

ESET Endpoint Security for macOS

Käyttöopas

[Napsauta tätä jos haluat nähdä tämän asiakirjan online-version](#)

Copyright ©2023, ESET, spol. s r.o.

ESET Endpoint Security for macOS -tuotteen on kehittänyt ESET, spol. s r.o.

Lisätietoja on osoitteessa <https://www.eset.com>.

Kaikki oikeudet pidätetään. Mitään tämän dokumentaation osaa ei saa kopioida, tallentaa hakujärjestelmään eikä lähettää missään muodossa tai millään tavalla sähköisesti, mekaanisesti, valokopioimalla, tallentamalla, skannaamalla tai muulla tavoin ilman tekijän kirjallista lupaa.

ESET, spol. s r.o. pidättää oikeuden muuttaa mitä tahansa edellä kuvattuja sovellusohjelmistoja ilman erillistä ilmoitusta.

Tekninen tuki: <https://support.eset.com>

REV. 17.3.2023

1 ESET Endpoint Security for macOS	1
1.1 Version 6 uudet ominaisuudet	1
1.2 Järjestelmävaatimukset	2
2 Johdanto: ESET PROTECT	2
3 Johdanto: ESET PROTECT CLOUD	4
4 Etäasennus	4
4.1 Luo etäasennuspakkaus	6
5 Paikallinen asennus	9
5.1 Tyypillinen asennus	10
5.2 Mukautettu asennus	11
5.3 Järjestelmäajennusten salliminen paikallisesti	12
5.4 Levyn täysien käyttöoikeuksien salliminen paikallisesti	13
6 Tuoteaktivointi	14
7 Asennuksen poistaminen	15
8 Peruskatsaus	15
8.1 Pikanäppäimet	16
8.2 Järjestelmän toiminnan tarkistaminen	16
8.3 Mitä tehdä, jos ohjelma ei toimi oikein?	17
9 Tietokoneen suojaus	17
9.1 Virustentorjunta ja vakoiluohjelasuojaus	17
9.1 Yleiset	18
9.1 Poikkeukset	18
9.1 Käynnistyksen suojaus	19
9.1 Reaaliaikainen tiedostojärjestelmän suojaus	19
9.1 Lisäasetukset	19
9.1 Milloin reaaliaikaisen suojauksen asetuksia kannattaa muuttaa?	20
9.1 Reaaliaikaisen suojauksen tarkistaminen	20
9.1 Toimenpiteet reaaliaikaisen suojauksen toimintahäiriön ilmetessä	21
9.1 Tarvepohjainen tietokoneen tarkistus	21
9.1 Tarkistustyyppi	22
9.1 Smart Scan	22
9.1 Mukautettu tarkistus	22
9.1 Tarkistuskohdeet	23
9.1 Tarkistusprofiilit	23
9.1 ThreatSense-järjestelmän parametrien asetukset	24
9.1 Kohteet	25
9.1 Asetukset	25
9.1 Puhdistaminen	25
9.1 Poikkeukset	26
9.1 Rajat	26
9.1 Muut	27
9.1 Tunkeutumisen havaitseminen	27
9.2 Internet- ja sähköpostisuojaus	28
9.2 Internetin käytön suojaus	28
9.2 Portit	28
9.2 URL-osoiteluettelot	28
9.2 Sähköpostisuojaus	29
9.2 POP3-protokollan tarkistus	30
9.2 IMAP-protokollan tarkistus	30
9.3 Tietokalastelun esto	30

10	Palomuuuri	31
10.1	Suodatustilat	31
10.2	Palomuurisäännöt	32
10.2	Uusien sääntöjen luominen	33
10.3	Palomuurivyyöhykkeet	33
10.4	Palomuuriprofiilit	33
10.5	Palomuurilokit	33
11	Laittehallinta	34
11.1	Sääntöeditori	35
12	Internetin hallinta	36
13	Työkalut	38
13.1	Lokitiedostot	38
13.1	Lokin ylläpito	38
13.1	Lokisuodatus	39
13.2	Ajastin	40
13.2	Uusien tehtävien luominen	41
13.2	Käyttäjän määrittämisen tehtävän luominen	42
13.3	LiveGrid®	43
13.3	Epäilyttävät tiedostot	43
13.4	Karanteeni	44
13.4	Tiedostojen lisääminen karanteeniin	44
13.4	Karanteeniin asetetun tiedoston palauttaminen	44
13.4	Tiedoston lähettäminen karanteenista	45
13.5	Käyttöoikeudet	45
13.6	Esitystila	45
13.7	Käynnissä olevat prosessit	46
14	Käyttöliittymä	47
14.1	Hälytykset ja ilmoitukset	47
14.1	Hälytysten näyttäminen	48
14.1	Suojauksen tilat	48
14.2	Pikavalikko	48
15	Päivitys	49
15.1	Päivitysasetukset	49
15.1	Lisäasetukset	50
15.2	Päivitystehtävien luominen	51
15.3	Järjestelmän päivitykset	51
15.4	Asetusten tuonti ja vienti	52
15.5	Välityspalvelimen asetukset	53
15.6	Jaettu paikallinen välimuisti	53
16	Käyttöoikeussopimus	53
17	Privacy Policy	60

ESET Endpoint Security for macOS

ESET Endpoint Security for macOS 6 edustaa uutta lähestymistapaa integroituun tietokoneen suojaukseen. ThreatSense®-tarkistusmoduulin uusin versioja mukautettava palomuuuri tarjoaa nopeutta ja tarkkuutta ja pitää tietokoneesi turvattuna. Tuloksena on älykäs järjestelmä, joka suojaa tietokonetta hyökkäyksiltä ja haittaohjelmilta tauotta.

ESET Endpoint Security for macOS 6 on täydellinen tietoturvaratkaisu. Se on tulos pitkäaikaisista pyrkimyksistämme yhdistää maksimaalinen suojaus ja minimaalinen järjestelmän kuormitus. Tekoälyyn perustuvat älykkäät tekniikat ehkäisevät proaktiivisesti virusten, vakoiluohjelmien, troijalaisten, matojen, mainosohjelmien, rootkit-ohjelmien ja muiden Internet-pohjaisten hyökkäysten pääsyä koneeseen heikentämättä järjestelmän suorituskykyä tai häiritsemättä tietokoneen käyttöä.

Tämä tuote on suunniteltu ensisijaisesti pien-/suuryritysympäristöissä käytettäviin työasemiin. Sitä voidaan käyttää yhdessä ESET PROTECT -ratkaisun (aiemmin ESET Security Management Center) kanssa, asiakastyöasemia voidaan hallita vaivattomasti niiden määrästä riippumatta, käytäntöjä ja sääntöjä voidaan ottaa käyttöön, tunnistuksia voidaan valvoa ja mistä tahansa verkossa olevasta tietokoneesta voidaan hallita muutoksia etänä.

Version 6 uudet ominaisuudet

Tuotteen ESET Endpoint Security for macOS graafinen käyttöliittymä on suunniteltu kokonaan uudestaan, jotta näkyvyys olisi parempi ja käyttökokemus intuitiivisempi. Version 6 sisältämiä parannuksia ovat muun muassa:

- ESET Enterprise Inspector -tuki – Versiosta ESET Endpoint Security for macOS 6.9 alkaen ESET Endpoint Security for macOS on yhdistettävissä ESET Enterprise Inspector -ratkaisuun. ESET Enterprise Inspector (EEI) on kattava pääteipisteiden tunnistus- ja reagointijärjestelmä, johon sisältyy esimerkiksi seuraavat ominaisuudet: tapausten tunnistus, tapausten hallinta ja niihin reagointi, tietojen kerääminen, vaaratilanteista ilmaisevien asioiden tunnistus, poikkeavuuksien tunnistus, käyttäytymisen tunnistus ja käytäntörikkomukset. Lisätietoja ESET Enterprise Inspector -ratkaisusta, sen asennuksesta ja toiminnoista on [ESET Enterprise Inspector -ohjeessa](#).
- **64-bittisen arkkitehtuurin tuki**
- **Palomuuuri** – nyt voit luoda palomuurisääntöjä suoraan lokista tai IDS (Intrusion detection system)-ilmoitusikkunasta ja osoittaa profiileja verkkokäyttöliittymille.
- **Internetin hallinta** – estää verkkosivut, joilla voi olla asiatonta tai haitallista materiaalia.
- **Internetin käytön suojaus** – valvoo Web-selaimien ja etäpalvelinten välistä tietoliikennettä.
- **Sähköpostisuojaus** – sen avulla voit hallita POP3- ja IMAP-protokollien kautta vastaanotettavaa sähköpostiliikennettä.
- **Tietojenkalastelusuojaus** – suojaa sinua laillisiksi web-sivuiksi naamioituneiden pahantahtoisten web-sivujen yrityksiltä hankkia salasanoja, pankkitietoja ja muita arkaluontoisia tietoja.
- **Laitehallinta** – voit tarkistaa, estää tai säätää laajennettuja suodattimia ja/tai lupia ja määrittää käyttäjän oikeudet laitteen käytölle ja työskentelylle. Tämä ominaisuus on saatavana tuotteen versiossa 6.1 ja uudemmissa versioissa.

- **Esitystila** – voit suorittaa tuotteen ESET Endpoint Security for macOS taustalla ja piilottaa ponnahdusikkunat ja ajoitetut tehtävät.
- **Jaettu paikallinen välimuisti** – parantaa tarkistusnopeutta virtuaaliympäristöissä.

Järjestelmävaatimukset

Jotta ESET Endpoint Security for macOS toimisi optimaalisesti, järjestelmän tulee täyttää seuraavat laitteisto- ja ohjelmistovaatimukset:

	Järjestelmävaatimukset:
Suorittimen arkkitehtuuri	Intel 64-bit, Apple ARM 64-bittinen
Käyttöjärjestelmä	macOS 10.12 ja uudemmat
Muisti	300 Mt
Vapaa kiintolevytila	200 Mt



Intel-tuen lisäksi ESET Endpoint Security for macOS versio 6.10.900.0 ja uudemmat tukevat Apple ARM -sirua Rosetta 2:lla

Johdanto: ESET PROTECT

ESET PROTECT auttaa hallinnoimaan ESET-tuotteita verkkoympäristössä olevissa työasemissa, palvelimissa ja mobiililaitteissa yhdestä keskitetystä sijainnista.

ESET PROTECT [E](#)verkkokonsolin avulla voit ottaa käyttöön ESET-ratkaisuja, hallinnoida tehtäviä, pakottaa suojauskäytäntöjä, valvoa järjestelmän tilaa ja reagoida nopeasti etätietokoneissa ilmeneviin ongelmiin ja uhkiin. Katso myös [ESET PROTECT \[E\]\(#\)arkkitehtuurin ja \[E\]\(#\)infrastruktuurien osien yleiskuvaus](#), [ESET PROTECT \[E\]\(#\)verkkokonsolin käytön aloittaminen](#) ja [Tuetut työpöytäsovelluksen käyttöönottoympäristöt](#).

ESET PROTECT sisältää seuraavat osat:

- [ESET PROTECT-palvelin](#) – ESET PROTECT-palvelimen voi asentaa Windows- ja Linux-palvelimiin ja se on saatavilla myös virtuaalisena laitteena. Viestintä käsitellään agenttien avulla, ja sovellustiedot kerätään ja tallennetaan tietokantaan.
- [ESET PROTECT \[E\]\(#\)verkkokonsoli](#) – ESET PROTECT [E](#)verkkokonsoli toimii ensisijaisena liittymänä, jolla voi hallita ympäristöön kuuluvia asiakastietokoneita. Konsolissa on yleiskuvaus verkon asiakaskoneiden tiloista, ja voit sen avulla ottaa käyttöön ESET-ratkaisuja etäsijainnista tietokoneissa, joita ei ole hallinnoitu. Kun olet asentanut ESET PROTECT [E](#)palvelimen, voit käyttää verkkokonsolia selaimella. Jos määrität, että verkkopalvelin on käytettävissä Internetin kautta, ESET PROTECT on käytettävissä mistä tahansa tai millä tahansa laitteella, joka on muodostanut Internet-yhteyden.
- [ESET Management \[E\]\(#\)agentti](#) – ESET Management [E](#)agentti toimii ESET PROTECT [E](#)palvelimen ja asiakastietokoneiden välisenä viestintävälineenä. Agentti on asennettava asiakastietokoneeseen, jotta tietokoneen ja ESET PROTECT [E](#)palvelimen välillä voi olla tietoliikennettä. Koska se sijaitsee asiakastietokoneessa ja se voi tallentaa useita tietoturvaskenaarioita, ESET Management [E](#)agentti nopeuttaa

uusiin ughiin reagoimista huomattavasti. ESET PROTECT -verkkokonsolin avulla voit [ottaa ESET Management Agentin](#) käyttöön hallinnoimattomissa tietokoneissa, jotka Active Directoryn tai ESETin [RD-tunnistin](#) on tunnistanut. Voit myös tarvittaessa [asentaa ESET Management Agentin manuaalisesti](#) asiakastietokoneisiin.

- [Rogue Detection Sensor](#) – ESET PROTECT Rogue Detection (RD) Sensor tunnistaa verkossa olevat hallinnoimattomat tietokoneet ja lähettää niiden tiedot ESET PROTECT-palvelimeen. Tämän avulla voit lisätä uudet asiakastietokoneet vaivattomasti suojattuun verkkoon. RD-tunnistin muistaa havaitut tietokoneet, eikä lähetä samoja tietoja kahta kertaa.
- [Apache HTTP -välityspalvelin](#) – Tämä on palvelu, jota voidaan käyttää yhdessä ESET PROTECT -konsolin kanssa:

OJakamaan päivitykset asiakastietokoneisiin ja asennuspaketit ESET Management -agentille

OVälittämään tietoliikennettä ESET Management Agenttien ja ESET PROTECT -palvelimen välillä.

- [Mobile Device Connector](#) – Tämä on komponentti, jolla voidaan hallita mobiililaitteita, kuten Android- ja iOS-laitteita, ja ESET Endpoint Security for Android -palvelua ESET PROTECT -konsolissa.
- [ESET PROTECT Virtuaalinen laite](#) – Virtuaalinen ESET PROTECT-laite on tarkoitettu käyttäjille, jotka haluavat suorittaa ESET PROTECT -konsolin virtualisoidussa ympäristössä.
- [ESET PROTECT Virtual Agent Host](#) – Tämä on ESET PROTECT -komponentti, joka virtualisoi agenttikokonaisuuksia, jotta ilman agentteja toimivia virtuaalisia koneita voidaan hallita. Tämä ratkaisu mahdollistaa automaation, dynaamisten ryhmien käytön ja samantasoisien tehtävnhallinnan kuin ESET Management -agentti fyysisissä tietokoneissa. Virtuaalinen agentti kerää tietoja virtuaalisista koneista ja lähettää ne ESET PROTECT-palvelimeen.
- [Peilityökalu](#) – Peilityökalua tarvitaan offline-moduulien päivityksiin. Jos asiakastietokoneissa ei ole Internet-yhteyttä, peilityökalulla voi ladata päivitystiedostoja ESET-päivityspalvelimista ja tallentaa niitä paikallisesti.
- [ESET Remote Deployment Tool](#) – Tämä työkalu käyttää kaikenkattavia paketteja, jotka on luotu <%PRODUCT%>-verkkokonsolissa. Se on kätevä tapa jakaa ESET Management -agentti ESET-tuotteen mukana verkossa olevissa tietokoneissa.
- [ESET Business Account](#) – Uusi ESET-yritystuotteiden käyttöoikeusportaali mahdollistaa käyttöoikeuksien hallinnan. Tuotteen aktivointiohjeet ovat tämän asiakirjan [ESET Business Account](#)-osiossa, ja ESET Business Account-[käyttöoppaassa](#) on lisätietoja ESET Business Account:n käytöstä. Jos sinulla on jo ESETin antama käyttäjänimi ja salasana, jotka haluat muuntaa käyttöoikeusavaimeksi, lisätietoja on [vanhojen käyttöoikeustietojen muuntamista](#) käsittelevässä osiossa.
- [ESET Enterprise Inspector](#) – Kattava päätepisteiden tunnistus- ja reagointijärjestelmä, johon sisältyy esimerkiksi seuraavat ominaisuudet: tapausten tunnistus, tapausten hallinta ja niihin reagointi, tietojen kerääminen, vaaratilanteista ilmaisevien asioiden tunnistus, poikkeavuuksien tunnistus, käyttäytymisen tunnistus ja käytäntörikkomukset.

ESET PROTECT -verkkokonsolin avulla voit ottaa käyttöön ESET-ratkaisuja, hallinnoida tehtäviä, pakottaa suojauskäytäntöjä, valvoa järjestelmän tilaa ja reagoida nopeasti etätietokoneissa ilmeneviin ongelmiin ja ughiin.

i Lisätietoja on [ESET PROTECTin online-käyttöoppaassa](#).

Johdanto: ESET PROTECT CLOUD

ESET PROTECT CLOUD -ratkaisulla voit hallita työasemissa ja palvelimissa olevia ESET-tuotteita verkkoympäristössä yhdestä keskitetystä sijainnista käyttämättä fyysistä tai virtuaalista palvelinta (kuten ESET PROTECT tai ESET Security Management Center). ESET PROTECT CLOUD-verkkokonsolin avulla voit ottaa käyttöön ESET-ratkaisuja, hallinnoida tehtäviä, varmistua tietoturvakäytäntöjen noudattamisesta, valvoa järjestelmän tilaa ja reagoida nopeasti etätietokoneissa ilmeneviin ongelmiin ja uhkiin.

- [Lisätietoja tästä on ESET PROTECT CLOUDin Online-käyttöoppaassa](#)

Etäasennus

Toimet ennen asennusta

^ [macOS 10.15 ja vanhemmat](#)

Ennen kuin ESET Endpoint Security for macOS asennetaan macOS-versioon 10.13 tai uudempaan versioon, suosittelemme, että sallit ESET-ydinlaajennukset ja macOS-versiossa 10.14 ja uudemmissa myönnät lisäksi täydet levyn käyttöoikeudet kohdetietokoneisiin. Jos nämä oikeudet myönnetään vasta asennuksen jälkeen, käyttäjät saavat ilmoituksen **järjestelmälaajennusten estosta** ja **Tietokone on osittain suojattu** -ilmoituksen, kunnes ESET-ydinlaajennukset on sallittu ja levyn täydet käyttöoikeudet myönnetty.

Jos haluat sallia ESET-ydinlaajennukset ja myöntää levyn käyttöoikeuden etäsijainnista, tietokoneesi on oltava rekisteröityneenä [mobiililaitteiden MDM-hallintapalvelimelle](#), kuten Jamf.

ESET-järjestelmälaajennusten salliminen

Voit sallia ydinlaajennukset laitteessasi etäsijainnista seuraavasti:

OJos MDM-ratkaisusi on Jamf, katso ohjeet [tietopankin artikkelista](#).

OJos käytät jotakin toista MDM-ratkaisua, [lataa .plist-kokoonpanoprofiili](#). Luo kaksi UUID-tunnistetta haluamallasi UUID-editorilla ja korvaa tekstieditorissa ladatun kokoonpanoprofiilin tekstikohdat `insert your UUID 1 here` ja `insert your UUID 2 here` luoduilla tunnuksilla. Ota .plist-kokoonpanoprofiilitiedosto käyttöön MDM-palvelinta käyttämällä. Tietokoneesi on oltava rekisteröitynä MDM-palvelimeen, jotta voit ottaa kokoonpanoprofiilit käyttöön näissä tietokoneissa.

Levyn täysien käyttöoikeuksien salliminen

MacOS-käyttöjärjestelmän versiossa 10.14 saat ilmoituksen **Tietokone on osittain suojattu** tuotteelta ESET Endpoint Security for macOS asennuksen jälkeen. Jotta ESET Endpoint Security for macOS ja kaikki sen toiminnot toimisivat täysin, ESET Endpoint Security for macOS tarvitsee **täydet levyn käyttöoikeudet** ennen tuotteen asennusta. Voit sallia **täydet levyn käyttöoikeudet** etäsijainnista seuraavasti:

OJos MDM-ratkaisusi on Jamf, katso ohjeet [tietopankin artikkelista](#).

OVoit sallia **täydet levyn käyttöoikeudet** etätoimilla [lataamalla .plist-kokoonpanotiedoston](#). Luo kaksi UUID-tunnistetta haluamallasi UUID-editorilla ja korvaa tekstieditorissa ladatun kokoonpanoprofiilin tekstikohdat `insert your UUID 1 here` ja `insert your UUID 2 here` luoduilla tunnuksilla. Ota .plist-

kokoonpanoprofiilitiedosto käyttöön MDM-palvelinta käyttämällä. Tietokoneesi on oltava rekisteröitynä MDM-palvelimeen, jotta voit ottaa kokoonpanoprofiilit käyttöön näissä tietokoneissa.

^ macOS Big Sur (11)

Ennen kuin ESET Endpoint Security for macOS asennetaan macOS Big Sur -versioon, sinun on sallittava ESET-järjestelmäajennukset ja täydet levyn käyttöoikeudet kohdetietokoneissa. Jos nämä oikeudet myönnetään vasta asennuksen jälkeen, käyttäjät saavat ilmoituksen **järjestelmäajennusten estosta** ja **Tietokone on osittain suojattu** -ilmoituksen, kunnes ESET-järjestelmäajennukset ja levyn täydet käyttöoikeudet on sallittu. Järjestelmäajennukset voi sallia etänä vain ennen tuotteen ESET Endpoint Security for macOS asennusta.

Jos haluat sallia ESET-järjestelmäajennukset ja myöntää levyn käyttöoikeuden etäsijainnista, tietokoneesi on oltava rekisteröityneenä [mobiililaitteiden MDM-hallintapalvelimelle](#), kuten Jamf.

ESET-järjestelmäajennusten salliminen

Voit sallia järjestelmäajennukset laitteessasi etäsijainnista seuraavasti:

OJos MDM-ratkaisusi on Jamf, katso ohjeet [tietopankin artikkelista](#).

OJos käytät jotakin toista MDM-ratkaisua, [lataa .plist-kokoonpanoprofiilitiedosto](#). Ota .plist-kokoonpanoprofiilitiedosto käyttöön MDM-palvelinta käyttämällä. Tietokoneesi on oltava rekisteröitynä MDM-palvelimeen, jotta voit ottaa kokoonpanoprofiilit käyttöön näissä tietokoneissa. Voit luoda oman kokoonpanoprofiilin seuraavilla asetuksilla:

Ryhmätunniste (TeamID)	P8DQRPVLP
Pakkaustunniste (BundleID)	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

Levyn täysien käyttöoikeuksien salliminen

Voit sallia **levyn täydet käyttöoikeudet** etäsijainnista seuraavasti:

OJos MDM-ratkaisusi on Jamf, katso ohjeet [tietopankin artikkelista](#).

OVoit sallia **täydet levyn käyttöoikeudet** etätoimilla [lataamalla .plist-kokoonpanotiedoston](#). Ota .plist-kokoonpanoprofiilitiedosto käyttöön MDM-palvelinta käyttämällä. Tietokoneesi on oltava rekisteröitynä MDM-palvelimeen, jotta voit ottaa kokoonpanoprofiilit käyttöön näissä tietokoneissa. Voit luoda oman kokoonpanoprofiilin seuraavilla asetuksilla:

ESET Endpoint Security	
Tunniste	com.eset.ees.6
Tunnisteen tyyppi	bundleID
Koodivaatimus	identifier "com.eset.ees.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRPVLP
Sovellus tai palvelu	SystemPolicyAllFiles
Käyttö	Allow

ESET Endpoint Antivirus ja ESET Endpoint Security	
Tunniste	com.eset.devices
Tunnisteen tyyppi	bundleID
Koodivaatimus	identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQXPVLP
Sovellus tai palvelu	SystemPolicyAllFiles
Käyttö	Allow

ESET Endpoint Antivirus ja ESET Endpoint Security	
Tunniste	com.eset.endpoint
Tunnisteen tyyppi	bundleID
Koodivaatimus	identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQXPVLP
Sovellus tai palvelu	SystemPolicyAllFiles
Käyttö	Allow

Asennus

Ennen asennusta voit luoda etäasennuspakkauksen, jossa on ESET Endpoint Security for macOS esimääritys, jonka voit myöhemmin ottaa käyttöön käyttämällä haluamaasi ESET PROTECT- tai MDM-tuotetta.

- [Luo etäasennuspakkaus.](#)

Asenna ESET Endpoint Security for macOS etäyhteyden kautta luomalla **ohjelmiston asennustehtävä** ESETin hallintajärjestelmän avulla:

- [Ohjelmiston asennus: ESET PROTECT](#)
- [Ohjelmiston asennus: ESET Security Management Center](#)

Asennuksen jälkeen

Käyttäjät saavat seuraavan ilmoituksen: "ESET Endpoint Security for macOS" haluaa suodattaa verkkosisältöä. Kun käyttäjät saavat tämän ilmoituksen, valitse **Salli**. Jos valitset **Älä salli**, internetin käytön suojaus ei toimi.

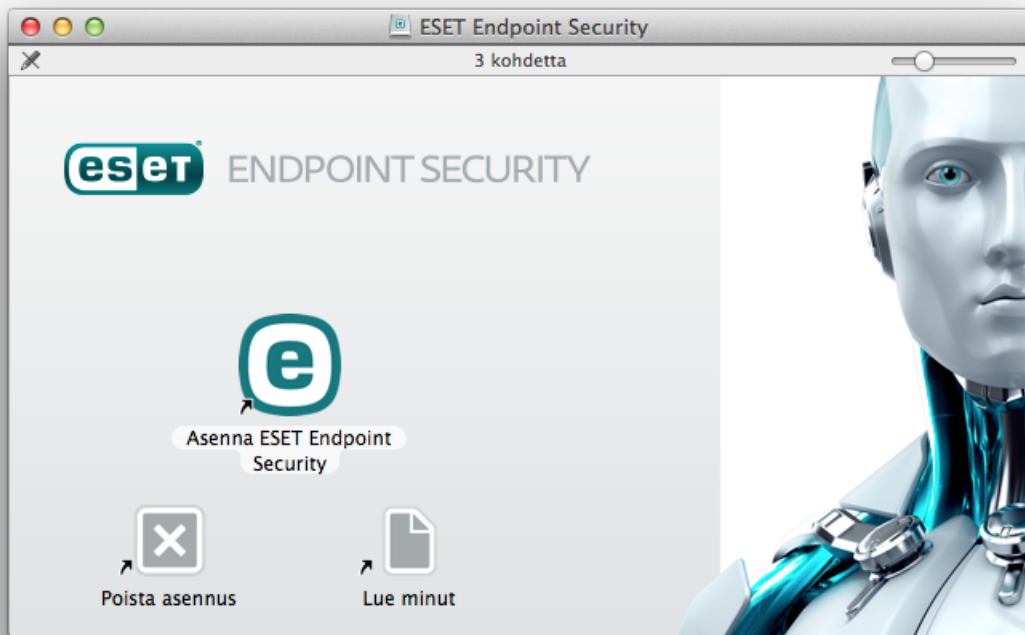
Luo etäasennuspakkaus

Asennuspakkauksen luominen Apple Remote Desktop -asennusta varten

1. Lataa vakioasennuspakkaus ESETin verkkosivustolta:

[ESET Endpoint Security for macOS](#)

2. Voit käynnistää tuotteen ESET Endpoint Security for macOS asennusohjelman kaksoisnapsauttamalla ladattua tiedostoa.



1. Valitse **Asenna**ESET Endpoint Security for macOS.
2. Kun saat kehoitteen, valtuuta **Salli**-komennolla asennusohjelma määrittämään, voiko ohjelmiston asentaa.
3. Valitse **Jatka**. Jos luot etäasennuspakkausta, ESET Endpoint Security for macOS ei tule asennetuksi.
4. Tarkista järjestelmävaatimukset ja valitse **Jatka**.
5. Lue ESETin käyttöoikeussopimus ja valitse **Jatka** → **Hyväksy**, jos hyväksyt sopimuksen.
6. Valitse **Asennustila**-vaiheessa **Etä**.
7. Valitse, mitkä tuotteen osat haluat asentaa. Kaikki osat valitaan oletusarvoisesti. Valitse **Jatka**.
8. Valitse **Välityspalvelin**-vaiheessa vaihtoehto, joka vastaa Internet-yhteyttäsi. Jos et ole varma, käytä järjestelmän oletusasetuksia. Valitse **Seuraava**. Jos käytät välityspalvelinta, seuraavassa vaiheessa sinua pyydetään antamaan välityspalvelimen osoite, käyttäjänimi ja salasana.
9. Valitse, kuka voi muokata ohjelman kokoonpanoa. Vain etuoikeutetut käyttäjät ja ryhmät voivat muuttaa sitä. Järjestelmänvalvojaryhmä valitaan oletusarvoisesti etuoikeutetuksi. Valitse **Näytä kaikki käyttäjät** tai **Näytä kaikki ryhmät** -valintaruutu, jos haluat näyttää kaikki virtuaaliset käyttäjät ja ryhmät, kuten ohjelmat ja prosessit.
10. Ota tarvittaessa käyttöön ESET LiveGrid kohdetietokoneessa.
11. Mahdollisesti ei-toivotun sovelluksen tunnistus kohdetietokoneessa, jos mahdollista.
12. Valitse palomuuritila:

Automaattinen tila – Oletustila. Tämä tila soveltuu käyttäjille, jotka suosivat vaivatonta tapaa käyttää palomuuria ilman sääntömäärityksiä. Automaattisessa tilassa sallitaan tietyn järjestelmän lähtevä vakioliikenne ja estetään kaikki verkon puolelta tulevat yhteydet, joita käyttäjä ei ole aloittanut. Voit myös lisätä mukautettuja, käyttäjän määrittämiä sääntöjä.

Vuorovaikutteinen tila – Voit muodostaa mukautettuja määrittämiä palomuuria varten. Kun tietoliikennettä havaitaan, eikä sille ole olemassa sääntöjä, näkyviin tulee valintaikkuna, joka ilmoittaa tuntemattomasta yhteydestä. Valintaikkunassa voidaan sallia tai estää tietoliikenne, ja päätös sallia tai estää tietoliikenne voidaan muistaa uutena palomuurin sääntönä. Jos päätät luoda uuden säännön, kaikki samantyyppiset tulevat yhteydet sallitaan tai estetään säännön mukaan.

13. Tallenna asennustiedosto tietokoneellesi. Jos olet aiemmin luonut asennustiedoston oletussijaintiin, sinun on muutettava kohdekansion sijaintia tai poistettava aiemmat tiedostot, ennen kuin voit jatkaa. Tämä viimeistelee etäasennuksen ensimmäisen vaiheen. Paikallinen asennusohjelma poistuu ja luo etäasennustiedostot valitsemaasi kohdekansioon.

Etäasennustiedostot ovat seuraavat:

- *esets_setup.dat* - Asennusohjelman asetusosiossa syöttämiäsi asennustietoja
- *program_components.dat* - Valittujen ohjelmakomponenttien asennustiedot. (Tämä tiedosto on valinnainen. Se luodaan, kun päätät olla asentamatta tiettyjä ESET Endpoint Security for macOS -komponentteja.)
- *esets_remote_install.pkg* - Etäasennuspakkaus
- *esets_remote_uninstall.sh* - Komentosarja asennuksen etäpoistoa varten

Asenna Apple Remote Desktop

1. Avaa Apple Remote Desktop ja muodosta yhteys kohdetietokoneeseen. Lisätietoja on [Apple Remote Desktop -ohjeissa](#).
2. Kopioi seuraavat tiedostot kohdetietokoneen */tmp*-kansioon käyttämällä **tiedoston tai kansion kopiointia** Apple Remote Desktopissa:

Jos asennat kaikki osat, kopioi:

- *esets_setup.dat*

Jos et asenna kaikkia tuotteen osia, kopioi:

- *esets_setup.dat*

- *product_components.dat*

3. Käytä **Asenna paketit** -komentoa ja asenna *esets_remote_install.pkg* kohdetietokoneeseen.

Poista Apple Remote Desktop -asennus etänä

1. Avaa Apple Remote Desktop ja muodosta yhteys kohdetietokoneeseen. Lisätietoja on [Apple Remote Desktop -ohjeissa](#).
2. Kopioi *esets_remote_uninstall.sh* -komentosarja Apple Remote Desktopin **tiedoston tai kansion kopiointitoiminnon** avulla kohdetietokoneen */tmp*-kansioon.

3. Lähetä Apple Remote Desktop -palvelussa seuraava komento **Lähetä UNIX-komento** -toiminnolla kohdetietokoneeseen:

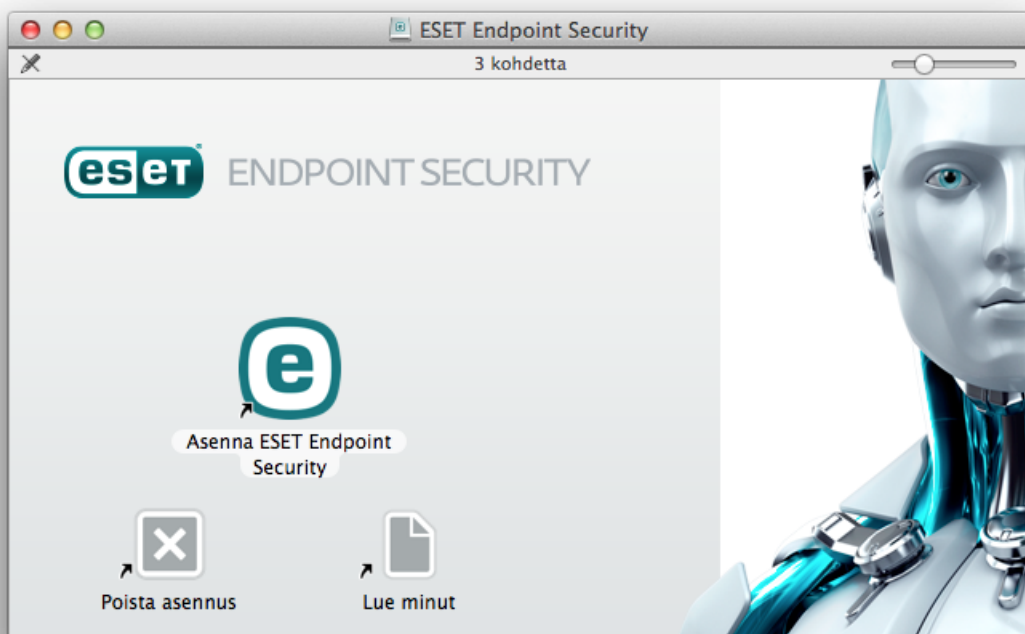
```
/tmp/esets_remote_uninstall.sh
```

Kun poistoprosessi on päättynyt, konsoli näkyy kohdetietokoneen Apple Remote Desktop -palvelussa.

Asennus

Ohjattu asennustoiminto opastaa perusasetusten tekemisessä. Lisätietoja on [asennusta koskevassa tietopankin artikkelissa](#).

1. Voit käynnistää tuotteen ESET Endpoint Security for macOS asennusohjelman kaksoisnapsauttamalla ladattua tiedostoa.



1. Aloita asennus valitsemalla **Asenna** ESET Endpoint Security for macOS.

Asentaminen .pkg-tiedostosta

! Kun ESET-tuotteet asennetaan macOS-käyttöjärjestelmään ja käynnistetään siinä, Mac-tietokoneessa on oltava internet-yhteys käytössä, jotta Apple voi vahvistaa ESET-järjestelmälaajennusten oikeudet.

2. Kun saat kehoitteen, valtuuta **Salli**-komennolla asennusohjelma määrittämään, voiko ohjelmiston asentaa.

3. Poista tietokoneesta kaikki aiemmin asennetut tietoturvasovellukset, kuten virustentorjunta, vakoiluohjelmasuojaus ja palomuuuri, jos et ole vielä tehnyt niin. Valitse **Jatka**, jos muita tietoturvasovelluksia ei ole asennettu.

4. Tarkista järjestelmävaatimukset ja valitse **Jatka**.
 5. Lue ESETin käyttöoikeussopimus ja valitse **Jatka** → **Hyväksy**, jos hyväksyt sopimuksen.
 6. Valitse asennustapa, jota haluat käyttää.
- [Tyypillinen asennus](#)
 - [Mukautettu asennus](#)
 - [Etäasennus](#)

i **Versiopäivitys**
Asennuksen alkuvaiheessa asennusohjelma tarkistaa uusimman tuoteversion verkosta automaattisesti. Jos uudempi versio löytyy, voit ladata uusimman version ennen asennusprosessin jatkamista.

Tyypillinen asennus

Tyypillinen asennustila sisältää kokoonpanoasetukset, jotka sopivat useimmille käyttäjille. Nämä asetukset suojaavat järjestelmää parhaalla mahdollisella tavalla ja ylläpitävät erinomaisen suorituskyvyn. Tyypillinen asennus on oletusasetus ja sitä suositellaan, jos tiettyjen asetusten edellyttämät vaatimukset eivät täyty.

1. Valitse **ESET LiveGrid** -ikkunassa haluamasi asetus ja valitse **Jatka**. Jos päätät myöhemmin, että haluat muuttaa tätä asetusta, voit tehdä niin **LiveGrid-asetuksissa**. Lisätietoja ESET LiveGrid -ratkaisusta on [sanastossa](#).
2. Valitse **Mahdollisesti ei-toivotut sovellukset** -ikkunassa haluamasi asetus (katso kohtaa [Mikä on mahdollisesti ei-toivottu sovellus?](#)) ja valitse **Jatka**. Jos päätät myöhemmin, että haluat muuttaa tätä asetusta, voit tehdä niin **lisäasetuksissa**.
3. Valitse **Asenna**. Jos saat kehoitteen antaa macOS-salasana, anna se ja valitse **Asenna ohjelmisto**.

Viimeistele tuotteen ESET Endpoint Security for macOS asennus seuraavasti:

macOS Big Sur (11)

1. [Järjestelmälaajennusten salliminen](#).
2. [Levyn täysien käyttöoikeuksien salliminen](#).
3. Salli ESETin lisätä välityspalvelinkokoonpanoja. Saat seuraavan ilmoituksen: "ESET Endpoint Security for macOS" haluaa suodattaa verkon sisältöä. Kun saat tämän ilmoituksen, valitse **Salli**. Jos valitset **Älä salli**, internetin käytön suojaus ei toimi.



[macOS 10.15 ja vanhemmat](#)

1. MacOS 10.13 ja sitä uudemmat versiot näyttävät **järjestelmälaajennuksen estosta** ilmoittavan viestin, minkä lisäksi ESET Endpoint Security for macOS näyttää **Tietokonettasi ei ole suojattu** -ilmoituksen. Kaikkien ESET Endpoint Security for macOS -toimintojen käyttöönotto edellyttää, että ydintunnisteet on sallittu laitteessa. Voit sallia ydintunnisteet laitteessa valitsemalla **Järjestelmäasetukset > Suojaus ja**

yksityisyys ja sitten **Salli**, jotta ohjelmistokehittäjän **ESET, spol. s.r.o.** järjestelmäohjelmistot sallitaan. Lisätietoja on [tietopankin artikkelissa](#).

2. Jos käytössä on MacOS 10.14 ja uudemmat, ESET Endpoint Security for macOS näyttää **Tietokone on osittain suojattu** -ilmoituksen. Kaikkien ESET Endpoint Security for macOS -toimintojen käyttäminen edellyttää, että **koko levyn käyttö** on sallittu ESET Endpoint Security for macOS -tuotteelle. Avaa **Järjestelmäasetukset > Suojaus ja yksityisyys**. Valitse **Yksityisyys**-välilehti ja valitse **Koko levyn käyttö** -vaihtoehto. Napsauta lukituskuvaketta muokkauksen ottamiseksi käyttöön. Napsauta pluskuvaketta ja valitse ESET Endpoint Security for macOS. Tietokone näyttää ilmoituksen uudelleenkäynnistyksestä. Napsauta **Myöhemmin**. Älä käynnistä tietokonetta uudelleen nyt. Valitse **Käynnistä uudelleen** ESET Endpoint Security for macOS -ilmoitusikkunassa tai käynnistä tietokone uudelleen. Lisätietoja on [tietopankin artikkelissa](#).

Tuotteen ESET Endpoint Security for macOS asentamisen jälkeen on tarkistettava, onko tietokoneessa haitallista koodia. Valitse ohjelman pääikkunasta **Tietokoneen tarkistus > Smart Scan**. Lisätietoja tarvepohjaisista tietokoneen tarkistuksista on kohdassa [Tarvepohjainen tietokoneen tarkistus](#).

Mukautettu asennus

Mukautettu asennustila on suunniteltu kokeneille käyttäjille, jotka haluavat muokata lisäasetuksia asennusprosessin aikana.

- **Ohjelmakomponentit**

Tuotteen ESET Endpoint Security for macOS avulla voit asentaa tuotteen ilman joitakin sen ydinkomponenteista (esimerkiksi Internetin ja sähköpostin suojaus). Poista komponentti asennuksesta poistamalla valinta sen vieressä olevasta valintaruudusta.

- **Välityspalvelin**

Jos käytät välityspalvelinta, määritä sen parametrit valitsemalla **Käytän välityspalvelinta**. Kirjoita seuraavassa ikkunassa välityspalvelimen IP-osoite tai URL-osoite **Osoite**-kenttään. Määritä **Portti**-kenttään portti, josta välityspalvelin hyväksyy yhteyksiä (3128 on oletusarvo). Jos välityspalvelimen käyttö edellyttää todennusta, anna kelvollinen **käyttäjänimi** ja **salasana**, joiden avulla välityspalvelinta voidaan käyttää. Jos et käytä välityspalvelinta, valitse **En käytä välityspalvelinta**. Jos et ole varma, käytätkö välityspalvelinta, voit käyttää nykyisiä järjestelmäasetuksia valitsemalla vaihtoehdon **Käytä järjestelmäasetuksia (suositus)**.

- **Käyttöoikeudet**

Seuraavassa vaiheessa määritetään käyttöoikeudet saaneet käyttäjät tai ryhmät, jotka voivat muokata ohjelman asetuksia. Valitse käyttäjät vasemmalla olevasta käyttäjäluettelosta ja **lisää** heidät **Käyttöoikeudet saaneet käyttäjät** -luetteloon. Voit tuoda järjestelmän kaikki käyttäjät näkyviin valitsemalla **Näytä kaikki käyttäjät**. Jos jätät Käyttöoikeudet saaneet käyttäjät -luettelon tyhjäksi, kaikkien käyttäjien oletetaan saaneen käyttöoikeudet.

- **ESET LiveGrid®**

Lisätietoja ESET LiveGrid -ratkaisusta on [sanastossa](#).

- **Mahdollisesti ei-toivotut sovellukset**

Lisätietoja mahdollisesti ei-toivotuista sovelluksista on [sanastossa](#).

- **Palomuuuri**

Valitse palomuurin suodatustila. Lisätietoja on kohdassa [Suodatustilat](#).

Viimeistele tuotteen ESET Endpoint Security for macOS asennus seuraavasti:

macOS Big Sur (11)

1. [Järjestelmäajennusten salliminen](#).
2. [Levyn täysien käyttöoikeuksien salliminen](#).
3. Salli ESETin lisätä välityspalvelinkokoonpanoja. Saat seuraavan ilmoituksen: "ESET Endpoint Security for macOS" haluaa suodattaa verkon sisältöä. Kun saat tämän ilmoituksen, valitse **Salli**. Jos valitset **Älä salli**, internetin käytön suojaus ei toimi.



[macOS 10.15 ja vanhemmat](#)

1. MacOS 10.13 ja uudemmat ja sitä uudemmat versiot näyttävät **järjestelmäajennuksen estosta** ilmoittavan viestin, minkä lisäksi ESET Endpoint Security for macOS näyttää **Tietokonettasi ei ole suojattu** -ilmoituksen. Kaikkien ESET Endpoint Security for macOS -toimintojen käyttöönotto edellyttää, että ydintunnisteet on sallittu laitteessa. Voit sallia ydintunnisteet laitteessa valitsemalla **Järjestelmäasetukset > Suojaus ja yksityisyys** ja sitten **Salli**, jotta ohjelmistokehittäjän **ESET, spol. s.r.o.** järjestelmäohjelmistot sallitaan. Lisätietoja on [tietopankin artikkelissa](#).
2. Jos käytössä on MacOS 10.14 ja uudemmat, ESET Endpoint Security for macOS näyttää **Tietokone on osittain suojattu** -ilmoituksen. Kaikkien ESET Endpoint Security for macOS -toimintojen käyttäminen edellyttää, että **koko levyn käyttö** on sallittu ESET Endpoint Security for macOS -tuotteelle. Avaa **Järjestelmäasetukset > Suojaus ja yksityisyys**. Valitse **Yksityisyys**-välilehti ja valitse **Koko levyn käyttö** -vaihtoehto. Napsauta lukituskuvaketta muokkauksen ottamiseksi käyttöön. Napsauta pluskuvaketta ja valitse ESET Endpoint Security for macOS. Tietokone näyttää ilmoituksen uudelleenkäynnistyksestä. Napsauta **Myöhemmin**. Älä käynnistä tietokonetta uudelleen nyt. Valitse **Käynnistä uudelleen** ESET Endpoint Security for macOS -ilmoitusikkunassa tai käynnistä tietokone uudelleen. Lisätietoja on [tietopankin artikkelissa](#).

Tuotteen ESET Endpoint Security for macOS asentamisen jälkeen on tarkistettava, onko tietokoneessa haitallista koodia. Valitse ohjelman pääikkunasta **Tietokoneen tarkistus > Smart Scan**. Lisätietoja tarvepohjaisista tietokoneen tarkistuksista on kohdassa [Tarvepohjainen tietokoneen tarkistus](#).

Järjestelmäajennusten salliminen paikallisesti

macOS 11:ssä (Big Sur) ydinlaajennukset korvattiin järjestelmäajennuksilla. Uudet kolmansien osapuolten järjestelmäajennukset voidaan ladata vasta, kun käyttäjä on hyväksynyt ne.

Kun ESET Endpoint Security for macOS on asennettu macOS Big Sur (11) -järjestelmään tai uudempaan, saat järjestelmältä ilmoituksen järjestelmäajennuksen estämisestä ja tuotteelta ESET Endpoint Security for macOS Tietokonettasi ei ole suojattu -ilmoituksen. Jos haluat käyttää kaikkia tuotteen ESET Endpoint Security for macOS toimintoja, järjestelmäajennukset on sallittava laitteessa.

Päivitä aiempi macOS-järjestelmä Big Sur -versioon.



Jos ESET Endpoint Security for macOS on jo asennettu, ja aiot päivittää macOS Big Sur -järjestelmään, sinun on sallittava ESET-ydinlaajennukset manuaalisesti päivityksen jälkeen. Asiakaskonetta on voitava käyttää fyysisesti: jos sitä käytetään etäsijainnista, Salli-painike on poistettu käytöstä.

Kun asennat ESET-tuotetta macOS Big Sur -järjestelmään tai uudempaan, sinun on sallittava ESET-järjestelmälaajennukset manuaalisesti. Asiakaskonetta on voitava käyttää fyysisesti: jos sitä käytetään etäsijainnista, Salli-painike on poistettu käytöstä.

Järjestelmälaajennusten salliminen manuaalisesti

1. Valitse **Avaa järjestelmäasetukset** tai **Avaa tietoturva-asetukset** jossakin hälytysikkunassa.
2. Salli muutokset asetusikkunassa napsauttamalla vasemmalla alhaalla olevaa lukkokuvausta.
3. Käytä Touch ID:tä tai valitse **Käytä salasanaa** ja kirjoita käyttäjänimesi ja salasanasi ja valitse sitten **Avaa lukitus**.
4. Napsauta **Tiedot**-painiketta.
5. Valitse kaikki kolme ESET Endpoint Security for macOS.app-vaihtoehtoa.
6. Valitse **OK**.

Yksityiskohtaiset vaiheittaiset ohjeet löytyvät [tietopankkimme artikkelista](#). (Tietopankin artikkelit eivät ole saatavilla kaikilla kielillä.)

Levyn täysien käyttöoikeuksien salliminen paikallisesti

macOS-käyttöjärjestelmän versiossa 10.14 saat ilmoituksen **Tietokone on osittain suojattu** tuotteelta ESET Endpoint Security for macOS. Tuotteen ESET Endpoint Security for macOS kaikkien toimintojen käyttäminen edellyttää, että **levyn täydet käyttöoikeudet** on sallittu tuotteelle ESET Endpoint Security for macOS.

1. Valitse **Avaa järjestelmäasetukset** hälytysikkunassa.
2. Salli muutokset asetusikkunassa napsauttamalla vasemmalla alhaalla olevaa lukkokuvausta.
3. Käytä Touch ID:tä tai valitse **Käytä salasanaa** ja kirjoita käyttäjänimesi ja salasanasi ja valitse sitten **Avaa lukitus**.
4. Valitse luettelosta ESET Endpoint Security for macOS.app.
5. Tuotteen ESET Endpoint Security for macOS uudelleenkäynnistysilmoitus tulee näkyviin. Valitse Myöhemmin.
6. Valitse luettelosta ESETin **reaaliaikainen tiedostojärjestelmän suojaus**.

ESETin reaaliaikainen tiedostojärjestelmän suojaus ei ole saatavilla




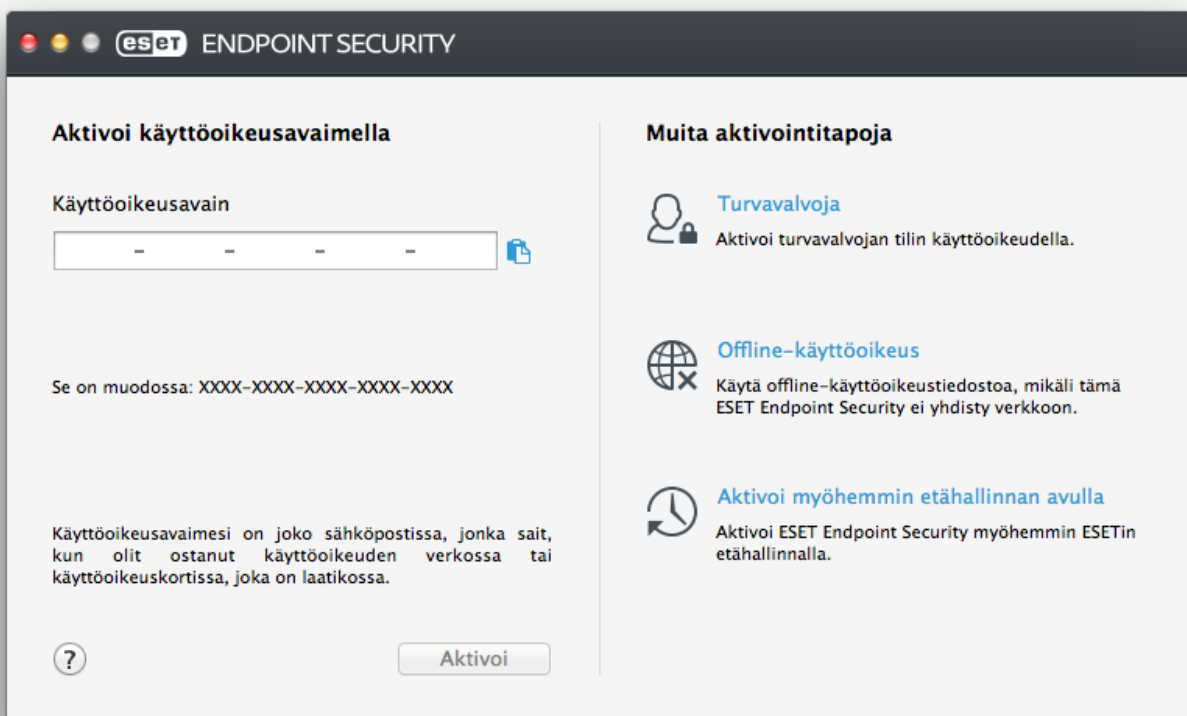
Jos reaaliaikainen tiedostojärjestelmän suojaus ei ole luettelossa, sinun on [sallittava ESET-tuotteesi järjestelmälaajennukset](#).

7. Valitse Käynnistä uudelleen tuotteen ESET Endpoint Security for macOS hälytysikkunassa tai käynnistä tietokone uudelleen. Lisätietoja on [tietopankin artikkelissa](#).

Tuoteaktivointi

Kun asennus on valmis, sinua pyydetään aktivoimaan tuote. Käytettävissä on useita aktivointitapoja. Tietyn aktivointitavan saatavuus tuotteellesi saattaa vaihdella maan ja jakelutavan (CD/DVD, ESET-web-sivu jne.) mukaan.

Voit aktivoida tuotteen ESET Endpoint Security for macOS kopion suoraan ohjelmasta napsauttamalla tuotteen ESET Endpoint Security for macOS kuvaketta , joka sijaitsee macOS-valikkopalkissa (näytön yläosassa), ja valitsemalla **Tuoteaktivointi**-vaihtoehdon. Voit aktivoida tuotteesi myös päävalikosta, osiosta **Ohje > Hallitse käyttöoikeutta** tai **Suojauksen tila > Aktivoi tuote**.



Voit aktivoida tuotteen ESET Endpoint Security for macOS jollakin seuraavista tavoista:

- **Aktivoi käyttöoikeusavaimella** – Ainutlaatuinen muodossa XXXX-XXXX-XXXX-XXXX-XXXX oleva merkkiketju, jota käytetään käyttöoikeuden haltijan tunnistamiseen ja käyttöoikeuden aktivoimiseen. Käyttöoikeusavain on joko sähköpostiviestissä, jonka sait käyttöoikeuden ostamisen jälkeen, tai tuotepakkauksessa olevassa käyttöoikeuskortissa.
- **Turvaluoja** – Tili, joka on luotu [ESETin käyttöoikeudenhallintaportalissa](#) käyttöoikeustunnuksillasi (sähköpostiosoite + salasana). Tämän menetelmän avulla voit hallita useita käyttöoikeuksia yhdestä paikasta.

- **Offline-käyttöoikeus** – Automaattisesti luotu tiedosto, joka siirretään ESET-tuotteeseen tarjoamaan käyttöoikeustiedot. Offline-käyttöoikeustiedostosi luodaan ESET-käyttöoikeusportaalista ja sitä käytetään ympäristöissä, joissa sovellus ei voi yhdistyä käyttöoikeusvaltuuttajaan.

Voit aktivoida sovelluksen myös myöhemmin, jos tietokoneesi on osa valvottua verkkoa ja jos järjestelmänvalvojas aikoo aktivoida tuotteen ESET Remote Administrator:n avulla.

Hiljainen aktivointi



ESET Remote Administrator voi aktivoida asiakastietokoneita äänettömästi käyttämällä järjestelmänvalvojan saataville tuomia käyttöoikeuksia.

Tuotteen ESET Endpoint Security for macOS versiossa 6.3.85.0 (ja uudemmissa) on vaihtoehto, jolla tuotteen voi aktivoida Pääte-ohjelmalla. Voit tehdä niin antamalla seuraavan komennon:

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

Vaihda XXXX-XXXX-XXXX-XXXX-XXXX käyttöoikeusavaimen, jota on jo käytetty tuotteen ESET Endpoint Security for macOS aktivointiin tai joka on rekisteröity [ESET License Administrator](#) -ohjelmalla. Komento palauttaa joko "OK"-tilan tai virheen, jos aktivointi epäonnistuu.

Asennuksen poistaminen

ESET Endpoint Security for macOS-asennuksen poistaja voidaan käynnistää usealla eri tavalla:

- Avaa ohjelman ESET Endpoint Security for macOS asennustiedosto (.dmg) ja kaksoisnapsauta **Poista asennus**.
- Käynnistä **Finder**, avaa kiintolevyllä oleva **Sovellukset**-kansio, paina Ctrl-näppäintä ja napsauta kuvaketta **ESET Endpoint Security for macOS** ja valitse **paketin sisällön näyttämismenü**. Avaa kansio **Contents > Helpers** ja kaksoisnapsauta **Uninstaller**-kuvaketta.

Asennuksen poistaminen



Asennuksen poistamisen aikana sinun on annettava järjestelmänvalvojan salasana useita kertoja, jotta tuotteen ESET Endpoint Security for macOS asennus voidaan poistaa kokonaan.

Peruskatsaus

Ohjelman ESET Endpoint Security for macOS pääikkuna on jaettu kahteen pääosaan. Oikealla oleva ensisijainen ikkuna sisältää tiedot, jotka vastaavat päävalikosta vasemmalta valittua asetusta.


Päävalikosta pääsee seuraaviin osioihin:

- **Suojauksen tila** – sisältää tietoja tietokoneen, palomuurin, Internetin ja sähköpostin suojaustilasta.
- **Tietokoneen tarkistus** – tässä osiossa voi määrittää [tarvepohjaisen tietokoneen tarkistuksen](#) ja käynnistää sen.
- **Päivitys** – näyttää moduulipäivitysten tiedot.

- **Asetukset** – valitse tämä osio, jos haluat säätää tietokoneen suojauksen tasoa.
- **Työkalut** – tässä ovat [Lokitiedostot](#), [Ajastin](#), [Karanteeni](#), [Käynnissä olevat prosessit](#) ja muut ohjelman toiminnot.
- **Ohje** – sisältää ohjetiedostot, Internet-tietämyskannan, tukipyyntölomakkeen ja ohjelmaa koskevia lisätietoja.

Pikanäppäimet

Pikanäppäimiä, joita voidaan käyttää tuotetta ESET Endpoint Security for macOS käytettäessä:

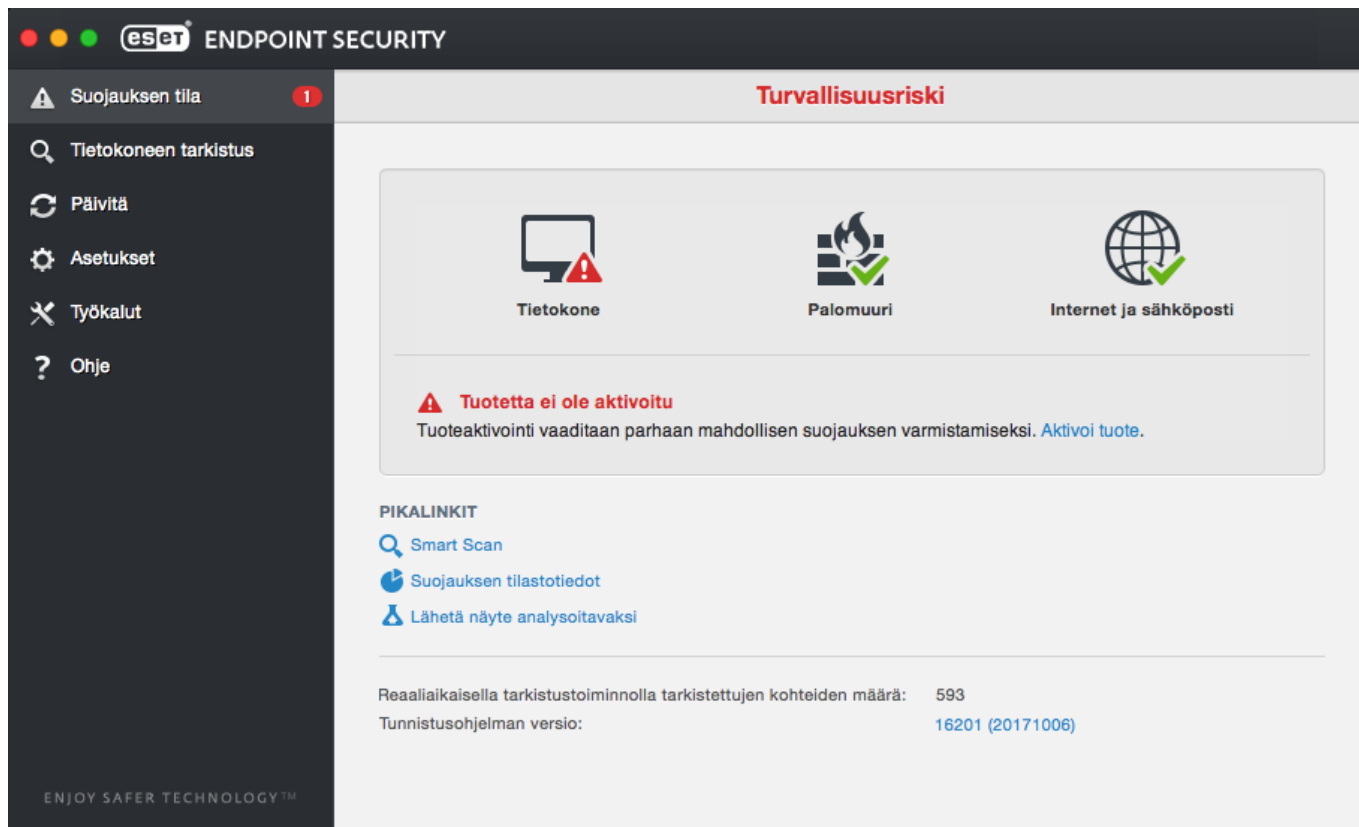
- *cmd+,* – tuo tuotteen ESET Endpoint Security for macOS oletusasetukset näkyviin.
- *cmd+O* - muuttaa ohjelman ESET Endpoint Security for macOS pääikkunan koon oletuskokoon ja siirtää sen näytön keskelle,
- *cmd+Q* – Piilottaa tuotteen ESET Endpoint Security for macOS pääikkunan. Voit avata sen napsauttamalla tuotteen ESET Endpoint Security for macOS kuvaketta  macOS-valikkopalkista (näytön yläosassa).
- *cmd+W* - sulkee ohjelman ESET Endpoint Security for macOS pääikkunan.

Seuraavat pikanäppäimet toimivat vain, jos **Käytä vakiovalikkoa** -asetus on otettu käyttöön kohdassa **Asetukset > Anna sovelluksen oletusasetukset... > Liittymä**:

- *cmd+alt+L* – avaa **Lokitiedostot**-osion.
- *cmd+alt+S* – avaa **Ajastin**-osion.
- *cmd+alt+Q* – avaa **Karanteeni**-osion.

Järjestelmän toiminnan tarkistaminen

Näet suojauksesi tilan valitsemalla päävalikosta **Suojauksen tila**. Ohjelman ESET Endpoint Security for macOS moduulien toiminnan ilmaiseva tilayhteenveto näytetään ensisijaisessa ikkunassa.



Mitä tehdä, jos ohjelma ei toimi oikein?

Jos moduuli toimii oikein, näkyvissä on vihreä oikeinmerkki. Jos moduuli ei toimi oikein, näkyvissä on punainen huutomerkki tai oranssi ilmoituskuvake. Moduulia koskevat lisätiedot ja ongelman korjausehdotusratkaisu näytetään ohjelman pääikkunassa. Yksittäisten moduulien tilaa voi muuttaa napsauttamalla kunkin ilmoituksen alla olevaa sinistä linkkiä.

Jos ongelmaa ei voi ratkaista ehdotetuilla ratkaisutavoilla, voit hakea ratkaisua [ESET-tietämyskannasta](#) tai ottamalla yhteyden [ESETin asiakastukeen](#). Asiakastuki vastaa nopeasti kysymyksiin ja auttaa ratkaisemaan tuotteeseen ESET Endpoint Security for macOS liittyvät ongelmat.

Tietokoneen suojaus

Tietokoneen kokoonpano on **Asetukset**-valikossa kohdassa **Tietokone**. Se näyttää **reaaliaikaisen tiedostojärjestelmän suojauksen** tilan. Yksittäisiä moduuleja voi poistaa käytöstä vaihtamalla halutun moduulin tilaan **POIS KÄYTÖSTÄ**. Huomaa, että tämä saattaa heikentää tietokoneen suojausta. Voit käsitellä kunkin moduulin yksityiskohtaisia asetuksia valitsemalla **Asetukset**.

Virustentorjunta ja vakoiluohjelman suojaus

Virustentorjunta suojaa järjestelmää haitallisilta hyökkäyksiltä muokkaamalla tiedostoja, jotka ovat mahdollisia uhkia. Jos haittaohjelmia sisältävä uhka havaitaan, virustentorjuntamoduuli voi estää sen toiminnan, minkä jälkeen se puhdistetaan, poistetaan tai siirretään karanteeniin.

Yleiset

Yleiset-osiossa (**Asetukset > Anna sovelluksen oletusasetukset... > Yleiset**) voi ottaa seuraavantyyppisten sovellusten tunnistuksen käyttöön:



- **Mahdollisesti ei-toivotut sovellukset** – Näitä sovelluksia ei ole välttämättä tarkoitettu haitallisiksi, mutta ne saattavat heikentää tietokoneen suorituskykyä. Näiden sovelluksien asentaminen vaatii yleensä käyttäjän suostumuksen. Jos tietokoneessa on tällaisia sovelluksia, järjestelmä ei toimi samalla tavoin kuin ennen sovellusten asentamista. Merkittävimpiä muutoksia ovat ei-toivotut ponnahdusikkunat, piilotettujen prosessien aktivointi ja suoritus, järjestelmäresurssien lisääntynyt käyttö, muutokset hakutuloksissa ja etäpalvelinten kanssa tietoliikenneyhteydessä olevat sovellukset.
- **Mahdollisesti vaaralliset sovellukset** – Nämä sovellukset viittaavat kaupallisiin sovelluksiin, joita voidaan käyttää myös haitallisiin tarkoituksiin, jos ne on asennettu ilman käyttäjän lupaa. Tähän luokitukseen sisältyvät erilaiset ohjelmat, kuten etäkäyttötyökalut, mistä syystä tämä asetus on oletusarvoisesti poistettu käytöstä.
- **Epäilyttävät sovellukset** – Näihin sovelluksiin sisältyvät pakkaajilla tai suojaustoiminnoilla pakatut ohjelmat. Haittaohjelmien tekijät hyödyntävät tällaisia suojaustoimintoja usein tunnistuksen välttämiseen. Pakkaaja on itsestään purkautuva suorituksenaikainen ohjelmätiedosto, joka sisältää erilaisia haittaohjelmia yhdessä paketissa. Yleisimpiä pakkaajia ovat UPX, PE_Compact, PKLite ja ASPack. Sama haittaohjelma saatetaan havaita eri tavalla, jos se on pakattu eri pakkaajalla. Pakkaajat voivat myös muuntaa "allekirjoituksiaan" ajan mittaan, mikä vaikeuttaa haittaohjelmien havaitsemista ja poistamista.

Voit määrittää [tiedostojärjestelmän tai Internetin ja sähköpostin suojauspoikkeukset](#) napsauttamalla **Asetukset**.

Poikkeukset

Osiassa Poikkeukset voit ohittaa tarkistuksesta tiettyjä tiedostoja tai kansioita, sovelluksia tai IP-/IPv6-osoitteita.

Tiedostojärjestelmä-välilehdessä olevat tiedostot ja kansiot jätetään pois kaikista tarkistuksista: käynnistys, reaaliaikainen ja tarvepohjainen (tietokoneen tarkistus).

- **Polku** - Ohitettujen tiedostojen ja kansioden tiedostopolku.
- **Uhka** - Jos ohitetun tiedoston vieressä on jonkin uhan nimi, se tarkoittaa, että tiedosto ohitetaan vain kyseisen uhan osalta mutta ei kokonaan. Jos kyseinen tiedosto saa myöhemmin jonkin toisen haittaohjelman aiheuttaman tartunnan, virustentorjuntamoduuli havaitsee sen.
-  – Luo uuden tietueen. Anna polku kohteeseen (voit käyttää myös yleismerkkejä * ja ?) tai valitse kansio tai tiedosto puurakenteesta.
-  – poistaa valitut kohteet
- **Oletusarvo** – poikkeukset palautetaan viimeksi tallennettuun tilaan.


Internet ja sähköposti -välilehdessä protokollatarkistuksesta voi jättää pois tiettyjä **sovelluksia** ja **IP-/IPv6-osoitteita**.

Käynnistystuksen suojaus

Käynnistystiedostojen tarkistus tarkistaa tiedostot automaattisesti järjestelmän käynnistystuksen yhteydessä. Oletusasetusten mukaan tämä tarkistus suoritetaan säännöllisesti ajoitettuna tehtävänä käyttäjän kirjautumisen jälkeen tai onnistuneen moduulien päivityksen jälkeen. Jos haluat muokata käynnistystarkistukseen liittyviä ThreatSense-järjestelmän parametrien asetuksia, napsauta **Asetukset**. Saat lisätietoja ThreatSense-järjestelmän asetuksista lukemalla [tämän osion](#).

Reaaliaikainen tiedostojärjestelmän suojaus

Reaaliaikainen tiedostojärjestelmän suojaustoiminto tarkistaa kaikki tallennusvälinetyypit. Erilaiset tapahtumat voivat käynnistää tarkistuksen. ThreatSense-tekniikkaa (kuvattu osiossa nimeltä [ThreatSense-moottorin parametrien asetukset](#)) käyttävän reaaliaikaisen tiedostojärjestelmän suojauksen juuri luoduille ja vanhoille tiedostoille suorittamat toimenpiteet voivat olla erilaisia. Juuri luotuja tiedostoja voi hallita tarkemmin.

Oletuksena kaikki tiedostot tarkistetaan **tiedosto auki**, **tiedoston luonti** tai **tiedoston suoritus**. Suosittelemme säilyttämään oletusasetukset, sillä ne antavat tietokoneelle parhaan reaaliaikaisen suojaus tason. Reaaliaikainen suojaus käynnistyy järjestelmän käynnistystuksen yhteydessä ja tekee tarkistuksia keskeytymättä. Tietyissä tapauksissa (esimerkiksi ristiriidan ilmetessä jonkin toisen reaaliaikaisen tarkistustoiminnon kanssa) reaaliaikainen tiedostojärjestelmän suojaus voidaan poistaa käytöstä napsauttamalla (näytön yläosassa) valikkorivillä olevaa tuotteen ESET Endpoint Security for macOS kuvaketta  ja valitsemalla sitten **Poista reaaliaikainen tiedostojärjestelmän suojaus käytöstä** -vaihtoehdon. Reaaliaikainen tiedostojärjestelmän suojaus voidaan poistaa käytöstä myös ohjelman pääikkunasta (valitsemalla **Asetukset > Tietokone** ja vaihtamalla **Reaaliaikainen tiedostojärjestelmän suojaus** -asetukseksi **POIS KÄYTÖSTÄ**).

Seuraavat kohteet voidaan ohittaa Real-time -tarkistuksesta:

- **Paikalliset asemat** - järjestelmän kiintolevyt
- **Siirrettävä tietoväline** - CD-/DVD-levyt, USB-laitteet, Bluetooth-välineet jne.
- **Verkkomedia** - kaikki verkkoon liitetyt asemat

Suosittelamme, että käytät oletusasetuksia ja että muutat tarkistuksessa ohitettavia kohteita vain erityistapauksissa, esimerkiksi silloin, kun tietyn tallennusvälineen tarkistaminen hidastaa tiedonsiirtoa merkittävästi.

Voit muokata reaaliaikaisen tiedostojärjestelmän suojaus lisäasetuksia siirtymällä kohtaan **Asetukset > Anna sovelluksen oletusasetukset...** (tai painamalla `cmd+,`) > **Reaaliaikainen suojaus** ja napsauttamalla **Lisäasetukset**-kohdan vieressä olevaa **Asetukset...**-painiketta (kuvattu [Tarkistuksen lisäasetuksissa](#)).

Lisäasetukset

Tässä ikkunassa voit määrittää ThreatSense-järjestelmän tarkistamien kohteiden tyyppin. Lisätietoja **Itsepurkautuvista arkistoista**, **Ajonaikaisista pakkaajista** ja **Kehittyneestä heuristiikasta** saat kohdasta [ThreatSense-järjestelmän parametrien asetukset](#).

Emme suosittele tekemään muutoksia **Oletusarkistointiasetukset**-kohdassa, ellei muuttamista tarvita tietyn

ongelman selvittämiseen, sillä suuret arkiston sisäkkäisyysarvot voivat heikentää järjestelmän suorituskykyä.

Suoritettujen tiedostojen ThreatSense-parametrit - oletusarvon mukaan **kehittyntä heuristiikkaa** käytetään, kun tiedostoja suoritetaan. On suositeltavaa pitää Smart-optimointi ja ESET LiveGrid® käytössä, jotta vaikutus järjestelmän suorituskykyyn vähenisi.

Paranna verkkoasemien yhteensopivuutta - tällä asetuksella parannat suorituskykyä käyttäessäsi tiedostoja verkon välityksellä. Tätä asetusta kannattaa käyttää, jos järjestelmä hidastuu verkkoasemia käytettäessä. Ominaisuus käyttää järjestelmän tiedostojärjestelijää OS X 10.10:ssä ja sitä uudemmissa versioissa. Huomaathan, että kaikki sovellukset eivät tue tiedostojärjestelijää. Esimerkiksi Microsoft Word 2011 ei tue sitä, kun taas, Word 2016 tukee.

Milloin reaaliaikaisen suojauksen asetuksia kannattaa muuttaa?

Reaaliaikainen suojaus on keskeistä järjestelmän suojauksen kannalta. Reaaliaikaisen suojauksen parametreja muutettaessa on syytä olla varovainen. Suosittelemme, että näitä parametreja muutetaan vain erityistapauksissa, esimerkiksi silloin, jos jonkin sovelluksen tai toisen virustentorjuntaohjelman reaaliaikaisen tarkistuksen kanssa ilmenee yhteensopivuusongelmia.

Kun ESET Endpoint Security for macOS on asennettu, kaikki asetukset optimoidaan siten, että ne suojaavat käyttäjien järjestelmiä parhaalla mahdollisella tavalla. Oletusasetukset voidaan palauttaa napsauttamalla **Reaaliaikainen suojaus** -ikkunassa alavasemmalla olevaa **Oletus**-painiketta (**Asetukset > Anna sovelluksen oletusasetukset... > Reaaliaikainen suojaus**).

Reaaliaikaisen suojauksen tarkistaminen

Reaaliaikaisen suojauksen toiminta voidaan varmistaa lataamalla eicar.com-testitiedosto. Testitiedosto on vaaraton erikoistiedosto, joka kaikkien virustorjuntaohjelmien pitäisi havaita. Tiedosto on EICAR-instituutin (European Institute for Computer Antivirus Research) luoma ja sillä testataan virustorjuntaohjelmien toiminta.

Kun haluat tarkistaa Reaaliaikaisen suojauksen tilan käyttämättä ESET Security Management Center, muodosta asiastietokoneeseen etäyhteys **päätteellä** ja syötä seuraava komento:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Reaaliaikaisen suojauksen tila näytetään joko viestillä **RTPStatus=Enabled** tai **RTPStatus=Disabled**.

Päätteen bash-tulos sisältää seuraavat statukset:

- asiakaskoneelle asennetun ohjelman ESET Endpoint Security for macOS versio
- tunnistusohjelman päiväys ja versio
- päivityspalvelimen polku



Pääte-ohjelman käyttö

Suosittelimme, että vain edistyneet käyttäjät käyttävät Pääte-ohjelmaa.

Toimenpiteet reaaliaikaisen suojauksen toimintahäiriön ilmetessä

Tässä kohdassa on esimerkkejä reaaliaikaisen suojaustoiminnon käyttöön liittyvistä ongelmatilanteista sekä ohjeita vianmäärittelyyn.

Reaaliaikainen suojaus on pois käytöstä

Jos käyttäjä on vahingossa poistanut reaaliaikaisen suojauksen käytöstä, se on aktivoitava uudelleen.

Reaaliaikainen suojaus voidaan aktivoida uudelleen siirtymällä kohtaan **Asetukset > Tietokone** ja vaihtamalla **Reaaliaikainen tiedostojärjestelmän suojaus** -asetukseksi **KÄYTÖSSÄ**. Reaaliaikaisen tiedostojärjestelmän suojauksen voi ottaa käyttöön myös sovelluksen oletusasetusikkunassa kohdassa **Reaaliaikainen suojaus** valitsemalla **Ota reaaliaikainen tiedostojärjestelmän suojaus käyttöön** -vaihtoehdon.

Reaaliaikainen suojaus ei havaitse tai puhdistaa tunkeutumisia

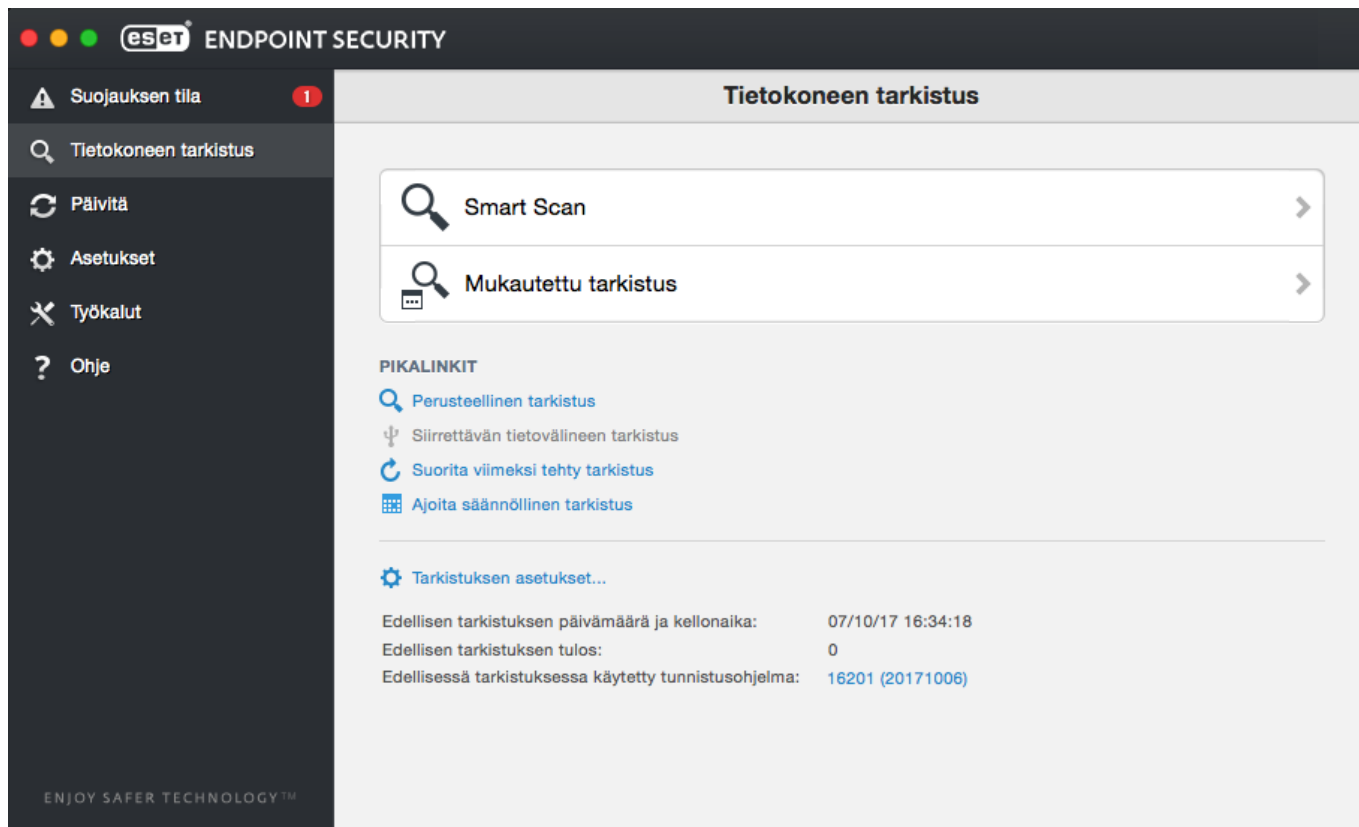
Varmista, ettei tietokoneeseen ole asennettu muita virustorjuntaohjelmia. Jos kaksi reaaliaikaista suojaussovellusta on käytössä samanaikaisesti, ne saattavat haitata toistensa toimintaa. Suosittelemme poistamaan mahdolliset muut virustorjuntaohjelmat tietokoneesta.

Reaaliaikainen suojaus ei käynnisty


Jos reaaliaikainen suojaus ei käynnisty tietokoneen käynnistyksen yhteydessä, ohjelma saattaa olla ristiriidassa muiden sovelluksien kanssa. Jos tämä ongelma ilmenee, ota yhteys ESET-asiakaspalveluun.

Tarvepohjainen tietokoneen tarkistus

Jos epäilet, että tietokoneessa on virustartunta (se käyttäytyy epätavallisesti), etsi tietokoneesta tartuntoja suorittamalla **Smart Scan**. Tietokone kannattaa tarkistaa säännöllisesti osana rutiinitoimia, ei pelkästään tartuntaa epäiltäessä, jotta tietoturva pysyy mahdollisimman hyvänä. Säännöllisten tarkistuksien avulla voidaan havaita tartuntoja, joita ei ole havaittu reaaliaikaisissa tarkistuksissa tiedostoja tallennettaessa. Näin voi käydä, jos reaaliaikainen tarkistustoiminto on ollut pois käytöstä tartunnan aikaan tai jos moduulit eivät ole ajan tasalla.



Tarvepohjainen tietokoneen tarkistus on suositeltavaa suorittaa vähintään kerran kuukaudessa. Tarkistus voidaan määrittää ajoitetuksi tehtäväksi valitsemalla **Työkalut > Ajastin**.

Voit myös vetää ja pudottaa valikoituja tiedostoja ja kansioita työpöydältä tai **Finder**-ikkunasta ohjelman ESET Endpoint Security for macOS päänäyttöön, Dock-kuvakkeeseen, valikkorivikuvakkeeseen  (näytön yläosassa) tai sovelluskuvakkeeseen (/Sovellukset-kansiossa).

Tarkistustyyppi

Tarvepohjaisia tietokoneen tarkistuksia on kahdentyyppisiä. **Smart Scan** tarkistaa järjestelmän nopeasti. Tarkistusparametreja ei tarvitse muuttaa. **Mukautettu tarkistus** -asetuksen avulla voit valita ennalta määritetyn tarkistusprofiilin ja valita määrätty tarkistettavat kohteet.

Smart Scan

Smart Scan -tarkistus on nopea tapa käynnistää tietokoneen tarkistus ja puhdistaa viruksen tartuttamat tiedostot ilman käyttäjän toimenpiteitä. Yksi sen tärkeimmistä eduista on helppokäyttöisyys: tarkkoja tarkistusasetuksia ei tarvitse tehdä. Smart Scan tarkistaa kaikkien kansioiden kaikki tiedostot ja puhdistaa tai poistaa havaitut tartunnat automaattisesti. Puhdistustasona käytetään oletusasetusta. Lisätietoja puhdistustyypeistä on kohdassa [Puhdistaminen](#).

Mukautettu tarkistus

Mukautettu tarkistus mahdollistaa tarkistusparametrien, kuten tarkistettavien kohteiden ja tarkistustapojen, käyttämisen. Mukautetun tarkistuksen etu on sen mahdollisuus määrittää tarkistusparametrit tarkasti. Eri kokoonpanoja voidaan tallentaa käyttäjän määrittämiksi tarkistusprofiileiksi, jotka ovat hyödyllisiä erityisesti, jos

tarkistus suoritetaan toistuvasti samoilla parametreilla.

Valitse tarkistuksen kohteet valitsemalla **Tietokoneen tarkistus > Mukautettu tarkistus** ja valitse määrätty **Tarkistettavat kohteet** puurakenteesta. Tarkistettavan kohteen voi määrittää myös tarkemmin määrittämällä polun lisääviin kansioihin tai tiedostoihin. Jos vain järjestelmä halutaan tarkistaa ilman lisäpuhdistustoimintoja, valitse **Tarkista puhdistamatta**. Lisäksi voidaan valita puhdistustaso kolmesta vaihtoehdosta napsauttamalla **Asetukset... > Puhdistaminen**.

Mukautettua tarkistusta

i Tietokoneen tarkistaminen mukautetussa tarkistustilassa soveltuu vain edistyneille käyttäjille, joilla on kokemusta virustorjuntaohjelmien käyttämisestä.

Tarkistuskohteet

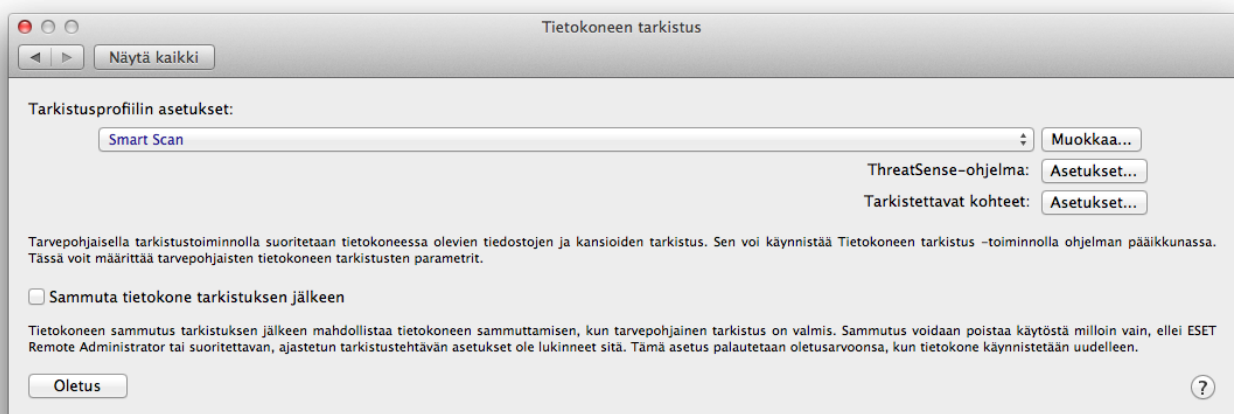
Tarkista kohteet -puurakenteesta voit valita tiedostot ja kansiot, joista etsitään viruksia. Kansioita voi valita myös profiilin asetusten mukaan.

Tarkistettavan kohteen voi määrittää tarkemmin määrittämällä polun niihin kansioihin tai tiedostoihin, jotka lisätään tarkistukseen. Valitse kohteet puurakenteesta, jossa on luettelo kaikista tietokoneessa käytettävissä olevista kansioista valitsemalla se valintaruutu, joka vastaa määrättyä tiedostoa tai kansiota.

Tarkistusprofiilit

Ensisijaiset tarkistusasetukset voi tallentaa tulevia tarkistuksia varten. Suosittelemme luomaan eri profiilin (erilaisilla tarkistuskohdeilla ja -tavoilla sekä muilla parametreilla) kullekin säännöllisesti käytettävälle tarkistukselle.

Voit luoda uuden profiilin valitsemalla päävalikosta **Asetukset > Anna sovelluksen oletusasetukset...** (tai painamalla *cmd+,*) > **Tietokoneen tarkistus** ja valitsemalla profiililuettelon vierestä **Muokkaa...**



Voit luoda tarkistusprofiilin tarpeidesi mukaan kohdassa [ThreatSense-moduulin parametrien asetukset](#) olevien tarkistuksen asetusten parametrikuvausten mukaisesti.

Esimerkki

- ✓ Käyttäjä haluaa luoda oman tarkistusprofiilin ja Smart Scan -kokoonpano on osittain sopiva, mutta käyttäjä ei kuitenkaan halua tarkistaa suorituksenaikaisia pakkaajia tai mahdollisesti vaarallisia sovelluksia. Sen lisäksi halutaan käyttää tarkkaa puhdistusta. Kirjoita profiilin nimi **Tarvepohjaisen tarkistustoiminnon profiililuettelo** -ikkunaan, napsauta **Lisää** ja vahvista valinta valitsemalla **OK**. Sääda parametreja vaatimustesi mukaan **ThreatSense-ohjelmalla** ja **Tarkistettavat kohteet** -asetuksilla.

Jos haluat sulkea käyttöjärjestelmän ja sammuttaa tietokoneen tarvepohjaisen tarkistuksen päätyttyä, käytä vaihtoehtoa **Sammuta tietokone tarkistuksen jälkeen**.

ThreatSense-järjestelmän parametrien asetukset

ThreatSense on ESETin oma, useista uhkien havaitsemismenetelmistä muodostuva tekniikka. Tekniikka toimii aktiivisesti, mikä tarkoittaa sitä, että se suojaa tietokonetta myös uuden uhan leviämisen alkuvaiheissa. Tekniikassa hyödynnetään useita menetelmiä (koodien analyysia, koodien emulaatiota, yleisiä määrittäjiä jne.), jotka yhdessä parantavat merkittävästi järjestelmän suojausta. Tarkistusmoduuli pystyy hallitsemaan samanaikaisesti useita tietovirtoja, mikä parantaa tehokkuutta ja tunnistustulosta. ThreatSense-tekniikan avulla voidaan päästä myös rootkit-ohjelmista eroon.

ThreatSense-tekniikan asetuksissa käyttäjä voi määrittää useita tarkistuksen parametreja:

- tarkistettavat tiedostotyytit ja -tunnisteet
- erilaisten tunnistusmenetelmien yhdistelmän
- puhdistuksen tason jne.

Voit siirtyä asetusikkunaan valitsemalla **Asetukset > Anna sovelluksen oletusasetukset...** (tai painamalla *cmd+*) ja napsauttamalla sitten ThreatSense-ohjelman **Asetukset**-painiketta, joka sijaitsee **Järjestelmän suojaus**-, **Reaaliaikainen suojaus**- ja **Käynnistyksen suojaus** -moduuleissa. Ne kaikki käyttävät ThreatSense-tekniikkaa (lisätietoja alla). Erilaiset suojaukseen kohdistuvat vaatimukset edellyttävät erilaisia kokoonpanoja. ThreatSense-asetukset voidaankin määrittää käyttäjäkohtaisesti seuraavien moduulien osalta:

- **Käynnistyksen suojaus** – Automaattinen käynnistystiedostojen tarkistus
- **Reaaliaikainen suojaus** – Reaaliaikainen tiedostojärjestelmän suojaus
- **Tietokoneen tarkistus** – Tarvepohjainen tietokoneen tarkistus
- **Internet-käytön suojaus**
- **Sähköpostisuojaus**

ThreatSense-parametrit on optimoitu jokaisen moduulin osalta erikseen, ja muutokset voivat vaikuttaa merkittävästi järjestelmän toimintaan. Esimerkiksi järjestelmä voi hidastua merkittävästi, jos asetuksia muutetaan siten, että suorituksenaikaisia pakkaajia etsitään aina tai että kehittynyt heuristiikka otetaan käyttöön

reaaliaikaisessa tiedostojärjestelmän suojausmoduulissa. Siksi suosittelemme, että tietokoneen tarkistusta lukuun ottamatta oletusarvoisia ThreatSense-parametreja ei muuteta.

Kohteet

Kohteet-osiossa voidaan määrittää, mitkä tiedostot tarkistetaan tunkeutumisten varalta.

- **Symboliset linkit** – (vain Tietokoneen tarkistus) tarkistaa sellaisen tekstimerkkijonon sisältävät tiedostot, joka tulkitaan poluksi tiedostoon tai hakemistoon.
- **Sähköpostitiedostot** – (ei käytettävissä reaaliaikaisessa suojauksessa) tarkistaa sähköpostitiedostot.
- **Postilaatikot** – (ei käytettävissä reaaliaikaisessa suojauksessa) tarkistaa järjestelmän postilaatikot. Tämän asetuksen virheellinen käyttö voi aiheuttaa ristiriidan sähköpostisovelluksessa. Lisätietoja tämän asetuksen eduista ja haitoista on seuraavassa [tietämyskanta-artikkelissa](#).
- **Arkistot** – (ei käytettävissä reaaliaikaisessa suojauksessa) tarkistaa arkistoihin pakatut tiedostot (.rar, .zip, .arj, .tar jne.).
- **Itsepurkautuvat arkistot** – (ei käytettävissä reaaliaikaisessa suojauksessa) tarkistaa itsepurkautuvissa arkistotiedostoissa olevat tiedostot.
- **Tarkistettu Suorituksenaikaiset pakkaajat** – Suorituksenaikaiset pakkaajat purkautuvat muistiin, toisin kuin vakimuotoiset arkistotyyppit. Kun tämä asetus on valittuna, myös vakimuotoiset staattiset pakkaajat (esim. UPX, yoda, ASPack, FGS) tarkistetaan.

Asetukset

Asetukset-osiossa voit valita menetelmät, joilla järjestelmä tarkistetaan. Käytettävissäsi ovat seuraavat asetukset:

- **Heuristiikka** – Heuristiikka tarkoittaa algoritmia, joka analysoi ohjelmien (haitallista) toimintaa. Heuristiikkatunnistuksen tärkein etu on kyky tunnistaa uusia haitallisia ohjelmistoja, joita ei aiemmin ollut.
- **Kehittynyt heuristiikka** – Kehittynyt heuristiikka koostuu ESETin kehittämistä, ainutlaatuisista algoritmeista, jotka on optimoitu tunnistamaan madot ja troijalaiset. Algoritmit on laadittu korkean tason ohjelmointikielillä. Ohjelman tunnistuskyky on kehittyneen heuristiikan ansiosta merkittävästi muita ohjelmia parempi.

Puhdistaminen


Puhdistusasetukset määrittävät tavan, jolla tarkistustoiminto puhdistaa tartunnan saaneet tiedostot.

Puhdistustasoja on kolme:

- **Ei puhdistusta** – Tartunnan saaneita kohteita ei puhdisteta automaattisesti. Ohjelma näyttää varoitusikkunan ja antaa käyttäjän valita toimenpiteen.
- **Normaali puhdistus** – Ohjelma yrittää automaattisesti puhdistaa tai poistaa viruksen tartuttaman tiedoston. Jos tarvittavaa toimenpidettä ei voida valita automaattisesti, ohjelma tarjoaa jatkotoimenpidevaihtoehtoja. Vaihtoehdot näytetään myös, jos ennalta määritettyä toimintoa ei voida suorittaa.



- **Tarkka puhdistus** – Ohjelma puhdistaa tai poistaa kaikki viruksen tartuttamat tiedostot (mukaan lukien arkistot). Tämä ei koske järjestelmätiedostoja. Jos tiedostoa ei voida puhdistaa, saat asiasta ilmoituksen, ja sinua pyydetään valitsemaan suoritettava toimenpide.

Vakiopuhdistustila – arkiston puhdistus

 Oletusarvoisessa vakiopuhdistustilassa koko arkistotiedostot poistetaan vain, jos kaikki arkiston sisältämät tiedostot ovat saaneet tartunnan. Jos arkistossa on sekä puhtaita että tartunnan saaneita tiedostoja, sitä ei poisteta. Jos viruksen tartuttama arkistotiedosto havaitaan, kun Tarkka puhdistus -tila on käytössä, koko arkisto poistetaan, vaikka se sisältäisi myös puhtaita tiedostoja.

Poikkeukset

Tiedostotunniste on tiedoston nimen osa, joka on erotettu pisteellä. Tiedostotunniste määrittää tiedoston tyyppin ja sisällön. Näiden ThreatSense-parametriasetusten avulla voidaan määrittää tarkistuksessa ohitettavat tiedostot.

Oletuksena kaikki tiedostot tarkistetaan niiden tiedostotunnisteista riippumatta. Tiedostotunnisteita voidaan lisätä tarkistuksessa ohitettavien tiedostojen luetteloon. - ja -painikkeilla voidaan ottaa käyttöön tiettyjen tiedostotunnisteiden tarkistus tai estää se.

Tiedostojen ohittaminen tarkistuksessa saattaa olla hyödyllistä, jos tiettyjen tiedostotyyppien tarkistaminen estää ohjelmaa toimimasta oikein. Voi esimerkiksi olla järkevää ohittaa *log*, *cfg* ja *tmp*-tiedostot. Tiedostotunnisteiden oikea muoto on

log

cfg

tmp

Rajat

Rajat-kohdassa voit määrittää tarkistettavien kohteiden suurimman koon ja arkiston sisennyksen enimmäistason:

- **Enimmäiskoko:** Määrittää tarkistettavien kohteiden suurimman koon. Virustentarkistusmoduuli tarkistaa vain määritettyä kokoa pienemmät kohteet. Emme suosittele oletusarvon muuttamista, koska sitä ei tavallisesti tarvitse muokata. Vain sellaisten kokeneiden käyttäjien tulisi muuttaa tätä asetusta, joilla on jokin syy ohittaa suuria kohteita tarkistuksesta.
- **Enimmäistarkistusaika:** Määrittää kohteen tarkistamiseen varatun enimmäisajan. Jos tähän on määritetty jokin arvo, virustentarkistusmoduuli lopettaa kohteen tarkistamisen kyseisen ajan kuluttua huolimatta siitä, onko tarkistus päättynyt.
- **Sisäkkäisyystaso enimmillään:** Määrittää arkiston tarkistuksen suurimman sallitun sisäkkäisyystason. Emme suosittele oletusarvon 10 muuttamista, koska tavallisesti sen muuttamiseen ei pitäisi olla mitään syytä. Jos tarkistus päättyy ennenaikaisesti sisäkkäisten arkistojen määrän vuoksi, arkisto jää tarkistamatta.
- **Enimmäistiedostokoko:** Tämän asetuksen avulla voit määrittää tarkistettavien arkistoissa olevien tiedostojen suurimman koon (kun ne puretaan). Jos tarkistus päättyy ennenaikaisesti tämän rajan vuoksi, arkisto jää tarkistamatta.

Muut

Ota Smart-optimointi käyttöön

Smart-optimointia käytettäessä asetukset optimoidaan, mikä varmistaa tehokkaimman tarkistustason laskematta tarkistusnopeutta. Erilaiset suojausmoduulit suorittavat tarkistuksia hyödyntämällä eri tarkistusmenetelmiä. Smart-optimointia ei ole määritetty tarkasti tuotteessa. ESETin kehitystyöryhmä ottaa uusia muutoksia käyttöön jatkuvasti. Niitä integroidaan tuotteeseen ESET Endpoint Security for macOS säännöllisillä päivityksillä. Jos Smart-optimointi on poistettu käytöstä, vain käyttäjän määrittämät asetukset tietyn moduulin ThreatSense-ytimessä otetaan käyttöön tarkistusta suoritettaessa.

Tarkista vaihtoehtoinen tietovirta (vain tarvepohjainen tarkistus)

Tiedostojärjestelmän vaihtoehtoiset tietovirrät (resurssi-/data-fork-toiminnot) ovat tiedosto- ja kansiolitoksia, jotka eivät näy tavallisissa tarkistustekniikoissa. Monet tunkeutumiset yrittävät välttää paljastumisen näyttäytymällä vaihtoehtoisina tietovirtoina.

Tunkeutumisen havaitseminen

Tunkeutumiset voivat päästä järjestelmään useita reittejä: Web-sivustojen, jaettujen kansioden, sähköpostin tai siirrettävien tallennuslaitteiden (esimerkiksi USB-laitteiden, ulkoisien levyjen, CD- ja DVD-levyjen) välityksellä.

Jos tietokone vaikuttaa saaneen haittaohjelmataartunnan eli jos se esimerkiksi toimii hitaammin tai jumittuu usein, suosittelemme seuraavia toimenpiteitä:

1. Valitse **Tietokoneen tarkistus**.
2. Napsauta **Smart Scan** -painiketta (lisätietoja on kohdassa [Smart Scan](#)).
3. Tarkistettujen, tartunnan saaneiden ja puhdistettujen tiedostojen lokia voidaan tarkastella tarkistuksen jälkeen.

Jos vain osa levystä halutaan tarkistaa, valitse **Mukautettu tarkistus** ja valitse sitten kohteet, joista etsitään haittaohjelmia.

Seuraavassa on kuvattu esimerkki tartunnan käsittelystä ESET Endpoint Security for macOS -ohjelmassa. Ensin reaaliaikainen tiedostojärjestelmän tarkkailutoiminto havaitsee tartunnan oletuspuhdistustasoa käyttämällä. Reaaliaikainen suojaus yrittää puhdistaa tai poistaa tiedoston. Jos reaaliaikaisella suojausmoduulilla ei ole käytettävissä ennalta määritettyä toimintoa, käyttäjää pyydetään valitsemaan toiminto hälytysikkunasta. Yleensä valittavana on **Puhdista**-, **Poista**- ja **Ei toimintoa** -toiminnot. **Ei toimintoa** -toiminnon valitseminen ei ole suositeltavaa, sillä tällöin tartunnan saaneet tiedostot jäävät tähän tilaan. Tämä asetus on tarkoitettu vain tilanteisiin, joissa voidaan olla varmoja siitä, että tiedosto on vaaraton ja että tarkistustoiminto on määrittänyt sen virheellisesti vahingolliseksi.

Puhdistaminen ja poistaminen

Puhdistustoimintoa tulee käyttää, jos tiedostossa on virustartunta, joka on lisännyt haittaohjelmaa tiedostoon. Tässä tapauksessa kannattaa ensin yrittää puhdistaa viruksen tartuttama tiedosto ja palauttaa se alkuperäiseen tilaansa. Jos tiedosto sisältää vain haitallista koodia, se poistetaan.

Arkistoissa olevien tiedostojen poistaminen

Oletuspuhdistustilassa koko arkisto poistetaan vain, jos se sisältää ainoastaan viruksen tartuttamia tiedostoja. Toisin sanoen arkistoja ei poisteta, jos niissä on myös vaarattomia, puhtaita tiedostoja. Tarkkaa puhdistustarkistusta tulee käyttää harkiten. **Tarkka puhdistus** poistaa arkiston, jos se sisältää yhdenkin tartunnan saaneen tiedoston, muiden arkiston tiedostojen tilasta riippumatta.

Internet- ja sähköpostisuojaus

Voit käyttää Internetin ja sähköpostin suojausta valitsemalla päävalikosta **Asetukset > Internet ja sähköposti**. Tästä voit myös käyttää kunkin moduulin yksityiskohtaisia asetuksia valitsemalla **Asetukset**.



Tarkistuspoikkeukset

ESET Endpoint Security for macOS ei tarkista salattuja HTTPS-, POP3S- ja IMAPS-protokollia.

- **Internetin käytön suojaus** – valvoo Web-selaimien ja etäpalvelinten välistä HTTP-liikennettä.
- **Sähköpostisovelluksen suojaus** – tämän avulla voi hallita POP3- ja IMAP-protokollien kautta vastaanotettavaa sähköpostiliikennettä.
- **Tietokalastelun esto** – estää sivustoista tai toimialueilta tulevat mahdolliset tietokalasteluhyökkäykset.
- **Internetin hallinta** – estää verkkosivut, joilla voi olla asiatonta tai haitallista materiaalia.

Internet-käytön suojaus

Internet-käytön suojaus valvoo, että Web-selaimien ja etäpalvelinten välinen tietoliikenne noudattaa HTTP (Hypertext Transfer Protocol) -sääntöjä.

Web-suodatuksen voi asettaa määrittämällä [HTTP-liikenteen käyttämät porttinumerot](#) ja/tai [URL-osoitteet](#).

Portit

Portit-välilehdessä voit määrittää HTTP-tietoliikenteessä käytettävät porttinumerot. Oletusarvoisesti ennalta määritetyt porttinumerot ovat 80, 8080 ja 3128.

URL-osoiteluettelot

URL-osoiteluettelot-osassa voi määrittää estettävät, sallittavat ja tarkistuksesta pois jätettävät HTTP-osoitteet. Estettyjen osoitteiden luettelossa olevia Web-sivustoja ei voi avata. Pois jätettyjen osoitteiden luettelossa olevat Web-sivustot avataan tarkistamatta niitä haittaohjelmien varalta.

Jos haluat sallia vain **Sallittujen URL-osoitteiden** luettelossa olevat URL-osoitteet, valitse **Rajoita URL-osoitteita**.

Voit ottaa luettelon käyttöön valitsemalla luettelon nimen vierestä **Käytössä**. Jos haluat ilmoituksen, kun avaat luettelossa olevaa osoitetta, valitse **Ilmoitettu**.

Erikoismerkkejä * (tähti) ja ? (kysymysmerkki) voidaan myös käyttää URL-luetteloiden kokoamisessa. Tähtimerkillä

voi korvata minkä tahansa merkkijonon ja kysymysmerkillä minkä tahansa merkin. Pois jätettäviä osoitteiden määrittäessä pitää toimia erityisen huolellisesti, koska luetteloon saa lisätä vain luotettuja ja turvallisia osoitteita. Samaan tapaan on varmistettava, että merkkejä * ja ? käytetään oikein tässä luettelossa.

Sähköpostisuojaus

Sähköpostisuojauksen avulla voit hallita POP3- ja IMAP-protokollien kautta vastaanotettavaa sähköpostiliikennettä. Saapuvien viestien tarkistuksessa ESET Endpoint Security for macOS käyttää kaikkia ThreatSense-tarkistusmoduulin kehittyneitä tarkistustapoja. POP3- ja IMAP-protokollaliikenteen tarkistus tehdään aina, kun jotakin sähköpostiohjelmaa käytetään.

ThreatSense-ohjelma: Asetukset – Kehittyneen virustarkistuksen asetuksissa voit määrittää esimerkiksi tarkistuksen kohteet ja tunnistusmenetelmät jne. Voit tuoda yksityiskohtaiset tarkistusasetukset sisältävän ikkunan näkyviin valitsemalla **Asetukset**.

Lisää tunnisteviestit sähköpostin alatunnisteeseen – Kun sähköposti on tarkistettu, viestiin voidaan lisätä ilmoitus tarkistuksen tuloksista. Tunnisteviesteihin ei voi luottaa ainoana keinona, koska ne saatetaan jättää pois ongelmallisissa HTML-viesteissä ja koska jotkin virukset voivat väärentää niitä. Käytettävissäsi ovat seuraavat asetukset:

- **Ei koskaan** – tunnisteviestejä ei lisätä
- **Vain tartunnan saaneisiin sähköposteihin** – vain haitallisia ohjelmistoja sisältävät viestit merkitään tarkistetuiksi
- **Kaikkiin tarkistettuihin sähköposteihin** – ESET Endpoint Security for macOS liittää viestit kaikkiin tarkistettuihin sähköposteihin

Lisää huomautus viruksen tartuttamien vastaanotettujen ja luettujen viestien otsikkoon – Valitse tämä, jos haluat lisätä virusvaroituksen viruksen tartuttamiin sähköpostiviesteihin. Tämän toiminnon avulla tartunnan saaneita sähköposteja voi suodattaa kätevästi. Se lisää vastaanottajan uskottavuutta, ja jos tartunta havaitaan, se sisältää arvokkaita tietoja tietyn sähköpostin tai lähettäjän uhkatasosta.

Tartunnan sisältäneen sähköpostin aiheeseen lisätty malli – voit muokata tätä mallia, jos haluat muokata tartunnan saaneen sähköpostin aiheen etuliitteen muotoa.

- %avstatus% – Lisää sähköpostitartunnan tilan (esim. puhdistettu, tartunta...)
- %virus% – Lisää uhkan nimen
- %product% – Lisää ESET-tuotteen nimen (tässä tapauksessa ESET Endpoint Security for macOS)
- %product_url% – Lisää ESET-verkkosivuston linkin (www.eset.com)

Ikkunan alaosassa voit myös ottaa käyttöön tai poistaa käytöstä POP3- ja IMAP-protokollien kautta vastaanotettavan sähköpostiliikenteen tarkistuksen. Lisätietoja on seuraavissa aiheissa:

- [POP3-protokollan tarkistus](#)
- [IMAP-protokollan tarkistus](#)

POP3-protokollan tarkistus

POP3-protokolla on laajalti käytössä oleva protokolla, jolla vastaanotetaan sähköpostiviestejä sähköpostiasiakasohjelmalla. ESET Endpoint Security for macOS suojaa tätä protokollaa riippumatta siitä, mikä sähköpostiasiakasohjelma on käytössä.

Tämän toiminnon sisältävä suojausmoduuli käynnistetään automaattisesti järjestelmän käynnistyksen yhteydessä, ja se on sitten aktiivisena muistissa. Moduulin asianmukainen toiminta edellyttää, että se on otettu käyttöön; POP3-protokollatoiminto suoritetaan automaattisesti ilman, että sähköpostisovellusta tarvitsee määrittää uudelleen. Oletusarvon mukaan kaikki portin 110 tietoliikenne tarkistetaan, mutta muita tietoliikenneportteja voi lisätä tarvittaessa. Porttien numerot on eroteltava toisistaan pilkuilla.

Jos **Ota POP3-protokollan tarkistus käyttöön** on valittuna, kaikkea POP3-tietoliikennettä valvotaan haittaohjelmien varalta.

IMAP-protokollan tarkistus

(IMAP) (Internet Message Access Protocol) on toinen sähköpostin noutamiseen käytettävä Internet-protokolla. IMAP-protokollalla on joitain etuja POP3:een nähden. Useat sähköpostisovellukset voivat esimerkiksi yhdistää samaan sähköpostilaatikkoon ja ylläpitää viestien tilatietoja kuten viestien merkitsemistä luetuksi, vastatuksi ja viestien poistamista. ESET Endpoint Security for macOS suojaa tämän protokollan sähköpostisovelluksesta riippumatta.

Tämän toiminnon sisältävä suojausmoduuli käynnistetään automaattisesti järjestelmän käynnistyksen yhteydessä, ja se on sitten aktiivisena muistissa. Moduulin asianmukainen toiminta edellyttää, että se on otettu käyttöön; IMAP-protokollatoiminto suoritetaan automaattisesti ilman, että sähköpostisovellusta tarvitsee määrittää uudelleen. Oletusarvon mukaan kaikki portin 143 tietoliikenne tarkistetaan, mutta muita tietoliikenneportteja voi lisätä tarvittaessa. Porttien numerot on eroteltava toisistaan pilkuilla.

Jos **Ota IMAP-protokollan tarkistus käyttöön** on valittuna, kaikkea IMAP-tietoliikennettä valvotaan haittaohjelmien varalta.

Tietojenkalastelusuojaus

Käsitteellä tietojenkalastelu tarkoitetaan rikollista toimintaa, jossa käytetään hyväksi sosiaalista manipulointia (käyttäjän manipulointia luottamuksellisten tietojen saamiseksi). Tietojenkalastelulla pyritään usein hankkimaan pääsy arkaluonteisiin tietoihin kuten pankkitilinumeroihin, luottokorttinumeroihin, PIN-koodeihin tai käyttäjänimiin ja salasanoihin.

Tietojenkalastelusuojaus (**Asetukset > Anna sovelluksen oletusasetukset... > Tietojenkalastelusuojaus**)

kannattaa ottaa käyttöön. Kaikki vaarallisista sivustoista tai vaarallisilta toimialueilta tulevat mahdolliset tietojenkalasteluhyökkäykset estetään, ja hyökkäyksestä ilmaiseva varoitus tulee näkyviin.

Palomuuuri

Palomuuuri ohjaa kaikkea järjestelmään tulevaa ja siitä lähtevää verkkotietoliikennettä sallimalla tai estämällä yksittäisiä verkkoyhteyksiä määritettyjen suodatussääntöjen perusteella. Se suojaaa järjestelmää etätietokoneiden hyökkäyksiltä ja mahdollistaa joidenkin palvelujen estämisen. Se sisältää myös HTTP-, POP3- ja IMAP-protokollien virustentorjunnan.



Tarkistuspoikkeukset

ESET Endpoint Security for macOS ei tarkista salattuja HTTPS-, POP3S- ja IMAPS-protokollia.

Palomuurikokoonpano on **Asetukset**-valikossa kohdassa **Palomuuuri**. Voit säätää suodatustilaa, sääntöjä ja yksityiskohtaisia asetuksia. Tästä voit myös käyttää ohjelman yksityiskohtaisia asetuksia.

Jos otat käyttöön **Estä kaikki verkkoliikenne: katkaise verkkoyhteys**, palomuuuri estää kaiken saapuvan ja lähtevän tietoliikenteen. Käytä tätä asetusta vain silloin, jos epäilet vakavien tietoturvariskien vaativan järjestelmän verkkoyhteyden katkaisemista.

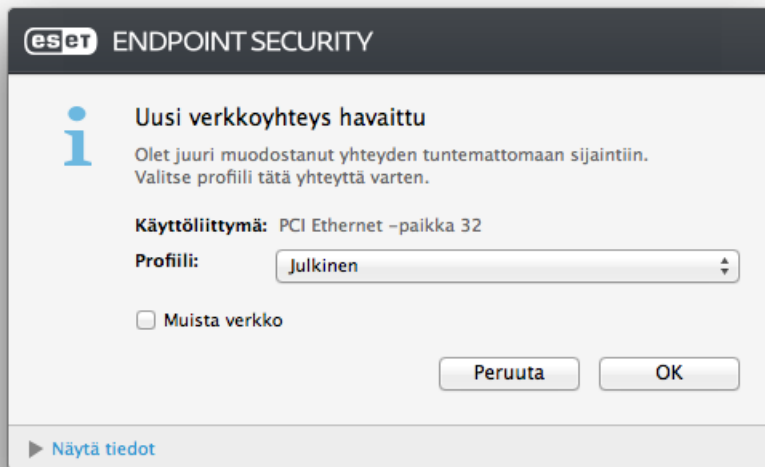
Suodatustilat

Ohjelman ESET Endpoint Security for macOS palomuurille on saatavilla kolme suodatustilaa. Suodatustilan asetukset ovat osiossa Asetukset > **Anna sovelluksen oletusasetukset...** > **Palomuuuri**. Palomuurin toiminta muuttuu valitun tilan mukaan. Suodatustilat vaikuttavat myös tarvittaviin käyttäjätoimiin.

Kaikki liikenne on estetty – kaikki saapuvat ja lähtevät yhteydet estetään.

Automaattinen ja poikkeukset – Oletustila. Tämä tila soveltuu käyttäjille, jotka suosivat vaivatonta tapaa käyttää palomuuria ilman sääntömäärittämiä. Automaattisessa tilassa sallitaan tietyn järjestelmän lähtevä vakioliikenne ja estetään kaikki verkon puolelta tulevat yhteydet, joita käyttäjä ei ole aloittanut. Voit myös lisätä mukautettuja, käyttäjän määrittämiä sääntöjä.

Vuorovaikutteinen – Voit muodostaa mukautettuja määrittämiä palomuuria varten. Kun tietoliikennettä havaitaan, eikä sille ole olemassa sääntöjä, näkyviin tulee valintaikkuna, joka ilmoittaa tuntemattomasta yhteydestä. Valintaikkunassa voidaan sallia tai estää tietoliikenne, ja päätös sallia tai estää tietoliikenne voidaan muistaa uutena palomuurin sääntönä. Jos päätät luoda uuden säännön, kaikki samantyyppiset tulevat yhteydet sallitaan tai estetään säännön mukaan.



Jos haluat tallentaa yksityiskohtaisia tietoja estetyistä yhteyksistä lokitiedostoon, valitse **Kirjaa kaikki estetyt yhteydet**. Voit tarkistaa palomuurin lokitiedostot valitsemalla päävalikosta **Työkalut > Lokit** ja valitsemalla avattavasta **Loki**-valikosta **Palomuri**.

Palomuurisäännöt

Säännöt edustavat ehtojen ryhmää, jonka avulla voidaan testata kaikkia verkkoyhteyksiä ja päättää ehtoihin liittyviä toimenpiteitä. Palomuurisäännöillä voit määrittää, millaisia toimenpiteitä on tehtävä, jos säännön määrittämä yhteys muodostetaan.

Saapuvissa yhteyksissä etätietokone yrittää muodostaa yhteyden paikalliseen järjestelmään. Lähtevät yhteydet toimivat vastakkaisella tavalla – paikallinen järjestelmä muodostaa yhteyden etätietokoneeseen.

Jos uusi tuntematon yhteys havaitaan, sen sallimista tai estämistä on harkittava huolellisesti. Ei-toivotut, suojaamattomat tai tuntemattomat yhteydet voivat vaarantaa järjestelmän turvallisuuden. Jos tällainen yhteys muodostetaan, suosittelemme erityisen huomion kiinnittämistä etätietokoneeseen ja yhteyden muodostamista yrittävään sovellukseen. Monissa tietomurroissa yritetään hankkia ja lähettää yksityisiä tietoja tai ladata haitallisia sovelluksia isäntinä toimiviin työasemiin. Palomuurin avulla voit havaita ja katkaista tällaiset yhteydet.

Salli Applen allekirjoittaman ohjelmiston käyttää verkkoa automaattisesti – Oletusarvon mukaan Applen allekirjoittamat sovellukset voivat käyttää verkkoa automaattisesti. Jotta sovellus voi olla vuorovaikutuksessa Applen palvelujen kanssa tai jotta sovelluksen voi asentaa laitteisiin, kyseinen sovellus on allekirjoitettava Applen myöntämällä varmenteella. Jos haluat poistaa tämän käytöstä, poista asetuksen valinta käytöstä. Jos sovellusta ei ole allekirjoitettu Applen varmenteella, verkon käyttö edellyttää käyttäjän toimia tai sääntöä.

Jos tämä asetus on poistettu käytöstä, verkkoyhteys Applen allekirjoitamiin palveluihin edellyttää käyttäjän hyväksyntää, ellei sitä ole määritetty palomuurisäännöllä.

Aiempiin versioihin, tuotteeseen ESET Endpoint Security for macOS 6.8 ja vanhempiin, tehdyt muutokset estivät saapuvan tietoliikenteen Apple-varmennetta käyttäviin palveluihin. Nykyinen tuotteen ESET Endpoint Security for macOS versio tunnistaa saapuvan tietoliikenteen paikallisen vastaanottajan, ja jos tämä asetus on käytössä, saapuva tietoliikenne sallitaan.

Uusien sääntöjen luominen

Säännöt-välilehti sisältää luettelon kaikista yksittäisten sovellusten muodostamassa liikenteessä käyttöön otetuista säännöistä. Säännöt lisätään automaattisesti uuden tietoliikenteen saaman käyttäjäpalautteen perusteella.

1. Voit luoda uuden säännön napsauttamalla **Lisää...** Anna sitten säännölle nimi ja vedä ja pudota sovelluksen kuvake tyhjään kenttään tai napsauta **Selaa**, jos haluat etsiä ohjelman */Applications*-kansioista. Voit ottaa säännön käyttöön kaikissa tietokoneeseen asennetuissa sovelluksissa valitsemalla **Kaikki sovellukset**.
2. Määritä seuraavassa ikkunassa **Toiminto** (salli tai estä valitun sovelluksen ja verkon välinen tietoliikenne) ja tietoliikenteen **Suunta** (saapuva, lähtevä tai molemmat). Tallenna kaikki tätä sääntöä käyttävät yhteydet valitsemalla **Kirjaa sääntö**. Voit tarkastella palomuurin lokitiedostoja valitsemalla **Työkalut > Lokit** ohjelman ESET Endpoint Security for macOS pääikkunasta ja valitsemalla **Loki**-alasvetovalikosta **Palomuuuri**.
3. Aseta **Protokolla/portit**-osiossa protokolla ja portti, jota sovellus käyttää (jos TCP- tai UDP-protokolla on valittuna) tietoliikenteeseen. Siirtoprotokollataso suojaa ja tehostaa tiedonsiirtoa.
4. Määritä lopuksi säännölle **Kohde**-asetuksen ehdot (IP-osoite, alue, aliverkko, Ethernet tai Internet).

Palomuurivyöhykkeet

Vyöhyke vastaa kokoelmaa verkko-osoitteita, jotka muodostavat yhden loogisen ryhmän. Kullekin tietyn ryhmän osoitteelle määritetään samankaltaiset säännöt, jotka on määritetty keskitetysti koko ryhmälle.

Näitä vyöhykkeitä voi luoda napsauttamalla **Lisää**. Anna vyöhykkeelle **Nimi** ja **Kuvaus** (valinnainen), valitse profiili, johon tämä vyöhyke kuuluu, ja lisää IPv4-/IPv6-osoite, osoitealue, aliverkko, WiFi-verkko tai liittymä.

Palomuuriprofiilit

Profiilien avulla voit hallita ohjelman ESET Endpoint Security for macOS palomuurin toimintaa. Kun luot tai muokkaat palomuurin sääntöä, määrität sen tietylle profiilille. Kun valitset profiilin, vain yleiset säännöt (joille ei ole määritetty profiilia) ja kyseiselle profiilille määritetyt säännöt otetaan käyttöön. Voit luoda useita profiileja eri säännöillä, jolloin voit muuttaa palomuurin toimintaa vaivattomasti.

Palomuurilokit

Tuotteen ESET Endpoint Security for macOS palomuuuri tallentaa kaikki tärkeät tapahtumat lokitiedostoon. Pääset palomuurin lokitiedostoihin valitsemalla päävalikosta **Työkalut > Lokit** ja valitsemalla sitten avattavasta **Loki**-valikosta **Palomuuuri**.

Lokitiedostot ovat hyvä väline virheiden tunnistamiseen ja järjestelmään tehtyjen tunkeutumisten paljastamiseen. ESETin palomuuuri kirjaa seuraavat tiedot:

- Tapahtuman päivämäärä ja aika
- Tapahtuman nimi
- Lähde
- Kohdeverkko-osoite
- Verkon tietoliikenneprotokolla
- Sääntöä käytetty
- Sovellus, johon tapahtuma liittyy
- Käyttäjä

Näiden tietojen perusteellinen analyysi auttaa havaitsemaan tapahtumat, jotka voivat heikentää järjestelmän suojausta. Monet muut tekijät viittaavat mahdollisiin tietoturvariskeihin. Niitä vastaan voi puolustautua palomuurilla ja niitä ovat esimerkiksi: tiheään muodostetut yhteydet tuntemattomista sijainneista, useat yritykset muodostaa yhteyksiä, tuntemattomien sovellusten tietoliikenne ja käytetyt epätavalliset porttien numerot.

Laitehallinta

Tuotteen ESET Endpoint Security for macOS avulla voit tarkistaa, estää tai säätää laajennettuja suodattimia ja lupia ja määrittää käyttäjän oikeudet muistilaitteen käytölle ja työskentelylle. Tämä on hyödyllistä, jos tietokoneen valvoja haluaa estää sellaisten laitteiden käytön, joissa on ei-toivottua sisältöä.

Laitehallinta macOS 11:ssä ja uudemmissa



ESET Endpoint Security for macOS, joka on asennettu macOS 11:een ja uudempiin, voi tarkistaa vain tallennusvälineitä (kuten USB-asemia ja CD-/DVD-levyjä).

macOS 10.15:ssä ja vanhemmissa tuetut ulkoiset laitteet:

- Levytila (HDD, USB-flash-asema)
- CD/DVD
- USB-tulostin
- Kuvankäsittelylaite
- Sarjaportti
- Verkko
- Kannettava laite




Jos koneeseen asetetaan laite, jonka estää jokin olemassa oleva sääntö, näkyviin tulee ilmoitusikkuna, eikä laitetta voi käyttää.

Laitehallintalokiin tallennetaan tiedot kaikista tapahtumista, jotka laukaisevat laitehallinnan. Lokimerkintöjä voi tarkastella tuotteen ESET Endpoint Security for macOS pääohjelmistoikkunassa kohdassa **Työkalut** > [Lokitiedostot](#).

Sääntöeditori

Laitehallinnan asetuksia voi muokata kohdassa **Asetukset** > **Anna sovelluksen oletusasetukset...** > **Laitehallinta**.

Ota laitehallinta käyttöön -valinta aktivoi tuotteen ESET Endpoint Security for macOS laitehallintaominaisuuden. Kun laitehallinta on käytössä, voit hallita ja muokata laitehallintarooleja. Voit poistaa säännön käytöstä poistamalla säännön nimen vieressä olevan valintaruudun valinnan.

 ja  -painikkeilla voit lisätä ja poistaa sääntöjä. Säännöt ovat luettelossa tärkeysjärjestyksessä niin, että etusijalla olevat säännöt ovat lähempänä yläpäättä. Voit muuttaa sääntöjen järjestystä vetämällä ja pudottamalla haluamasi säännön uuteen paikkaan ja valitsemalla ensin  ja sitten jonkin vaihtoehtoista.

ESET Endpoint Security for macOS tunnistaa automaattisesti kaikki asennettuna olevat laitteet ja niiden parametrit (kuten laitteen tyyppi, toimittaja, malli ja sarjanumero). Sen sijaan, että loisit säännöt manuaalisesti, voit luoda säännön valitsemalla **Täytä**, valitsemalla laitteen ja valitsemalla sitten **Jatka**.

Tiettyjä laitteita voidaan sallia tai estää käyttäjä- tai käyttäjäryhmäkohtaisesti tai minkä tahansa useista muista sääntökokoonpanoon määritettävien lisälaiteparametrien perusteella. Sääntöluettelossa on useita sääntökuvauksia, kuten nimi, laitteen tyyppi, kirjausvakavuus ja laitteen tietokoneeseen liittämisen jälkeen suoritettava toiminto.

Nimi

Kirjoita säännön kuvaus **Nimi**-kenttään, jotta helpotat tunnistusta. **Sääntö käytössä** -valintaruudun valitseminen poistaa tämän säännön käytöstä tai ottaa sen käyttöön. Tästä voi olla hyötyä, jos et halua poistaa sääntöä pysyvästi.

Laitteen tyyppi

Valitse ulkoisen laitteen tyyppi avattavasta valikosta. Laitetyyppitiedot kerätään käyttöjärjestelmästä. Tallennuslaitteita ovat USB:n tai FireWiren kautta liitetyt ulkoiset levyt ja tavanomaiset muistikortinlukijat. Kuvankäsittelylaitteita ovat esimerkiksi skannerit ja kamerat. Koska nämä laitteet antavat tietoja vain niiden toimenpiteistä eivätkä käyttäjistä, ne voi estää globaalisti.

Toimenpide

Muiden kuin tallennuslaitteiden käyttö voidaan sallia tai estää. Tallennuslaitteiden säännöt mahdollistavat vastaavasti jonkin seuraavan oikeusasetuksen valitsemisen:

Luku/kirjoitus – Laitteen täysimittainen käyttö sallitaan.

Vain luku – Vain laitteesta lukeminen sallitaan.

Estä – Laitteen käyttö estetään.

Kriteerityyppi

Valitse **Laiteryhmä** tai **Laite**. Sääntöjä voi hienosäätää ja räätelöidä laitekohtaisesti muilla, alla esitellyillä parametreilla.

Toimittaja – Suodatus toimittajan nimen tai tunnuksen mukaan.

Malli – Laitteelle annettu nimi.

Sarjanumero – Ulkoisilla laitteilla on yleensä omat sarjanumeronsa. CD-/DVD-levyissä tämä on kyseisen tietovälineen, ei CD/DV-aseman, sarjanumero.

Ei määritettyjä parametreja

i Jos näitä parametreja ei ole määritetty, sääntö jättää nämä kentät huomiotta täsmäystä tehdessä. Tekstikentissä olevat suodatusparametrit eivät erota isoja ja pieniä kirjaimia, eikä yleismerkkejä (* ja ?) tueta.

VIHJE

i Voit tarkastella laitteen tietoja luomalla laitteen tyyppille säännön ja yhdistämällä laitteen tietokoneeseesi. Yhdistetyn laitteen tiedot näkyvät [laitehallintalokissa](#).

Kirjaamisen vakavuus

Aina – Kirjaa kaikki tapahtumat.

Vianmäärittystiedot – Kirjaa tietoa, jota tarvitaan ohjelman hienosäätämiseen.

Tiedot – Kirjaa informatiiviset viestit ja kaikki edellä luetellut tiedot.

Varoitus – Kirjaa vakavat virheet ja varoitusviestit.

Ei mitään – Mitään lokitietoja ei kirjata.

Käyttäjäluettelo

Säännöt voidaan rajata tietyille käyttäjille tai käyttäjäryhmille lisäämällä ne käyttäjäluetteloon:

Muokkaa... – Avaa **identiteettieditorin**, jossa voit valita käyttäjät tai ryhmät. Käyttäjien luettelon voi määrittää valitsemalla heidät vasemmalla puolella olevasta **Käyttäjät**-luettelosta ja valitsemalla **Lisää**. Käyttäjän voi poistaa valitsemalla hänen nimensä **Valitut käyttäjät** -luettelosta ja valitsemalla **Poista**. Voit tuoda järjestelmän kaikki käyttäjät näkyviin valitsemalla **Näytä kaikki käyttäjät**. Jos luettelo on tyhjä, kaikilla käyttäjillä on käyttöoikeus.

Käyttäjäsääntörajoitukset

! Kaikkia laitteita ei voi rajoittaa käyttäjäsäännöillä (esimerkiksi kuvankäsittelylaitteet eivät anna tietoja käyttäjästä vaan ainoastaan toimista).


Internetin hallinta

Internetin hallinta -ominaisuuden avulla voit määrittää asetukset, jotka suojaavat yritystäsi laillisen vastuun aiheuttamilta riskeiltä. Internetin hallinta voi valvoa sellaisten web-sivujen käyttöä, jotka rikkovat immateriaalioikeuksia. Tarkoituksena on estää työntekijöiltä pääsy sivuille, joilla on sopimatonta tai haitallista sisältöä tai jotka saattavat vaikuttaa tehoon negatiivisesti. Työnantajat tai järjestelmänvalvojat voivat estää jopa

yli 27 ennalta määritetyn Web-sivustoluokan ja yli 140 alaluokan käytön.

Internetin hallinta on oletusarvoisesti pois käytöstä. Voit ottaa sen käyttöön valitsemalla **Asetukset > Anna sovelluksen oletusasetukset > Internetin hallinta** ja valitsemalla sitten **Ota Internetin hallinta käyttöön - valintaruudun**.

Sääntöeditori-ikkunassa näytetään olemassa olevat, URL- tai Luokkakohtaiset säännöt. Sääntöluettelossa on useita sääntökuvauksia, kuten nimi, estotyyppi, suoritettava toiminto Internetin hallinnan säännön vahvistamisen jälkeen ja [lokin](#) kirjausvakavuus.

Voit luoda uuden säännön napsauttamalla painiketta . Jotta tunnistaminen olisi helpompaa, kaksoisnapsauta **Nimi**-kenttää ja kirjoita säännön kuvaus.

Käytössä-kentässä olevan valintaruudun avulla voit ottaa säännön käyttöön tai poistaa sen käytöstä. Tästä voi olla hyötyä, jos haluat käyttää sääntöä myöhemmin, etkä halua poistaa sitä pysyvästi.

Tyyppi

URL-perustainen toimenpide – Tietyn Web-sivuston käyttöoikeus. Kaksoisnapsauta **URL-/Luokka**-kenttää ja kirjoita asianmukainen URL-osoite.

URL-osoiteluettelossa ei voi käyttää erikoismerkkejä * (tähtimerkki) ja ? (kysymysmerkki). Useita TLD-määrittäjiä sisältävät Web-sivuosoitteet on kirjoitettava luotuun ryhmään (*esimerkkisivu.com*, *esimerkkisivu.sk* jne.). Kun lisäät toimialueen luetteloon, kaikki tällä toimialueella ja kaikilla alialueilla (esimerkiksi *ali.esimerkkisivu.com*) oleva sisältö estetään tai sallitaan tekemäsi URL-pohjaisen toimenpiteen perusteella.

Luokkaperustainen toimenpide – kaksoisnapsauta **URL-/Luokka**-kenttää ja valitse luokat.

Identiteetti

Tämän avulla voit valita käyttäjät, joita sääntö koskee.

Käyttöoikeudet

Salli – URL-osoitteen/luokan käyttöoikeus myönnetään.

Estä – URL-osoite tai luokka estetään.

Vakavuus (lokitiedostojen [suodattamiselle](#))

Aina – Kirjaa kaikki tapahtumat.

Vianmäärittystiedot – Kirjaa tietoa, jota tarvitaan ohjelman hienosäätämiseen.

Tiedot – Kirjaa informatiiviset viestit ja kaikki edellä luetellut tiedot.

Varoitus – Kirjaa vakavat virheet ja varoitusviestit.

Ei mitään – Mitään lokitietoja ei luoda.

Työkalut

Työkalut-valikko sisältää moduulit, jotka helpottavat ohjelmien hallintaa ja tuovat lisäasetuksia kehittyneiden käyttäjien käyttöön.

Lokitiedostot

Lokitiedostot sisältävät tietoja kaikista tärkeistä ohjelmatapahtumista ja yleistietoja havaituista uhkista. Lokitallennus on välttämätöntä järjestelmän analysoinnin, uhkien tunnistamisen ja vianmäärityksen kannalta. Kirjaaminen suoritetaan aktiivisesti taustalla, eikä se edellytä käyttäjän toimia. Tiedot tallennetaan nykyisten lokin sisältöasetusten mukaan. Tekstiviestejä ja lokeja voi tarkastella suoraan ESET Endpoint Security for macOS -ympäristössä. Siellä lokeja voi myös arkistoida.

Lokitiedostot voidaan avata valitsemalla ESET Endpoint Security for macOS -ohjelman päävalikosta **Työkalut > Lokitiedostot**. Valitse haluamasi lokityyppi avattavasta Loki-valikosta ikkunan yläosassa. Käytettävissä ovat seuraavat lokit:

1. **Havaitut uhat** – tartuntojen tunnistamiseen liittyvien tapahtumien tiedot.
2. **Tapahtumat** – kaikki tuotteen ESET Endpoint Security for macOS tekemät tärkeät toimet kirjataan tapahtumalokiin.
3. **Tietokoneen tarkistus** – Kaikkien tehtyjen tarkistusten tulokset näkyvät tässä ikkunassa. Kaksoisnapsauttamalla mitä tahansa merkintää voit tarkastella yksittäisen tietokoneen tarkistuksen tietoja.
4. **Laitehallinta** – Sisältää tiedot tietokoneeseen liitetystä siirrettävistä tietovälineistä ja laitteista. Vain laitteet, joilla on laitehallinnan sääntö, tallennetaan lokitiedostoon. Jos sääntö ei vastaa liitettyä laitetta, liitetyn laitteen lokimerkintää ei luoda. Tässä on myös lisätietoja, kuten laitteen tyyppi, sarjanumero, toimittajan nimi ja tietovälineen koko (jos saatavilla).
5. **Palomuuuri** – Palomuurin loki näyttää kaikki palomuurin tunnistamat etähyökkäykset. Palomuurin lokeissa on tiedot kaikista tietokonetta vastaan tehdyistä havaituista hyökkäyksistä. **Tapahtuma**-sarakkeessa on luettelo havaituista hyökkäyksistä, **Lähde**-sarakkeessa hyökkääjän tiedot ja **Protokolla**-sarakkeessa hyökkäyksessä käytetty yhteysprotokolla.
6. **Internetin hallinta** – näyttää estetyt tai sallitut URL-osoitteet ja tietoja siitä, miten ne on luokiteltu.
7. **Suodatetut Internet-sivustot** – Tämä loki sisältää luettelon kaikista Internet-sivustoista, joiden käytön on estänyt [Internetin käytön suojaus](#) tai [Internetin hallinta](#). Näistä lokeista näet Internet-sivustoyhteyden luomisen ajan, URL-osoitteen, IP-osoitteen, yhteyden muodostaneen käyttäjän ja käytetyn sovelluksen.

Voit kopioida minkä tahansa lokitiedoston sisällön leikepöydälle napsauttamalla lokitiedostoa hiiren kakkospainikkeella ja valitsemalla **Kopioi**.

Lokin ylläpito

Tuotteen ESET Endpoint Security for macOS lokikirjauksen asetukset ovat käytettävissä ohjelman pääikkunassa. Valitse **Asetukset > Anna sovelluksen oletusasetukset > Työkalut > Lokitiedostot**. Voit valita seuraavat asetukset lokitiedostoille:

- **Poista vanhat lokitietueet automaattisesti** – määritettyä enimmäisikää vanhemmat lokimerkinnot poistetaan automaattisesti.
- **Optimoi lokitiedostot automaattisesti** – lokitiedostot voidaan eheyttää automaattisesti, jos käyttämättömien tietueiden määritetty prosenttiluku ylittyy.

Kaikki graafisessa käyttöliittymässä ja uhka- ja virheilmoituksissa esitetyt tarpeelliset tiedot voidaan tallentaa luettavaan muotoon, esimerkiksi tekstitiedostoina tai CSV-tiedostoina (Comma-separated values). Jos haluat, että näitä tiedostoja voidaan käsitellä kolmannen osapuolen välineillä, napsauta valintaruutua kohdassa **Ota kirjaus tekstitiedostoihin käyttöön**.

Kansio, johon lokitiedostot tallennetaan, määritetään napsauttamalla **Asetukset** kohdan **Lisäasetukset** vieressä.

Niiden asetusten mukaan, jotka valittiin kohdassa **Tekstilokitiedostot: Muokkaa**, voit tallentaa lokeja, joihin on kirjoitettu seuraavat tiedot:

- Tapahtumat, kuten *Virheellinen käyttäjänimi tai salasana, Moduuleja ei voitu päivittää* jne. kirjataan *eventslog.txt*-tiedostoon.
- Käynnistystarkastuksen, reaaliaikaisen suojauksen tai tietokoneen tarkistuksen poistamat uhat on tallennettu tiedostoon nimeltä *threatslog.txt*.
- Kaikkien tehtyjen tarkistusten tulokset tallennetaan *scanlog.NUMBER.txt*-muotoon.
- Laitehallinnan estämät laitteet on kirjattu lokitiedostoon *devctllog.txt*
- Kaikki tapahtumat, jotka liittyvät palomuurin kautta tapahtuvaan tiedonsiirtoon kirjataan lokitiedostoon *firewallog.txt*
- Internetin hallinnan estämät Internet-sivut kirjataan lokitiedostoon *webctllog.txt*

Voit määrittää suodattimet **tietokoneen tarkistuksen oletusarvoisille lokitietueille** valitsemalla **Muokkaa** ja valitsemalla tarvittavat lokityypit tai poistamalla niiden valinnan. Lisätietoja eri lokityypeistä löytyy [lokisuodatuksista](#).

Lokisuodatus

Lokeissa on tietoja tärkeistä järjestelmä tapahtumista. Lokisuodatus-ominaisuuden avulla voit tuoda näyttöön tiettyä tapahtumia käsitteleviä tietueita.

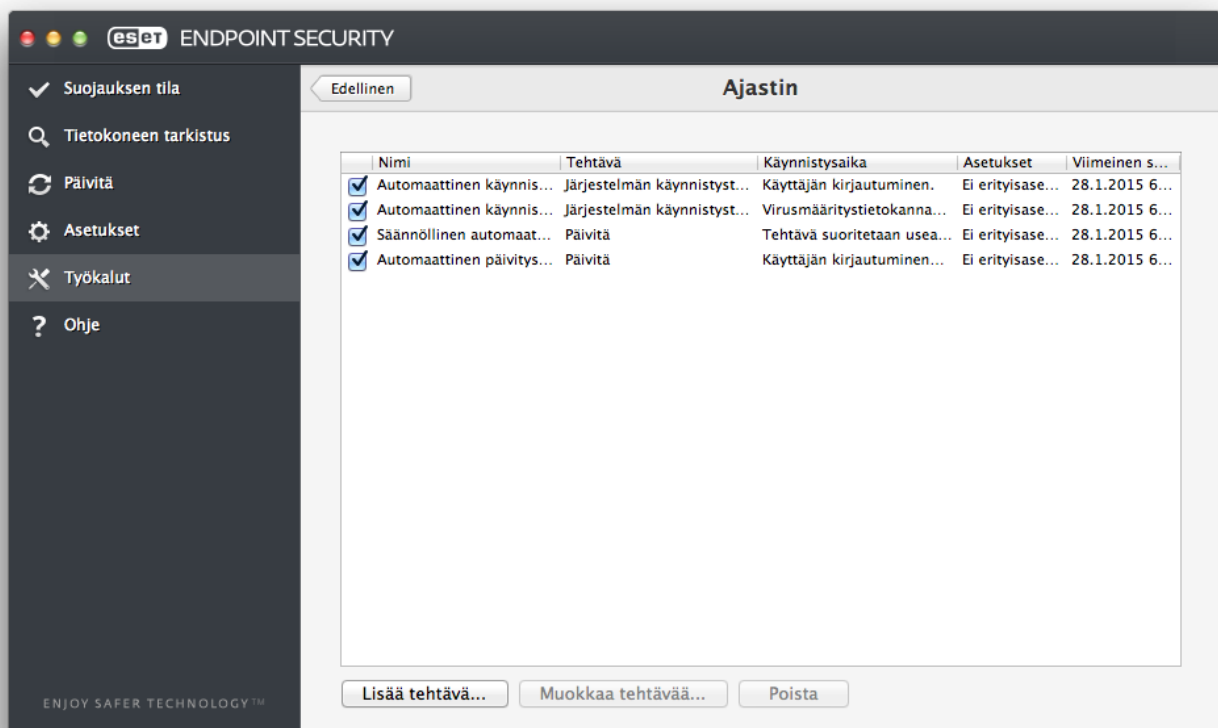
Useimmiten käytetyt lokityypit on eritelty alla:

- **Vakavat virheet** – vakavat järjestelmävirheet (kuten Virustentorjunta ei käynnistynyt).
- **Virheet** – Virhesanomien, esimerkiksi *tiedoston lataamisvirheet* ja vakavat virheet.

- **Varoitukset** – varoitusviestit
- **Informatiiviset tiedot** – Tiedotusviestit, kuten ilmoitukset onnistuneista päivityksistä ja hälytyksistä.
- **Vianmäärittystiedot** – ohjelman hienosäätöön tarvittavat tiedot sekä kaikki edellä mainitut tiedot.

Ajastin

Ajastin on ohjelman ESET Endpoint Security for macOS päävalikossa **Työkalut**-kohdassa. **Ajastin** sisältää luettelon kaikista ajoitetuista tehtävistä ja asetuksista, joita ovat esimerkiksi esimääritetty päivämäärä, kellonaika ja käytetty tarkistusprofiili.



Ajastinta käytetään kokoonpanoltaan ja ominaisuuksiltaan ennalta määritettyjen ajoitettujen tehtävien hallintaan ja käynnistämiseen. Kokoonpano ja ominaisuudet voivat sisältää erilaisia tietoja, kuten päivämäärän ja kellonajan sekä tehtävän suorittamisessa käytettävän profiilin.

Oletusarvoisesti seuraavat ajoitetut tehtävät näkyvät ajastimessa:

- Lokin ylläpito (kun **Näytä järjestelmätehtävät** on otettu käyttöön ajastimen asetuksissa)
- Käynnistystiedostojen tarkistus käyttäjän kirjautumisen jälkeen
- Käynnistystiedostojen tarkistus onnistuneen tunnistusmoduulien päivityksen jälkeen
- Säännöllinen automaattinen päivitys

- Automaattinen päivitys käyttäjän kirjautumisen jälkeen

Voit muokata aiemmin lisätyn ajoitetun (sekä oletusarvoisen että käyttäjän määrittämän) tehtävän asetuksia näppäinyhdistelmällä CTRL+napsautus, valitsemalla muokattavan tehtävän ja valitsemalla **Muokkaa** tai valitsemalla tehtävän ja napsauttamalla **Muokkaa tehtävää**.

Uusien tehtävien luominen

Jos haluat luoda uuden tehtävän ajastimessa, valitse **Lisää tehtävä** tai paina CTRL-näppäintä ja napsauta tyhjää kenttää ja valitse sitten pikavalikosta **Lisää**. Käytettävissä on neljä erityyppistä ajoitettua tehtävää:

- Sovelluksen suoritus
- Päivitys
- Tarvepohjainen tietokoneen tarkistus
- Järjestelmän käynnistystiedostojen tarkistus

Käyttäjän määrittämät tehtävät

- i** Oletusarvoisesti sovellukset suorittaa erityinen ESETin luoma käyttäjä, jolla on rajoitetut oikeudet. Jos haluat vaihtaa oletuskäyttäjän, kirjoita komennon edelle käyttäjänimi ja kaksoispiste (:). Voit käyttää myös pääkäyttäjän käyttäjänimeä **root** tässä toiminnossa.

Esimerkki: tehtävän suorittaminen käyttäjänä

Tässä esimerkissä laskinsovellus ajoitetaan käynnistymään valittuna ajankohtana käyttäjänimellä **UserOne**:

1. Valitse **ajastimessa Lisää tehtävä**.
2. Kirjoita tehtävän nimi. Valitse **Suorita sovellus** -asetukseksi **Ajoitettu tehtävä**. Määritä tehtävä suoritettavaksi vain kerran valitsemalla **Suorita tehtävä** -ikkunassa **Kerran**. Valitse **Seuraava**.
- ✓ 3. Valitse Selaa ja valitse sitten laskinsovellus.
4. Kirjoita **UserOne**: sovelluksen polun eteen (UserOne:'/Applications/Calculator.app/Contents/MacOS/Calculator') ja valitse **Seuraava**.
5. Valitse tehtävän suoritusaika ja valitse **Seuraava**.
6. Valitse vaihtoehtoinen valinta tilanteeseen, jossa tehtävän suoritus ei onnistu, ja valitse sitten **Seuraava**.
7. Napsauta **Valmis**-painiketta.
8. ESET-ajastin käynnistää laskinsovelluksen valittuna ajankohtana.

Käyttäjänimen rajoitukset

- !** Käyttäjänimen eteen ei saa asettaa välilyöntejä. Välilyöntejä ei voi käyttää myöskään itse käyttäjänimessä. Niiden sijaan on käytettävä tyhjämerkkejä.

Tarkistus hakemiston omistajana

Voit tarkistaa hakemistoja hakemiston omistajan käyttäjänimellä:

- i** root:for VOLUME in /Volumes/*; do sudo -u \#`stat -f %u "\$VOLUME" '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "\$VOLUME"; done

Voit myös tarkistaa /tmp-kansion kirjautuneena olevan käyttäjän käyttäjänimellä:

root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

Esimerkki: päivitystehtävä

Tässä esimerkissä luodaan määritettynä ajankohtana suoritettava päivitystehtävä.

1. Valitse **Ajoitettu tehtävä** -alasvetovalikosta **Päivitä**.
2. Kirjoita tehtävän nimi **Tehtävän nimi** -kenttään.
- ✓ 3. Valitse tehtävän suoritusväli avattavasta **Suorita tehtävä** -valikosta. Järjestelmä pyytää sinua määrittämään eri päivitysparametrit valitun suoritusvälin perusteella. Jos valitset **Käyttäjän määrittämä** -vaihtoehdon, saat kehoitteen määrittää päivämäärän/ajan cron-muodossa (lisätietoja on kohdassa [Käyttäjän määrittämän tehtävän luominen](#)).
4. Määritä vaihtoehto seuraavassa vaiheessa, jos tehtävää ei voi suorittaa ajoitettuna aikana.
5. Napsauta **Valmis**-painiketta. Uusi ajoitettu tehtävä lisätään nykyisten ajoitettujen tehtävien luetteloon.

ESET Endpoint Security for macOS sisältää oletusarvoisesti ennalta määritettyjä ajoitettuja tehtäviä, joilla on tarkoitus varmistaa, että tuote toimii oikein. Näihin tehtäviin ei saa tehdä muutoksia, ja ne ovat oletusarvon mukaan piilotettuina. Voit tarkastella näitä tehtäviä siirtymällä päävalikkoon ja valitsemalla **Asetukset > Anna sovelluksen oletusasetukset > Ajastin** ja sitten **Näytä järjestelmätehtävät**.

Käyttäjän määrittämän tehtävän luominen

Jos valitset Suorita tehtävä -alasvetovalikosta "käyttäjän määrittämä", sinun on määritettävä joitakin erityisiä parametreja.

Käyttäjän määrittämän tehtävän päivämäärä ja kellonaika on määritettävä vuoden sisältävään cron-muotoon (merkkijono, jossa on 6 välilyönnillä toisistaan erotettua kenttää):

minuutti(0-59) tunti(0-23) kuukauden päivä(1-31) kuukausi(1-12) vuosi(1970-2099)
viikonpäivä(0-7)(sunnuntai = 0 tai 7)

✓ **Esimerkki:**
30 6 22 3 2012 4

Seuraavat erikoismerkit ovat sallittuja cron-lausekkeissa:

- tähti (*) – lauseke vastaa kaikkia kentän arvoja: esimerkiksi tähtimerkki kolmannessa kentässä (kuukauden päivä) tarkoittaa "joka päivä".
- viiva (-) – määrittää alueen: esim. 3-9
- pilkku (,) – käytetään luettelon erottimena: esim. 1,3,7,8
- kauttaviiva (/) – määrittää alueiden lisäykset: esim. 3-28/5 kolmannessa kentässä (kuukauden päivä) tarkoittaa kuukauden kolmas päivä ja sitten joka viides päivä.

Päivien ((Monday-Sunday)) ja kuukausien ((January-December)) nimiä ei tueta.

Käyttäjän määrittämät tehtävät
i Jos määrität sekä kuukauden päivän että viikonpäivän, komento suoritetaan vain, kun molempien kenttien arvot vastaavat.

Varhaisen varoituksen antava LiveGrid® -järjestelmä pitää ESETin välittömästi ja jatkuvasti ajan tasalla uusista tunkeutumisista. Kaksisuuntaisella varhaisen varoituksen antavalla LiveGrid® -järjestelmällä on yksi tarkoitus: parantaa sinulle antamaamme suojasta. Paras tapa varmistaa, että näemme uudet uhat mahdollisimman pian niiden ilmestymisen jälkeen, on luoda yhteys mahdollisimman moneen asiakkaaseemme ja pitää tunnistusmoduulimme tiedot jatkuvasti ajan tasalla heidän keräämiensä tietojen avulla. Valitse LiveGrid® -järjestelmälle yksi kahdesta vaihtoehdosta:

1. Voit olla ottamatta varhaisen varoituksen antavaa LiveGrid® -järjestelmää käyttöön. Et menetä ohjelmiston mitään toimintoja, mutta joissakin tapauksissa ESET Endpoint Security for macOS voi vastata nopeammin uusiin uhkiin kuin tunnistusmoduulien päivityksiin.
2. Voit määrittää varhaisen varoituksen antavan LiveGrid® -järjestelmän siten, että se lähettää nimettömiä tietoja uusista uhista ja uusien uhkaavien koodien esiintymispaikasta yhdessä tiedostossa. Nämä tiedot voidaan lähettää ESETille analysoitavaksi. Näitä uhkia analysoimalla ESET voi päivittää uhkatietokantaansa ja parantaa uhkien havaitsemiskykyämme.

Varhaisen varoituksen antava LiveGrid® -järjestelmä kerää tietokoneesta tietoja, jotka liittyvät juuri havaittuihin uhkiin. Tiedot voivat sisältää näytteen uhan sisältäneestä tiedostosta tai tiedoston kopion, tiedoston polun, tiedostonimen, päivämäärän ja kellonajan, prosessin, jonka yhteydessä uhka esiintyi, sekä tietoja tietokoneen käyttöjärjestelmästä.

Vaikka on mahdollista, että ESETin uhkalaboratorio saa tällä tavalla joitakin tietoja sinusta ja tietokoneestasi (käyttäjänimet hakemistopoluissa jne.), tietoja ei käytetä MIHINKÄÄN muuhun tarkoitukseen kuin auttamaan meitä vastaamaan välittömästi uusiin uhkiin.

Voit käyttää LiveGrid® -asetuksia valitsemalla päävalikosta **Asetukset > Anna sovelluksen oletusasetukset > LiveGrid®**. Aktivoi LiveGrid® valitsemalla **Ota ESET LiveGrid® -mainejärjestelmä käyttöön (suositus)** ja valitse sitten **Lisäasetukset**-kohdan vierestä **Asetukset**.

Epäilyttävät tiedostot

Oletusarvoisesti ESET Endpoint Security for macOS on määritetty lähettämään epäilyttävät tiedostot analysoitavaksi ESETin uhkalaboratorioon. Jos et halua lähettää näitä tiedostoja automaattisesti, poista valinta kohdasta **Epäilyttävien tiedostojen lähettäminen (Asetukset > Anna sovelluksen oletusasetukset > LiveGrid® > Asetukset)**.

Jos havaitset epäilyttävän tiedoston, voit lähettää sen uhkalaboratorioomme analysoitavaksi. Voit tehdä näin valitsemalla ohjelman pääikkunasta **Työkalut > Lähetä tiedosto analysoitavaksi**. Jos kyseessä on haitallinen sovellus, sen tunnistus lisätään tulevaan päivitykseen.

Nimettömien tilastotietojen lähetys – varhaisen varoituksen ESET LiveGrid® -järjestelmä kerää tietokoneesta anonymoituja tietoja, jotka liittyvät juuri havaittuihin uhkiin. Nämä tiedot sisältävät tunkeutumisen nimen, tietoja tunnistamispäivämäärästä ja -ajasta, ESET-tietoturvaluottien version sekä tietoja käyttöjärjestelmäversiosta ja sijainti-asetuksesta. Tilastot lähetetään yleensä ESETin palvelimiin kerran tai kaksi kertaa päivässä.

Esimerkki: Lähetetty tilastopakkaus

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
✓ # osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

Poikkeussuodatin – Tämän asetuksen avulla tiettyjä tiedostotyyppejä voidaan jättää lähettämättä. Saattaa esimerkiksi kannattaa ohittaa tiedostoja, joissa voi olla mahdollisesti luottamuksellisia tietoja, kuten asiakirjoja ja laskentataulukoita. Yleisimmät tiedostotyytit (.doc, .rtf jne.) ohitetaan oletusarvoisesti. Voit lisätä tiedostotyyppejä ohitettavien tiedostojen luetteloon.

Yhteystiedon sähköpostiosoite (valinnainen) – Sähköpostiosoitetta voidaan käyttää, jos analyysi edellyttää lisätietoja. Huomaa, että ESET ei lähetä vastausta, ellei lisätietoja tarvita.

Karanteeni

Karanteenin tärkein tehtävä on toimia tartunnan saaneiden tiedostojen turvallisena säilytyspaikkana. Tiedostot kannattaa asettaa karanteeniin, jos niitä ei voi puhdistaa, jos niiden poistaminen ei ole turvallista tai suositeltavaa tai ESET Endpoint Security for macOS havaitsee ne perusteettomasti.

Minkä tahansa tiedoston voi asettaa karanteeniin. Tämä on suositeltavaa, jos tiedosto käyttäytyy epäilyttävästi, mutta virustentorjuntaohjelma ei havaitse sitä. Karanteenissa olevat tiedostot voidaan lähettää analysoitavaksi ESETin uhkalaboratorioon.

Karanteenikansiossa olevia tiedostoja voidaan tarkastella taulukossa, jossa näkyvät karanteeniin lisäämisen päivämäärä ja kellonaika, tartunnan saaneen tiedoston alkuperäisen sijainnin polku, tiedoston koko tavuina, karanteeniin asettamisen syy (esimerkiksi "kohde on käyttäjän lisäämä") ja havaittujen uhkien määrä. Karanteenikansio (/Library/Application Support/Eset/esets/cache/quarantine) säilyy järjestelmässä, vaikka ESET Endpoint Security for macOS poistetaan. Karanteeniin asetetut tiedostot tallennetaan turvalliseen salattuun muotoon, ja ne voidaan palauttaa uudelleen tuotteen ESET Endpoint Security for macOS asennuksen jälkeen.

Tiedostojen lisääminen karanteeniin

ESET Endpoint Security for macOS lisää poistetut tiedostot automaattisesti karanteeniin (jos et ole poistanut tämän asetuksen valintaa hälytysikkunassa). Voit lisätä tiedoston manuaalisesti karanteeniin napsauttamalla Karanteeni-ikkunassa "Karanteeni". Voit lähettää tiedoston karanteeniin myös pitämällä Ctrl-näppäintä painettuna, kun napsautat tiedostoa, ja valitsemalla sitten pikavalikosta **Palvelut > ESET Endpoint Security for macOS – Lisää tiedostoja karanteeniin**.

Tiedostojen palauttaminen karanteenista

Karanteeniin asetetut tiedostot voidaan palauttaa myös niiden alkuperäiseen sijaintiin. Voit tehdä tämän valitsemalla karanteeniin lisättävän tiedoston ja napsauttamalla **Palauta**. Palautuksen voi tehdä myös pitämällä CTRL-näppäintä painettuna tiedostoa napsautettaessa ja valitsemalla sitten pikavalikosta **Palauta**. Voit palauttaa

tiedoston myös muuhun sijaintiin kuin siihen, missä se oli ennen karanteeniin asettamista. Voit tehdä tämän valitsemalla **Palauta sijaintiin**.

Tiedoston lähettäminen karanteenista

Jos olet liittänyt karanteeniin epäilyttävän tiedoston, jota ohjelma ei ole havainnut, tai jos tiedosto on virheellisesti todettu tartunnan saaneeksi (esimerkiksi koodin heuristiikka-analyysin perusteella) ja lisätty sen jälkeen karanteeniin, lähetä tiedosto ESETin uhkalaboratorioon. Voit lähettää tiedoston karanteenista pitämällä CTRL-näppäintä painettuna, kun napsautat tiedostoa, ja valitsemalla sitten pikavalikosta **Lähetä analysoitavaksi**.

Käyttöoikeudet

Tuotteen ESET Endpoint Security for macOS asetukset voivat olla erittäin tärkeitä organisaation tietoturvakäytännön kannalta. Luvattomat muokkaamiset voivat vaarantaa järjestelmän vakauden ja tietoturvan. Ohjelman kokoonpanon muokkausoikeudet ovatkin määritettävissä.

Voit määrittää käyttöoikeuden saaneet käyttäjät osiossa **Asetukset > Anna sovelluksen oletusasetukset > Käyttäjä > Käyttöoikeudet**.

Järjestelmän suojaaminen parhaalla mahdollisella tavalla edellyttää, että ohjelman asetukset on määritetty oikein. Luvattomat muokkaamiset voivat johtaa tärkeiden tietojen menetykseen. Käyttöoikeudet saavien käyttäjien luettelon voi määrittää valitsemalla heidät vasemmalla puolella olevasta **Käyttäjät**-luettelosta ja valitsemalla **Lisää**. Käyttäjän voi poistaa valitsemalla hänen nimensä **Käyttöoikeudet saaneet käyttäjät** -luettelosta oikealta puolelta ja valitsemalla **Poista**. Voit tuoda kaikki käyttäjät näkyviin valitsemalla **Näytä kaikki käyttäjät**.

i Tyhjä käyttöoikeudet saaneiden käyttäjien luettelo
Jos käyttöoikeudet saaneiden käyttäjien luettelo on tyhjä, kaikilla järjestelmän käyttäjillä on oikeudet muokata ohjelman asetuksia.

Esitystila

Esitystila on suunnattu käyttäjille, jotka vaativat ohjelmiston keskeytymätöntä käyttöä, jotka eivät halua ponnahdusikkunoiden häiritsevän ja jotka haluavat minimoida suorittimen kuormituksen. Esitystila voidaan ottaa käyttöön myös esitysten aikana, jolloin virustentorjunta ei aiheuta keskeytystä. Kun esitystila on käytössä, ponnahdusikkunat ovat pois käytöstä eikä ajoitettuja tehtäviä suoriteta. Järjestelmän suojaus on kuitenkin käynnissä taustalla, mutta se ei vaadi käyttäjän toimenpiteitä.

Voit ottaa esitystilan käyttöön manuaalisesti valitsemalla **Asetukset > Anna sovelluksen oletusasetukset... > Esitystila > Ota esitystila käyttöön**.

Käynnistä esitystila automaattisesti, kun sovelluksia suoritetaan koko näytön tilassa, valitsemalla **Ota esitystila automaattisesti käyttöön koko näytössä** -vaihtoehdon viereinen valintaruutu. Kun tämä ominaisuus on käytössä, esitystila käynnistyy aina, kun käynnistät koko näytön sovelluksen ja loppuu automaattisesti suljettuasi sovelluksen. Tämä on erityisen hyödyllistä esitelmää aloittaessa.

Voit valita myös vaihtoehdon **Poista esitystila käytöstä automaattisesti kun**, jos haluat määrittää ajan minuuteissa, jonka jälkeen esitystila poistetaan automaattisesti käytöstä.

Esitystilan käyttöönotosta aiheutuu tietoturvariski, minkä vuoksi tuotteen ESET Endpoint Security for macOS suojausten tilan kuvake muuttuu oranssiksi ja tuo varoituksen näyttöön.

Vuorovaikutteinen tila ja esitystila palomuurissa

Jos palomuuuri on vuorovaikutteisessa tilassa ja esitystila otetaan käyttöön, Internet-yhteyden kanssa voi tulla ongelmia. Tämä voi olla haitallista, jos käynnistät sovelluksen, joka vaatii Internet-yhteyden.

i Tavallisesti sinulta kysyttäisiin varmistus toiminnon suorittamiseen (jos yhteyssääntöjä tai -poikkeuksia ei ole määritetty), mutta esitystilassa käyttäjän toimenpiteitä ei vaadita. Asian voi ratkaista määrittelemällä yhteyssääntö jokaiselle sovellukselle, jonka kanssa toiminto saattaa aiheuttaa ristiriidan tai käyttää erilaista suodatustilaa palomuurissa. Kannattaa muistaa, että jos esitystila on käytössä ja siirryt Web-sivulle tai sovellukseen, joka saattaa sisältää tietoturvariskin, se voidaan estää, mutta et saa estämisestä minkäänlaista selitystä tai varoitusta, koska pelitilassa käyttäjän toimenpiteet on poistettu käytöstä.

Käynnissä olevat prosessit

Käynnissä olevat prosessit -luettelossa näkyvät tietokoneessa käynnissä olevat prosessit. ESET Endpoint Security for macOS sisältää lisätietoja käynnissä olevista prosesseista ja suojaa käyttäjiä ESET LiveGrid® -tekniikalla.

- **Prosessi** – Parhaillaan tietokoneessa käynnissä olevan prosessin nimi. Voit tarkistaa kaikki tietokoneessasi käynnissä olevat prosessit myös käyttämällä Activity monitor -ohjelmaa, jonka sijainti on */Applications/Utilities*).
- **Riskitaso** – Useimmissa tapauksissa ESET Endpoint Security for macOS ja ESET LiveGrid® -tekniikka määrittävät kohteille (tiedostot, prosessit jne.) riskitasoja käyttämällä heuristiikkasääntöjä, jotka tutkivat kunkin kohteen ominaisuuksia ja sitten arvioivat niiden haittamahdollisuutta. Kohteille määritetään riskitaso näiden heurististen tietojen perusteella. Vihreällä merkityt tunnetut sovellukset ovat varmuudella puhtaita (sallittujen luettelossa), ja ne jätetään pois tarkistuksesta. Tämä nopeuttaa sekä tarvepohjaista että reaaliaikaista tarkistusta. Kun sovellus on merkitty tuntemattomaksi (keltainen), se ei ole välttämättä haittaohjelma. Se on yleensä vain uusi sovellus. Jos et ole varma tiedostosta, voit lähettää sen ESETin uhkalaboratorioon analysoitavaksi. Jos tiedosto todetaan haitalliseksi sovellukseksi, sen määrittäminen lisätään tulevaan päivitykseen.
- **Käyttäjämäärä** – Tiettyä sovellusta käyttävien käyttäjien määrä. ESET LiveGrid® -tekniikka kerää nämä tiedot.
- **Havaitsemisaika** – ajanjakso, jolloin ESET LiveGrid® -tekniikka havaitsi sovelluksen.
- **Sovelluspaketin tunnus** – toimittajan tai sovellusprosessin nimi.

Kun valitset tietyn prosessin, seuraavat tiedot tulevat näkyviin ikkunan alaosaan:

- **Tiedosto** – sovelluksen sijainti tietokoneessa
- **Tiedoston koko** – levyllä olevan tiedoston fyysinen koko
- **Tiedoston kuvaus** – tiedoston ominaisuudet käyttäjärjestelmästä saadun kuvauksen perusteella
- **Sovelluspaketin tunnus** – toimittajan tai sovellusprosessin nimi
- **Tiedostoversio** – tiedot sovelluksen julkaisijalta


- **Tuotteen nimi** – sovelluksen ja/tai yrityksen nimi.

Käyttöliittymä

Käyttöliittymän kokoonpanoon liittyvillä asetuksilla voidaan säätää työympäristöä tarpeen mukaan. Näitä asetuksia voi käsitellä päävalikosta valitsemalla **Asetukset > Anna sovelluksen oletusasetukset... > Liittymä**.

- Ohjelman ESET Endpoint Security for macOS käynnistyskuvan voi näyttää käynnistuksen yhteydessä valitsemalla **Näytä käynnistyskuva käynnistettäessä**.


- **Näytä sovellus pikakäynnistyspalkissa** -asetuksen avulla ohjelman ESET Endpoint Security for macOS

kuvakkeen  voi näyttää macOS:n Dockissa. Ohjelman ESET Endpoint Security for macOS ja muiden käynnissä olevien ohjelmien välillä voi siirtyä painamalla näppäinyhdistelmää `cmd+tab`. Muutokset tulevat voimaan, kun ESET Endpoint Security for macOS on käynnistetty uudelleen (yleensä tietokoneen uudelleenkäynnistuksen yhteydessä).

- **Käytä vakiovalikkoa** -asetuksen avulla voit käyttää tiettyjä pikanäppäimiä (lisätietoja on kohdassa [Pikanäppäimet](#)) ja tarkastella vakiovalikkokohteita (Käyttöliittymä, Asetukset ja Työkalut) macOS-valikkorivillä (näytön yläosassa).

- Ota käyttöön **Näytä työkaluvihjeet** näyttääksesi työkaluvihjeet, kun osoitin on tiettyjen asetusten kohdalla tuotteessa ESET Endpoint Security for macOS.

- **Näytä piilotetut tiedostot** -asetuksen avulla voi tarkastella ja valita piilotettuja tiedostoja **Tietokoneen tarkistus** -kokoonpanon **Tarkistettavat kohteet** -asetuksissa.

- Oletusarvon mukaan ohjelman ESET Endpoint Security for macOS kuvake  näkyy valikkorivin lisätilassa, joka sijaitsee macOS-valikkorivin oikealla puolella (näytön yläosassa). Jos haluat poistaa kuvakkeen käytöstä, poista asetuksen **Näytä kuvake valikkorivin lisätilassa** valinta. Tämä muutos tulee voimaan, kun ESET Endpoint Security for macOS on käynnistetty uudelleen (yleensä tietokoneen uudelleenkäynnistuksen yhteydessä).

Hälytykset ja ilmoitukset

Hälytykset ja ilmoitukset -kohdassa voit määrittää, miten ESET Endpoint Security for macOS käsittelee uhkahälytykset ja suojaustila- ja järjestelmäilmoitukset.

Jos **Näytä hälytykset** poistetaan käytöstä, kaikki hälytysikkunat poistetaan käytöstä, joten sitä suositellaan vain joihinkin erityistilanteisiin. Useimmille käyttäjille suosittelemme oletusasetuksen käyttämistä (käytössä). Lisäasetuksista kerrotaan [tässä luvussa](#).

Näytä ilmoitukset työpöydällä -asetuksen valitseminen ottaa käyttöön hälytysikkunat, jotka eivät edellytä käyttäjän toimia näkyäkseen työpöydällä (oletusarvoisesti näytön oikeassa yläkulmassa). Voit määrittää ajanjakson, jolloin ilmoitus näytetään, säätämällä **Sulje ilmoitukset automaattisesti sen jälkeen, kun X sekuntia** -arvoa (oletuksena on 5 sekuntia).

Tuotteen ESET Endpoint Security for macOS version 6.2 myötä voit myös estää tiettyjen **Suojauksen tilat**

näkymistä ohjelman pääikkunassa (**Suojaustila**-ikkuna). Lisätietoja on osiossa [Suojauksen tilat](#).

Hälytysten näyttäminen

ESET Endpoint Security for macOS näyttää hälytysikkunat, jotka ilmoittavat uudesta ohjelmaversiosta ja käyttöjärjestelmäpäivityksistä, poistavat tiettyjä ohjelmakomponentteja käytöstä, poistavat lokeja ja niin edelleen. Voit piilottaa kunkin ilmoituksen yksitellen valitsemalla **Älä näytä tätä valintaikkunaa enää**.

Valintaikkunaluettelo (löytyy kohdasta **Asetukset > Anna sovelluksen oletusasetukset... > Hälytykset ja ilmoitukset > Näytä hälytykset: Asetukset...**) näyttää kaikki hälytysikkunat, jotka ESET Endpoint Security for macOS voi aktivoida. Voit sallia ilmoituksen näytön valitsemalla **valintaikkunan nimen** vasemmalla puolella olevan valintaruudun tai estää ilmoituksen näytön poistamalla valintaruudun valinnan. Kun valintaruutu on valittuna, kyseinen ilmoitus näytetään aina eikä **Näyttöehdot**-asetuksia sovelleta. Jos halua nähdä tiettyjä ilmoituksia, poista valintaruudun valinta. Tällöin voit määrittää **Näyttöehdot**-asetusten avulla tehtäväksi tietyjä toimintoja tiettyinä aikoina.

Suojauksen tilat

Käytössä olevaa tuotteen ESET Endpoint Security for macOS suojauksen tilaa voi muuttaa aktivoimalla tiloja kohdassa **Asetukset > Anna sovelluksen oletusasetukset...** tai poistamalla niiden aktivointeja. **> Hälytykset ja ilmoitukset > Näytä suojauksen tilan näytössä: Asetukset**. Erilaisten ohjelmaominaisuuksien tilat näytetään tai piilotetaan tuotteen ESET Endpoint Security for macOS pääikkunassa (**Suojauksen tila** -ikkuna).

Voit piilottaa seuraavien ohjelmaominaisuuksien suojauksen tilan:

- Palomuuuri
- Tietokalastelun esto
- Internet-käytön suojaus
- Sähköpostisovelluksen suojaus
- Esitystila
- Käyttöjärjestelmäpäivitys
- Käyttöoikeuden vanheneminen
- Tietokone on käynnistettävä uudelleen

Pikavalikko

Voit lisätä tuotteen ESET Endpoint Security for macOS ominaisuudet pikavalikkoon napsauttamalla **Asetukset > Anna sovelluksen oletusasetukset > Pikavalikko** ja valitsemalla kohdan **Integroi pikavalikkoon** vieressä oleva valintaruutu. Muutokset tulevat voimaan sen jälkeen, kun kirjautut ulos tai käynnistät tietokoneen uudelleen. Pikavalikon vaihtoehdot ovat käytettävissä työpöydällä ja **Finder**-ikkunassa, kun painat CTRL-näppäintä ja valitset jonkin tiedoston tai kansion.

Päivitä

ESET Endpoint Security for macOS on päivitettävä säännöllisesti, jotta suojaustaso pysyy mahdollisimman hyvänä. Päivitysmoduuli varmistaa ohjelman ajantasaisuuden lataamalla uusimmat tunnistusmoduulit.

Kun valitset päävalikosta **Päivitä**, näet voimassa olevan päivityksen tilan, mukaan lukien edellisen onnistuneen päivityksen ajankohdan sekä päivitystarpeen. Päivitysprosessin voi aloittaa manuaalisesti valitsemalla **Päivitä moduulit**.

Normaalioloissa, joissa päivitysten lataaminen on onnistunut, Päivitä-ikkunassa näkyy ilmoitus *Päivitystä ei tarvitse tehdä - asennetut moduulit ovat voimassa*, jos sinulla on uusimmat moduulit. Jos moduuleja ei voi päivittää, suosittelemme, että tarkistat [päivitysasetukset](#) – tämän virheen tavallisimmat syyt ovat väärin määritetyt käyttöoikeustiedot tai virheellisesti määritetyt [käyttöoikeustiedot](#) tai [yhteysasetukset](#).

Päivitys-ikkunassa näkyy myös tunnistusohjelman versionumero. Tämä numeerinen ilmaisin on linkitetty ESET-sivustoon, jolla tunnistusohjelman päivitystiedot näkyvät.

Päivitysasetukset

Päivitysasetuksissa määritetään päivityksen lähdetiedot, kuten päivityspalvelimet ja palvelinten todennustiedot. Oletusarvon mukaan avattavan **Päivityspalvelin**-valikon asetukseksi on määritetty **Valitse automaattisesti**, jotta päivitystiedostot ladataan automaattisesti ESET-palvelimesta mahdollisimman vähäisellä verkkoliikenteellä.

Käytettävissä olevien palvelinten luettelo on saatavilla avattavasta **Päivityspalvelin**-valikosta. Voit lisätä uuden päivityspalvelimen napsauttamalla **Muokkaa**, syöttämällä uuden palvelimen osoitteen **Päivityspalvelin**-


syötekenttään ja napsauttamalla **Lisää**.

Tuotteen ESET Endpoint Security for macOS avulla voit valita vaihtoehtoisen päivityspalvelimen tai vikatilanteessa käytettävän päivityspalvelimen. **Ensisijainen** palvelin voi olla peilauspalvelin ja **toissijainen palvelin** voi olla ESETin vakiopäivityspalvelin. Toissijaisen palvelimen on oltava eri kuin ensisijainen palvelin tai muuten sitä ei käytetä. Jos et määritä toissijaista päivityspalvelinta, käyttäjänimeä ja salasanaa, vikatilanteessa käytettävä päivitys ei toimi. Voit myös antaa tuotteen ESET Endpoint Security for macOS valita käytettäväksi paras päivityspalvelin valitsemalla vaihtoehto Valitse automaattisesti ja antamalla käyttäjänimesi ja salasanasi niille varattuihin kenttiin.

Välityspalvelintilan avulla voit päivittää tunnistusmoduulit välityspalvelimen välityksellä (esimerkiksi paikallinen HTTP-välityspalvelin). Palvelin voi olla sama tai eri kuin yleinen välityspalvelin, jota käytetään kaikkien niiden ohjelman ominaisuuksien kohdalla, jotka vaativat yhteyden. Yleisen välityspalvelimen asetukset on määritetty jo asennuksen aikana, tai ne voidaan määrittää osiossa [Välityspalvelimen asetukset](#).

Voit määrittää sovelluksen lataamaan päivitykset vain välityspalvelimen kautta näin:

1. Valitse avattavasta valikosta **Yhteys välityspalvelimen kautta**.
2. Valitse **Havaitse**, jotta ESET Endpoint Security for macOS täyttää IP-osoitteen ja porttinumeron (**3128** on oletusarvo).
3. Anna voimassa oleva **Käyttäjänimi** ja **Salasana** niille varattuihin kenttiin, jos viestintä välityspalvelimen kanssa edellyttää todennusta.

ESET Endpoint Security for macOS havaitsee välityspalvelinasetukset macOS-järjestelmän oletusasetuksista. Nämä voidaan määrittää macOS:ssä osiossa  > **Järjestelmän oletusasetukset** > **Verkko** > **Lisäasetukset** > **Välityspalvelimet**.

Jos otat asetuksen **Käytä suoraa yhteyttä, jos HTTP-välityspalvelin ei ole käytettävissä** käyttöön, ESET Endpoint Security for macOS yrittää muodostaa yhteyden päivityspalvelimiin automaattisesti ilman välityspalvelinta. Tätä asetusta suositellaan paljon liikkuville MacBook-käyttäjille.

Jos sinulla on vaikeuksia tunnistusmoduulien päivitysten lataamisessa, valitse **Tyhjennä päivitysvälimuisti poistaaksesi väliaikaiset päivitystiedostot**.

Lisäasetukset

Jos haluat poistaa kunkin onnistuneen päivityksen jälkeen näytettävät ilmoitukset käytöstä, valitse **Älä näytä ilmoitusta onnistuneesta päivityksestä**.

Ottamalla julkaisua edeltävät päivitykset käyttöön voit ladata kehitysmoduuleita, jotka ovat vielä testattavana. Julkaisua edeltävät voivat auttaa ratkaisemaan tuoteongelmia. Lykätty päivitys lataa päivitykset muutama tunti niiden julkaisun jälkeen. Tämän tarkoituksena on varmistaa, että asiakaskoneisiisi ei asenneta päivityksiä, ennen kuin ne on todettu virheettömiksi käytössä.

ESET Endpoint Security for macOS tallentaa vedoksia tunnistus- ja ohjelmamoduuleista, joita voi käyttää **Päivityksen peruutus** -toiminnolla. Anna asetuksen **Luo vedokset päivitystiedoista** olla käytössä, jotta ESET Endpoint Security for macOS tallentaa vedokset automaattisesti. Jos epäilet, että uusi tunnistusmoduulin ja/tai

ohjelmamoduulin päivitys saattaa olla epävakaa tai vioittunut, voit Päivityksen peruutus -toiminnolla palata edelliseen versioon ja poistaa päivitykset käytöstä tietyksi ajaksi. Voit vaihtoehtoisesti ottaa aiemmin poistetut päivitykset käyttöön, jos olet aiemmin ohittanut ne. Kun palaat edelliseen päivitykseen Päivityksen peruutus -toiminnolla, määritä avattavasta Aseta keskeytettäväksi ajanjaksoksi -valikosta ajanjakso, jolta haluat keskeyttää päivitykset. Jos valitset kunnes perutaan -vaihtoehdon, normaaleja päivityksiä jatketaan vasta, kun palautat ne käyttöön manuaalisesti. Päivitysten keskeytysajanjaksoa määritettäessä on syytä olla varovainen.

Määritä tunnistusohjelman enimmäisikä automaattisesti – Voit asettaa enimmäisajan (päivissä), jonka jälkeen tunnistusmoduulien ilmoitetaan vanhentuneen. Oletusarvo on seitsemän päivää.

Päivitystehtävien luominen

Käynnistä tunnistusmoduulien päivitys manuaalisesti valitsemalla Päivitä > **Päivitä moduulit**.

Päivitykset voidaan suorittaa myös ajoitettuina tehtävinä. Jos haluat määrittää ajoitetun tehtävän, valitse **Työkalut > Ajastin**. Oletusarvoisesti tuotteessa ESET Endpoint Security for macOS on käytössä seuraavat tehtävät:

- **Säännöllinen automaattinen päivitys**
- **Automaattinen päivitys käyttäjän kirjautumisen jälkeen**

Kaikkia päivitystehtäviä voidaan muokata käyttäjän tarpeiden mukaan. Oletusarvoisten päivitystehtävien lisäksi käyttäjä voi luoda myös uusia päivitystehtäviä, joiden asetukset voidaan määrittää käyttäjäkohtaisesti. Lisätietoja päivitystehtävien luomisesta ja määrittämisestä on kohdassa [Ajastin](#).

Järjestelmäpäivitykset

macOS-järjestelmän päivitystoiminto on tärkeä komponentti, joka on suunniteltu suojaamaan käyttäjiä haitallisilta ohjelmistoilta. Suojausta kannattaa tehostaa asentamalla nämä päivitykset heti, kun ne ovat saatavilla. ESET Endpoint Security for macOS ilmoittaa puuttuvista päivityksistä tärkeystason mukaan. Voit muokata päivityksen tärkeystasoa näytettävien ilmoitusten osalta kohdassa **Asetukset > Anna sovelluksen oletusasetukset > Hälytykset ja ilmoitukset > Asetukset käyttämällä Näyttöehdot**-alasvetovalikko, joka on kohdan **Käyttäjärjestelmäpäivitykset** vieressä.

- **Näytä kaikki päivitykset** – ilmoitus näytetään aina, kun järjestelmäpäivitys puuttuu
- **Näytä vain suositellut** – sinulle ilmoitetaan vain suositelluista päivityksistä

Jos et halua ilmoituksia puuttuvista päivityksistä, poista **Käyttäjärjestelmän päivitykset** -valintaruudun valinta.

Ilmoitusikkunassa on yleiskuvaus macOS-käyttäjärjestelmälle saatavilla olevista päivityksistä ja macOS-ohjelmistopäivitystyökalun kautta päivitettävistä sovelluksista. Voit suorittaa päivityksen suoraan ilmoitusikkunasta tai ohjelman ESET Endpoint Security for macOS **Aloit**-osasta valitsemalla **Asenna puuttuva päivitys**.

Ilmoitusikkunassa on sovelluksen nimi, versio, koko, ominaisuudet (merkinnät) ja lisätietoja saatavilla olevista päivityksistä. **Merkinnät**-sarakeessa on seuraavat tiedot:

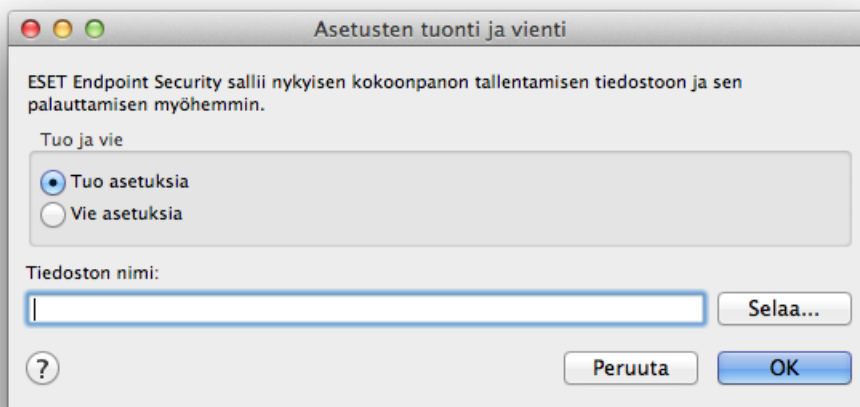
- **[suositus]** – käyttöjärjestelmän valmistaja suosittelee, että asennat tämän päivityksen, jotta järjestelmän tietoturva ja vakaus paranee
- **[uudelleenkäynnistys]** – tietokone on käynnistettävä uudelleen asennuksen jälkeen
- **[sammutus]** – tietokone on sammutettava ja sen virta on sitten kytkettävä uudelleen päälle asennuksen jälkeen

Ilmoitusikkunassa näkyvät komentorivityökalulla nimeltä "softwareupdate" noudetut päivitykset. Tällä työkalulla noudetut päivitykset voivat poiketa ohjelmistopäivitystyökalun näyttämistä päivityksistä. Jos haluat asentaa kaikki saatavilla olevat päivitykset, jotka näkyvät puuttuvien järjestelmäpäivitysten ikkunassa, ja myös päivitykset, joita ohjelmistopäivitystyökalu ei näytä, sinun on käytettävä "softwareupdate"-komentorivityökalua. Lisätietoja tästä työkalusta on "softwareupdate"-oppaassa, jota voit lukea kirjoittamalla `man softwareupdate` **Pääte**-ikkunaan. Tätä suositellaan vain edistyneille käyttäjille.

Tuo ja vie asetuksia

Voit tuoda olemassa olevan kokoonpanon tai viedä tuotteen ESET Endpoint Security for macOS määrittelyn valitsemalla **Asetukset > Tuo ja vie asetuksia**.

Tuonti ja vienti ovat hyödyllisiä myös, jos tuotteen ESET Endpoint Security for macOS nykyinen kokoonpano on varmuuskopioitava myöhempää käyttöä varten. Asetusten vienti on myös kätevä vaihtoehto käyttäjille, jotka haluavat käyttää ensisijaista tuotteen ESET Endpoint Security for macOS kokoonpanoa useissa järjestelmissä. Halutut asetukset voi tuoda vaivattomasti kokoonpanotiedostossa.



Tuo määrittäjävalitsemalla **Tuo asetukset** ja valitse haluamasi määrittystiedosto napsauttamalla **Selaa**. Vie määrittäjä valitsemalla **Vie asetukset** ja valitse selaimella määrittystiedoston tallennuspaikka tietokoneeltasi.

Välityspalvelimen asetukset

Voit määrittää välityspalvelimen asetukset valitsemalla **Asetukset > Anna sovelluksen oletusasetukset > Välityspalvelin**. Välityspalvelimen määrittäminen tällä tasolla määrittää yleiset välityspalvelimen asetukset kaikille tuotteen ESET Endpoint Security for macOS toiminnoille. Kaikki Internet-yhteyttä edellyttävät moduulit käyttävät näitä parametreja ESET Endpoint Security for macOS tukee Basic Access- ja NTLM (NT LAN Manager) -todennuksia.

Voit määrittää välityspalvelimen asetukset tälle tasolle valitsemalla **Käytä välityspalvelinta** ja antamalla välityspalvelimen IP- tai URL-osoitteen **Välityspalvelin**-kenttään. Määritä Portti-kenttään portti, josta välityspalvelin hyväksyy yhteyksiä (3128 on oletusarvo). Voit myös antaa ohjelman täyttää molemmat kentät napsauttamalla **Havaitse**.

Jos viestintä välityspalvelimen kanssa vaatii todennusta, anna voimassa oleva **Käyttäjänimi** ja **Salasana** niille varattuihin kenttiin.

Jaettu paikallinen välimuisti

Voit ottaa jaetun paikallisen välimuistin käyttöön napsauttamalla Asetukset > Anna sovelluksen oletusasetukset > Jaettu paikallinen välimuisti ja valitsemalla vaihtoehdon "Ota välimuisti käyttöön ESETin jaetulla paikallisella välimuistilla" vieressä oleva valintaruutu. Tämän ominaisuuden käyttö parantaa suorituskykyä virtuaaliympäristöissä karsimalla verkosta kaksinkertaiset tarkistukset. Tällä varmistetaan, että jokainen tiedosto tarkistetaan vain kerran ja tallennetaan jaettuun välimuistiin. Kun ominaisuus on käytössä, verkostossasi olevien tiedostojen ja kansioden tarkistukseen liittyvät tiedot tallennetaan paikalliseen välimuistiin. Jos suoritat tarkistuksen, ESET Endpoint Security for macOS etsii välimuistista tarkistettuja tiedostoja. Jos tiedostot täsmäyvät, ne ohitetaan tarkistuksessa.

Jaetun paikallisen välimuistin asetukset sisältävät seuraavat tiedot:

- **Palvelimen osoite** – sen tietokoneen nimi tai IP-osoite, jolla välimuisti sijaitsee.
- **Portti** – sen portin numero, jota käytetään tiedonsiirtoon (oletuksena (3537).
- **Salasana** – jaetun paikallisen välimuistin salasana (valinnainen).

Yksityiskohtaiset ohjeet



Tarkat ohjeet ESETin jaetun paikallisen välimuistin ottamisesta käyttöön on [ESETin jaetun paikallisen välimuistin käyttöoppaassa](#). (Opas on saatavana vain englanniksi.)

Käyttöoikeussopimus

TÄRKEÄÄ: Lue seuraavat tuotteen käyttöä koskevat käyttöehdot huolellisesti ennen tuotteen lataamista, asentamista, kopiointia tai käyttöä. **LATAAMALLA, ASENTAMALLA TAI KOPIOIMALLA OHJELMISTON TAI KÄYTTÄMÄLLÄ SITÄ ILMAISET, ETTÄ HYVÄKSYT NÄMÄ KÄYTTÖEHDOT JA [TIETOSUOJAKÄYTÄNTÖ](#).**

Käyttöoikeussopimus

Tämän käyttöoikeussopimuksen (jäljempänä "Sopimus") osapuolet ovat ESET, spol. s r. o., kotipaikka Einsteinova 24, 85101 Bratislava, Slovak Republic, merkitty Bratislavan I. käräjäoikeuden kaupparekisteriin, osa Sro, rekisteröintinumerolla 3586/B, BIN: 31333532 (jäljempänä "ESET" tai "Toimittaja") ja sinä, fyysinen tai juridinen henkilö (jäljempänä "Sinä" tai "Loppukäyttäjä"), ja Sinulla on oikeus käyttää tämän Sopimuksen kohdassa 1 eriteltyä Ohjelmistoa. Sopimuksen kohdassa 1 määritetty Ohjelmisto voidaan tallentaa tallennusvälineeseen, lähettää sähköpostitse, ladata Internetistä, ladata Toimittajan palvelimelta tai hankkia muista lähteistä alla mainittujen ehtojen mukaisesti.

TÄMÄ ON LOPPUKÄYTTÄJÄN OIKEUKSIA KOSKEVA SOPIMUS, EI MYYNTISOPIMUS. Toimittaja omistaa edelleen Ohjelmiston kopion ja myyntipaketin sisältämän fyysisen median sekä kaikki muut kopiot, joiden käyttövaltuudet Loppukäyttäjällä on tämän sopimuksen mukaisesti.

Napsauttamalla "Hyväksyn"- tai "Hyväksyn..."-painiketta Ohjelmiston asennuksen, lataamisen, kopioinnin tai käytön aikana ilmoitat hyväksyväsi tämän Sopimuksen ehdot. Jos et hyväksy kaikkia tämän Sopimuksen ehtoja, napsauta peruutusvaihtoehtoa, peruuta asennus tai lataaminen tai hävitä tai palauta Ohjelmisto, asennusväline, Ohjelmistoon liittyvä dokumentaatio ja myyntikuitti Toimittajalle tai jälleenmyyntipisteeseen, josta olet hankkinut Ohjelmiston.

KÄYTTÄMÄLLÄ OHJELMISTOA OSOITAT, ETTÄ OLET LUKENUT TÄMÄN SOPIMUKSEN, OLET YMMÄRTÄNYT SEN JA SITOUUDUT NOUDATTAMAAN SEN EHTOJA.

1. Ohjelmisto. Tässä Sopimuksessa sanalla "Ohjelmisto" viitataan seuraaviin: (i) se tietokoneohjelma kaikkine osineen, jonka mukana tämä Sopimus toimitetaan, (ii) kaikkien niiden levyjen, CD-levyjen DVD-levyjen, sähköpostiviestien ja liitteiden tai muiden tallennusvälineiden sisältö, joiden mukana tämä Sopimus toimitetaan, mukaan lukien tietovälineellä, sähköpostilla tai Internet-latauksella toimitetun Ohjelmiston objektikoodi, (iii) kaikki kirjallinen selventävä aineisto ja muut Ohjelmistoon liittyvät mahdolliset dokumentaatiot, erityisesti kaikki Ohjelmiston kuvaukset, tekniset tiedot, Ohjelmiston ominaisuuksien ja toimintojen kuvaukset, kuvaukset Ohjelmiston käyttöympäristöstä, Ohjelmiston asennus- tai käyttöohjeet ja muut ohjeet Ohjelmiston käyttämisestä (jäljempänä yhteisesti "Ohjeet"), ja (iv) Ohjelmiston kopiot, Ohjelmiston mahdollisten ohjelmistovirheiden korjaukset, Ohjelmiston lisäykset ja laajennukset, Ohjelmiston muokatut versiot ja Ohjelmiston osien mahdolliset päivitykset, joihin Toimittaja myöntää käyttöoikeuden tämän Sopimuksen kohdan 3 mukaisesti. Ohjelmisto toimitetaan yksinomaan suoritettavan objektikoodin muodossa.

2. Asennus, tietokone ja käyttöoikeusavain. Palveluntarjoajalta, sähköpostitse, Internetistä ladattu, Toimittajan palvelimelta ladattu tai muusta lähteestä hankittu Ohjelmisto edellyttää asennusta. Ohjelmisto on asennettava oikein määritettyyn tietokoneeseen, joka on dokumentaatioissa eriteltyjen vähimmäisvaatimusten mukainen. Asennustapa on kuvattu dokumentaatioissa. Tietokoneeseen, johon ohjelmisto asennetaan, ei saa asentaa mitään tietokoneohjelmia eikä laitteita, jotka voivat vaikuttaa haitallisesti ohjelmistoon. Tietokone tarkoittaa laitteistoa, joka voi olla mukaan lukien rajoituksetta PC-tietokoneet, kannettavat tietokoneet, työasemat, kämmenlaitteet, älypuhelimet, kannettavat elektroniset laitteet tai muut elektroniset laitteet, joille ohjelmisto on suunniteltu, joihin se asennetaan ja/tai joissa sitä käytetään. Käyttöoikeusavain tarkoittaa yksilöllistä merkkien, kirjainten, numeroiden tai erikoismerkkien ketjua, joka toimitetaan loppukäyttäjälle, jotta hän voi jatkaa Ohjelmiston, sen tietyn version tai Käyttöoikeuskauden käyttöä laillisesti tämän Sopimuksen mukaan.

3. Käyttöoikeus. Toimittaja myöntää Sinulle seuraavat oikeudet (jäljempänä "Käyttöoikeus") edellyttäen, että olet hyväksynyt tämän Sopimuksen ehdot ja noudatat niitä:

a) Asennus ja käyttö. Sinulla on ei-yksinoikeudellinen, ei-siirrettävä oikeus asentaa Ohjelmisto tietokoneen kiintolevylle tai muulle tietojen pysyvään tallennukseen tarkoitettulle välineelle, asentaa ja tallentaa Ohjelmisto tietokonejärjestelmän muistiin sekä ottaa Ohjelmisto käyttöön, tallentaa se ja näyttää se.

b) Käyttöoikeuksien määrää koskeva sopimusehto. Oikeus käyttää Ohjelmistoa on sidottu loppukäyttäjien määrään. Yhdellä Loppukäyttäjällä viitataan seuraavaan: (i) Ohjelmiston asentaminen yhteen

tietokonejärjestelmään, tai (ii) jos käyttöoikeuksien määrä on sidottu postilaatikoiden määrään, yhdellä Loppukäyttäjällä tarkoitetaan tietokoneen käyttäjää, joka vastaanottaa sähköpostia käyttäjäagentin (Mail User Agent, jäljempänä "MUA") välityksellä. Jos MUA vastaanottaa sähköpostiviestit ja jakaa ne automaattisesti usealle käyttäjälle, Loppukäyttäjien määrä määräytyy niiden todellisten käyttäjien määrän mukaan, joille sähköpostia jaetaan. Jos postipalvelin toimii postiporttina, Loppukäyttäjien määrä vastaa niiden postipalvelimien määrää, joille kyseinen portti tarjoaa palveluita. Jos määrittämättömään määrään sähköpostiosoitteita (esim. aliaisten kautta) saapuvat viestit ohjataan yhdelle käyttäjälle, joka hyväksyy ne, ja sähköpostiohjelma ei enää jaa viestejä automaattisesti useammille käyttäjille, Käyttöoikeus on hankittava vain yhteen tietokoneeseen. Samaa Käyttöoikeutta ei saa käyttää samaan aikaan useissa tietokoneissa. Loppukäyttäjällä on oikeus syöttää käyttöoikeusavain Ohjelmistoon vain, jos Ohjelmistoa käytetään Toimittajan myöntämien Käyttöoikeuksien määrärajoituksen mukaisesti. Käyttöoikeusavain on luottamuksellinen, eikä sitä saa jakaa kolmansille osapuolille eikä kolmansille osapuolille saa antaa käyttöoikeusavainta käyttöön, ellei tässä Sopimuksessa tai Toimittajan kanssa ole muutoin sovittu. Jos epäilet, että käyttöoikeusavain on joutunut väärin käsiin, ilmoita siitä heti Toimittajalle.

c) **Business Edition.** Ohjelmiston Business Edition -versio on hankittava, jos Ohjelmistoa halutaan käyttää postipalvelimissa, postin välityspalvelimissa, postiyhdyskäytävissä tai Internet-yhdyskäytävissä.

d) **Sopimuksen voimassaoloaika.** Ohjelmiston käyttöoikeutta on rajoitettu ajallisesti.

e) **OEM-ohjelmisto.** OEM-ohjelmistoa voi käyttää tietokoneessa, jolla se on hankittu. Sitä ei voi siirtää muuhun tietokoneeseen.

f) **NFR- ja kokeiluohjelmistot.** Ohjelmistot, jotka luokitellaan NFR ("Not-for-resale")- tai kokeiluversioiksi, eivät ole ostettavissa, vaan niitä saa käyttää ainoastaan ohjelmiston ominaisuuksien esittelyyn tai testaukseen.

g) **Käyttöoikeuden päättymisen.** Käyttöoikeus päättyy automaattisesti sille määritetyn ajanjakson lopussa. Jos et noudata jotakin tämän Sopimuksen ehtoa, Toimittajalla on tällaisessa tilanteessa oikeus irtisanoa Sopimus rajoituksetta Toimittajalle suotujen oikeuksien tai oikeussuojan puitteissa. Jos Käyttöoikeus perutaan, Sinun on heti poistettava, tuhottava tai palautettava Ohjelmisto ja kaikki sen varmuuskopiot omalla kustannuksellasi ESETille tai jälleenmyyntipisteeseen, josta Ohjelmisto on hankittu. Käyttöoikeuden päätyttyä Toimittajalla on lisäksi oikeus peruuttaa Loppukäyttäjän oikeudet Ohjelmiston sellaisten toimintojen käyttöön, jotka edellyttävät yhteystä Toimittajan tai kolmannen osapuolen palvelimiin.

4. **Tietojen keräämiseen liittyvät toiminnot ja Internet-yhteyden edellytykset.** Ohjelmiston asianmukainen käyttö edellyttää Internet-yhteyttä. Ohjelmiston on muodostettava säännöllisesti yhteys Toimittajan palvelimiin tai kolmansien osapuolten palvelimiin ja kerättävä sovellettavia tietoja Tietosuojakäytännön mukaisesti. Internet-yhteys ja sovellettavien tietojen kerääminen on edellytys seuraaville Ohjelmiston toiminnoille:

a) **Ohjelmistopäivitykset.** Toimittajalla on oikeus toimittaa aika ajoin ohjelmistopäivityksiä ("Päivitykset"), mutta Toimittajalla ei ole velvollisuutta toimittaa Päivityksiä. Tämä toiminto on otettu käyttöön Ohjelmiston vakioasetuksissa, ja Päivitykset asennetaan siksi automaattisesti, ellei Loppukäyttäjä ole poistanut Päivitysten automaattista asennusta käytöstä. Päivitysten hankkiminen edellyttää Käyttöoikeuden todentamista sekä tietokonetta ja/tai Ohjelmiston asennusympäristöä koskevien tietojen keräämistä Tietosuojakäytännön mukaisesti.

b) **Tietomurtojen ja tietojen välittäminen Toimittajalle.** Ohjelmisto sisältää toimintoja, joiden tehtävänä on kerätä näytteitä tietokoneviruksista ja muista haitallisista tietokoneohjelmista ja epäilyttävistä, ongelmallisista ja mahdollisesti tarpeettomista tai vaarallisista objekteista, kuten tiedostoista, URL-osoitteista, IP-paketeista ja Ethernet-kehyksistä (jäljempänä "Tietomurrot") ja lähettää ne Toimittajalle, mukaan lukien rajoituksetta tiedot asennusprosessista, tietokoneesta ja/tai Ohjelmiston asennusympäristöstä, Ohjelmiston toiminnoista ja paikallisen verkon laitteista, kuten tiedot niiden tyypeistä, toimittajista, malleista ja/tai nimistä (jäljempänä

"Tiedot"). Tiedoissa ja Tietomurroissa voi olla tietoja (myös satunnaisesti tai vahingossa hankittuja henkilökohtaisia tietoja) sen tietokoneen Loppukäyttäjältä tai muista käyttäjistä, johon Ohjelmisto on asennettu, ja Tietomurron kohteeksi joutuneista tiedostoista ja niihin liittyvistä metatiedoista.

Ohjelmisto saattaa kerätä Tietoja ja Tietomurtoja seuraavilla toiminnoilla:

i. LiveGrid-mainejärjestelmätoiminto kerää ja lähettää Tietomurtoihin liittyviä yksisuuntaisia hash-tunnisteita Toimittajalle. Tämä toiminto on otettu käyttöön Ohjelmiston vakioasetuksissa.

ii. LiveGrid-palautejärjestelmään kuuluu tunkeutumistietojen ja niihin liittyvien metatietojen muiden tietojen kerääminen ja lähettäminen Toimittajalle. Loppukäyttäjä voi aktivoida tämän toiminnon Ohjelmiston asennusprosessin aikana.

Toimittaja saa käyttää saamiaan tietoja ja tunkeutumistietoja vain tunkeutumisen analysointiin ja tutkimiseen, Ohjelmiston parantamiseen ja Käyttöoikeuden todentamisen parantamiseen. Toimittaja on varmistettava asianmukaisesti, että saadut tunkeutumistiedot ja muut tiedot pysyvät turvassa. Kun tämä Ohjelmiston toiminto aktivoidaan, Toimittaja voi kerätä ja käsitellä tunkeutumistietoja ja muita tietoja Tietosuojakäytännössä eritellyllä tavalla ja asiaankuuluvan lainsäädännön mukaisesti. Nämä toiminnot voi poistaa käytöstä milloin tahansa.

Tämän Sopimuksen mukainen käyttötarkoitus edellyttää, että tietoja kerätään, käsitellään ja tallennetaan Tietosuojakäytännön mukaisesti, jotta Toimittaja voi tunnistaa Sinut. Hyväksyt täten, että Toimittaja tarkistaa omilla keinoillaan, käytätkö Ohjelmistoa tämän Sopimuksen ehtojen mukaisesti. Hyväksyt täten, että tämän Sopimuksen mukainen käyttötarkoitus edellyttää, että tietoja siirretään Ohjelmiston ja Toimittajan tai sen liiketoimintakumppaneiden tietokonejärjestelmien välisen tietoliikenteen yhteydessä osana Toimittajan jakelu- ja tukiverkostoa, mikä varmistaa Ohjelmiston toimivuuden ja käyttövaltuutuksen ja Toimittajan oikeuksien suojauksen.

Tämän Sopimuksen solmimisen jälkeen Toimittajalla tai sen liikekumppaneilla on laskutustarkoituksessa, tämän Sopimuksen toteuttamistarkoituksessa ja ilmoitusten lähettämistarkoituksessa oikeus siirtää, käsitellä ja tallentaa tietoja, joilla Sinut voidaan tunnistaa. Hyväksyt täten ilmoitukset ja viestit, mukaan lukien rajoituksetta markkinointitiedot.

Tietosuoja, henkilötietojen suojausta ja Sinun tietosubjektioikeuksiasi koskevat tiedot on eritelty Tietosuojakäytännössä, joka on saatavilla Toimittajan sivustosta ja käytettävissä suoraan asennusprosessissa. VOIT MYÖS LUKEA TIEDOT OHJELMISTON OHJEOSIESTA.

5. Loppukäyttäjän oikeuksien harjoittaminen. Loppukäyttäjän oikeuksien harjoittamiseen olet oikeutettu sinä itse ja työntekijäsi. Sinulla on oikeus käyttää Ohjelmistoa vain toimintojesi turvaamiseen ja niiden tietokoneiden tai tietokonejärjestelmien suojaamiseen, joille olet hankkinut Käyttöoikeuden.

6. Oikeuksien rajoitukset. Et saa kopioida, jakaa etkä purkaa komponentteja etkä tehdä johdannaisia Ohjelmistosta. Kun käytät Ohjelmistoa, Sinun on noudatettava seuraavia rajoituksia:

a) Voit luoda Ohjelmistosta yhden kopion pysyvään tallennukseen tarkoitetulle tallennusvälineelle arkistointivarmuuskopiointia varten, mutta arkistoitua varmuuskopiota ei saa asentaa mihinkään muuhun tietokoneeseen tai käyttää siinä. Kaikki muut Ohjelmistosta tehdyt kopiot tulkitaan sopimusrikkomukseksi.

b) Et saa käyttää, muokata, kääntää etkä jäljentää Ohjelmistoa tai sen kopioita etkä siirtää sen oikeuksia mitenkään muutoin kuin tässä Sopimuksessa eritellyllä tavalla.

c) Et saa myydä, alilisensoida, liisata tai vuokrata tai lainata Ohjelmistoa tai käyttää Ohjelmistoa kaupallisten palveluiden toimittamiseen.

d) Ohjelmiston luontitapaa ei saa selvittää eikä Ohjelmistoa saa muuntaa eikä purkaa tai muutoin yrittää selvittää Ohjelmiston lähdekoodia, ellei tätä rajoitusta ole erikseen lailla kielletty.

e) Hyväksyt, että käytät Ohjelmistoa vain kaikkien lainkäyttöalueella sovellettavien lakien mukaisesti, mukaan lukien rajoituksetta tekijänoikeuksia ja muita immateriaalioikeuksia koskevat sovellettavat rajoitukset.

f) Sitoudut käyttämään ohjelmistoa ja sen toimintoja vain tavoilla, jotka eivät rajoita näiden palvelujen käyttöä muilta loppukäyttäjiltä. Palveluntarjoaja pidättää oikeuden rajoittaa yksittäisille loppukäyttäjille tarjottavia palveluja, jotta palveluja voitaisiin tarjota mahdollisimman monelle loppukäyttäjälle. Tarjottavien palvelujen rajoittaminen voi tarkoittaa myös ohjelmiston kaikkien toimintojen täydellistä käytön estämistä ja ohjelmiston tiettyihin toimintoihin liittyvien Tietojen ja Informaation poistamista palveluntarjoajan tai kolmansien osapuolten palvelimilta.

g) Hyväksyt, ettet tee mitään käyttöoikeusavaimeen liittyviä, tämän Sopimuksen vastaisia toimia tai toimia, jotka johtavat käyttöoikeusavaimen päätymiseen henkilölle, jolla ei ole oikeutta Ohjelmistoon, kuten siirrä käytettyä tai käyttämätöntä käyttöoikeusavainta missään muodossa tai kopioi tai jaa luvatta kopioitua tai luotua käyttöoikeusavainta tai käytä Ohjelmistoa joltakin muulta taholta kuin Toimittajalta hankituilla käyttöoikeusavaimella.

7. Tekijänoikeus. Ohjelmisto ja sen kaikki oikeudet, muun muassa rajoituksetta omistusoikeudet ja immateriaalioikeudet, kuuluvat ESETille ja/tai sen lisensoijille. Niitä suojaavat kansainvälisten sopimusten määräykset ja soveltuvien osien kaikkien niiden maiden kansalliset lait, joissa Ohjelmistoa käytetään. Ohjelmiston rakenne, jäsennys ja koodi ovat ESETin ja/tai sen lisensoijien liikesalaisuuksia ja luottamuksellisia tietoja. Kohdassa 6(a) mainittua poikkeusta lukuun ottamatta Ohjelmistoa ei saa kopioida. Kaikki kopiot, joiden oikeudet Sinulla tämän sopimuksen mukaisesti on, sisältävät samat tekijänoikeudet ja muut ohjelmistossa näkyvät omistusoikeutta koskevat ilmoitukset. Jos selvität Ohjelmiston lähdekoodin luontitavan, muunat lähdekoodia, purat sen tai muutoin yrität selvittää sen tämän Sopimuksen ehtoja rikkovalla tavalla, hyväksyt täten, että kaikki tällä tavalla hankitut tiedot siirretään automaattisesti ja peruuttamattomasti Toimittajalle, joka myös saa tietojen omistusoikeuden täysimittaisesti, siitä hetkestä lähtien, kun kyseiset tiedot hankitaan ja huolimatta Toimittajan oikeuksista suhteessa tämän Sopimuksen rikkomiseen.

8. Oikeuksien pidättäminen. Toimittaja pidättää täten kaikki Ohjelmistoon liittyvät oikeudet lukuun ottamatta oikeuksia, jotka on myönnetty erikseen tämän Sopimuksen ehtojen mukaisesti Sinulle Ohjelmiston Loppukäyttäjänä.

9. Eri kieliversiot, monimediaohjelmisto ja useat kopiot. Jos Ohjelmisto tukee useita alustoja tai kieliä tai jos saat useita kopioita ohjelmistosta, Ohjelmistoa saa käyttää vain siinä määrässä tietokonejärjestelmiä ja vain niissä versioissa, joille Käyttöoikeus on hankittu. Et saa myydä, vuokrata, leasing-vuokrata, alilisenoida, lainata tai siirtää mitään Ohjelmiston versiota tai kopiota, jota et itse käytä.

10. Sopimuksen voimassaoloaika ja lopettaminen. Tämä sopimus on voimassa tämän sopimuksen ehtojen hyväksymispäivästä alkaen. Voit päättää tämän Sopimuksen poistamalla pysyvästi, tuhoamalla tai palauttamalla omalla kustannuksellasi Ohjelmiston, kaikki sen varmuuskopiot ja siihen liittyvät materiaalit, jotka olet saanut Toimittajalta tai sen liikekumppaneilta. Sopimuksen päättymistavasta riippumatta kohtien 7, 8, 11, 13, 19 ja 21 ehdot jäävät voimaan ilman ajallista rajoitusta.

11. LOPPUKÄYTTÄJÄÄ KOSKEVAT ILMOITUKSET. LOPPUKÄYTTÄJÄNÄ HYVÄKSYT, ETTÄ OHJELMISTO TOIMITETAAN "SELLAISENAAN" ILMAN MINKÄÄNLAISIA SUORIA TAI EPÄSUORIA TAKUITA SOVELLETTAVAN LAIN SALLIMISSA MÄÄRIN. TOIMITTAJA, SEN LISENSOIJAT TAI TYTÄRYHTIÖT TAI TEKIJÄNOIKEUKSIEN OMISTAJAT EIVÄT ANNA MITÄÄN SUORIA TAI EPÄSUORIA ESITYKSIÄ TAI TAKUITA MUKAAN LUKIEN RAJOITUKSETTA TAKUUT SOVELTUVUUDESTA KAUPANKÄYNTIIN TAI TIETTYYN KÄYTTÖTARKOITUKSEEN JA TAKUUT SIITÄ, ETTÄ OHJELMISTO EI RIKO MINKÄÄN KOLMANNEN OSAPUOLEN PATENTTEJA, TEKIJÄNOIKEUKSIA, TAVARAMERKKEJÄ TAI MUITA OIKEUKSIA. TOIMITTAJA TAI MUUT OSAPUOLET EIVÄT ANNA MITÄÄN TAKUUTA SIITÄ, ETTÄ

OHJELMISTON SISÄLTÄMÄT TOIMINNOT VASTAAVAT VAATIMUKSIASI TAI ETTÄ OHJELMISTO TOIMII KESKEYTYKSETTÄ JA VIRHEITTÄ. VASTAAT ITSE OHJELMISTON VALINTAAN, ASENNUKSEEN JA KÄYTTÖÖN SEKÄ OHJELMISTON AVULLA SAAVUTETTAVIIN TULOKSIIN LIITTYVISTÄ RISKEISTÄ.

12. **Ei muita velvollisuuksia.** Tämä Sopimus ei aseta Toimittajalle eikä sen lisensoijille mitään muita velvoitteita kuin mitä tässä on eritelty.

13. **TAKUUNRAJOITUS.** TOIMITTAJA, SEN TYÖNTEKIJÄT TAI SEN LISENSOIJAT EIVÄT LAIN SALLIMISSA MÄÄRIN OLE MISSÄÄN TAPAUKSESSA VASTUUSSA VOITTOJEN, TUOTTOJEN TAI MYYNIN MENETYKSESTÄ, TIETOJEN MENETYKSESTÄ, VARAOSIEN TAI PALVELUIDEN HANKINTAAN LIITTYVISTÄ KULUISTA, OMAISUUDELLE AIHEUTUVISTA VAHINGOISTA, HENKILÖVAHINGOISTA, LIIKETOIMINNAN KESKEYTYMISESTÄ, LIIKETOIMINTAAN LIITTYVIEN TIETOJEN MENETYKSESTÄ TAI MUISTA ERITYISISTÄ, SUORISTA, EPÄSUORISTA, TAHATTOMISTA, TALOUDELLISISTA, KORVAAMISESTA AIHEUTUVISTA, RIKOLLISISTA, ERITYISISTÄ TAI SEURANNAISISTA VAHINGOISTA NIIDEN SYNTYTAIVASTA RIIPPUMATTA, OLIPA KYSEESSÄ SOPIMUKSEEN, TAHALLISEEN RIKKOMUKSEEN, LAIMINLYÖNTIIN TAI MUUHUN SEIKKAAN LIITTYVÄ SYY, JOKA ON JOHTUNUT OHJELMISTON KÄYTÖSTÄ TAI SEN KÄYTÖN ESTYMISESTÄ, VAIKKA TOIMITTAJALLE TAI SEN LISENSOIJALLE OLISI ILMOITETTU KYSEISTEN VAHINKOJEN MAHDOLLISUUDESTA. KOSKA TIETYISSÄ MAISSA JA TIETYILLÄ LAINKÄYTTÖALUEILLA EI SALLITA VASTUUN POISSULKEMISTA MUTTA SAATETAAN SALLIA VASTUUN RAJOITTAMINEN, TOIMITTAJAN, SEN TYÖNTEKIJÖIDEN TAI LISENSOIJIEN VASTUU RAJOITTUU TÄLLAISISSA TILANTEISSA KÄYTTÖOIKEUDESTA MAKSETTUUN SUMMAAN.

14. Mikään tässä Sopimuksessa ei rajoita kenenkään kuluttajan ominaisuudessa toimivan osapuolen lainsäädäntöön perustuvia oikeuksia, jos Sopimus on ristiriidassa niiden kanssa.

15. **Tekninen tuki.** ESET tai ESETin valtuuttamat kolmannet osapuolet antavat teknistä tukea oman harkintansa mukaan ilman mitään takuita tai julkilausumia. Loppukäyttäjää edellytetään varmuuskopioimaan kaikki tiedot sekä ohjelmistoon ja ohjelmaan liittyvä ympäristö ennen teknisen tuen pyytämistä. ESET ja/tai ESETin valtuuttamat kolmannet osapuolet eivät ole vastuussa teknisen tuen pyytämisestä aiheutuvasta tietojen, omaisuuden, ohjelmistojen tai laitteistojen menetyksestä tai voittojen menetyksestä. ESET ja/tai ESETin valtuuttamat kolmannet osapuolet pidättävät oikeuden määrittää, että ongelman selvittäminen ei kuulu teknisen tuen piiriin. ESET pidättää oikeuden kieltäytyä toimittamasta teknistä tukea tai keskeyttää tai lopettaa sen toimittamisen oman harkintansa mukaan. Teknisen tuen saaminen saattaa edellyttää tämän Tietosuojakäytännön mukaisten käyttöoikeustietojen ja muiden tietojen toimittamista.

16. **Käyttöoikeuden siirtäminen.** Ohjelmiston voi siirtää tietokonejärjestelmästä toiseen, ellei Sopimuksen ehdoissa toisin mainita. Jos Sopimuksen ehdoissa ei toisin mainita, Loppukäyttäjällä on oikeus siirtää Käyttöoikeus ja kaikki tässä Sopimuksessa myönnetty oikeudet pysyvästi toiselle Loppukäyttäjälle vain Toimittajan luvalla sillä ehdolla, että (i) alkuperäinen Loppukäyttäjä ei säilytä mitään Ohjelmiston kopioita, (ii) oikeudet siirretään suoraan eli alkuperäiseltä Loppukäyttäjältä uudelle Loppukäyttäjälle, (iii) uusi Loppukäyttäjä hyväksyy kaikki tämän Sopimuksen ehtojen mukaiset alkuperäisen Loppukäyttäjän oikeudet ja velvoitteet, (iv) alkuperäinen Loppukäyttäjä toimittaa uudelle Loppukäyttäjälle dokumentaation, joka vahvistaa Ohjelmiston aitouden kohdassa 17 eritellyllä tavalla.

17. **Ohjelmiston aitouden vahvistaminen.** Loppukäyttäjä voi esittää Ohjelmiston käyttöoikeuden jollakin seuraavista tavoista: (i) Toimittajan tai Toimittajan nimittämän kolmannen osapuolen antamalla käyttöoikeustodistuksella, (ii) kirjallisella käyttöoikeussopimuksella, jos sellainen on tehty, (iii) Toimittajalle lähetetyllä sähköpostilla, joka sisältää päivitysten käyttöönottoon tarvittavat käyttöoikeustiedot (käyttäjänimen ja salasanan). Ohjelmiston aitouden vahvistamiseen saatetaan tarvita Tietosuojakäytännön mukaisesti toimitettavat Käyttöoikeuden tiedot ja Loppukäyttäjän tunnistetiedot.

18. **Viranomaisten ja Yhdysvaltojen valtionhallinnon käyttöoikeudet.** Ohjelmisto toimitetaan viranomaisille, Yhdysvaltojen valtionhallinto mukaan lukien, tässä Sopimuksessa eriteltyjen käyttöoikeuksien ja rajoitusten

mukaisesti.

19. Kauppaa säätelevän lainsäädännön noudattaminen.

a) Et saa suoraan tai epäsuorasti viedä, viedä uudelleen, siirtää tai muutoin tehdä ohjelmistoa käytettäväksi kenellekään etkä käyttää sitä millään tavalla tai osallistaa sitä mihinkään toimenpiteeseen, joka voisi johtaa siihen, että ESET tai sen holding-yhtiö, tytäryhtiö tai jokin sen holding-yhtiön tytäryhtiö tai jokin sen holding-yhtiön hallinnoima taho (jäljempänä yhteisesti "tytäryhtiöt") rikkoo kauppaa säätelevää lainsäädäntöä tai muutoin vaikuttaa negatiivisesti kauppaa säätelevään lainsäädäntöön, johon kuuluvat

i. lait, joilla säädellään, rajoitetaan tai asetetaan tavaroiden, ohjelmistojen, tekniikan tai palvelujen viennille, uudelleenviennille tai siirrolle lisensointivaatimuksia, joita on voinut asettaa tai soveltaa mikä tahansa valtionhallinto, osavaltio tai viranomainen Yhdysvalloissa, Singaporessa, Isossa-Britanniassa, Euroopan unionissa tai jossakin sen jäsenvaltiossa, tai missä tahansa maassa, jossa sopimusvelvoitteita noudatetaan tai jossa ESET tai jokin sen tytäryhtiö toimii (jäljempänä "vientä säätelevä lainsäädäntö"), ja

ii. kaikki taloudelliset, rahoitukselliset, kaupankäyntiin liittyvät tai muut pakotteet, rajoitukset, kauppasaarrot, tuonti- tai vientikiellot, varojen tai resurssien siirtokiellot tai palvelujen suorituskiellot tai vastaavat toimenpiteet, joita on voinut määrätä mikä tahansa valtionhallinto, osavaltio tai viranomainen Yhdysvalloissa, Singaporessa, Isossa-Britanniassa, Euroopan unionissa tai jossakin sen jäsenvaltiossa, tai missä tahansa maassa, jossa sopimusvelvoitteita noudatetaan tai jossa ESET tai jokin sen tytäryhtiö toimii (jäljempänä "pakotteita koskeva lainsäädäntö").

b) ESETillä on oikeus pidättäytyä näihin ehtoihin liittyvien velvoitteidensa noudattamisesta tilapäisesti tai kokonaan heti, jos:

i. ESET määrittää oman kohtuullisen arvionsa mukaan, että käyttäjä on rikkonut tai todennäköisesti rikkoo sopimuksen artiklan 19.a ehtoa tai

ii. loppukäyttäjään ja/tai ohjelmistoon kohdistuu kauppaa säätelevän lainsäädännön mukaisia uusia rajoituksia, minkä seurauksena ESET määrittää oman kohtuullisen näkemyksensä mukaan, että se ei voi enää tarjota sopimuksen mukaisia velvoitteitaan ilman, että ESET tai sen tytäryhtiö rikkoisi kauppaa säätelevää lainsäädäntöä tai kokisi siitä muutoin negatiivisia seuraamuksia.

c) Mitään sopimuksessa ei ole tarkoitettu eikä mitään siinä olevaa pidä tulkita siten, että kumpikaan osapuoli voisi toimia tai olla toimimatta (tai sopia toimimisesta tai toimimattomuudesta) millään tavalla, joka ei noudata sovellettavaa kauppaa säätelevää lainsäädäntöä tai josta voitaisiin rangaista tai joka voitaisiin kieltää kyseisen lainsäädännön nojalla.

20. Ilmoitukset. Kaikki ilmoitukset, palautettava Ohjelmisto ja Dokumentaatio on lähetettävä osoitteeseen: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

21. Sovellettava laki. Tähän Sopimukseen sovelletaan Slovakian tasavallan lakeja. Loppukäyttäjä ja Toimittaja sopivat täten, että lakiristiriistojen riidanratkaisumenettelyitä ja YK:n kansainvälistä tavarankäytön kauppaa koskevista sopimuksista tehtyä yleissopimusta ei sovelleta tähän Sopimukseen. Hyväksyt erikseen, että kaikki tästä Sopimuksesta aiheutuvat, Toimittajaa koskevat kiistat tai vaatimukset tai kaikki Ohjelmiston käyttöön liittyvät kiistat tai vaatimukset käsitellään Bratislava I:n käräjäoikeudessa, ja hyväksyt tämän tuomioistuimen päätäntävällän.

22. Yleiset ehdot. Jos jokin tämän Sopimuksen ehto ei ole voimassa tai sitä ei voida panna toimeen, se ei vaikuta Sopimuksen muiden ehtojen voimaansaamiseen, vaan ne pysyvät voimassa ja toimeenpantavina Sopimuksessa eriteltyjen ehtojen mukaan. Jos tämän sopimuksen kieliversioissa ilmenee eroavaisuuksia, englanninkielinen versio on voimassa. Tätä sopimusta voi muokata vain kirjallisesti, ja allekirjoitusoikeus on vain Toimittajan

valtuuttamalla edustajalla tai erikseen tähän toimenpiteeseen annetulla valtakirjalla.

Tämä muodostaa koko Sopimuksen Toimittajan ja Sinun välille, ja se korvaa kaikki aikaisemmat Ohjelmistoon liittyvät esitykset, keskustelut, toimenpiteet, viestinnän tai mainonnan.

EULA ID: BUS-STANDARD-20-01

Privacy Policy

ESET, spol. s r. o., kotipaikka Einsteinova 24, 851 01 Bratislava, Slovakia, merkitty Bratislavan I. kärjäoikeuden kaupparekisteriin, osa Sro, rekisteröintinumeroilla 3586/B, BIN: 31333532, haluaa toimia rekisterinpitäjänä ("ESET" tai "me") läpinäkyvällä tavalla asiakkaidensa henkilötietoja ja tietosuojaa käsiteltäessä. Tämä tietosuojakäytäntö on julkaistu tämän periaatteen mukaisesti ja sen ainoa tarkoitus on ilmoittaa asiakkaallemme ("loppukäyttäjä" tai "sinä") seuraavista asioista:

- henkilötietojen käsittely,
- tietojen luottamuksellisuus,
- rekisteröidyn oikeudet.

Henkilötietojen käsittely

Tuotteeseemme sisältyvät ESETin tarjoamat palvelut toimitetaan loppukäyttäjän käyttöoikeussopimuksen ("käyttöoikeussopimus") ehtojen mukaan, mutta osa niistä saattaa edellyttää erityistä huomiota. Haluamme ilmoittaa tietoja palvelujemme toimittamiseen kuuluvasta tietojen keräämisestä. Tarjoamme erilaisia palveluja, joita kuvataan EULA: ssa ja tuoteasiakirjoissa, kuten päivitys- / päivityspalvelu, ESET LiveGrid®, suojaus tietojen väärinkäytöstä, tuesta jne. Jotta kaikki toimisi, meidän on kerättävä seuraavat tiedot:

- Päivitystilastot ja muut tilastot, joissa on tietoja asennusprosessista ja tietokoneesta, kuten tuotteemme asennusympäristöstä, ja tuotteidemme toiminnoista, kuten käyttöjärjestelmästä, laitteistosta, asennustunnuksista, käyttöoikeustunnuksista, IP-osoitteesta, MAC-osoitteesta ja tuotteen kokoonpanoasetuksista.
- Tunkeutumisiin liittyvät yksisuuntaiset hajautustunnisteet. Ne ovat osa ESET LiveGrid® -mainejärjestelmää, joka parantaa haittaohjelmien suojausratkaisujen tehokkuutta vertaamalla tarkistettuja tiedostoja sallittujen ja kiellettyjen kohteiden pilvitietokantaan.
- Epäilyttävien kohteiden näytteet ja metatiedot osana ESET LiveGrid® -palautejärjestelmää, jonka avulla ESET voi reagoida välittömästi loppukäyttäjien tarpeisiin ja pitää uusimmilta uhilta suojautumisen toimivana. Me tarvitsemme sinulta tietoja

Otunkeutumisista esimerkiksi näytteinä viruksista ja muista haitallisista ohjelmista ja epäilyttävistä, ongelmallisista, mahdollisesti tarpeettomista tai mahdollisesti vaarallisista objekteista, kuten ohjelmätiedostoista ja sähköpostiviesteistä, jotka olet ilmoittanut tai tuotteemme on merkinnyt roskapostiksi

Opaikallisen verkon laitteista, kuten laitteen tyyppin, valmistajan, mallin ja/tai nimen

OInternetin käytöstä, kuten IP-osoitteen ja maantieteellisen sijainnin, IP-paketit, URL-osoitteet ja Ethernet-kehykset

Okaatumistapauksissa laadituista vedostiedostoista ja niiden sisältämistä tiedoista.

Vaikka emme tarkoituksellisesti kerää muita tietoja, niiden satunnaista keruuta voi olla mahdoton estää. Vahingossa (tietämättäsi tai luvattasi) kerätyt tiedot voivat esimerkiksi sisältyä itse haittaohjelmaan tai olla osa tiedostonimiä tai URL-osoitteita. Tarkoituksemme ei ole, että nämä tiedot muodostavat osan järjestelmiämme tai että niitä käsitellään tässä tietosuojakäytännössä ilmoitetulla tavalla.

- Käyttöoikeuteen liittyvät tiedot, kuten käyttöoikeustunnus ja henkilötiedot, kuten nimi, sukunimi, osoite, sähköpostiosoite, ovat pakollisia laskutustarkoituksissa, käyttöoikeuden aitouden vahvistamisessa ja palvelujemme toimittamisessa.
- Yhteystietoja ja tukipyyntöissä olevia tietoja saatetaan tarvita tukipalveluihin. Saatamme valitsemasi yhteydenottokanavan mukaan kerätä sähköpostiosoitteesi, puhelinnumerosi, käyttöoikeustiedot, tuotetiedot ja tukitapauksesi kuvauksen. Sinulta saatetaan pyytää muita tietoja tukipalvelun toimittamiseksi.

Tietojen luottamuksellisuus

ESET on jakelu-, palvelu- ja tukiverkostoonsa kuuluvien tytäryhtiöidensä tai kumppaneidensa kautta maailmanlaajuisesti toimiva yritys. ESETin käsittelemiä tietoja saatetaan siirtää tytäryhtiöille tai kumppaneille tai niiltä ESETille käyttöoikeussopimuksen mukaisten ehtojen täyttämiseksi esimerkiksi palvelujen toimittamisen tai tuen tai laskutuksen osalta. Saatamme sijaintisi ja valitsemasi palvelun mukaan edellyttää sinua siirtämään tietojasi maahan, joka ei täytä Euroopan komission vastaavuusmääräyksiä. Myös tässä tapauksessa kaikki tietojen siirrot tehdään tietosuojalainsäädännön mukaisesti ja vain tarvittaessa. Vakiosopimuslausekkeet, sitovat yrityssäännöt ja muut asianmukaiset turvatoimet on toteutettava poikkeuksetta.

Teemme parhaamme estääksemme tietojen säilytysajan pitenemisen tarpeettomasti käyttöoikeussopimuksen mukaisia palveluja toimittaessamme. Säilytysjakso saattaa olla käyttöoikeuden voimassaoloa pidempi, jotta tilauksen uusinta sujuu vaivattomasti. ESET LiveGrid® -järjestelmän minimaalisessa määrin nimettömästi keräämiä tilastotietoja ja muita tietoja saatetaan käsitellä tilastointitarkoituksissa.

ESET toteuttaa asianmukaiset tekniset ja organisaatiotason toimenpiteet, joilla varmistetaan mahdollisten riskien edellyttämä tietoturvasäilytys. Teemme parhaamme varmistaaksemme käsittelyjärjestelmiemme ja -palvelujemme jatkuvan luottamuksellisuuden, eheyden, saatavuuden ja kestävyys. Jos tietorikkomus kuitenkin vaarantaa oikeuksiasi ja vapauksiasi, olemme valmiina ilmoittamaan siitä valvovalle viranomaiselle sekä rekisteröidyille käyttäjille. Rekisteröitynä sinulla on oikeus tehdä valitus valvovalle viranomaiselle.

Rekisteröidyn oikeudet.

ESET noudattaa Slovakian lakeja ja on Euroopan unionin tietosuojalainsäädännön alainen. Sovellettavien tietosuojalakien mukaisesti sinulla on rekisteröitynä oikeus:

- pyytää henkilötietojasi ESETiltä,
- korjata virheelliset henkilötiedot (ja myös lisätä puuttuvat henkilötiedot),
- pyytää henkilötietojesi poistoa,
- pyytää henkilötietojesi käsittelyn rajoittamista,
- kieltää käsittely,
- tehdä valitus ja,
- siirtää tiedot.

Jos haluat käyttää jotakin rekisteröidyn käyttäjän oikeutta tai sinulla on kysyttävää, lähetä viesti osoitteeseen:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk