimus.

Persiųsti pranešimai – pasirinkite, kurie darbalaukio pranešimai bus persiųsti į el. paštą.



SMTP serveris

SMTP serveris – SMTP serveris, naudojamas pranešimams siųsti (pvz., *smtp.provider.com:587*, iš anksto nustatytas 25 prievadas).

ESET Endpoint Security nepalaiko SMTP serverių su TLS šifravimu.

Vartotojo vardas ir slaptažodis – jeigu SMTP serveriui reikalinga autentiškumo patvirtinimo procedūra, į šiuos laukus reikia įrašyti galiojantį vartotojo vardą ir slaptažodį, kad būtų galima prisijungti prie SMTP serverio.

Siuntėjo adresas – šiame lauke nurodomas siuntėjo adresas, kuris bus rodomas pranešimų el. laiškų antraštėje.

Gavėjų adresai – šiame lauke nurodomi gavėjo adresai, kurie bus rodomi pranešimų el. laiškų antraštėje. Kelis el. pašto adresus atskirkite kabliataškiu „;“.

Įjungti TLS – įjunkite perspėjimų ir pranešimų siuntimo funkciją, su kuria dera TLS šifravimo funkcija.

El. pašto nustatymai

Išskleidžiamajame meniu **Minimalus pranešimų daugiažodiškumas** galite pasirinkti pradinį siunčiamų pranešimų griežtumo lygį.

- **Diagnostika** – registruoja informaciją, reikalingą norint tiksliai suderinti programą ir visus anksčiau

paminėtus įrašus.

- **Informacija** – įrašo informacinius pranešimus, pvz., neįprastus tinklo įvykius, įskaitant sėkmingų naujinimų pranešimus ir visus pirmiau nurodytus įrašus.
- **Įspėjimai** – registruoja kritines klaidas ir įspėjamuosius pranešimus (apsauga nuo slaptųjų virusų veikia netinkamai arba nepavyko atnaujinti).
- **Klaidos** – registruojamos klaidos (nepaleista dokumento apsauga) ir kritinės klaidos.
- **Kritiniai** – registruoja tik kritines klaidas (klaida paleidžiant apsaugą nuo virusų arba sistema užkrėsta).

Siųsti kiekvieną pranešimą atskiru el. laišku – įjungus šią funkciją, gavėjas kiekvieną atskirą pranešimą gaus naujame el. laiške. Taip per trumpą laiką gali būti gauta daug el. laiškų.

Intervalas, kuriuo bus siunčiami pranešimai el. paštu (min.) – intervalas (minutėmis), po kurio nauji pranešimai bus siunčiami el. paštu. Jei šią reikšmę nustatysite kaip 0, pranešimai bus siunčiami iškart.

Pranešimo formatas

Ryšys tarp programos ir nuotolinio vartotojo arba sistemos administratoriaus yra palaikomas el. paštu arba LAN pranešimais (naudojant „Windows“ žinučių siuntimo paslaugą). Numatytasis įspėjimo pranešimų ir perspėjimų formatas bus optimalus daugeliu atvejų. Kai kuriomis aplinkybėmis gali prireikti pakeisti įvykių pranešimų formatą.

Įvykių pranešimų formatas – suformatuokite įvykių pranešimus, kurie rodomi nuotoliniuose kompiuteriuose.

Grėsmės įspėjimo pranešimų formatas – grėsmių perspėjimai ir pranešimai turi iš anksto apibrėžtą numatytąjį formatą. Mes patariame nekeisti šio formato. Tačiau kai kuriomis aplinkybėmis (pvz., jeigu turite automatinę el. pašto apdorojimo sistemą) jums gali tekti pakeisti pranešimo formatą.

Simbolių rinkinys – el. laišką konvertuoja į ANSI simbolių šifravimą pagal „Windows“ regiono parametrus (pvz., windows-1250, Unicode (UTF-8), ACSII 7-bit arba Japonų (ISO-2022-JP)). Todėl "á" bus pakeista į "a", o nežinomas simbolis į "?".

Naudoti spausdinamą šifravimą su kabutėmis – el. laiško šaltinis bus koduotas į „Quoted-printable“ (QP) formatą, kuris naudoja ASCII simbolius ir gali teisingai perduoti specialiuosius simbolius el. paštu 8 bitų formatu (áéíóú).

Raktažodžiai (eilutės, atskirtos ženklais „%“) pranešime yra pakeičiami realia informacija, kaip nurodyta. Galimi šie raktažodžiai:

- **%TimeStamp%** – įvykio data ir laikas
- **%Scanner%** – susijęs modulis
- **%ComputerName%** – kompiuterio, iš kurio gautas įspėjimas, pavadinimas
- **%ProgramName%** – programa, sukūrusi įspėjimą
- **%InfectedObject%** – užkrėsto failo, laiško ir t. t. pavadinimas
- **%VirusName%** – užkrato identifikavimas
- **%Action%** – veiksmas, kurio imtasi dėl įsiskverbimo
- **%ErrorDescription%** – nevirusinio įvykio aprašas

Raktažodžiai **%InfectedObject%** ir **%VirusName%** naudojami tik perspėjimų apie grėsmes pranešimuose, o **%ErrorDescription%** naudojamas tik įvykių pranešimuose.

Profilių tvarkytuvas

Profilių tvarkytuvas yra naudojamas dviejose ESET Endpoint Security vietose – skyriuje **Kompiuterio nuskaitymas pareikalavus** ir **Naujinimas**.

Kompiuterio nuskaitymas pareikalavus

Jūsų pasirinkti nuskaitymo parametrai gali būti įrašyti, kad galėtumėte juos panaudoti nuskaitymui ateityje. Rekomenduojame susikurti skirtingus profilius (su skirtingais nuskaitymo tikslais, nuskaitymo metodais ir kitais parametrais) kiekvienam reguliariai atliekamam nuskaitymui.

Naujam profiliui sukurti atverkite išplėstinių nustatymų langą (F5) ir spustelėkite **Antivirusinė programa** > **Kompiuterio nuskaitymas pareikalavus**, tada paspauskite **Redaguoti** (šalia punkto **Profilių sąrašas)**. Išskleidžiamajame meniu **Naujinimo profilis** pateikiami esami nuskaitymo profiliai. Norėdami sukurti nuskaitymo profilį, kuris atitiktų jūsų poreikius, žiūrėkite skyrių ThreatSense modulio parametrų nustatymas, kuriame aprašytas kiekvienas nuskaitymo nustatymų parametras.

> Tarkime, norite sukurti savo nuskaitymo profilį ir jums iš dalies tinka **kompiuterio nuskaitymo** konfigūracija, tačiau nenorite nuskaityti momentinio pakavimo arba galimai nesaugių programų, be to, norite taikyti **griežto valymo**. Įveskite savo naujojo profilio pavadinimą į langą **Profilių tvarkytuvas** ir spustelėkite **Pridėti**. **Pasirinkto profilio** išskleidžiamajame meniu pasirinkite naująjį profilį ir pakeiskite likusius parametrus pagal savo reikalavimus, tada spustelėkite **Gerai**, kad naująjį profilį įrašytumėte.

Naujinti

Profilių rengyklė naujinimų nustatymo skyriuje leidžia vartotojams kurti naujus naujinimų profilius. Kurkite ir naudokite savo pasirinktinius profilius (kitus nei numatytasis **Mano profilis**), tik jeigu kompiuteris naudoja kelis būdus jungtis prie naujinimo serverių.

Pavyzdžiui, nešiojamasis kompiuteris, kuris paprastai jungiasi prie vietinio (veidrodinio atspindžio) serverio vietiniame tinkle, bet kuris atsisiunčia naujinimų failus tiesiai iš ESET naujinimo serverių, kai yra atjungtas nuo vietinio tinklo (komandiruotėje), gali naudoti du profilius: pirmasis naudojamas jungtis prie vietinio serverio, kitas – prie ESET serverių. Kai šie profiliai yra sukonfigūruoti, eikite į **Įrankiai** > **Planuoklė** ir redaguokite naujinimo užduoties parametrus. Nustatykite vieną profilį kaip pagrindinį, o kitą kaip antrinį.

Naujinimo profilis – šiuo metu naudojamas naujinimo profilis. Norėdami jį pakeisti, pasirinkite profilį iš išskleidžiamojo meniu.

Profilių sąrašas – sukurkite naują arba pašalinkite esamus naujinimo profilius.

Spartieji klavišai

Patogesnį ESET Endpoint Security naršymą užtikrina šie spartieji klavišai:

Spartieji klavišai	Atliktas veiksmas
F1	atidaro žinyno puslapius
F5	atidaro išplėstinį nustatymą
Up/Down	produkto elementų naršymas

Spartieji klavišai	Atliktas veiksmas
TAB	perkelia žymeklį lange
Esc	uždaro aktyvų dialogo langą
Ctrl+U	rodo informaciją apie ESET licenciją ir jūsų kompiuterį (išsamią informaciją apie techninę pagalbą)
Ctrl+R	iš naujo nustato produkto lango numatytąjį dydį ir padėtį ekrane

Diagnostika

Diagnostikos skiltyje pateikiamos ESET procesų programos strigčių atminties išklotinės (pvz., „ekrn“). Programos strigties atveju parengiama atminties išklotinė. Ji gali padėti programuotojams taisyti klaidas ir šalinti įvairias ESET Endpoint Security problemas.

Spustelėkite išskleidžiamąjį meniu, esantį šalia punkto **Atminties išklotinės tipas**, ir pasirinkite vieną iš trijų galimybių:

- Pasirinkite **Išjungti**, kad išjungtumėte šią savybę.
- **Miniatiūrinis** (numatytoji) – įrašo mažiausią naudingos informacijos rinkinį, kuris gali padėti identifikuoti, kodėl programa netikėtai sugedo. Šis atminties išklotinės failas gali būti naudojamas, kai yra riboti vietos ištekliai, o kadangi įtraukiamas tik ribotas informacijos kiekis, analizuojant šį failą gali būti neaptiktos klaidos, kurios nebuvo tiesiogiai susijusios su gija, vykdoma, kai iškilo problema.
- **Visas** – įrašo visą sistemos atminties turinį, kai programa nenumatytai sustoja. Visos atminties išklotinėje gali būti procesų, kurie buvo vykdomi, kai buvo renkama atminties išklotinė, duomenys.

Paskirties katalogas – katalogas, kuriame bus sukuriama atminties išklotinė įvykus gedimui.

Atidaryti diagnostikos aplanką – spustelėkite **Atidaryti**, kad atidarytumėte šį katalogą naujame *Windows explorer* lange.

Sukurti diagnostikos išklotinę – spustelėkite **Sukurti** ir sukurkite diagnostikos išklotinės failą **Paskirties kataloge**.

Išplėstinis prisijungimas

Įjungti išplėstinį apsaugos nuo brukalo modulio registravimą – įrašo visus įvykius, kurie įvyksta apsaugos nuo brukalo nuskaitymo metu. Tai padeda programų kūrėjams nustatyti ir pašalinti su ESET apsaugos nuo brukalo moduliu susijusias problemas.

Įjungti išplėstinį prisijungimą prie kompiuterio nuskaitymo programos – įrašykite visus įvykius, kurie įvyksta Kompiuterio nuskaitymo arba Failų sistemos apsaugos realiuoju laiku failų ir aplankų nuskaitymo metu.

Įjungti išplėstinį įrenginio kontrolės registravimą – įrašykite visus įvykius, kurie įvyksta veikiant įrenginio kontrolei. Tai padeda programų kūrėjams nustatyti ir pašalinti su įrenginio kontrole susijusias problemas.

Įgalinti „Direct Cloud“ išplėstinis prisijungimas – Įrašykite visą produkto ryšį tarp produkto ir „Direct Cloud“ serverių.

Įjungti išplėstinį dokumentų apsaugos registravimą – įrašykite visus įvykius, kuriuos fiksuoja dokumento apsauga, kad būtų lengviau nustatyti ir išspręsti problemas.

Įjungti išplėstinį prisijungimą prie branduolio – įrašykite visus įvykius, kurie nutinka ESET branduolio tarnyboje (ekrn), kad galėtumėte diagnozuoti ir spręsti problemas (pasiekiama 7.2 ir naujesnėse versijose).

Įjungti išplėstinį licencijos registravimą – įrašo visus produkto ryšius su ESET aktyvinimo ir ESET Business Account serveriais.

Įjungti atminties sekimą – Įrašykite visus įvykius, kad padėtumėte kūrėjams aptikti atminties nutekėjimą.

Įjungti išplėstinį tinklo apsaugos registravimą – PCAP formatu įrašo visus tinklo duomenis, kurie pereina užkardą, kad programų kūrėjai galėtų nustatyti ir išspręsti problemas, susijusias su užkarda.

Įjungti išplėstinį operacinės sistemos registravimą – bus renkama papildoma informacija apie operacinę sistemą, pvz., vykdomus procesus, centrinio procesoriaus aktyvumą, disko operacijas. Tai gali padėti plėtotojams nustatyti ir ištaisyti nesklandumus, susijusius su ESET produktų veikimu jūsų operacinėje sistemoje.

Įjungti išplėstinį protokolų filtravimo registravimą – PCAP formatu įrašo visus duomenis, kurie pereina protokolų filtravimo modulį, kad programų kūrėjai galėtų nustatyti ir išspręsti problemas, susijusias su asmenine užkarda.

Įjungti išplėstinį „push“ pranešimų registravimą – Įrašykite visus įvykius, kurie įvyksta siunčiant „push“ pranešimus, kad leistumėte diagnostiką ir problemų sprendimą.

Įjungti išplėstinį Failų sistemos apsaugos realiuoju laiku registravimą – įrašomi visi įvykiai, kuriuos fiksuoja Failų sistemos apsauga realiuoju laiku, kad būtų lengviau nustatyti ir išspręsti problemas.

Įjungti išplėstinį prisijungimą prie saugios naršyklės – Įrašykite visus įvykius, kurie įvyksta naudojant saugią naršyklę, kad būtų galima lengviau nustatyti ir išspręsti problemas.

Įjungti išplėstinį naujinimo modulio registravimą – įrašo visus įvykius, kurie įvyksta naujinimo proceso metu. Tai gali padėti programuotojams diagnozuoti ir išspręsti problemas, susijusias su naujinimo moduliu.

Įjungti išplėstinį saityno kontrolės registravimą – įrašykite visus įvykius, kurie įvyksta veikiant saityno kontrolei. Tai padeda programų kūrėjams nustatyti ir pašalinti su saityno kontrole susijusias problemas.

Žurnalo failų vieta

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

Komandos eilutės skaitytuvas

ESET Endpoint Security antivirusinės programos modulis gali būti paleidžiamas komandos eilute – rankiniu būdu (komanda „ecls“) arba naudojant paketinį („bat“) failą.

ESET komandų eilutės skaitytuvo naudojimas:

```
ecls [OPTIONS..] FILES..
```

Šiuos parametrus ir jungiklius galima naudoti paleidžiant nuskaitymo programą pagal pareikalavimą iš komandos eilutės:

Parinktys

/base-dir=APLANKAS	įkelti modulius iš APLANKO
/quar-dir=APLANKAS	karantino APLANKAS
/exclude=KAUKĖ	nenuskaityti KAUKĘ atitinkančių failų
/subdir	nuskaityti poaplankius (numatyta)
/no-subdir	nenuskaityti poaplankių
/max-subdir-level=LYGIS	maksimalus nuskaitomų poaplankių lygis aplankuose
/symlink	sekti simbolinius saitus (numatyta)
/no-symlink	praleisti simbolinius saitus
/ads	nuskaityti ADS (numatyta)
/no-ads	nenuskaityti ADS
/log-file=FAILAS	registruoti išvestis į FAILĄ
/log-rewrite	perrašyti išvesties failą (numatyta – papildyti)
/log-console	registruoti išvestį pulte (numatyta)
/no-log-console	neregistruoti išvesties pulte
/log-all	registruoti ir švarius failus
/no-log-all	neregistruoti švarių failų (numatyta)
/aind	rodyti veiklos indikatorių
/auto	nuskaityti ir automatiškai valyti visus vietinius diskus

Nuskaitymo programos parinktys

/files	nuskaityti failus (numatyta)
/no-files	nenuskaityti failų
/memory	nuskaityti atmintį
/boots	nuskaityti paleidimo sektorius
/no-boots	nenuskaityti paleidimo sektorių (numatyta)
/arch	nuskaityti archyvus (numatyta)
/no-arch	nenuskaityti archyvų
/max-obj-size=DYDIS	nuskaityti tik failus, jei jie mažesni nei nurodytas DYDIS megabaitais (numatytoji reikšmė 0 = neribotas)
/max-arch-level=LYGIS	maksimalus nuskaitomas papildomas vidinių archyvų lygis (įdėtieji archyvai)
/scan-timeout=RIBA	nuskaityti archyvus ne ilgiau nei nurodyta RIBA sekundėmis
/max-arch-size=DYDIS	nuskaityti failus archyve, tik jeigu jie mažesni nei nurodytas DYDIS (numatyta, kad 0 = neribotas)
/max-sfx-size=DYDIS	nuskaityti tik išsiskleidžiančiajame archyve esančius failus, jeigu jie mažesni nei nurodytas DYDIS megabaitais (numatytoji reikšmė 0 = neribotas)
/mail	nuskaityti el. pašto failus (numatyta)
/no-mail	nenuskaityti el. pašto failų
/mailbox	nuskaityti pašto dėžutes (numatyta)

/no-mailbox	nenuskaityti pašto dėžučių
/sfx	nuskaityti išsiskleidžiančiuosius archyvus (numatyta)
/no-sfx	nenuskaityti išsiskleidžiančiųjų archyvų
/rtp	nuskaityti momentinio pakavimo programas (numatyta)
/no-rtp	nenuskaityti momentinio pakavimo programų
/unsafe	nuskaityti galimas nesaugias taikomąsias programas
/no-unsafe	nenuskaityti galimų nesaugių taikomųjų programų (numatyta)
/unwanted	nuskaityti galimas nepageidaujamas taikomąsias programas
/no-unwanted	nenuskaityti galimų nepageidaujamų taikomųjų programų (numatyta)
/suspicious	ieškoti įtartinų programų (numatytasis)
/no-suspicious	neieškoti įtartinų programų
/pattern	naudoti kodus (numatyta)
/no-pattern	nenaudoti kodų
/heur	įjungti euristiką (numatyta)
/no-heur	išjungti euristiką
/adv-heur	įjungti išplėstinę euristiką (numatyta)
/no-adv-heur	išjungti išplėstinę euristiką
/ext-exclude=PLĖTINIAI	neįtraukti dvitaškiu atskirtų failų PLĖTINIŲ
/clean-mode=REŽIMAS	naudoti valymo REŽIMĄ užkrėstiems objektams Galimos šios parinktys: • `nona` (numatytoji) – automatinis valymas nevykdomas. • `standard` – „ecls.exe“ pabandys automatiškai išvalyti arba panaikinti užkrėstus failus. • `Reiklus` – „ecls.exe“ pamėgins automatiškai išvalyti arba panaikinti užkrėstus failus be vartotojo įsikišimo (jūs nebūsite informuojami apie naikinamus failus). • `Griežtas` – „ecls.exe“ panaikins failus nebandydamas išvalyti jų, neatsižvelgiant į tai, kokie failai naikinami. • `Naikinti` – „ecls.exe“ panaikins failus nebandydamas jų išvalyti, tačiau svarbių failų (pvz., „Windows“ sisteminių failų) nepanaikins.
/quarantine	kopijuoti užkrėstus failus (jeigu išvalyti) į karantiną (papildo valant atliekamus veiksmus)
/no-quarantine	nekopijuoti užkrėstų failų į karantiną

Bendrosios parinktys

/help	rodyti žinyną ir baigti
/version	rodyti versijos informaciją ir baigti
/preserve-time	išsaugoti paskutinės prieigos laiko žymą

Išėjimo kodai

0	grėsmių nerasta
1	aptikta grėsmių ir jos išvalytos
10	kai kurių failų nepavyko nuskaityti (gali būti grėsmių)

50	rasta grėsmė
100	klaida

Didesni nei 100 išėjimo kodai reiškia, kad failas buvo nenuskaitytas, todėl gali būti užkrėstas.

ESET CMD

Tai – funkcija, kuri įjungia išplėstines „ecmd“ komandas. Ji leidžia eksportuoti ir importuoti parametrus naudojantis komandos eilute (ecmd.exe). Iki šiol parametrus buvo galima eksportuoti tik naudojant GUI. ESET Endpoint Security konfigūraciją galima eksportuoti į *.xml* failą.

Kai įjungiate ESET CMD, galimi du įgaliojimo būdai:

- **Nėra** – įgaliojimo nėra. Šio būdo nerekomenduojame, nes jis suteikia galimybę importuoti bet kokią nepasirašytą konfigūraciją, o tai gali būti rizikinga.
- **Išplėstinių nustatymų slaptažodis** – reikalingas slaptažodis, norint importuoti konfigūraciją iš *.xml* failo; šis failas turi būti pasirašytas (žr. toliau apie *.xml*xml konfigūracijos failo pasirašymą). Slaptažodis, nurodytas dalyje Prieigos nustatymai turi būti pateiktas prieš importuojant naują konfigūraciją. Jei prieigos nustatymo nesate įjungę, slaptažodis neteisingas arba *.xml* formato konfigūracijos failas nepasirašytas, konfigūracija nebus importuojama.

Įjungę ESET CMD, galite importuoti ar eksportuoti ESET Endpoint Security konfigūracijas naudodami komandos eilutę. Galite tai daryti rankiniu būdu arba automatizuotai, naudodami susikurtą scenarijų.

Jei norite naudotis išplėstinėmis „ecmd“ komandomis, jas reikia paleisti turint administratoriaus privilegijas arba „Windows“ komandinę eilutę (cmd) atidaryti naudojantis funkcija **Paleisti administratoriaus teisėmis**. Kitaip jums bus parodytas pranešimas **Error executing command**. Be to, kai eksportuojate konfigūraciją, paskirties aplankas turi būti egzistuojantis. Kai ESET CMD nustatymai yra išjungtas, eksportavimo komanda vis dar veikia.

Išplėstines „ecmd“ komandas leisti galima tik vietoje. „ecmd“ komandų pristabdymas gali būti vykdomas tik naudojant kliento užduotį **Vykdyti komandą**, naudojant ESET PROTECT.

Parametrų eksportavimo komanda:
`ecmd /getcfg c:\config\settings.xml`

Parametrų importavimo komanda:
`ecmd /setcfg c:\config\settings.xml`

.xml formato konfigūracijos failo pasirašymas:

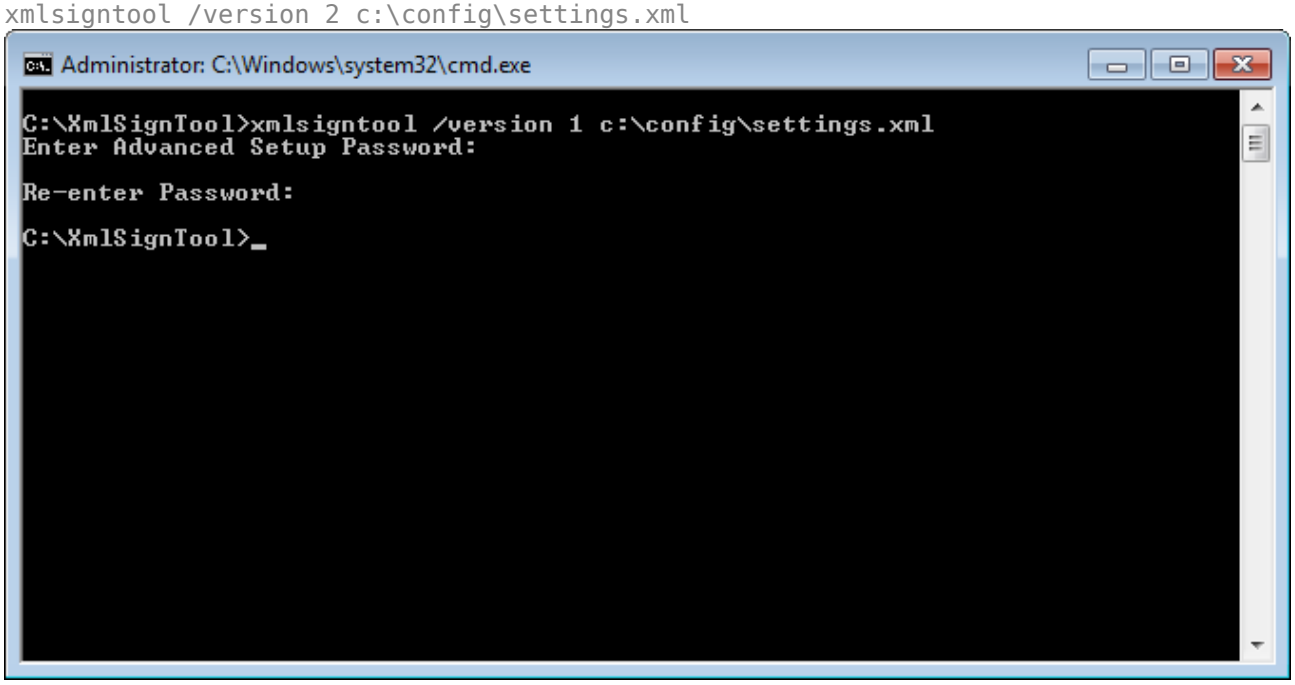
1. Atsisiųskite „XmlSignTool“ vykdomąjį failą.
2. Atidarykite „Windows“ komandinę eilutę (cmd) naudodamiesi funkcija **Paleisti administratoriaus teisėmis**.
3. Eikite į įrašymo vietą `xmlsigntool.exe`
4. Įvykdykite *.xml* formato konfigūracijos failo pasirašymo komandą: `xmlsigntool /version 1|2 <xml_file_path>`

`/version` Parametro reikšmė priklauso nuo jūsų ESET Endpoint Securityversijos. Naudokite `/version 2` 7 arba naujesnę versiją.

5. Įveskite ir pakartokite Išplėstinių nustatymų slaptažodį, kai „XmlSignTool“ to paprašo. Jūsų *.xml* formato konfigūracijos failas dabar yra pasirašytas ir gali būti naudojamas importuoti į kitą ESET Endpoint Security egzempliorių naudojant ESET CMD suteikiant įgaliojimą slaptažodžiu.

Pasirašykite eksportuojamos konfigūracijos failo komandą:

```
xmlsigntool /version 2 c:\config\settings.xml
```



Jei pakeitėte savo Prieigos nustatymo slaptažodį ir norite importuoti konfigūraciją, kuri anksčiau buvo pasirašyta naudojant senąjį slaptažodį, turite dar kartą pasirašyti *.xml* formato konfigūracijos failą naudodami dabartinį slaptažodį. Tai leidžia naudoti ankstesnį konfigūracijos failą, prieš importavimą jo neeksportuojant į kitą įrenginį, kuriame veikia ESET Endpoint Security.

ESET CMD nerekomenduojama įjungti be įgaliojimo suteikimo, nes taip bus leidžiama importuoti bet kokią nepatvirtintą konfigūraciją. Meniu elemente **Išplėstinis nustatymai** > **Vartotojo sąsaja** > **Prieigos nustatymas** nustatykite slaptažodį, kuris neleistų vartotojams daryti nesankcionuotų pakeitimų.

ecmd komandų sąrašas

Atskiras saugos funkcijas galima įjungti ir laikinai išjungti, naudojant ESET PROTECT klientų užduočių vykdymo komandą. Komandos neapeina politikos nustatymų ir visi pristabdyti nustatymai grąžinami įvykdžius komandą arba paleidus įrenginį iš naujo. Norėdami naudoti šią funkciją, nurodykite komandos eilutę, kad ji būtų vykdoma to paties pavadinimo laukelyje.

Peržiūrėkite kiekvienos saugos funkcijos komandų sąrašą toliau:

Saugos funkcija	Laikinai pristabdyti komandą	Įjungti komandą
Failų sistemos apsauga realiuoju laiku	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Dokumentų apsauga	ecmd /setfeature document pause	ecmd /setfeature document enable
Įrenginio kontrolė	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable

Saugos funkcija	Laikinai pristabdyti komandą	Įjungti komandą
Pristatymo režimas	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Apsaugos nuo slaptųjų virusų technologijos	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Asmeninė užkarda	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Apsauga nuo atakos iš tinklo (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Apsauga nuo botnet	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Saityno kontrolė	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Prieigos prie saityno apsauga	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
El. pašto programų apsauga	ecmd /setfeature email pause	ecmd /setfeature email enable
Apsauga nuo brukalo	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Apsauga nuo sukčiavimo apsimetant	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Laukimo būsenos aptikimas

Laukimo būsenos aptikimo parametrus galima konfigūruoti pasirinkus **Išplėstiniai nustatymai** iš **Aptikimo modulis** > **Kenkėjiškų programų nuskaitymai** > **Laukimo būsenos nuskaitymas** > **Laukimo būsenos aptikimas**. Šie parametrai nurodo Laukimo būsenos nuskaitymo paleidimo sąlygas, kai:

- veikia ekrano užsklanda,
- kompiuteris yra užrakintas,
- vartotojas išsiregistruoja.

Naudokite kiekvienos atitinkamos būsenos jungiklius skirtingų laukimo būsenų aptikimo paleidimo sąlygoms įjungti arba išjungti.

Parametrų importavimas ir eksportavimas

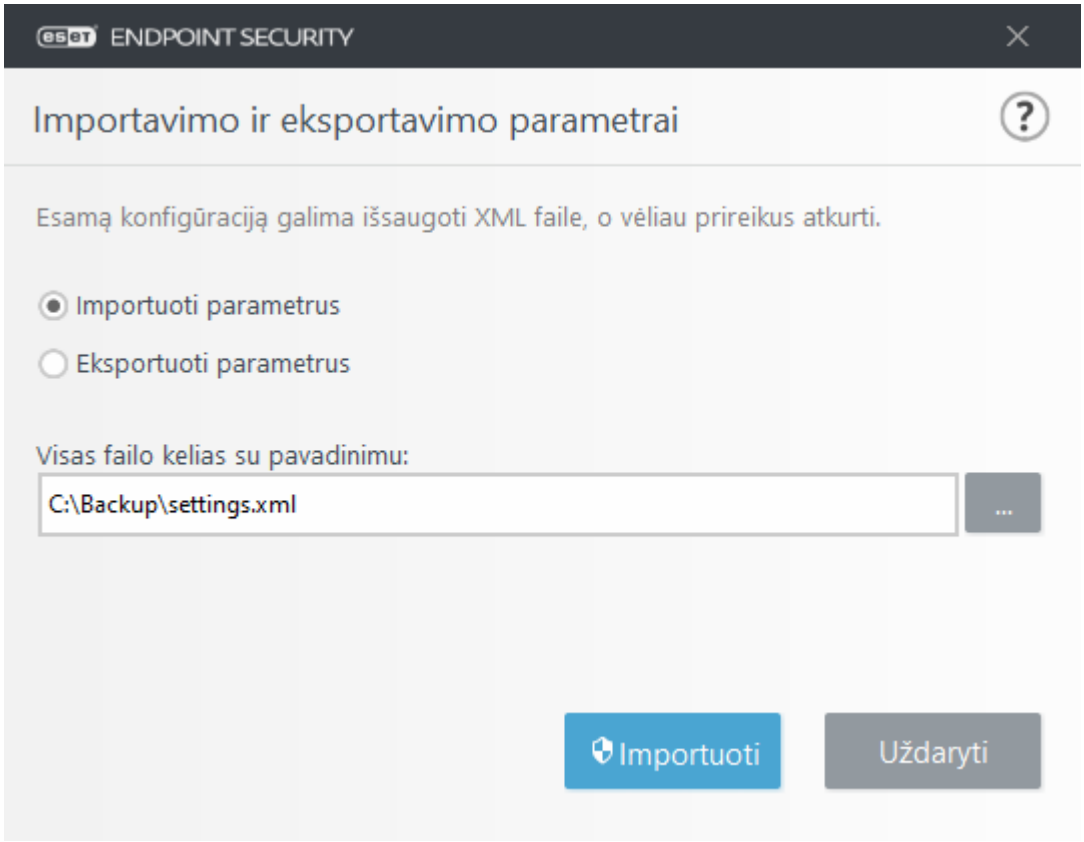
Galite importuoti arba eksportuoti pasirinktinius ESET Endpoint Security .xml konfigūracijos failus iš **Nustatymų** meniu.

Konfigūravimo failų importavimas ir eksportavimas yra naudingas, jeigu reikia padaryti ESET Endpoint Security dabartinės konfigūracijos atsarginę kopiją, kurią galėtumėte naudoti vėliau. Be to, parametrų eksportavimo parinktis yra patogi vartotojams, kurie nori pageidautiną konfigūraciją naudoti keliose sistemose – jie gali lengvai importuoti .xml failą ir perkelti šiuos parametrus.

Importuoti konfigūraciją labai paprasta. Pagrindiniame programos lange spustelėkite **Nustatymai** > **Parametrų importavimas / eksportavimas**, tada nurodykite parinktį **Parametrų importavimas**. Įveskite kelią į konfigūracijos failą arba spustelėkite mygtuką **...**, kad galėtumėte naršydami rasti konfigūracijos failą, kurį norite importuoti.

Veiksmai norint eksportuoti konfigūraciją yra labai panašūs. Pagrindiniame programos lange spustelėkite **Nustatymai** > **Parametrų importavimas / eksportavimas**. Pasirinkite **Eksportuoti parametrus** ir įveskite konfigūracijos failo pavadinimą (pvz., *export.xml*). Naudodami naršyklę pasirinkite, kurioje kompiuterio vietoje įrašyti konfigūracijos failą.

Eksportuojant parametrus gali įvykti klaida, jeigu neturite visų teisių rašyti eksportuojamą failą į nurodytą katalogą.



Grąžinti visus parametrus į numatytuosius

Išplėstinėje sąrankoje (F5) spustelėkite **Numatytieji**, norėdami atkurti visų modulių visus programos nustatymus. Tai atstatys visų modulių programų parametrus į būseną, kuri būtų iš naujo įdiegus.

Taip pat žr. Parametrų importavimas ir eksportavimas.

Atkurti visus esamojo skyriaus parametrus

Spustelėkite lenktą rodyklę ⍰, norėdami grąžinti visus parametrus esamajame skyriuje ties ESET nustatytais numatytaisiais nustatymais.

Atminkite: spustelėjus **Atkurti numatytąsias**, bus prarasti visi padaryti pakeitimai.

Atkurti lentelių turinį – įjungus šią funkciją, bus prarastos visos rankiniu ar automatiniu būdu įtrauktos taisyklės, užduotys bei profiliai.

Taip pat žr. Parametrų importavimas ir eksportavimas.

Klaida išsaugant konfigūraciją

Šis klaidos pranešimas nurodo, kad parametrai nebuvo tinkamai įrašyti dėl klaidos.

Paprastai tai reiškia, kad programos parametrus bandęs keisti naudotojas:

- neturi pakankamai prieigos teisių arba neturi reikalingų operacinės sistemos privilegijų, reikalingų konfigūracijos failų ir sistemos registro keitimui.
  > Norint atlikti norimus pakeitimus, turi prisijungti sistemos administratorius.
- neseniai įjungė HIPS arba užkardos mokymosi režimą ir bandė pakeisti išplėstinius nustatymus.
  > Jei norite įrašyti konfigūraciją ir išvengti konfigūracijos konfliktų, uždarykite išplėstinius nustatymus nejrašę ir bandykite dar kartą atlikti norimus pakeitimus.

Kitas dažniausiai pasitaikantis atvejis gali būti, kad programa tinkamai nebeveikia, yra sugadinta, todėl turi būti įdiegta iš naujo.

Nuotolinis stebėjimas ir valdymas

Nuotolinis stebėjimas ir valdymas (RMM) – tai programinės įrangos sistemų stebėjimo ir valdymo procesas, vykdomas naudojant vietoje įdiegtą agentą, kurį gali pasiekti valdymo paslaugos teikėjas.

ERMM – ESET papildinys, skirtas RMM

- Numatytame ESET Endpoint Security diegime yra failas `ermm.exe`, esantis „Endpoint“ programos kataloge: *C:\Program Files\ESET\ESET Security\ermm.exe*
- `ermm.exe` yra komandos eilutės įrankis, skirtas palengvinti įrenginių produktų valdymą ir ryšį su bet kuriuo RMM papildiniu.
- `ermm.exe` pakeičia duomenis su RMM papildiniu, kuris palaiko ryšį su RMM agentu, susietu su RMM serveriu. Pagal numatytuosius nustatymus ESET RMM įrankis yra išjungtas.

Papildomi ištekliai

- ERMM komandinė eilutė
- ERMM JSON komandų sąrašas
- Kaip suaktyvinti nuotolinio stebėjimo ir valdymo funkcijąESET Endpoint Security

ESET Direct Endpoint Management papildiniai trečiųjų šalių RMM sprendimams

RMM serveris veikia kaip paslauga trečiosios šalies serveryje. Daugiau informacijos rasite šiuose ESET Direct Endpoint Management internetiniuose naudotojo vadovuose:

- ESET Direct Endpoint Management priedas, skirtas „ConnectWise Automate“
- ESET Direct Endpoint Management papildinys, skirtas „DattoRMM“

- ESET Direct Endpoint Management, skirtas „Solarwinds N-Central“
- ESET Direct Endpoint Management, skirtas „NinjaRMM“

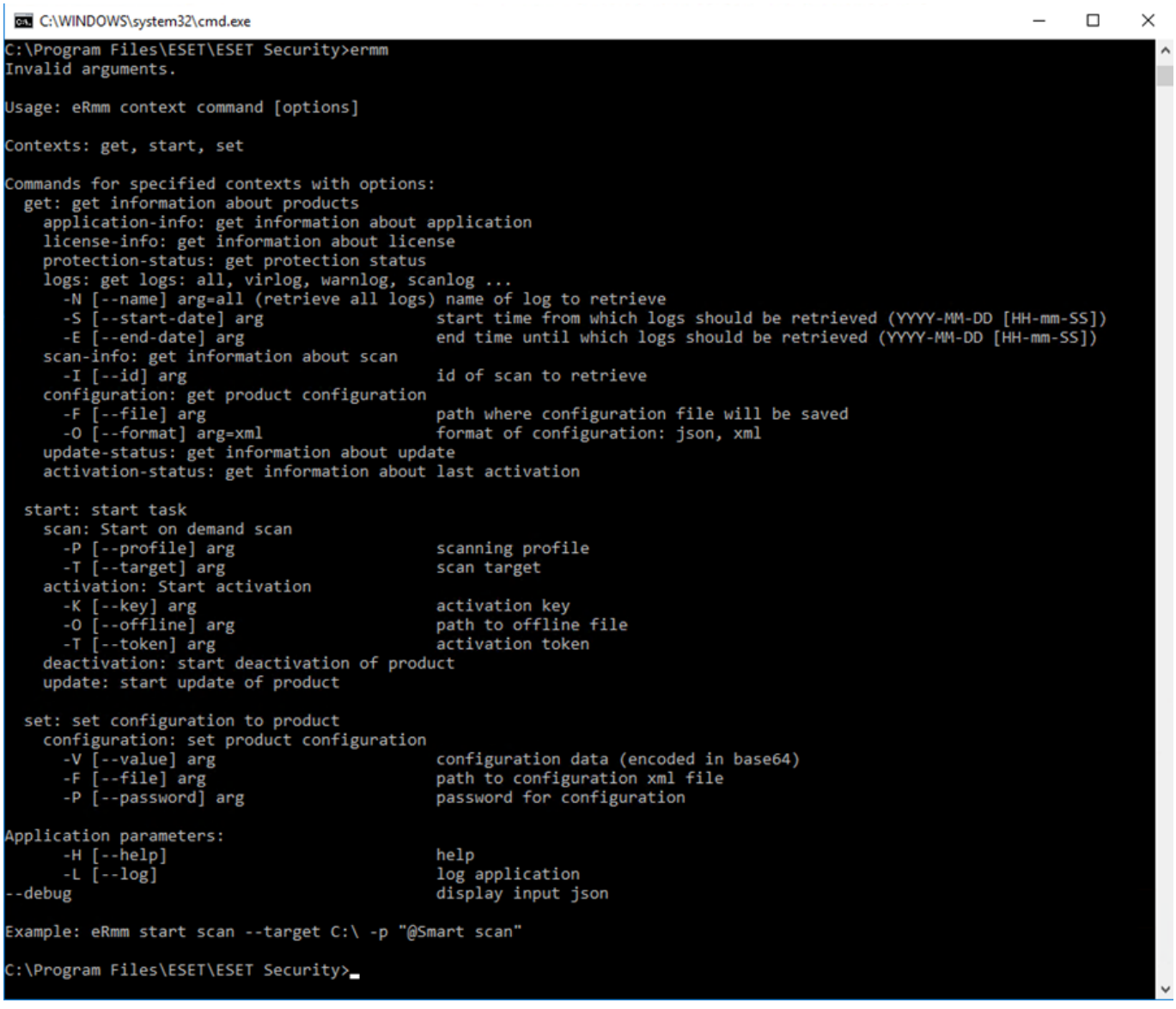
ERMM komandinė eilutė

Remote monitoring management is run using the command line interface. The default ESET Endpoint Security installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter

`--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	application-info	Get information about product
	license-info	Get information about license
	protection-status	Get protection status
	logs	Get logs
	scan-info	Get information about running scan
	configuration	Get product configuration
	update-status	Get information about update
	activation-status	Get information about last activation
start		**Start task**
	scan	Start on demand scan
	activation	Start activation of product
	deactivation	Start deactivation of product
	update	Start update of product
set		**Set options for product**
	configuration	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

ERMM JSON komandų sąrašas

- 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

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

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

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
"command":"get_application_info",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"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":"ANTISTEALTH32",
"description":"Anti-Stealth support module",
"version":"1106",
"date":"2016-10-17"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

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

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

Name	Value
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])

Example

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be {

success, running, failure }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
"command":"get_activation_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"status":"success"
},
"error":null
}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
"command":"get_scan_info",
"id":1,
"version":"1"
}
```

result


```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
"command":"get_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml"
}
}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value

key	Activation key
offline	Path to offline file

Example

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

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

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

Command line

```
ermm.exe start update
```

Parameters

None

Example

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 }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved

password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

Dažnai užduodami klausimai

Šiame skyriuje pateikiami kai kurie dažniausiai užduodami klausimai ir problemos, su kuriomis susiduriama. Jei norite sužinoti, kaip spręsti problemą, spustelėkite temos pavadinimą:

- Kaip naujinti ESET Endpoint Security
- Kaip suaktyvinti ESET Endpoint Security
- Kaip panaudoti esamus kredencialus naujam produktui suaktyvinti
- Kaip pašalinti virusą iš mano kompiuterio
- Kaip leisti ryšį tam tikroms taikomosioms programoms
- Kaip sukurti naują užduotį planuoklėje
- Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą
- Kaip tvarkyti pranešimus ir interaktyvius įspėjimus
- Kaip prijungti mano produktą prie ESET PROTECT
  - Kaip naudoti nepaisymo režimą
  - Kaip taikyti rekomenduojamą politiką ESET Endpoint Security
- Kaip sukonfigūruoti veidrodį
- Kaip atnaujinti į „Windows 10“, naudojant ESET Endpoint Security
- Kaip suaktyvinti nuotolinio stebėjimo ir valdymo funkciją
- Kaip blokuoti konkrečių failų tipų atsisiuntimą iš interneto
- Kaip sumažinti ESET Endpoint Security naudotojo sąsają

Jei jūsų problemos nėra pirmiau pateikiamame žinyno puslapių sąraše, pabandykite ESET Endpoint Security žinyno puslapiuose ieškoti pagal raktažodį arba frazę, apibūdinančią jūsų problemą.

Jei nepavyksta rasti problemos sprendimo ar atsakymo į klausimą žinyno puslapiuose, apsilankykite ESET žinių bazėje, kurioje rasite atsakymų į dažnai užduodamus klausimus ir įvairių problemų sprendimų.

- Geriausi būdai apsisaugoti nuo kenkėjiškos failų šifravimo programos (išpirkos reikalaujančio kenkėjo)
- „ESET Endpoint Security“ ir „ESET Endpoint Antivirus“ DUK
- Kuriuos adresus ir prievadus savo trečiosios šalies užkardoje turiu atverti, kad mano ESET produktas veiktų pilnai?

Jeigu reikia, galite kreiptis į mūsų interneto techninės priežiūros centrą ir pateikti savo klausimus arba problemas. Saitą į mūsų internetinę kreipimosi formą rasite pagrindinio programos lango polangyje **Žinynas ir palaikymas**.

DUK apie automatinius naujinimus

Daugiau informacijos apie ESET Endpoint Security produkto naujinius skaitykite ESET žinių bazės straipsnyje:
- Kokių skiriasi skirtingų tipų ESET produktų naujiniai ir leidimų tipai?

Ar kompiuteriai bus naujinami automatiškai? Ar naujinys atsisiuntė prieš paleidžiant iš naujo ar jau paleidus?

Atsisiuntimas vyksta prieš iš naujo paleidžiant, todėl atnaujinti failai taip pat ruošiami šiame etape. Paleidus iš naujo atnaujinti failai vis dar ruošiami naudoti, o tuo metu įdiegta versija suteikia nepertraukiamą apsaugą. Pakeitimai taikomi kitąkart paleidus ESET įrenginio produktą.

Turiu apie 3 000 kompiuterių. Ar į visus juos naujiniai bus atsisiųsti tuo pačiu metu? Esant tokiam kompiuterių skaičiui, ar galiu naudoti įgaliotąjį serverį automatiniams naujiniams atsisiųsti?

Didesniems tinklams ESET siūlo veidrodžio įrankio ir tarpinio serverio sprendimus, todėl naujinimai iš interneto atsisiunčiami tik vieną kartą ir yra tiekiami vietoje. Naujinimai yra mažesni, paprastai 5–10 MB, ir per pirmąsias kelias pasiekiamumo savaites bus ribojami. Todėl ne visi tiesiogiai prie ESET serverių prisijungę klientai pradės atsisiuntimą vienu metu.

Ar galiu pasirinkti, kiek ir kokių kompiuterių bus atnaujinta automatiškai? Noriu, kad naujinys būtų atsisiunčiamas ne daugiau kaip į dešimt kompiuterių per valandą arba norėčiau atnaujinti dešimt kompiuterių dabar, o kitus – po poros dienų.

Valdomose aplinkose galioja automatinio naujinimo politika, kurioje galite nurodyti naujausią norimą versiją. Taip pat palaikomi pakaitos simboliai (pvz., 2032 0 9.*). Daugiau informacijos žr. ESET PROTECT arba ESET PROTECT Cloud interneto žinyno automatinių atnaujinimų skyriuje. Deja, šiuo metu nėra jokių kitų automatinių atnaujinimų ribojimo pasirinkimų. Galite priskirti įvairias politikas kelioms grupėms. Galite priskirti įvairias politikas kelioms grupėms.

Ar galiu išjungti politiką, jei nenoriu, kad ESET produktas būtų naujinamas? Ar galiu tiesiog išjungti politiką, jei nenoriu, kad ESET produktas būtų naujinamas?

Jei ESET įrenginio produktui yra numatyta skubių taisymų, produktas bus atnaujintas net tada, kai automatiniai naujinimai bus išjungti, kaip nurodyta galiojančios Galutinio naudotojo licencijos sutarties sąlygose. ESET taiko Skubius saugos ir stabilumo pataisymus, kad išspręstų esmines problemas ir užtikrintų maksimalų jūsų ESET produkto saugumą ir stabilumą.

Automatinio naujinimo politiką galite priskirti bet kuriai įrenginių grupei, nepriklausomai nuo jų dabartinės automatinio naujinimo konfigūracijos. Nevaldomose aplinkose vartotojas gali lokaliai konfigūruoti automatinius naujinimus ESET įrenginio produkto išplėstinio nustatymo ekrane.

Ką daryti, jei sukonfigūravau politiką naudoti anksčiausią galimą versiją? Ar ESET vis tiek atnaujins mano produktus?

Įprasti skubūs taisymai priskiriami automatiniams naujinimams, kurių svarba tvirtinant naudotojo parametrus yra standartinė. Kritiniai skubūs taisymai taikomi numatant aukščiausio lygio svarbą, nepriklausomai nuo naudotojo nustatymų. Kritiniai skubūs taisymai taikomi numatant aukščiausio lygio svarbą, nepriklausomai nuo naudotojo nustatymų.

Kada naudotojai naudojasi neprijungta saugykla? Kada naudotojai naudojasi neprijungta saugykla?

Neprijungtoje saugykloje taip pat yra .dup ir .fup failai. Saugyklos skyrių turi atsisiųsti naudojant veidrodžio įrankį, o ne modulio naujinimą. Daugiau sužinosite perskaitę šį ESET žinių bazės straipsnį.

Kaip ESET produktai žino, kad reikalingas naujinimas? Iš saugyklos? Ar į serverius siunčiami kokie nors duomenys? ESET produktai atsisiunčia automatinius naujinius iš saugyklos.

ESET produktai atsisiunčia automatinius naujinius iš saugyklos. Serveriai yra tam pasiruošę, nes kritiniai naujiniai užima vos kelis kilobaitus. Kritinių naujinimų metu ESET saugyklų serveriuose netaikys jokių veiksmų draudimų. Tačiau yra galimybė įgalinti veiksmų draudimą serveriuose, jei automatiniai naujiniai užima daugiau vietos. Toliau pateiktoje lentelėje matysite skubių taisymų dydžių pavyzdį, jei atliekamas skirtuminis automatinis naujinimas.

Ankstesnė versija	Nauja versija	Dydis
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

Jei skirtuminis automatinis naujinimas nesėkmingas, ESET produktas gali pradėti visos apimties naujinimą. Tai vis dar yra automatinis naujinimas su funkcijų garantija, tačiau vietoj .dup failo bus atsisiųstas daugiau vietos užimantis .fup failas. Versija 9.0.2032.2 užima 27 MB. Tačiau toks scenarijus pasitaiko retai.

Ar „ESET Endpoint Security“ / „ESET Endpoint Antivirus“ versijos atnaujinimas vyks su veiksmų draudimu? Jei taip, kiek laiko naujinimas bus ribojamas po išleidimo?

ESET riboja naujinimus pirmąsias kelias savaites po to, kai išleidžiama nauja versija, kad sumažintų mūsų serverių apkrovą ir tolygiai paskirstytų naują versiją.

Automatiniai naujinimai taps vienu iš pagrindinių atnaujinimo būdų. Kaip tai veikia išsamiai?

ESET siekia atnaujinti kuo daugiau klientų per automatinius atnaujinimus. Sunku palaikyti tokį didelį ankstesnių versijų skaičių. Automatinio naujinimo funkcija veikia paprastai – .dup failai yra atsisiunčiami per pirmąjį modulio naujinimo tikrinimą. Naujinimo procedūros metu produktas yra visiškai funkcionalus ir apsaugo kompiuterį. Nauja versija aktyvinama paleidus iš naujo. ESET PROTECT (serverio pusėje) galite naudoti politiką, kad nurodytumėte naujausią versiją, iki kurios norite atnaujinti, arba naudotumėte pakaitos simbolius. Daugiau informacijos žr. ESET PROTECT arba ESET PROTECT Cloud interneto žinyno automatinių naujinimų skyriuje.

Ar tiesa, kad automatiniai naujinimai veikia 1/10? Dabar naudoju „ESET Endpoint Security 8.0.2028.1“. Paleidus automatinius naujinimus, į kokią versiją bus atnaujinta?

Produktų naujinimas naudojant automatinius naujinimus gali būti atidėtas dėl saugyklos serverių veiksmo draudimo. Jei produkto naujinimas išleidžiamas su veiksmo draudimu, jų gavimas automatinio naujinimo patikrinimuose gali vėluoti. Jei naujinys saugus ir stabilus, veiksmo draudimo keitimas vėliau gali būti sumažintas arba visiškai pašalintas, kad visi likę klientai gautų naujinį.

Veiksmo draudimo procedūra gali užtrukti įvairiai atliekant kiekvieną naujinimą. Laikas priklauso nuo to, kiek klientų prašo naujinio, koks yra srautas mūsų serveriuose bei kitų veiksnių. Ši procedūra nuolat tobulinama, pokyčiai vyksta visą laiką. Be to, kadangi automatinio naujinimo funkcija yra nauja, šią procedūrą ateityje dar greičiausiai tobulinsime ir toliau gerinsime klientų patirtį.

Jei įjungsiu kompiuterį 8:45 val. ir išjungsiu 17:00 val., kada bus vykdomi automatiniai naujinimai?

Kito sėkmingo suplanuoto modulio naujinimo metu, ne daugiau kaip kartą per 24 valandas.

Jei kompiuteris išsijungia, kol vyksta automatiniai naujinimai, kada naujinimas bus pratęstas?

Naujinimas bus vykdomas kitame suplanuotame naujinimo lange. Yra numatytas patikimas automatinio naujinimo procedūros (anksčiau uPCU) saugos mechanizmas. Atsisiuntus naujinį ir iš naujo paleidus kompiuterį, atnaujinti failai vis dar ruošiami naudoti, o tuo metu įdiegta versija suteikia nepertraukiamą apsaugą. Pakeitimai taikomi kitąkart paleidus ESET įrenginio produktą.

Kaip galiu paleisti automatinius naujinimus iš karto, nelaukdamas įprasto ryšio kas 24 valandas? Ar yra koks nors kitas būdas spustelėti „Naujinimų tikrinimas“?

Automatinio naujinimo procedūrą neautomatiniu būdu galite iškviesti tik atidarę pagrindinės programos langą ir spustelėję **Naujinti** > **Naujinimų tikrinimas**. Visi kiti modulio naujinimų iškvietimo būdai veikia pagal 24 valandų automatinio naujinimo planuoklės politiką. Šiuo metu neįmanoma nuotoliniu būdu paleisti automatinio naujinio atsisiuntimo. Šią funkciją įtrauksime ateityje.

Kaip naujinti ESET Endpoint Security

Naujinti ESET Endpoint Security galima rankiniu būdu arba automatiškai. Norėdami paleisti naujinimą, spustelėkite **Naujinti** pagrindiniame programos lange, tada spustelėkite **Ieškoti atnaujinimų**.

Pagal numatytuosius diegimo parametrus sukuriama automatinio naujinimo užduotis, kuri atliekama kas valandą. Jei norite keisti intervalą, pereikite į **Įrankiai** > **Planuoklė** (žr. daugiau informacijos apie planuoklę).

Kaip suaktyvinti ESET Endpoint Security

Baigus diegti jums bus pasiūlyta suaktyvinti savo produktą.

Yra keletas būdų aktyvinti produktą. Konkretus aktyvinimo scenarijus aktyvinimo lange gali būti naudojamas atsižvelgiant į šalį ir platinimo būdą (ESET tinklalapis, diegimo programos tipas .msi ar .exe ir t. t.).

Norėdami aktyvinti savo ESET Endpoint Security kopiją tiesiai iš programos, atidarykite ESET Endpoint Security pagrindinį programos langą ir pagrindiniame meniu spustelėkite **Žinynas ir palaikymas** > **Aktyvinti produktą** arba **Apsaugos būsena** > **Aktyvinti produktą**.

Kad suaktyvintumėte ESET Endpoint Security, galite naudoti bet kurį iš šių metodų:

- **Naudokite įsigytą licencijos raktą** – tai unikali simbolių seka, atitinkanti formatą „XXXX-XXXX-XXXX-XXXX-XXXX“ ir naudojama licencijos savininkui identifikuoti bei licencijai suaktyvinti.
- **ESET Business Account** – paskyra sukurta ESET Business Account portale naudojant kredencialus (el. pašto adresą ir slaptažodį). Šis metodas leidžia valdyti kelias licencijas iš vienos vietos.
- **Autonominė licencija** – tai automatiškai sukurtas failas, kuris persiunčiamas į ESET produktą licencinei informacijai pateikti. Jei licencija leidžia atsisiųsti autonominės licencijos failą (.lf), jį galima panaudoti suaktyvinant atsijungus. Autonominių licencijų skaičius atimamas iš bendrojo pasiekiamų licencijų skaičiaus. Išsamesnės informacijos apie autonominio failo kūrimą rasite ESET Business Account vartotojo vadove.

Jei jūsų kompiuteris priklauso valdomam tinklui, spustelėkite **Aktyvinti vėliau**, o jūsų administratorius aktyvinimą atliks nuotoliniu būdu per ESET PROTECT. Šią parinktį galite naudoti ir tada, kai šį klientą nusprendžiate aktyvinti vėliau.

Jei turite vartotojo vardą bei slaptažodį, kuriuos naudojote senesniems ESET produktams aktyvinti, tačiau nežinote, kaip suaktyvinti ESET Endpoint Security, konvertuokite savo senus kredencialus į licencijos raktą.

Nepavyko aktyvinti produkto?

Produkto licenciją galite pasikeisti bet kuriuo metu. Jei norite tai padaryti, pagrindiniame programos lange spustelėkite **Žinynas ir palaikymas** > **Keisti licenciją**. Matysite viešą licencijos ID, kuriuo ESET techninės pagalbos tarnybai identifikuojama jūsų licencija. Vartotojo vardas, kuriuo registruotas jūsų kompiuteris, saugomas skyriuje **Apie**, kurį galite pamatyti dešiniuoju pelės mygtuku spustelėję sistemos dėklo piktogramą.

> „ESET PROTECT“ 7.2 arba „ESET PROTECT“ 9 gali tyliai suaktyvinti kliento kompiuterius, naudodamasis administratoriaus suteiktomis licencijomis. Kaip tai padaryti, žr. „ESET PROTECT“ internetinį žinyną.

Licencijos rakto įvedimas aktyvinimo metu

Automatiniai naujinimai yra labai svarbūs jūsų saugumui. ESET Endpoint Security gaus naujinimus tik jį suaktyvinus naudojant **Licencijos raktą**.

Jei licencijos rakto neįvedėte baigę diegti, jūsų produktas nebus suaktyvintas. Licenciją galite pakeisti pagrindiniame programos lange. Tai galite padaryti spustelėdami **Žinynas ir palaikymas** > **Aktyvinti licenciją** ir į

produkto aktyvinimo langą įvesdami licencijos duomenis, kuriuos gavote su ESET saugos produktu.

Įvedant **Licencijos raktą** labai svarbu jį įvesti tiksliai taip, kaip jis parašytas:

- Licencijos raktas – tai unikali simbolių seka, atitinkanti formatą XXXX-XXXX-XXXX-XXXX-XXXX ir naudojama licencijos savininkui identifikuoti bei licencijai suaktyvinti.

Kad viską atliktumėte tiksliai, licencijos raktą rekomenduojame įklijuoti nukopijavus iš registracijos el. laiško.

Prisijungimas prie ESET Business Account

Saugumo administratoriaus paskyra – tai paskyra, sukurta ESET Business Account portale naudojant jūsų **el. pašto adresą** ir **slaptažodį**, su kuriais galima pamatyti visas vietos autorizacijas. Saugumo administratoriaus paskyra leidžia jums valdyti kelias licencijas. Jei dar neturite saugumo administratoriaus paskyros, spustelėkite **Sukurti paskyrą**, ir būsite nukreipti į ESET Business Account portalą, kuriame galėsite užsiregistruoti, naudodami savo kredencialus.

Jei pamiršote savo slaptažodį, spustelėkite **Pamiršau slaptažodį**, ir būsite nukreipti į ESET Business Account portalą. Įveskite savo el. pašto adresą ir spustelėkite **Prisijungti**, kad patvirtintumėte. Po to gausite pranešimą su instrukcijomis, kaip nustatyti slaptažodį iš naujo.

Kaip naudoti pasenusius licencijos duomenis naujesniam ESET įrenginio produktui aktyvini

Jei jau turite vartotojo vardą bei slaptažodį ir norite gauti licencijos raktą, apsilankykite ESET Business Account portale, kuriame galima konvertuoti savo kredencialus į naują licencijos raktą.

Kaip pašalinti virusą iš mano kompiuterio

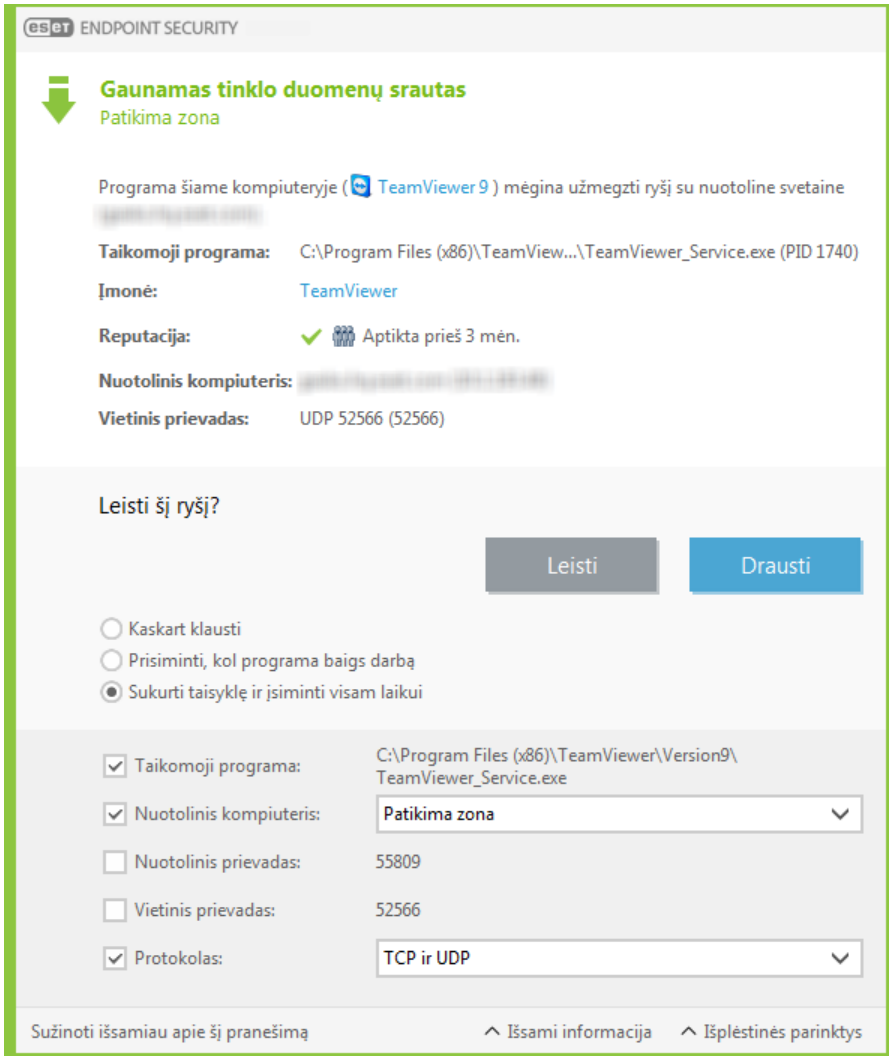
Jei kompiuteryje pastebite užsikrėtimo kenkimo programa požymių, pvz., jis pradeda lėčiau veikti, dažnai užstringa, rekomenduojame atlikti šiuos veiksmus:

1. Pagrindiniame programos lange spustelėkite **Kompiuterio nuskaitymas**.
2. Spustelėkite **Išmanusis nuskaitymas**, kad prasidėtų jūsų sistemos nuskaitymas.
3. Kai nuskaitymas bus baigtas, peržiūrėkite žurnalą su nuskaitytų, užkrėstų ir išvalytų failų skaičiumi.
4. Jeigu norite nuskaityti tik tam tikrą disko dalį, spustelėkite **Pasirinktinis nuskaitymas** ir pasirinkite tikslus, kuriuos reikia nuskaityti ieškant virusų.

Papildomos informacijos rasite mūsų reguliariai atnaujinamame ESET žinių bazės straipsnyje.

Kaip leisti ryšį tam tikroms taikomosioms programoms

Jeigu interaktyviuoju režimu aptinkamas naujas ryšys ir jeigu nėra atitinkamos taisyklės, jums bus pasiūlyta leisti arba uždrausti ryšį. Jeigu norite, kad ESET Endpoint Security atliktų tą patį veiksmą kiekvieną kartą, kai taikomoji programa bando užmegzti ryšį, pasirinkite žymės langelį **Įsiminti veiksmą (sukurti taisyklę)**.



Galite kurti naujas užkardos taisykles programoms, kol jų dar neaptiko ESET Endpoint Security. Tai padarysite užkardos sąrankos lange, atidarę pagrindinį programos langą > **Sąranka** > **Tinklas-** > **Užkarda** > spustelėkite krumpliaratį > **Konfigūruoti** > **Išplėstiniai** > **Taisyklės** ir spustelėję **Redaguoti**.

Spustelėkite **Pridėti**, kad pridėtumėte taisyklę. Skirtuke **Bendra** įveskite taisyklės pavadinimą, kryptį ir ryšio protokolą. Šiame lange galite nustatyti veiksmą, kuris bus atliktas pritaikius taisyklę.

Įveskite kelią į programos vykdomąjį failą ir vietinį ryšio prievadą skirtuke **Vietinis**. Eikite į skirtuką **Nuotolinis** ir įveskite nuotolinį adresą ir prievadą (jeigu naudojama). Naujai sukurta taisyklė bus taikoma, kai tik taikomoji programa bandys dar kartą užmegzti ryšį.

Kaip sukurti naują užduotį planuoklėje

Norėdami sukurti naują užduotį, skyriuje **Įrankiai** > **Planuoklė** spustelėkite **Pridėti užduotį** arba spustelėkite dešiniuoju pelės klavišu ir iš kontekstinio meniu pasirinkite **Pridėti**. Yra penki planinių užduočių tipai:

- **Vykdyti išorinę taikomąją programą** – leidžia planuoti išorinės taikomosios programos vykdymą.
- **Žurnalo priežiūra** – žurnalo failuose taip pat gali būti panaikintų įrašų likučių. Ši užduotis reguliariai optimizuoja įrašus žurnalo failuose, kad darbas būtų efektyvus.
- **Sistemos paleidimo failo patikra** – tikrina failus, kurie leidžiami vykdyti paleidžiant sistemą arba registruojantis.
- **Sukurti kompiuterio būsenos momentinę kopiją** – sukuria ESET SysInspector kompiuterio momentinę

kopiją – surenka išsamią informaciją apie sistemos dalis (pvz., tvarkykles, programas) ir įvertina kiekvienos dalies rizikos lygį.
- **Kompiuterio nuskaitymas pareikalavus** – atlieka kompiuterio failų ir katalogų nuskaitymą.
- **Naujinti** – atnaujinant modulius suplanuojama naujinimo užduotis.

Kadangi **Naujinimas** yra viena iš dažniausiai naudojamų planinių užduočių, toliau paaiškinsime, kaip pridėti naują naujinimo užduotį:

Išskleidžiamajame meniu **Planuota užduotis** pasirinkite **Naujinimas**. Į lauką **Užduoties pavadinimas** įveskite užduoties pavadinimą ir spustelėkite **Toliau**. Pasirinkite užduoties vykdymo dažnumą. Galimos šios parinktys: **Vieną kartą**, **Pakartotinai**, **Kasdien**, **Kas savaitę** ir **Įvykus įvykiui. Nurodykite Praleisti užduotį, kai naudojama akumuliatoriaus energija**, kad maksimaliai apribotumėte energijos sąnaudas, kai nešiojamasis kompiuteris veikia maitinamas akumuliatoriaus. Užduotis bus vykdoma laukuose **Užduoties vykdymas** nurodytą datą ir laiku. Po to apibrėžkite, kokį veiksmą vykdyti, jei užduoties negalima atlikti arba užbaigti suplanuotu laiku. Galimos šios parinktys:

- **Kitu suplanuotu laiku**
- **Kaip įmanoma greičiau**
- **Iškart, jei nuo paskutinio vykdymo praėjo daugiau laiko nei nurodyta vertėje** (intervalą galima nustatyti naudojantis slinkimo laukeliu **Nuo paskutinio vykdymo praėjo**)

Kitame žingsnyje parodomas suvestinės langas su informacija apie suplanuotąją užduotį. Atlikę pakeitimus spustelėkite **Baigti**.

Pasirodys dialogo langas, suteikiantis galimybę pasirinkti profilius, kurie bus naudojami suplanuotai užduočiai. Čia galima nustatyti pirminį ir alternatyvųjį profilį. Alternatyvusis profilis naudojamas tuo atveju, jei užduoties nepavyksta užbaigti naudojant pirminį profilį. Patvirtinkite paspausdami **Baigti**. Nauja suplanuota užduotis bus įtraukta į esamų suplanuotų užduočių sąrašą.

Kaip suplanuoti kassavaitinį kompiuterio nuskaitymą

Norėdami planuoti reguliarią užduotį, atidarykite pagrindinį programos langą ir spustelėkite **Įrankiai** > **Planuoklė**. Žemiau rasite trumpus nurodymus, kaip suplanuoti užduotį, kuri nuskaitys jūsų vietinius diskų įrenginius kas savaitę. Jei reikia daugiau nurodymų, skaitykitežinių bazės straipsnį.

Norėdami suplanuoti nuskaitymo užduotį:

1. Spustelėkite **Pridėti** pagrindiniame planuoklės lange.
2. Iš išskleidžiamojo meniu pasirinkite **Kompiuterio nuskaitymas pareikalavus**.
3. Įveskite užduoties pavadinimą ir pasirinkite **Kas savaitę, kaip užduoties dažnumą**.
4. Nustatykite dieną ir laiką, kada užduotis bus vykdoma.
5. Pasirinkite **Vykdyti užduotį, kai tik bus įmanoma**, kad užduotis būtų įvykdyta vėliau, jei dėl kokios nors priežasties suplanuota užduotis nepradedama vykdyti pagal planą (pvz., išjungtas kompiuteris).
6. Peržiūrėkite suplanuotos užduoties suvestinę ir spustelėkite **Baigti**.
7. Išskleidžiamajame meniu **Tikslai** pasirinkite **Vietiniai įrenginiai**.
8. Spustelėkite **Baigti**, kad priskirtumėte užduotį.

Kaip prijungti ESET Endpoint Security prie ESET PROTECT

Įdiegę ESET Endpoint Security kompiuteryje ir norėdami prisijungti per ESET PROTECT, įsitikinkite, kad taip pat įdiegėte ESET Management agentą savo kliento darbo vietoje. Tai būtina kiekvieno kliento sprendimo dalis, kuri palaiko ryšį su ESET PROTECT Serveriu.

- ESET Management agento diegimas kliento darbo vietose

Taip pat skaitykite:

- Dokumentai apie nuotoliniu būdu valdomus įrenginius
- Kaip naudoti nepaisymo režimą
- Kaip taikyti rekomenduojamą politiką ESET Endpoint Security

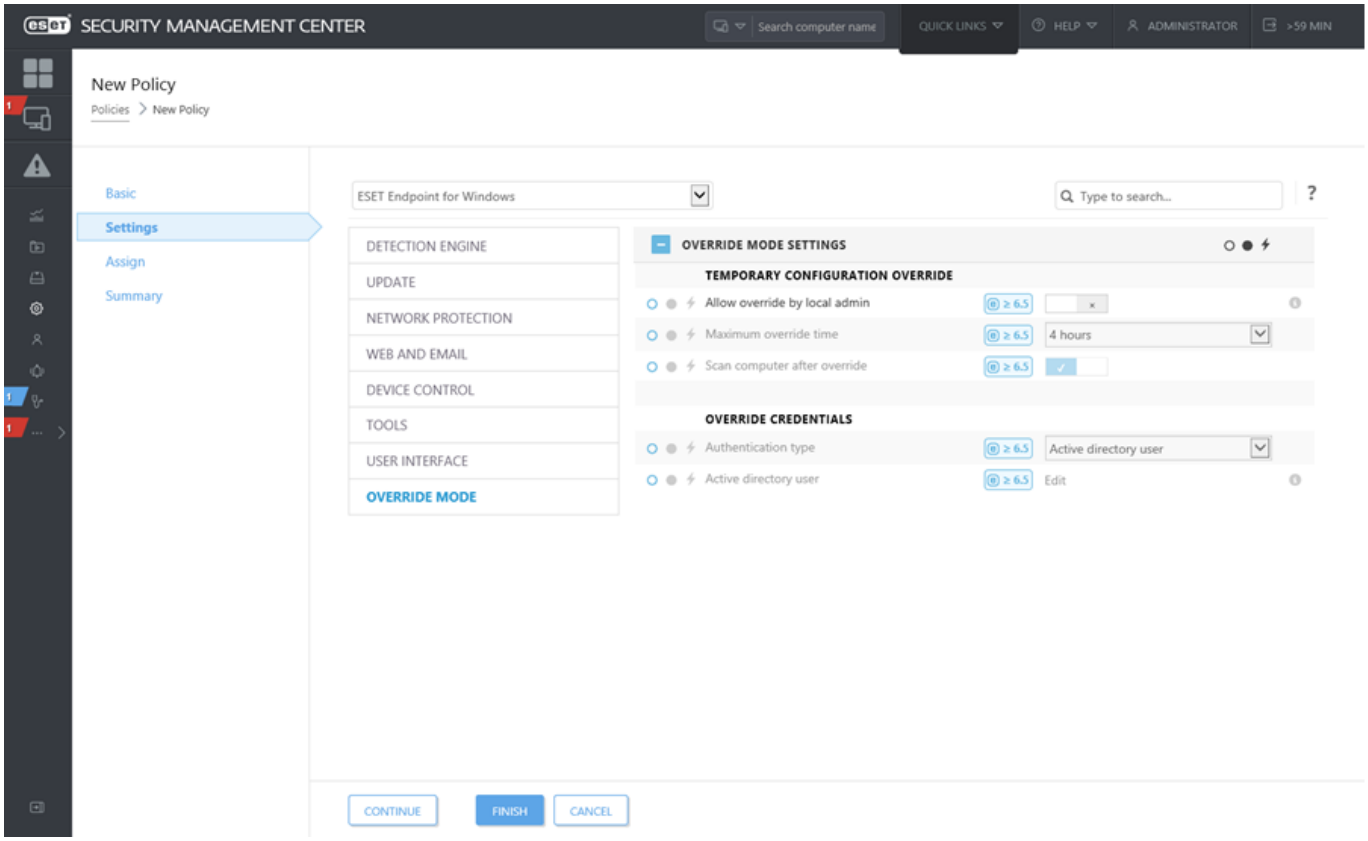
Kaip naudoti nepaisymo režimą

Naudotojai, kurių „Windows“ kompiuteriuose įdiegti „ESET Endpoint“ produktai (6.5 ir paskesnės versijos), gali naudotis nepaisymo funkcija. Nepaisymo režimas suteikia vartotojams galimybę klientinio kompiuterio lygiu keisti įdiegto ESET produkto parametrus, net ir tais atvejais, kai šiems parametrams taikoma politika. Galimybė naudotis nepaisymo režimu gali būti suteikta tam tikriems AD vartotojams arba ji gali būti apsaugota slaptažodžiu. Šios funkcijos negalima įjungti ilgesniam nei keturių valandų laikotarpiui.

⚠ • Nepaisymo režimo negalima sustabdyti iš ESET PROTECT tinkle valdomos konsolės, kai jis įjungtas. Nepaisymo režimas bus išjungtas, kai pasibaigs nepaisymo laikotarpis. Jį taip pat galima išjungti kliento įrenginyje.
• Naudotojas, kuris naudoja nepaisymo režimą, taip pat turi turėti „Windows“ administratoriaus teises. Kitu atveju naudotojas negali įrašyti keitimų ESET Endpoint Security nustatymuose.
• „Active Directory“ grupės autentifikavimas palaikomos ESET Endpoint Security 7.0.2100.4 ir naujesnėse versijose.

Nepaisymo režimo nustatymas:

1. Eikite į **Politikos** > **Nauja politika**.
2. Skirsnyje **Bendra** įveskite šios politikos parametrų **Pavadinimas** ir **Aprašymas** vertes.
3. Skirsnyje **Parametrai** pasirinkite **„ESET Endpoint for Windows“**.
4. Spustelėkite **Nepaisymo režimas** ir sukonfigūruokite nepaisymo režimo taisykles.
5. Skirsnyje **Priskyrimas** pasirinkite kompiuterį ar kompiuterių grupę, kuriai bus taikoma ši politika.
6. Peržiūrėkite parametrus, rodomus skirsnyje **Suvestinė** ir spustelėkite **Baigti**, kad politiką pritaikytumėte.



Tarkime, kad *Jonas* susiduria su keblumais: jo „Endpoint“ parametrai blokuoja tam tikrą svarbią funkciją arba galimybę naudotis saitynu iš jo kompiuterio. Administratorius gali *Jonui* leisti nepaisyti tuometinės jo „Endpoint“ politikos ir kompiuterio parametrus nusistatyti pačiam. Po to šių naujųjų parametrų gali paprašyti ESET PROTECT, kad administratorius iš jų galėtų sukurti naują politiką.

Tam atlikite šiuos veiksmus:

1. Eikite į **Politikos** > **Nauja politika**.
2. Užpildykite laukus **Pavadinimas** ir **Aprašymas**. Skirsnyje **Parametrai** pasirinkite **„ESET Endpoint for Windows“**.
3. Spustelėkite **Nepaisymo režimas**, įjunkite nepaisymo režimą vienai valandai ir kaip AD naudotoją pasirinkite *Joną*.
4. Priskirkite politiką *Jono kompiuteriui* ir spustelėkite **Baigti**, kad politiką įrašytumėte.
5. *Jonas* turi įjungti **Nepaisymo režimą** savo „ESET Endpoint“ ir savo kompiuteryje parametrus pakeisti rankiniu būdu.
6. ESET PROTECT saityno pulte eikite į **Kompiuteriai**, pasirinkite *Jono kompiuterį* ir spustelėkite **Rodyti išsamią informaciją**.
7. Skirsnyje **Konfigūracija** spustelėkite **Prašyti konfigūracijos** ir suplanuokite kliento užduotį – nedelsiant iš kliento gauti konfigūraciją.
8. Naujoji konfigūracija parodoma netrukus. Spustelėkite produktą, kurio parametrus pageidaujate įrašyti, tada spustelėkite **Atidaryti konfigūraciją**.
9. Galite šiuos parametrus peržiūrėti, tada spustelėkite **Konvertuoti į politiką**.
10. Užpildykite laukus **Pavadinimas** ir **Aprašymas**.
11. Jei reikia, skirsnyje **Parametrai** galite pakeisti parametrus.
12. Skirsnyje **Priskyrimas** galite šią politiką priskirti *Jono kompiuteriui* (arba kitiems).
13. Tam, kad parametrai būtų įrašyti, spustelėkite **Baigti**.
14. Jei politikos nepaisymas nebereikalingas, nepamirškite jo pašalinti.

Kaip taikyti rekomenduojamą politiką ESET Endpoint Security

Geriausia praktika prijungus ESET Endpoint Security prie ESET PROTECT yra taikyti rekomenduojamą politiką arba pasirinktinę politiką.

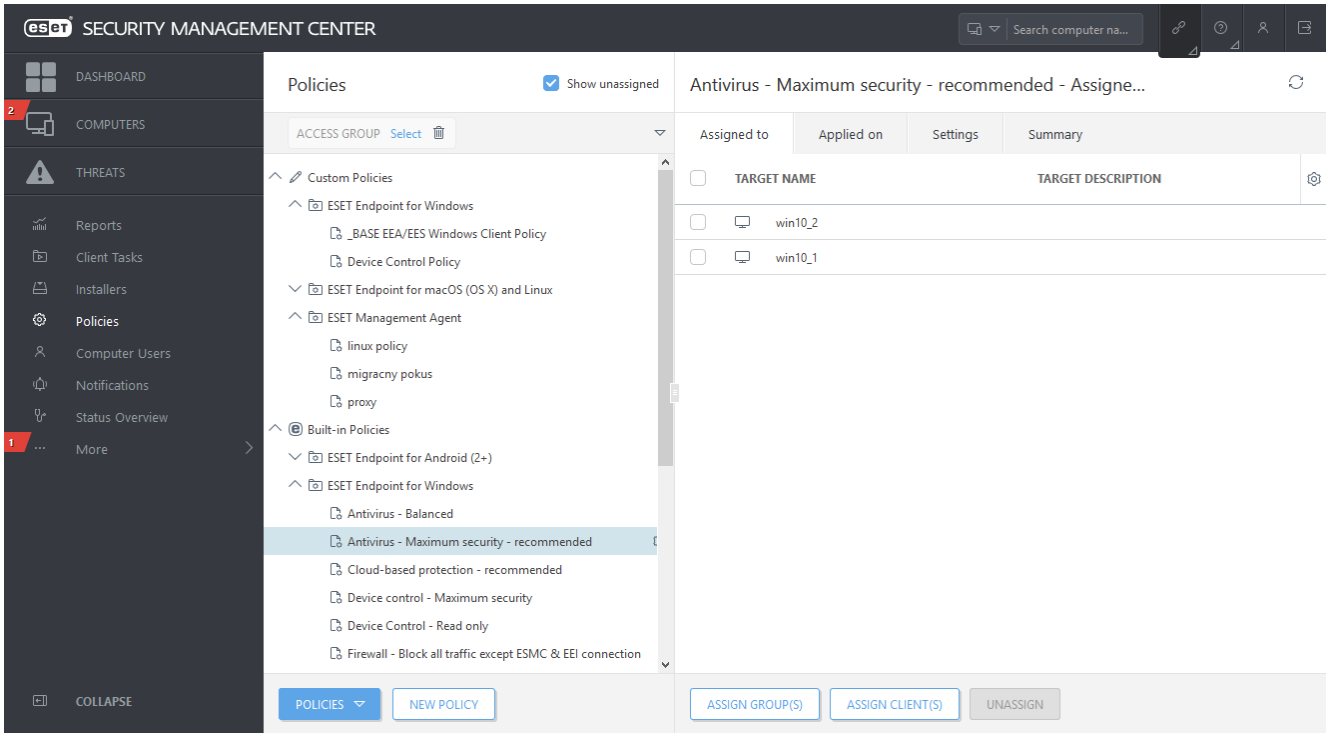
ESET Endpoint Security turi keletą integruotų politikų:

Politika	Aprašymas
Apsauga nuo virusų – subalansuota	Apsaugos konfigūracija rekomenduojama daugumai atvejų.
Apsauga nuo virusų – maksimali apsauga	Mašininio mokymosi, išsamios elgesio analizės ir SSL filtravimo naudojimas. Taikoma galimai nesaugių, nepageidaujamų ir įtartinų programų aptikimui.
Debesies pagrindo reputacijos ir atsiliepimų sistema	Įgalina „ESET LiveGrid®“ debesies pagrindo reputacijos ir atsiliepimų sistemą, kad pagerintų naujausių grėsmių aptikimą ir padėtų bendrinti kenkėjiškas arba nežinomas potencialias grėsmes tolesnei analizei.
Įrenginio kontrolė – maksimali apsauga	Visi įrenginiai blokuojami. Kai kuris nors įrenginys nori prisijungti, tai turi leisti administratorius.
Įrenginio kontrolė – tik skaitoma	Visi įrenginiai gali būti tik nuskaitomi. Įrašyti neleidžiama.
Užkarda – blokuojamas visas srautas, išskyrus ESET PROTECT ir „ESET Inspect“ ryšį	Blokuokite visą srautą, išskyrus ryšį su ESET PROTECT ir „ESET Inspect“ serveriu (tik ESET Endpoint Security).
Registravimas – visas diagnostinis registravimas	Šis šablonas užtikrina, kad administratorius turėtų visus žurnalus, kai tik jų prireikia. Viskas registruojama glaustai, įskaitant HIPS ir „Threatsense“ parametrus, užkardą. Žurnalai automatiškai naikinami po 90 dienų.
Registravimas – registruoti tik svarbius įvykius	Politika užtikrina, kad būtų registruojami įspėjimai, klaidos ir kritiniai įvykiai. Žurnalai automatiškai naikinami po 90 dienų.
Matomumas – subalansuotas	Numatytieji nustatymai matomumui. Įjungiamos būsenos ir pranešimai.
Matomumas – nematomas režimas	Išjungti pranešimai, įspėjimai, GUI, integracija į kontekstinį meniu. Nevykdoma egui.exe. Tinka valdymui tik iš ESET PROTECT Cloud.
Matomumas – sumažinta sąveika su naudotoju	Išjungtos būsenos, išjungti pranešimai, GUI pateikiama.

Norėdami nustatyti politiką **Apsauga nuo virusų – maksimali apsauga**, kuri taiko daugiau kaip 50 rekomenduojamų nustatymų ESET Endpoint Security, įdiegtų darbo stotyse, atlikite šiuos veiksmus:

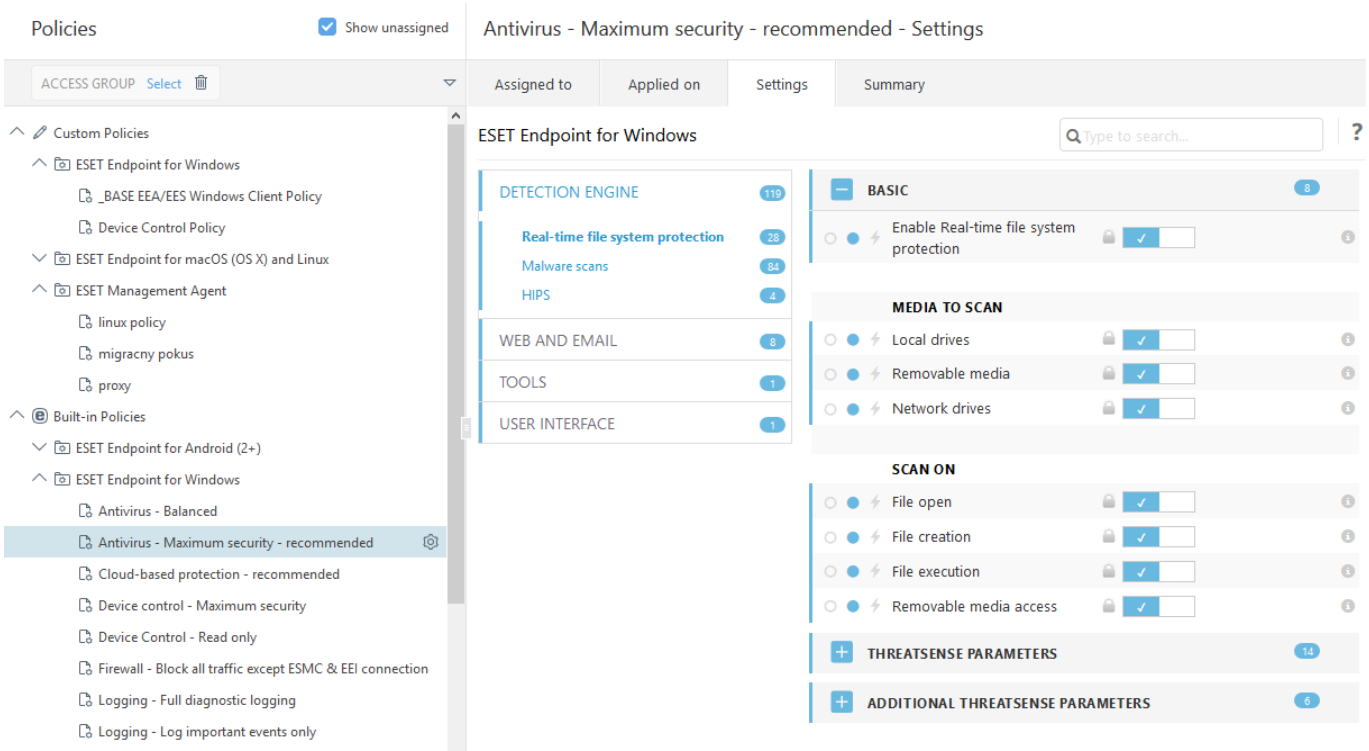
> Tolesni ESET žinių bazės straipsniai gali būti pasiekiami tik anglų kalba:
> • Pritaikykite rekomenduojamą arba iš anksto nustatytą politiką, skirtą ESET Endpoint Security, naudodami ESET PROTECT

1. Atidarykite ESET PROTECT tinkle valdomą konsolę.
2. Eikite į **Politikos** ir išplėskite **Integruotos politikos** > **„ESET Endpoint for Windows“**.
3. Spustelėkite **Apsauga nuo virusų – maksimali apsauga – rekomenduojama**.
4. Skirtuke **Priskirta** spustelėkite **Priskirti klientui (-ams)** arba **Priskirti grupę (-es)** ir pasirinkite atitinkamus kompiuterius, kuriems norite taikyti šią politiką.



Norėdami pamatyti, kurie nustatymai taikomi šiai politikai, spustelėkite skirtuką **Nustatymai** ir išplėskite išplėstinio nustatymo medį.

- Mėlynas taškelis žymi pakeistą šios politikos nustatymą
- Skaičius mėlyname taškelyje nurodo pakeistų šios politikos nustatymų skaičių
- Daugiau apie ESET PROTECT politiką skaitykite



Kaip sukonfigūruoti veidrodį

ESET Endpoint Security galima sukonfigūruoti įrašyti aptikimo modulio naujinimo failų kopijas ir paskirstyti naujinimus po kitas darbo stotis, kuriose veikia „ESET Endpoint Security“ arba „ESET Endpoint Antivirus“.

ESET Endpoint Security konfigūravimas veidrodiniu serveriu ir teikti naujinimus per vidinį HTTP serverį

1. Paspauskite **F5**, kad atidarytumėte Išplėstiniai nustatymai ir išskleiskite **Naujinimas** > **Profiliai** > **Naujinimo veidrodinis atspindys**.
2. Išskleiskite **Naujinimai** ir įsitikinkite, kad dalyje **Modulių naujinimai** įjungta parinktis **Pasirinkti automatiškai**.
3. Išskleiskite **Naujinimo veidrodinis atspindys** ir įjunkite **Sukurti naujinimo veidrodinį atspindį** bei **Įjungti HTTP serverį**.

Daugiau informacijos žr.:
- Naujinimo veidrodinis atspindys
- Naujinimas iš veidrodinio atspindžio

Veidrodinio serverio konfigūravimas naujinimams per bendrinamą tinklo aplanką teikti

1. Vietiniame arba tinklo įrenginyje sukurkite bendrinamą aplanką. Šis aplankas turi būti skaitomas visiems vartotojams, vykdantiems ESET saugumo sprendimus ir rašomas iš vietinės SISTEMOS paskyros.
2. Suaktyvinkite parinktį **Kurti naujinimo veidrodinį atspindį**, esančią **Išplėstiniai nustatymai** > **Naujinimas** > **Profiliai** > **Veidrodinis atspindys**.
3. Pasirinkite atitinkamą **Saugojimo aplanką** spustelėdami **Išvalyti** ir **Redaguoti**. Naršydami pasirinkite sukurtą bendrinimo aplanką.

Jei nenorite naujinti modulių per vidinį HTTP serverį, išjunkite parinktį **Kurti naujinimo veidrodinį atspindį**.

Kaip atnaujinti į „Windows 10“, naudojant ESET Endpoint Security

Mes primygtinai rekomenduojame prieš naujinant į „Windows 10“ atnaujinti į naujausią turimo ESET produkto versiją, tada atsisiųsti naujausius modulio naujinimus. Taip bus užtikrinta maksimali apsauga ir išsaugoti jūsų programos nustatymai bei licencijos informacija naujinant į „Windows 10“.

7.x versija.

Spustelėkite atitinkamą toliau pateiktą saitą, kad atsisiųstumėte ir įdiegtumėte naujausią versiją – taip paruošite naujinti į „Microsoft Windows 10“:

Atsisiųsti „ESET Endpoint Security 7“, 32 bitų Atsisiųsti „ESET Endpoint Antivirus 7“, 32 bitų

Atsisiųsti „ESET Endpoint Security 7“, 64 bitų Atsisiųsti „ESET Endpoint Antivirus 7“, 64 bitų

5.x versija.

Prasidėjo 5 versijos „ESET Endpoint“ produktų gyvavimo ciklo pabaigos etapas. Tai reiškia, kad komponavimo versijos nebėra viešai prieinamos atsisiųsti. Primygtinai rekomenduojame įsidiegti naujausią „ESET Endpoint“ produktų versiją.

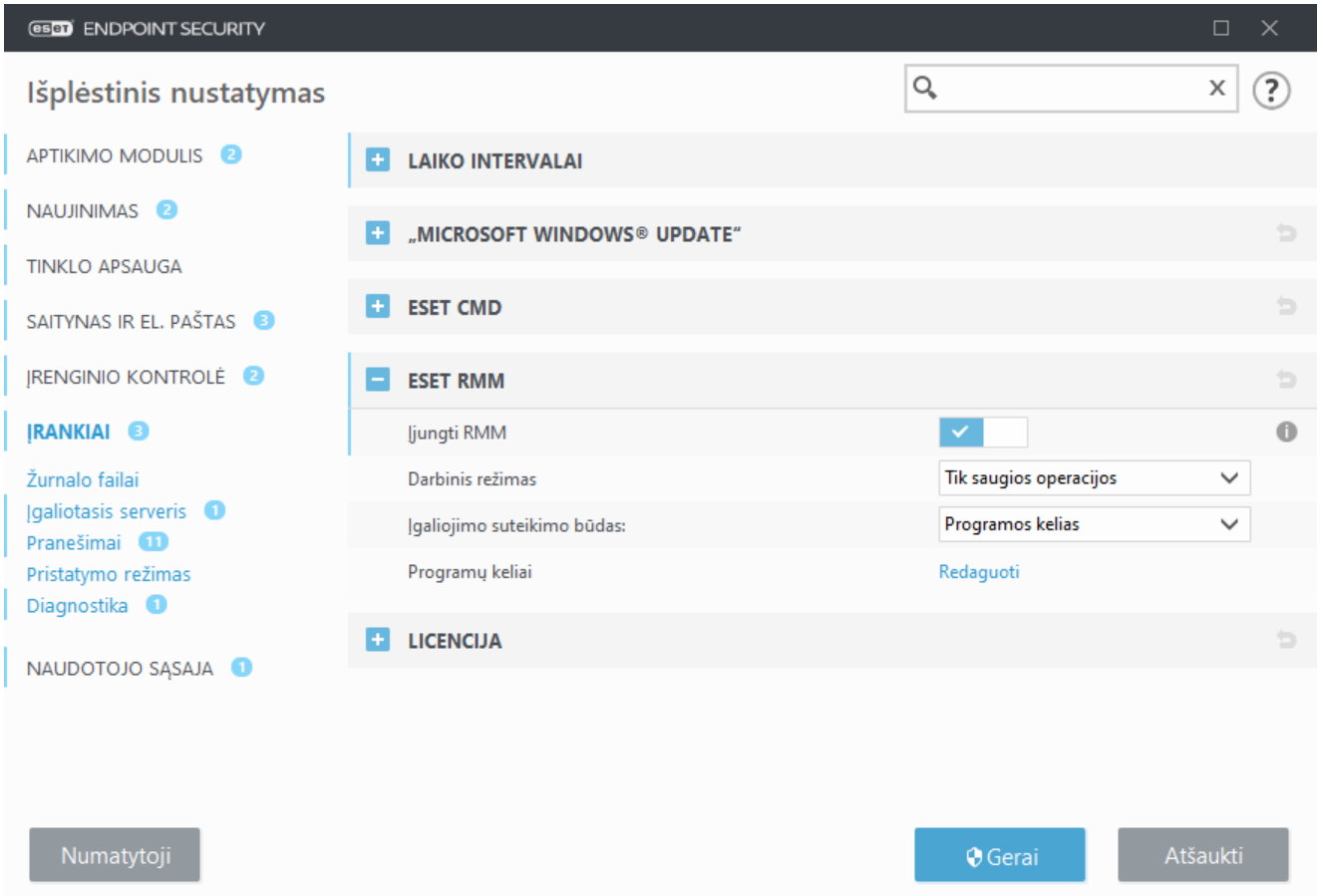
Versijos kitomis kalbomis:

Jei ieškote savo „ESET Endpoint“ produkto versijos kita kalba, apsilankykite mūsų atsisiuntimo puslapyje.

Papildoma informacija apie „ESET“ verslo produktų suderinamumą su „Windows 10“.

Kaip suaktyvinti nuotolinio stebėjimo ir valdymo funkciją

Nuotolinis stebėjimas ir valdymas (RMM) – tai programinės įrangos sistemų (pvz., stalinių kompiuterių, serverių ir mobiliųjų įrenginių) stebėjimo ir valdymo procesas, vykdomas naudojant vietoje įdiegtą agentą, kurį gali pasiekti valdymo paslaugos teikėjas. ESET Endpoint Security galima valdyti, naudojant RMM 6.6.2028.0 versiją.



Pagal numatytuosius nustatymus ESET RMM yra išjungta. Jei ESET RMM norite įjungti, paspauskite **F5**, kad atidarytumėte išplėstinį nustatymą, spustelėkite **Įrankiai**, išplėskite **ESET RMM** ir įjunkite jungiklį šalia **Įjungti RMM**.

Darbinis režimas – Pasirinkite **Tik saugios operacijos**, jei norite įjungti RMM sąsają saugioms ir tik skaityti skirtoms

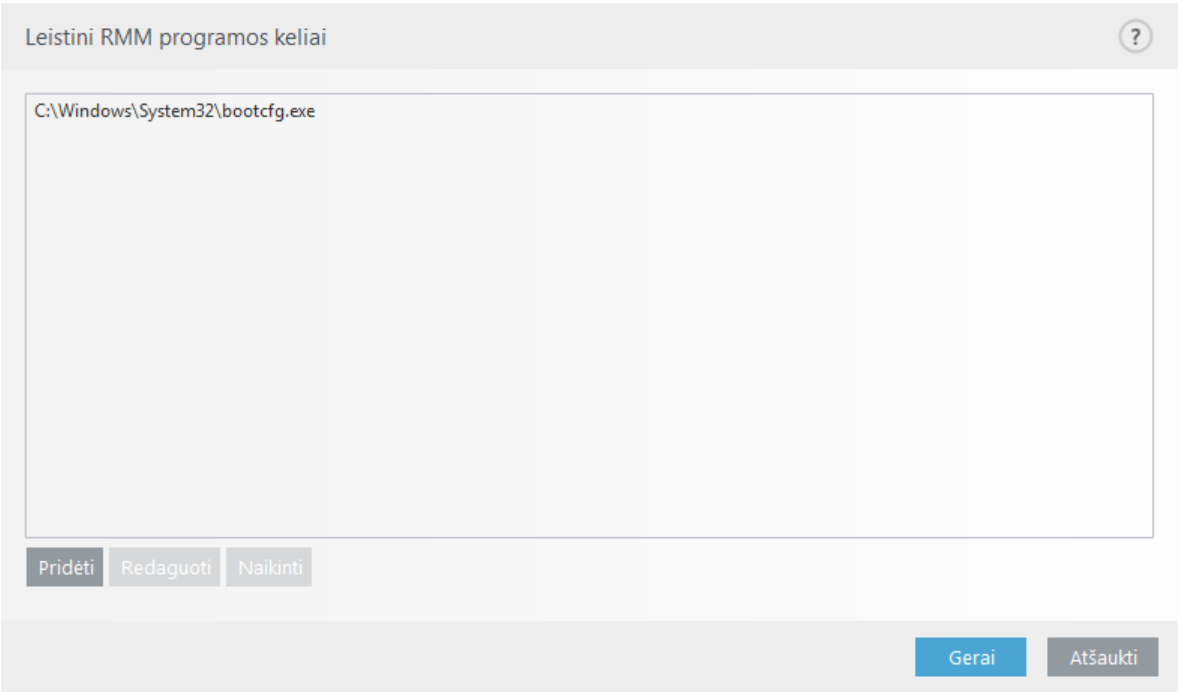
operacijoms. Pažymėkite **Visos operacijos**, jei norite įjungti RMM sąsają visoms operacijoms.

Operacija	Režimas Tik saugios operacijos	Režimas Visos operacijos
Gauti informaciją apie programą	✔	✔
Gauti konfigūraciją	✔	✔
Gauti licencijos informaciją	✔	✔
Gauti žurnalus	✔	✔
Gauti apsaugos būseną	✔	✔
Gauti naujinimo būseną	✔	✔
Nustatyti konfigūraciją		✔
Pradėti aktyvinimą		✔
Pradėti nuskaitymą	✔	✔
Pradėti naujinimą	✔	✔

Įgaliojimo būdas – nustatykite RMM įgaliojimo būdą. Jei norite naudoti įgaliojimą, išskleidžiamajame meniu pasirinkite **Programos kelias**, kitu atveju pasirinkite **Joks**.

RMM visada turėtų naudoti įgaliojimą, kad kenkėjiškos programos neišjungtų arba neapeitų „ESET Endpoint“ apsaugos.

Programų keliai – konkreti programa, kuriai leidžiama vykdyti RMM. Jei kaip įgaliojimo būdą pasirinkote **Programos kelias**, spustelėkite **Redaguoti** ir pereikite į konfigūracijos langą **Leistini RMM programų keliai**.



Pridėti – sukurkite naują leistiną RMM programos kelią. Įveskite kelią arba spustelėkite mygtuką **…**, kad pasirinktumėte vykdomąjį failą.

Redaguoti – pakeiskite esamą programos kelią. Parinktį **Redaguoti** naudokite, jei vykdomojo failo vieta buvo perkelta į kitą aplanką.

Naikinti – panaikinkite esamą leistiną kelią.

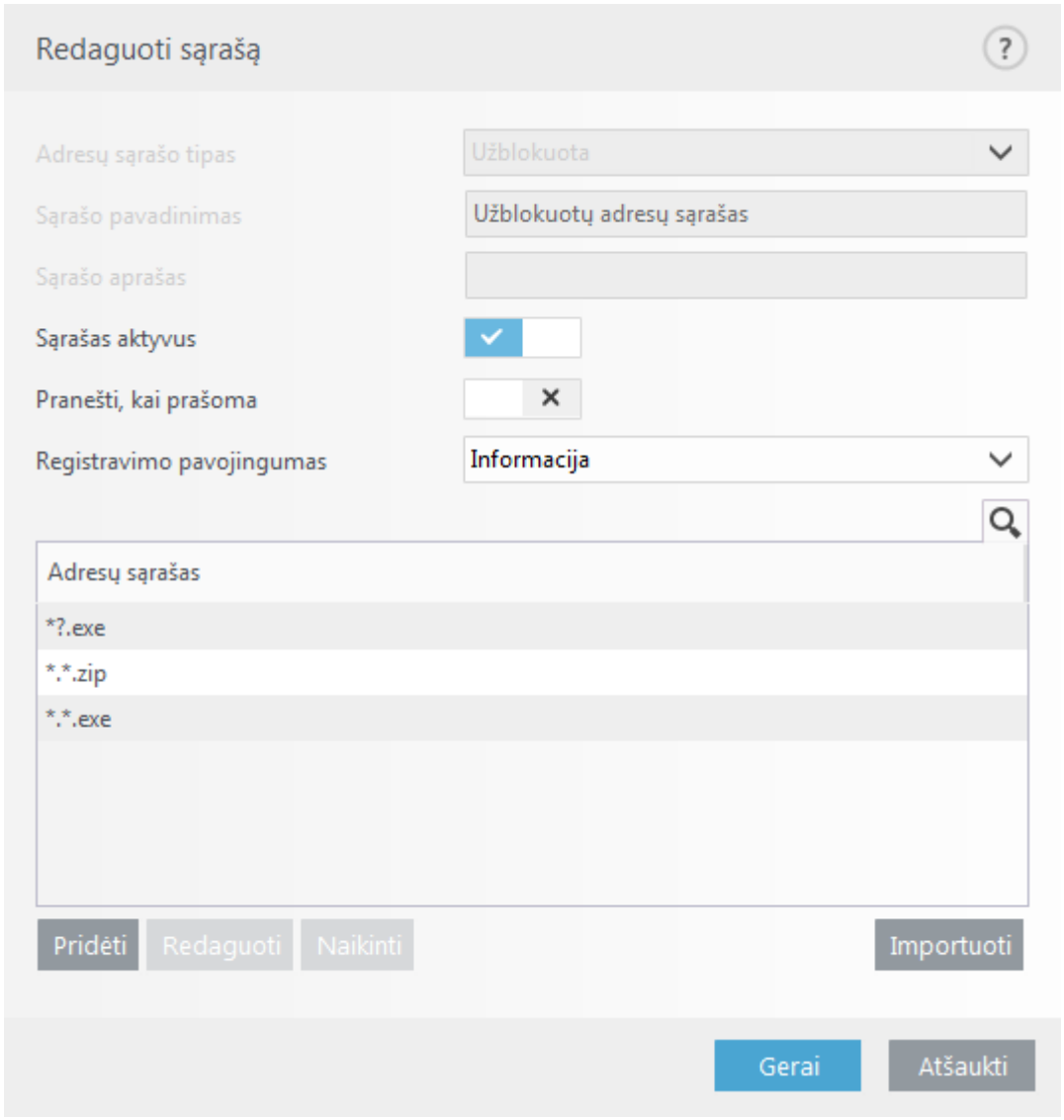
Numatytajame ESET Endpoint Security diegime yra failas „ermm.exe“, esantis „Endpoint“ programos kataloge (numatytasis kelias C*:\Program Files\ESET\ESET Security*). „ermm.exe“ keičiasi duomenimis su RMM papildiniu, kuris palaiko ryšį su RMM agentu, susietu su RMM serveriu.

- „ermm.exe“ – komandos eilutės priemonė, kurią sukūrė ESET ir kuri leidžia tvarkyti „Endpoint“ produktus bei ryšį su visais RMM papildiniais.
- RMM papildinys yra trečiosios šalies programa, veikianti vietoje, „Endpoint Windows“ sistemoje. Šis papildinys yra skirtas ryšiui su konkrečiu RMM agentu (pvz., tik „Kaseya“) ir „ermm.exe“ palaikykite.
- RMM agentas yra trečiosios šalies programa (pvz., „Kaseya“), veikianti vietoje, „Endpoint Windows“ sistemoje. Agentas palaiko ryšį su RMM papildiniu ir RMM serveriu.

Kaip blokuoti konkrečių failų tipų atsisiuntimą iš interneto

Jei nenorite leisti iš interneto atsisiųsti konkrečių tipų failų (pvz., „exe“, „pdf“ ar „zip“), naudokite URL adresų valdymo funkciją su pakaitos simbolių kombinacija. Paspauskite klavišą „F5“, kad atidarytumėte **išplėstinius nustatymus**. Spustelėkite **„Web and Email“** (saitynas ir el. paštas) > **„Web access protection“** (prieigos prie saityno apsauga) ir išplėskite **„URL Address Management“** (URL adresų valdymas). Spustelėkite **„Edit“** (redaguoti) šalia **adresų sąrašo**.

Adresų sąrašo lange pasirinkite **„List of blocked addresses“** (užblokuotų adresų sąrašas) ir spustelėkite **„Edit“** (redaguoti) arba spustelėkite **„Add“** (pridėti), jei norite sukurti naują sąrašą. Atsivers naujas langas. Jei kuriate naują sąrašą, išskleidžiamajame meniu **„Address list type“** (adresų sąrašo tipas) pasirinkite **„Blocked“** (užblokuota) ir pavadinkite sąrašą. Jeigu norite gauti pranešimą, kai pasiekiamas failo tipas iš esamo sąrašo, įjunkite **„Notify“** (pranešti) pastumdami slankiklio juostą. Išskleidžiamajame meniu pasirinkite **„Logging severity“** (registravimo svarba). Nuotolinis administratorius gali rinkti įrašus su įspėjimų **daugiažodiškumu**.



Spustelėkite „**Add**“ (pridėti), jei norite įvesti kaukę, nurodančią failų tipus, kurių atsisiuntimą norite blokuoti. Įveskite visą URL, jei norite blokuoti konkretaus failo atsisiuntimą iš konkrečios svetainės, pavyzdžiui, *http://example.com/file.exe*. Galite naudoti pakaitos simbolius, norėdami paslėpti failų grupę. Klaustukas (?) reiškia vieną kintamąjį simbolį, o žvaigždutė (*) reiškia kintamąją eilutę iš nulio ar daugiau simbolių. Pavyzdžiui,kaukė „**/*.zip*“ blokuoja visus „zip“ formato suglaudintus failus, kuriuos ketinama atsisiųsti.

Turėkite omenyje, kad galite blokuoti tik konkrečių failų tipų atsisiuntimą naudojant šį būdą, kai failų plėtiniai yra failo URL dalis. Jei žiniatinklio puslapis naudoja failų atsisiuntimo URL, pvz., *www.example.com/download.php?fileid=42*, visi šioje nuorodoje esantys failai būtų atsisiųsti, net jei kuris nors plėtinys yra blokuojamas.

Kaip sumažinti ESET Endpoint Security naudotojo sąsają

Kai valdoma nuotoliniu būdu, galite taikyti iš anksto nustatytą „Matomumo“ politiką.

Priešingu atveju, atlikite veiksmus rankiniu būdu:

1. Paspauskite **F5**, norėdami atidaryti išplėstinius nustatymus ir išskleiskite **Naudotojo sąsaja** > **Naudotojo sąsajos elementai**.
2. **Paleidimo režimas** nustatykite ties norima reikšme. Daugiau informacijos paleidimo režimus.
3. Išjunkite **Rodyti prisistatymo langą paleidžiant** ir **Naudoti garso signalą**.

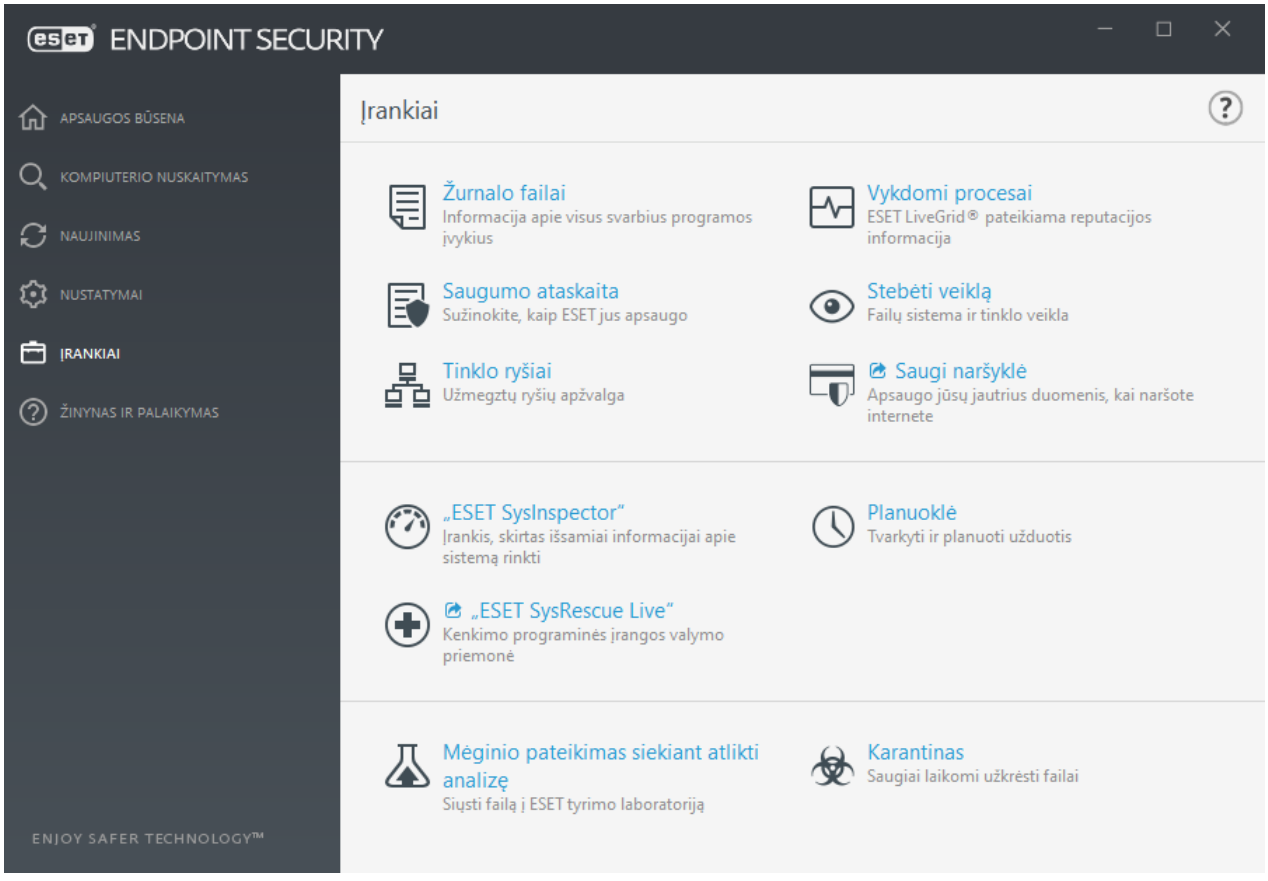
4. Konfigūruokite Pranešimai.
5. Konfigūruokite Programa būsenos.
6. Konfigūruokite Patvirtinimo pranešimai.
7. Konfigūruokite Įspėjimai ir pranešimų langai.

Kaip išspręsti klaidą „Secure Browser could not be redirected to the requested web page“ (saugios naršyklės nepavyko nukreipti į pageidaujamą tinklalapį)

Norėdami išspręsti šią klaidą, vadovaukitės tolesnėmis instrukcijomis:

Atlikę kiekvieną veiksmą patikrinkite, ar veikia saugi naršyklė
Jei naršyklės langas vis dar neveikia, atlikite kitą veiksmą, kol jis pradės veikti.

1. Paleiskite kompiuterį iš naujo.
2. Įsitikinkite, kad naudojate naujausią operacinės sistemos Windows ir savo ESET Windows verslo produkto versiją: Patikrinkite, ar naudojama naujausią ESET verslui skirtų produktų versija.



3. Gali būti, kad kilo konfliktas su trečiosios šalies apsaugine programine įranga arba užkarda. Rekomenduojame patikrinti ir pašalinti šią trečiosios šalies programinę įrangą programų diegimo/šalinimo lange. Spustelėkite **Įrankiai** > **Saugi naršyklė**. Atidarytame saugios naršyklės lange atlikite kitą veiksmą.
4. Išjunkite visus trečiųjų šalių naršyklių plėtinius.
5. Išvalykite naršyklės podėlį. Kaip išvalyti „Firefox“ podėlį arba kaip išvalyti „Google Chrome“ podėlį mano naršyklėje?
6. Įsitikinkite, kad jūsų numatytoji naršyklė nėra išskirta dalyje **Išplėstinis nustatymas** > **Saitynas ir el. paštas** >

Protokolų filtravimas > **Neįtrauktos programos**.

7. Jei ankstesniais veiksmais neatnaujinote ESET produkto, išdiekite ir iš naujo įdiekite savo ESET produktą. Kai kompiuteris bus paleistas iš naujo, išjunkite saugią naršyklę ir dar kartą paleiskite kompiuterį iš naujo. Vėl įjunkite saugią naršyklę ir pabandykite paleisti saugios naršyklės langą.

Saugi naršyklė – tai papildomas apsaugos lygis, skirtas finansiniams duomenims apsaugoti, kai atliekate operacijas internetu.

Dažniausiai saugi naršyklė paleidžiama naudojant numatytąją naršyklę, kai apsilankote žinomoje bankininkystės svetainėje. Norėdami tiesiogiai pasiekti apsaugotą naršyklę spustelėkite **Įrankiai** ESET Endpoint Security ir tada spustelėkite **Saugi naršyklė**.

Norėdami gauti daugiau informacijos apie saugios naršyklės funkcijas, perskaitykite toliau nurodytus ESET žinių bazės straipsnius anglų ir kai kuriomis kitomis kalbomis:

- Kaip naudotis ESET saugia naršykle?
- Įjunkite arba išjunkite ESET Banko mokėjimų apsaugą konkrečiai svetainei
- Banko mokėjimų apsaugos pristabdymas arba išjungimas ESET „Windows“ namų produktams
- ESET banko mokėjimų apsauga – dažniausios klaidos
- ESET terminų žodynas | Banko mokėjimų apsauga

Jeigu vis tiek negalite išspręsti problemos, kreipkitės į ESET techninės pagalbos tarnybą.

Galutinio vartotojo licencijos sutartis

Galioja nuo 2021 m. spalio 19 d.

SVARBU. prieš atsisiųsdami, diegdami, kopijuodami ar naudodami šį produktą, atidžiai perskaitykite produkto taikymo sąlygas. **ATSISIŲSDAMI, DIEGDAMI, KOPIJUODAMI AR NAUDODAMI ŠIĄ PROGRAMINĘ ĮRANGĄ JŪS IŠREIŠKIATE SAVO SUTIKIMĄ SU ŠIOMIS SĄLYGOMIS IR PRIPAŽĮSTATE PRIVATUMO POLITIKA.**

Galutinio vartotojo licencijos sutartį

Pagal šią Galutinio naudotojo licencijos sutartį (toliau – Sutartis), sudarytą tarp „ESET, spol. s r. o.“, kurios buveinė yra registruota adresu Einsteinova 24, 85101 Bratislava, Slovak Republic, ir kuri yra įtraukta į Bratislavos I apygardos teismo administruojamą Įmonių registrą (skyrius SRO, įrašo Nr. 3586/B), registracijos Nr. 31333532, (toliau – ESET arba Teikėjas) ir jūsų, fizinio ar juridinio asmens (toliau – Jūs ar Galutinis naudotojas), turite teisę naudotis Programine įranga, nurodyta Sutarties 1 straipsnyje. Sutarties 1 straipsnyje nurodyta Programinė įranga gali būti saugoma duomenų laikmenoje, siunčiama el. paštu, atsisiunčiama iš interneto, atsisiunčiama iš Teikėjo serverių ar įsigyjama iš kitų šaltinių, kaip tai apibrėžta toliau nurodytomis sąlygomis.

TAI GALUTINIO VARTOTOJO, O NE PARDAVIMO SUTARTIS. Programinės įrangos kopija ir fizinė laikmena iš įsigyto paketo, taip pat visos kitos kopijos, kurias Galutiniam vartotojui yra leista pasigaminti pagal Sutartį, toliau lieka pas Tiekėją.

Diegdami, kopijuodami ar naudodami Programinę įrangą spustelėję „Sutinku“, patvirtinsite, kad sutinkate su Sutarties sąlygomis ir Privatumo politika. Jei yra Sutarties ir (arba) Privatumo politikos sąlygų, su kuriomis Jūs

nesutinkate, nedelsdami spustelėkite parinktį „Nesutinku“, atšaukite diegimą ar siuntimą arba Programinę įrangą, diegimo laikmeną, susijusius dokumentus ir pirkimo kvitą sunaikinkite arba grąžinkite ESET ar prekybos įmonei, iš kurios įsigijote Programinę įrangą.

JŪS SUTINKATE, KAD NAUDODAMI PROGRAMINĘ ĮRANGĄ PRIPAŽĮSTATE, KAD PERSKAITĖTE ŠIĄ SUTARTĮ, SU JA SUSIPAŽINOTE IR SUTINKATE VYKDYTI JOJE IŠDĖSTYTAS SĄLYGAS.

1. **Programinė įranga**. Šioje Sutartyje vartojama sąvoka „Programinė įranga“ reiškia: (i) pagal šią Sutartį tiekiama kompiuterio programa ir visi jos komponentai; (ii) visą diskų, CD-ROM, DVD diskų, el. laiškų ir kitų priedų turinį ar kitą laikmeną, su kuria gavote šią Sutartį, įskaitant Programinės įrangos objektinį kodą, gautą duomenų laikmenoje, el. paštu ar atsisiunčiant internetu; (iii) visą susijusią aiškinamąją rašytinę medžiagą ir visą kitą galimą dokumentaciją, susijusią su Programine įranga, bei visus Programinės įrangos aprašymus, techninius duomenis, Programinės įrangos ypatybių ar veikimo aprašymus, visus veikimo aplinkos, kurioje Programinė įranga yra naudojama, aprašymus, Programinės įrangos naudojimo ar diegimo instrukcijas arba visus Programinės įrangos naudojimo būdo aprašymus („Dokumentacija“); (iv) Programinės įrangos kopijas, galimų Programinės įrangos klaidų pataisas, Programinės įrangos priedus, Programinės įrangos plėtinius, modifikuotas Programinės įrangos versijas ir Programinės įrangos komponentų naujinius (jei tokių yra), kuriais naudotis jums teisę suteikia Teikėjas pagal šios Sutarties 3 straipsnį. Programinė įranga bus pateikiama išskirtinai tik vykdomo objektinio kodo forma.

2. **Diegimas, kompiuteris ir licencijos raktas**. Programinę įrangą, gautą duomenų laikmenoje, atsiųstą el. paštu, atsisiųstą internetu, atsisiųstą iš Teikėjo serverių ar gautą iš kito šaltinio, reikia įdiegti. Programinę įrangą turite įdiegti tinkamai sukonfigūruotame kompiuteryje, kuris atitinka dokumentacijoje nurodytus reikalavimus. Diegimo būdas aprašomas Dokumentacijoje. Kompiuteryje, kuriame ketinate diegti Programinę įrangą, negali būti įdiegta kompiuterių programų ar aparatinės įrangos, kuri galėtų neigiamai paveikti Programinę įrangą. Kompiuteris apima aparatinę įrangą, įskaitant (bet neapsiribojant) asmeninius kompiuterius, nešiojamuosius kompiuterius, kompiuterizuotas darbo vietas, delninius kompiuterius, išmaniuosius telefonus, delninukus ir kitus elektroninius įrenginius, kuriems programinė įranga kuriama, kuriuose ji diegiama arba naudojama. Licencijos raktas yra unikali simbolių, raidžių arba specialiųjų ženklų seka, suteikta Galutiniam naudotojui, kad šis galėtų teisėtai naudotis Programine įranga, jos konkrečia versija arba pratęsti Licencijos laikotarpį pagal Sutarties sąlygas.

3. **Licencija**. Jei sutikote su šios Sutarties sąlygomis ir laikotės visų čia nustatytų sąlygų, Teikėjas suteikia Jums šias teises („Licenciją“):

a) **Diegimas ir naudojimas.** Jums suteikiama neišskirtinė, neperduodama teisė įdiegti Programinę įrangą kompiuterio standžiajame diske ar kitoje nuolatinėje laikmenoje, skirtoje Programinės įrangos duomenims saugoti, jai diegti ir saugoti kompiuterinės sistemos atmintyje, ir Programinę įrangą realizuoti, saugoti bei atkurti.

b) **Susitarimas dėl licencijų skaičiaus.** Teisė naudoti Programinę įrangą yra susieta su Galutinių vartotojų skaičiumi. Vienas Galutinis vartotojas reiškia, kad: i) Programinė įranga yra įdiegta vienoje kompiuterinėje sistemoje arba ii) jei licencijos apimtis yra susieta su pašto dėžučių skaičiumi, tuomet vienas Galutinis vartotojas reiškia kompiuterio naudotoją, kuris gauna el. paštą per Pašto naudojimo programą („PNP“). Jei PNP priima el. laišką ir jį automatiškai paskirsto keliems naudotojams, Galutinių vartotojų skaičius bus nustatomas pagal faktinį naudotojų, kuriems el. laiškai yra paskirstomi, skaičių. Jei pašto serveris atlieka pašto apsaugos (vartų) funkciją, Galutinių vartotojų skaičius sutaps su pašto serverio naudotojų, kuriems teikiama pašto apsaugos funkcija, skaičiumi. Jei vienam naudotojui nukreipiamas nenurodytas el. pašto adresų skaičius ir jis juos priima (pvz., naudojant alternatyviuosius vardus), o programa automatiškai nepaskirsto el. laiškų didesniam naudotojų skaičiui, vienam kompiuteriui yra privaloma viena licencija. Draudžiama naudoti tą pačią Licenciją vienu metu daugiau nei viename kompiuteryje. Galutinis naudotojas turi teisę įvesti Programinės įrangos Licencijos raktą ir naudotis Programine įranga tiek, kiek Galutinis naudotojas turi teisę tai daryti, atsižvelgiant į apribojimus, atsirandančius dėl Teikėjo suteiktų licencijų skaičiaus. Licencijos raktas laikomas konfidencialiu ir Jūs negalite bendrinti licencijos su trečiosiomis šalimis arba leisti trečiosioms šalimis naudoti licencijos raktą, jei to neleidžia ši Sutartis arba Teikėjas. Jei Licencijos raktas pažeistas, nedelsdami informuokite Teikėją.

c) **„Home Edition“ / „Business Edition“ (namams / įmonėms skirta versija).** Programinės įrangos „Home Edition“ versija skirta naudoti tik privačioje ir (arba) nekomercinėje aplinkoje namų ar šeimos reikmėms. Programinės įrangos „Business Edition“ versiją privaloma įsigyti, jei Programinė įranga bus naudojama komercinėje aplinkoje, pašto serveriuose, pašto perdavimo serveryje, pašto apsaugos serveryje ar interneto tinklų sietuve.

d) **Licencijos galiojimo laikas.** Teisė naudoti Programinę įrangą yra suteikiama ribotą laiką.

e) **OEM programinė įranga.** OĮG programinė įranga gali būti naudojama tik Kompiuteryje, su kuriuo ją įsigijote. Jos negalima perkelti į kitą kompiuterį.

f) **NESKIRTA PERPARDUOTI BANDOMOJI programinės įrangos versija.** Programinė įranga, KURI YRA NESKIRTA PERPARDUOTI ar BANDOMOJI, nėra apmokestinama ir turi būti naudojama tik Programinės įrangos funkcijoms pademonstruoti ar išbandyti.

g) **Licencijos nutraukimas.** Licencija automatiškai nutraukiama pasibaigus jos galiojimo laikui. Jei Jūs nesilaikysite Sutarties nuostatų, Tiekėjas turės teisę atsisakyti Sutarties ir pasinaudoti visomis teisėmis ar teisinėmis priemonėmis, kurios Tiekėjui prieinamos tokiais atvejais. Licencijos atšaukimo atveju privalote nedelsdami savo sąskaita Programinę įrangą ir visas jos atsargines kopijas ištrinti, sunaikinti arba grąžinti ESET arba prekybos įmonei, iš kurios Programinę įrangą įsigijote. Nutraukus licenciją, Tiekėjas taip pat turi teisę atšaukti galutinio vartotojo teisę naudotis Programinės įrangos funkcijomis, kurioms reikalingas prisijungimas prie Tiekėjo serverių ar trečiųjų šalių serverių.

4. **Funkcijos, kurios renka duomenis ir kurioms reikalingas interneto ryšys.** Kad tinkamai veiktų, programinei įrangai reikalingas interneto ryšys ir ji turi reguliariai užmegzti ryšį su Teikėjo serveriais arba trečiųjų šalių serveriais ir taikomu duomenų rinkimu, kaip tai numatoma Privatumo politikoje. Interneto ryšys ir atitinkamas duomenų rinkimas būtinas toliau nurodomoms programinės įrangos funkcijoms.

a) **Programinės įrangos naujinimai.** Tiekėjas turi teisę kartais išleisti Programinės įrangos naujinimus (toliau – Naujinimai), tačiau jų teikti neprivalo. Ši funkcija įjungiama standartiniuose Programinės įrangos nustatymuose, todėl, jei Galutinis naudotojas automatinio Naujinimų diegimo funkcijos neišjungė, Naujinimai yra įdiegiami automatiškai. Teikiant Naujinimus reikalingas Licencijų autentiškumo patvirtinimas, įskaitant informaciją apie Kompiuterį ir (arba) platformą, kurioje įdiegta Programinė įranga, kaip nurodyta Privatumo politikoje.

Bet kokių Naujinimų teikimui gali būti taikoma gyvavimo ciklo pabaigos politika (toliau – EOL politika), kurią galima rasti https://go.eset.com/eol_business. Jokie Naujinimai nebus teikiami po to, kai Programinė įranga ar bet kuri jos funkcija pasieks gyvavimo ciklo pabaigos datą, kaip apibrėžta EOL politikoje.

b) **Įsiskverbčių ir informacijos peradresavimas Teikėjui.** Programinėje įrangoje įdiegta funkcijų, kurios renka kompiuterinių virusų, kitų kompiuterinių kenkimo programų bei įtartinų, probleminių, galimų nepageidaujamų ar galimų nesaugių objektų (failų, URL, IP paketų ir eterneto kadrų) pavyzdžius („Įsiskverbtimis“) ir siunčia juos Teikėjui kartu su (neapsiribojant vien tik tuo) informacija apie diegimo procesą, kompiuterį ir (arba) platformą, kurioje Programinė įranga įdiegta, ir informacija apie Programinės įrangos operacijas bei funkcijas („Informacija“). Informacijoje ir Įsiskverbtyse gali būti duomenų (įskaitant atsitiktinai ar netyčia gautus asmeninius duomenis) apie Galutinį naudotoją ar kitus kompiuterio, kuriame įdiegta Programinė įranga, naudotojus, taip pat – failų, kuriuos paveikia Įsiskverbtys su susijusiais metaduomenimis.

Informaciją ir Įsiskverbtis gali rinkti šios Programinės įrangos funkcijos:

i. „LiveGrid“ reputacijos sistemos funkcija renka ir Teikėjui siunčia vienpusius informacijos rinkinius, susijusius su Įsiskverbtimis. Ši funkcija įjungiama Programinės įrangos standartinėse nuostatose.

ii. „LiveGrid“ grįžtamojo ryšio sistemos funkcija apima Infiltravimų su susijusiais metaduomenimis ir Informacijos rinkimą ir siuntimą Teikėjui. Galutinis vartotojas šią funkciją gali įjungti programinės įrangos diegimo metu.

Teikėjas gautą informaciją ir infiltravimus gali naudoti tik analizei ir atliekant infiltravimų tyrimus, tobulinant programinę įrangą ir licencijų autentiškumo patvirtinimą ir privalo imtis atitinkamų priemonių, kad būtų užtikrintas gautų infiltravimų ir informacijos saugumas. Suaktyvinus šią programinės įrangos funkciją, Teikėjas gali rinkti ir apdoroti infiltravimus ir informaciją taip, kaip tai nurodoma Privatumo politikoje ir vadovaujantis galiojančiais įstatymais. Šias funkcijas galima išjungti bet kuriuo metu.

Įgyvendinant šią Sutartį, būtina rinkti, apdoroti ir saugoti duomenis, kurie įgalina Teikėją identifikuoti jus vadovaujantis Privatumo politika. Jūs sutinkate, kad Teikėjas, norėdamas patikrinti, ar Jūs naudojate Programinę įrangą pagal Sutarties sąlygas, naudotų savo priemones. Jūs pateikiate sutikimą, kad ryšio tarp Programinės įrangos ir Teikėjo kompiuterių sistemų ar jo verslo partnerių kompiuterių sistemų metu būtų vykdomas duomenų perdavimas, kurio tikslas yra užtikrinti Programinės įrangos funkcionalumą ir leidimą ją naudoti bei Teikėjo teisių apsaugą.

Sudarius Sutartį Teikėjas ar bet kuris jo verslo partneris, kaip Teikėjo platinimo ir palaikymo tinklo dalis, sąskaitų pateikimo tikslu, vykdydamas šią Sutartį ir perduodamas pranešimus į jūsų kompiuterį, turi teisę perduoti, apdoroti ir saugoti pagrindinius Jus identifikuojančius duomenis.

Duomenys apie privatumą, asmeninių duomenų apsaugą ir jūsų teises pateikiami Privatumo politikoje, kurią rasite Teikėjo svetainėje ir galėsite pasiekti diegimo proceso metu. Taip pat galite ją rasti Programinės įrangos žinyno skyriuje.

5. **Galutinio vartotojo teisių įgyvendinimas**. Galutinio vartotojo teises galite įgyvendinti asmeniškai arba per savo darbuotojus. Jūs turite teisę Programinę įrangą naudoti tik tam, kad apsaugotumėte savo veiklą ir apsaugotumėte kompiuterines sistemas, kurioms Licencija yra taikoma.

6. **Teisių apribojimai.** Neturite teisės kopijuoti, platinti, išimti Programinės įrangos sudedamąsias dalis ar gaminti iš jos išvestinius produktus. Naudodami Programinę įrangą privalote laikytis šių apribojimų.

a) Nuolatinėje atminties laikmenoje galite pasigaminti vieną Programinės įrangos kopiją kaip archyvinę atsarginę kopiją su sąlyga, kad jūsų archyvinė atsarginė kopija nebus įdiegta ir naudojama kitame kompiuteryje. Visos kitos Jūsų pagamintos Programinės įrangos kopijos bus laikomos Sutarties pažeidimu.

b) Draudžiama naudoti, keisti, versti ar atgaminti Programinę įrangą, perleisti teises naudoti Programinę įrangą ar Programinės įrangos kopijas kokiu nors Sutartyje nenurodytu būdu.

c) Draudžiama parduoti, sublicencijuoti, nuomoti ar nuomotis, skolintis Programinę įrangą arba naudoti Programinę įrangą norint teikti komercines paslaugas.

d) Draudžiama keisti duomenis, perdaryti ar išardyti Programinę įrangą ar kitais būdais bandyti nustatyti pradinį Programinės įrangos kodą, išskyrus atvejus, kai šį apribojimą aiškiai draudžia įstatymas.

e) Sutinkate Programinę įrangą naudoti tik tokiu būdu, kuris neprieštarauja įstatymams, galiojantiems jurisdikcijoje, kurioje naudojate Programinę įrangą, įskaitant galiojančius apribojimus dėl autorių teisių ir kitas intelektinės nuosavybės teises, bet tuo nepasiribojant.

f) Sutinkate, kad Programine įranga ir jos funkcijomis naudositės tik taip, kad neribotumėte kitų galutinių vartotojų prieigos prie šių paslaugų. Tiekėjas pasilieka teisę apriboti atskiriems galutiniams vartotojams teikiamų paslaugų apimtį, kad paslaugomis galėtų naudotis kuo didesnis galutinių vartotojų skaičius. Apribojus paslaugų apimtį taip pat visiškai panaikinama galimybė naudotis bet kuriomis Programinės įrangos ir Duomenų trynimo funkcijomis bei su kuria nors iš Programinės įrangos funkcijų susijusia informacija, kuri saugoma Tiekėjo ar trečiųjų šalių serveriuose.

g) Jūs sutinkate neatlikti jokių veiksmų naudodamiesi licencijos raktu, kurie prieštarautų šios Sutarties sąlygoms

arba suteiktų Licencijos raktą asmeniui, kuris neturi teisės naudotis programine įranga, pvz., naudotos arba nenaudotos Licencijos rakto perdavimas bet kokia forma, taip pat neteisėtas atkūrimas, dubliuotų arba sugeneruotų licencijos raktų platinimas, arba programinės įrangos naudojimas pritaikius ne iš Teikėjo gautą licencijos raktą.

7. **Autorių teisės**. Programinė įranga ir visos teisės be apribojimų, įskaitant nuosavybės teises ir intelektinės nuosavybės teises, priklauso ESET ir (arba) jos licencijų išdavėjams. Jas gina tarptautinių susitarimų nuostatos ir visi kiti šalies, kurioje Programinė įranga yra naudojama, galiojantys nacionaliniai įstatymai. Programinės įrangos struktūra, organizacija ir kodas yra vertingos prekybos paslaptys ir konfidenciali ESET ir (arba) jos licencijos išdavėjų informacija. Draudžiama daryti Programinės įrangos kopijas, išskyrus 6 straipsnio a dalyje numatytus atvejus. Visoms kopijoms, kurias Jūs galite pasidaryti remdamasis šia Sutartimi, galioja tos pačios autorių teisės ir kiti nuosavybės reikalavimai, nurodyti ant Programinės įrangos. Jei Jūs pažeisdami Sutartį pakeisite duomenis, perdarysite ar išardysite Programinę įrangą ar kitais būdais pabandysite nustatyti pradinį Programinės įrangos kodą, sutinkate tokiu būdu gautą informaciją automatiškai ir neatšaukiamai perduoti vien tik Tiekėjo nuosavybėn nuo to momento, kai tokia informacija atsiranda, nepaisant Tiekėjo teisių, susijusių su Sutarties pažeidimu.

8. **Teisių išlaikymas**. Teikėjas išlaiko visas teises į Programinę įrangą, išskyrus pagal Sutarties sąlygas Jums kaip Programinės įrangos Galutiniam vartotojui aiškiai suteiktas teises.

9. **Versijos keliomis kalbomis, sudvejintos laikmenos su programine įranga, keli kopijų egzemplioriai**. Tuo atveju, kai Programinė įranga palaiko kelias platformas ar kalbas arba jei Jūs gavote kelis Programinės įrangos kopijos egzempliorius, kompiuterinių sistemų, kuriose turite teisę naudoti Programinę įrangą ir Jūsų įsigytas versijas, skaičius priklauso nuo įsigytų Licencijų skaičiaus. Draudžiama Jūsų nenaudojamas Programinės įrangos versijas ar kopijas parduoti, nuomoti, sublicencijuoti, skolinti ar perduoti.

10. **Sutarties įsigaliojimas ir nutraukimas.** Sutartis įsigalioja nuo tos dienos, kai sutinkate su Sutarties sąlygomis. Sutartį bet kada galite nutraukti visam laikui savo sąskaita pašalindami, sunaikindami ar grąžindami Programinę įrangą, visas atsargines kopijas ir susijusią medžiagą, pateiktą Tiekėjo ar jo verslo partnerių. Jūsų teisei naudotis Programine įranga ir bet kuria jos funkcija gali būti taikoma EOL politika. Jūsų teisė naudotis Programine įranga pasibaigs po to, kai Programinė įranga ar bet kuri jos funkcija pasieks gyvavimo ciklo pabaigos datą, kaip apibrėžta EOL politikoje. Nepriklausomai nuo Sutarties nutraukimo būdo, 7, 8, 11, 13, 19 ir 21 straipsnių nuostatos toliau galioja neribotą laiką.

11. **GALUTINIO VARTOTOJO PAREIŠKIMAI**. BŪDAMAS GALUTINIU VARTOTOJU JŪS PATVIRTINATE, KAD PROGRAMINĖ ĮRANGA YRA „PATEIKTA TOKIA, KOKIA YRA“, BE JOKIOS GARANTIJOS, TIKSLIAI APIBRĖŽTOS ARBA NUMANOMOS, PAGAL GALIOJANČIUS ĮSTATYMUS. NEI TIEKĖJAS, JO LICENCIJOS IŠDAVĖJAI AR ANTRINĖS BENDROVĖS, NEI AUTORIŲ TEISIŲ SAVININKAI NEPATEIKIA JOKIŲ PASTABŲ AR NESUTEIKIA GARANTIJŲ, TIKSLIAI APIBRĖŽTŲ ARBA NUMANOMŲ, ĮSKAITANT GARANTIJAS DĖL PERKAMUMO AR TINKAMUMO TAM TIKRAM TIKSLUI ARBA, KAD PROGRAMINĖ ĮRANGA NEPAŽEIS JOKIŲ TREČIŲJŲ ASMENŲ PATENTŲ, AUTORIŲ TEISIŲ, PREKIŲ ŽENKLŲ AR KITŲ TEISIŲ, BET TUO NEAPSIRIBOJANT. NEI TIEKĖJAS, NEI JOKIA KITA ŠALIS NESUTEIKIA GARANTIJOS, KAD PROGRAMINĖS ĮRANGOS FUNKCIJOS ATITIKS VARTOTOJO REIKALAVIMUS ARBA, KAD PROGRAMINĖ ĮRANGA VEIKS NEPERTRAUKIAMAI, AR BE JOKIŲ KLAIDŲ. PASIRINKDAMI PROGRAMINĘ ĮRANGĄ PRISIIMATE VISĄ ATSAKOMYBĘ IR RIZIKĄ, TAIP PAT ATSAKOMYBĘ DĖL PROGRAMINĖS ĮRANGOS ĮDIEGIMO, NAUDOJIMO IR REZULTATŲ, PASIEKTŲ NAUDOJANT PROGRAMINĘ ĮRANGĄ.

12. **Kitų įsipareigojimų nėra**. Sutartis nenumato kitų Teikėjo ir jo licencijų išdavėjų įsipareigojimų, išskyrus šiame dokumente konkrečiai numatytus įsipareigojimus.

13. **ATSAKOMYBĖS APRIBOJIMAS**. ATSIŽVELGDAMAS Į GALIOJANČIUS ĮSTATYMUS, GAMINTOJAS, JO DARBUOTOJAI AR LICENCIJŲ IŠDAVĖJAI JOKIU ATVEJU NĖRA ATSAKINGI DĖL PRARASTO PELNO, PAJAMŲ, PARDAVIMO, DUOMENŲ AR PIRKIMO KAINŲ, TURTO NUOSTOLIŲ, ASMENINIŲ SUSIŽEIDIMŲ, VERSLO TRUKDŽIŲ, VERSLO INFORMACIJOS NUTEKĖJIMO AR DĖL JOKIŲ SPECIALIŲ, TIESIOGINIŲ, NETIESIOGINIŲ, ATSITIKTINIŲ,

EKONOMINIŲ, DRAUDIMO, TEISMO PRITEISTŲ, YPATINGŲ NUOSTOLIŲ, KAIP NORS KILUSIŲ AR KYLANČIŲ DĖL SUTARTIES, CIVILINĖS TEISĖS PAŽEIDIMŲ, NEAPDAIRUMO AR KITŲ ATSAKOMYBĖS ATVEJŲ, KYLANČIŲ DĖL PROGRAMINĖS ĮRANGOS ĮDIEGIMO, NAUDOJIMO AR NEGALĖJIMO NAUDOTIS JA, NET JEI GAMINTOJUI YRA ŽINOMA GALIMYBĖ PATIRTI TOKIĄ ŽALĄ. KADANGI KAI KURIOSE ŠALYSE IR JURISDIKCIJOSE DRAUDŽIAMA IŠSKIRTI TAM TIKRĄ ATSAKOMYBĘ, TAČIAU LEIDŽIAMAS ATSAKOMYBĖS APRIBOJIMAS, TEIKĖJO, JO DARBUOTOJŲ, LICENCIJŲ IŠDAVĖJŲ AR ANTRINIŲ ĮMONIŲ ATSAKOMYBĖ APSIRIBOJA MOKESČIO UŽ LICENCIJĄ SUMA.

14. Šios Sutarties nuostatos neapriboja bet kuriai šaliai, veikiančiai kaip vartotojui, įstatymais suteiktų teisių, jei jos prieštarauja čia pateiktoms.

15. **Techninė pagalba**. ESET ar ESET įgaliotosios trečiosios šalys techninę pagalbą teikia savo nuožiūra, nesuteikdamos jokių garantijų ar pareiškimų. Jokie techninė pagalba nebus teikiama po to, kai Programinė įranga ar bet kuri jos funkcija pasieks gyvavimo ciklo pabaigos datą, kaip apibrėžta EOL politikoje. Prieš suteikiant techninę pagalbą Galutinis vartotojas privalo pasigaminti turimų duomenų, programinės įrangos ir programų atsargines kopijas. ESET ir (arba) ESET įgaliotosios šalys neprisiima atsakomybės už žalą ar prarastus duomenis, turtą, programinę įrangą ar aparatinę įrangą, ar dėl techninės pagalbos prarastą pelną. ESET ir (arba) ESET įgaliotosios šalys pasilieka teisę nuspręsti, ar problemos pašalinimui gali būti teikiama techninė pagalba. ESET pasilieka teisę savo nuožiūra atsisakyti suteikti techninę pagalbą, laikinai ją sustabdyti ar nutraukti. Vadovaujantis Privatumo politika, licencijos informacija, informacija ir kiti duomenys gali būti reikalingi teikiant techninio palaikymo pagalbą.

16. **Licencijos perdavimas**. Programinę įrangą galima perkelti iš vienos kompiuterinės sistemos į kitą, jei tai neprieštarauja Sutarties sąlygoms. Jei tai neprieštarauja Sutarties sąlygoms, tik gavęs Tiekėjo sutikimą Galutinis naudotojas turės teisę visam laikui perduoti Licenciją ir visas iš šios Sutarties kylančias teises kitam Galutiniam naudotojui, su sąlyga, kad (i) pradinis Galutinis naudotojas nepasiliko Programinės įrangos kopijų; (ii) teisių perdavimas vykdomas tiesiogiai, t. y. pradinis Galutinis naudotojas jas perduoda naujajam Galutiniam naudotojui; (iii) naujasis Galutinis naudotojas prisiims visas teises ir įsipareigojimus, pagal Sutartį priklausančius pradiniam Galutiniam naudotojui; (iv) pradinis Galutinis naudotojas pateiks naujajam Galutiniam naudotojui dokumentus, leidžiančius įsitikinti 17 straipsnyje nurodytos Programinės įrangos autentiškumu.

17. **Programinės įrangos autentiškumo patikrinimas.** Galutinis vartotojas teisę naudotis Programine įranga gali įrodyti vienu iš toliau pateikiamų būdų: (i) pateikdamas Teikėjo ar Teikėjo paskirtos trečiosios šalies išduotą licencijos pažymėjimą; (ii) pateikdamas rašytinę licencijos sutartį, jei tokia sutartis buvo sudaryta; (iii) pateikdamas Teikėjo siųstą el. laišką, kuriame yra licencijavimo informacijos (naudotojo vardas ir slaptažodis). Pagal Privatumo politiką Licencijos informacija ir Galutinio vartotojo identifikavimo duomenys gali būti reikalingi patvirtinant Programinės įrangos autentiškumą.

18. **Licencijos išdavimas valstybės įstaigoms ir JAV vyriausybei**. Programinė įranga teikiama valstybės įstaigoms, įskaitant Jungtinių Amerikos Valstijų vyriausybę, taikant licencijavimo teises ir apribojimus, aprašytus šioje Sutartyje.

19. **Prekybos kontrolės reikalavimų laikymasis**.

a) Tiesiogiai ar netiesiogiai neeksportuosite, nereeksportuosite, neperleisite ar kitaip nesuteiksite programinės įrangos jokiam asmeniui, nenaudosite jos jokiais būdais ir nedalyvausite jokiuose veiksmuose, dėl kurių ESET arba jos kontroliuojančiosios bendrovės, jos patronuojamosios įmonės ir bet kurios jos kontroliuojančiosios bendrovės patronuojamosios įmonės, taip pat jos kontroliuojančiųjų bendrovių kontroliuojami subjektai (filialai) gali pažeisti prekybos kontrolės įstatymus arba patirti dėl jų neigiamų pasekmių, įskaitant:

i. bet kokius įstatymus, kuriais kontroliuojami, ribojami arba nustatomi licencijų išdavimo reikalavimai prekių, programinės įrangos, technologijų ar paslaugų eksportui, reeksportui ar perdavimui, kuriuos išduoda arba priima bet kuri Jungtinių Amerikos Valstijų, Singapūro, Jungtinės Karalystės, Europos Sąjungos ar bet kurios jos valstybės narės vyriausybė, valstija ar reguliavimo institucija ar bet kuri šalis, kurioje turi būti vykdomi įsipareigojimai pagal

Susitarimą arba kurioje ESET ar bet kuris jos filialas yra įregistruoti arba veikia, ir

ii. bet kokią ekonominę, finansinę, prekybos ar kitą sankciją, apribojimą, embargą, importo ar eksporto draudimą, draudimą pervesti lėšas ar turtą arba teikti paslaugas, taip pat lygiavertę priemonę, kurią nustato bet kuri Jungtinių Amerikos Valstijų, Singapūro, Jungtinės Karalystės, Europos Sąjungos ar bet kurios jos valstybės narės vyriausybė, valstija ar reguliavimo institucija ar bet kuri šalis, kurioje turi būti vykdomi įsipareigojimai pagal Susitarimą arba kurioje ESET ar bet kuris jos filialas yra įregistruoti arba veikia.

(i ir ii punktuose nurodyti teisės aktai kartu vadinami Prekybos kontrolės įstatymais).

b) ESET turi teisę nedelsdama sustabdyti savo įsipareigojimus pagal šias sąlygas arba nutraukti sąlygų galiojimą, jei:

i. ESET nustato, kad, jos pagrįsta nuomone, naudotojas pažeidė arba gali pažeisti Susitarimo 19 straipsnio a dalį, arba

ii. galutiniam naudotojui ir (arba) programinei įrangai taikomi prekybos kontrolės įstatymai, todėl ESET nustato, kad, jos pagrįsta nuomone, dėl nuolatinių įsipareigojimų pagal Susitarimą vykdymo ESET arba jos filialai gali pažeisti prekybos kontrolės įstatymus arba patirti dėl jų neigiamų pasekmių.

c) Susitarime nėra numatyta ir jo nuostatos neturėtų būti aiškinamos ar vertinamos taip, kad kuri nors šalis būtų skatinama ar verčiama imtis veiksmų arba nuo jų susilaikyti (arba sutikti imtis veiksmų arba nuo jų susilaikyti) tokiu būdu, kuris prieštarauja galiojantiems prekybos kontrolės įstatymams, už kurį yra baudžiama arba kuris yra draudžiamas.

20. **Pranešimai**. Visi pranešimai turi būti siunčiami, o Programinė įranga ir Dokumentai grąžinami adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, nepažeidžiant ESET teisės pranešti jums apie bet kokius šios Sutarties, Privatumo politikos, EOL politikos ir Dokumentų pakeitimus pagal Sutarties 22 straipsnį. ESET gali siųsti jums el. laiškus ir pranešimus programoje per jūsų Programinę įrangą arba paskelbti pranešimą mūsų svetainėje. Jūs sutinkate elektroninėmis priemonėmis gauti ESET teisinius pranešimus, įskaitant bet kokius pranešimus apie Sąlygų, Specialiųjų sąlygų ar Privatumo politikos pakeitimus, bet kokį sutarties pasiūlymą / priėmimą ar kvietimus tvarkyti, pranešimus ar kitus teisinius pranešimus. Toks bendravimas elektroninėmis priemonėmis laikomas raštišku, išskyrus atvejus, kai pagal galiojančius įstatymus konkrečiai reikalaujama kitokios bendravimo formos.

21. **Taikomi teisės aktai**. Ši sutartis sudaryta pagal Slovakijos Respublikos įstatymus. Galutinis vartotojas ir Tiekėjas sutinka, kad jai netaikomi teisių konflikto principai ir Jungtinių Tautų konvencija dėl tarptautinio prekių pirkimo-pardavimo sutarčių. Jus sutinkate, kad visi ginčai ar pretenzijos, kylantys iš šios Sutarties ir susiję su Tiekėju, ar visi ginčai ar pretenzijos, susijusios su Programinės įrangos naudojimu, yra sprendžiami Bratislavos I apygardos teisme, ir Jūs aiškiai sutinkate su šio teismo jurisdikcija.

22. **Bendrosios nuostatos**. Jei kuri nors Sutarties nuostata pasirodys negaliojanti ir negalinti būti ieškinio pagrindas, ji nepaveiks bendro kitų Sutarties nuostatų teisėtumo, o Sutartis galios toliau ir bus vykdoma remiantis Sutartyje numatytomis sąlygomis. Ši Sutartis sudaryta anglų kalba. Jei patogumo ar kitais tikslais buvo parengtas šios Sutarties vertimas ir jei Sutarties kalbos versijos skiriasi, pirmenybė teikiama versijai anglų kalba.

ESET pasilieka teisę keisti Programinę įrangą, taip pat bet kuriuo metu peržiūrėti šią Sutartį, jos Priedus, Priedėlius, Privatumo politiką, EOL politiką ir Dokumentus arba jų dalį, atnaujindama atitinkamą dokumentą, i) kad būtų atsižvelgta į Programinės įrangos pakeitimus arba į tai, kaip ESET vykdo veiklą, ii) dėl teisinių, reguliavimo ar saugumo priežasčių arba iii) siekiant užkirsti kelią piktnaudžiavimui ar žalai. Apie bet kokią Sutarties peržiūrą jums bus pranešta el. paštu, pranešimu programoje ar kitomis elektroninėmis priemonėmis. Jei nesutinkate su siūlomais Sutarties pakeitimais, per 30 dienų nuo pranešimo apie pakeitimus gavimo galite ją nutraukti pagal 10 straipsnį. Jei per šį laikotarpį Sutarties nenutrauksite, siūlomi pakeitimai bus laikomi priimtais ir įsigalios jums

nuo tos dienos, kai gausite pranešimą apie pakeitimą.

Tai yra visa Teikėjo ir Jūsų sudaryta Sutartis dėl Programinės įrangos; ji panaikina visus su Programine įranga susijusius ankstesnius teiginius, pokalbius, įsipareigojimus, pranešimus ar reklaminius teiginius.

EULAID: EULA-PRODUCT-LG; 3537.0

Privatumo politika

„ESET, spol. s ro“, kurios registruota buveinė yra Einsteinova 24, 851 01 Bratislava, Slovakijos Respublika, užregistruota prekybos registre, kurį administruoja Bratislava I apygardos teismas, Sro skyrius, įrašo Nr. 3586/B, įmonės registracijos numeris: 31333532, kaip duomenų valdytojas (toliau – „ESET“ arba „mes“), norėtų skaidriai tvarkyti asmens duomenis ir rūpintis savo klientų privatumu. Šią Privatumo politiką skelbiame tam, kad pasiektume šį tikslą ir informuotume savo klientą (toliau – „galutinis naudotojas“ arba „jūs“) toliau nurodytomis temomis:

- asmens duomenų tvarkymas,
- duomenų konfidencialumas,
- duomenų subjekto teisės.

Asmens duomenų tvarkymas

ESET paslaugos, įdiegtos mūsų gaminyje, yra teikiamos pagal galutinio naudotojo licencijos sutarties (toliau – „GNLS“) sąlygas, tačiau kai kurioms iš jų gali reikėti ypatingo dėmesio. Norėtume suteikti jums daugiau informacijos apie duomenų rinkimą, susijusį su mūsų teikiamomis paslaugomis. Mes teikiame įvairias paslaugas, aprašytas GNLS ir produkto dokumentacijoje, pvz., naujinimo / naujovinimo paslaugą, „ESET LiveGrid®“, apsaugą nuo netinkamo duomenų panaudojimo, pagalbą ir t. t. Kad visos jos veiktų, turime rinkti arba turėti prieigą prie šios informacijos:

- Naujinimo ir kitą statistiką apžvelgianti informacija, susijusi su diegimo procesu ir jūsų kompiuteriu, įskaitant platformą, kurioje įdiegtas jūsų produktas, ir informacija apie mūsų gaminių operacijas ir funkcijas, pvz., operacinė sistema, aparatūros informacija, diegimo ID, licencijų ID, IP adresas, MAC adresas, produkto konfigūracijos nustatymai.
- Vienakrypčiai maišos ženklai, susiję su įsiskverbimu dėl reputacija grindžiamos sistemos „ESET LiveGrid®“, kuri didina mūsų apsaugos nuo kenkėjiškos programinės įrangos sprendimų efektyvumą, palygindama nuskaitytus failus su debesyje laikomų baltojo ir juodojo sąrašų elementais.
- Įtartini pavyzdžiai ir metaduomenys iš nevaldomo aplinkos yra reputacija grindžiamos sistemos „ESET LiveGrid®“ dalis, kuri suteikia ESET galimybę nedelsiant reaguoti į mūsų galutinių naudotojų poreikius ir į naujausias grėsmes. Mums būtini jūsų
  - įsiskverbimai, pvz., galimų virusų ir kitų kenkėjiškų programų pavyzdžiai bei kiti įtartini, problemiški, galimai nepageidaujami ir galimai nesaugūs objektai, pvz., vykdomieji failai, el. laiškai, kuriuos jūs arba mūsų produktas laiko brukalu;
  - informacija apie įrenginius vietiniame tinkle, pvz., įrenginio tipas, gamintojas, modelis ir (arba) įrenginio pavadinimas;
  - informacija, susijusi su interneto naudojimu, pvz., IP adresas ir geografinė informacija, IP paketai, URL ir interneto kadrai;

- strigčių atminties failai ir jų informacija.

Mes nenorime rinkti jokių kitų jūsų duomenų, tačiau kartais to išvengti neįmanoma. Atsitiktinai surinkti duomenys gali būti įtraukti į pačią kenkėjišką programinę įrangą (surinktą be jūsų žinios arba pritarimo) arba į jos failo pavadinimą arba URL, todėl mes nesiekiame, kad jie būtų mūsų sistemose arba tvarkyti jų šioje privatumo politikoje nurodytu tikslu.

- Licencijavimo informacija, pvz., licencijos ID ir asmeniniai duomenys, pvz., vardas, pavardė, adresas, el. pašto adresas, būtina atsikaitymui, licencijos autentiškumo patikrai ir mūsų paslaugų teikimui.
- Palaikymo paslaugai teikti gali reikėti kontaktinės informacijos ir jūsų palaikymo užklausų duomenų. Remdamiesi jūsų pasirinktu susisiekimo su mumis kanalu, galime rinkti jūsų el. pašto adresą, telefono numerį, licencijos informaciją, produkto informaciją ir jūsų palaikymo atvejo aprašymą. Kad būtų lengviau teikti palaikymo paslaugą, galite būti paprašyti pateikti kitą informaciją.

Duomenų konfidencialumas

ESET yra įmonė, veikianti visame pasaulyje per susijusius subjektus ar partnerius, kurie priklauso mūsų platinimo, paslaugų ir palaikymo tinklui. ESET tvarkoma informacija gali būti perduodama susijusiems subjektams ar partneriams arba perduodama jų, kad būtų galima vykdyti GNLS, pvz., teikti paslaugas ar palaikymą arba pateikti sąskaitas. Remiantis jūsų buvimo vieta ir paslauga, kurią pasirinkote naudoti, mums gali tekti perduoti jūsų duomenis į šalį, dėl kurios nėra priimtas Europos Komisijos sprendimas dėl tinkamumo. Net ir šiuo atveju kiekvienas informacijos perdavimas yra reglamentuojamas duomenų apsaugos teisės aktų ir vykdomas tik prireikus. Standartinės sutarčių sąlygos, įmonei privalomos taisyklės arba kita tinkama apsauga turi būti taikoma be jokių išimčių.

Visomis išgalėmis stengiamės nesaugoti duomenų ilgiau nei būtina, teikdami paslaugas pagal GNLS. Saugojimo laikotarpis gali būti ilgesnis nei licencijos galiojimas, vien tam, kad galėtumėte lengvai ir patogiai atnaujinti. Be to statistiniams tikslams gali būti apdorojami minimizuoti ir pseudonimizuoti statistiniai ir kiti duomenys iš jūsų „ESET LiveGrid®“.

ESET įgyvendina tinkamas technines ir organizacines priemones, užtikrinančias galimą riziką atitinkantį saugumo lygį. Stengiamės užtikrinti apdorojimo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą. Tačiau jei duomenų saugumo pažeidimas kelia pavojų jūsų teisėms ir laisvėms, esame pasirengę pranešti priežiūros institucijai ir duomenų subjektams. Kaip duomenų subjektas, turite teisę pateikti skundą priežiūros institucijai.

Duomenų subjekto teisės

ESET taikomi Slovakijos įstatymai, ir, kadangi priklausome Europos Sąjungai, esame saistomi jos duomenų apsaugos teisės aktų. Laikantis taikytinų duomenų apsaugos įstatymų nustatytų sąlygų, jūs, kaip duomenų subjektas, turite šias teises:

- teisę reikalauti ESET leisti susipažinti su savo asmens duomenimis,
- teisę į asmens duomenų ištaisymą, jei jie yra netikslūs (jūs taip pat turite teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys),
- teisę reikalauti ištrinti savo asmens duomenis,
- teisę reikalauti apriboti asmens duomenų tvarkymą,
- teisę nesutikti su tvarkymu,

- teisę pateikti skundą ir,
- teisę į duomenų perkeliamumą.

Manome, kad visa mūsų tvarkoma informacija yra vertinga ir reikalinga mūsų teisėto intereso, t. y. paslaugų teikimo ir produktų tiekimo mūsų klientams, tikslais.

Jei norėtumėte pasinaudoti savo, kaip duomenų subjekto, teise arba jei turite klausimų ar problemų, atsiųskite mums pranešimą šiuo adresu:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk