ESET ENDPOINT SECURITY 6

Brukerhåndbok

Microsoft® Windows® 10/8.1/8/7/Vista/XP x86 SP3/XP x64 SP2
Klikk her for å laste ned den nyeste versjonen av dette dokumentet

ENJOY SAFER TECHNOLOGY™

ESET **ENDPOINT SECURITY 6**

Internasjonal kundestøtte: www.eset.com/support

REV. 1/18/2016

Innhold

Innhold

1. ESET Endpoint Security

ESET Endpoint Security 6 representerer en ny tilnærming til virkelig integrert datamaskinsikkerhet. Den nyeste versjonen av ThreatSense®-skannemotoren, kombinert med vår tilpassede personlige brannmur og antispammodul, fungerer raskt og presist. Resultatet er et intelligent system som alltid er på vakt for å oppdage angrep og skadelig programvare som utsetter datamaskinen for fare.

ESET Endpoint Security 6 er en komplett sikkerhetsløsning som er et resultat av vårt langsiktige arbeid for å kombinere maksimal beskyttelse og et minimalt systemavtrykk. Den avanserte teknologien, som er basert på kunstig intelligens, er i stand til proaktivt å bekjempe virus, spyware, trojanske hester, ormer, adware, rootkits og andre typer angrep som utføres via Internett – uten å redusere systemytelsen eller føre til forstyrrelser på datamaskinen.

ESET Endpoint Security 6 er først og fremst utformet for bruk på arbeidsstasjoner i miljøer med små virksomheter/bedrifter. Kombinert med ESET Remote Administrator kan du enkelt håndtere et hvilket som helst antall klientarbeidsstasjoner, bruke policyer og regler, overvåke gjenkjenning og konfigurere eksternt fra en hvilken som helst datamaskin i nettverket.

1.1 Hva er nytt?

Det grafiske brukergrensesnittet til ESET Endpoint Security har blitt fullstendig omformet for å gi bedre synlighet og en mer intuitiv brukeropplevelse. Noen av de mange forbedringene i ESET Endpoint Security versjon 6 inkluderer:

Forbedret funksjonalitet og brukervennlighet

- Nettkontroll – definerer én enkelt regel for flere URL-er, eller definerer forskjellige policyer for forskjellige nettverksområder. «Myke» blokkeringspolicyer er nytt for versjon 6 i tillegg til evnen til delvis å tilpasse blokkerings- og advarselssiden.
- Personlig brannmur – Du kan nå opprette brannmurregler direkte fra loggen eller -varslingsvinduet og tilordne profiler til nettverksgrensesnitt.
- En ny Botnet-beskyttelse – hjelper med å oppdage skadelig programvare ved å analysere nettverkskommunikasjonsmønstre og -protokoller.
- Enhetskontroll – inkluderer nå evnen til å fastslå enhetstype og serienummer, og definere enkelte regler for flere enheter.
- En ny Smart modus for HIPS – befinner seg mellom automatisk og interaktiv modus. Evne til å identifisere mistenkelige aktiviteter og skadelige prosesser i systemet.
- Oppdatering/Speil-forbedringer – Du kan nå oppdatere mislykkede oppdateringer av virussignaturdatabasen og/eller produktmoduler.
- Ny tilnærming til fjernadministrasjon av datamaskinene med ESET Remote Administrator – Send logger når ERA installeres på nytt eller i forbindelse med testing, installer ESET-sikkerhetsløsninger eksternt, få en oversikt over sikkerhetstilstanden til nettverksmiljøet ditt og sorter ulike data for senere bruk.
- Forbedringer av brukergrensesnittet – Legger til et ettklikksalternativ for å kjøre en manuell oppdatering av virussignaturdatabasen og moduler fra systemstatusfeltet i Windows. Støtte for berøringsskjermer og skjermer med høy oppløsning.
- Forbedret deteksjon og fjerning av tredjeparts sikkerhetsløsninger.

Ny funksjonalitet

- Anti-Phishing – Beskytter deg mot forsøk på å stjele passord og annen sensitiv informasjon ved å begrense tilgang til skadelige nettsteder som utgir seg for å være legitime nettsteder.
- Forbedret skannehastigheter – bruker et lokal hurtigbuffer i virtualiserte miljøer.

Deteksjons – og beskyttelsesteknologier

- Forbedret installasjonshastighet og pålitelighet.
- Avansert minneskanner – Overvåker prosessatferd og skanner skadelige prosesser når de fjerner maskering i minnet.
- Forbedret blokkering av utnyttelse – utviklet for å befeste typer programmer som utnyttes ofte, som for eksempel nettlesere, PDF-lesere, e-postklienter og MS Office-komponenter. Blokkering av utnyttelse støtter nå Java og hjelper med å forbedre påvisning og beskyttelse fra disse typer sårbarheter.
- Forbedret deteksjon og fjerning av rootkits.
- Beskyttelse mot sårbarhet – Mer avanserte filtreringsalternativer for å oppdage ulike typer angrep og sårbarheter.
- Skanning i inaktiv tilstand – Utfører en stille skanning på alle lokale stasjoner når datamaskinen din er i inaktiv tilstand.

1.2 Systemkrav

For å oppnå en sømløs drift av ESET Endpoint Security, må systemet oppfylle følgende krav til maskinvare og programvare:

Prosessorer som støttes: Intel® eller AMD x86-x64

Operativsystemer: Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 32-bit/XP SP2 64-bit

1.3 Forebygging

Når du arbeider på datamaskinen, og spesielt når du er på Internett, må du være klar over at ingen antivirusprogrammer kan fjerne all risiko for infiltrasjoner og angrep. For å oppnå maksimal beskyttelse er det viktig at du bruker antivirusløsningen riktig samt følger noen nyttige regler:

Oppdater jevnlig

I følge statistikker fra ESET Live Grid blir tusenvis av nye, unike infiltrasjoner opprettet hver dag for å forbigå eksisterende sikkerhetstiltak og gi skaperne fortjeneste – på brukernes kostnad. Spesialistene ved ESETs viruslaboratorier analyserer disse truslene hver dag, og forbereder og lanserer oppdateringer for å kontinuerlig forbedre beskyttelsesnivået for brukerne våre. For å sikre at disse oppdateringene er så effektive som mulig er det viktig at oppdateringer konfigureres riktig på systemet ditt. Du finner mer informasjon om hvordan du konfigurerer oppdateringer i kapittelet Oppsett for oppdatering.

Last ned sikkerhetsoppdateringer

Forfatterne av skadelig programvare foretrekker å utnytte forskjellige systemsvakheter for å øke effektiviteten av den skadelige koden de sprer. Med dette i tankene følger programvareprodusenter nøye med på om det finnes svakheter i programmene de lager, og lanserer regelmessige sikkerhetsoppdateringer som fjerner potensielle trusler. Det er viktig å laste ned disse sikkerhetsoppdateringene når de blir lansert. Microsoft Windows og nettlesere som Internet Explorer er to eksempler på programmer det regelmessig blir lansert sikkerhetsoppdateringer for.

Ta sikkerhetskopi av viktige data

Forfattere av skadelig programvare bryr seg ikke om hvem de rammer, og aktiviteten til skadelige programmer fører ofte til total funksjonsfeil i operativsystemet og tap av viktige data. Det er viktig å jevnlig sikkerhetskopiere viktige og følsomme data til en ekstern kilde, for eksempel DVD-er eller en ekstern harddisk. Dette vil gjøre det mye enklere og raskere å gjenopprette data i tilfelle systemfeil.

Skann datamaskinen for virus jevnlig

Oppdagelse av flere kjente og ukjente virus, ormer, trojanere og rootkits håndteres av modulen Sanntidsbeskyttelse av filsystemet. Dette betyr at en fil skannes med tanke på aktivitet fra skadelig programvare hver gang du åpner den. Vi anbefaler at du kjører en fullstendig Datamaskinskanning minst én gang i måneden, da skadelig programvare kan variere og virussignaturdatabasen oppdateres hver dag.

Følg grunnleggende sikkerhetsregler

Dette er den nyttigste og mest effektive regelen av alle – vær alltid forsiktig. I dag krever mange infiltrasjoner brukerintervensjon for å kjøres eller distribueres. Hvis du er forsiktig når du åpner nye filer, vil du spare mye tid og arbeid som ellers måtte brukes på å rense infiltrasjoner fra datamaskinen din. Her er noen nyttige retningslinjer:

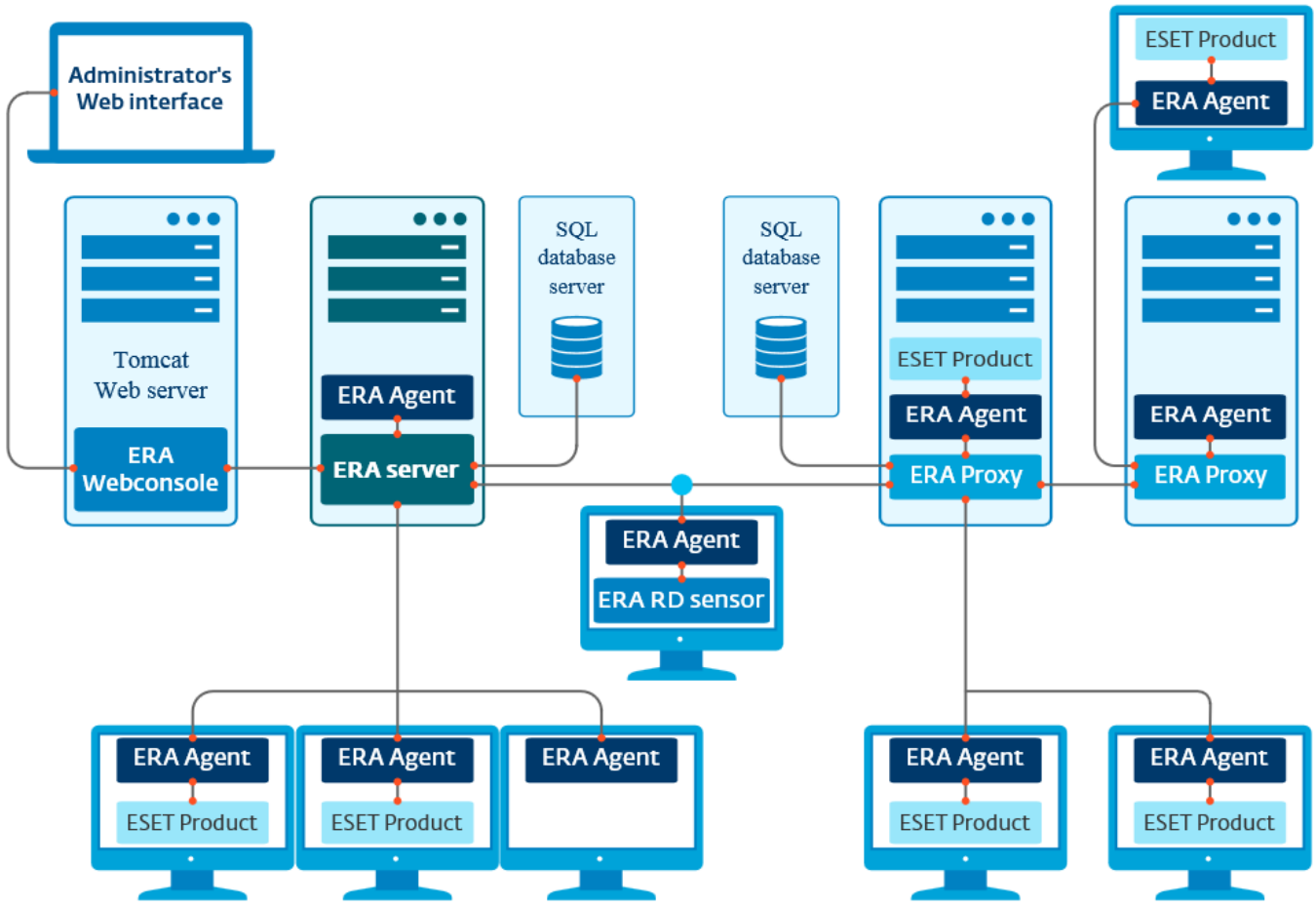
- Ikke besøk mistenkelige nettsteder med mange popup-vinduer og blinkende annonser.
- Vær forsiktig når du installerer gratisprogrammer, kodek-pakker osv. Bruk bare trygge programmer, og besøk bare trygge nettsteder.
- Vær forsiktig når du åpner e-postvedlegg, spesielt vedlegg til meldinger som kommer fra masseutsendelser og fra ukjente avsendere.
- Ikke bruk en administratorkonto for daglig arbeid på datamaskinen.

2. Dokumentasjon for brukere som er koblet til via ESET Remote Administrator

ESET Remote Administrator (ERA) er et program som lar deg administrere ESET-produkter i et nettverksmiljø fra én sentral plassering. Med ESET Remote Administrator-systemet for oppgavebehandling kan du installerer ESETs sikkerhetsløsninger på eksterne datamaskiner og reagere raskt på nye problemer og trusler. ESET Remote Administrator gir ikke beskyttelse mot skadelig kode, men er avhengig av tilstedeværelsen av ESETs sikkerhetsløsninger på hver klient.

ESETs sikkerhetsløsninger støtter nettverker som inkluderer flere plattformtyper. Nettverket ditt kan inneholde en kombinasjon av gjeldende Microsoft-, Linux-baserte og Mac OS-operativsystemer som kjører på mobilenheter (mobiltelefoner og nettbrett).

Bildet nedenfor viser en prøvearkitektur for et nettverket som er beskyttet med ESETs sikkerhetsløsninger som administreres av ERA:



MERKNAD: For mer informasjon, se ESET Remote Administrator brukerveiledning.

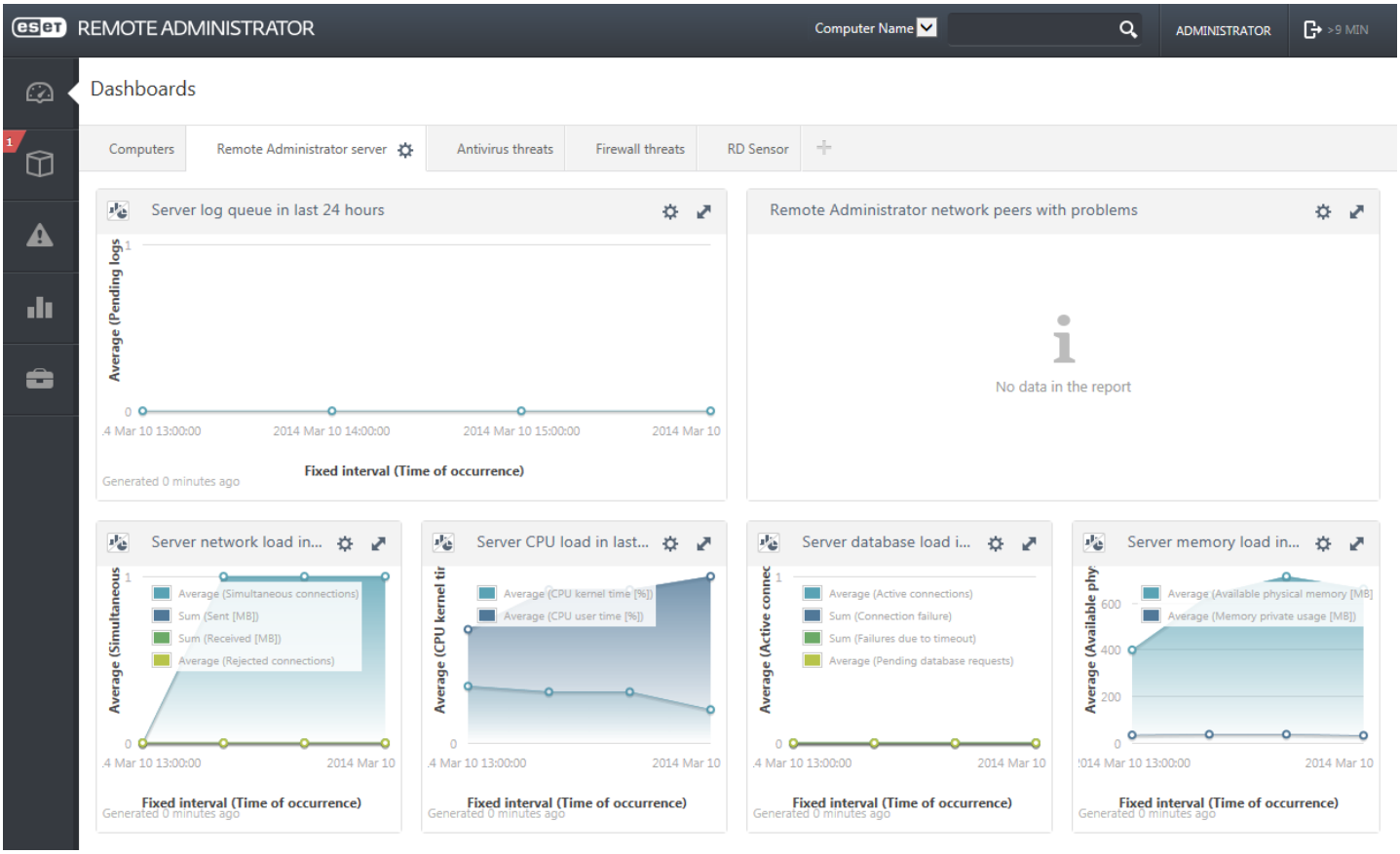
2.1 ESETs server for fjernadministrering

ESETs server for fjernadministrering er en primær komponent som hører til ESET Remote Administrator. Det er det overordnede programmet som behandler alle data som blir mottatt fra klienter som kobles til serveren (via ERA Agent). ERA Agent muliggjør kommunikasjon mellom klient og server. Data (klientlogger, konfigurasjoner, agentreplikeringer osv.) lagres i en database. For at data skal kunne behandles på riktig måte, krever ERA Server en stabil tilkobling til en databaseserver der data er lagret. Vi anbefaler at du installerer ERA Server og databasen din på separate servere for å optimalisere ytelse. Datamaskinen der ERA Server er installert må konfigureres for å akseptere alle Agent/Proxy/RD Sensor-tilkoblinger, som verifiseres ved bruk av sertifikater. Når den er installert, kan du åpne ERA nettkonsoll, som kobler til ERA Server (som man kan se i diagrammet). Fra nettkonsollen utføres alle ERA Server-handlinger når du administrerer ESET sikkerhetsløsninger innenfor nettverket ditt.

2.2 Nettkonsoll

ERA nettkonsoll er et nettbasert brukergrensesnitt som presenterer data fra ERA Server og lar deg administrere ESET sikkerhetsløsninger i nettverket ditt. Du kan få tilgang til nettkonsollen via en nettleser. Den viser en oversikt over statusen til klienter på nettverket, og kan brukes til å distribuere ESET-løsninger til uadministrerte datamaskiner eksternt. Du kan velge å gjøre nettserveren tilgjengelig fra internett, slik at du kan bruke ESET Remote Administrator nesten overalt og på alle mulige enheter.

Dette er nettkonsollens instrumentbord:



Hurtigsøk-verktøyet finner du øverst på nettkonsollen. Velg **Datamaskinnavn**, **IPv4**/**IPv6-adresse** eller **Trusselnavn** fra rullgardinmenyen, skriv inn søket i tekstfeltet og trykk på forstørrelsesglasset eller **Enter** for å søke. Dette vil ta deg til **Grupper**-delen, der søkeresultatet vises.

MERKNAD: For mer informasjon, se ESET Remote Administrator brukerveiledning.

2.3 Proxy

ERA Proxy er et annet komponent til ESET Remote Administrator og brukes til to ting. I et mellomstort eller enterprise-nettverk med mange klienter (f.eks. 10 000 klienter eller mer), kan du bruke ERA Proxy til å distribuere belastning mellom flere ERA-proxyer ved å bruke hoved-ERA Server. Den andre fordelen med ERA Proxy er at du kan bruke den når du kobler til et ekstern avdelingskontor med en svak lenke. Dette betyr at ERA Agenten på hver klient ikke kobler til hoved-ERA Server direkte via ERA Proxy, som er på samme lokalnettverk som avdelingskontoret. Denne konfigurasjonen frigjør linken til avdelingskontoret. ERA Proxy godtar tilkoblinger fra alle lokale ERA Agenter, summerer opp dataene fra dem og laster dem opp til hoved-ERA Serveren (eller en annen ERA Proxy). Dette gjør at nettverket kan imøtekomme flere klienter uten at kvaliteten på databasespørringene reduseres.

Avhengig av nettverkskonfigurasjonen, er det mulig for en ERA Proxy å koble til en annen ERA Proxy og deretter koble til hoved-ERA Serveren.

For at ERA Proxy skal fungere riktig, må vertsdatamaskinen der du installerte ERA Proxy ha en ESET Agent installert og må være tilkoblet det øvre nivået (enten ERA Server eller øvre ERA Proxy, hvis det er en) på nettverket.

2.4 Agent

ERA Agent er en viktig del av produktet ESET Remote Administrator. ESET sikkerhetsløsninger på klientmaskiner (for eksempel ESET Endpoint Security) kommuniserer med ERA Server via agenten. Denne kommunikasjonen gjør det mulig å behandle ESET-sikkerhetsløsninger på alle eksterne klienter fra en sentral plassering. Agenten samler informasjon fra klienten og sender den til serveren. Hvis serveren sender en oppgave for klienten, sendes den til agenten og agenten sender denne oppgaven til klienten. All nettverkskommunikasjon foregår mellom agenten og den øvre delen av ERA-nettverket – server og proxy.

ESET Agent kobler til serveren ved bruk av én av følgende tre metoder:

1. Klientens agent er direkte tilkoblet serveren.
2. Klientens agent er koblet til via en proxy som er koblet til serveren.
3. Klientens agent er koblet til serveren via flere proxier.

ESET Agent kommuniserer med ESET-løsninger som er installert på en klient, samler informasjon fra programmer på den klienten og sender konfigurasjonsinformasjonen den mottar fra serveren til klienten.

MERKNAD: ESET-proxien har sin egen agent som håndterer alle kommunikasjonsoppgaver mellom klienter, andre proxier og serveren.

2.5 RD Sensor

RD (Rogue Detection) Sensor er en del av ESET Remote Administrator og er utformet for å oppdage maskiner på nettverket. Dette er en praktisk måte å legge nye datamaskiner til ESET Remote Administrator på uten å måtte søke etter og legge dem til manuelt. Hver datamaskin som oppdages på nettverket vises i nettkonsollen, og legges til den standard **Alle**-gruppen. Herfra kan du gjøre ytterligere handlinger med hver av klientdatamaskinene.

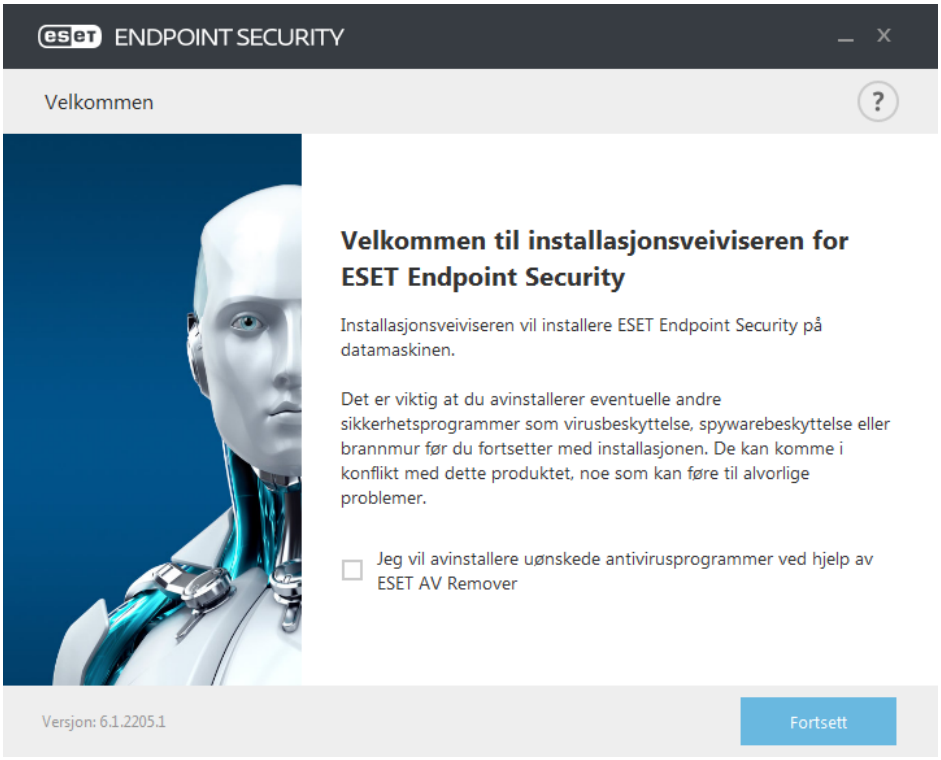
RD Sensor er et passivt lytteverktøy som oppdager datamaskiner som finnes på nettverket og sender informasjon om dem til ERA Server. ERA Server vurderer om datamaskinene som er funnet på nettverket er ukjente eller om de allerede administreres.

3. Bruke ESET Endpoint Security alene

Denne delen av brukerveiledningen er dedikert til brukere som bruker ESET Endpoint Security uten ESET Remote Administrator. Alle funksjoner og funksjonaliteter i ESET Endpoint Security er fullt tilgjengelig avhengig av brukerens kontorettigheter.

3.1 Installasjonen med ESET AV Remover

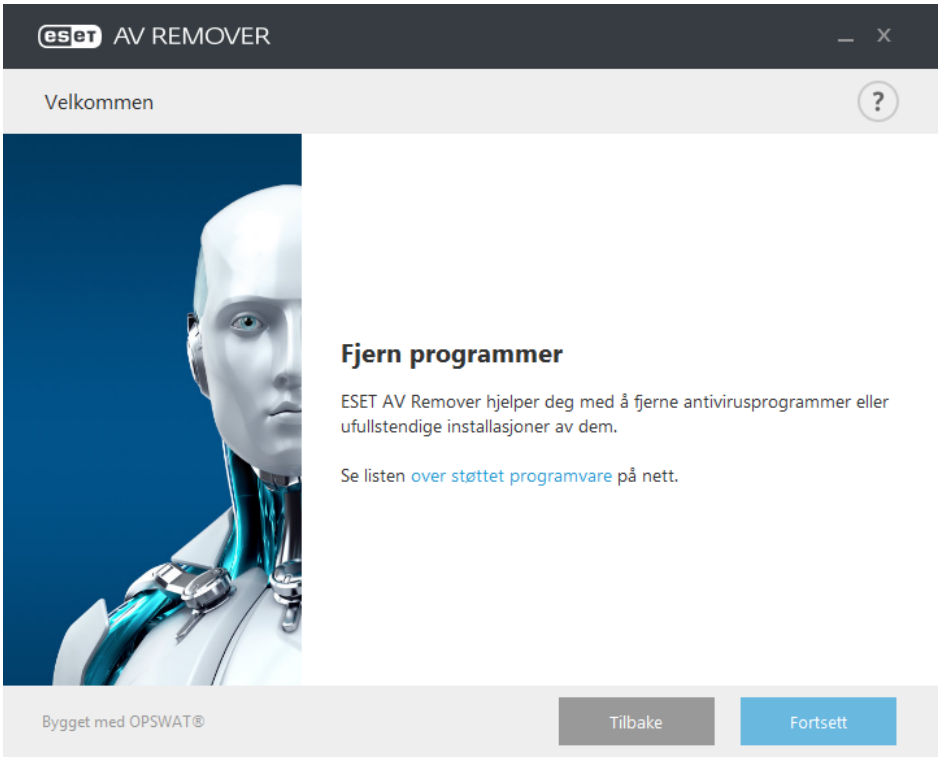
Før du fortsetter med installasjonsprosessen, er det viktig at du avinstallerer eventuelle sikkerhetsprogrammer på datamaskinen din. Merk av i avmerkingsboksen ved siden av **Jeg vil avinstallere uønskede antivirusprogrammer ved hjelp av ESET AV Remover** for å få ESET AV Remover til å skanne systemet og fjerne støttede sikkerhetsprogrammer. La avmerkingsboksen være umerket og klikk på **Fortsett** for å installere ESET Endpoint Security uten å kjøre ESET AV Remover.



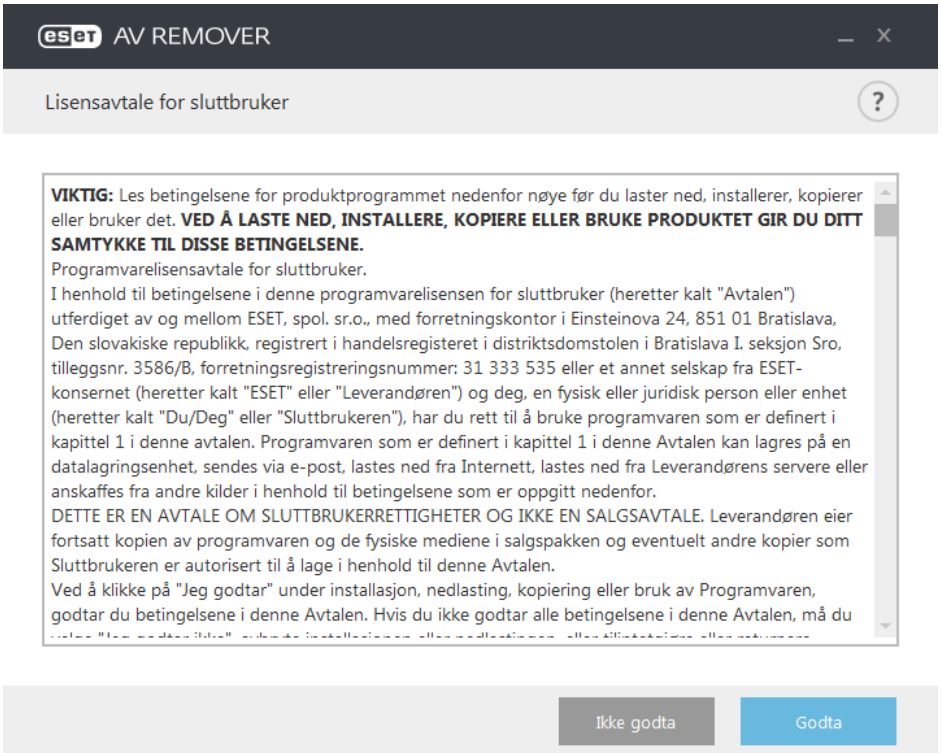
3.1.1 ESET AV Remover

Verktøyet ESET AV Remover hjelper deg med å fjerne nesten all virusbeskyttelsesprogramvare som er installert på systemet ditt. Følg instruksjonene nedenfor for å fjerne et eksisterende virusbeskyttelsesprogram ved bruk av ESET AV Remover:

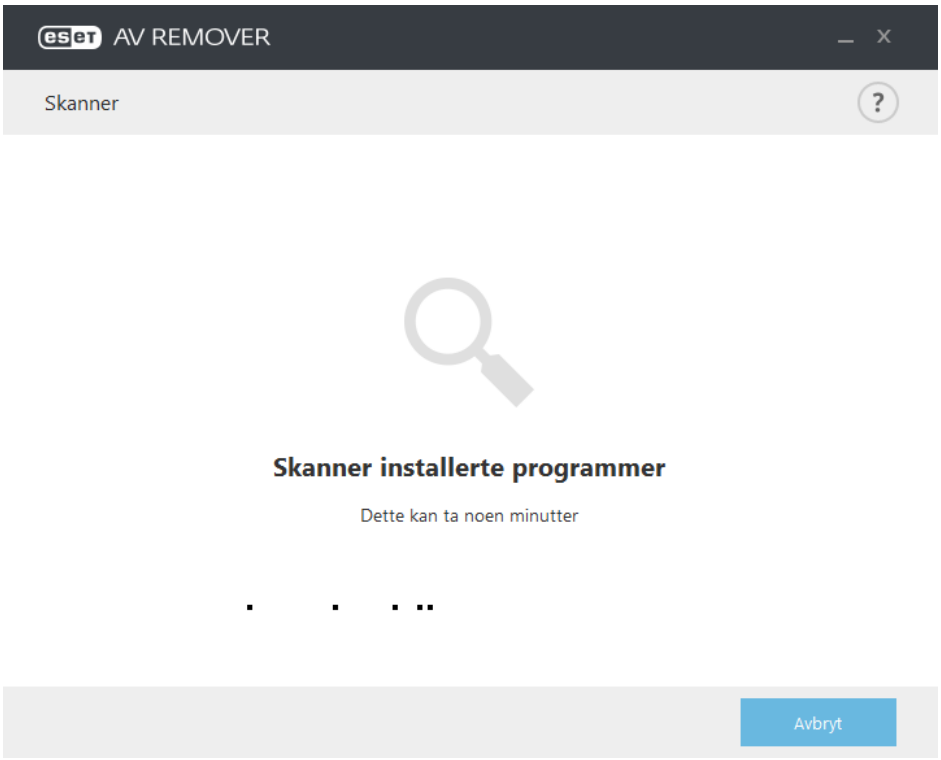
1. Hvis du vil se en liste over virusbeskyttelsesprogramvarer som kan fjernes med ESET AV Remover, kan du gå til ESET-kunnskapsartikkelen.



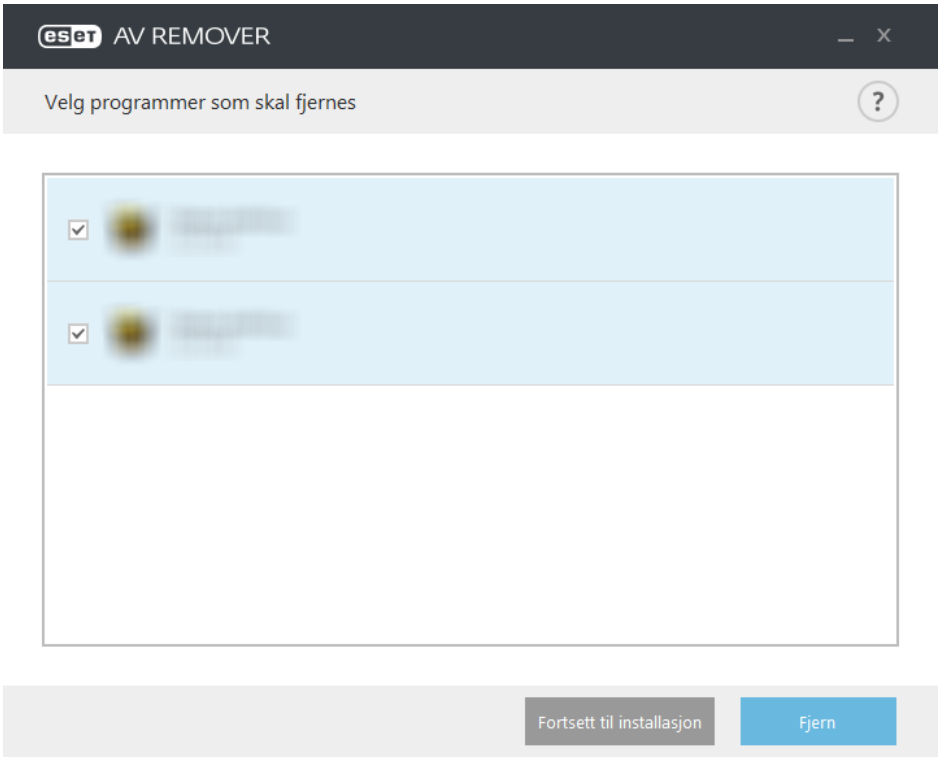
2. Les og klikk **Godta** for å angi at du godtar lisensavtalen for sluttbrukere. Hvis du klikker **Jeg godtar ikke** vil installasjonen av ESET Endpoint Security fortsette uten av eksisterende sikkerhetsprogrammer fjernes på datamaskinen.



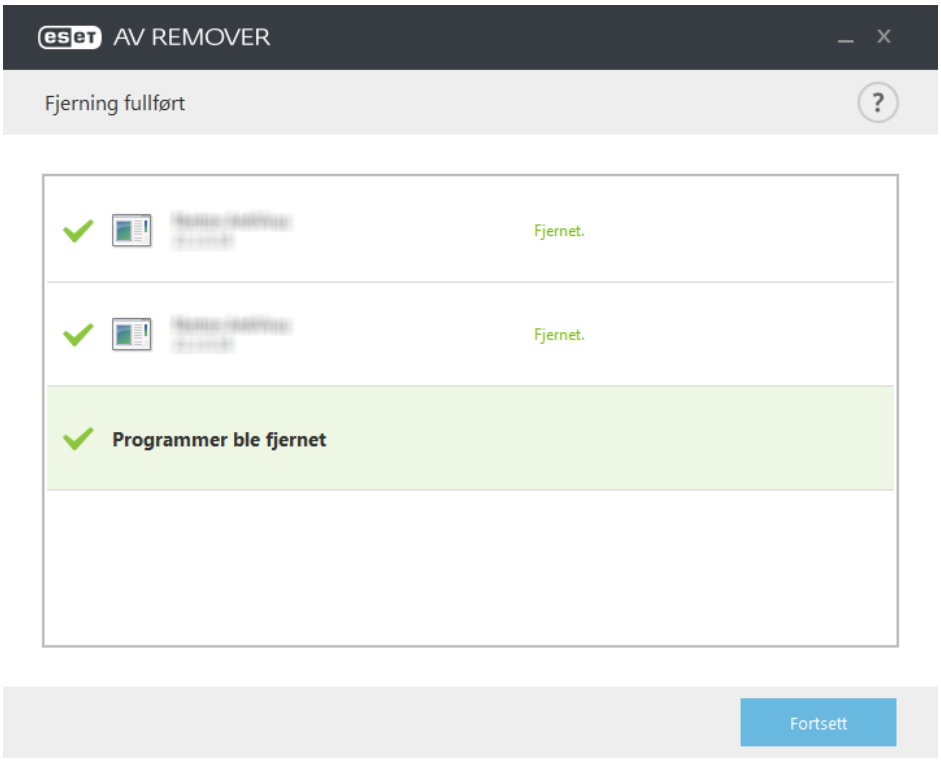
3. ESET AV Remover vil begynne å søke etter virusbeskyttelsesprogramvare i systemet.



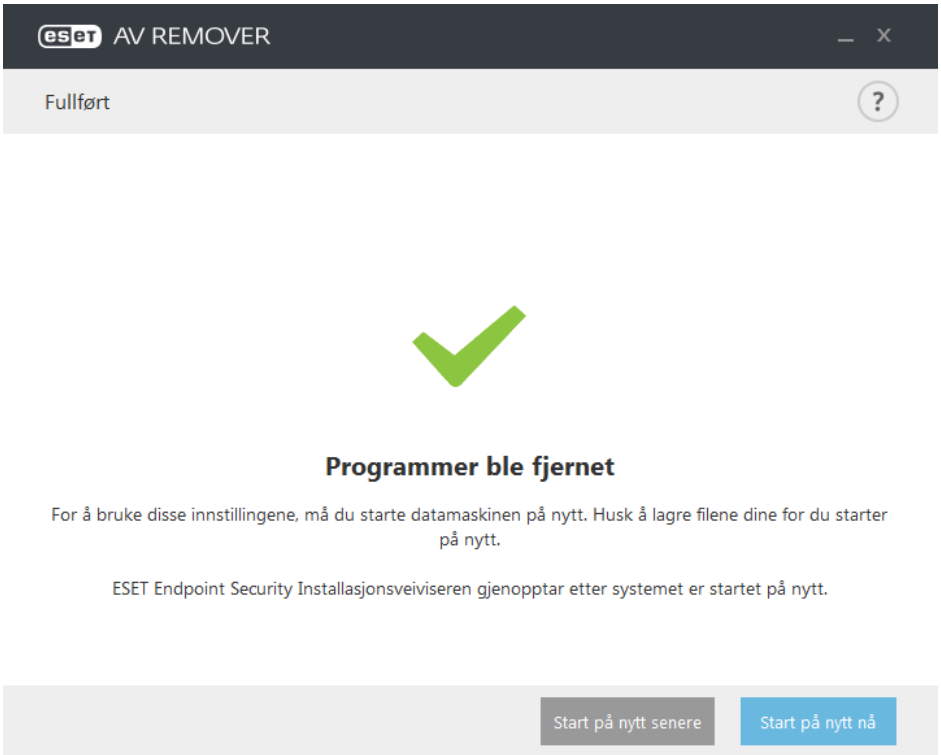
4. Velg alle oppførte virusbeskyttelsesprogrammer og klikk Fjern. Dette kan ta noen minutter.



5. Når programmene er fjernet, klikker du **Fortsett**.



6. Start datamaskinen på nytt for å bruke innstillingene og fortsett installasjonen av<%PRODUCTNAME.%> Hvis avinstalleringen er mislykket, kan du se avsnittetAvinstallering med ESET AV Remover ble avsluttet med en feil i denne håndboken.



3.1.2 Avinstalleringen med ESET AV Remover ble avsluttet med feil

Hvis du ikke kan fjerne et virusbeskyttelsesprogram med ESET AV Remover, får du et varsel om at programmet du prøver å fjerne kanskje ikke støttes av ESET AV Remover. Gå til listen over støttede produkter eller avinstallerere for vanlige Windows virusbeskyttelsesprogramvare i ESET Kunnskapsbase for å se om dette programmet kan fjernes.

Når avinstalleringen av sikkerhetsproduktet mislykkes eller noen av produktkomponentene avinstalleres delvis, kan du få meldingen **Start på nytt og skann igjen**. Bekreft UAC etter oppstart og fortsett med skanningen og avinstalleringen.

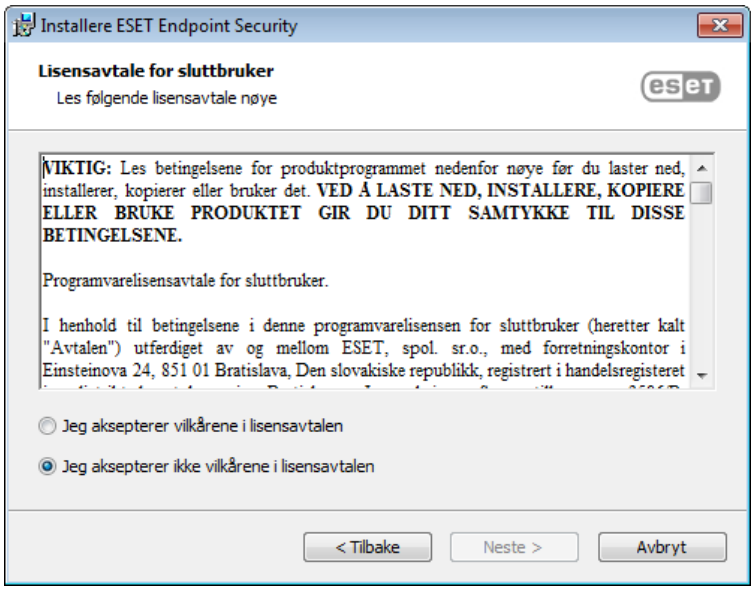
Ta kontakt med ESETs brukerstøtte for å åpne en forespørsel til brukerstøtte, og ha **AppRemover.log**-filen tilgjengelig for å hjelpe teknikerne hos ESET. **AppRemover.log**-filen ligger i **eset**-mappen. Bla gjennom til *%TEMP%* i Windows Explorer for å få tilgang til denne mappen. ESETs brukerstøtte vil svare så rast som mulig for å hjelpe deg med å løse problemet ditt.

3.2 Installasjon

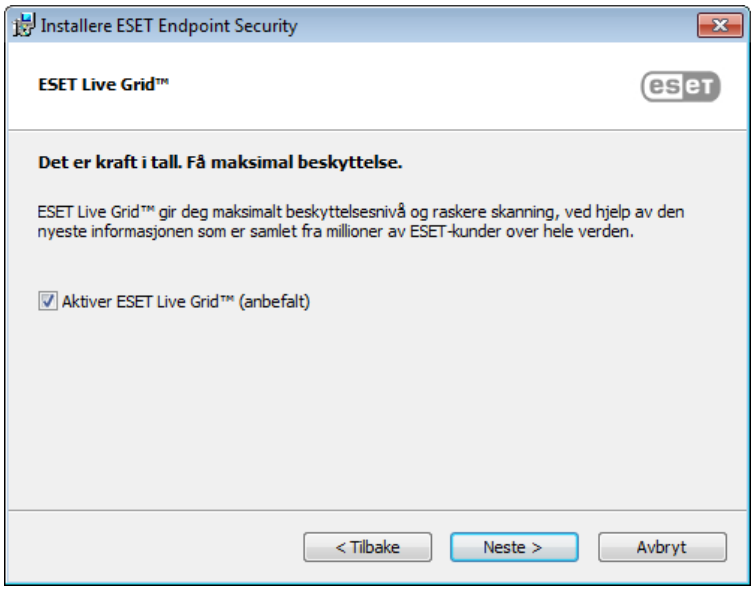
Så snart du har startet installasjonsprogrammet, vil installasjonsveiviseren ta deg gjennom installasjonsprosessen.

Viktig: Forsikre deg om at ingen andre virusprogrammer er installert på datamaskinen. Hvis to eller flere virusbeskyttelsesløsninger installeres på samme datamaskin, kan de komme i konflikt med hverandre. Vi anbefaler at du avinstallerer andre virusprogrammer på systemet. Du finner en liste over avinstalleringsverktøy for vanlige antivirusprogrammer i vår kunnskapsbaseartikkel (tilgjengelig på engelsk og flere andre språk).

I neste trinn vil lisensavtale for sluttbruker bli vist. Les og klikk **Godta** for å angi at du godtar lisensavtalen for sluttbrukere. Klikk **Neste** etter at du har akseptert vilkårene for å fortsette med installasjonen.



Når du velger "Jeg godtar ..." klikker **Neste**, blir du bedt om å konfigurere ESET Live Grid. ESET Live Grid hjelper deg å sikre at ESET umiddelbart og alltid blir informert om nye infiltreringer slik at kundene kan beskyttes raskt. Systemet tillater innsending av nye trusler til ESETs viruslaboratorium, hvor de blir analysert, behandlet og lagt til i virussignaturdatabasen.



Det neste trinnet i installasjonen er å konfigurere oppdagelse av potensielt uønskede programmer. Disse programmene er ikke nødvendigvis skadelige, men kan ofte ha negativ innvirkning på atferden til operativsystemet. Du finner mer informasjon i kapittelet Potensielt uønskede programmer. Du kan få tilgang til ytterligere innstillinger ved å klikke **Avanserte innstillinger** (for eksempel for å installere ESET-produktet ditt i en spesifikk mappe eller aktivere automatisk skanning etter installasjonen).

Det siste trinnet er å bekrefte installasjonen ved å trykke **Installer**.

3.2.1 Avansert installasjon

Med avansert installasjon kan du tilpasse en rekke installasjonsparametere som ikke er tilgjengelige når du utfører en typisk installasjon.

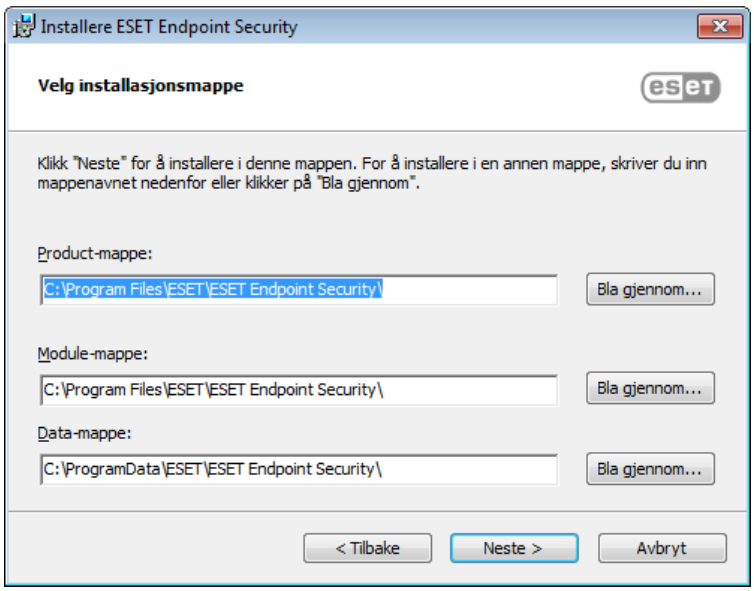
Når du velger preferanser for gjenkjenning av potensielt uønskede programmer og klikker **Avanserte innstillinger**, blir du bedt om å velge en plassering for installasjonspakken for produktet. Som standard blir programmet installert i følgende katalog:

C:\Program Files\ESET\ESET Endpoint Security

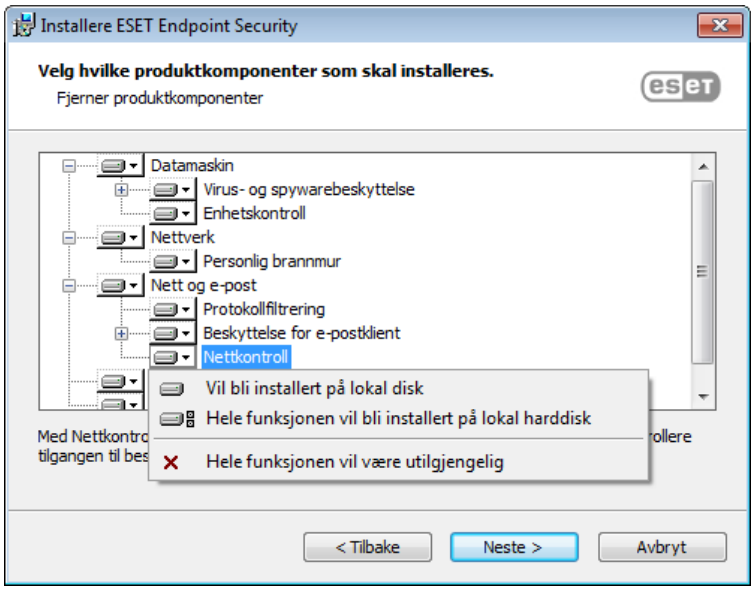
Du kan angi en plassering for programmoduler og data. Som standard blir de installert i følgende kataloger, henholdsvis:

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

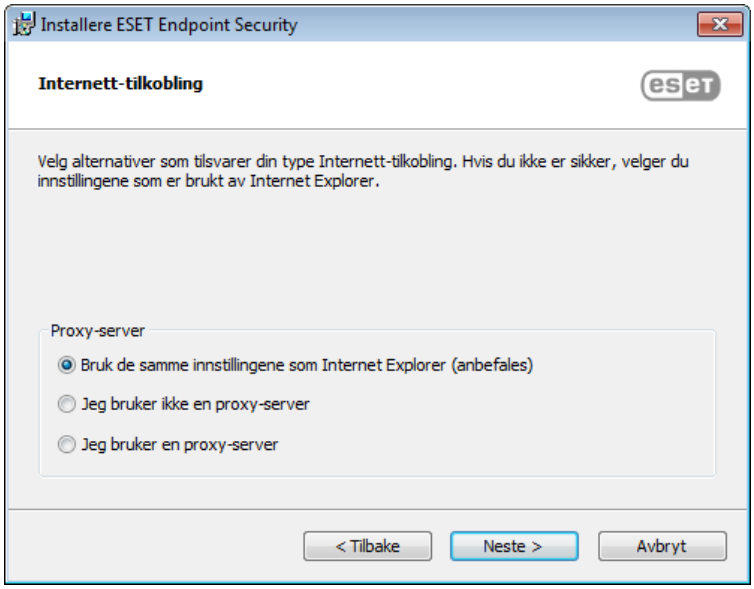
Klikk **Bla gjennom ...** for å endre disse plasseringene (ikke anbefalt).



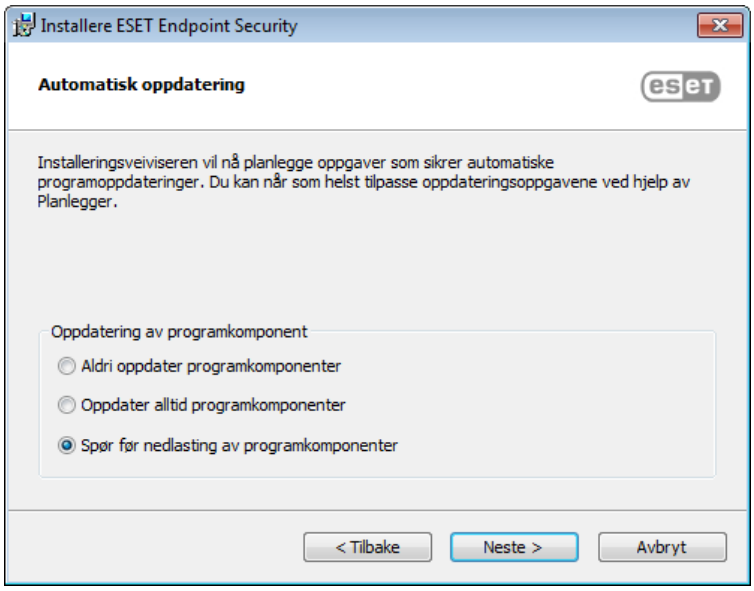
I det neste vinduet, kan du velge hvilke produktkomponenter som skal installeres. Produktkomponenter i Datamaskin-delen inkluderer Filsystembeskyttelse i sanntid, Datamaskinskanning, Dokumentbeskyttelse og Enhetskontroll. Vær klar over at de første komponentene er nødvendige for at sikkerhetsløsningen skal fungere. Nettverk-delen tilbyr muligheten til å installere den personlige brannmuren. Brannmuren overvåker all innkommende og utgående trafikk og bruker regler for individuelle nettverkstilkoblinger. Personlig brannmur gir også beskyttelse mot angrep fra eksterne datamaskiner. Komponenter i Nett og e-post-delen gir beskyttelse når du er på Internett og når du kommuniserer via e-post. Komponenten Oppdateringsfeil kan brukes til å oppdatere andre datamaskiner på nettverket. Microsoft NAP-støtte gir en agent fra NAP for å sikre full kompatibilitet med NAP-arkitekturen.



Du konfigurerer proxy-serverinnstillingene ved å velge **Jeg bruker proxy-server** og klikke **Neste**. Legg inn IP-adresse eller URL til proxy-serveren i feltet **Adresse**. Hvis du ikke er sikker på om du bruker en proxy-server for å koble til Internett, velger du **Bruk samme innstillinger som Internet Explorer (Anbefalt)** og klikker **Neste**. Hvis du ikke bruker en proxy-server, velger du alternativet **Jeg bruker ikke en proxy-server**. For mer informasjon, se Proxy-server.

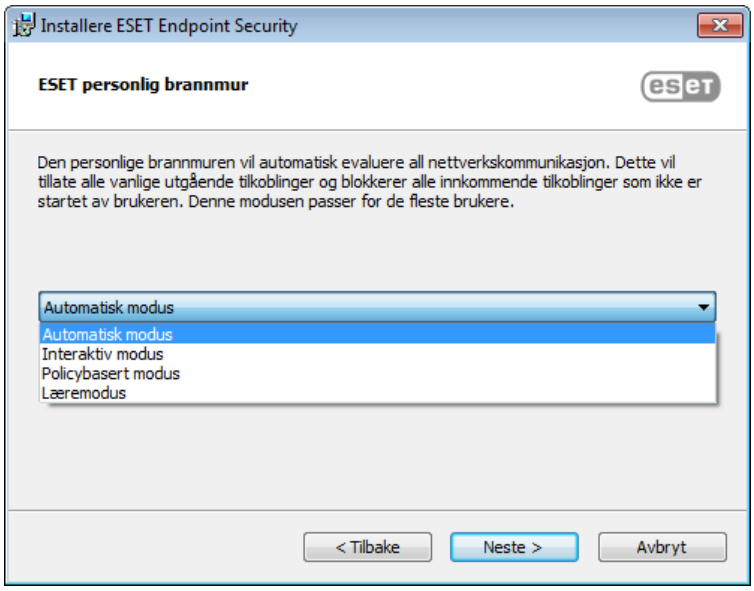


Med dette installasjonstrinnet kan du angi hvordan automatiske programoppdateringer skal håndteres på systemet. Klikk **Endre ...** for å gå inn i de avanserte innstillingene.

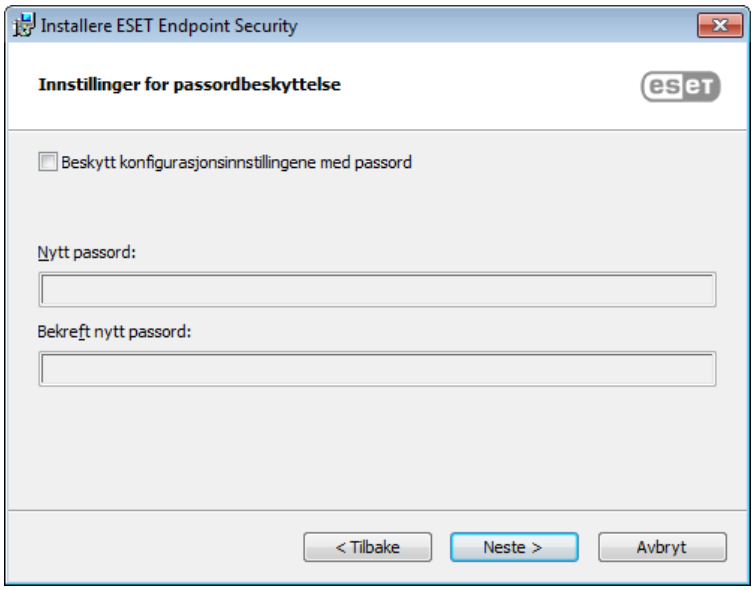


Hvis du ikke vil at programkomponentene skal oppdateres, velger du alternativet **Ikke oppdater programkomponenter**. Velg alternativet **Spør før nedlasting av programkomponenter** for å vise et bekreftelsesvindu hver gang systemet prøver å laste ned programkomponenter. Hvis du vil laste ned programkomponentoppgraderinger automatisk, velger du alternativet **Oppdater alltid programkomponenter**.

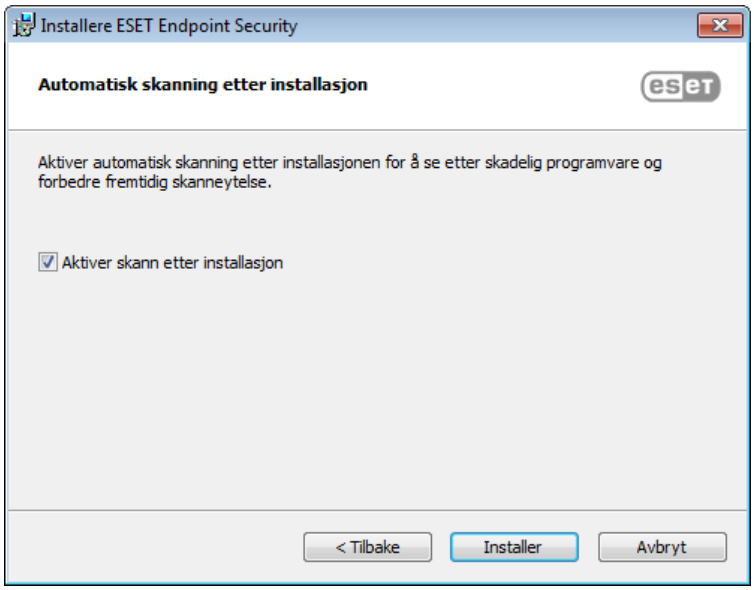
Deretter velger du en filtreringsmodus for ESET personlig brannmur. Fire filtreringsmoduser er tilgjengelige for ESET Endpoint Security personlig brannmur. Brannmurens funksjonalitet endres etter hvilken modus som er valgt. Filtreringsmoduser påvirker også nivået av nødvendig brukerhandling.



Neste installasjonsvindu viser alternativet for å angi passord for å beskytte programinnstillingene. Velg alternativet **Beskytt konfigurasjonsinnstillingene med passord** og angi passordet i feltene **Nytt passord** og **Bekreft nytt passord**. Dette passordet kreves for å endre eller få tilgang til innstillingene for ESET Endpoint Security. Når begge passordfeltene samsvarer, klikker du **Neste** for å fortsette.



Avmerk avkrysningsboksen ved siden av Aktiver skanning etter installasjon hvis du ønsker å deaktivere **første skanning etter installasjon**. Denne gjennomføres vanligvis når installasjonen avsluttes for å søke etter skadelige koder.



Klikk **Installer** for å starte installasjonen.

3.3 Produktinstallasjon via ERA (kommandolinje)

Følgende innstillinger bare ment å brukes med **nivåene redusert**, **enkel og ingen** på brukergrensesnittet. Se dokumentasjonen for **msiexec**-versjonen som brukes for de riktige kommandolinjebryterne.

Støttede parametere:

APPDIR=<path>
- bane – Gyldig mappebane
- Programinstallasjonsmappe.
- Eksempel: `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>
- bane – Gyldig mappebane
- Installasjonsmappe for programdata.

MODULEDIR=<path>
- bane – Gyldig mappebane
- Modulinstallasjonsmappe.

ADDLOCAL=<list>
- Komponentinstallering – liste over ikke-obligatoriske funksjoner som skal installeres lokalt.
- Bruk med ESET .msi-pakker: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- For flere detaljer om ADDLOCAL-egenskapen, se http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

Regler

- **ADDLOCAL-liste** er en kommaseparert med alle funksjonsnavn som skal installeres.
- Når du velger en funksjon du vil installere, må hele banen (alle overordnede funksjoner) eksplisitt være inkludert i listen.
- Se ytterligere regler for riktig bruk.

Tilstedeværelse av funksjoner

- **Obligatorisk** – funksjonen vil alltid være installert
- **Valgfritt** – funksjonen vil kanskje ikke være valgt for installering
- **Usynlig** – logisk funksjon som kreves for at andre funksjoner skal fungere riktig
- **Placeholder** –funksjon som ikke påvirker produktet, men må være oppført med delfunksjoner

Funksjonstre for Endpoint 6.1 er:

Funksjonstre	Funksjonsnavn	Tilstedeværelse av funksjoner
Datamaskin	Datamaskin	Obligatorisk
Datamaskin / Virus- og spywarebeskyttelse	Virusbeskyttelse	Obligatorisk
Datamaskin / Virus- og spywarebeskyttelse > Filsystembeskyttelse i sanntid	Sanntidsbeskyttelse	Obligatorisk
Datamaskin / Virus- og spywarebeskyttelse > Datamaskinskanning	Skann	Obligatorisk
Datamaskin / Virus- og spywarebeskyttelse > Dokumentbeskyttelse	Dokumentbeskyttelse	Valgfritt
Datamaskin / Enhetskontroll	DeviceControl	Valgfritt
Nettverk	Nettverk	Placeholder
Nettverk / Personlig brannmur	Brannmur	Valgfritt
Nett og e-post	Nett og e-post	Placeholder
Protokollfiltrering for nett og e-post	Protokollfiltrering	Usynlig
Nett og e-post / Beskyttelse for nettilgang	Beskyttelse for nettilgang	Valgfritt
Nett og e-post / Beskyttelse for e-postklient	Beskyttelse for e-postklient	Valgfritt

Nett og e-post / Beskyttelse for e-postklient / MailPlugins	MailPlugins	Usynlig
Nett og e-post / Beskyttelse for e-postklient / Spambeskyttelse	Antispam	Valgfritt
Nett og e-post / Nettkontroll	Nettkontroll	Valgfritt
Oppdater speil	Oppdateringsfeil	Valgfritt
Microsoft NAP-støtte	MicrosoftNAP	Valgfritt

Ytterligere regler

- Hvis noen av **Nett og e-post**-funksjonene er valgt for installering, må den usynlige**Protokollfiltrering**-funksjonen være eksplisitt inkludert i listen.
- Hvis noen av **Beskyttelse for e-postklient**-funksjonene er valgt for installering, må den usynlige**MailPlugins**-funksjonen være eksplisitt inkludert i listen

Eksempler:

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Liste over CFG_ egenskaper:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 – Deaktivert, 1 – Aktivert
• PUA

CFG_LIVEGRID_ENABLED=1/0
• 0 – Deaktivert, 1 – Aktivert
• LiveGrid

FIRSTSCAN_ENABLE=1/0
• 0 – Deaktiver, 1 – Aktiver
• Planlegg en ny FirstScan etter installasjon.

CFG_EPFW_MODE=0/1/2/3
• 0 – Automatisk, 1 – Interaktiv, 2 – Policy, 3 – Læring

CFG_PROXY_ENABLED=0/1
• 0 – Deaktivert, 1 – Aktivert

CFG_PROXY_ADDRESS=<ip>
• Proxy-IP-adresse.

CFG_PROXY_PORT=<port>
• Proxy-portnummer.

CFG_PROXY_USERNAME=<user>
• Brukernavn for godkjenning.

CFG_PROXY_PASSWORD=<pass>
• Passord for godkjenning.

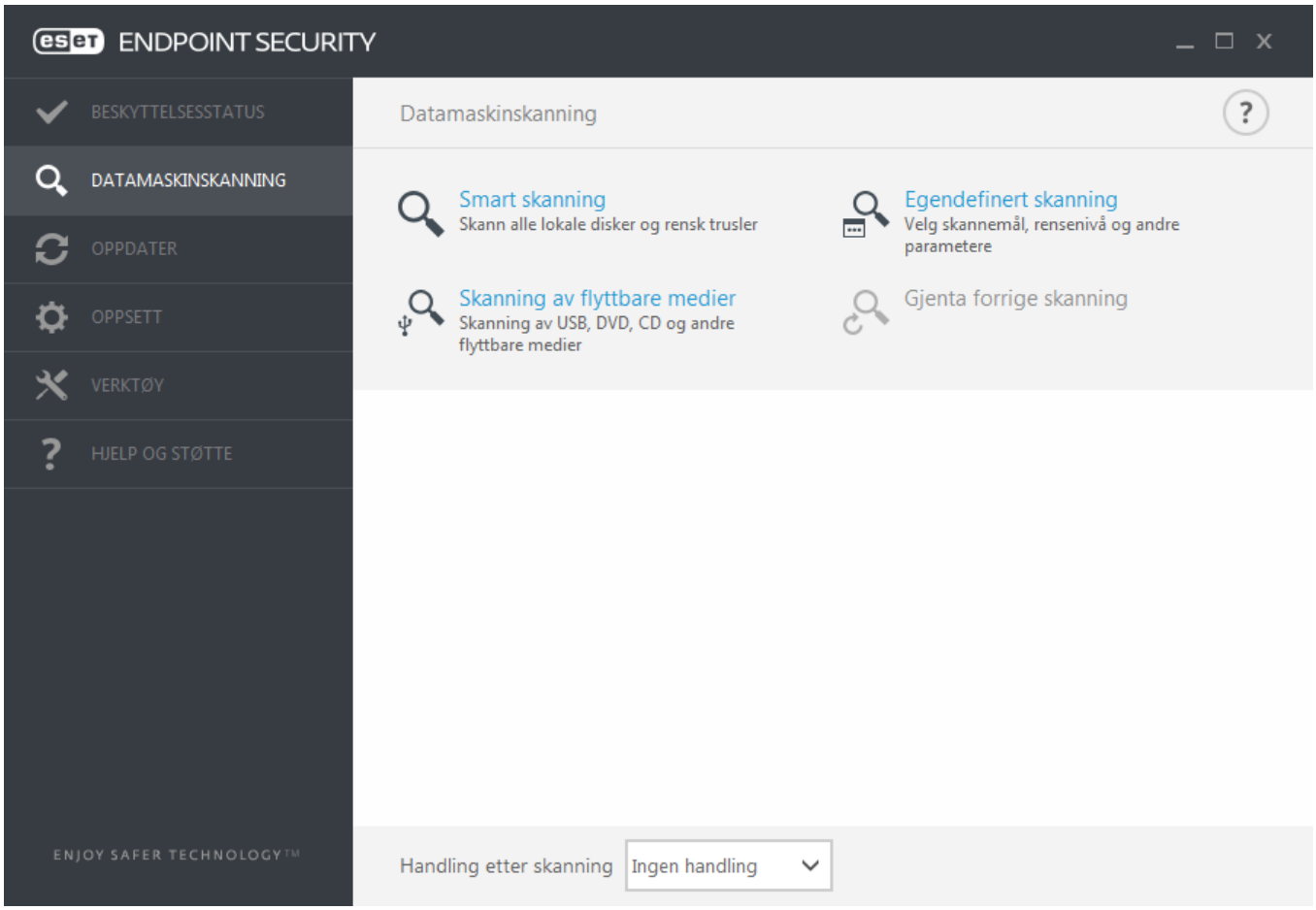
3.4 Produktaktivering

Når installasjonen er fullført, blir du bedt om å aktivere produktet.

Velg en av de tilgjengelige metodene for å aktivere ESET Endpoint Security. Se Hvordan å aktivere ESET Endpoint Security for mer informasjon.

3.5 Datamaskinskanning

ESET Endpoint Security vil automatisk utføre en datamaskinskanning, ikke lenger enn 15 minutter etter at installasjonen er ferdig (det kan være nødvendig å starte datamaskinen på nytt). I tillegg til den innledende skanningen, anbefaler vi at du utfører regelmessige skanninger, eller planlegger en regelmessig skanning, for å se etter trusler. Klikk **Datamaskinskanning** i hovedvinduet for programmet, og klikk deretter **Smart skanning**. For mer informasjon om datamaskinskanninger, se Datamaskinskanning.



3.6 Oppgraderer til en nyere versjon

Nye versjoner av ESET Endpoint Security utgis for å levere forbedringer eller reparere problemer som ikke kan ordnes ved automatisk oppdatering av programmodulene. Du kan oppgradere til en nyere versjon på flere måter:

1. Automatisk ved hjelp av en programoppdatering.
   Siden programoppdateringen distribueres til alle brukere og kan ha påvirke visse systemkonfigurasjoner, utgis den etter en lang periode med testing på alle mulige systemkonfigurasjoner. Hvis du trenger å oppgradere til en nyere versjon rett etter at den er utgitt, bruker du en av metodene under.
2. Manuelt ved å laste ned og installere en nyere versjon over den forrige.
3. Manuelt, med automatisk distribusjon i et nettverksmiljø via ESET Remote Administrator.

3.7 Veiledning for nybegynnere

Dette kapittelet gir en innledende oversikt over ESET Endpoint Security og produktets grunninnstillinger.

3.7.1 Brukergrensesnittet

Hovedvinduet i ESET Endpoint Security er delt inn i to hoveddeler. Det primære vinduet til høyre viser informasjon som svarer til alternativet som er valgt i hovedmenyen til venstre.

Her er en beskrivelse av alternativer i hovedmenyen:

Beskyttelsesstatus – Gir informasjon om beskyttelsesstatusen til ESET Endpoint Security.

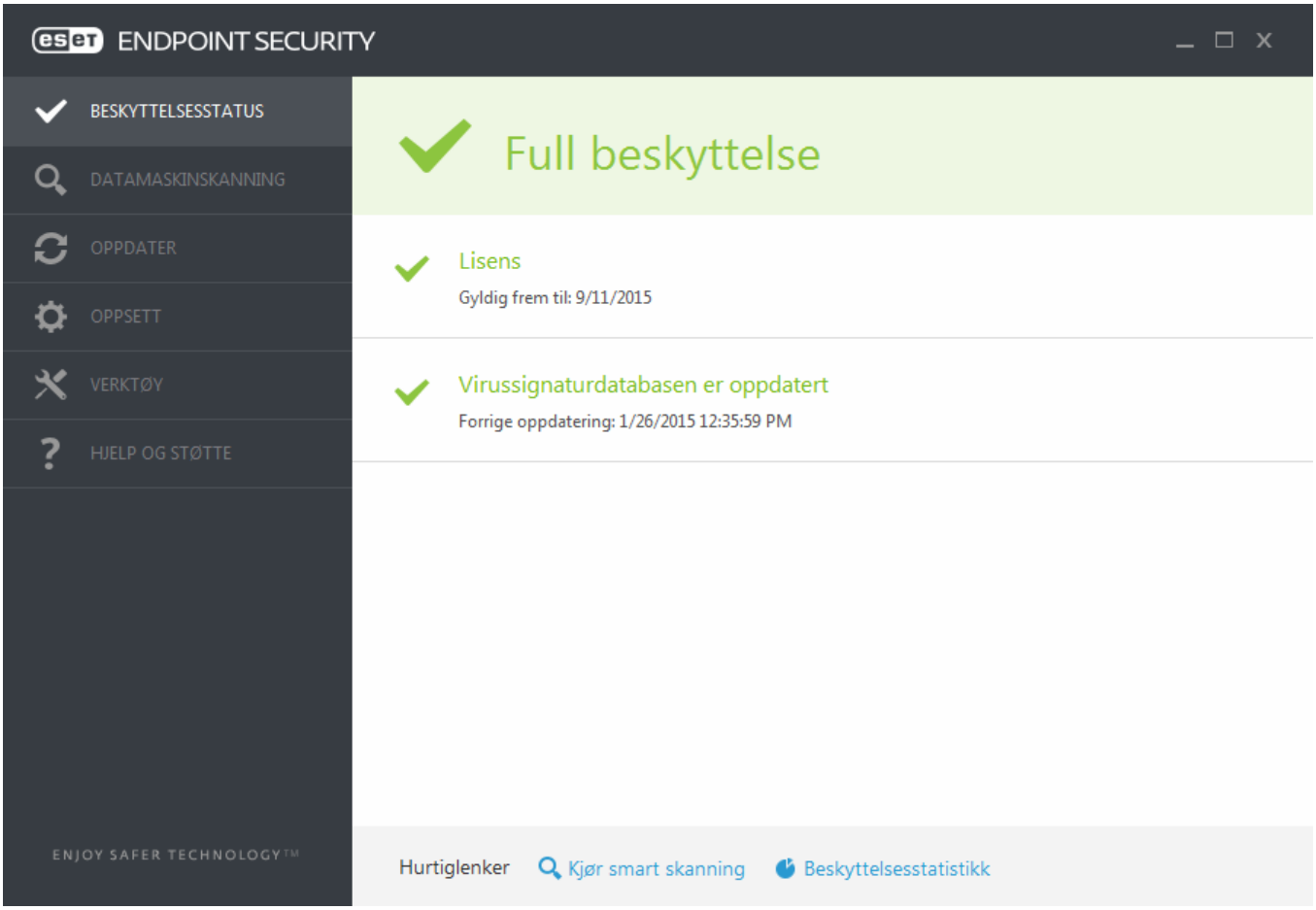
Datamaskinskanning – Med dette alternativet kan du konfigurere og starte Smart skanning, Egendefinert skanning eller Skanning av flyttbare medier. Du kan også gjenta den siste skanningen som ble utført.

Oppdatering – Viser informasjon om oppdateringer av virussignaturdatabasen.

Oppsett – Velg dette alternativet for å justere sikkerhetsinnstillinger for datamaskin,, nettverk eller nett og e-post.

Verktøy – Gir tilgang til loggfiler, beskyttelsesstatistikk, overvåkingsaktivitet, kjørende prosesser, planlegger, karantene, nettverkstilkoblinger, ESET SysInspector og ESET SysRescue for å opprette en rednings-CD. Du kan også sende inn en prøve til analyse.

Hjelp og støtte – Gir tilgang til hjelpefiler, ESETs kunnskapsbase og ESETs nettsted. Du vil også finne koblinger for å sende spørsmål til brukerstøtte, støtteverktøy og informasjon om produktaktivering.

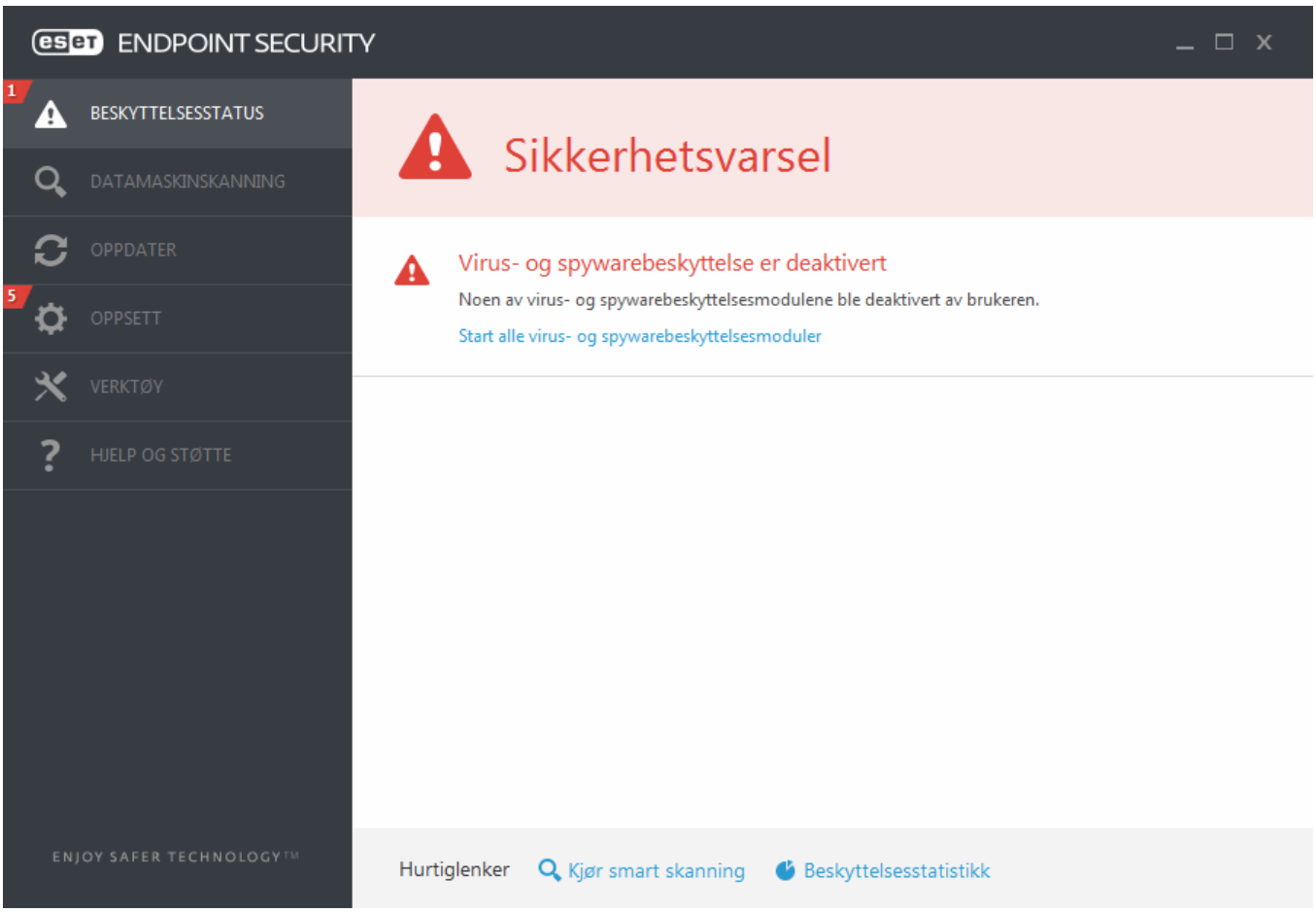


Beskyttelsesstatus-skjermbildet informerer deg om sikkerheten og gjeldende beskyttelsesnivå for datamaskinen. Den grønne **Maksimal beskyttelse**-statusen angir at høyeste sikkerhetsnivå er aktivert.

Statusen viser også hurtigkoblinger til ofte brukte funksjoner i ESET Endpoint Security og informasjon om den siste oppdateringen.

Hva må gjøres hvis programmet ikke fungerer som det skal?

Hvis de aktiverte modulene fungerer som de skal, vises de med et grønt kontrollmerke. Hvis ikke vises det et rødt utropstegn eller et oransje varselikon. Mer informasjon om modulen vises i øvre del av vinduet. Forslag til løsning for å reparere modulen vises også. Klikk **Oppsett** i hovedmenyen for å endre status på individuelle moduler, og klikk på den ønskede modulen.



Det røde ikonet med en "!" angir kritiske problemer – full beskyttelse av datamaskinen er ikke tilgjengelig. Mulige årsaker er:

- **Virus- og spywarebeskyttelse deaktivert** – Du kan reaktivere virus- og spywarebeskyttelsen ved å klikke på **Aktiver beskyttelse i sanntid** i **Beskyttelsesstatus**-ruten eller **Aktiver virus- og spywarebeskyttelse** i **Oppsett**-ruten i hovedprogramvinduet.
- **ESETs personlige brannmur er deaktivert** – Dette problemet angis med et rødt ikon og en sikkerhetsmelding ved siden av elementet **Nettverk**. Du kan reaktivere beskyttelsen for nettverk ved å klikke **Aktiver filtreringsmodus**.
- **Utdatert virussignaturbase** – Du bruker en utdatert virussignaturdatabase.
- **Produktet er ikke aktivert** eller **Lisensen er utløpt** – Dette angis av at ikonet for beskyttelsesstatus blir rødt. Programmet kan ikke oppdateres etter at lisensen er utløpt. Vi anbefaler at du følger instruksjonene i varselvinduet og fornyer lisensen.

Det oransje ikonet med en «i-» angir at ESET-produktet krever din oppmerksomhet i forbindelse med et ikke-kritisk problem. Mulige årsaker er blant annet:

- **Beskyttelse for nettilgang er deaktivert** – Du kan reaktivere Beskyttelse for nettilgang ved å klikke sikkerhetsmeldingen og deretter klikke **Aktiver beskyttelse for nettilgang**.
- **Lisensen utløper snart** – Dette angis ved at ikonet for beskyttelsesstatus viser et utropstegn. Etter at lisensen har utløpt, vil ikke programmet kunne oppdateres, og ikonet for beskyttelsesstatus blir rødt.

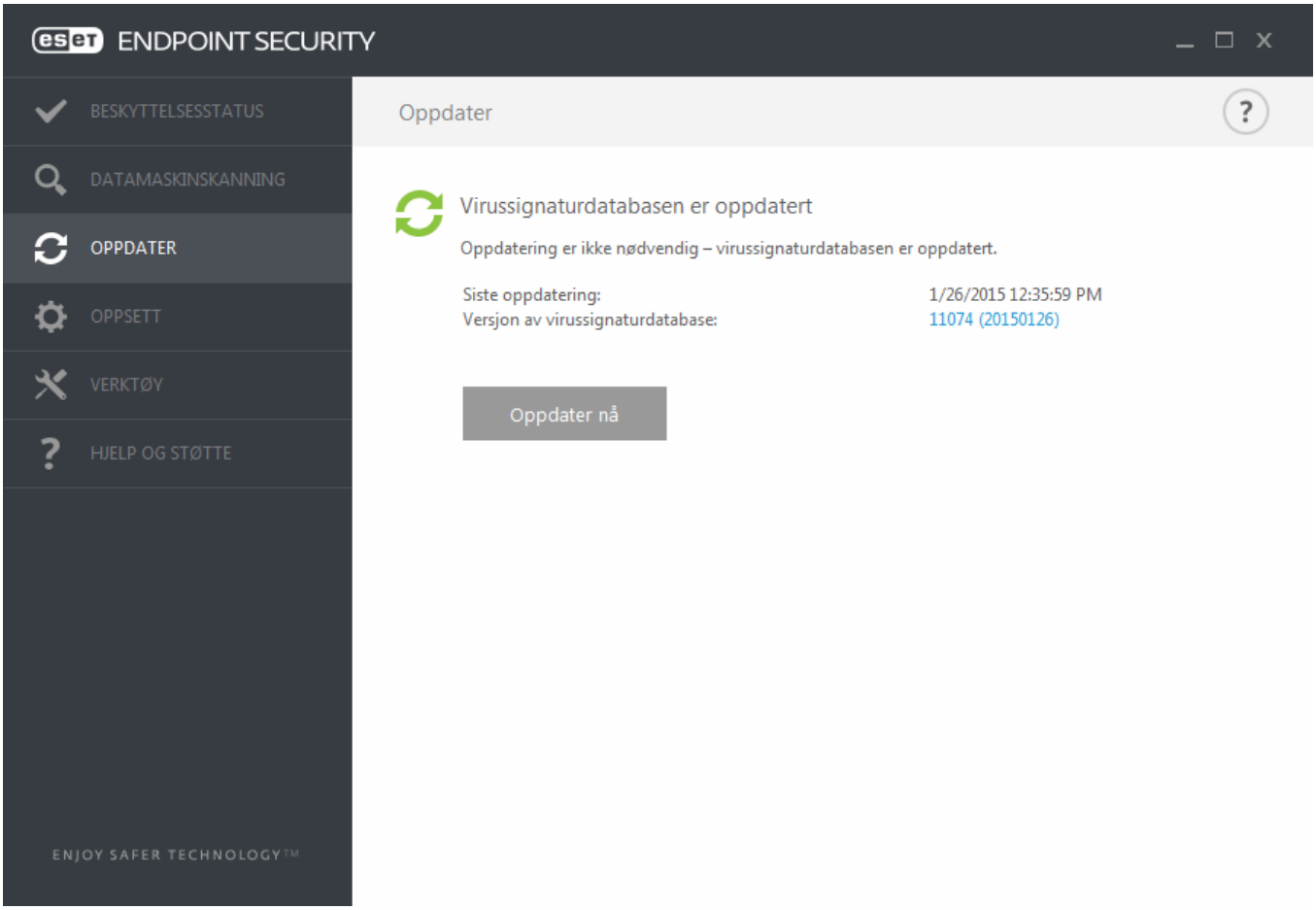
Hvis du ikke kan løse et problem ved hjelp av de foreslåtte løsningene, kan du klikke **Hjelp og støtte** for å åpne hjelpefilene eller søke i ESET kunnskapsbase. Hvis du fortsatt trenger hjelp, kan du sende inn en støtteforespørsel

til ESETs brukerstøtte. ESETs brukerstøtte vil raskt gi svar på spørsmålene og hjelpe til med å finne en løsning.

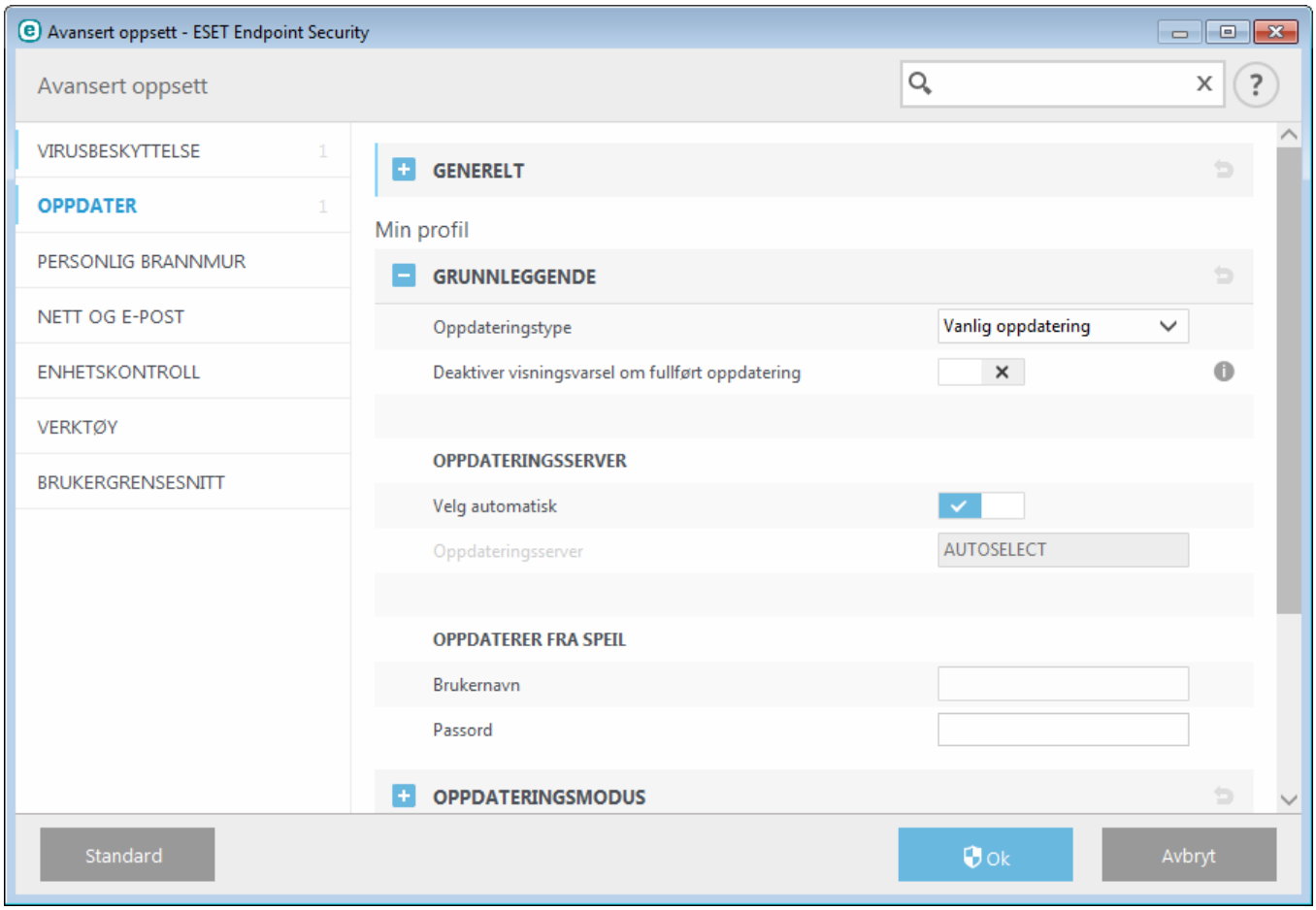
3.7.2 Oppsett for oppdatering

Oppdatering av virussignaturdatabasen og programkomponenter er en viktig del av å skaffe full beskyttelse mot skadelig kode. Du bør følge nøye med på konfigurasjonen og bruken av oppdateringene. Fra hovedmenyen velger du **Oppdaterer** og klikker deretter **Oppdater nå** for å se etter en nyere databaseoppdatering.

Hvis **lisensnøkkel** ikke er angitt ennå, kan du ikke motta nye oppdateringer og du blir bedt om å aktivere produktet.



Vinduet for Avansert oppsett (klikk **Oppsett** > **Avansert oppsett** fra hovedmenyen og klikk deretter eller trykk **F5** på tastaturet) inneholder flere oppdateringsalternativer. Når du vil konfigurere avanserte oppdateringsalternativer som f.eks. oppdateringsmodus, proxyservertilgang, LAN-tilkoblinger og innstillinger for oppdatering av virussignaturkopier, klikker du **Oppdater** i treet for avansert oppsett. Hvis du opplever problemer med en oppdatering, klikker du på **Rens** for å slette den midlertidige oppdateringsmappen. Som standard er menyen **Oppdateringsserver** satt til **AUTOMATISK VALG**. Når du bruker en ESET-server, anbefaler vi at du lar alternativet **Velg automatisk** være markert. Hvis du ikke vil at meldingen i systemstatusfeltet nederst til høyre på skjermen skal vises, velger du **Ikke vis melding om gjennomført oppdatering**.



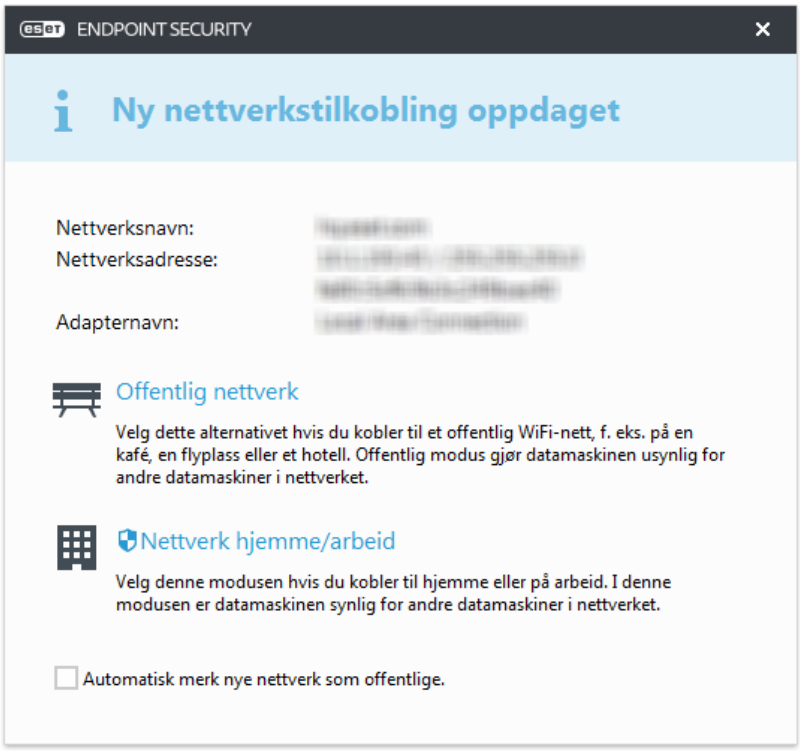
For å oppnå optimal funksjonalitet er det viktig at programmet oppdateres automatisk. Dette er bare mulig hvis du tastet inn riktig **lisensnøkkel** i **Hjelp og støtte** > **Aktiver produkt**.

Hvis du ikke angir **lisensnøkkelen** etter installasjonen, kan du gjøre det når som helst. For mer detaljert informasjon om aktivering, kan du se Hvordan aktivere ESET Endpoint Security og skrive inn lisensdataene du mottok sammen med ESET-sikkerhetsproduktet i vinduet **Lisensinformasjon**.

3.7.3 Oppsett for soner

Det er nødvendig å konfigurere klarerte soner for å beskytte datamaskinen i et nettverksmiljø. Du kan la andre brukere få tilgang til datamaskinen ved å konfigurere en klarert sone til å tillate deling. Klikk **Avansert oppsett** (F5) > **Personlig Brannmur** > **Soner** for å få tilgang til innstillinger for klarerte soner.

Gjenkjenning av klarerte soner oppstår etter installasjon av ESET Endpoint Security og hver gang datamaskinen din kobler seg til et nytt nettverk. Det er derfor ikke nødvendig å definere den klarerte sonen. Som standard vises det et dialogboksvindu når det blir gjenkjent en ny sone, slik at du kan angi beskyttelsesnivå for sonen.



Advarsel: En feil konfigurert klarert sone kan utgjøre en trussel mot datamaskinen.

MERKNAD: Arbeidsstasjoner fra en klarert sone får som standard tilgang til delte filer og skrivere, har innkommende RPC-kommunikasjon aktivert og har tilgang til ekstern skrivebordsdeling.

3.7.4 Verktøy for nettkontroll

Hvis du allerede har aktivert Nettkontroll i ESET Endpoint Security, må du også konfigurere Nettkontroll for ønskede brukerkontoer for at Nettkontroll skal fungere på rett måte. Se kapittelet Nettkontroll for instruksjoner om hvordan å opprette spesifikke restriksjoner på klientarbeidsstasjoner for å beskytte dem mot potensielt støtende innhold.

3.8 Vanlige spørsmål

Dette kapitlet dekker noen av de vanligste spørsmålene og problemene man kommer over. Klikk emnets tittel for å finne ut hvordan du kan løse problemet:

Slik oppdaterer du ESET Endpoint Security
Hvordan aktivere ESET Endpoint Security
Hvordan bruke gjeldende legitimasjon til å aktivere et nytt produkt
Fjerne virus fra PC-en
Tillate kommunikasjon for et bestemt program
Hvordan opprette en ny oppgave i Planlegger
Planlegge en skanningsoppgave (hver 24.time)
Hvordan koble produktet mitt til ESET Remote Administrator
Hvordan konfigurere et speil

Hvis problemet ditt ikke er med på hjelpesidene listet opp over, kan du prøve med nøkkelord eller uttrykk som beskriver problemet, og søke på hjelpesidene til ESET Endpoint Security.

Hvis du ikke finner løsningen på problemet/spørsmålet ditt på hjelpesidene, kan du prøve ESET-kunnskapsdatabase der du finner svare og løsninger for vanlige spørsmål og problemer.

Hvordan fjerner jeg den trojanske hesten Sirefef (ZeroAccess) trojan?
Sjekkliste for oppdateringsproblemer med speil
Hvilke adresser og porter på min tredjeparts brannmur skal jeg åpne for at ESET-produktet skal ha full funksjonalitet?

Du kan om nødvendig kontakte vårt nettbaserte tekniske støttesenter med spørsmål eller problemer. Kontaktskjemaet finner du direkte i programmet i kategorien **Hjelp og støtte**.

3.8.1 Slik oppdaterer du ESET Endpoint Security

ESET Endpoint Security kan oppdateres enten manuelt eller automatisk. For å starte oppdateringer, klikker du **Oppdater nå** i delen **Oppdater** i hovedmenyen.

Standardinstillingene ved installasjon oppretter en automatisk oppdateringsoppgave som blir utført hver time. Hvis du vil endre intervallet, går du til **Verktøy** > **Planlegger** (klikk her hvis du vil vite mer om Planlegger).

3.8.2 Hvordan aktivere ESET Endpoint Security

Når installasjonen er fullført, blir du bedt om å aktivere produktet.

Du kan aktivere produktet på flere måter. Om ett bestemt aktiveringsscenario er tilgjengelig i aktiveringsvinduet kan avhenge av både land og distribusjonsmåte (CD/DVD, ESETs nettside, osv.).

For å aktivere din utgave av ESET Endpoint Security direkte fra programmet, klikker du ikonet i systemstatusfeltet og velger **Aktiver produktlisens** fra menyen. Du kan også aktivere produktet ditt fra hovedmenyen under **Hjelp og støtte** > **Aktiver produkt** eller **Beskyttelsesstatus** > **Aktiver produkt**.

Du kan bruke en av følgende metoder til å aktivere ESET Endpoint Security:

- **Lisensnøkkel** – en unik tegnstreng i formatet XXXX-XXXX-XXXX-XXXX-XXXX som brukes til å identifisere lisenseieren og aktivere lisensen.
- **Sikkerhetsadmin** – En konto opprettet på ESET lisensadministratorportalen med legitimasjon (e-postadresse + passord). Denne metoden gjør det mulig å administrere flere lisenser fra ett sted.
- **Offline-lisens** – En automatisk generert fil som skal overføres til ESET-produktet for å gi lisensinformasjon. Hvis en lisens kan brukes til å laste ned en lisensfil (.lf), kan den filen brukes til å utføre offline aktivering. Antall offline-lisenser vil bli trukket fra det totale antallet tilgjengelige lisenser. For flere opplysninger om opprettelse av en offline-fil, se ESET License Administrator brukerhåndboken.

Klikk **Aktiver senere** hvis datamaskinen din er et medlem av et administrert nettverk. Administratoren din vil da

utføre en ekstern aktivering via ESET Remote Administrator. Du kan også bruke dette alternativet hvis du vil aktivere klienten på et senere tidspunkt.

Hvis du har et brukernavn og passord og vet ikke hvordan du skal aktivere ESET Endpoint Security, klikk **Jeg har brukernavn og passord. Hva gjør jeg**. Du vil bli omdirigert til ESET License Administrator, der du kan konvertere legitimasjonen til en lisensnøkkel.

Du kan endre produktlisensen når som helst. For å gjøre dette, klikker du på **Hjelp og støtte** > **Administrer lisens** i hovedvinduet til programmet. Du vil se den offentlige lisens-IDen som brukes til å identifisere din lisens for ESET Support. Brukernavnet som datamaskinen registreres for lagres i delen **Om** som du kan se ved å høyreklikke ikonet i systemstatusfeltet  .

MERKNAD: ESET Remote Administrator kan aktivere klientdatamaskiner i stillhet ved bruk av lisenser som administratoren gjør tilgjengelig. For instrukser for hvordan du gjør det, se ESET Remote Administrator brukerveiledning.

3.8.3 Hvordan bruke gjeldende legitimasjon til å aktivere et nytt produkt

Hvis du allerede har et brukernavn og passord og vil motta en lisensnøkkel, gå til ESET License Administrator-portalen, der du kan konvertere legitimasjonen din til en ny lisensnøkkel.

3.8.4 Fjerne virus fra PC-en

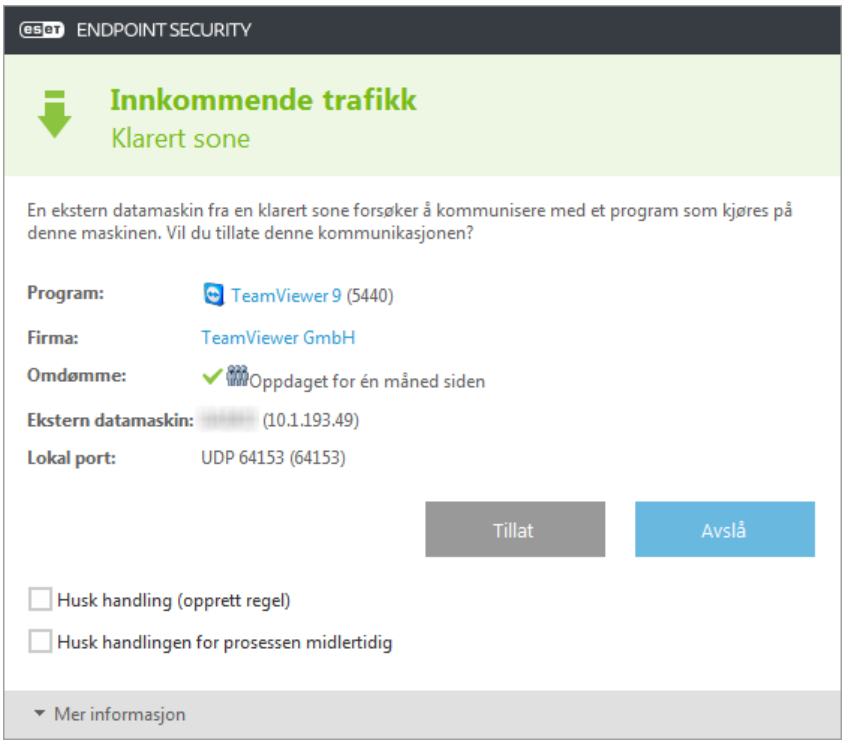
Hvis datamaskinen viser symptomer på å være infisert av skadelig programvare, for eksempel at den er tregere, fryser ofte eller lignende, anbefaler vi at du gjør følgende:

1. Klikk **Datamaskinskanning** i hovedprogramvinduet.
2. Klikk **Smart skanning** for å begynne å skanne gjennom systemet.
3. Etter at skanningen er fullført, kan du gjennomgå loggen med antall skannede, infiserte og rensede filer.
4. Hvis du bare vil skanne en bestemt del av harddisken, velger du **Egendefinert skanning** og angir målene som skal skannes etter virus.

Se vår regelmessig oppdaterte ESET Kunnskapsbaseartikkel for mer informasjon.

3.8.5 Tillate kommunikasjon for et bestemt program

Hvis en ny tilkobling blir oppdaget i interaktiv modus og det ikke er en regel som samsvarer med den, blir du bedt om å tillate eller avslå tilkoblingen. Hvis du ønsker at ESET Endpoint Security skal utføre samme handling hver gang programmet prøver å opprette en tilkobling, merker du av for **Husk handling (opprett regel)**.



I oppsettvinduet for den personlige brannmuren kan du opprette nye personlig brannmurregler for programmer før de blir gjenkjent av ESET Endpoint Security. Dette vinduet finner du under **Avansert oppsett** > **Personlig brannmur** > **Grunnleggende** > **Regler** ved å klikke **Rediger**.

Klikk **Legg til** for å legge til regelen. I kategorien **Generelt** skriver du inn navn, retning og kommunikasjonsprotokoll for regelen. I vinduet kan du definere handlingen du vil at skal utføres når regelen brukes.

Skriv inn banen til programmets kjørbare fil og den lokale kommunikasjonsporten, i kategorien **Lokalt punkt**. Klikk kategorien **Eksternt punkt** for å skrive inn ekstern adresse og port (hvis relevant). Den nyopprettede regelen blir brukt så snart programmet prøver å kommunisere igjen.

3.8.6 Hvordan opprette en ny oppgave i Planlegger

For å opprette en ny oppgave i **Verktøy** > **Planlegger**, Klikker du **Legg til oppgave** eller høyreklikker og velger **Legg til ...** fra hurtigmenyen. Fem typer planlagte oppgaver er tilgjengelig:

- **Kjør eksternt program** – Planlegger kjøring av et eksternt program.
- **Vedlikehold av logg**– Loggfiler inneholder også rester av slettede poster. Denne oppgaven optimerer poster i loggfiler regelmessig for å arbeide effektivt.
- **Filkontroll ved systemstart** – Kontrollerer filer som har lov til å kjøre ved systemstart eller pålogging.
- **Opprett avbildning av datamaskinstatus**– Oppretter datamaskinavbildningen ESET SysInspector– samler detaljert informasjon om systemkomponenter (f.eks. drivere, programmer) og vurderer risikonivået for hver komponent.
- **Datamaskinskanning ved forespørsel** – Utfører en datamaskinskanning av filene og mappene på datamaskinen din.
- **Første skanning**– Som standard 20 minutter etter installasjon eller omstart, gjennomføres en datamaskinskanning som en lavprioritet-oppgave.
- **Oppdater** – Planlegger en oppdateringsoppgave ved å oppdatere virussignaturdatabasen og ved å oppdatere programmoduler.

Fordi **Oppdatering** er en av de mest brukte planlagte oppgavene, vil vi forklare hvordan du legger til en ny oppdateringsoppgave nedenfor:

Velg **Oppdater** i rullegardinmenyen **Planlagt oppgave**. Skriv inn navnet på oppgaven i feltet **Oppgavenavn** og klikk **Neste**. Velg hvor ofte oppgaven skal utføres. Følgende alternativer er tilgjengelige: **Én gang**, **Gjentatte ganger**, **Daglig**, **Ukentlig** og **Utløst av handling**. Velg **Hopp over oppgave hvis datamaskinen kjører på batteri** for å begrense systemressursene mens en laptop kjører på batteristrøm. Oppgaven vil kjøre på datoen og klokkeslettet som er angitt i **Oppgaveutførelse**-feltene. Deretter definerer du hva som skal skje hvis oppgaven ikke kan utføres eller fullføres til planlagt tid. Følgende alternativer er tilgjengelige:

- **På neste planlagte tidspunkt**
- **Så snart som mulig**
- **Umiddelbart, hvis tiden fra forrige utførelse overskrider en angitt verdi** (intervallet kan defineres ved bruk av rulleboksen **Tid fra siste utførelse**)

I neste trinn vises et sammendragsvindu med informasjon om den gjeldende planlagte oppgaven. Klikk **Fullfør** når du er ferdig med endringene.

Et dialogvindu vises, der du kan velge profilene som skal brukes for den planlagte oppgaven. Her kan du angi en primær og alternativ profil. Den alternative profilen blir brukt hvis oppgaven ikke kan fullføres med den primære profilen. Når du bekrefter ved å klikke **Fullført** legges den nye, planlagte oppgaven til listen over gjeldende planlagte oppgaver.

3.8.7 Planlegge en skanningsoppgave (hver 24.time)

For å planlegge en regelmessig oppgave kan du åpne hovedprogramvinduet og klikke **Verktøy** > **Planlegger**. Nedenfor finner du en hurtigguide om hvordan du planlegger en oppgave som skanner lokale stasjoner hver 24. time.

Slik planlegger du en skanningsoppgave:

1. klikk **Legg til** på hovedskjermen for Planlegger.
2. Velg **Datamaskinskanning ved forespørsel** fra rullegardinmenyen.
3. Gi oppgaven et navn, og velg **Gjentatte ganger**.
4. Velg å kjøre oppgaven hver 24. time.
5. Velg en handling som skal utføres hvis den planlagte oppgaven av en eller annen grunn ikke kan kjøres.
6. Gjennomgå sammendraget av den planlagte oppgaven, og klikk **Fullfør**.
7. Velg **Lokale stasjoner** fra rullegardinmenyen **Mål**.
8. Klikk **Fullfør** for å ta i bruk oppgaven.

3.8.8 Hvordan koble ESET Endpoint Security til ESET Remote Administrator

Når du har installert ESET Endpoint Security på datamaskinen og vil koble til via ESET Remote Administrator må du sørge for at du også har installert ERA Agent på klientens arbeidsstasjon. ERA Agent er en essensiell klientløsning som kommuniserer med ERA Server. ESET Remote Administratorbruker RD Sensor-verktøyet til å søke etter datamaskiner på nettverket. Datamaskiner på nettverket som oppdages av RD Sensor vises i nettkonsollen.

Når Agenten er i bruk, kan du gjennomføre ekstern installasjon av ESET sikkerhetsprodukter på klientmaskinen. De nøyaktige trinnene for ekstern installasjon står beskrevet i ESET Remote Administrator-brukerveiledningen.

3.8.9 Hvordan konfigurere et speil

ESET Endpoint Security kan konfigureres ved å lagre kopier av oppdateringsfiler for virussignatur og distribuere oppdateringene til andre arbeidsstasjoner som kjører ESET Endpoint Security eller ESET Endpoint Antivirus.

Konfigurere ESET Endpoint Security som en speilserver for å gi oppdateringer via en intern HTTP-server

Trykk på **F5** for å gå inn i Avansert oppsett og utvid deretter **Oppdatere** > **Grunnleggende**. Sørg for at **Oppdateringsserver** er satt til **AUTOMATISK VALG**. Velg **Opprett oppdateringsspeil** og **Last ned oppdateringsfiler via intern HTTP-server** fra **Avansert oppsett** > **Grunnleggende** > **Speil**.

Konfigurere en speilserver til å gi oppdateringer via en delt nettverksmappe

Opprett en delt mappe på en lokal stasjon eller nettverksstasjon. Denne mappen må kunne leses av alle som kjører ESETs sikkerhetsløsninger og være skrivbar fra den lokale SYSTEM-kontoen. Aktiver **Opprett oppdateringsspeil** under **Avansert oppsett** > **Grunnleggende** > **Speil**. Bla gjennom og velg den delte mappen som ble opprettet.

MERKNAD: Hvis du ikke vil oppdatere via intern HTTP-server, koble ut **Last ned oppdateringsfiler via intern HTTP-server**.

3.8.10 Hvordan oppgraderer jeg til Windows 10 med ESET Endpoint Security

 Vi anbefaler at du oppgraderer til den nyeste versjonen av ditt ESET-produkt og laster ned den nyeste virussignaturdatabasen, før du oppgraderer til Windows 10. Dette gir maksimal beskyttelse og bevarer programinnstillingene og lisensinformasjonen når du oppgraderer til Windows 10.

Versjon 6.x og nyere:

Klikk på den passende koblingen for å laste ned og installere den siste versjonen for å gjøre klart for oppgraderingen til Windows 10:

Last ned ESET Endpoint Security 6 32-bit Last ned ESET Endpoint Antivirus 6 32-bit

Last ned ESET Endpoint Security 6 64-bit Last ned ESET Endpoint Antivirus 6 64-bit

Versjon 5.x og eldre:

Klikk på den passende koblingen for å laste ned og installere den siste versjonen for å gjøre klart for oppgraderingen til Windows 10:

Last ned ESET Endpoint Security 5 32-bit Last ned ESET Endpoint Antivirus 5 32-bit

Last ned ESET Endpoint Security 5 64-bit Last ned ESET Endpoint Antivirus 5 64-bit

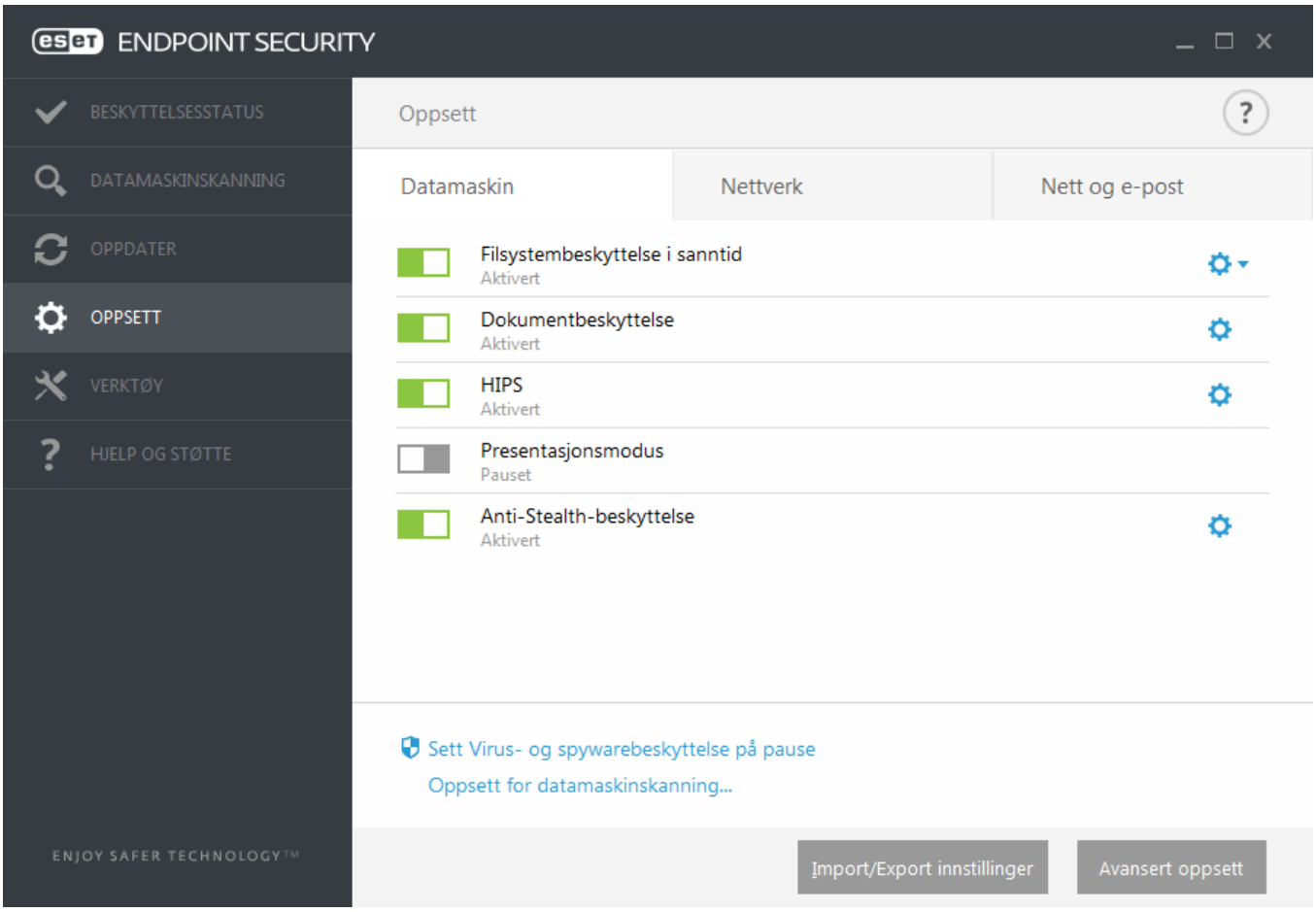
Versjoner på andre språk:

Hvis du ser etter en versjon av ditt ESET-endepunktprodukt på et annet språk, gå til vår nedlastingsside.

MERKNAD: Mer informasjon om kompatibilitet til ESET-produkter med Windows 10.

3.9 Arbeide med ESET Endpoint Security

Med oppsettalternativene for ESET Endpoint Security kan du justere beskyttelsesnivået for datamaskinen, Internett, e-post og nettverket.



Oppsett-menyen inneholder følgende deler:

- **Datamaskin**
- **Nettverk**
- **Nett og e-post**

I Oppsett av **Datamaskin**-beskyttelse kan du aktivere eller deaktivere følgende komponenter:

- **Filsystembeskyttelse i sanntid** – Alle filer blir skannet for ondsinnet kode det øyeblikket de blir åpnet, opprettet eller kjørt på datamaskinen.
- **Dokumentbeskyttelse** – Dokumentbeskyttelsen skanner Microsoft Office-dokumenter før de åpnes, samt filer som lastes ned automatisk fra Internet Explorer, f.eks. Microsoft ActiveX-elementer.
- **HIPS** – HIPS-systemet overvåker hendelser som oppstår i operativsystemet og reagerer på dem i henhold til et tilpasset sett med regler.
- **Presentasjonsmodus** – en funksjon for brukere som krever uavbrutt bruk av programvaren, og som ikke ønsker å bli forstyrret av popup-vinduer som dukker opp og som ønsker å minimere bruken av CPU. Du vil få en advarsel (potensiell sikkerhetsrisiko) og hovedprogramvinduet vil bli gult etter at Presentasjonsmodus er aktivert.
- **Anti-Stealth-beskyttelse** Oppdager farlige programmer, for eksempel rootkits, som er i stand til å skjule seg selv for operativsystemet. Det betyr at det ikke er mulig å oppdage dem ved hjelp av vanlige teknikker for testing.

Nettverk-delen lar deg aktivere eller deaktivere den **Personlige brannmuren**.

I oppsettet for **Nett og e-post**-beskyttelse kan du aktivere eller deaktivere følgende komponenter:

- **Nettkontroll** – blokkerer nettsider som kan inneholde potensielt støtende materiale. I tillegg kan systemansvarlige angi tilgangen til tilgangspreferanser for 27 forhåndsdefinerte nettstedskategorier.
- **Beskyttelse for nettilgang** – Hvis denne er aktivert, blir all trafikk gjennom HTTP eller HTTPS skannet for skadelig programvare.
- **Beskyttelse for e-postklient** – overvåker kommunikasjon mottatt gjennom POP3- og IMAP-protokollen.
- **Spambeskyttelse** – skanner uønsket e-post, dvs. spam.
- **Anti-phishing-beskyttelse** – beskytter deg mot forsøk på å få tilgang til passord, bankdata eller annen sensitiv informasjon ved å maskere seg som et troverdig webområde.

Hvis du vil deaktivere enkeltmoduler midlertidig, klikker du den grønne bryteren  ved siden av ønsket modul. Legg merke til at dette kan redusere beskyttelsen av datamaskinen.

Hvis du vil aktivere beskyttelsen av den deaktiverte sikkerhetskomponenten på nytt, klikker du den røde bryteren  for å aktivere en komponent på nytt.

MERKNAD: Alle beskyttelsestiltak som deaktiveres på denne måten aktiveres på nytt etter at datamaskinen har blitt startet på nytt.

Hvis du vil vise detaljerte innstillinger for hver enkelt modul, klikker du tannhjulet ⚙ ved siden av en hvilken som helst komponent**.**

Det er flere alternativer nederst i oppsettvinduet. For å laste inn oppsettparametere ved bruk av en *.xml*-konfigureringsfil, eller for å lagre gjeldende oppsettparametere i en konfigureringsfil, brukes **Importer/Eksporter innstillinger**. Se Importer/eksporter innstillinger for detaljert informasjon.

Hvis du vil angi mer detaljerte alternativer, klikker du **Avansert oppsett** eller trykk på **F5**.

3.9.1 Datamaskin

Datamaskin-modulen finner du under **Oppsett** > **Datamaskin**. Den viser en oversikt over beskyttelsesmodulene beskrevet i forrige kapittel. Følgende innstillinger er tilgjengelige i denne delen:

Klikk tannhjulet ⚙ ved siden av **Filsystembeskyttelse i sanntid** og klikk **Rediger utelatelser** for å åpne oppsettvinduet Utelatelse. Med dette vinduet kan du utelate filer og mapper fra skanning.

MERKNAD: Dokumentbeskyttelsesstatus vil kanskje ikke være tilgjengelig før du aktiverer det i **Avansert oppsett** (F5) > **Antivirus** > **Dokumentbeskyttelse**. Etter du har aktivert det, må du starte datamaskinen på nytt fra ruten Oppsett > Datamaskin, ved å klikke på **Start på nytt** under enhetskontroll, eller du kan gjøre det fra ruten beskyttelsesstatus ved å klikke på **Start datamaskinen på nytt**.

Sett virus- og spywarebeskyttelse på pause – Hvis du midlertidig deaktiverer modulene, Antivirus, Spywarebeskyttelse eller Personlig brannmur, kan du velge tidsperioden du ønsker at den valgte komponenten skal være deaktivert ved å bruke rullegardinmenyen og deretter klikke **Bruk** for å deaktivere sikkerhetskomponenten. Når du skal reaktivere beskyttelsen, klikker du **Aktiver virus- og spywarebeskyttelse**.

Oppsett for datamaskinskanning ... – Klikk her for å justere parameterne til datamaskinskanningen (manuelt utført skanning).

3.9.1.1 Virusbeskyttelse

Virusbeskyttelse beskytter mot skadelige systemangrep ved å kontrollere filer, e-postmeldinger og Internett-kommunikasjon. Hvis det oppdages en trussel, kan virusmodulen eliminere den ved først å blokkere den og deretter rense den, slette den eller flytte den i karantene.

Hvis vil konfigurere innstillinger for antivirusmodulen i detalj, klikker du **Avansert oppsett** eller trykker **F5**.

Alternativer for skanner for alle beskyttelsesmoduler (for eksempel Filsystembeskyttelse i sanntid, Beskyttelse for nettilgang, ...) lar deg aktivere eller deaktivere gjenkjenning av følgende:

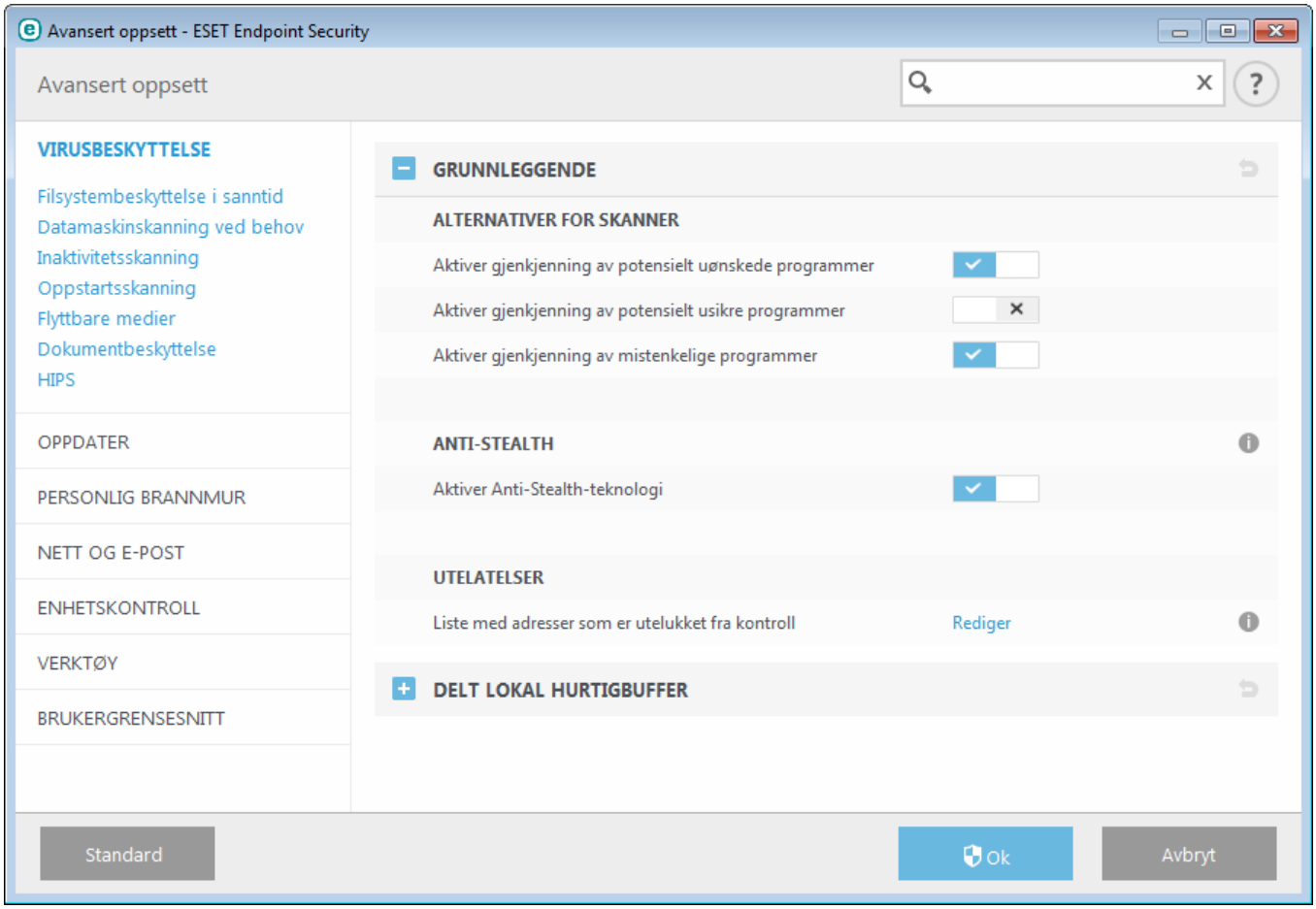
- **Potensielt uønskede programmer** (PUAer) er ikke nødvendigvis ment å være skadelige, men kan påvirke datamaskinens ytelse negativt.

Du kan lese mer om denne typen programmer i ordlisten.

- **Potensielt usikre programmer** henviser til legitim, kommersiell programvare som har potensial til å bli misbrukt til ondsinnede formål. Eksempler på potensielt usikre programmer inkluderer verktøy for ekstern tilgang, programmer for å knekke passord samt keyloggere (programmer som registrerer alle tastetrykk som foretas av en bruker). Dette alternativet er deaktivert som standard.
  Du kan lese mer om denne typen programmer i ordlisten.
- **Mistenkelige programmer** omfatter programmer som er komprimert med pakkere eller beskyttere. Disse typene programmer utnyttes ofte av forfattere av skadelig programvare for å unngå oppdagelse.

Anti-Stealth-teknologien er et avansert system som oppdager farlige programmer, for eksempel rootkits, som er i stand til å skjule seg selv for operativsystemet. Det betyr at det ikke er mulig å oppdage dem ved hjelp av vanlige teknikker for testing.

Med **Unntak** kan du utelate filer og mapper fra skanning. For å sikre at alle objekter skannes for trusler, anbefaler vi at du kun oppretter unntak hvis det er absolutt nødvendig. Tilfeller der du vil kunne ha behov for å ekskludere et objekt kan inkludere skanning av store databaseoppføringer som vil gjøre datamaskinen treg ved skanning, eller programvare som er i konflikt med skanningen. Utelukke et objekt fra skanning, se Unntak.



3.9.1.1.1 En infiltrering er gjenkjent

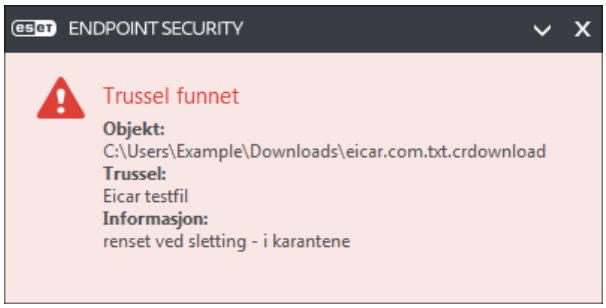
Infiltrasjon kan nå systemet fra forskjellige inngangspunkter, for eksempel nettsider, delte mapper, via e-post eller fra flyttbare enheter (USB, eksterne harddisker, CD-er, DVD-er, disketter osv.).

Standard atferd

Som et generelt eksempel på hvordan infiltrasjoner blir håndtert i ESET Endpoint Security, kan infiltrasjoner oppdages ved hjelp av:

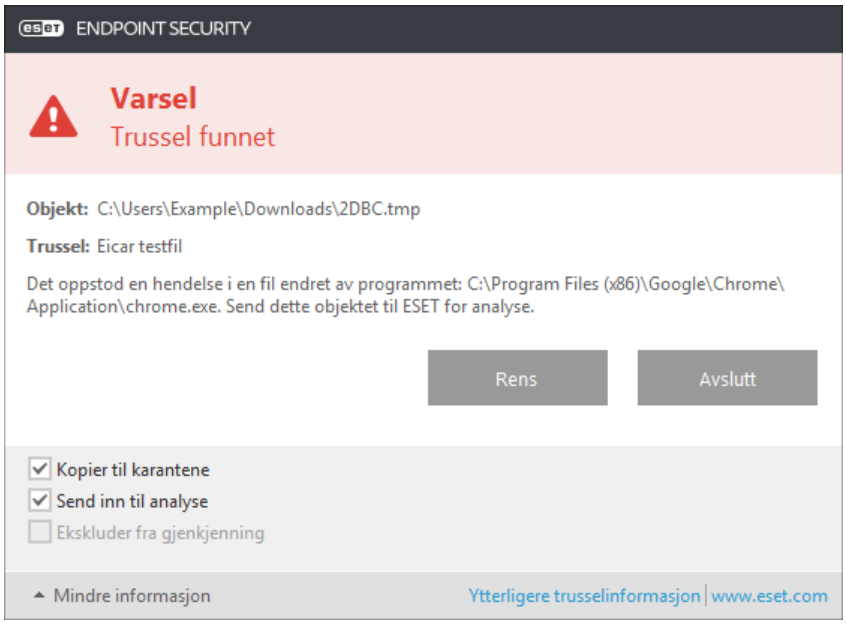
- Filsystembeskyttelse i sanntid
- Beskyttelse for nettilgang
- Beskyttelse for e-postklient
- Datamaskinskanning ved behov

Hver enkelt bruker standard rensenivå og vil prøve å rense filen og flytte den til Karantene eller avslutte tilkoblingen. Det vises et meldingsvindu i meldingsområdet nederst til høyre på skjermen. Hvis du ønsker mer informasjon om rensenivåer og atferd, se Rensing.



Rensing og sletting

Hvis det ikke er en forhåndsdefinert handling som skal utføres av Filsystembeskyttelse i sanntid, blir du alltid bedt om å velge et alternativ i varselsvinduet. Vanligvis er alternativene **Rens**, **Slett** og **Ingen handling** tilgjengelig. Det frarådes å velge **Ingen handling**, ettersom dette lar infiserte filer forbli urenset. Unntaket er når du er sikker på at en fil er sikker og har blitt oppdaget ved en feil.



Bruk rensing hvis en fil har blitt angrepet av et virus som har lagt til ondsinnet kode til filen. Hvis dette er tilfellet, vil den først prøve å rense den infiserte filen for å gjenopprette den til original tilstand. Hvis filen består utelukkende av skadelig kode, blir den slettet.

Hvis en infisert fil er "låst" eller i bruk av en systemprosess, blir den vanligvis først slettet etter at den er frigjort (vanligvis etter at systemet er startet på nytt).

Flere trusler

Hvis det finnes infiserte filer som ikke blir renset i en Datamaskinskanning (eller Rensenivå er satt til **Ingen rensing**), kommer det frem et varselsvindu som ber deg om å velge handling for filene som vises.

Sletting av filer i arkiver

I standard rensemodus blir hele arkivet slettet hvis det bare inneholder infiserte filer og ingen rene filer. Med andre ord blir ikke arkivene slettet hvis de også inneholder sikre, rene filer. Du må utvise forsiktighet når du utfører en grundig renseskanning, med Grundig rensing aktivert blir arkivet slettet hvis det inneholder minst én infisert fil, uavhengig av status på de andre filene i arkivet.

Hvis datamaskinen viser tegn til å være infisert av skadelig programvare, det vil si at den er tregere, fryser ofte osv., anbefaler vi at du gjør følgende:

- Åpne ESET Endpoint Security og klikk Datamaskinskanning
- Klikk **Smart skanning** (du finner mer informasjon i delen Datamaskinskanning)
- Etter at skanningen er fullført, kan du gjennomgå loggen for antall skannede, infiserte og rensede filer

Hvis du ønsker å skanne en bestemt del av harddisken, velger du **Egendefinert skanning** og velger målene som skal skannes for virus.

3.9.1.2 Delt lokal hurtigbuffer

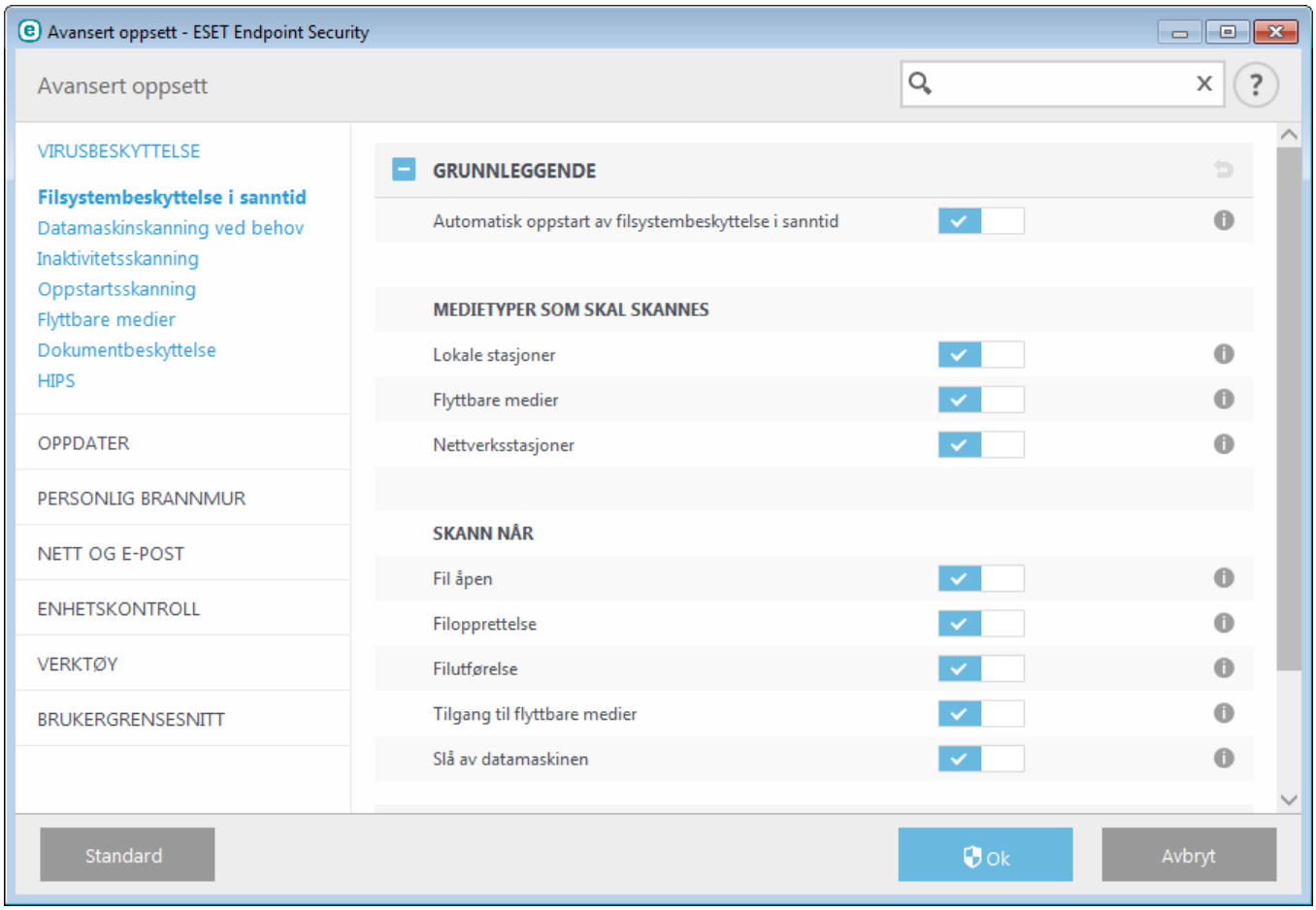
Delt lokal hurtigbuffer vil øke ytelsen i virtualiserte miljøer ved å eliminere identiske skanninger i nettverket. Dette sikrer at hver fil skannes bare én gang og lagres i den delte bufferen. Slå på bryteren **Bufferalternativ** for å lagre informasjon om filskanninger og mapper på nettverket ditt til den lokale hurtigbufferen. Hvis du utfører en ny skanning, vil ESET Endpoint Security søke etter skannede filer i hurtigbufferen. Matchende filer utelukkes fra skanning.

Oppsettet av **Hurtigbufferserveren** inneholder følgende**:**

- **Vertsnavn** – Navn eller IP-adresse til datamaskinen der hurtigbufferen befinner seg.
- **Port** – Antall porter som brukes til kommunikasjon (samme antall som ble angitt i Delt lokal hurtigbuffer).
- **Passord** – Spesifiser passordet for ESET Delt lokal hurtigbuffer etter behov.

3.9.1.3 Filsystembeskyttelse i sanntid

Filsystembeskyttelse i sanntid kontrollerer alle virusrelaterte hendelser på systemet. Alle filer blir skannet for ondsinnet kode det øyeblikket de blir åpnet, opprettet eller kjørt på datamaskinen. Filsystembeskyttelse i sanntid blir startet ved systemstart.



Som standard startes filsystembeskyttelse i sanntid samtidig med systemet for å sikre kontinuerlig skanning. I særskilte tilfeller (for eksempel hvis en konflikt oppstår med en annen sanntids-skanner), kan du deaktivere beskyttelse i sanntid ved å deaktivere **Automatisk oppstart av filsystembeskyttelse i sanntid** i **Avansert oppsett** i **Filsystembeskyttelse i sanntid**> **Grunnleggende**.

Medietyper som skal skannes

Som standard blir alle typer medier skannet for potensielle trusler:

Lokale stasjoner - kontrollerer alle systemharddisker.
Flyttbare medier – Kontroller CD/DVD, USB-lagring, Bluetooth-enheter, osv.
Nettverksstasjoner - skanner alle nettverksstasjoner.

Vi anbefaler at du bruker standardinnstillingene og at disse innstillingene bare endres i spesifikke tilfeller, som når skanning av bestemte medier reduserer dataoverføringer betydelig.

Skann når

Standardinnstillingen er at alle filer blir skannet ved åpning, utførelse eller opprettelse. Vi anbefaler at du beholder standardinnstillingene, fordi disse gir maksimalt nivå av beskyttelse i sanntid for datamaskinen:

- **Fil åpen** – aktiverer eller deaktiverer skanning av åpne filer.
- **Filopprettelse** – aktiverer eller deaktiverer skanning av nylig opprettede filer.
- **Filutførelse** – aktiverer eller deaktiverer skanning når filer kjøres.
- **Tilgang til flyttbare medier**– Aktiverer eller deaktiverer skanning som er utløst ved tilgang til spesielle flyttbare medier med lagringsplass.
- **Avslutning av datamaskin** – aktiverer eller deaktiverer skanning som utløses ved avslutning.

Filsystembeskyttelsen i sanntid kontrollerer alle medietyper, og kontrollen blir utløst av forskjellige systemhendelser, for eksempel at en fil tas i bruk. Bruk av oppdagelsesmetoder som er basert på ThreatSense-teknologi (beskrives i avsnittet Oppsett av parametere for ThreatSenseengine parameter setup) kan føre til at filsystembeskyttelse i sanntid konfigureres til å behandle nyopprettede filer annerledes enn eksisterende filer. Du kan for eksempelkonfigurere filsystembeskyttelse i sanntid til å overvåke nyopprettede filer nøyere.

For å sikre et minimalt systemavtrykk ved bruk av beskyttelse i sanntid blir filer som allerede er skannet, ikke skannet gjentatte ganger (med mindre de har blitt endret). Filene skannes på nytt umiddelbart etter at virussignaturdatabasen er oppdatert. Denne atferden kan endres ved bruk av **Smartoptimalisering**. Hvis **Smartoptimalisering** deaktiveres, skannes alle filene hver gang de åpnes. Denne innstillingen endres ved å trykke **F5** for å åpne Avansert oppsett og utvide **Antivirus** > **Filsystembeskyttelse i sanntid**. Klikk **ThreatSense-parameter** > **Annet** og velg eller velg bort **Aktiver smart optimalisering**.

3.9.1.3.1 Ytterligere ThreatSense-parametere for utførte filer

Tilleggsparametere for ThreatSense for nye og modifiserte filer – Sannsynligheten for infeksjon i nyopprettede eller endrede filer er høyere enn i eksisterende filer. Derfor kontrollerer programmet disse filene med ekstra skanneparametere. Sammen med felles signaturbaserte metoder brukes også avansert heuristikk, noe som kan oppdage nye trusler før en oppdatering av virussignaturdatabasen utgis. I tillegg til nyopprettede filer skannes selvutpakkende filer (.sfx) og kjøretidspakker (internt komprimerte kjørbare filer). Arkivene skannes som standard opptil det 10. dybdenivået, og kontrolleres uavhengig av faktisk størrelse. Hvis du vil endre skanneinnstillingene for arkiver, fjerner du merket for **Standardinnstillinger for skanning av arkiv**.

For å lære mer om **Kjøretidspakker**, **Selvutpakkende arkiver** og **Avansert heuristikk**, se ThreatSense oppsett av motorparametere.

Tilleggsparametere for ThreatSense for utførte filer – Som standard brukes det ikke Avansert heuristikk når filer kjøres. Når dette er aktivert, anbefaler vi å la Smartoptimalisering og ESET Live Grid være aktivert for å holde systempåkjenning til et minimum.

3.9.1.3.2 Rensenivåer

Beskyttelsen i sanntid har tre rensenivåer (du får tilgang ved å klikke **Oppsett av parametere for ThreatSense-motor** i delen **Filsystembeskyttelse i sanntid** og deretter klikke **Rensing**).

Ingen rensing – Infiserte filer blir ikke renset automatisk. Programmet viser et varselvindu og lar brukeren velge en handling. Dette nivået er utformet for mer avanserte brukere som vet hvilke trinn de skal utføre i tilfelle en infiltrasjon.

Vanlig rensing – Programmet vil prøve å rense eller slette en infisert fil automatisk basert på en forhåndsdefinert handling (avhengig av typen infiltrering). Gjenkjennelse og sletting av en infisert fil blir varslet med en melding nede i høyre hjørne på skjermen.. Hvis det ikke er mulig å velge riktig handling automatisk, gir programmet andre handlingsmuligheter. Det samme skjer hvis en forhåndsdefinert handling ikke kan fullføres.

Grundig rensing – Programmet vil rense eller slette alle infiserte filer. Det eneste unntaket er systemfilene. Hvis det ikke er mulig å rense dem, blir brukeren bedt om å velge en handling i et varselvindu.

Advarsel: Hvis et arkiv inneholder én eller flere infiserte filer, har du to alternativer for å behandle arkivet. I standardmodus (Standardrensing) blir hele arkivet slettet hvis alle filene i arkivet er infiserte filer. I modusen **Grundig rensing** blir arkivet slettet hvis det inneholder minst én infisert fil, uavhengig av statusen til de andre filene i arkivet.

3.9.1.3.3 Kontrollere beskyttelse i sanntid

For å bekrefte at beskyttelsen i sanntid fungerer og gjenkjenner virus, brukes en testfil fra eicar.com. Denne testfilen er en ufarlig fil som alle antivirusprogrammer kan finne. Filen ble opprettet av EICAR (European Institute for Computer Antivirus Research) for å teste funksjonaliteten til virusprogrammer. Filen er tilgjengelig for nedlastning på http://www.eicar.org/download/eicar.com

MERKNAD: Før en beskyttelseskontroll i sanntid utføres, er det nødvendig å deaktivere brannmuren. Hvis brannmuren er aktivert, vil den gjenkjenne filene og forhindre nedlastning av testfilene. Sørg for at du reaktiverer brannmuren umiddelbart etter at du har utført en kontroll av filsystembeskyttelse i sanntid.

3.9.1.3.4 Når skal du endre konfigurasjonen av beskyttelsen i sanntid

Filsystembeskyttelse i sanntid er den viktigste komponenten i å holde et sikkert system ved like. Derfor må du være forsiktig når du endrer parameterne. Vi anbefaler at du endrer parametrene for sanntidsbeskyttelse bare i spesielle tilfeller.

Når ESET Endpoint Security installeres, er alle innstillingene optimalisert for å gi brukerne det høyeste nivået av systemsikkerhet. Standardinnstillingene kan tilbakestilles ved å klikke ↩ ved siden av hver kategori i vinduet (**Avansert oppsett** > **Antivirus** > **Filsystembeskyttelse i sanntid**).

3.9.1.3.5 Hva du skal gjøre hvis beskyttelse i sanntid ikke fungerer

I dette kapittelet beskriver vi problemer som kan oppstå ved bruk av beskyttelse i sanntid, og hvordan du kan løse problemene.

Beskyttelsen i sanntid er deaktivert

Hvis beskyttelsen i sanntid utilsiktet ble deaktivert av en bruker, må den aktiveres på nytt. Du aktiverer beskyttelsen i sanntid på nytt ved å gå til **Oppsett** i hovedvinduet og klikke **Sanntidsbeskyttelse av filsystemet**.

Hvis sanntidsbeskyttelsen ikke starter når systemet starter, er det vanligvis fordi alternativet **Automatisk oppstart av filsystembeskyttelse i sanntid** er deaktivert. Du aktiverer dette alternativet ved å navigere til **Avansert oppsett** (**F5**) og klikke på **Antivirus** > **Filsystembeskyttelse i sanntid**> **Grunnleggende**. Sørg for at bryteren **Automatisk oppstart av filsystembeskyttelse i sanntid** er slått på.

Hvis beskyttelsen i sanntid ikke oppdager og renser infiltrasjoner

Forsikre deg om at ingen andre virusprogrammer er installert på datamaskinen. Hvis to beskyttelsesskjold i sanntid er aktivert samtidig, kan det skape en konflikt. Vi anbefaler at du avinstallerer andre virusprogrammer på systemet før du installerer ESET.

Beskyttelsen i sanntid starter ikke

Hvis beskyttelsen i sanntid ikke starter når systemet starter opp (og alternativet **Automatisk oppstart av filsystembeskyttelse i sanntid** er aktivert), kan det være på grunn av konflikter med andre programmer. Ta gjerne kontakt med ESET brukerstøtte for hjelp til å løse dette problemet.

3.9.1.4 Datamaskinskanning ved behov

Skanning ved behov er en viktig del av ESET Endpoint Security. Den brukes til å utføre skanning av filer og mapper på datamaskinen. For å være på den sikre siden er det viktig at datamaskinskanning ikke bare kjøres når det er mistanke om en infisering, men jevnlig som en del av rutinemessige sikkerhetstiltak. Vi anbefaler at du utfører regelmessige dybdeskanninger av systemet for å oppdage virus som ikke fanges opp av Filsystembeskyttelse i sanntid. Dette kan skje hvis Filsystembeskyttelse i sanntid ble deaktivert på det tidspunktet, hvis virusdatabasen var foreldet eller hvis filen ikke ble oppdaget som et virus da den ble lagret til disken.

Du kan velge mellom to typer **Datamaskinskanning**. **Smart skanning** skanner systemet raskt uten behov for ytterligere konfigurasjon av skanneparameterne. **Egendefinert skanning** lar deg velge en av de forhåndsdefinerte skanneprofilene og definere spesifikke skannemål.

Se Skannefremdrift for mer informasjon om skanneprosessen.

Smart skanning

Smart skanning lar deg raskt starte datamaskinskanning og rense infiserte filer uten at du trenger å foreta deg noe. Fordelen med Smart skanning er at den er lett å bruke og ikke krever detaljert skanningskonfigurasjon. Smart skanning kontrollerer alle filer på lokale stasjoner, og renser eller sletter automatisk infiltreringer som blir funnet. Rensenivået blir automatisk stilt inn til standardverdien. Se Rensing for mer detaljert informasjon om typer rensing.

Egendefinert skanning

Egendefinert skanning er en optimal løsning hvis du vil spesifisere skanneparametrene, for eksempel mål som skal skannes, og skannemetoder. Fordelen med Egendefinert skanning er muligheten til å konfigurere parametrene detaljert. Konfigurasjonene kan lagres i brukerdefinerte skanneprofiler, som kan være nyttig hvis skanningen gjentas med de samme parameterne.

Du velger skannemål ved å velge **Datamaskinskanning** > **Egendefinert skanning** og velger er alternativ fra rullegardinmenyen **Skannemål**, eller velger spesifikke mål fra trestrukturen. Mål for skanning kan også defineres ved å skrive inn banen til mappen eller filen(e) du ønsker å ta med. Hvis du bare er interessert i å skanne systemet uten ekstra rensingstiltak, velger du alternativet **Skann uten å rense**. Når du utfører en skanning kan du velge fra tre rensenivåer, ved å klikke **Oppsett ...**. > **Oppsett av parametere for ThreatSense** > **Rengjøring**.

Datamaskinskanning med egendefinert skanning er egnet for avanserte brukere som har erfaring i å bruke virusbeskyttelsesprogrammer.

Skanning av flyttbare medier

Lignende Smart skanning – start raskt en skanning av flyttbare medier (som CD/DVD/USB) som for øyeblikket er koblet til datamaskinen. Dette kan være nyttig når du kobler en USB-minnepinne til en datamaskin og ønsker å skanne innholdet for skadelig programvare eller andre potensielle trusler.

Denne typen skanning kan også startes ved å klikke **Egendefinert skanning** og deretter velge **Flyttbare medier** fra rullegardinmenyen **Skannemål** og klikke **Skann**.

Du kan bruke rullegardinmenyen **Handling etter skanning** til å velge handlingen (Ingen handling, Slå av, Omstart og Dvale) som skal utføres etter skanning.

Aktiver avslutning etter skanning – aktiverer en planlagt stans av systemet når datamaskinkanningen etter behov avsluttes. Et bekreftelsesdialogvindu for avslutning viser en 60 sekunders nedtelling. Klikk **Avbryt** for å avbryte avslutningen du bad om.

MERKNAD: Vi anbefaler at du kjører en datamaskinskanning minst én gang i måneden. Skanning kan konfigureres som en planlagt oppgave fra **Verktøy** > **Planlegger**.

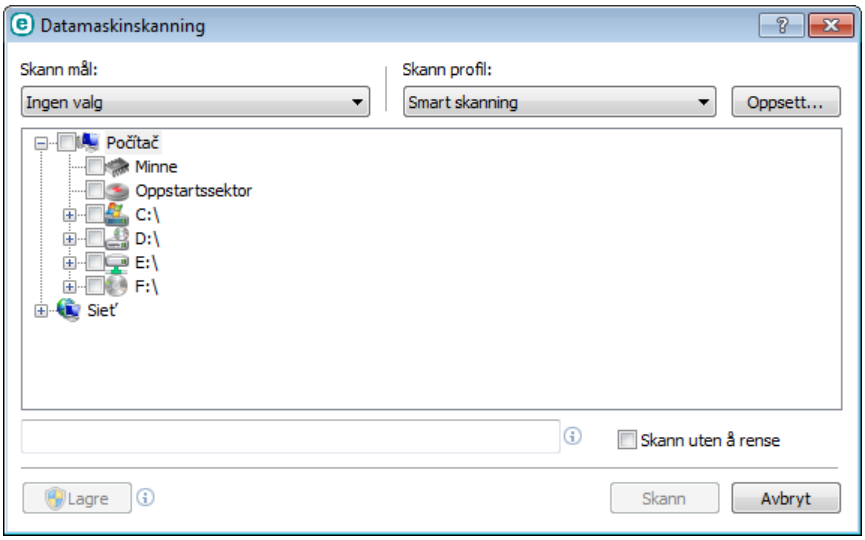
3.9.1.4.1 Oppstartsprogram for egendefinert skanning

Hvis du ønsker å skanne et bestemt mål, kan du velge Egendefinert skanning ved å klikke **Datamaskinskanning** > **Egendefinert skanning** og velge et alternativ fra rullegardinmenyen **Skannemenyen** eller velge bestemte mål fra mappestrukturen.

I vinduet Skann mål for skanning kan du definere hvilke objekter (minne, stasjoner, sektorer, filer og mapper) som skal skannes for infiltrasjoner. Velg mål fra trestrukturen som viser alle tilgjengelige enheter på datamaskinen. I rullegardinmenyen til **Skann mål** kan du velge forhåndsdefinerte skannemål.

- **Etter profilinnstillinger** – Velger mål angitt i den valgte skanneprofilen.
- **Flyttbare medier** – Velger disketter, USB-lagringsenheter, CD/DVD.
- **Lokale stasjoner** – Velger alle systemharddisker.
- **Nettverksstasjoner** – Velger alle tilordnede nettverksstasjoner.
- **Ikke valg** – avbryter alle valg.

Du kan raskt gå til et skannemål eller direkte legge til et ønsket mål (mappe eller fil(er)) ved å skrive det inn i det tomme feltet under mappelisten. Dette er bare mulig hvis ingen mål er valgt i trestrukturen, og menyen **Skann mål** er satt til **Ikke valg**.



Infiserte elementer renses ikke automatisk. Skanning uten å rense kan brukes for å få en oversikt over den gjeldende beskyttelsesstatusen. Hvis du bare er interessert i å skanne systemet uten ekstra rensingstiltak, velger du alternativet **Skann uten å rense**. Videre kan du velge blant tre rensenivåer ved å klikke **Oppsett ...** > **Oppsett av parametere for ThreatSense** > **Rengjøring**. Informasjon om skanningen blir lagret i en skannelogg.

Du kan velge en profil som skal brukes for å skanne valgte mål, fra rullegardinmenyen **Skanneprofil**. Standardprofilen er **Smart skanning**. Det er to andre forhåndsdefinerte skanneprofiler som heter **Dybdeskanning** og **Hurtigmenyskanning**. Disse skanneprofilene bruker forskjellige ThreatSense motorparametere. Klikk på **Oppsett ...** hvis du ønsker å opprette valgt skanneprofil fra menyen Skanneprofil i detalj. De tilgjengelige alternativene er beskrevet i ai delen **Annet** i Oppsett av parametere for ThreatSense-motor.

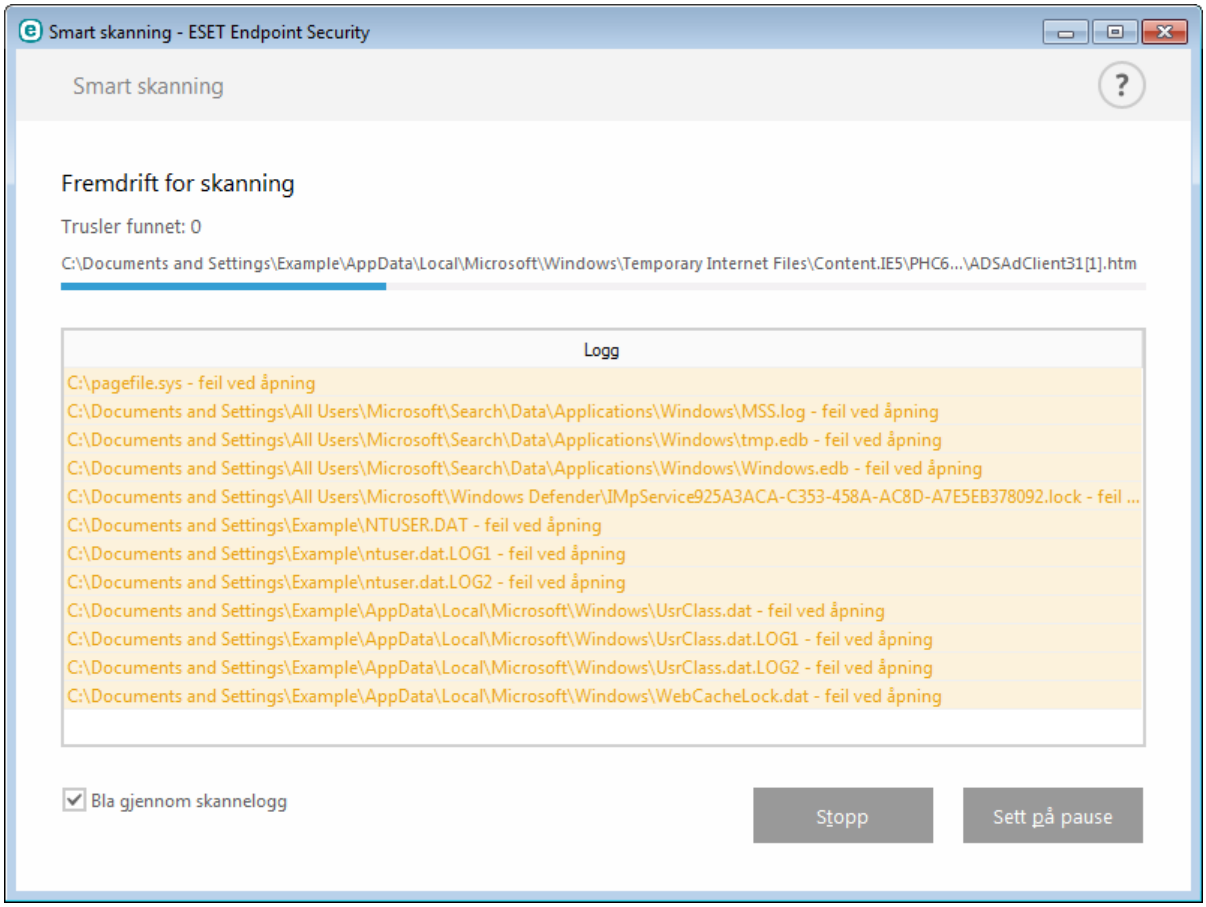
Klikk **Lagre** for å lagre endringer du har gjort i målvalget, inkludert valg innenfor mappestrukturen.

Klikk **Skann** for å utføre skanningen med egendefinerte parametre som du har angitt.

Knappen **Skann som administrator** lar deg utføre skanningen under administratorkontoen. Klikk dette hvis gjeldende påloggede bruker ikke har nok rettigheter til å få tilgang til riktige filer som skal skannes. Merk at denne knappen ikke er tilgjengelig hvis gjeldende påloggede bruker ikke kan kontakte UAC-operasjoner som administrator.

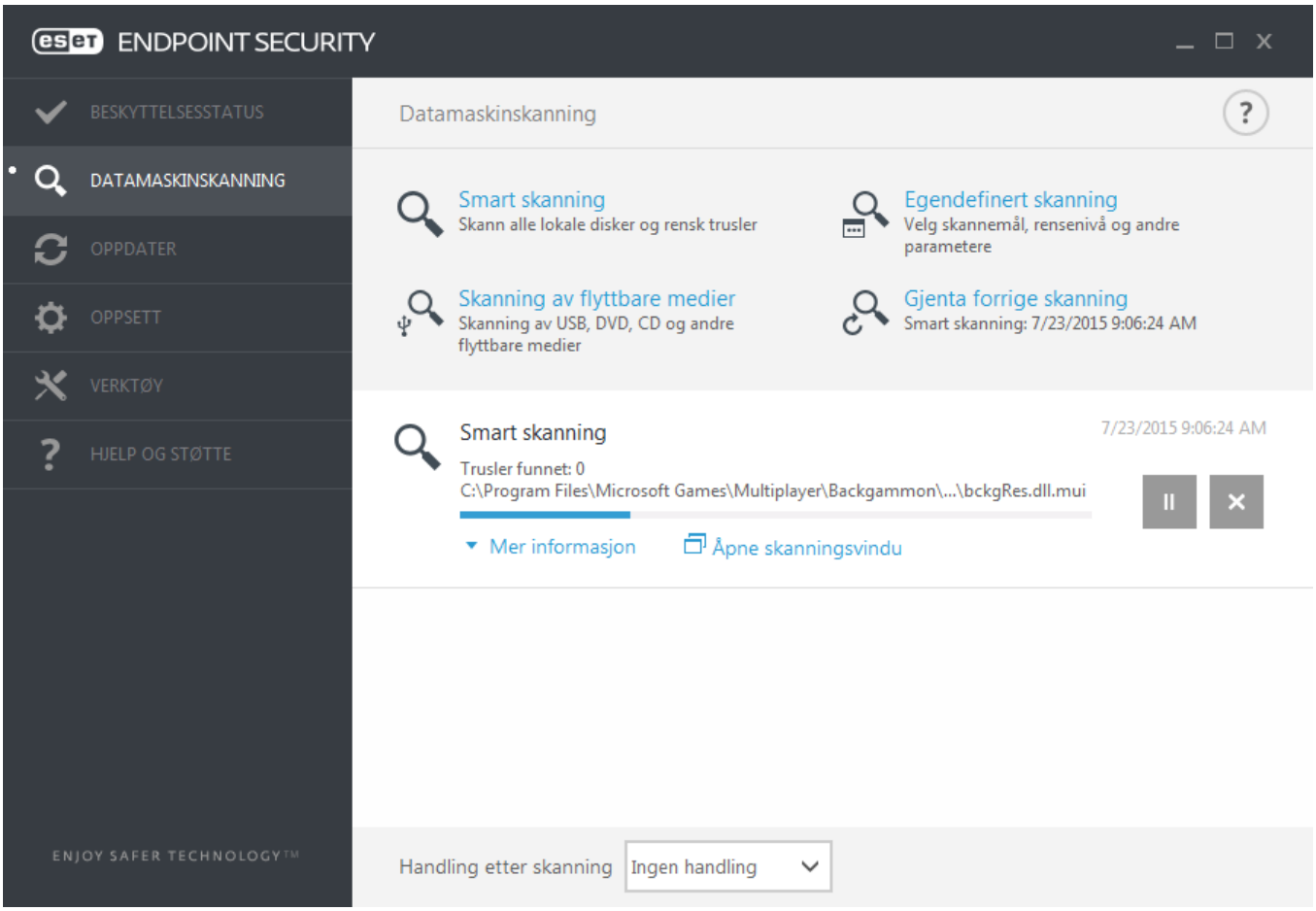
3.9.1.4.2 Skannefremdrift

Skannefremdriftsvinduet viser gjeldende status for skanning og informasjon om antall filer funnet med skadelig kode.



MERKNAD: Det er normalt at noen filer, slik som passordbeskyttede filer eller filer som utelukkende brukes av systemet (vanligvis *pagefile.sys* og visse loggfiler), ikke kan skannes.

Skannefremdrift – Fremdriftsstolpen viser prosentandelen av allerede skannede objekter sammenlignet med objekter som ennå ikke er skannet. Verdien på skannefremdrift er avledet av det totale antallet objekter som er inkludert i skanningen.
Mål – navnet på objekter som skannes i øyeblikket, og deres plassering.
Trusler funnet – viser samlet antall trusler funnet under en skanning.
Pause – tar pause i skanningen.
Fortsett – Dette alternativet er synlig når skannefremdriften har hatt pause. Klikk **Fortsett** for å fortsette skanningen.
Stopp – avslutter skanningen.
Bla gjennom skannelogg – hvis aktivert, vil skanneloggen rulle ned automatisk ettersom nye registreringer legges til slik at de nyeste registreringene er synlig.



3.9.1.5 Enhetskontroll

ESET Endpoint Security gir kontroll av automatiske medier (CD/DVD/USB/...). Med denne modulen kan du skanne, blokkere eller tilpasse utvidede filtre/tillatelser og angi hvordan brukeren kan få tilgang til og arbeide med en gitt enhet. Dette kan være nyttig hvis datamaskinadministratoren ønsker å hindre bruk av medier med uønsket innhold.

Støttede eksterne enheter:

- Disklagring (HDD, flyttbar USB-diskett)
- CD/DVD
- USB-skriver
- FireWire-lagringsplass
- Bluetooth-enhet
- Smartkortleser
- Avbildningsenhet
- Modem
- LPT/COM-port
- Bærbar enhet
- Alle enhetstyper

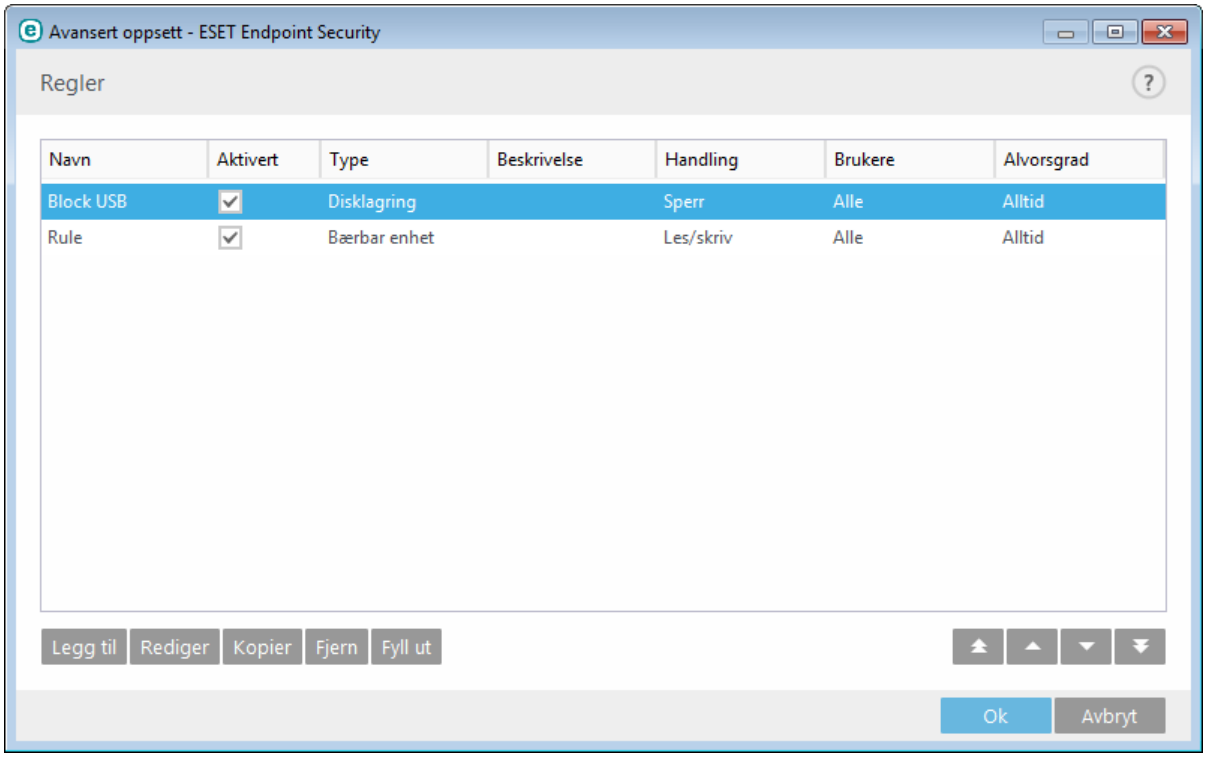
Oppsettsvalgene for enhetskontroll kan endres i **Avansert oppsett** (F5) > **Enhetskontroll**.

Når du slår på bryteren ved siden av **Integrer med system**, aktiveres enhetskontrollfunksjonen i ESET Endpoint Security. Du må starte datamaskinen på nytt for at endringen skal tre i kraft. Når enhetskontroll er aktivert, blir **Regler** aktiv. Da kan du åpne vinduet Regelredigering.

Hvis en enhet som blokkeres av en eksisterende regel settes inn, vises et varslingsvindu og du vil ikke få tilgang til enheten.

3.9.1.5.1 Regelredigering for enhetskontroll

Vinduet **Regelredigering for enhetskontroll** viser eksisterende regler og tillater nøyaktig kontroll av eksterne enheter som brukerne kobler til datamaskinen.



Bestemte enheter kan tillates eller blokkeres av en bruker, eller en av de ytterligere parameterne som kan angis i regelkonfigurasjon. Regellisten inneholder flere beskrivelser av reglene, for eksempel navn, typen ekstern enhet, handlingen som skal utføres etter at en ekstern enhet er tilkoblet datamaskinen, og logger alvorlighetsgraden.

Klikk **Legg til** eller **Rediger** for å ordne en regel. Velg den **Aktiverte** markeringsboksen ved siden av en regel for å deaktivere den til du vil bruke den i fremtiden. Velg én eller flere regler og klikk på **Fjern** for å slette regelen/reglene permanent.

Kopier – Oppretter en ny regel med forhåndsdefinerte alternativer som brukes for en annen valgt regel.

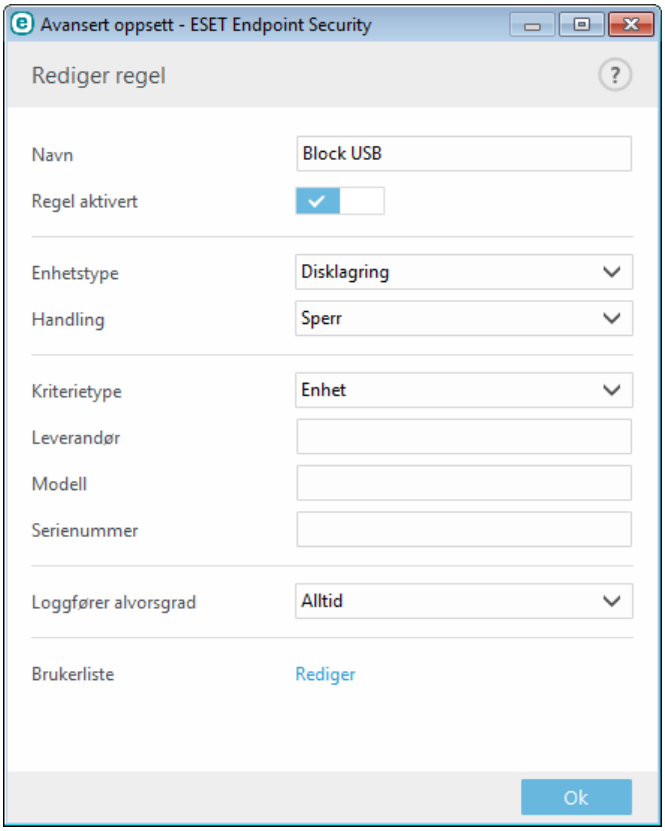
Klikk **Fyll ut** for automatisk å fylle opp eksterne medieenhetsparametere for enheter koblet til datamaskinen din.

Reglene er oppført i prioritert rekkefølge, og regler med høyere prioritet ligger øverst på listen. Regler kan flyttes ved å klikke på **Øverst/Opp/Ned/Nederst** og kan fjernes enkeltvis eller i grupper.

Loggen for enhetskontroll registrerer alle tilfeller der enhetskontroll utløses. Du kan se lagrede oppføringer fra hovedprogramvinduet til ESET Endpoint Security i **Verktøy** > **Loggfiler**.

3.9.1.5.2 Legger til enhetskontrollregler

Enhetskontrollregelen definerer handlingen som blir utført når en enhet som oppfyller regelkriteriet kobles til datamaskinen.



Angi en beskrivelse av regelen i **Navn**-feltet for bedre å kunne identifisere den. Klikk bryteren ved siden av **Regel aktivert** for å deaktivere eller aktivere denne regelen. Dette kan være nyttig hvis du ikke vil slette regelen permanent.

Enhetstype

Velg den eksterne enhetstypen fra rullegardinmenyen (Disklagring/Bærbar enhet/FireWire/...). Enhetstypene er nedarvet fra operativsystemet og kan sees i systemets Enhetsbehandling gitt at en enhet er tilkoblet datamaskinen. Lagringsenheter dekker eksterne harddisker eller konvensjonelle minnekortlesere tilkoblet via USB eller FireWire. Smartkortlesere omfatter smartkortlesere med innebygde, integrerte kretsløp, f.eks. SIM-kort eller godkjenningskort. Eksempler på bildeenheter er skannere eller fotoapparater. Fordi disse enhetene ikke gir informasjon om brukere, kun om handlingene deres, kan de kun blokkeres globalt.

Handling

Tilgang til ikke lagrende enheter kan enten tillates eller sperres. Med regler for lagringsenheter kan du imidlertid velge enn av følgende innstillinger:

- **Lesing/Skriving**– Full tilgang til enheten vil være tillatt.
- **Blokker** – Tilgang til enheten fil ikke bli gitt.
- **Skrivebeskyttet** – Bare lesetilgang fra enheten vil være tillatt.
- **Varsle** – Hver gang en enhet er koblet til, blir brukeren varslet om den er tillatt/blokkert, og en loggoppføring opprettes. Enheter blir ikke husket, en varsling vises allikevel når den samme enheten kobles til flere ganger.

Legg merke til at ikke alle handlinger (rettigheter) er tilgjengelige for alle enhetstyper. Hvis enheten har lagringsplass, er alle fire handlingene tilgjengelige. Ikke-lagrende enheter har bare to (for eksempel **Skrivebeskyttet** er ikke er tilgjengelig for Bluetooth, så Bluetooth-enheter kan bare være tillatt, sperret eller advart).

Kriterietype – Velg **Enhetsgruppe** eller **Enhet.**

Ytterligere parametere som vises nedenfor som kan brukes til å finjustere regler og tilpasse dem til enheter. Parametrene skiller ikke mellom store og små bokstaver:

- **Leverandør** – filtrering etter forhandlernavn eller -ID.
- **Modell** – det gitte navnet på enheten.
- **Serienummer** – Eksterne enheter har vanligvis deres egne serienummer. Når det gjelder CD/DVD, er dette serienummeret på det gitte medium, ikke CD-stasjon.

MERKNAD: Hvis disse parametrene er tomme, ignorerer regelen disse feltene under matchingen. Filtreringsparametere i alle tekstfelt skiller mellom små og store bokstaver og støtter ikke jokertegn (*, ?).

TIPS: For å vise informasjon om en enhet, oppretter du en regel for den typen enheter, kobler enheten til datamaskinen og kontrollerer detaljer om enheten i Logg for enhetskontroll.

Alvorsgrad

- **Alltid** – Logger alle hendelser.
- **Diagnostisering** – Logger informasjon som trengs for å finjustere programmet.
- **Informasjon** – Registrerer informative meldinger, inkludert vellykkede oppdateringsmeldinger, pluss alle registreringene ovenfor.
- **Advarsel** – Logger alle kritiske feil og varselsmeldinger.
- **Ingen** – Ingen logger registreres.

Reglene kan begrenses til visse brukere eller brukergrupper ved å legge dem til **Brukerliste**:

- **Legg til** – Åpner **Objekttyper: Brukere eller grupper**, der du kan velge ønskede brukere.
- **Fjern** – fjerner den valgte brukeren fra filteret.

MERKNAD: Alle enheter kan filtreres etter brukerregler, (for eksempel kan ikke bildeenheter gi informasjon om brukere, bare om brukte handlinger).

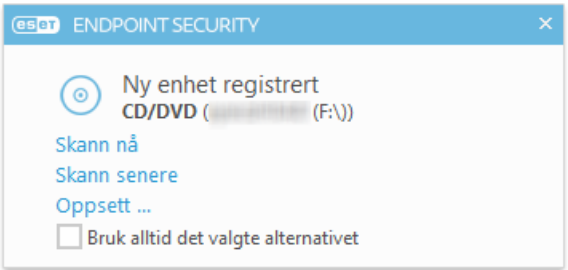
3.9.1.6 Flyttbare medier

ESET Endpoint Security tilbyr automatisk skanning av flyttbare medier (CD/DVD/USB/...). Med denne modulen kan du skanne et tilkoblet media. Dette kan være nyttig hvis datamaskinadministratoren ønsker å hindre at brukerne bruker flyttbare medier med uønsket innhold.

Handling som skal utføres etter at et flyttbart medium er satt inn – Velg standardhandlingen som skal utføres når et flyttbart medium settes inn i datamaskinen (CD/DVD/USB). Hvis det er merket av for alternativet **Vis skannealternativer** vises det en melding der du kan velge en handling:

- **Ikke skann** – Ingen handling utføres og vinduet **Ny enhet registrert** lukkes.
- **Automatisk enhetsskanning** – Det utføres en datamaskinskanning av den flyttbare medieenheten som settes inn, ved behov.
- **Vis skannealternativer** – Åpner oppsettdelen for flyttbare medier.

Når en flyttbar medieenhet settes inn, vises følgende dialog:



Skann nå – Dette utløser skanning av flyttbare medier.

Skann senere – Skanning av flyttbare medier utsettes.

Oppsett – Åpner Avansert oppsett.

Bruk alltid det valgte alternativet – Velg hvilken handling som vil utføres når en flyttbar medieenhet settes inn i datamaskinen.

Dessuten støtter ESET Endpoint Security Enhetskontroll-funksjonen, som lar deg definere regler for bruk av eksterne enheter på en gitt datamaskin. Mer informasjon om Enhetskontroll finnes i delen Enhetskontroll.

3.9.1.7 Inaktivitetsskanning

Du kan aktivere skanning i inaktiv tilstand i **Avansert oppsett** under **Antivirus** > **Inaktivitetsskanning** > **Grunnleggende**. Sett bryteren ved siden av **Aktiver Inaktivitetsskanning** til **På** for å aktivere denne funksjonen. Når datamaskinen er i inaktiv tilstand, vil en stille datamaskinskanning utføres på alle lokale stasjoner. Se Utløsere for avsløring av inaktiv tilstand for en fullstendig oversikt over forutsetninger som må oppfylles for å utløse skanning i inaktiv tilstand.

Som standard, vil skanning i inaktiv tilstand ikke kjøre når datamaskinen (notatbok) går på batteri. Denne innstillingen kan du overskrive ved å aktivere bryteren ved siden av **Kjør selv om datamaskinen går på batteri** i Avansert oppsett.

Slå på bryteren **Aktiver loggføring** i Avansert oppsett hvis du ønsker å lagre resultatet av en datamaskinskanning i delen Loggfiler (i hovedprogramvinduet klikker du på **Verktøy** > **Loggfiler** og velger **Datamaskinskanning** fra rullegardinmenyen **Logg**).

Gjenkjenning av inaktiv tilstand vil kjøre når datamaskiner i følgende tilstander:

- Skjermbeskytter
- Datamaskin låst
- Bruker logget av

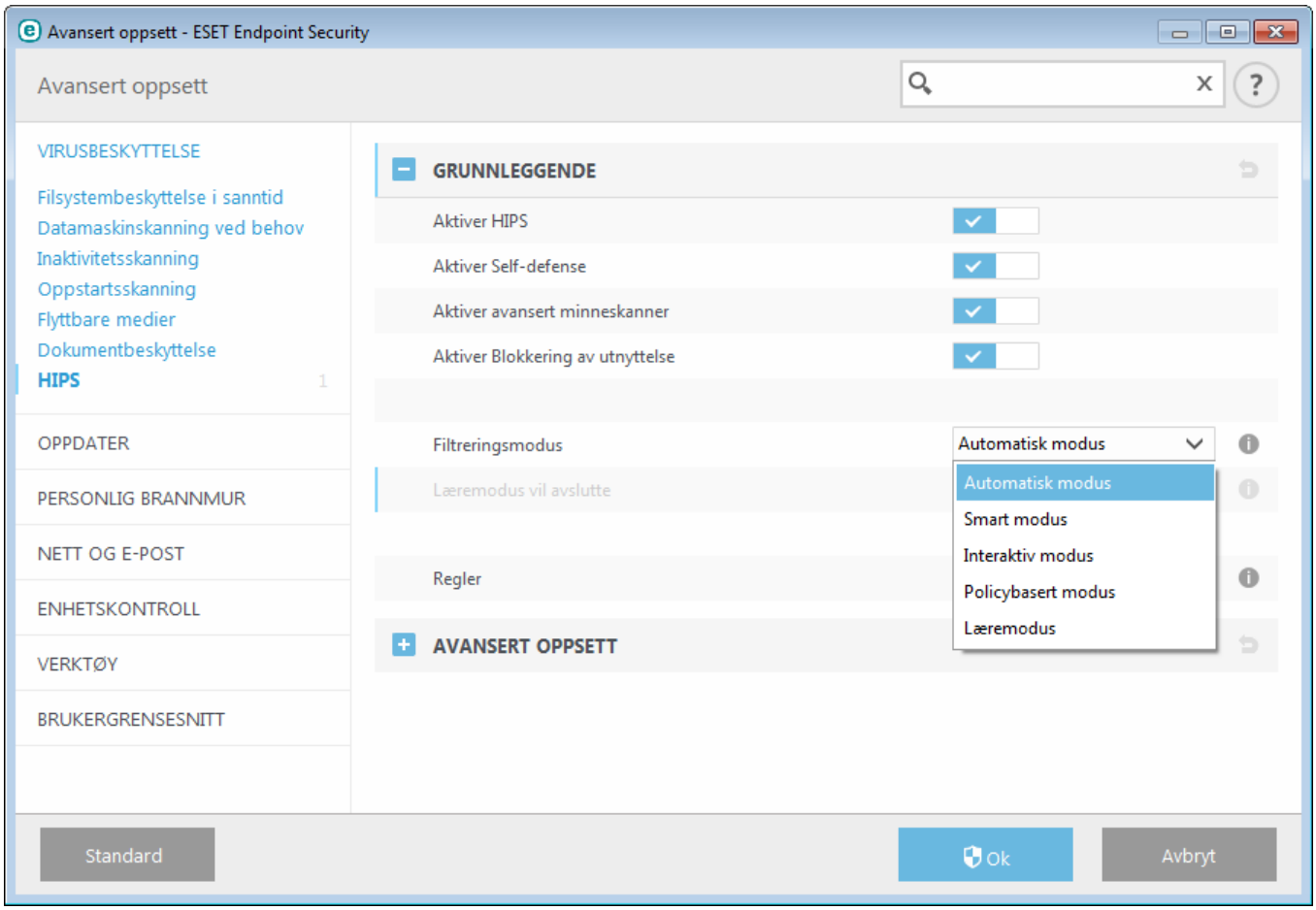
Klikk Oppsett av parametere forThreatSense-motor for å endre skanningsparametere (for eksempel gjenkjenningsmetoder) for skanning i inaktiv tilstand.

3.9.1.8 HIPS (Host-based Intrusion Prevention System)

 Endringer i HIPS-innstillinger må bare gjøres av en erfaren bruker. Feil konfigurasjon av HIPS-innstillinger kan føre til instabilt system.

Host-based Intrusion Prevention System (HIPS) beskytter systemet mot skadelig programvare og uønskede aktiviteter som prøver å skade datamaskinen. HIPS bruker avansert atferdsanalyse og gjenkjenningsmulighetene i nettverksfiltrering til å overvåke prosessene som kjøres, filer og registernøkler. HIPS er separat fra Filsystembeskyttelse i sanntid og er ikke en brannmur – den overvåker kun prosesser som kjører innen operativsystemet.

HIPS-innstillingene er å finne i **Avansert oppsett** (F5) > **Antivirus** > **HIPS** > **Grunnleggende**. HIPS-tilstanden (aktivert/deaktivert) vises i hovedvinduet til ESET Endpoint Security i **Oppsett** > **Datamaskin**.



ESET Endpoint Security har innebygd Self-defense-teknologi som hindrer skadelig programvare i å ødelegge eller deaktivere virus- og spywarebeskyttelsen, slik at du kan være sikker på at systemet ditt er beskyttet hele tiden. Du m starte Windows på nytt for å deaktivere HIPS eller Self-defense.

Avansert minneskanner jobber sammen med blokkeringen av utnyttelse til å styrke beskyttelsen mot skadelig programvare som er utviklet for å unngå å bli oppdaget av produkter mot skadelig programvare ved bruk av villedning eller kryptering. Avansert minneskanner er aktivert som standard. Du kan lese mer om denne programtypen i ordlisten.

Blokkering av utnyttelse er utviklet for å befeste typer programmer som utnyttes ofte, som for eksempel nettlesere, PDF-lesere, e-postklienter og MS Office-komponenter. Blokkeringen av utnyttelse er aktivert som standard. Du kan lese mer om denne programtypen i ordlisten.

Filtreringen kan gjøres i en av fire moduser:

Automatisk modus – Operasjoner er aktivert, unntatt forhåndsdefinerte regler som beskytter systemet.

Interaktiv modus – Brukeren vil bli bedt om å bekrefte operasjonene.

Policybasert modus – Operasjoner blokkeres.

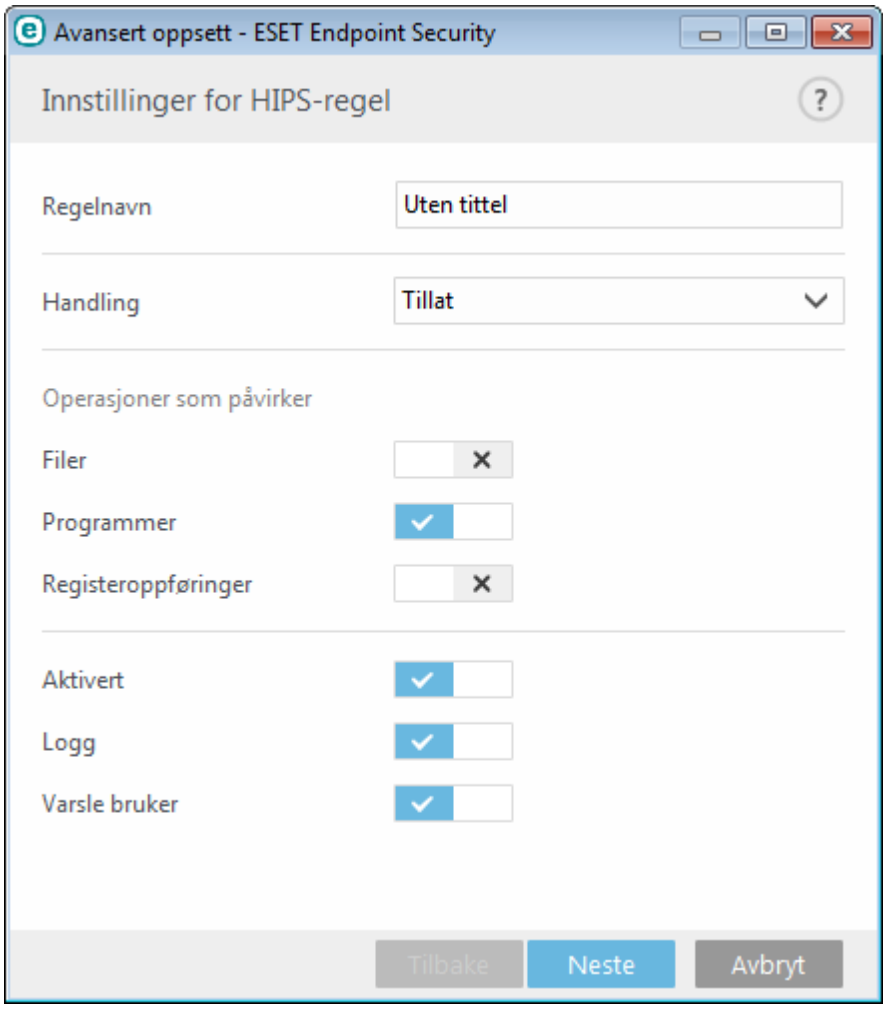
Læremodus – Operasjoner er aktivert og en regel opprettet etter hver operasjon. Regler opprettet i denne modusen kan vises i Regelredigering, men de har lavere prioritet enn regler opprettet manuelt eller regler opprettet i automatisk modus. Når du velger Læremodus fra rullgardinmenyen HIPS filtreringsmodus, blir innstillingen **Læremodus vil avsluttes** tilgjengelig. Velg varigheten du vil ha læremodus aktivert – maksimal varighet er 14 dager. Når den spesifiserte varigheten er over, blir du bedt om å redigere reglene som ble opprettet av HIPS når det var i læremodus. Du kan også velge en annen filtreringsmodus, eller utsette valget og fortsette å bruke læremodus.

Smart-modus – Bruker blir varslet kun om veldig mistenkelige hendelser.

HIPS-systemet overvåker hendelser i operativsystemet og reagerer på disse i henhold til regler som ligner på reglene som den personlige brannmuren bruker. Klikk **Rediger** for å åpne vinduet for HIPS-regelbehandling. Her kan du velge, opprette, redigere eller slette regler.

I følgende eksempel vil vi vise hvordan du kan begrense uønsket atferd for visse programmer:

1. Navngi regelen og velg **Blokker** fra rullegardinmenyen **Handling**.
2. Aktiver bryteren **Varsle bruker** for å vise en melding hver gang en regel brukes.
3. Velg minst én operasjon som regelen gjelder for. I vinduet **Kildeprogrammer**, velg **Alle programmer** fra rullgardinmenyen for å bruke den nye regelen på alle programmer som prøver å utføre en av de merkede operasjonene i programmene du har markert.
4. Velg **Endre tilstanden til et annet program**(alle operasjoner er beskrevet i produkthjelpen, som du kan se ved å trykke på F1).
5. Velg **Bestemte programmer** fra rullgardinmenyen og **Legg til** ett eller flere programmer som skal beskyttes.
6. Klikk **Fullfør** for å lagre den nye regelen.



3.9.1.8.1 Avansert oppsett

De følgende alternativene er nyttige til feilsøking og analysering av hvordan et program oppfører seg:

Drivere alltid tillatt til å laste – Valgte drivere har alltid tillatelse til å laste uavhengig av filtreringsmodusen, med mindre den er eksplisitt blokkert av brukerregelen.

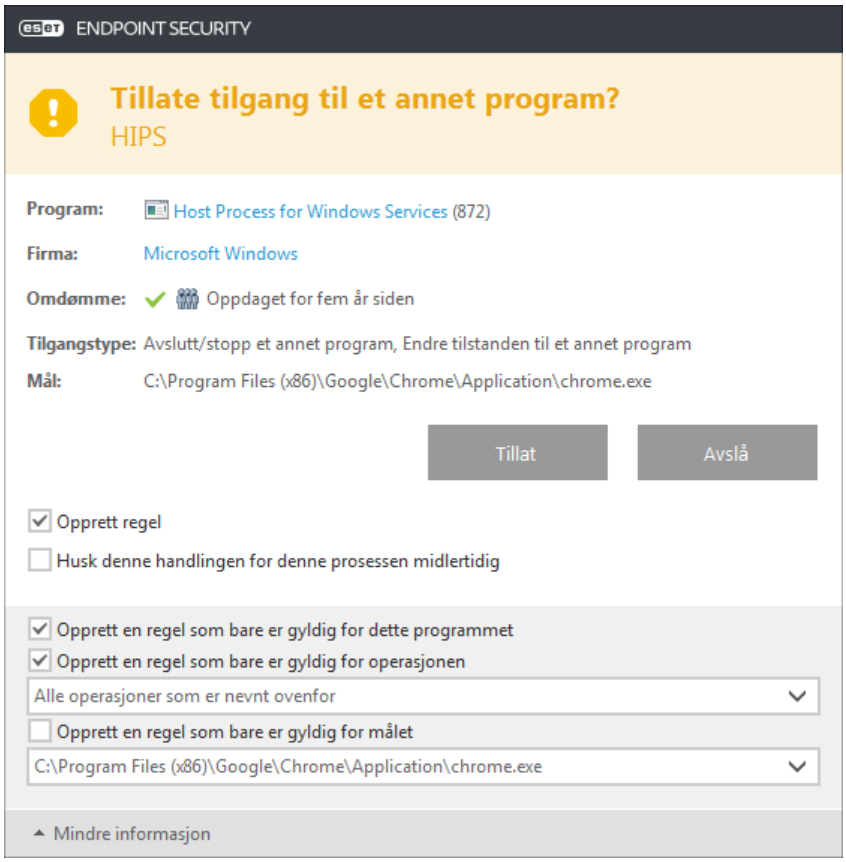
Logg alle blokkerte operasjoner– Alle blokkerte operasjoner vil bli skrevet til HIPS-loggen.

Rapporter hvis det skjer endringer i oppstartsprogrammer– Viser et skrivebordsvarsling hver gang et program blir lagt til i eller fjernet fra systemoppstart.

Du finner en oppdatert versjon av denne hjelpesiden i følgende kunnskapsbaseartikkel.

3.9.1.8.2 HIPS interaktivt vindu

Hvis standardhandlingen for en regel er satt til **Spør**, vil et dialogvindu vises hver gang regelen utløses. Du kan velge mellom å **Avvise** eller **Tillate** operasjonen. Hvis du ikke velger en handling innenfor gitt tid, velges en ny handling basert på reglene.



Dialogvinduet lar deg opprette en regel basert på eventuelle nye handlinger som HIPS oppdager og deretter definerer forholdene denne handlingen skal tillates eller blokkeres under. Du får tilgang til innstillingene for de nøyaktige parameterne ved å klikke **Mer informasjon**. Regler opprettet på denne måten betraktes som likeverdige med reglene opprettet manuelt, slik at en regel opprettet fra et dialogvindu kan være mindre spesifikk enn regelen som utløste dialogvinduet. Dette betyr at etter å ha opprettet en slik regel, kan den samme operasjonen utløse det samme vinduet.

Husk denne handlingen for denne prosessen midlertidig fører til at handlingen **Tillate/Avvise** brukes inntil reglene eller filtreringsmodusen endres, en HIPS-modul oppdateres eller systemet starter på nytt. Etter enhver av disse tre handlingene, vil midlertidige regler slettes.

3.9.1.9 Presentasjonsmodus

Presentasjonsmodus er en funksjon for brukere som krever uavbrutt bruk av programvaren, og som ikke ønsker å bli forstyrret av popup-vinduer som dukker opp og som ønsker å minimere bruken av CPU. Presentasjonsmodus kan også brukes under presentasjoner som ikke kan bli avbrutt av antivirusaktivitet. Når denne modusen er aktiver, deaktiveres alle popup-vinduer og planlagte oppgaver kjøres ikke. Systembeskyttelsen kjører fortsatt i bakgrunnen, men brukeren behøver ikke å gripe inn.

Klikk **Oppsett** > **Datamaskin** og klikk deretter på bryteren ved siden av **Presentasjonsmodus** for å aktivere presentasjonsmodus manuelt. I **Avansert oppsett** (F5), klikker du **Verktøy** > **Presentasjonsmodus**, og klikker deretter bryteren ved siden av **Aktiver presentasjonsmodus automatisk når du kjører programmer i fullskjermsmodus.** Når dette gjøres, vil ESET Endpoint Security aktivere Presentasjonsmodus automatisk når du kjører programmer i fullskjerm. Å aktivere Presentasjonsmodus er en potensiell sikkerhetsrisiko, så ikonet for beskyttelsesstatus på oppgavelinjen blir gult og viser en advarsel. Denne advarselen vises også i hovedvinduet, der du vil se **Presentasjonsmodus aktivert** i oransje.

Når du aktiverer **Aktiver Spillmodus automatisk ved kjøring av programmer i fullskjermsmodus**, aktiveres

Presentasjonsmodus når du starter et fullskjermprogram, og avsluttes automatisk når du avslutter programmet. Dette er spesielt nyttig for å aktivere Presentasjonsmodus rett etter at et spill er startet, et fullskjermprogram er åpnet eller en presentasjon er startet.

Du kan velge **Deaktiver presentasjonsmodus automatisk etter** for å definere antall minutter det vil ta før Presentasjonsmodus deaktiveres automatisk.

MERKNAD: Hvis den personlige brannmuren er i interaktiv modus og Presentasjonsmodus er aktivert, kan det hende du har problemer med å koble deg til Internett. Dette kan være problematisk hvis du starter et spill som kobler seg til Internett. Normalt sett ville du blitt bedt om å bekrefte denne handlingen (hvis ingen kommunikasjonsregler eller unntak har blitt definert), men brukerhandlinger er deaktivert i Presentasjonsmodus. Løsningen er å definere en kommunikasjonsregel for hvert program som kan være i konflikt med denne atferden, eller bruke en annen filtreringsmodus i den personlige brannmuren. Husk at hvis Presentasjonsmodus er aktivert og du går til en nettside eller et program som kan utgjøre en sikkerhetsrisiko, kan risikoen bli blokkert, men du ser ingen forklaring eller advarsel fordi brukerhandlinger er deaktivert.

3.9.1.10 Oppstartsskanning

Automatisk filkontroll ved oppstart utføres som standard ved oppstart av systemet eller ved oppdatering av virussignaturdatabasen. Skanningen er avhengig av Konfigurasjon og oppgaver i Planlegger.

Alternativene for oppstartsskanning er en del av Planlegger-oppgaven **Filkontroll ved systemstart**. Når du skal endre innstillingene for oppstartsskanning, går du til **Verktøy** > **Planlegger**, klikker på **Automatisk filkontroll ved oppstart** og klikker deretter **Rediger**. I det siste trinnet vises vinduet Automatisk filkontroll ved oppstart (se neste kapittel for mer informasjon).

Hvis du ønsker mer informasjon om opprettelse og behandling av Planlegger-oppgaver, se Lage nye oppgaver.

3.9.1.10.1 Automatisk filkontroll ved oppstart

Når du oppretter en Filkontroll ved systemstart som planlagt oppgave, har du flere alternativer for å justere de følgende parameterne:

Rullgardinmenyen **Filer som brukes av og til** angir skannedybden for filer som kjører ved systemoppstart, basert på hemmelig, sofistikert algoritme. Filer blir sortert i stigende rekkefølge i henhold til følgende kriterier:

- **Alle registrerte filer** (de fleste filene blir skannet)
- **Filer som brukes sjelden**
- **Filer som brukes av og til**
- **Ofte brukte filer**
- **Bare de mest hyppig brukte filene** (minst filer skannet)

To spesifikke grupper er også inkludert:

- **Filer som kjøres før bruker logger på** - Inneholder filer fra plasseringer som tillater tilgang til disse filene uten at brukeren er logget på (omfatter nesten alle oppstartsplasseringer, f.eks. tjenester, hjelperobjekter for nettleser, winlogon-varsling, oppføringer i Windows-planleggervinduet, kjente dll-er, osv.).
- **Filer som kjøres etter at bruker har logget på** – Inneholder filer fra plasseringer som bare tillater tilgang til disse filene etter at brukeren har logget på (omfatter filer som bare kjøres for en spesifikk bruker, vanligvis filer i *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Lister over filer som skal skannes er fast for hver tidligere nevnte gruppe.

Skanningsprioritet – Prioritetsnivået som brukes for å avgjøre når en skanning skal starte:

- **Ved inaktivitet** – oppgaven blir bare utført når systemet er inaktivt,
- **Lavest** – når systembelastningen er så lav som mulig,
- **Lavere** – ved lav systembelastning,
- **Normal** – ved gjennomsnittlig systembelastning.

3.9.1.11 Dokumentbeskyttelse

Dokumentbeskyttelsen skanner Microsoft Office-dokumenter før de åpnes, samt filer som lastes ned automatisk fra Internet Explorer, f.eks. Microsoft ActiveX-elementer. Dokumentbeskyttelse gir et lag med beskyttelse i tillegg til Sanntidsbeskyttelse av filsystemet og kan deaktiveres for å forbedre ytelsen til systemer som ikke eksponeres for et høyt volum Microsoft Office-dokumenter.

Systemintegrering aktiverer beskyttelsessystemet. Dette alternativet kan endre ved å trykke F5 for å åpne vinduet Avansert oppsett og klikke **Antivirus** > **Dokumentbeskyttelse** i treet for avansert oppsett.

Funksjonen aktiveres av programmer som bruker Microsoft Antivirus API (f.eks. Microsoft Office 2000 eller nyere eller Microsoft Internet Explorer 5.0 eller nyere).

3.9.1.12 Utelatelser

Det er mulig å utelate filer og mapper fra skanning. For å sikre at alle objekter skannes for trusler, anbefaler vi at du kun oppretter unntak hvis det er absolutt nødvendig. Tilfeller der du vil kunne ha behov for å ekskludere et objekt kan inkludere skanning av store databaseoppføringer som vil gjøre datamaskinen treg ved skanning, eller programvare som er i konflikt med skanningen (for eksempel, sikkerhetskopieringsprogrammer).

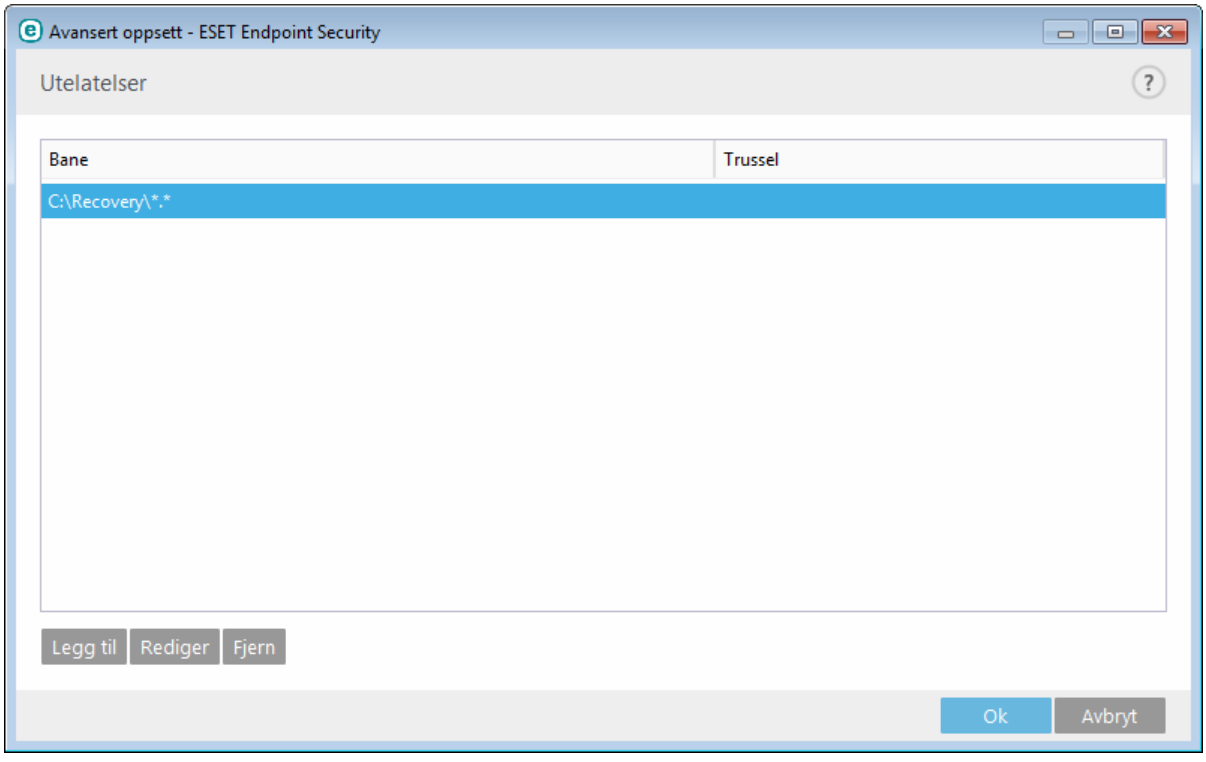
Utelukke et objekt fra skanning:

1. Klikk **Legg til**,
2. Skriv inn banen til et objekt, eller velg den fra trestrukturen.

Du kan bruke jokertegn for å legge til en gruppe med filer. Et spørsmålstegn (?) står for ett enkelt variabelt tegn, mens en stjerne (*) står for en variabel streng bestående av null eller flere tegn.

Eksempler

- Hvis du vil utelate alle filene i en mappe, skriver du banen til mappen og bruker masken "*.*".
- Hvis du vil utelate en hel stasjon, inkludert alle filer og undermapper, bruker du masken "D:*".
- Hvis du kun vil utelate doc-filer, bruker du masken "*.doc".
- Hvis navnet på en eksekverbar fil har et bestemt antall tegn (og tegnene varierer) og du bare er helt sikker på det første tegnet (for eksempel "D"), bruker du følgende format: "D????.exe". Spørsmålstegn erstatter de manglende (ukjente) tegnene.



MERKNAD: En trussel i en fil vil ikke oppdages av modulene for filsystembeskyttelse i sanntid og

datamaskinskanning hvis filen oppfyller kriteriene for ekskludering fra skanning.

Kolonner

Bane - Banen til utelatte filer og mapper.

Trussel – Hvis navnet på en trussel står ved siden av en ekskludert fil, betyr det at filen bare er ekskludert for den bestemte trusselen. Hvis filen på et senere tidspunkt blir infisert med annen skadelig programvare, vil dette bli gjenkjent av antivirusmodulen. Denne typen utelatelse kan bare brukes for bestemte typer infiltrasjoner og opprettes enten i trusselvarselsvinduet hvor det rapporteres om infiltrasjonen (klikk **Vis avanserte alternativer** og velg deretter **Ekskluder fra gjenkjenning**), eller **Verktøy** > **Karantene** ved å høyreklikke på filen i karantene og deretter velge **Gjenopprett og utelat fra gjenkjenning** fra hurtigmenyen.

Kontrollelementer

Legg til – Utelukker objekter fra gjenkjenning.

Rediger – Lar deg redigere valgte oppføringer.

Fjern – Fjerner valgte oppføringer.

3.9.1.13 Oppsett av parametere for ThreatSense-motor

ThreatSense er en teknologi som omfatter mange sammensatte metoder for gjenkjenning av trusler. Denne teknologien er proaktiv, noe som betyr at den gir beskyttelse også ved tidlig spredning av en ny trussel. Den benytter en kombinasjon av flere metoder (kodeanalyse, kodeemulering, generiske signaturer, virussignaturer) som jobber sammen slik at systemsikkerheten får en betydelig forbedring. Skannemotoren er i stand til å kontrollere flere datastrømmer samtidig, noe som øker effektiviteten og gjenkjenningsmengden. ThreatSense-teknologien eliminerer også rootkit på en vellykket måte.

Med oppsettalternativene for ThreatSense-teknologien kan du angi flere skanneparametere:

- Filtyper og filendelser som skal skannes
- Kombinasjoner av ulike gjenkjenningsmetoder
- Rensingsnivåer osv.

Du kommer inn i oppsettvinduet ved å klikke **ThreatSense Oppsett av motorparametere** i vinduet Avansert oppsett for alle moduler som benytter ThreatSense-teknologi (se nedenfor). Det kan være nødvendig med ulike konfigurasjoner for ulike sikkerhetsscenarier. Med tanke på dette kan ThreatSense konfigureres individuelt for følgende beskyttelsesmoduler:

- Filsystembeskyttelse i sanntid,
- Inaktivitetsskanning,
- Oppstartsskanning,
- Dokumentbeskyttelse,
- Beskyttelse for e-postklient,
- Beskyttelse for nettilgang
- Datamaskinskanning.

ThreatSense-parameterne er sterkt optimalisert for hver modul, og hvis de endres, kan dette påvirke systemdriften betydelig. Hvis du for eksempel endrer parametere slik at kjøretidspakker alltid skal skannes, eller aktiverer avansert heuristikk i modulen for filsystembeskyttelse i sanntid, kan det føre til et langsommere system (normalt blir bare nyopprettede filer skannet ved hjelp av disse metodene). Vi anbefaler at du lar standardparameterne for ThreatSense forbli uendret for alle modulene bortsett fra Datamaskinskanning.

Objekter som skal skannes

I denne delen kan du definere hvilke datamaskinkomponenter og filer som skal skannes for infiltreringer.

Minne – Skanner etter trusler som angriper minnet på datamaskinen.

Oppstartssektorer – Skanner oppstartssektorer etter virus i MBR-oppføringen (Master Boot Record).

E-postfiler – Programmet støtter følgende filtyper: DBX (Outlook Express) og EML.

Arkiver – Programmet støtter følgende filtyper: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE og mange andre.

Selvutpakkende arkiver – Selvutpakkende arkiver (SFX) er arkiver som ikke trenger spesielle programmer for å dekomprimeres.

Kjøretidspakker – Etter kjøring dekomprimeres kjøretidspakkerne i minnet (til forskjell fra standard arkivtyper). I tillegg til standard statiske pakkere (UPX, yoda, ASPack, FSG, osv.) støtter skanneren mange flere typer pakkere takket være kodeemulering.

Skannealternativer

Velg metodene som skal brukes når systemet skannes etter infiltreringer. Følgende alternativer er tilgjengelige:

Heuristikk – Heuristikk er en algoritme som analyserer (skadelig) aktivitet fra programmer. Hovedfordelen ved denne teknologien er evnen til å identifisere skadelig programvare som ikke eksisterte eller var kjent for den siste virussignaturdatabasen. Ulempen er en (svært liten) mulighet for falsk alarm.

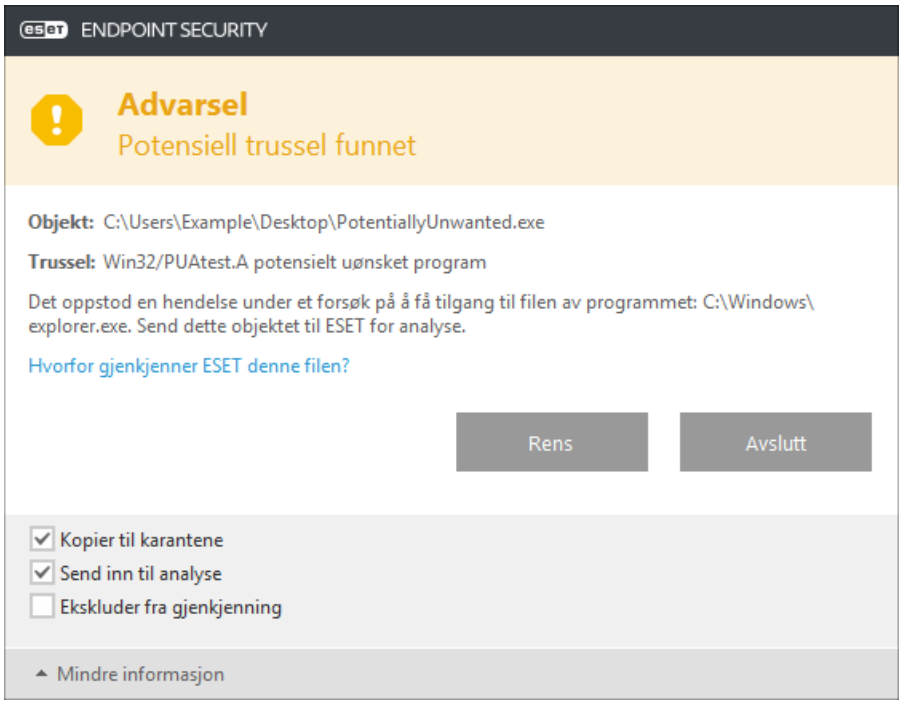
Avansert heuristikk/DNA/Smarte signaturer – Avansert heuristikk består av en unik heuristisk algoritme utviklet av ESET, optimalisert for å gjenkjenne ormer og trojanske hester, og er skrevet i høynivå-programmeringsspråk. Bruk av avansert heuristikk øker ESET-produktenes evne til å gjenkjenne trusler betraktelig. Signaturer kan gjenkjenne og identifisere virus pålitelig. Ved hjelp av det automatiske oppdateringssystemet er nye signaturer tilgjengelige i løpet av få timer etter at en trussel er oppdaget. Ulempen med signaturer er at de bare gjenkjenner virus de kjenner fra før (eller litt endrede versjoner av disse virusene).

Et potensielt uønsket program er et program som inneholder adware, installerer verktøylinjer, sporer søkeresultater, eller har andre uklare mål. Det er noen situasjoner hvor du kan føle at fordelene med det uønskede programmet oppveier risikoene. Av denne grunnen tildeler ESET slike programmer en lavere risikokategori sammenlignet med andre typer skadelig programvare, slik som trojanske hester og ormer.

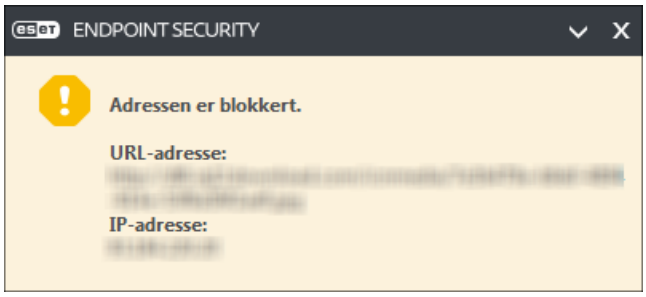
Advarsel – Potensiell trussel funnet

Når et potensielt uønsket program oppdages, vil du kunne velge hvilke handlinger du til utføre:

1. **Rengjøre/Koble fra**: Dette alternativet avslutter handlingen og forhindrer at mulige trusler kommer inn i systemet.
2. **Ingen handling**: Dette alternativet tillater at mulige trusler kommer inn i systemet.
3. For å la programmet kjøre på datamaskinen din i fremtiden uten avbrudd, klikker du på **Mer informasjon/Vis avanserte alternativer** og velg avkrysningsboksen ved siden av **Ekskluder fra gjenkjenning**.



Når et potensielt uønsket program gjenkjennes og det ikke kan rengjøres, vises det et meldingsvindu **Adresse har blitt blokkert** i meldingsområdet nederst til høyre på skjermen. For mer informasjon om denne hendelsen, se **Verktøy** > **Loggfiler** > **Filtrerte nettsteder** på hovedmenyen.



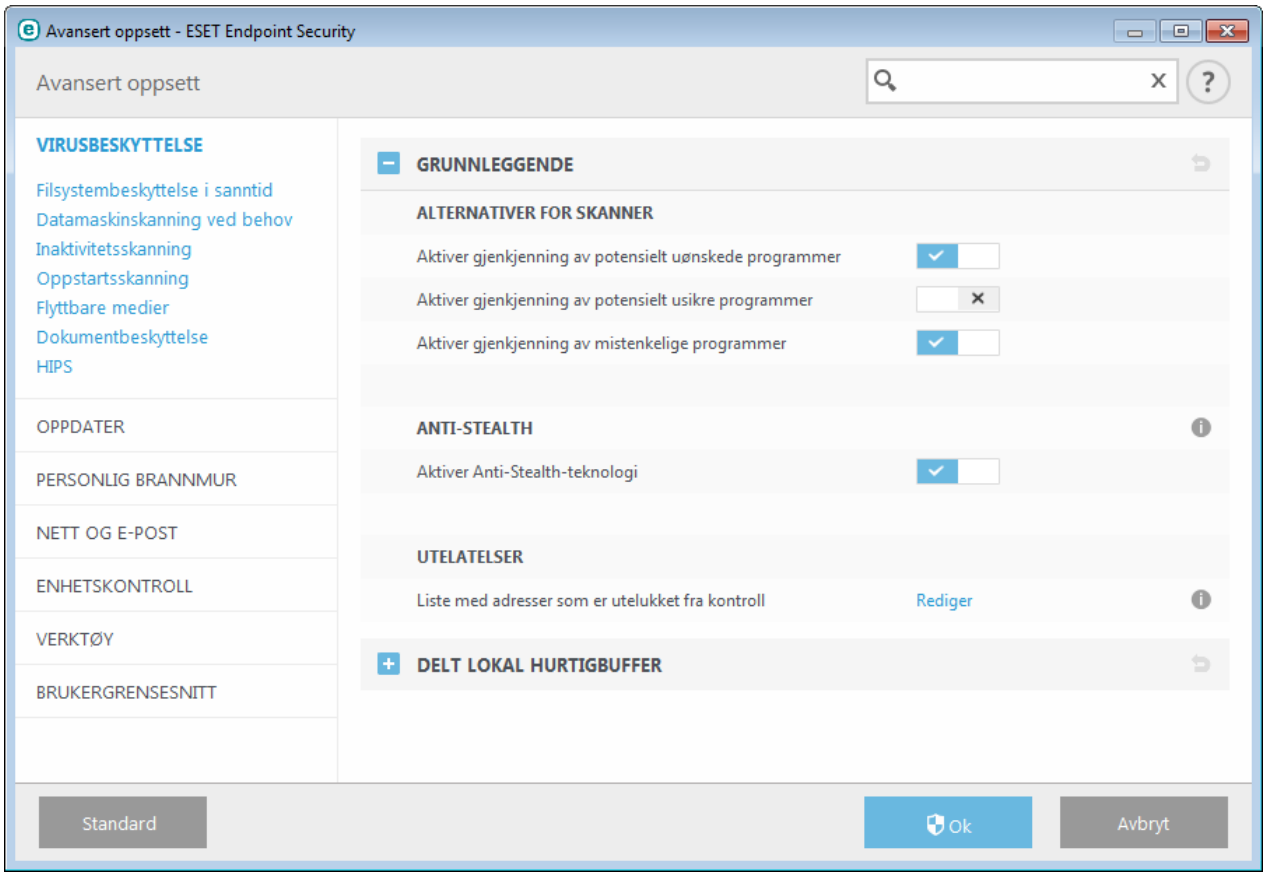
Potensielt uønskede programmer – Innstillinger

Når du installerer ESET-produktet ditt, kan du velge om du vil aktivere gjenkjenning av potensielt uønskede programmer, som vist nedenfor:

Potensielt uønskede programmer kan installere adware, verktøyslinjer eller inneholde andre uønskede og usikre programfunksjoner.

Disse innstillingene kan endres i programinnstillinger til enhver tid. For å aktivere eller deaktivere gjenkjennelse av potensielt uønskede, usikre eller mistenkelige programmer, følg disse instruksene:

1. Åpne ditt ESET-produkt. Hvordan åpner jeg ESET-produktet?
2. Trykk på **F5** for å gå inn på **Avansert oppsett**.
3. Klikk **Virusbeskyttelse** og aktiver eller deaktiver alternativene **Aktiver gjenkjenning av potensielt uønskede programmer**, **Aktiver gjenkjenning av potensielt usikre programmer** og **Aktiver gjenkjenning av mistenkelige programmer** alt ettersom du vil. Bekreft ved å klikke **OK**.



Potensielt uønskede programmer – Programvarepakkere

En programvarepakker er en spesiell type programmodifikasjon som brukes av noen nettsteder som tilbyr filhosting. Dette er et tredjeparts verktøy som installerer programmet du ønsket å laste ned, men legger til ekstra programvare, slik som verktøyslinjer eller reklameprogrammer. Den ekstra programvaren kan også gjøre endringer på nettleserens hjemmeside og søkeinnstillinger. Nettsteder for filhosting varsler ofte ikke programvareleverandøren eller nedlastingsmottakeren at endringer har blitt utført, og tillater ikke enkle måter å velge bort modifikasjoner på. Av slike grunner, klassifiserer ESET programvarepakkere som en type potensielt uønsket program som lar brukere godta nedlastingen eller ikke.

Du finner en oppdatert versjon av denne hjelpesiden i denne ESET-kunnskapsbaseartikkelen.

Potensielt usikre programmer – Potensielt usikre programmer er en klassifisering som brukes om kommersiell, lovlig programvare. Eksempler på dette inkluderer verktøy for ekstern tilgang, programmer for å knekke passord samt keyloggere (programmer som registrerer alle tastetrykk som foretas av en bruker). Dette alternativet er deaktivert som standard.

Rensing

Renseinnstillingene angir skannerens virkemåte når infiserte filer renses. Det finnes tre rensenivåer:

Ingen rensing – Infiserte filer blir ikke renset automatisk. Programmet viser et varselvindu og lar brukeren velge en handling. Dette nivået er utformet for mer avanserte brukere som vet hvilke trinn de skal utføre i tilfelle en infiltrasjon.

Vanlig rensing – Programmet vil prøve å rense eller slette en infisert fil automatisk basert på en forhåndsdefinert handling (avhengig av typen infiltrering). Gjenkjennelse og sletting av en infisert fil blir varslet med en melding nede i høyre hjørne på skjermen.. Hvis det ikke er mulig å velge riktig handling automatisk, gir programmet andre handlingsmuligheter. Det samme skjer hvis en forhåndsdefinert handling ikke kan fullføres.

Grundig rensing – Programmet vil rense eller slette alle infiserte filer. Det eneste unntaket er systemfilene. Hvis det ikke er mulig å rense dem, blir brukeren bedt om å velge en handling i et varselvindu.

Advarsel: Hvis et arkiv inneholder én eller flere infiserte filer, har du to alternativer for å behandle arkivet. I standardmodus (Standardrensing) blir hele arkivet slettet hvis alle filene i arkivet er infiserte filer. I modusen

Grundig rensing blir arkivet slettet hvis det inneholder minst én infisert fil, uavhengig av statusen til de andre filene i arkivet.

Utelatelser

En filtype er delen av filnavnet som er skilt ut med et punktum. Filtypen definerer type fil og innholdet i den. I denne delen av oppsettet for ThreatSense-parametere kan du definere hvilke filtyper som skal skannes.

Annet

Ved konfigurering av parametere for ThreatSense-motor for en datamaskinskanning, er følgende alternativer også tilgjengelige i **Annet**-delen:

Skann alternative dataflyter (ADS) – Alternative dataflyter, som brukes av NTFS-filsystemet, er fil- og mappetilknytninger som er usynlige for vanlige skanneteknikker. Mange infiltreringer prøver å unngå å bli oppdaget ved å skjule seg som alternative dataflyter.

Kjør bakgrunnsskanning med lav prioritet – Hver skannesekvens forbruker en viss mengde systemressurser. Hvis du arbeider med programmer som bruker mye systemressurser, kan du aktivere bakgrunnsskanning med lav prioritet og spare ressursene til programmene.

Logg alle objekter – Hvis dette alternativet er valgt, viser loggfilen alle skannede filer, også filer som ikke er infisert. Hvis det for eksempel finnes en infiltrering i et arkiv, vil loggen også angi rene filer i det arkivet.

Aktiver smart optimalisering – Når smart optimalisering er aktivert, brukes de mest optimale innstillingene for å sikre det mest effektive skannenivået, samtidig som den høyeste skannehastigheten opprettholdes. De ulike beskyttelsesmodulene skanner på en intelligent måte, og tar i bruk ulike skannemetoder og benytter dem på spesifikke filtyper. Hvis smart optimalisering deaktiveres, benyttes bare de brukerdefinerte innstillingene i ThreatSense-kjernen for de bestemte modulene når skanningen utføres.

Bevar tidsmerket for forrige tilgang – Velg dette alternativet for å beholde det opprinnelige tidspunktet for tilgang til skannede filer i stedet for å oppdatere dem (f.eks. til bruk med sikkerhetskopieringssystemer).

Grenser

I delen Grenser kan du angi maksimal størrelse for objekter og arkivdybdenivåer som skal skannes:

Objektinnstillinger

Maksimal objektstørrelse – Definerer den maksimale størrelsen til objekter som skal skannes. Den aktuelle antivirusmodulen skanner da bare objekter som er mindre enn størrelsen som er oppgitt. Dette alternativet bør bare endres av avanserte brukere som har en bestemt grunn til å utelukke større objekter fra skanningen. Standardverdi: *ubegrenset*.

Maksimal skannetid for objekt (sek.) – Definerer maksimaltiden som settes av til skanning av et objekt. Hvis det er oppgitt en brukerdefinert verdi her, stopper antivirusmodulen skanningen av objektet etter at tiden er ute, uavhengig av om skanningen er fullført eller ikke. Standardverdi: *ubegrenset*.

Oppsett for skanning av arkiv

Arkivdybdenivå – Angir maksimal dybde for skanning av arkiver. Standardverdi: *10*.

Maksimal filstørrelse i arkiv – Velg dette alternativet for å angi den maksimale filstørrelsen (utpakket størrelse) for filer i arkiv som skal skannes. Standardverdi: *ubegrenset*.

MERKNAD: Det anbefales ikke at standardverdiene endres. Dette er under normale omstendigheter ikke nødvendig.

3.9.1.13.1 Utelatelser

En filtype er delen av filnavnet som er skilt ut med et punktum. Filtypen definerer type fil og innholdet i den. I denne delen av oppsettet for ThreatSense-parametere kan du definere hvilke filtyper som skal skannes.

Standardinnstillingen er at all filer skannes. Alle filtyper kan legges til i listen over filer som skal utelates fra skanning.

Det kan noen ganger være nødvendig å utelate filer hvis programmet som bruker filtypen, ikke fungerer som det skal dersom visse filtyper skannes. Det kan for eksempel være tilrådelig å utelate endelsene .edb, .eml og .tmp ved bruk av Microsoft Exchange-servere.

Med bruk av knappene **Legg til** og **Fjern**, kan du aktivere eller deaktivere skanning av spesifikke filtyper. Når du skal legge en ny filtype til listen, klikker du **Legg til**, skriver inn utvidelsen i det tomme feltet og klikker **OK**. Når du velger **Angi flere detaljer**, kan du legge til flere filtyper som må skilles med linjer, kommaer eller semikoloner. Når flervalg er aktiver, vises filtyper i listen. Velg en filtype i listen, og klikk deretter **Fjern** for å slette filtypen fra listen. Hvis du vil redigere en valgt filtype, klikker du **Rediger**.

Spesialsymbolene * (stjerne) og ? (spørsmålstegn) kan brukes. Stjernen står for et tegnstreng, og spørsmålstegnet står for et symbol.

MERKNAD: For å se den eksakte filendelsen (hvis det finnes) til en fil i et Windows-operativsystem, må du oppheve markeringen av alternativet **Skjul endelser for kjente filtyper** i **Kontrollpanel** > **Mappealternativer** > **Vis** (fane) og anvende denne endringen.

3.9.2 Nettverk

Den personlige brannmuren kontrollerer all nettverkstrafikk til og fra systemet. Dette skjer ved å tillate eller avslå individuelle nettverkstilkoblinger basert på filtreringsreglene dine. Det gir beskyttelse mot angrep fra eksterne datamaskiner og blokkerer potensielt farlige tjenester. Den personlige brannmuren gir også IDS/IPS-funksjonalitet ved å inspisere innholdet i tillatt nettverkstrafikk og blokkere trafikk som anses å være potensielt farlig.

Konfigurasjonen av **Personlig brannmur** er å finne i **Oppsett**-ruten under **Nettverk**. Der kan du justere filtreringsmodus for ESET personlig brannmur. Du kan også få tilgang til mer detaljerte innstillinger ved å klikke tannhjulet > **Konfigurer** ved siden av **Personlig brannmur**, eller ved å trykke på **F5** for å gå inn på Avansert oppsett.

Beskyttelse mot nettverksangrep (IDS) – Analyserer innholdet i nettverkstrafikk som ikke snappes opp av brannmurreglene. All trafikk som anses som skadelig vil bli blokkert og trusselen vil bli nøytralisert. Du kan deaktivere beskyttelse mot nettverksangrep i en spesifikk tidsperiode ved å klikke på .

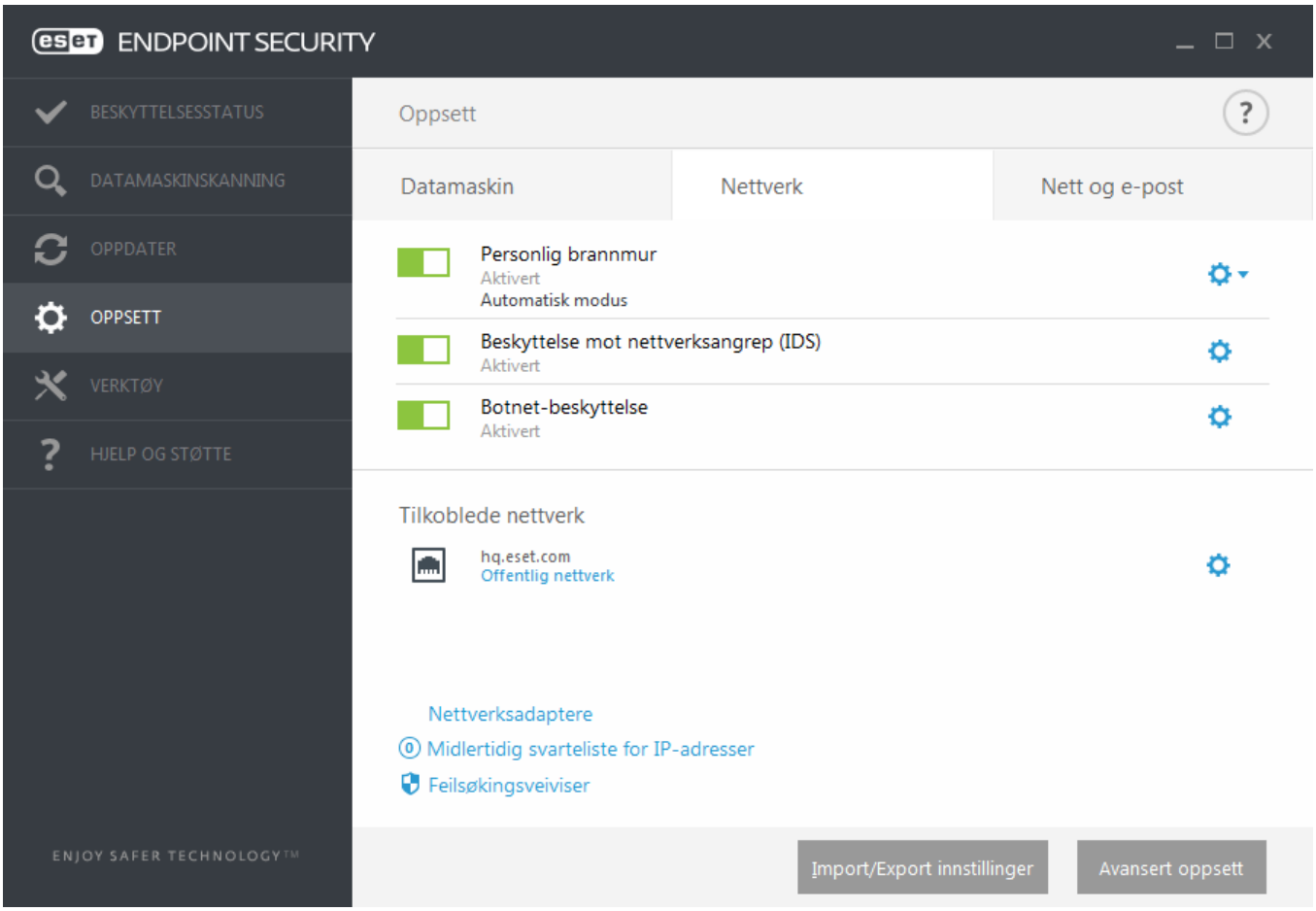
Botnet-beskyttelse – finner skadelig programvare raskt og nøyaktig på systemet. Du kan deaktivere botnet-beskyttelse i en spesifikk tidsperiode ved å klikke på .

Tilkoblede nettverker – Viser nettverker som nettverksadaptere er koblet til. Når du klikker på tannhjulet, blir du bedt om å velge en beskyttelsestype for nettverket du er koblet til via nettverksadapteren.

Nettverksadaptere – Her kan du se hver nettverksadapter og den tilordnede brannmurprofilen og klarerte sonen. Se Nettverksadaptere for mer detaljert informasjon.

Midlertidig svartelistede IP-adresser – Se en liste over IP-adresser som er avslørt som kilden til angrep og som føyes til svartelisten for å hindre tilkoblinger i en bestemt periode. Klikk dette alternativet og deretter F1 hvis du ønsker mer informasjon.

Feilsøkingsveiviser – Hjelper deg å løse tilkoblingsproblemer forårsaket av ESET personlig brannmur. Se Feilsøkingsveiviser for mer detaljert informasjon.



Klikk tannhjulet ⚙ ved siden av **Personlig brannmur** for å få tilgang til følgende innstillinger:

Konfigurer ... – Åpner vinduet Personlig brannmur i Avansert oppsett, der du kan definere hvordan brannmuren skal håndtere nettverkskommunikasjon.

Blokker all trafikk – All inngående og utgående kommunikasjon blir blokkert av den personlige brannmuren. Bruk dette alternativet bare hvis du har mistanke om en kritisk sikkerhetsrisiko som krever at du kobler systemet fra nettverket. Mens Filtrering av nettverkstrafikk er i modusen **Blokker all trafikk**, klikker du **Stopp blokkering av all trafikk** for å gjenopprette brannmuren til normal drift.

Sett brannmuren på pause (tillat all trafikk) – Det motsatte av blokkering av all nettverkstrafikk. Hvis du velger dette alternativet, blir alle filtreringsalternativene til den personlige brannmuren slått av, og alle innkommende og utgående tilkoblinger tillates. Mens Filtrering av nettverkstrafikk er i denne modusen, klikk på **Aktiver brannmur** for å aktivere brannmuren på nytt.

Automatisk modus – (når en annen filtreringsmodus er aktivert) – Klikk for å endre filtreringsmodusen til automatisk filtreringsmodus (med brukerdefinerte regler).

Interaktiv modus – (når en annen filtreringsmodus er aktivert) – Klikk for å endre filtreringsmodusen til interaktiv filtreringsmodus.

3.9.2.1 Personlig brannmur

Den personlige brannmuren kontrollerer all nettverkstrafikk til og fra systemet. Dette skjer ved å tillate eller avslå individuelle nettverkstilkoblinger basert på spesifiserte filtreringsregler. Det gir beskyttelse mot angrep fra eksterne datamaskiner og aktiverer blokkering av enkelte tjenester. Det gir også virusbeskyttelse for HTTP-, POP3- og IMAP-protokollen. Denne funksjonaliteten utgjør en svært viktig faktor innenfor datamaskinsikkerhet.

Aktiver Beskyttelse mot nettverksangrep (IDS) – Analyserer innholdet i nettverkstrafikk som ikke snappes opp av brannmurreglene. All trafikk som anses som skadelig vil bli blokkert og trusselen vil bli nøytralisert.

Aktiver Botnet-beskyttelse – Oppdager og blokkerer kommunikasjonen med ondsinnede kommando- og kontrollservere basert på typiske mønstre når datamaskinen er infisert og en bot forsøker å kommunisere.

Fire filtreringsmoduser er tilgjengelige for ESET Endpoint Security personlig brannmur. Filtreringsmodusinnstillingene er å finne i **Avansert oppsett** (F5) ved å klikke **Personlig brannmur**. Funksjonen til brannmuren endrer seg avhengig av filtreringsmodusen. Filtreringsmodiene påvirker også hvor mye brukeren må gjøre.

Filtreringen kan gjøres i en av fire moduser:

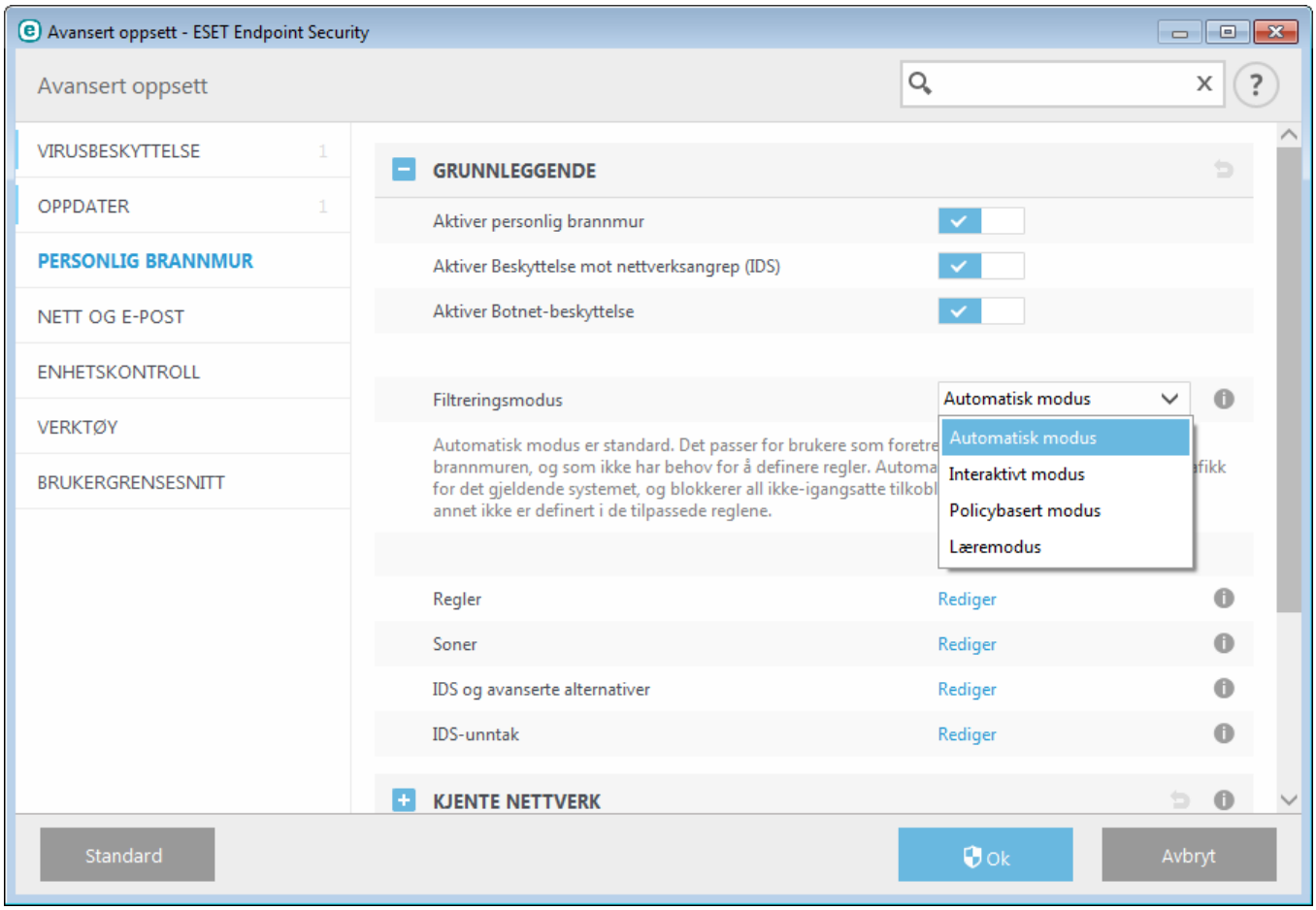
Automatisk modus – Standardmodusen. Denne modusen egner seg for brukere som foretrekker enkel og praktisk bruk av brannmuren uten å måtte definere regler. Tilpassede, brukerdefinerte regler kan opprettes, men dette kreves ikke i automatisk modus. Automatisk modus tillater all utgående trafikk for det gjeldende systemet, og blokkerer det meste av innkommende trafikk (unntatt visse typer trafikk fra klarert sone, som er tillatt i seksjonen IDS og avansert alternativ/Tillatte tjenester og innkommende trafikk som svarer på nylig utgående trafikk fra den samme eksterne siden).

Interaktiv modus – Gjør det mulig å lage en tilpasset konfigurasjon for den personlige brannmuren. Når kommunikasjon oppdages og ingen eksisterende regler gjelder for den, vises en dialogboks med melding om en ukjent forbindelse. I dialogvinduet kan du velge om du vil tillate eller avslå kommunikasjonen, og beslutningen kan lagres som en ny regel for den personlige brannmuren. Hvis du velger å opprette en ny regel, vil alle senere tilkoblinger av denne typen bli tillatt eller avslått i henhold til den regelen.

Policybasert modus – Blokkerer alle tilkoblinger hvis det ikke finnes en bestemt regel som tillater dem. Med denne modusen kan avanserte brukere definere regler som bare tillater ønskede og sikre tilkoblinger. Alle andre uspesifiserte tilkoblinger blokkeres av den personlige brannmuren.

Læremodus – Oppretter og lagrer regler automatisk og egner seg som innledende konfigurasjon for den personlige brannmuren. Det kreves ingen brukerhandling siden ESET Endpoint Security lagrer reglene i henhold til forhåndsdefinerte parametere. Læremodus er ikke sikker, og bør bare brukes fram til alle de nødvendige reglene for kommunikasjon er opprettet.

Profiler kan brukes til å tilpasse atferden til ESET Endpoint Security personlig brannmur ved å spesifisere ulike sett med regler i like situasjoner.



Regler – Her kan du legge til regler og definere hvordan den personlige brannmuren håndterer nettverkstrafikk.

Soner – Her kan du opprette soner som består av flere IP-adresser.

IDS og avanserte alternativer – Lar deg konfigurere avanserte filtreringsalternativer og IDS-funksjonaliteten (brukes til å oppdage flere typer angrep og utnyttelser).

IDS-unntak – Lar deg legge til IDS-unntak og tilpasse reaksjoner på ondsinnede aktiviteter.

3.9.2.1.1 Læremodus

Læremodus oppretter og lagrer automatisk en regel for hver kommunikasjon som opprettes i systemet. Det kreves ingen brukerhandling siden ESET Endpoint Security lagrer reglene i henhold til forhåndsdefinerte parametere.

Denne modusen kan utsette systemet for risiko, og bør kun brukes i forbindelse med innledende konfigurasjon av den personlige brannmuren.

Læremodus aktiveres ved å bruke alternativene for læremodus under **Avansert oppsett** (F5) > **Personlig brannmur** > **Innstillinger for læremodus**. Denne delen inneholder følgende elementer:

Advarsel: Den personlige brannmuren filtrerer ikke kommunikasjon i læremodus. All ut- og inngående kommunikasjon tillates. Datamaskinen er ikke fullstendig beskyttet av den personlige brannmuren i denne modusen.

Kommunikasjonstype – Velg individuelle prinsipper for opprettelse av regler for hver enkelt kommunikasjonstype. Det er fire typer kommunikasjon:

- **Innkommende trafikk fra klarert sone** – Et eksempel på en innkommende tilkobling innenfor den klarerte sonen kan være en ekstern datamaskin fra innenfor den klarerte sonen som prøver å opprette kommunikasjon med et lokalt program som kjører på datamaskinen din.

- **Utgående trafikk til klarert sone** – Et lokalt program som prøver å etablere en tilkobling med en annen datamaskin i det lokale nettverket eller innenfor et nettverk i den klarerte sonen.

- **Innkommende Internett-trafikk** – En ekstern datamaskin som prøver å kommunisere med et program som kjøres på datamaskinen.

- **Utgående Internett-trafikk** – Et lokalt program prøver å etablere en forbindelse med en annen datamaskin.

I hver del kan du definere parametere som skal legges til nyopprettede regler:

Legg til lokal port – Inneholder det lokale portnummeret for nettverkskommunikasjonen. Ved utgående kommunikasjon genereres som regel tilfeldige numre. Det anbefales derfor at dette alternativet kun aktiveres for innkommende kommunikasjon.

Legg til program – Inneholder navnet på det lokale programmet. Dette alternativet egner seg for fremtidige regler på programnivå (regler som definerer kommunikasjonen for et helt program). Du kan for eksempel aktivere kommunikasjon for bare én nettleser eller én e-postklient.

Legg til ekstern port – Inneholder det eksterne portnummeret for nettverkskommunikasjonen. Du kan for eksempel tillate eller avslå en bestemt tjeneste knyttet til et bestemt portnummer (HTTP – 80, POP3 - 110 osv.).

Legg til ekstern IP-adresse / Klarert sone – Du kan bruke en ekstern IP-adresse eller sone som parameter for nye regler som definerer alle nettverkstilkoblingene mellom det lokale systemet og den eksterne adressen/sonen. Dette er et godt alternativ hvis du vil definere handlinger for en bestemt datamaskin eller en gruppe datamaskiner i et nettverk.

Maksimalt antall forskjellige regler for et program– Hvis et program kommuniserer gjennom ulike porter, til ulike IP-adresser osv., opprettes det et nødvendig antall regler for dette programmet i brannmuren når den står i læremodus. Gjennom dette alternativet kan du begrense antallet regler som kan opprettes for et program.

3.9.2.2 Brannmurprofiler

Profiler kan brukes til å styre atferden til den personlige brannmuren i ESET Endpoint Security. Når du oppretter eller redigerer en regel for Personlig brannmur, kan du tilordne den til en spesifikk profil eller la den gjelde for alle. Når en profil er aktiv på et nettverksgrensesnitt, gjelder bare globale regler (regler som det ikke er spesifisert noen profil for) og reglene som er tildelt profilen. Du kan opprette flere ulike profiler med forskjellige regler som er tilordnet nettverksadaptere eller nettverker. Slik kan du enkelt endre oppførselen til den personlige brannmuren.

Klikk på **Rediger** ved siden av **Liste over profiler** for å åpne vinduet **Brannmurprofiler**, der du kan redigere profiler.

En nettverksadapter kan stilles inn til å bruke en profil som er konfigurert for et spesifikt nettverk når det er koblet til det nettverket. Du kan også velge en spesifikk profil som skal brukes når du er på et bestemt nettverk i **Avansert oppsett** (F5) > **Personlig brannmur** > **Kjente nettverker**. Velg et nettverk fra listen **Kjente nettverker** og klikk **Rediger** for å tilordne en brannmurprofil til det spesifikke nettverket fra rullegardinmenyen **Brannmurprofil**. Hvis det nettverket er blitt tildelt en profil, vil adapterens standardprofil bli brukt. Hvis adapteren er stilt inn til ikke å bruke nettverksprofilen, vil standardprofilen bli brukt uansett hvilket nettverk den er koblet til. Hvis det ikke finnes en profil for et nettverk eller for adapterkonfigurasjon, brukes den globale standardprofilen. Hvis du vil tilordne en profil til en nettverksadapter, velger du nettverksadapteren, klikker **Rediger** ved siden av **Profiler tildelt til nettverksadaptere**, velger profilen fra rullegardinmenyen **Standard brannmurprofil** og klikker deretter **Lagre**.

Hvis den personlige brannmuren bytter til en annen profil, vises en melding nede til høyre i nærheten av systemklokken.

3.9.2.2.1 Profiler tildelt til nettverksadaptere

Ved å bytte profiler, kan du raskt gjøre flere endringer i brannmurens atferd. Egendefinerte regler kan stilles inn og benyttes for bestemte profiler. Nettverksadapteroppføringer for alle adaptere på maskinen legges til listen **Nettverksadaptere** automatisk.

Kolonner

Navn – Navnet til nettverksadapteren.

Standard brannmurprofil – Standardprofilen brukes når nettverkene du er koblet til ikke har en konfigurert profil, eller nettverksadapteren er stilt inn til ikke å bruke en nettverksprofil.

Foretrekk nettverksprofil – Når **Foretrekk brannmurprofil for tilkoblet nettverk** er aktivert, vil nettverksadapteren bruke brannmurprofilen som er tilknyttet et tilkoblet nettverk når dette er mulig.

Kontrollelementer

Legg til – Legger til en ny nettverksadapter.

Rediger – Lar deg redigere en eksisterende nettverksadapter.

Fjern – Velg en nettverksadapter og klikk **Fjern** hvis du vil fjerne en nettverksadapter fra listen.

OK/Avbryt – Klikk **OK** hvis du vil lagre endringer eller klikk **Avbryt** for avslutte uten å foreta endringer.

3.9.2.3 Konfigurere og bruke regler

Regler representerer et sett med betingelser som brukes til å teste alle nettverkstilkoblinger og alle handlinger som er tilordnet disse betingelsene. Med personlige brannmurregler kan du definere handlingen som gjøres når ulike typer nettverkstilkoblinger etableres. Du får tilgang til oppsettet av regelfiltrering ved å gå til **Avansert oppsett** (F5) > **Personlig brannmur** > **Grunnleggende**. Noen av de forhåndsdefinerte reglene er bundet til avmerkingsboksene fra **tillatte tjenester** (IDS og avanserte alternativer) og det er ikke mulig å slå dem av direkte. Dette må isteden gjøres ved bruk av de relaterte avmerkingsboksene.

I motsetning til den forrige versjonen av ESET Endpoint Security, evalueres regler fra topp til bunn. Handlingen for den første matchende regelen brukes for hver nettverkstilkobling som evalueres. Dette er en viktig atferdsendring sammenlignet med forrige versjon, der prioriteten til reglene var automatiske og mer spesifikke regler hadde høyere prioritet enn mer generelle regler.

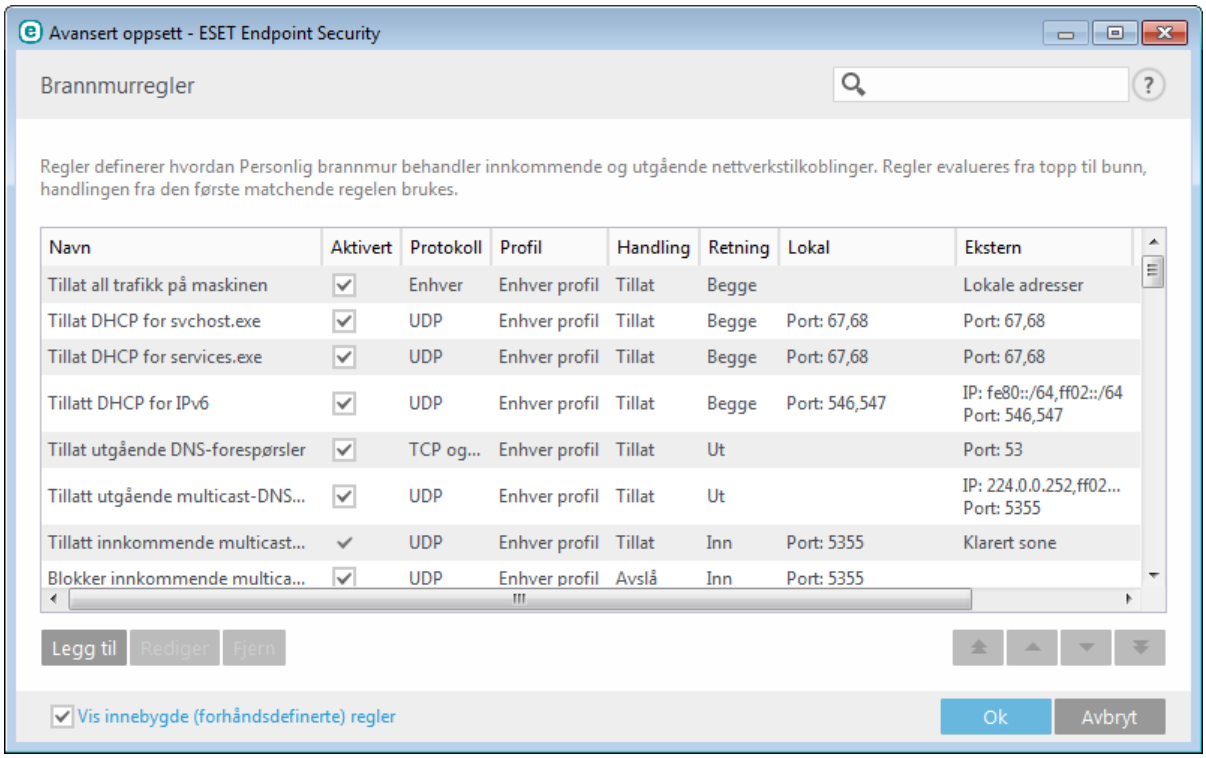
Tilkoblinger kan deles inn i innkommende og utgående tilkoblinger. Innkommende tilkoblinger er startet fra en ekstern datamaskin som forsøker å opprette en tilkobling med det lokale systemet. Utgående tilkoblinger virker på motsatt måte – det lokale systemet kontakter en ekstern datamaskin.

Hvis det blir oppdaget ny og ukjent kommunikasjon, må du tenke nøye gjennom om du vil tillate eller avvise den. Uønskede, usikrede eller ukjente tilkoblinger representerer en sikkerhetsrisiko for systemet. Hvis det blir opprettet en slik tilkobling, anbefaler vi at du er spesielt oppmerksom på den eksterne datamaskinen og det programmet som forsøker å koble seg til maskinen din. Mange infiltrasjoner forsøker å skaffe seg og sende private data, eller laste ned skadelige programmer til vertsarbeidsstasjonene. Med den personlige brannmuren kan du gjenkjenne og avslutte slike tilkoblinger.

3.9.2.3.1 Brannmurregler

Klikk **Rediger** ved siden av **Regler** i fanen **Grunnleggende** for å vise vinduet **Brannmurregler**, hvor en liste med alle reglene vises. **Legg til**, **Rediger** og **Fjerne** lar deg legge til, konfigurere eller slette regler. Du kan justere prioritetsnivået for en regel ved å klikke **Topp/Opp/Ned/Bunn** etter at du har valgt regelen du vil flytte.

TIPS: Du kan bruke feltet **Søk** for å finne en regel/regler etter navn, protokoll eller port.



Kolonner

Navn – Navnet til en regel.

Aktivert – Viser om regler er aktivert eller deaktivert. Den tilsvarende avmerkingsboksen må være valgt for å aktivere en regel.

Protokoll – Viser protokollen som denne regelen gjelder for.

Profil – Viser brannmurprofilen som denne regelen gjelder for.

Handling – Viser kommunikasjonsstatusen (blokker/tillat/spør).

Retning – Kommunikasjonsretningen (innkommende/utgående/begge).

Lokal – IP-adresse og port for den lokale datamaskinen.

Lokal – IP-adresse og port for den eksterne datamaskinen.

Programmer – Angir hvilket program regelen gjelder for.

Kontrollelementer

Legg til – Oppretter en ny regel.

Rediger – Lar deg redigere eksisterende regler.

Fjern – Fjerner eksisterende regler.

Vis innebygde (forhåndsdefinerte) regler – Regler forhåndsdefinert av ESET Endpoint Security til å tillate eller avslå spesifikk kommunikasjon. Du kan slå disse reglene av og på, men du kan ikke slette en forhåndsdefinert regel.

Topp/Opp/Ned/Bunn – Brukes til å justere prioritetsnivået for regler (regler utføres fra topp til bunn).

3.9.2.3.2 Arbeide med regler

En endring er nødvendig hver gang en av de overvåkede parameterne endres. Dersom det gjøres endringer som fører til at regelen ikke kan oppfylle betingelsene og den angitte handlingen ikke benytte, kan den angitte tilkoblingen bli avvist. Dette kan føre til problemer med bruken av programmet som påvirkes av regelen. Et eksempel er endring av nettverksadresse eller portnummer for den eksterne siden.

Den øvre delen av vinduet inneholder tre kategorier:

- **Generelt** – Angi et regelnavn, tilkoblingsretningen, handlingen (**Tillate**, **Avvise**, **Spør**), protokollen og profilen som reglen skal gjelde for.
- **Lokal** – Viser informasjon om den lokale siden av tilkoblingen, deriblant nummeret til den lokale porten eller portområdet og navnet på programmet som kommuniserer. Du kan også legge til en forhåndsdefinert eller opprettet sone med et område med IP-adresser her ved å klikke på **Legg til**.
- **Ekstern** - Denne kategorien inneholder informasjon om den eksterne porten (portområdet). Du kan også definere en liste over eksterne IP-adresser eller soner for en bestemt regel. Du kan også legge til en forhåndsdefinert eller opprettet sone med et område med IP-adresser her ved å klikke på **Legg til**.

Når du oppretter en ny regel, må du skrive inn et navn på regelen i **Navn**-feltet. Velg retningen som regelen gjelder for, fra rullegardinmenyen **Retningen** og handlingen som skal utføres kommunikasjon oppfyller regelen i rullegardinmenyen **Handling**.

Protokoll representerer overføringsprotokollen som brukes for regelen. Velg hvilken protokoll som skal brukes for en angitt regel fra rullegardinmenyen.

ICMP-type/kode står for en ICMP-melding som identifiseres med et nummer (for eksempel: 0 står for "Ekkosvar").

Alle regler er som standard aktivert for **Enhver profil**. Velg eventuelt en egendefinert brannmurprofil med rullegardinmenyen **Profiler**.

Hvis du aktiverer **Logg**, registreres aktiviteten som er tilknyttet regelen, i en logg. Alternativet **Varsle bruker** viser en varsling når regelen brukes.

Nedenfor er et eksempel der vi skaper en ny regel for å gi nettleserprogrammet tilgang til nettverket. I dette eksemplet må følgende konfigureres:

- I kategorien **Generelt** aktiverer du utgående kommunikasjon via protokollene TCP og UDP.
- Legg til nettleserprogrammet ditt (for Internet Explorer er det iexplore.exe) i kategorien **Lokal**.
- I kategorien **Ekstern** aktiverer du port nummer 80 hvis du vil tillate standard bruk av Internett.

MERKNAD: Vær oppmerksom på at forhåndsdefinerte regler kan modifiseres på en begrenset måte.

3.9.2.4 Klarert sone

Den klarerte sonen representerer en gruppe nettverk som den personlige brannmuren tillater at det kommer innkommende trafikk fra ved bruk av standardinnstillinger. Gå til IDS og avanserte alternativer for å bestemme innstillinger for funksjoner slik som fildeling og eksternt skrivebord.

Den faktisk klarerte sonen beregnes dynamisk og separat for hver nettverksadapter basert nettverket datamaskinen er koblet til for øyeblikket. Adresser som er definert som å være innenfor den klarerte sonen i soneredigering, er alltid klarerte. Hvis en nettverksadapter er koblet til et kjent nettverk, legges **Ytterligere klarerte adresser** som er konfigurert for det nettverket til den klarerte sonen for adapteren. Hvis nettverket bruker beskyttelsestypen Hjemme/Arbeid, vil alle tilkoblede delnett være inkludert i den klarerte sonen. Du kan se den faktiske klarerte sonen for hver nettverksadapter fra **Oppsett**-vinduet under **Nettverk** > **Nettverksadaptere**.

MERKNAD: Klarert sone per grensesnitt støttes ikke på Windows XP-operativsystemer. Alle adaptere fra disse operativsystemene har den samme klarerte sonen, og dette er også er synlig i Nettverksadaptere-siden.

3.9.2.5 Konfigurere soner

Soner er grupper med IP-adresser. Disse gruppene er nyttige når du må bruke det samme settet med adresser på nytt i flere regler. Disse sonene kan konfigureres i **Avansert oppsett** > **Personlig brannmur** > **Grunnleggende** ved å klikke knappen **Rediger** ved siden av **Soner**. Når du vil legge til en ny sone, klikker du **Legg til** angir et **Navn** for sonen og en **Beskrivelse**, og legger til en ekstern IP-adresse i feltet **Ekstern adresse (IPv4, IPv6, område, maske)**.

I oppsettvinduet **Brannmursoner** kan du angi et/en sonenavn, beskrivelse, nettverksadresseliste (se også Redigering for kjente nettverker).

3.9.2.6 Kjente nettverk

Når du bruker en datamaskin som ofte kobles til offentlige nettverker eller nettverker utenfor ditt normale arbeidsnettverk, anbefaler vi at du verifiserer nettverkstroverdigheten til nye nettverker som du kobler deg til. Når nettverkene er definert, kan ESET Endpoint Security gjenkjenne klarerte (Hjemme/arbeid) nettverker ved bruk av lukke nettverksparametere som konfigureres i **Nettverksidentifikasjon**. Datamaskiner går ofte inn på nettverk med IP-adresser som ligner på adressene til det klarerte nettverket. I slike tilfeller, kan ESET Endpoint Security registrere et ukjent nettverk som klarert (Hjemme/arbeid). Vi anbefaler at du bruker **Nettverksgodkjenning** for å unngå denne typen situasjon.

Når en nettverksadapter kobles til et nettverk eller adapterens nettverksinnstillinger rekonfigureres, vil ESET Endpoint Security søke etter en oppføring som samsvarer med det nye nettverket i listen over kjente nettverker. Hvis **Nettverksidentifikasjon** og **Nettverksgodkjenning** (valgfritt) matcher, markeres nettverket som tilkoblet i dette grensesnittet. Hvis ingen kjente nettverker oppdages, opprettes et nytt nettverk der nettverksidentifikasjonen er konfigurert slik at nettverket identifiseres neste gang du kobler til det. Den nye nettverkstilkoblingen bruker beskyttelsestypen **Offentlig** som standard. Dialogvinduet **Ny nettverkstilkobling oppdaget** vil oppfordre deg til å velge mellom beskyttelsestypen **Offentlig** eller **Hjemme/Arbeid**. Hvis en nettverksadapter er koblet til et kjent nettverk og det nettverket er markert som **Hjemme/Arbeid**, legges de lokale delnettene til adapteren til den klarerte sonen.

MERKNAD: Når du aktiverer **Marker nye nettverker som offentlige automatisk**, vil ikke dialogvinduet **Ny nettverkstilkobling oppdaget** vises, og nettverket du er koblet til vil markeres som offentlig automatisk. Dette vil føre til at enkelte funksjoner (for eksempel fildeling og eksternt skrivebord) blir utilgjengelige fra nye nettverker.

Kjente nettverker kan konfigureres manuelt i vinduet Redigering for kjente nettverker.

3.9.2.6.1 Redigering for kjente nettverker

Kjente nettverker kan konfigureres manuelt i **Avansert oppsett** > **Personlig brannmur** > **Kjente nettverker** ved å klikke **Rediger**.

Kolonner

Navn – Navnet til et kjent nettverk.

Beskyttelsestype – Viser om nettverket er satt til **Hjemme/arbeid** eller **Offentlig**.

Brannmurprofil – Velg en profil fra rullegardinmenyen **Vis regler brukt i profilen** for å vise regelfilteret for profiler.

Kontrollelementer

Legg til – Oppretter et nytt kjent nettverk.

Redigere – Klikk for å redigere et eksisterende kjent nettverk.

Fjern – Velg et nettverk og klikk **Fjern** for å fjerne det fra listen over kjente nettverker.

Topp/Opp/Ned/Bunn – Brukes til å justere prioritetsnivået for kjente nettverker (nettverker evalueres fra topp til bunn).

Innstillinger for nettverkskonfigurasjon er delt inn i følgende kategorier:

Nettverk

Her kan du definere nettverksnavnet og velge beskyttelsestype (**Offentlig** eller **Hjemme/arbeid**) for nettverket. Bruk rullegardinmenyen **Brannmurprofil** for å velge profilen for dette nettverket. Hvis nettverket bruker beskyttelsestypen **Hjemme/arbeid**, vil alle delnett regnes som klarert. Hvis for eksempel en nettverksadapter er koblet til dette nettverket med IP-adressen 192.168.1.5 og nettverksmasken 255.255.255.0, vil delnettet 192.168.1.0/24 bli lagt til den klarerte sonen for den adapteren. Hvis adapteren har flere adresser/delnett, vil de alle være klarerte, uavhengig av konfigureringen av **Nettverksindentifisering** for det kjente nettverket.

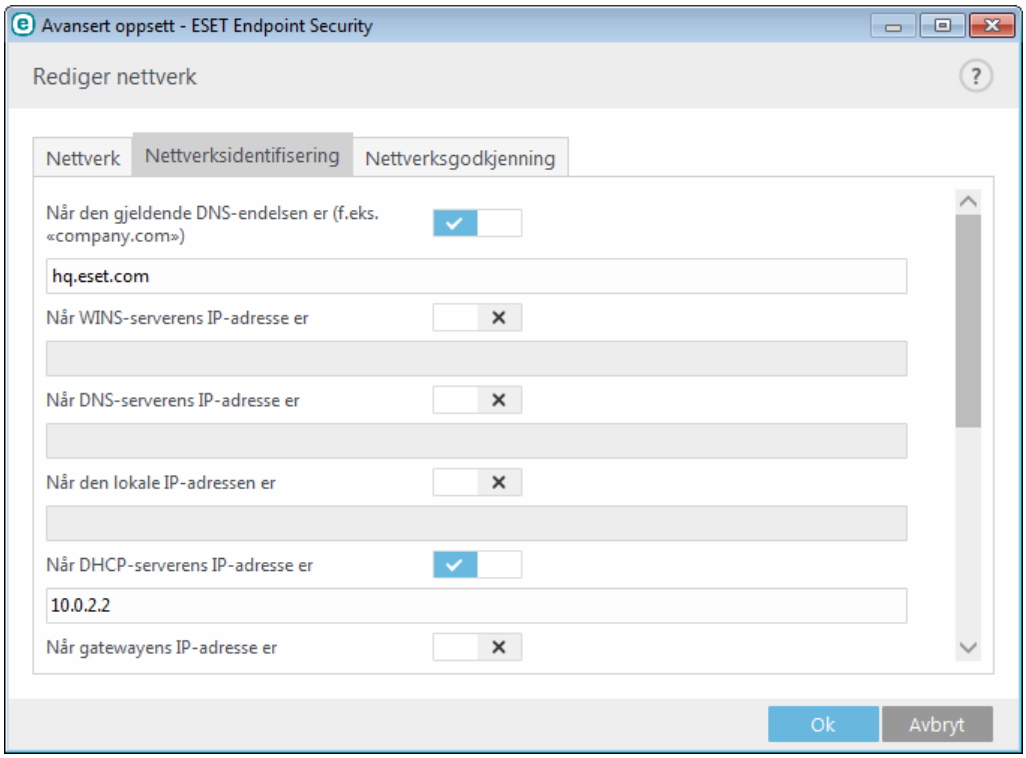
Adresser under **Ytterligere klarerte adresser** legges alltid til den klarerte sonen av adaptere som er koblet til dette nettverket (uavhengig av nettverkets beskyttelsestype).

Følgende betingelser må være møtt for at et nettverk før et nettverk kan markeres som tilkoblet i listen over tilkoblede nettverk:

- Nettverksidentifikasjon – Alle utfylte parametere må være de samme som parameterne for den aktive tilkoblingen.
- Nettverksgodkjenning – hvis en godkjenningsserver velges, må vellykket godkjenning med ESET Authentication Server finne sted.
- Nettverksrestriksjoner (bare Windows XP) – alle valgte globale restriksjoner må være møtt.

Nettverksidentifisering

Nettverksgodkjenning utføres på grunnlag av parameterne til en lokal nettverksadapter. Alle valgte parametere sammenlignes med de faktiske parameterne til aktive nettverksforbindelser. IPv4- og IPv6-adresse er tillatt.

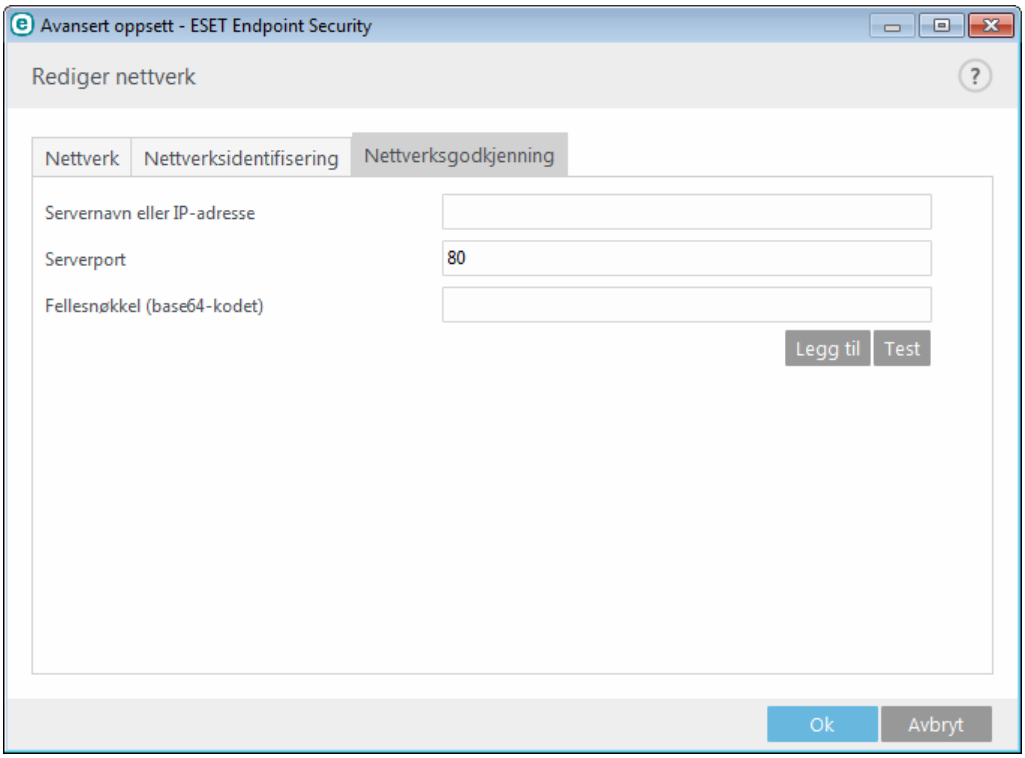


Nettverksgodkjenning

Nettverksgodkjenning søker etter en spesifikk server i nettverket og godkjenner serveren ved hjelp av asymmetrisk kryptering (RSA). Nettverket som godkjennes må ha samme navn som det som er angitt i innstillingene for godkjenningsserveren. Navnet skiller mellom store og små bokstaver. Oppgi et servernavn, en serverlytteport og en fellesnøkkel som samsvarer med den private servernøkkelen (se Nettverksgodkjenning – Serverkonfigurering). Servernavnet kan oppgis i form av en IP-adresse eller et, DNS- eller NetBios-navn. Servernavnet kan etterfølges av en bane som angir nøkkelens plassering på serveren (for eksempel server_name_/directory1/directory2/authentication). Du kan spesifisere alternative servere for bruk ved å føye dem til banen, separert med semikolon.

Fellesnøkkelen kan importeres ved bruk av følgende filtyper:

- PEM-kryptert fellesnøkkel (.pem), denne nøkkelen kan genereres gjennom ESET Authentication Server (se Nettverksgodkjenning – Serverkonfigurering).
- Kryptert fellesnøkkel
- Sertifikat for fellesnøkkel (.crt)



Når du vil teste innstillingene, klikker du **Test**. Hvis godkjenningen var vellykket, vises *Servergodkjenning lyktes*. Hvis godkjenningen ikke er korrekt konfigurert, vises en av følgende feilmeldinger:

Servergodkjenning mislyktes. Den digitale signaturen er ugyldig eller samsvarer ikke.
Serversignaturer samsvarer ikke med den nøkkelen du har angitt.

Servergodkjenning mislyktes. Nettverksnavnet samsvarer ikke.
Navnet på det konfigurerte nettverket stemmer ikke med sonen for servergodkjenning. Sjekk begge navnene, og kontroller at de er identiske.

Servergodkjenning mislyktes. Ugyldig eller ingen respons fra serveren.
Ingen gyldig respons blir mottatt hvis serveren ikke kjører eller er utilgjengelig. En ugyldig respons kan bli mottatt hvis en annen HTTP-server kjører på den spesifiserte adressen.

Ugyldig fellesnøkkel oppgitt.
Kontroller at fellesnøkkelfilen du oppga ikke er skadet.

Nettverksrestriksjoner (kun for Windows XP)

På moderne operativsystemer (Windows Vista og nyere versjoner), har hver nettverksadapter sin egen klarerte sone og aktive brannmurprofil. Dette oppsettet støttes dessverre ikke i Windows XP. Dette betyr at alle nettverksadaptere alltid deler samme klarerte sone og aktive brannmurprofil. Dette gir en potensiell sikkerhetsrisiko når maskinen er koblet til flere nettverker samtidig. I et slikt tilfelle kan trafikk fra ikke-klarerte nettverke evalueres ved å bruke den klarerte sonen og brannmurprofilen som er konfigurert for det andre tilkoblede nettverket. For å minske sikkerhetsrisikoer, kan du bruke følgende restriksjoner for å unngå at én nettverkskonfigurasjon benyttes globalt mens et annen (potensielt ikke-klarert) nettverk er tilkoblet.

På Windows XP benyttes nettverksinnstillinger (klarert sone og brannmurprofil) globalt med mindre en av disse restriksjonene er aktivert og ikke oppfylt:

a. Kun én tilkobling er aktiv
b. Ingen trådløs tilkobling er etablert
c. Ingen usikker trådløs tilkobling er etablert

3.9.2.6.2 Nettverksgodkjenning – Serverkonfigurering

Godkjenningsprosessen kan utføres av en hvilken som helst datamaskin/server som er koblet til nettverket som skal godkjennes. Programmet til ESET-godkjenningsserveren må være installert på en datamaskin/server som er tilgjengelig for godkjenning, på ethvert tidspunkt når klienter prøver å koble seg til nettverket. Installasjonsfilen til programmet for ESET-godkjenningsserveren er tilgjengelig for nedlasting på ESETs nettsted.

Etter at du har installert ESET-godkjenningsserveren, vises et dialogboksvindu (du har tilgang til programmet ved å klikke **Start** > **Programmer** > **ESET** > **ESET Authentication Server**).

For å konfigurere godkjenningsserveren skriver du inn navnet på godkjenningsnettverket, porten som serveren skal lytte til (standard er 80) og dessuten plasseringen der det felles og det private nøkkelparet skal lagres. Deretter genererer du den felles og den private nøkkelen som vil bli brukt i godkjenningsprosessen. Den private nøkkelen forblir på serveren, men fellesnøkkelen må importeres på klientsiden i delen Nettverksgodkjenning når et nettverk konfigureres i brannmuroppsettet.

3.9.2.7 Logging

Den innebygde personlige brannmuren i ESET Endpoint Security lagrer alle viktige hendelser i en loggfil som du kan vise direkte fra hovedmenyen. Klikk **Verktøy** > **Loggfiler**, og velg deretter **Personlig brannmur** fra rullegardinmenyen **Logg**. For å aktivere personlig brannmurlogging, gå til **Avansert oppsett** > **Verktøy** > **Loggfiler** og angi laveste detaljnivå for logging til **Diagnostisering**. Alle avviste tilkoblinger vil bli registrert.

Loggfiler kan brukes til å oppdage feil samt avsløre inntrenging i systemet. Loggene til ESET personlig brannmur inneholder følgende data:

- **Tid** – dato og klokkeslett for hendelsen.
- **Hendelse** – navn på hendelsen.
- **Kilde** – adresse til kildenettverk.
- **Kilde** – adresse til målnettverk.
- **Protokoll** – nettverkskommunikasjonsprotokoll.
- **Navn på regel/orm** – regel som er brukt, eller navnet på orm, hvis den er identifisert.
- **Program** – program som er involvert.
- **Bruker** – navn på brukeren som var pålogget da infiltrasjonen ble oppdaget.

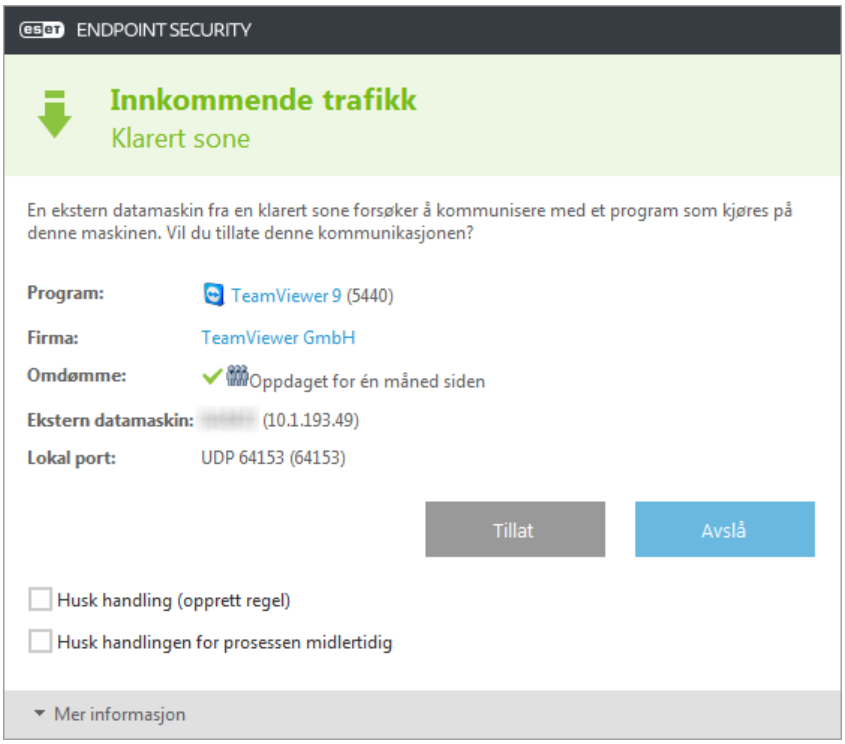
En grundig analyse av disse dataene kan hjelpe deg å oppdage angrep som svekker systemets sikkerhet. Mange andre faktorer angir potensielle sikkerhetsrisikoer, og gjør at du kan minimere virkningen av dem. Noen eksempler på potensielle trussellindikatorer inkluderer altfor hyppige tilkoblinger fra ukjente plasseringer, flere forsøk på å opprette tilkoblinger og ukjente programmer som kommuniserer eller uvanlige portnumre som er i bruk.

3.9.2.8 Etablere en tilkobling – gjenkjenning

Den personlige brannmuren gjenkjenner hver nyopprettet nettverkstilkobling. Den aktive brannmurmodusen avgjør hvilke handlinger som blir utført for den nye tilkobling. Hvis **Automatisk modus** eller **Policybasert modus** er aktivert, vil den personlige brannmuren utføre forhåndsdefinerte handlinger uten interaksjon.

I interaktiv modus vises et informasjonsvindu som forteller at en ny nettverkstilkobling er gjenkjent. Vinduet inneholder også detaljerte opplysninger om tilkoblingen. Du kan velge om du vil tillate tilkoblingen eller avslå (blokkere) den. Hvis du gjentatte ganger tillater den samme tilkoblingen i dialogvinduet, anbefaler vi at du oppretter en ny regel for tilkoblingen. Når du skal gjøre det, velger du alternativet **Husk handling (opprett regel)**, og lagrer handlingen som en ny regel for den personlige brannmuren. Hvis brannmuren senere gjenkjenner den samme tilkoblingen, vil den bruke regelen til å godta den.

Husk handlingen for prosessen midlertidig fører til at en handling (**Tillate**/**Avvise**) brukes inntil et program startes på nytt, reglene eller filtreringsmodusene endres, en brannmurmodul oppdateres eller systemet starter på nytt. Etter enhver av disse handlingene slettes midlertidige regler.



Vær forsiktig når du oppretter nye regler og tillat bare tilkoblinger som er sikre. Hvis du tillater alle tilkoblinger, har ikke den personlige brannmuren noen hensikt. Dette er de viktige parameterne for tilkoblinger:

- **Ekstern side** – Tillat bare tilkoblinger til klarerte og kjente adresser.
- **Lokalt program** – Det er ikke tilrådelig å tillate tilkoblinger til ukjente programmer og prosesser.
- **Portnummer** – Kommunikasjon på felles porter (f.eks. nettrafikk – portnummer 80) skal være tillatt under normale omstendigheter.

For å kunne formere seg, bruker ofte datamaskininfiltreringene Internett-tilkoblinger eller skjulte tilkoblinger for å kunne infisere eksterne systemer. Hvis reglene er konfigurert riktig, blir en personlig brannmur et nyttig verktøy for beskyttelse mot mange forskjellige angrep med skadelig kode.

3.9.2.9 Løse problemer med ESET personlig brannmur

Hvis du opplever tilkoblingsproblemer når ESET Endpoint Security er installert, kan du ta i bruk flere metoder for å finne ut om ESET personlig brannmur er årsaken til problemet. ESET personlig brannmur kan dessuten hjelpe deg å opprette nye regler eller unntak for å løse tilkoblingsproblemer.

Se følgende emner for hjelp med å løse problemer med ESET personlig brannmur:

- Feilsøkingsveiviser
- Loggføring og oppretting av regler eller unntak fra logg
- Opprette unntak fra brannmurmeldinger
- Avansert PCAP-loggføring
- Løse problemer med protokollfiltrering

3.9.2.9.1 Feilsøkingsveiviser

Feilsøkingsveiviseren overvåker i stillhet alle blokkerte tilkoblinger, og vil guide deg gjennom feilsøkingen for å korrigere brannmurproblemer med bestemte programmer eller enheter. Veivisere vil deretter foreslå å bruke et sett med regler hvis du godtar dem. Du finner **Feilsøkingsviseren** i hovedmenyen under **Oppsett** > **Nettverk**.

3.9.2.9.2 Loggføring og oppretting av regler eller unntak fra logg

Som standard logger ikke ESET personlig brannmur eller blokkerte tilkoblinger. Hvis du vil se hva som ble blokkert av den personlige brannmuren, kan du aktivere logging **Feilsøking**- delen av **Avansert oppsett** under **Personal brannmur** > **IDS og avanserte alternativer**. Hvis du ser noe i loggen som du ikke vil at den personlige brannmuren skal blokkere, kan du opprette en regel eller et IDS-unntak for dette ved å høyreklikke på det elementet og velge **Ikke blokker lignende hendelser i framtida**. Vær oppmerksom på at loggen over alle blokkerte tilkoblinger kan inneholde tusenvis av elementer, og det kan være vanskelig å finne én bestemt tilkobling i denne loggen. Du kan slå av loggingen etter at du har løst dette problemet.

For mer informasjon om loggen, se Loggfiler.

Merk: Bruk logging for å se i hvilken rekkefølge den personlige brannmuren blokkerte bestemte regler. Ved å opprette regler fra loggen, kan du dessuten opprette regler som gjør akkurat det du vil.

3.9.2.9.2.1 Opprett regel fra logg

Med den nye versjonen av ESET Endpoint Security kan du opprette en ny regel fra loggen. Fra hovedmenyen klikker du **Verktøy** > **Loggfiler**. Velg **Personlig brannmur** fra rullegardinmenyen, høyreklikk på ønsket loggoppføring og velg **Ikke blokker lignende hendelser i framtida** fra hurtigmenyen. Et varslingsvindu vil vise den nye regelen.

Før du kan opprette nye regler fra loggen, må ESET Endpoint Security være konfigurert med følgende innstillinger:

- sett laveste detaljnivå for loggføring til **Diagnostisering** i **Avansert oppsett** (F5) > **Verktøy** > **Loggfiler**,
- aktiver **Vis melding også for innkommende angrep mot sikkerhetshull** i **Avansert oppsett** (F5) > **Personlig brannmur** > **IDS og avanserte alternativer** > **Inntrengningsgjenkjenning**.

3.9.2.9.3 Opprette unntak fra personlige brannmurmeldinger

Når ESET personlig brannmur oppdager skadelig nettverksaktivitet, vises et varslingsvindu som beskriver hendelsen. Denne varslingen inneholder en kobling som du kan følge for å lære mer om hendelse og sette opp et unntak for denne hendelsen.

MERKNAD: Hvis et/en nettverksprogram eller -enhet ikke implementerer nettverksstandarder riktig, kan dette utløse gjentatte IDS-varslinger. Du kan opprette et unntak direkte fra varslingen for å hindre ESET personlig brannmur i å oppdage dette/denne programmet eller enheten.

3.9.2.9.4 Avansert PCAP-logging

Denne funksjonen er ment å gi mer komplekse loggfiler for ESETs kundestøtte. Bruk denne funksjonen bare når du blir bedt om det av ESETs kundestøtte, ettersom funksjonen kan generere en enorm loggfil og gjøre datamaskinen tregere.

1. Gå til **Avansert oppsett** > **Verktøy** > **Diagnostikk og Aktiver avansert protokollfiltreringslogging**.
2. Prøv å reprodusere problemet du opplever.
3. Deaktiver avansert PCAP-logging.
4. PCAP-loggfilen finner du i katalogen der diagnostiske minnedump genereres:

- Microsoft Windows Vista eller nyere

  C:\ProgramData\ESET\ESET Endpoint Sikkerhet\Diagnostics

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

3.9.2.9.5 Løse problemer med protokollfiltrering

Hvis du opplever problemer med nettleseren eller e-postklienten din, må du først finne ut om dette skyldes protokollfiltrering. Dette gjør du ved å deaktivere filtrering av programprotokoller midlertidig i avansert oppsett (husk å slå den på igjen når du er ferdig, eller så vil nettleseren og e-postklienten din forbli ubeskyttet). Hvis problemet forsvinner etter at du slår den av, kan du henvise til denne liste over vanlige problemer for en måte å løse dem på:

Problemer med oppdatering eller sikker kommunikasjon

Hvis programmet ditt indikerer at det ikke er i stand til å foreta oppdateringer eller at en kommunikasjonskanal ikke er sikker:

- Hvis SSL-protokollfiltrering er aktivert, slå den av midlertidig. Hvis dette hjelper, kan du fortsette å bruke SSL-filtrering og få oppdateringen til å fungere ved å ekskludere den problematiske kommunikasjonen:
  Sett SSL modusen for protokollfiltrering til interaktiv. Kjør oppdateringen på nytt. Det bør vises et dialogvindu som informerer deg om kryptert nettverkstrafikk. Sørg for at programmet matcher programmet du utfører feilsøking for og at sertifikatet virker som om det kommer fra serveren som det utfører oppdatering fra. Velg deretter å huske handlingen for dette sertifikatet og klikk ignorer. Hvis ingen flere relevante dialogvinduer vises, kan du sette filtreringsmodusen tilbake til automatisk. Problemet skal nå være løst.
- Hvis det aktuelle programmet ikke er en nettleser eller e-postklient, kan du helt utelukke det fra protokollfiltrering (å gjøre dette for nettlesere eller e-postklienter vil gjøre deg utsatt). Alle programmer som på et tidligere tidspunkt har fått kommunikasjonen sin filtrert, skal allerede være i listen som du får når du legger til unntak. Du trenger altså ikke å legge dem til manuelt.

Problem med å få tilgang til en enhet på nettverket

Hvis du ikke kan bruke alle funksjonene til en enhet på nettverket (dette kan være å åpne en webside av webkameraet ditt eller spille av video på en mediespiller), kan du prøve å legge til enhetens IPv4- og IPv6-adresser i listen over utelatte adresser.

Problemer med et bestemt nettsted

Du kan ekskludere bestemte nettsteder fra protokollfiltrering ved å bruke URL-adressebehandling. Hvis du ikke får tilgang til https://www.gmail.com/intl/en/mail/help/about.html, kan du for eksempel prøve å legge til *gmail.com* i listen over utelatte adresser.

Feil "Noen av programmene som kan importere rotsertifikatet kjører fortsatt"

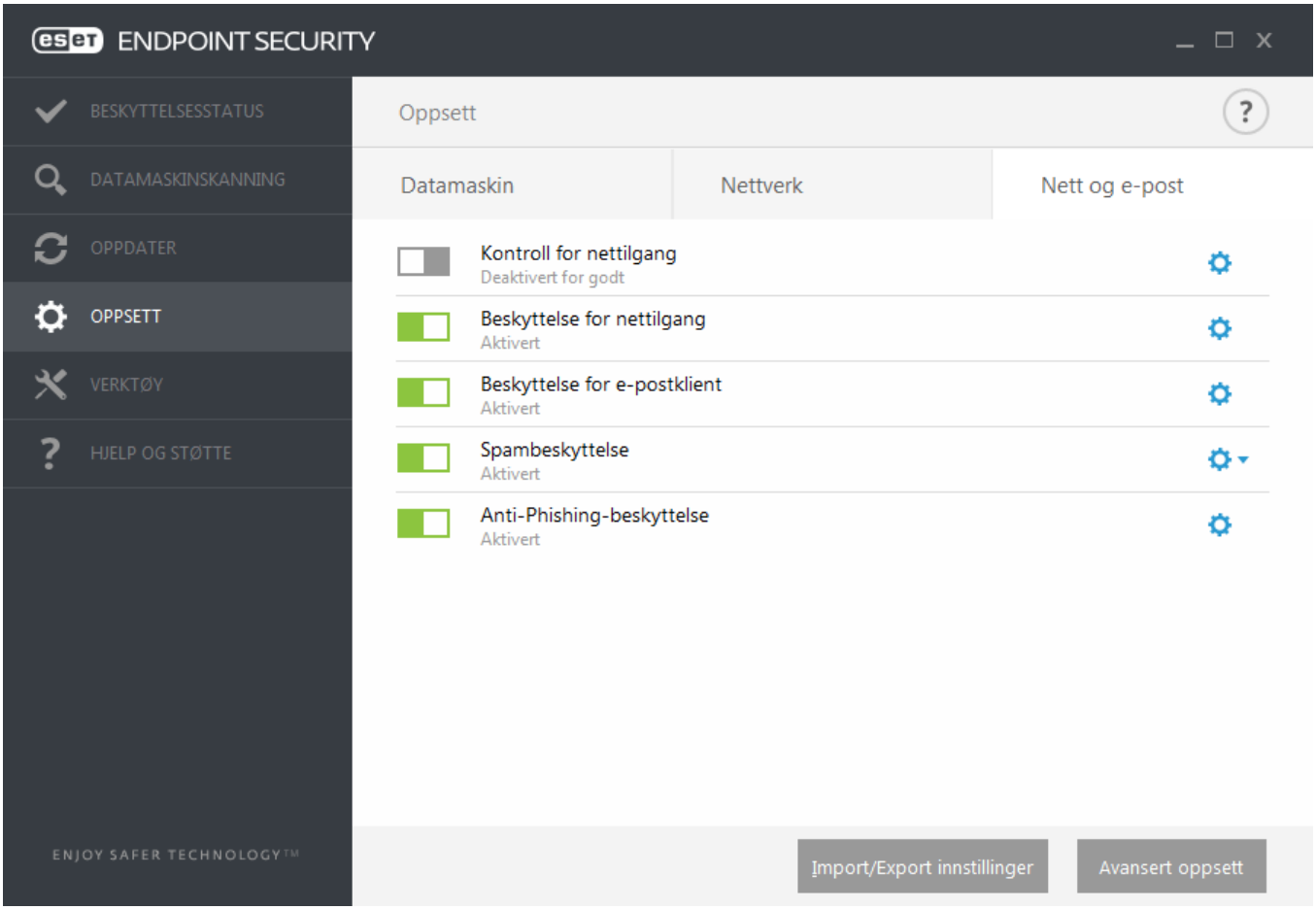
Når du aktiverer SSL-protokollfiltrering, sørger ESET Endpoint Security for at installerte programmer stoler på måten som SSL-protokollen filtreres på ved å importere et sertifikat til programmenes sertifikatlager. For enkelte programmer er det ikke mulig å gjøre dette mens de kjører. Dette inkluderer Firefox og Opera. Sørg for at ingen av dem kjører (den beste måten å gjøre dette på er å åpne Oppgavebehandling og sørge for at firefox.exe eller opera.exe ikke er til stede i Prosesser-fanen). Prøv deretter på nytt.

Feil i forbindelse ikke-klarert utsteder eller ugyldig signatur

Dette betyr sannsynligvis at importen beskrevet ovenfor har mislyktes. Først må du sørge for at ingen av programmene som er blitt nevnt kjører. Deretter deaktiverer du SSL-protokollfiltrering for så å aktivere den igjen. Dette vil kjøre importeringen på nytt.

3.9.3 Nett og e-post

Nett- og e-postkonfigurering finner du under **Oppsett** > **Nett og e-post**. Herfra får du tilgang til mer detaljerte programinnstillinger.



I modulen **Nettkontroll** kan du konfigurere innstillingene som gir administratorer automatiserte verktøy for å beskytte arbeidsstasjonene deres og angi restriksjoner for Internett-søk. Hensikten med nettkontroll er å forhindre tilgang til sider med upassende eller skadelig innhold. Se Nettkontroll for mer informasjon.

Internett-tilkobling er en standardfunksjon for PC-er. Dessverre har det også blitt hovedmediet for overføring av skadelig kode. Av denne grunn er det avgjørende at du vurderer din **Beskyttelse for nettilgang** nøye.

Beskyttelse for e-postklient gir kontroll over e-postkommunikasjon som mottas gjennom POP3- og IMAP-protokollene. Med plugin-programmet for e-postklienten, gir ESET Endpoint Security kontroll over all kommunikasjon fra e-postklienten (POP3, IMAP, HTTP, MAPI).

Spambeskyttelse filtrerer uønskede e-postmeldinger.

Når du klikker tannhjulet ⚙ ved siden av **Spambeskyttelse**, er følgende alternativ tilgjengelige:

Konfigurer ... – Åpner avanserte innstillinger for spambeskyttelse for e-postklient.

Brukerens hviteliste/svarteliste/unntaksliste – Åpner et dialogvindu hvor du kan legge til, redigere eller slette e-postadresser som blir ansett som trygge eller utrygge. Ifølge reglene som er definert her, vil ikke e-post fra disse adressene skannes eller behandles som spam. Klikk **Brukers unntaksliste** for å åpne et dialogvindu hvor du kan legge til, redigere eller slette e-postadresser som kan være misbrukt og brukt til å sende spam. E-postmeldinger som mottas fra adresser oppført på unntakslisten, skannes alltid for spam.

Anti-phishing-beskyttelse er et lag av beskyttelse som gir økt forsvar mot illegitim nettsteder som forsøker å stjele passord og annen sensitiv informasjon. Anti-phishing-beskyttelse finner du i **Oppsett**-ruten under **Nett og e-post**. Se Anti-phishing-beskyttelse for mer informasjon.

Deaktiver – Klikk bryteren for å deaktivere nett-/e-post/spambeskyttelse for nettlesere og e-postklienter.

3.9.3.1 Protokollfiltrering

Virusbeskyttelse for programprotokollene leveres av skannemotoren ThreatSense, som sømløst integrerer alle avanserte skanneteknikker mot skadelig programvare. Protokollfiltreringen virker automatisk, uavhengig av hvilken nettleser eller e-postklient som brukes. Når du skal redigere krypterte-innstillinger (SSL), går du til **Nett og e-post** > **SSL**.

Aktiver filtrering av programprotokollinnhold – kan brukes til å deaktivere protokollfiltering. Legg merke til at mange ESET Endpoint Security-komponenter (Beskyttelse for nettilgang, Beskyttelse for e-postprotokoller, Anti-Phishing, Nettkontroll) er avhengig av dette og vil ikke fungere med mindre det er aktivert.

Utelukkede programmer – Lar deg ekskludere spesifikke eksterne adresser fra protokollfiltrering. Nyttig når protokollfiltrering forårsaker kompatibilitetsproblemer.

Utelukkede IP-adresser – Lar deg ekskludere spesifikke eksterne adresser fra protokollfiltrering. Nyttig når protokollfiltrering forårsaker kompatibilitetsproblemer.

Nett og e-postklienter – Brukes bare på Windows XP-operativsystemer. Med dette alternativet kan du velge programmer der all trafikk filtreres med protokollfiltrering, uavhengig av portene som brukes.

3.9.3.1.1 Nettlesere og e-postklienter

MERKNAD: Fra og med Windows Vista Service Pack 1 og Windows Server 2008 vil den nye Windows Filtering Platform (WFP)-arkitekturen bli brukt til å kontrollere nettverkskommunikasjon. Ettersom WFP-teknologien bruker spesielle overvåkningsteknikker, vil ikke delen **Nettlesere og e-postklienter** være tilgjengelig.

På grunn av den store mengden skadelig kode som sirkulerer på Internett, er sikker bruk av Internett et svært viktig aspekt ved beskyttelse av datamaskiner. Svakheter i nettlesere og falske koblinger fører til at skadelig kode kommer ubemerket inn i systemet, og det er grunnen til ESET Endpoint Security fokuser på nettlesersikkerhet. Hvert enkelt program som bruker nettverket, kan merkes som en nettleser. Programmer som allerede brukte protokollene for kommunikasjon eller programmer den valgte banen kan legges inn i listen over nett- og e-postklienter.

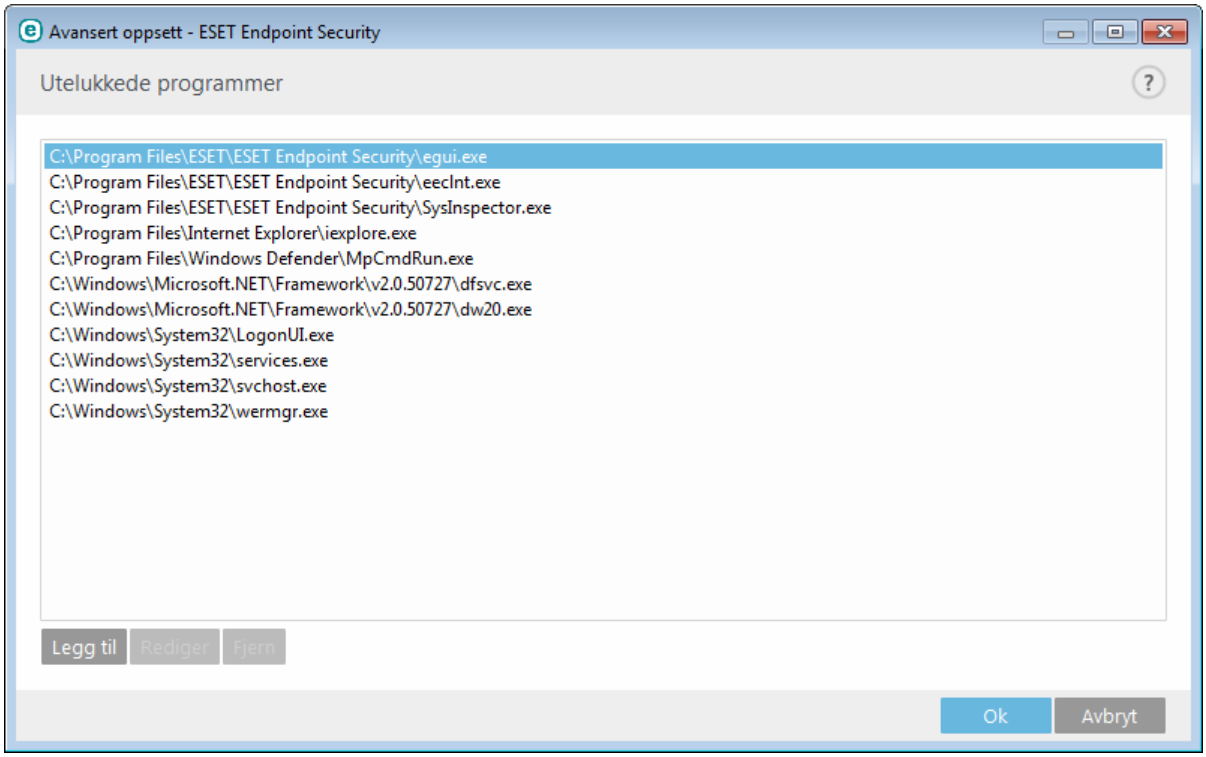
3.9.3.1.2 Utelukkede programmer

Du kan utelukke kommunikasjon for spesifikke nettverksfølsomme programmer fra protokollfiltrering, og legge dem til denne listen. HTTP-/POP3-/IMAP-kommunikasjon for de valgte programmene kontrolleres ikke for trusler. Vi anbefaler at du bare bruker denne teknikken i tilfeller der programmer ikke fungerer riktig når protokollfiltrering er aktivert.

Programmer og tjenester som allerede påvirkes av protokollfiltreringen, vises automatisk når du klikker **Legg til**.

Rediger – Redigerer de valgte oppføringene fra listen.

Fjern – Fjerner de valgte oppføringene fra listen.



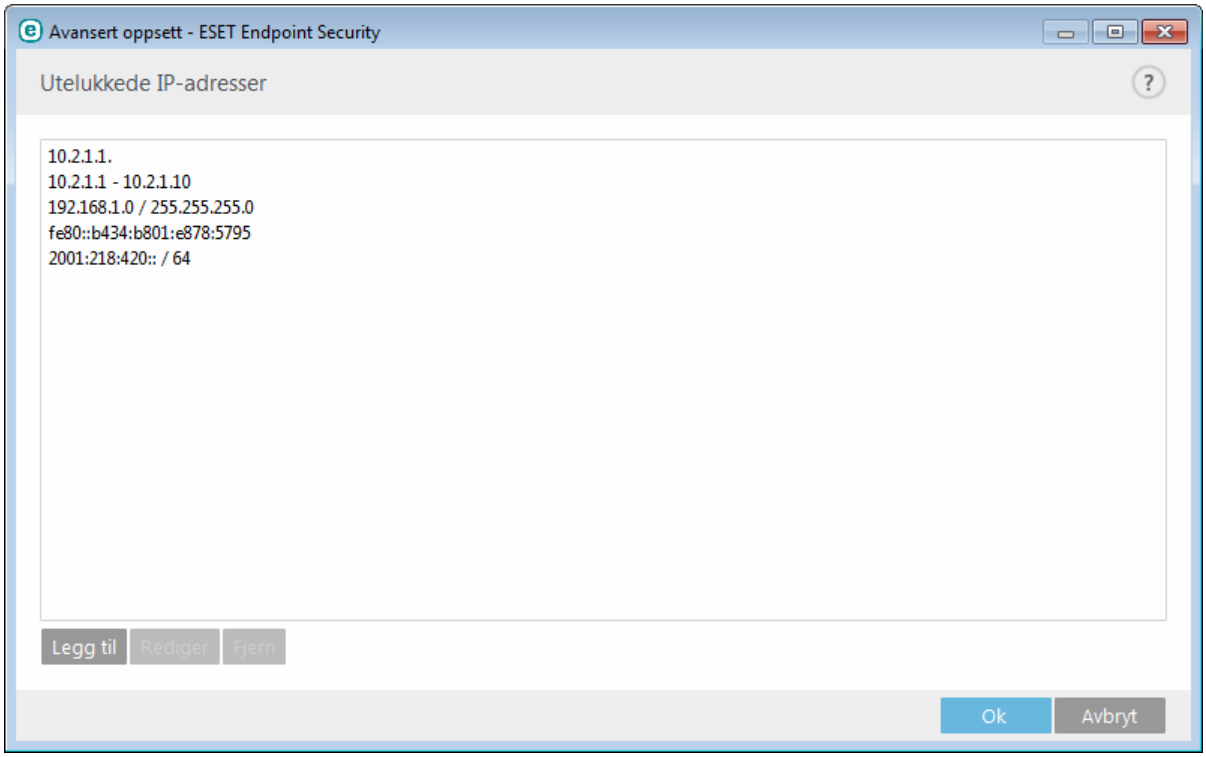
3.9.3.1.3 Utelukkede IP-adresser

IP-adressene i denne listen utelukkes fra protokollinnholdsfiltreringen. HTTP-/POP3-/IMAP-kommunikasjon fra/til de valgte adressene kontrolleres ikke for trusler. Vi anbefaler at dette alternativet bare brukes for adresser som du vet du kan stole på.

Legg til – Klikk for å legge til en IP-adresse/adresseområde/delnett til et eksternt punkt som regelen skal gjelde for.

Rediger – Redigerer de valgte oppføringene fra listen.

Fjern - Fjerner de valgte oppføringene fra listen.



3.9.3.1.4 SSL/TLS

ESET Endpoint Security er i stand til å se etter trusler i kommunikasjon som bruker SSL-protokollen. Du kan bruke ulike skannemetoder for å undersøke SSL-beskyttet kommunikasjon via klarerte sertifikater, ukjente sertifikater eller sertifikater som er utelukket fra kontroll av SSL-beskyttet kommunikasjon.

Aktiver SSL/TLS-protokollfiltrering – Hvis protokollfiltrering er deaktivert, vil ikke programmer skanne kommunikasjon over SSL.

Filtreringsmodus for SSL-protokoll er tilgjengelig i følgende alternativ:

Automatisk modus - Velg dette alternativet for å skanne all SSL-beskyttet kommunikasjon, bortsett fra kommunikasjon som er beskyttet av sertifikater som er utelukket fra kontroll. Hvis en ny kommunikasjon med et ukjent, signert sertifikat etableres, blir du ikke varslet, og kommunikasjonen filtreres automatisk. Når du kobler deg til en server med et ikke-klarert sertifikat som er markert som klarert av deg (det er på listen over klarerte sertifikater), tillates kommunikasjon med serveren, og innholdet i kommunikasjonskanalen filtreres.

Interaktiv modus – Hvis du besøker en ny, SSL-beskyttet nettside (med et ukjent sertifikat), vises det en dialogboks der du kan velge en handling. I denne modusen kan du opprette en liste over SSL-sertifikater som skal utelukkes fra skanning.

Blokker kryptert kommunikasjon ved hjelp av foreldet protokoll SSL v2 – Kommunikasjon som bruker eldre versjoner av SSL-protokollen, vil automatisk bli blokkert.

Rotsertifikat

Rotsertifikat – For at SSL-kommunikasjon skal fungere ordentlig i nettlesere/e-postklienter, er det avgjørende at rotsertifikatet for ESET legges til i listen over kjente rotsertifikater (utgivere). Derfor bør alternativet **Legg til**

rotsertifikatet i kjente nettlesere være aktivert. Velg dette alternativet hvis du vil legge til ESET-rotsertifikatet automatisk i kjente nettlesere (f.eks. Opera og Firefox). Sertifikatet legges automatisk til for nettlesere som bruker systemsertifiseringslageret (for eksempel, i Internet Explorer).

Hvis du vil legge til sertifikatet i nettlesere som det ikke er støtte for, klikker du **Vis sertifikat** > **Detaljer** > **Kopier til fil ...** og importerer sertifikatet til nettleseren manuelt.

Sertifikatgyldighet

Hvis sertifikatet ikke kan verifiseres ved hjelp av TRCA-sertifikatlageret – I noen tilfeller kan ikke sertifikatet verifiseres ved hjelp av lageret for klarerte rotsertifiseringsinstanser (TRCA). Dette betyr at sertifikatet er signert av noen (for eksempel administratoren for en nettserver eller en liten bedrift), og det er ikke alltid risikabelt å anse dette sertifikatet som klarert. De fleste store selskaper (for eksempel banker) bruker sertifikater som er signert av TRCA. Hvis alternativet **Spør om sertifikatgyldighet** (standard) er valgt, blir brukeren bedt om å velge hva som skal gjøres når kryptert kommunikasjon opprettes. Du kan aktivere alternativet **Blokker kommunikasjon som bruker sertifikatet** for alltid å avslutte krypterte tilkoblinger til nettstedet med ubekreftede sertifikater.

Hvis sertifikatet er ugyldig eller skadet – Dette betyr at sertifikatet har utløpt eller at det ble selvsignert feil. I så fall anbefaler vi at du lar **Blokker kommunikasjonen som bruker sertifikatet** være valgt.

Liste med kjente sertifikater lar deg tilpasse atferden til ESET Endpoint Security for spesifikke SSL-sertifikater.

3.9.3.1.4.1 Kryptert SSL-kommunikasjon

Hvis systemet er konfigurert til å bruke SSL-protokollskanning, vil et dialogvindu som ber deg om å velge en handling vises i to situasjoner:

Hvis et nettsted bruker et ukontrollerbart eller ugyldig sertifikat, og ESET Endpoint Security er konfigurert til å spørre brukeren i slike tilfeller (ja som standard for ukontrollerbare sertifikater, nei som standard for ugyldige sertifikater), vil en dialogboks be deg om enten å **Tillate** eller **Blokkere** tilkoblingen.

Deretter, hvis **Filtreringsmodus for SSL-protokoll** er satt til **Interaktiv modus**, vil en dialogboks for hvert nettsted be dem om ente å **Skanne** eller **Ignorere** trafikken. Noen programmer verifiserer at SSL-trafikken deres ikke er blitt endret eller inspisert av noen. I slike tilfeller må ESET Endpoint Security **Ignorere** den trafikken for at programmet skal kunne fungere.

Brukeren kan i begge tilfeller velge å huske den valgte handlingen. Lagrede handlinger lagres i **Liste over kjente sertifikater**.

3.9.3.1.4.2 Liste med kjente sertifikater

Listen med kjente sertifikater kan brukes til å tilpasse atferden til ESET Endpoint Security for spesifikke SSL-sertifikater, og til å huske valgte handlinger hvis **Interaktiv modus** er valgt i **filtreringsmodus for SSL/TLS-protokoll**. Listen kan vises og redigeres i **Avansert oppsett** (F5) > **Nett og e-post** > **SSL/TLS** > **Liste med kjente sertifikater**.

Vinduet **Liste med kjente sertifikater** består av:

Kolonner

Navn – Navnet på sertifikatet.

Sertifikatutsteder – Navnet på sertifikatet.

Sertifikatemne – Emnefeltet identifiserer enheten som er forbundet med fellesnøkkelen som er lagret i feltet for emnets fellesnøkkel.

Tilgang – Velg **Tillatte** eller **Blokkere** som **Tilgangshandling** tillater/blokkerer kommunikasjon som er sikret med dette sertifikatet, uavhengig av kommunikasjonens pålitelighet. Velg **Automatisk** for å tillatte klarerte sertifikater og be om ikke-klarerte sertifikater. Velg **Spør** for alltid å spørre en bruker om hva som skal gjøres.

Skanning – Velg **Skanning** eller **Ignorer** som **Skannehandling** for å skanne eller ignorere kommunikasjon som er sikret med dette sertifikatet. Velg **Auto** for å skanne i automatisk modus og spørre i Interaktiv modus. Velg **Spør**

for alltid å spørre en bruker om hva som skal gjøres.

Kontrollelementer

Legg til – Et sertifikat kan lastes ned manuelt som en fil med filtypen *.cer*, *.crt* eller *.pem*. Klikk Fil for å laste opp et lokalt sertifikat eller klikk **URL** for å angi plasseringen av et sertifikat på nettet.

Rediger – Velg sertifikatet som du vil konfigurere og klikk **Rediger**.

Fjerne – Velg sertifikatet du vil slette og klikk **Fjerne**.

OK/Avbryt – Klikk **OK** hvis du vil lagre endringer eller klikk **Avbryt** for avslutte uten å lagre.

3.9.3.2 Beskyttelse for e-postklient

3.9.3.2.1 E-postklienter

Integrasjon av ESET Endpoint Security i e-postklienter øker nivået for den aktive beskyttelsen mot ondsinnet kode i e-postmeldinger. Hvis e-postklienten din støttes, kan denne integrasjonen aktiveres i ESET Endpoint Security. Hvis integrasjon aktiveres, settes verktøylinjen for ESET Endpoint Security rett inn i e-postklienten (verktøy for nyere versjoner av Windows Live Mail settes ikke inn), slik at e-postbeskyttelsen blir mer effektiv. Integrasjonsinnstillingene finner du i **Oppsett** > **Avansert oppsett** > **Nett og e-post** > **Beskyttelse for e-postklient** > **E-postklienter**.

Integrasjon med e-postklienter

E-postklienter som støttes for øyeblikket, er Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. E-postbeskyttelsen fungerer som en plugin-modul for disse programmene. Hovedfordelen med kontroll ved hjelp av plugin-modul er at den er uavhengig av protokollen som brukes. Når e-postprogrammet mottar en kryptert melding, blir den dekryptert og sendt til virusskanneren. Du finner en komplett liste over e-postklienter som støttes, inkludert versjoner, i følgende artikkel i ESETs kunnskapsbase.

Selv om integrasjon ikke er aktivert, blir e-postkommunikasjonen fremdeles beskyttet av beskyttelsesmodulen til e-postklienten (POP3, IMAP).

Slå på **Deaktiver kontroll ved endringer i innboksens innhold** hvis du opplever at systemet fungerer tregt når du arbeider med e-postklienten (gjelder bare MS Outlook). Dette kan skje når du laster ned e-post fra Kerio Outlook Connector Store.

E-post som skal skannes

Aktiver e-postbeskyttelse etter klientplugins – Når beskyttelse for e-postklient etter klientplugins er deaktivert, vil det fremdeles ikke være mulig å sjekke e-postklient etter protokollfiltrering.
Mottatt e-post– Aktiverer/deaktiverer kontroll av mottatte meldinger.
Sendt e-post– Aktiverer/deaktiverer kontroll av sendte meldinger.
Lest e-post – Aktiverer/deaktiverer kontroll av leste meldinger.

Handling som skal utføres på infisert e-post

Ingen handling – Hvis programmet er aktivert, identifiserer det infiserte vedlegg, men lar e-postmeldingene forbli urørt uten å utføre noen handlinger.
Slett e-post – Programmet varsler brukeren om angrep og sletter meldingen.
Flytt e-post til mappen Slettede elementer – Infisert e-post sendes automatisk til mappen Slettede elementer.
Flytt e-post til mappen – Infisert e-post sendes automatisk til den spesifiserte mappen.

Mappe – Du kan spesifisere hvilken mappe du vil sende infiserte e-postmeldinger til når de gjenkjennes.

Gjenta skanning etter oppdatering– Aktiverer/deaktiverer ny skanning etter en oppdatering av virussignaturdatabasen.

Godta skanneresultater fra andre moduler – Hvis dette alternativet er valgt, godtar e-postmodulen skanneresultater fra andre beskyttelsesmoduler (skanning av protokollene POP3, IMAP).

MERKNAD: Vi anbefaler å ha alternativet **Aktiver e-postbeskyttelse etter klientplugins** og **Aktiver e-postbeskyttelse etter protokollfiltrering** aktivert.

3.9.3.2.2 E-postprotokoller

Protokollene IMAP og POP3 er de mest brukte protokollene for mottak av e-postkommunikasjon i et e-postklientprogram. ESET Endpoint Security beskytter disse protokollene, uavhengig av hvilken protokoll som brukes uten at det er nødvendig å konfigurere e-postklienten på nytt.

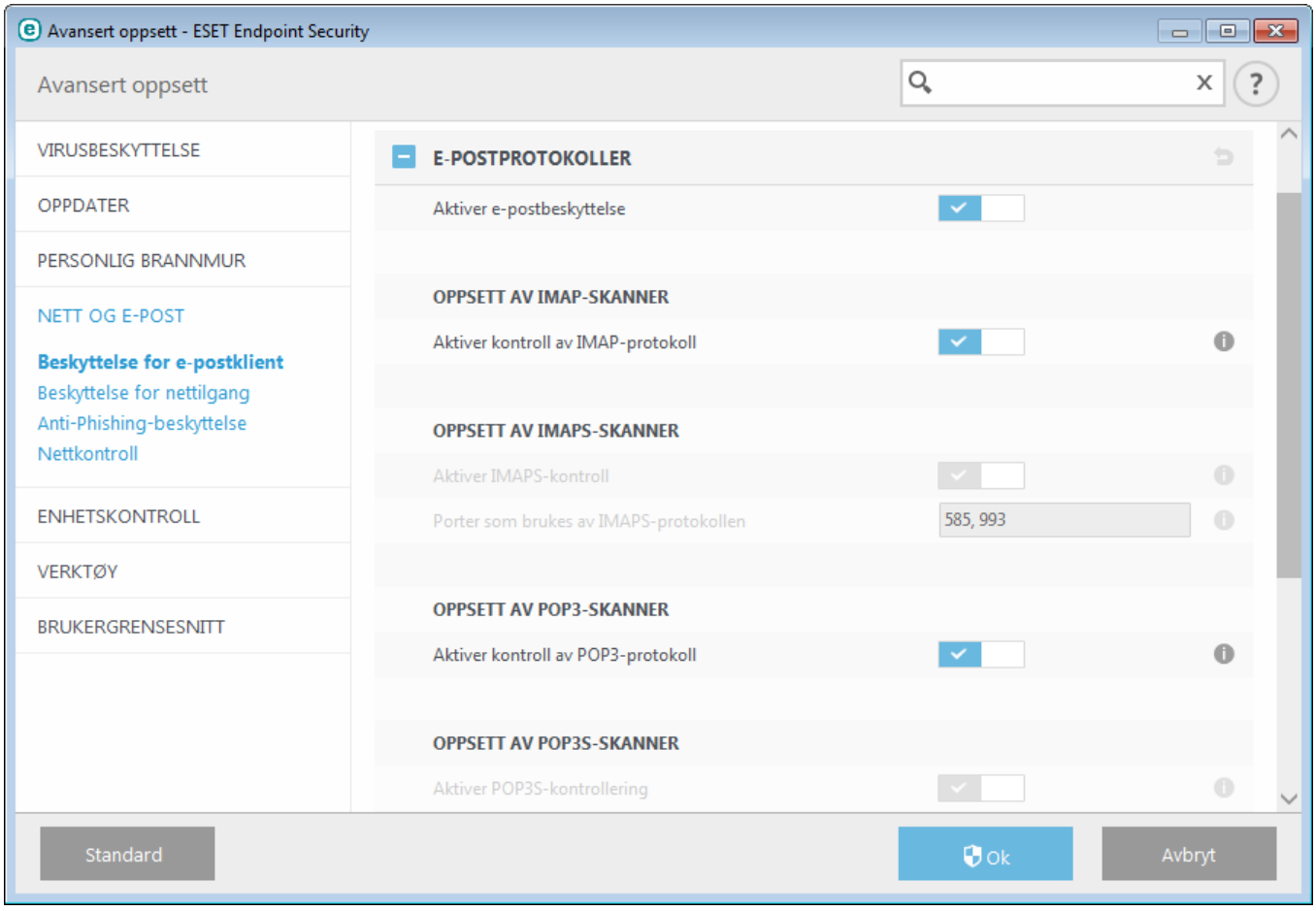
Du kan konfigurere protokollkontroll for IMAP/IMAPS og POP3/POP3S i Avansert oppsett. Du åpne denne innstillingen ved å utvide **Nett og e-post** > **Beskyttelse for e-postklient** > **E-postprotokoller**.

Aktiver e-postbeskyttelse – Aktiverer sjekking av e-postprotokoller.

I Windows Vista og senere operativsystemer, velges og skannes protokollene IMAP og POP3 automatisk på alle porter. I Windows XP, skannes bare konfigurerte **Porter og brukes av IMAPS/POP3S-protokollen** for alle programmene, og alle porter skannes for programmer som er markert som Nett og e-post-klienter.

ESET Endpoint Security støtter også skanning av protokollene IMAPS og POP3S, som bruker en kryptert kanal til å overføre informasjon mellom server og klient. ESET Endpoint Security kontrollerer kommunikasjonen som bruker protokollene SSL (Secure Socket Layer) og TLS (Transport Layer Security). Programmet vil bare skanne trafikk på porter som er definert i **Porter og brukes av IMAPS/POP3S-protokollen**, uavhengig av operativsystemversjonen.

Kryptert kommunikasjon vil ikke bli skannet når standardinnstillingene brukes. Du aktiverer skanning av kryptert kommunikasjon og viser skanneroppsettet ved å navigere til SSL/TLS i Avansert oppsett, klikke **Nett og e-post** > **SSL/TLS** og velge **Aktiver SSL/TLS-protokollfiltrering**.



3.9.3.2.3 Varsler og meldinger

E-postbeskyttelse gir kontroll over e-postkommunikasjon som mottas gjennom POP3- og IMAP-protokollene. Med plugin-programmet for Microsoft Outlook og andre e-postklienter gir ESET Endpoint Security kontroll over all kommunikasjon fra e-postklienten (POP3, MAPI, IMAP, HTTP). Når innkommende meldinger undersøkes, bruker programmet alle avanserte skannemetoder fra skannemotoren ThreatSense. Dette betyr at gjenkjennelse av skadelige programmer finner sted selv før de blir matchet mot virussignaturdatabasen. Skanning av kommunikasjon med POP3- og IMAP-protokollene er ikke avhengig av e-postklienten som blir brukt.

Alternativene for denne funksjonaliteten er tilgjengelige gjennom **Avansert oppsett** under **Nett og e-post** > **Beskyttelse for e-postklient** > **Varsler og meldinger**.

ThreatSenseOppsett av parametere for – I det avanserte oppsettet for virusskanneren kan du konfigurere skannemål, gjenkjenningsmetoder, osv. Klikk for å se vinduet for detaljert oppsett av virusskanneren.

Etter at en e-postmelding er kontrollert, kan en melding med skanneresultatet legges ved meldingen. Du kan velge **Legg ved markeringsmelding i mottatt og lest e-post** eller **Legg ved markeringsmelding i sendt e-post**. Vær oppmerksom på at markeringsmeldinger i sjeldne tilfeller kan utelates i vanskelige HTML-meldinger eller meldinger som er imitert av noen virustyper. Markeringsmeldingene kan legges til i mottatt og lest e-post eller i sendt e-post (eller begge deler). De tilgjengelige alternativene er:

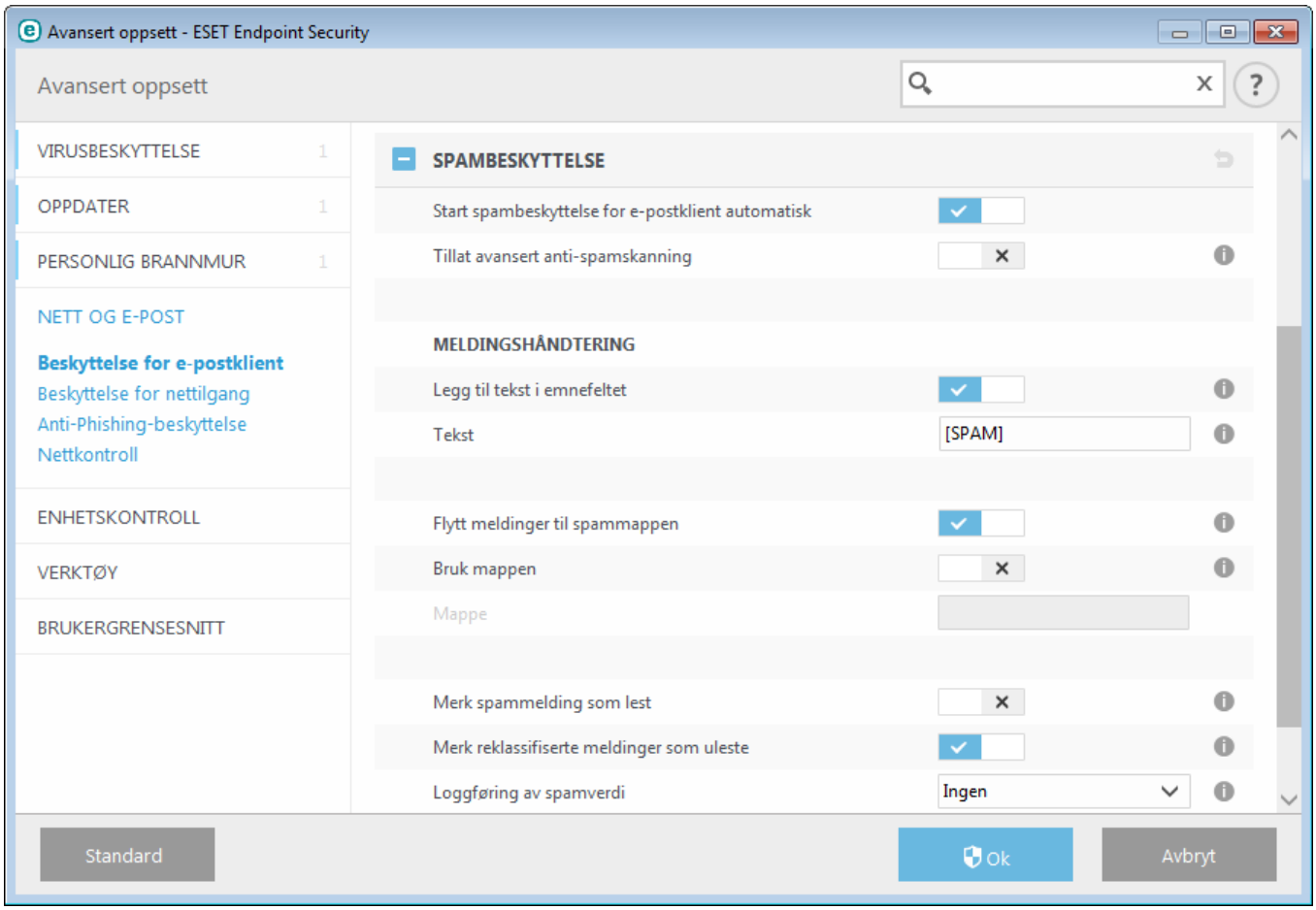
- **Aldri** - Ingen markeringsmeldinger blir lagt til.
- **Bare til infisert e-post** - Bare meldinger som inneholder skadelig programvare, blir merket som kontrollert (standard).
- **Til all e-post** - Programmet legger til meldinger i all skannet e-post.

Legg ved merknad i emnefeltet i infiserte e-postmeldinger som er sendt – Deaktiver dette hvis du ikke vil at e-postbeskyttelsen skal legge inn en virusadvarsel i emnefeltet i infiserte e-postmeldinger. Denne funksjonen gjør det mulig med en enkel, emnebasert filtrering av infisert e-post (hvis e-postprogrammet ditt støtter det). Det øker også troverdigheten for mottakeren, og hvis en infiltrering gjenkjennes, gir det verdifull informasjon om trusselnivået til en bestemt e-postmelding eller avsender.

Mal lagt til i emnefeltet på infisert e-post - Rediger denne malen hvis du ønsker å endre formatet til emneprefikset for infisert e-post. Denne funksjonen erstatter meldingsemnet *"Hallo"* med en bestemt prefiksverdi *"[virus]"* på følgende format: *"[virus] Hallo"*. Variabelen *%VIRUSNAME%* representerer den gjenkjente trusselen.

3.9.3.2.4 Spambeskyttelse

Uønsket e-post kalt spam rangeres som et av de største problemene ved elektronisk kommunikasjon. Spam representerer opptil 80 prosent av all e-postkommunikasjon. Spambeskyttelse beskytter mot dette problemet. Ved å kombinere flere prinsipper for e-postsikkerhet, gir modulen Antispam en utmerket filtrering som holder innboksen ren.



Et viktig prinsipp i gjenkjenning av spam er evnen til å kjenne igjen uønsket e-post basert på forhåndsdefinerte, klarerte adresser (hvitelistede) og spamadresser (svartelistede). Alle adressene fra kontaktlisten blir automatisk lagt til i hvitelisten, i tillegg til alle andre adresser som du merker som trygge.

Den primære metoden som blir brukt til å oppdage spam, er skanning av egenskapene til e-postmeldinger. Mottatte meldinger blir skannet for grunnleggende antispamkriterier (meldingsdefinisjoner, statistisk heuristikk, gjenkjennelse av algoritmer og andre unike metoder), og den resulterende indeksverdien fastslår om en melding er spam eller ikke.

Start spambeskyttelse for e-postklient automatisk – Når dette alternativet er aktivert, aktiveres spambeskyttelsen automatisk når systemet startes opp.

Tillat avansert anti-spamskanning – Flere antispamdata vil bli lastet ned, og dette øker mulighetene til spambeskyttelse og gir bedre resultater.

Spambeskyttelsen i ESET Endpoint Security gjør det mulig å angi forskjellige parametere for e-postlister. Du har disse alternativene:

Meldingshåndtering

Legg til tekst i emnefeltet – Lar deg legge til et egendefinert prefiks på emnelinjen i meldinger som er blitt klassifisert som spam. Standardverdien er "[SPAM]".

Flytt meldinger til spammappen – Når dette alternativet er aktivert, flyttes spammeldinger til standardmappen for søppelpost og meldinger som ikke omklassifiseres som spam flyttet til innboks. Når du høyreklikker en e-postmelding og velger ESET Endpoint Security fra kontekstmenyen, kan du kan velge blant følgende alternativer.

Bruk mappen – Dette alternativet flytter spam til en brukerdefinert mappe.

Merk spammelding som lest – Aktiver dette alternativet hvis du vil at spammeldinger automatisk skal merkes som lest. Det hjelper deg med å konsentrere deg om "rene" meldinger.

Merk reklassifisert melding som ulest - Meldinger som opprinnelig ble klassifisert som spam, men senere merket som "rene", blir vist som ulest.

Logging av spamverdi – Antispammotoren i ESET Endpoint Security gir alle skannede meldinger en spamverdi. Meldingen registreres i antispamloggen (**ESET Endpoint Security** > **Verktøy** > **Loggfiler** > **Spambeskyttelse**).

- **Ingen** – summen fra spamskanningen loggføres ikke.
- **Bare skriv omklassifiserte meldinger og meldinger merket som spam** – Bruk dette alternativet hvis du ønsker å registrere en spamverdi for meldinger som er merket som SPAM.
- **Alle** – Alle meldinger registreres med en spamverdi i loggen.

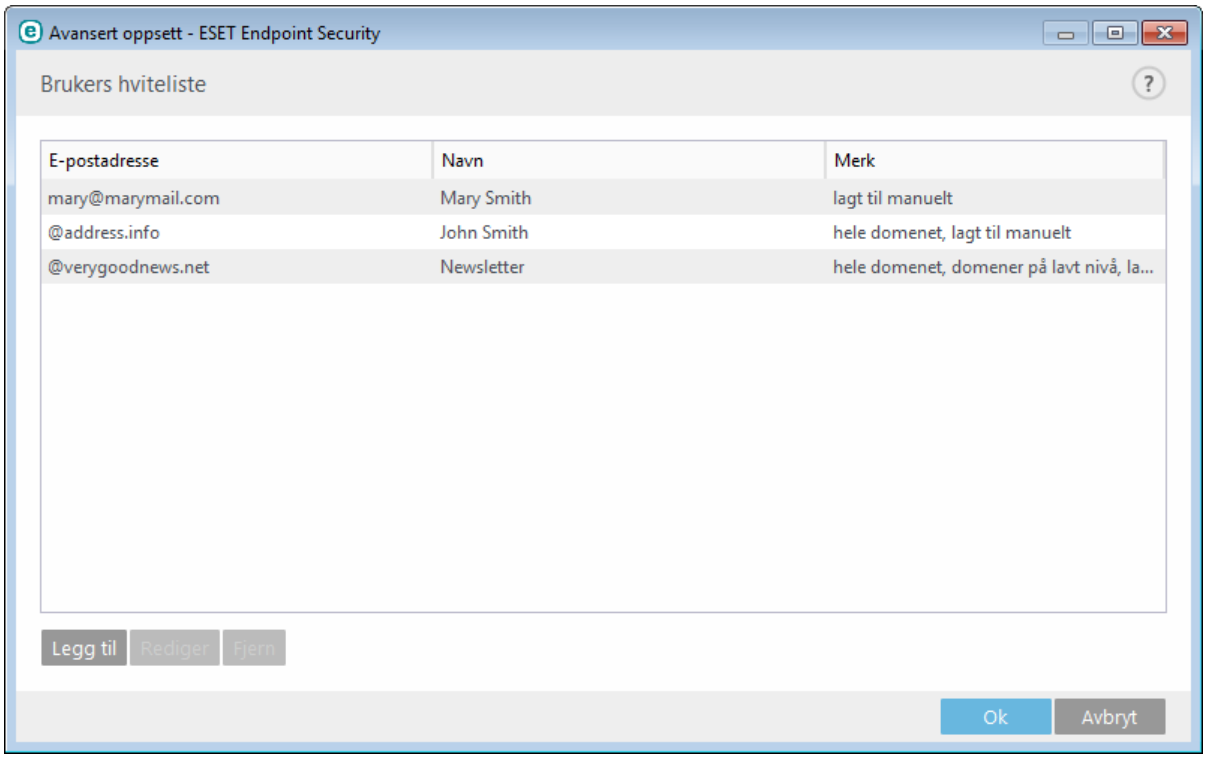
MERKNAD: Når du klikker en melding i mappen for søppelpost, kan du velge **Omklassifiser valgte meldinger som IKKE spam** og meldingen flyttes til innboksen. Når du klikker en melding du anser som spam i innboksen, kan du velge **Omklassifiser valgte meldinger som spam** og meldingen flyttes til innboksen. Du kan velge flere meldinger og utføre den samme handlingen på alle samtidig.

MERKNAD: ESET Endpoint Security støtter antispambeskyttelse for Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail.

3.9.3.2.4.1 Svarteliste/hviteliste/unntaksliste

For å beskytte mot uønsket e-post kan du klassifisere e-postadresser ved bruk av spesielle lister i ESET Endpoint Security. Hvitelisten inneholder e-postadresser du anser som trygge. Meldinger fra brukere på en hviteliste er alltid tilgjengelige i innboksen. Svartelisten inneholder e-postadresser klassifisert som spam, og alle meldinger fra senderne i svartelisten markeres deretter. Unntakslisten inneholder e-postadresser som alltid kontrolleres for spam, men kan også inneholde adresser fra uønsket e-post som ikke gjenkjennes som spam i første omgang.

Alle lister kan redigeres fra hovedvinduet til ESET Endpoint Security i **Avansert oppsett** > **Internett og e-post** > **Beskyttelse for e-postklient** > **adressebøker for spambeskyttelse** ved å klikke knappene Legg til, Rediger og Fjern i dialogvinduet for hver liste, eller på **Oppsett** > **Nett og e-post** etter du klikker på tannhjulet ⚙ ved siden av **Spambeskyttelse**.



ESET Endpoint Security legger som standard til alle adressene fra adresseboken med støttede e-postklienter i hvitelisten. Svartelisten er som standard tom. Unntakslisten inneholder bare brukerens egne e-postadresser som

standard.

3.9.3.2.4.2 Legge til adresser i hvite- og svartelisten

E-postadresser som tilhører folk du kommuniserer med ofte, kan legges til hvitelisten for å sikre at ingen meldinger som kommer fra en hvitelisteadresse blir klassifisert som spam. Kjente spamadresser kan legges til svartelisten og vil alltid bli klassifisert som spam. Du legger til en ny adresse i hvitelisten eller svartelisten ved å høyreklikke på e-postmeldingen og velge **ESET Endpoint Security** > **Legg til i hviteliste** eller **Legg til i svarteliste**, eller klikke på knappen **Klarert adresse** eller **Spamadresse** i ESET Endpoint Security-antispamverktøylinjen i e-postklienten din.

Prosessen gjelder også på samme måte for spamadresser. Hvis en e-postadresse står oppført i svartelisten, blir hver e-postmelding som kommer fra den adressen, klassifisert som spam.

3.9.3.2.4.3 Merke meldinger som spam eller ikke spam

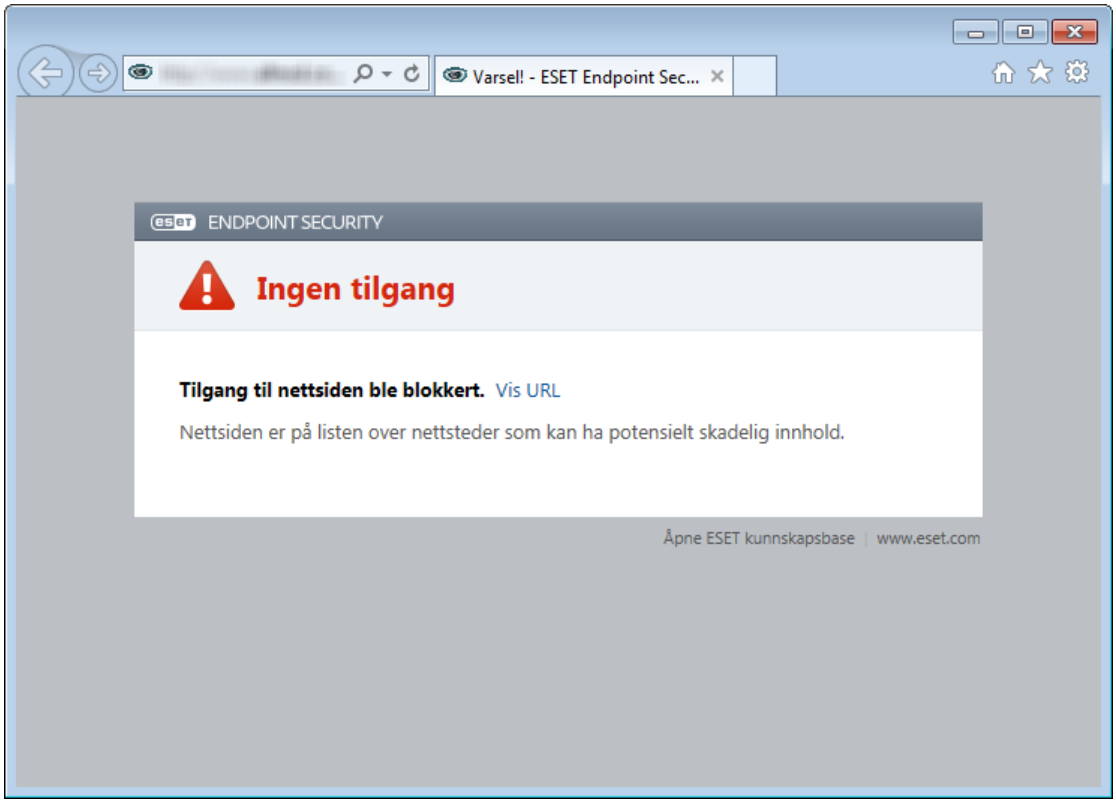
Enhver melding som vises i e-postklienten, kan merkes som spam. Det gjør du ved å høyreklikke meldingen og klikke **ESET Endpoint Security** > **Omklassifiser valgte meldinger som spam**, eller klikke **Spam** i ESET Endpoint Securitys antispamverktøylinje plassert i den øvre delen av e-postmeldingen din.

Omklassifiserte meldinger blir automatisk flyttet til SPAM-mappen, men avsenderadressen blir ikke lagt til **Svartelisten**. Likeledes kan du klassifisere meldinger som "ikke span" og klikke **ESET Endpoint Security** > **Omklassifiser valgte meldinger som ikke spam,** eller klikke **Ikke spam** i ESET Endpoint Securitys antispamverktøylinje plassert i den øvre delen av e-postmeldingen din. Hvis meldinger fra mappen **Spam** klassifiseres som ikke spam, blir de flyttet til den **innboks**-mappen. Hvis du merker en melding som ikke spam, blir avsenderadressen automatisk lagt til i **Hvitelisten**.

3.9.3.3 Beskyttelse for nettilgang

Internett-tilkobling er en standardfunksjon for de fleste PC-er. Dessverre har det også blitt hovedmediet for overføring av skadelig kode. Beskyttelse for nettilgang skjer ved overvåkning av kommunikasjonen mellom nettlesere og eksterne servere og er i samsvar med reglene for HTTP (Hypertext Transfer Protocol) og HTTPS (kryptert kommunikasjon).

Tilgang til nettsider det er kjent at har skadelig innhold blokkeres før innholdet lastes ned. Alle andre nettsider skannes av ThreatSense skannemotoren når de lastes ned og blokkerer hvis skadelig innhold oppdages. Beskyttelse for nettilgang tilbyr to nivåer av beskyttelse, blokkering etter svarteliste og blokkering etter innhold.



Vi anbefaler sterkt at du lar Beskyttelse for nettilgang være aktivert. Du får tilgang til dette alternativt fra hovedvinduet i ESET Endpoint Security ved å navigere til **Oppsett** > **Nett og e-post** > **Beskyttelse for nettilgang**.

Følgende alternativer er tilgjengelige i **Avansert oppsett** (F5) > **Nett og e-post** > **Beskyttelse for nettilgang**:

- **Nettprotokoller** – lar deg konfigurere overvåking for disse standardprotokollene som brukes av de fleste nettlesere.
- **URL-adressebehandling** – kan du angi HTTP-adresser som du vil blokkere, tillate eller utelukke fra kontroll.
- **Oppsett av parametere for ThreatSense-motor** – Avansert oppsett for virusskanner – lar deg konfigurere innstillinger for typer objekter som skal skannes (e-poster, arkiver, osv.), gjenkjenningsmetoder for Beskyttelse for nettilgang, osv.

3.9.3.3.1 Nettprotokoller

Som standard er ESET Endpoint Security konfigurert til å overvåke HTTP-protokollen som brukes av de fleste nettlesere.

I Windows Vista og senere versjoner, overvåkes HTTP-trafikk alltid på alle porter for alle programmer. I Windows XP, kan du endre **Porter og brukes av IMAPS/POP3S-protokollen** i **Avansert oppsett** (F5) > **Nett og e-post** > **Beskyttelse for nettilgang** > **Nettprotokoller** > **Oppsett av HTTP-skanner**. HTTP-trafikk overvåkes på spesifikke porter for alle programmer, og på alle porter som er markert som Nett og e-postklienter.

ESET Endpoint Security støtter også HTTPS-protokollkontroll. HTTPS-kommunikasjon bruker en kryptert kanal til å overføre informasjon mellom server og klient. ESET Endpoint Security kontrollerer kommunikasjon med protokollene SSL (Secure Socket Layer) og TLS (Transport Layer Security). Programmet vil bare skanne trafikk på porter som er definert i **Porter og brukes av HTTPS-protokollen**, uavhengig av operativsystemversjonen.

Kryptert kommunikasjon vil ikke bli skannet når standardinnstillingene brukes. Du aktiverer skanning av kryptert kommunikasjon og viser skanneroppsettet ved å navigere til SSL/TLS i Avansert oppsett, klikke **Nett og e-post** > **SSL/TLS** og velge **Aktiver SSL/TLS-protokollfiltrering**.

3.9.3.3.2 URL-adressebehandling

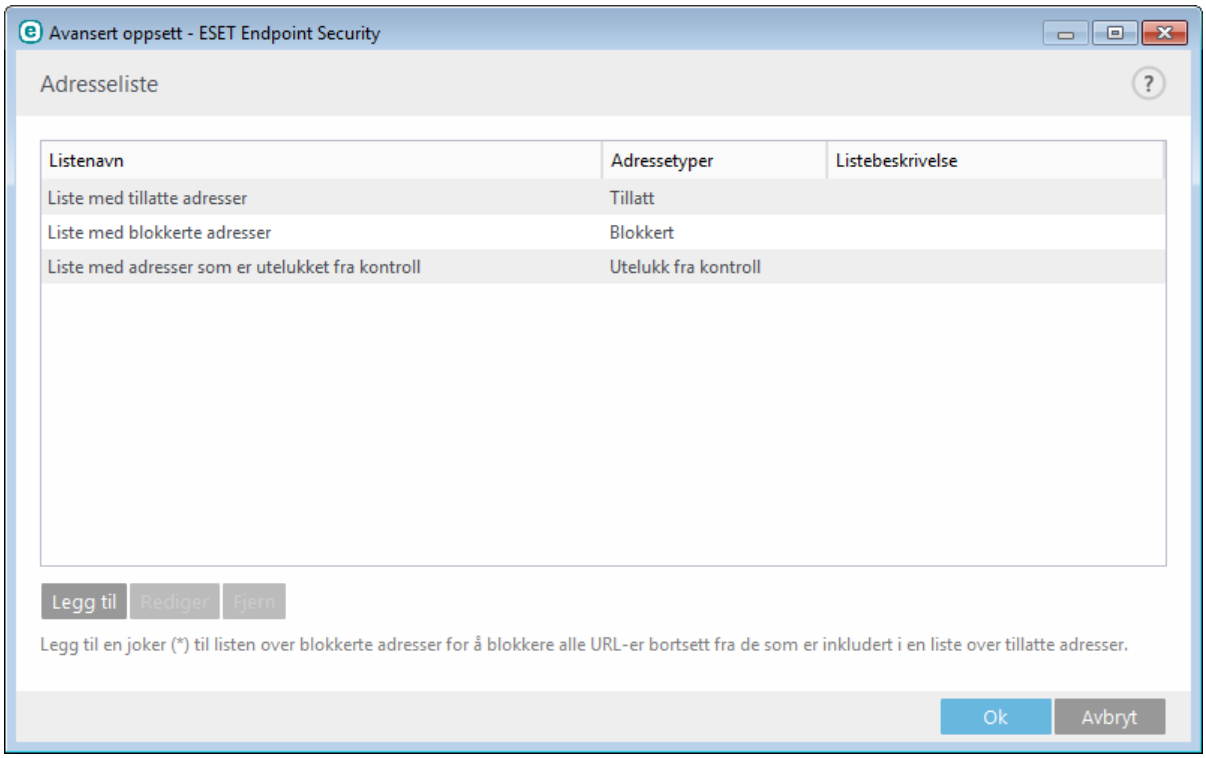
I delen for URL-adressebehandling kan du angi HTTP-adresser som du vil blokkere, tillate eller utelukke fra kontroll.

Du vil ikke ha tilgang til nettsidene som står oppgitt i **listen med blokkerte adresser** med mindre de også er inkludert **listen med tillatte adresser**. Nettsteder i **listen med tillatte adresser som er utelukket fra kontroll** skannes ikke for ondsinnet kode når du åpner dem.

Aktiver SSL-protokollfiltrering må være valgt hvis du vil filtrere HTTPS-adresser i tillegg til HTTP-nettsider. Hvis ikke vil bare domenene til HTTPS-sidene du har besøkt bli lagt til. Den fullstendige URL-en blir altså ikke lagt til.

I alle lister kan spesialsymbolene * (stjerne) og ? (spørsmålstegn) brukes på alle listene. Stjernetegnet står for et hvilket som helst nummer eller tegn, mens spørsmålstegnet står for ett enkelt variabelt tegn. Vær spesielt forsiktig når du spesifiserer ekskluderte adresser, ettersom listen bare skal inneholde klarerte og trygge adresser. Det er også veldig viktig at symbolene * og ? brukes riktig i denne listen. Se Legg til HTTP-adresse / domenemaske for å se hvordan et helt domene og alle underdomener kan matches på en sikker måte. Du aktiverer listen ved å aktivere alternativet**Liste aktiv**. Hvis du ønsker å få beskjed når en adresse fra den gjeldende listen skrives inn, aktiverer du **Varsle under søk**.

Hvis du vil blokkere alle HTTP-adresser unntatt adressene i den aktive **Liste med tillatte adresser**, legger du * til den aktive **Liste med blokkerte adresser**.



Legg til – Oppretter en ny liste i tillegg til de forhåndsdefinerte listene. Dette kan være nyttig hvis du vil dele ulike adressegrupper på en logisk måte. En liste med blokkerte adresser kan for eksempel inneholde adresser fra en ekstern offentlig svarteliste, og en annen liste kan inneholde din egen svarteliste. Dette gjør det enklere å oppdatere den eksterne listen og samtidig holde din egen liste intakt.

Rediger – Endrer eksisterende lister. Bruk dette alternativet til å legge til eller fjerne adresser fra listen.

Fjern – Fjerner eksisterende lister. Kan bare brukes på lister som ble opprettet med **Legg til**, ikke standardlistene.

3.9.3.4 Anti-Phishing-beskyttelse

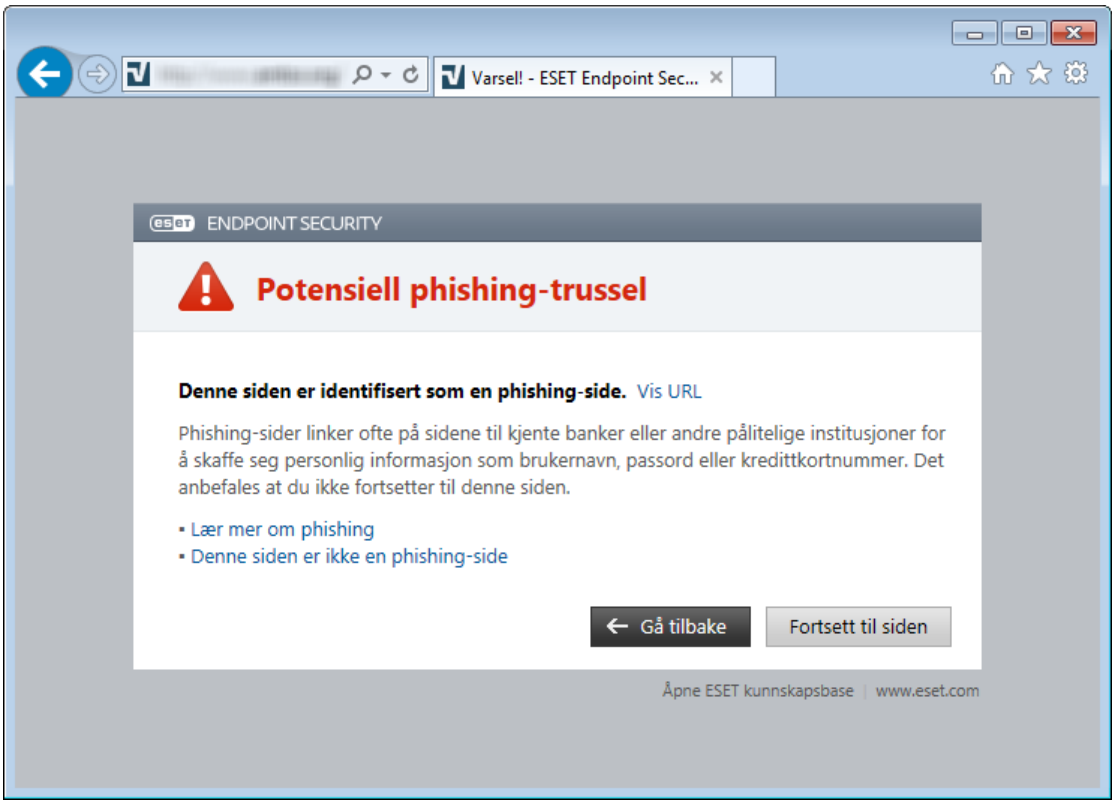
Begrepet phishing definerer en kriminell handling som bruker sosial manipulering for å få andre til å oppgi ellers hemmelig informasjon. Phishing brukes ofte for å få tilgang til sensitivt materiale som f.eks. bankkontonumre, PIN-koder osv. Du kan lese mer om denne aktiviteten i ordlisten. ESET Endpoint Security gir anti-phishing-beskyttelse. Nettsteder det er kjent at har slikt innhold, blir alltid blokkert.

Vi anbefaler deg på det sterkeste å aktivere Anti-phishing i ESET Endpoint Security. For å gjøre dette, åpner du **Avansert oppsett** (F5) og går til **Nett og e-post** > **Anti-phishing-beskyttelse**.

Besøk våre hjelpesider for mer informasjon om anti-phishing-beskyttelse i ESET Endpoint Security.

Åpne et phishing-nettsted

Når du åpner et kjent phishing-nettsted, vil du få følgende dialog i nettleseren din. Hvis du fortsatt vil gå inn på siden, klikk **Fortsett til siden** (anbefales ikke).



MERKNAD: Potensielle phishing-nettsteder som har blitt hvitelistede, vil som standard utløpe etter noen timer. For å tillate et nettsted permanent, bruker du verktøyet URL-adressebehandling. Fra **Avansert oppsett** (F5), utvider du **Nett og e-post** > **Beskyttelse for nettilgang** > **URL-adressebehandling** > **Adresseliste**, klikk **Rediger** og legg til nettstedet du vil endre på listen.

Rapportere et phishing-nettsted

Ved å følge lenken Rapporter kan du rapportere et phishing-nettsted eller et skadelig nettsted til ESET for analyse.

MERK: Før du sender inn et nettsted til ESET, må du kontrollere at den oppfyller ett eller flere av følgende kriterier:
- nettstedet gjenkjennes absolutt ikke,
- nettstedet blir feilaktig gjenkjent som en trussel. I dette tilfellet, kan du velge Rapporter et phishing-nettsted.

Du kan også sende inn nettstedet via e-post. Send e-posten til samples@eset.com. Husk å bruke et beskrivende emne og å legge ved så mye informasjon som mulig om nettstedet (f.eks. hvilket nettsted du ble sendt til den fra, hvordan du hørte om den osv.).

3.9.4 Nettkontroll

I delen Nettkontroll kan du konfigurere innstillinger som beskytter firmaet mot fare for rettslig ansvar. Nettkontroll kan regulere tilgang til nettsteder som krenker intellektuell eiendomsrett. Målet er å forhindre at ansatte får tilgang til sider med uegnet eller skadelig innhold, eller sider som kan ha negativ innvirkning på produktiviteten.

Med nettkontroll kan du blokkere nettsider som kan inneholde potensielt støtende materiale. I tillegg kan arbeidsgivere eller systemadministratorer hindre tilgang til mer enn 27 forhåndsdefinerte nettstedskategorier og over 140 underkategorier.

Nettkontroll er deaktivert som standard. Når du skal aktivere nettkontroll, trykker du F5 for å gå inn i **Avansert oppsett** og utvider **Nett og e-post** > **Nettkontroll**. Velg **Integrer med system** for å aktivere nettkontroll i ESET Endpoint Security. Klikk **Rediger** ved siden av **Regler** for å gå til vinduet Redigering for nettkontrollregler.

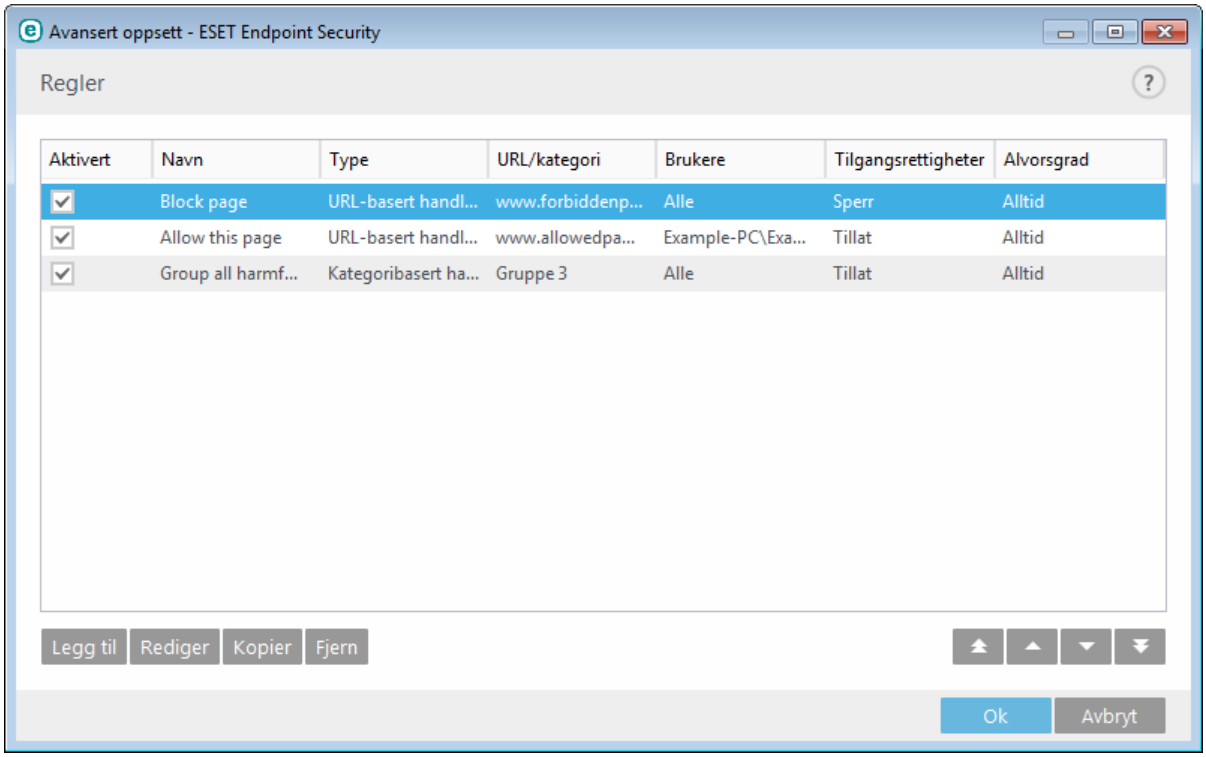
I feltene **Blokkert nettsidemelding** og **Blokkert nettsidegrafikk** kan du enkelt tilpasse meldingen som vises når et nettsted er blokkert.

TIPS: Et eksempel på en blokkert nettsidemelding kan være *Nettsiden ble blokkert fordi den anses som upassende eller har skadelig innhold. Ta kontakt med din administrator for flere detaljer* og du kan gå inn på et nettadresse eller nettverksbane med egendefinerte bilder, f.eks. *http://test.com/test.jpg*. Den egendefinerte bildestørrelse er

automatisk satt til 90 x 30. Bildene skaleres til denne størrelsen automatisk hvis de ikke er det allerede.

3.9.4.1 Regler

Vinduet **Regelredigering** viser eksisterende URL-baserte og kategoribaserte regler.



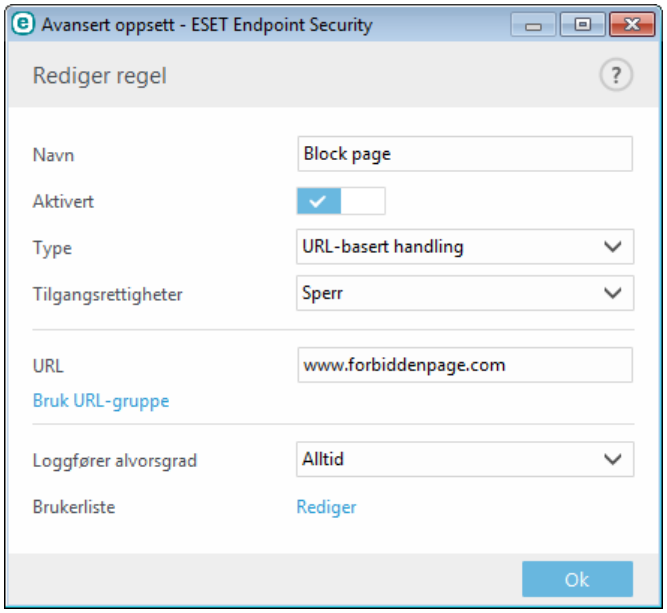
Regellisten inneholder flere beskrivelser av reglene, for eksempel navn, typen blokkering, hvilken handling som skal utføres etter matching med en nettkontrollregel, og logger alvorlighetsgraden.

Klikk **Legg til** eller **Rediger** for å ordne en regel. Klikk **Kopier** for å opprette en ny regel med forhåndsdefinerte alternativer som brukes for en annen valgt regel. Trykk **CTRL** og klikk for å velge flere regler og slette alle de valgte reglene. Avmerkingsboksen **Aktivert** deaktiverer eller aktiverer en regel. Dette kan være nyttig hvis du ikke vil slette en regel permanent i tilfelle du vil bruke den i fremtiden.

Regler sorteres i en rekkefølge som definerer prioriteringen, med regler med høyest prioritet øverst. Evaluering av regler basert på URL har alltid høyere prioritet enn evaluering basert på kategori. Hvis for eksempel en regel basert på en URL er under en regel basert på kategori i listen over regler, så vil den URL-baserte regelen ha høyere prioritet og evalueres først.

3.9.4.1.1 Legger til nettkontrollregler

I vinduet Nettkontrollregler kan du opprette eller endre den eksisterende filtreringsregelen for nettkontroll.



Angi en beskrivelse av regelen i **Navn**-feltet for bedre å kunne identifisere den. Klikk på bryteren **aktivert** for å deaktivere eller aktivere regelen; dette kan være nyttig hvis du ikke vil slette regelen permanent.

Handlingstype

- **URL-basert handling** – For regler som kontrollerer tilgang til et gitt nettsted, skriv inn URL i feltet **URL**.
- **Kategoribasert handling** – Når du har valgt dette alternativet, må du velge en kategori fra rullegardinmenyen.

Spesialsymbolene * (stjerne) og ? (spørsmålstegn) kan ikke brukes i URL-adresselisten. Når du oppretter en URL-gruppe som inneholder et nettsted med flere toppnivådomener (TLD-er), må hver TLD legges til enkeltvis. Når du legger et domene til listen blir alt innhold på dette domenet og alle underdomener (f.eks. *sub.examplepage.com*) blir sperret eller tillatt basert på ditt valg av URL-basert handling.

Tilgangsrettigheter

- **Tillat** – Tilgang til URL-adressen/kategorien vil bli gitt.
- **Advar** – Advarer om URL-adressen/kategorien.
- **Advar** – Blokkerer URL-adressen/kategorien.

URL eller **Bruk URL-gruppe** – bruker URL-linken eller gruppen av linker for å tillatte, blokkere eller advare brukeren når en av URL-ene oppdages.

Alvorlighetsnivå for logging:

- **Alltid** – Logger all nettkommunikasjon.
- **Diagnostisering** – Logger informasjon som trengs for å finjustere programmet.
- **Informasjon** – Registrerer informative meldinger, inkludert vellykkede oppdateringsmeldinger, pluss alle registreringene ovenfor.
- **Advarsel** – Logger alle kritiske feil og varselsmeldinger.
- **Ingen** – Ingen logger registreres.

Brukerliste

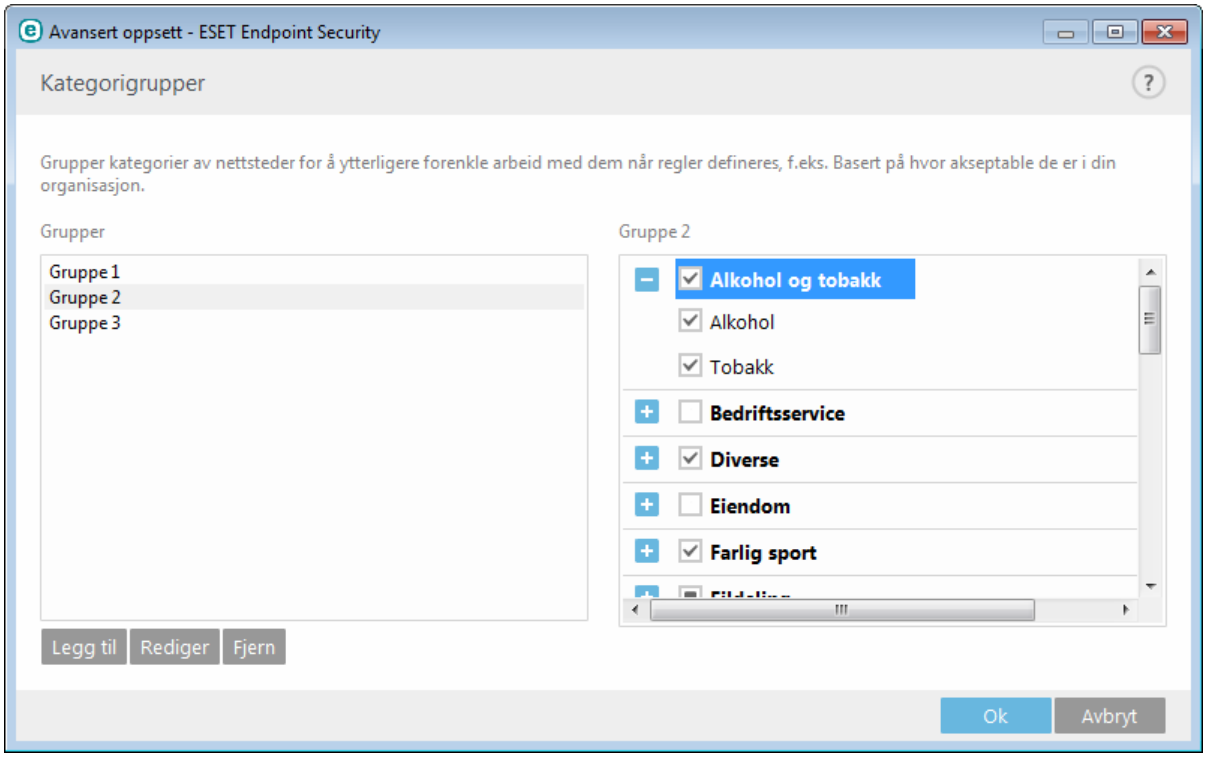
- **Legg til** – Åpner dialogvinduet **Velg brukere eller grupper**. dette vinduet brukes til å velge ønskede brukere. Når ingen bruker er angitt, gjelder regelen for alle brukerne.
- **Fjern** – fjerner den valgte brukeren fra filteret.

3.9.4.2 Kategorigrupper

Vinduet Kategorigrupper er delt inn i to deler. Høyre del av vinduet inneholder en liste over kategorier og underkategorier. Velg en kategori i listen Kategori for å vise underkategoriene.

Hver gruppe inneholder underkategorier med voksent eller generelt upassende innhold. Når du åpner vinduet Kategorigrupper og klikker på den første gruppen, kan du legge til eller fjerne kategorier/underkategorier fra listen med passende gruppe (for eksempel Vold eller Våpen). Nettsteder med upassende innhold kan blokkeres, eller brukere kan informeres etter at en regel med forhåndsdefinerte handlinger er opprettet.

Merk av i avmerkingsboksen for å fjerne en underkategori som tilhører en spesifikk gruppe.



Her er noen eksempler på kategorier som brukere kanskje ikke er kjent med:

Diverse – Vanligvis private (lokale) IP-adresser slik som intranet, 192.168.0.0/16, osv. Når du får en 403- eller 404-feilkode, vil også nettsiden passe inn under denne kategorien.
Ikke løst – Denne kategorien inkluderer nettsider som ikke løses på grunn av en feil ved tilkobling til databasemotoren for Nettkontroll.
Ikke kategorisert – Ukjente nettsteder som ennå ikke er i databasen for Nettkontroll.
Proxier – Nettsider slik som anonymiseringsnettsider, omadresseringsnettsider eller offentlige proxy-servere kan brukes til å få (anonym) tilgang til nettsider som vanligvis blokkeres av Nettkontroll-filteret.
Fildeling – Disse nettsidene inneholder store mengder data, som bilder, filmer eller e-bøker. Det finnes en risiko for at disse sidene inneholder potensielt støtende eller voksent innhold.

MERKNAD: En underkategori kan tilhøre hvilken som helst gruppe. Noen underkategorier er ikke inkludert i forhåndsdefinerte grupper (for eksempel Spill). Legg dem til i ønsket gruppe for å matche dem med ønsket underkategori med nettkontrollfilteret.

3.9.4.3 URL-grupper

Med URL-grupperedigeringen kan du opprette en gruppe som inneholder flere URL-koblinger som du vil opprette en regel for (tillate/ikke tillate et bestemt nettsted).

Klikk for å opprette en ny URL-gruppe, klikk på **Legg til**. Velg en URL-gruppe og klokk **Legg til** for å legge en ny URL-adresse til listen, eller klikk **Importer fra fil** for å importere en fil med URL-adresser (verdier må skilles fra hverandre med et linjeskift, for eksempel *.txt med kodingen UTF-8). Hvis du vil angi en handling som skal utføres for en spesifikk URL-gruppe, åpner du **Regelredigering for nettkontroll**, velger URL-gruppen din ved bruk av rullegardinmenyen, justerer andre parametere og bekrefter ved å trykke **OK**.

MERKNAD: Å sperre eller tillate en bestemt nettside kan være mer nøyaktig enn å sperre eller tillate en hel kategori med nettsider. Vær forsiktig når du endrer disse innstillingene og når du legger til en kategori/nettside i listen.

3.9.5 Oppdatere programmet

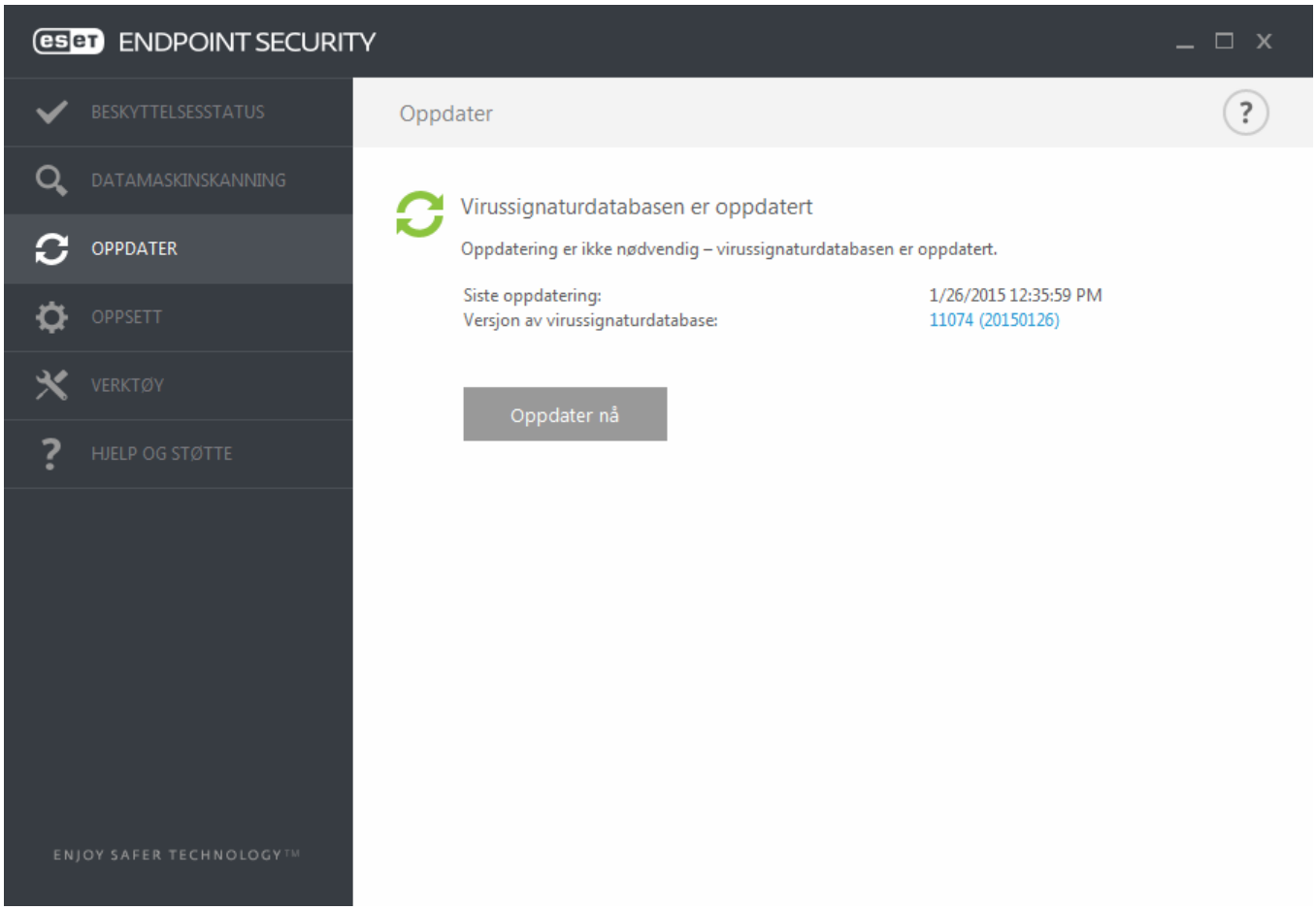
Regelmessig oppdatering av ESET Endpoint Security er den beste måten å oppnå maksimalt sikkerhetsnivå på for datamaskinen. Oppdateringsmodulen har to metoder for å sikre at programmet alltid er oppdatert, ved å oppdatere virussignaturdatabasen og ved å oppdatere systemkomponentene.

Du kan klikke **Oppdater** i hovedvinduet for å finne gjeldende oppdateringsstatus, blant annet dato og klokkeslett for siste vellykkede oppdatering og om en oppdatering er nødvendig. Det primære vinduet inneholder også virussignaturdatabaseversjonen. Denne numeriske indikatoren er en aktiv kobling til ESETs nettside som viser alle signaturer som er lagt til innen en gitt oppdatering.

I tillegg er alternativet å begynne oppdateringsprosessen manuelt, **Oppdater virussignaturdatabase**, tilgjengelig. Oppdatering av virussignaturdatabasen og oppdatering av programkomponentene er en viktig del av å opprettholde full beskyttelse mot skadelig kode. Du bør være oppmerksom på konfigurasjonen og bruken av oppdateringene. Hvis du ikke var inne på lisensinformasjonen under installasjonen, kan du skrive inn lisensnøkkelen ved å klikke på **Aktiver produkt** under oppdateringen for å få tilgang til ESETs oppdateringsservere.

Hvis du aktiverer ESET Endpoint Security med en offline lisensfil uten brukernavn og passord, og prøver å oppdatere, signaliserer den røde informasjonen **Oppdatering av virussignaturdatabasen endte med en feil** at du bare kan laste ned oppdateringer fra speilet.

MERKNAD: Du får lisensnøkkel av ESET etter at du har kjøpt ESET Endpoint Security.

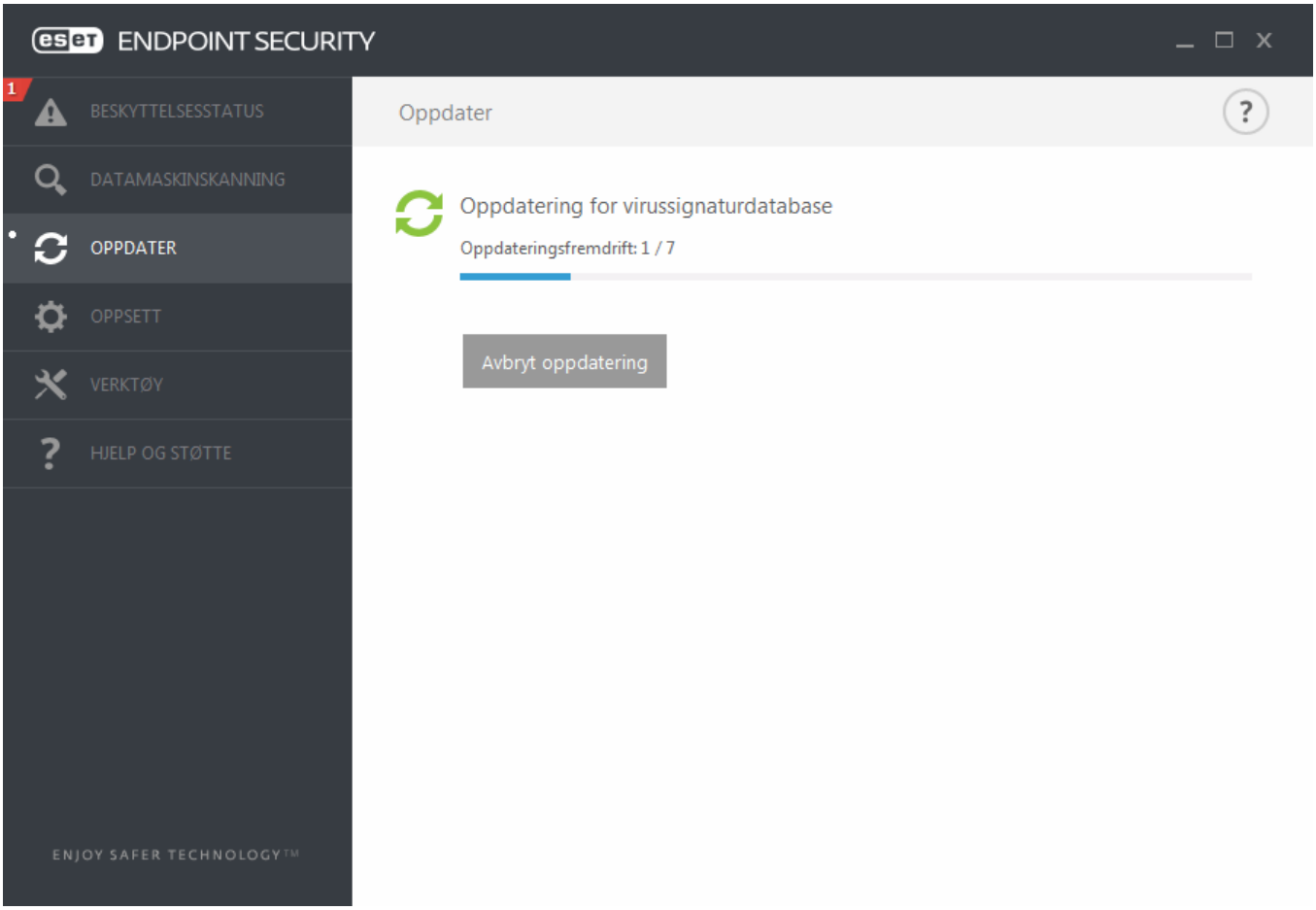


Siste fullførte oppdatering - viser dato for siste oppdatering. Kontroller at den refererer til en nylig dato, dvs. at virussignaturdatabasen nylig er oppdatert.

Virussignaturdatabase – Virussignaturdatabasenummeret, som også er en aktiv kobling til ESETs nettsted. Klikk for å vise en liste over alle signaturer som er lagt til i den gitte oppdateringen.

Oppdateringsprosessen

Nedlastingen starter når du klikker **Oppdater virussignaturdatabasen**. En fremdriftslinje for nedlastingen og gjenstående tid vises. Hvis du vil avbryte oppdateringen, klikker du **Avbryt oppdatering**.

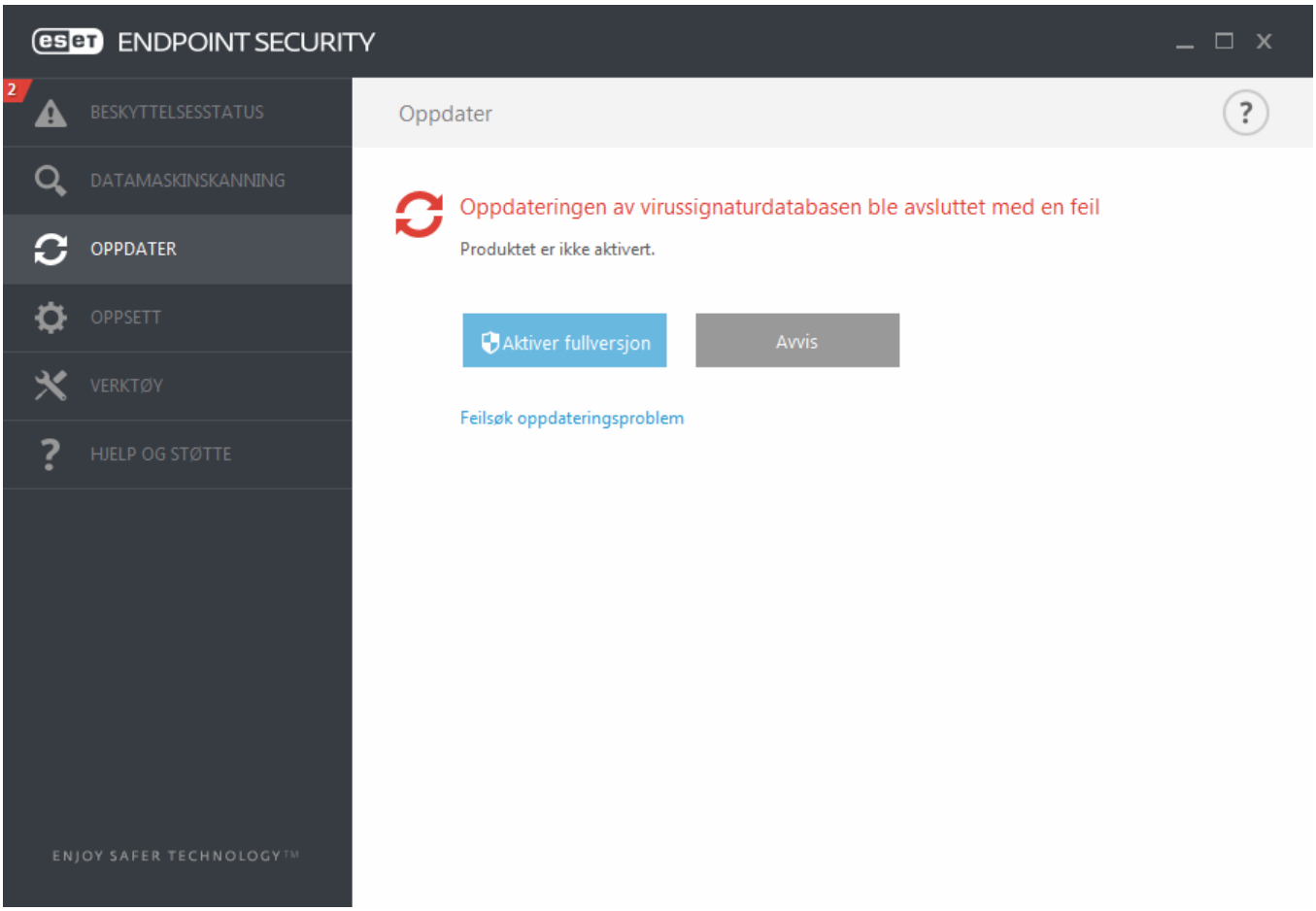


Viktig: Under normale omstendigheter, når oppdateringer blir lastet ned riktig, vises meldingen **Oppdatering ikke nødvendig - virussignaturdatabasen er oppdatert** i vinduet **Oppdater**. Hvis dette ikke er tilfelle, trenger programmet oppdatering og er mer utsatt for infeksjoner. Oppdater virussignaturdatabasen så snart som mulig.

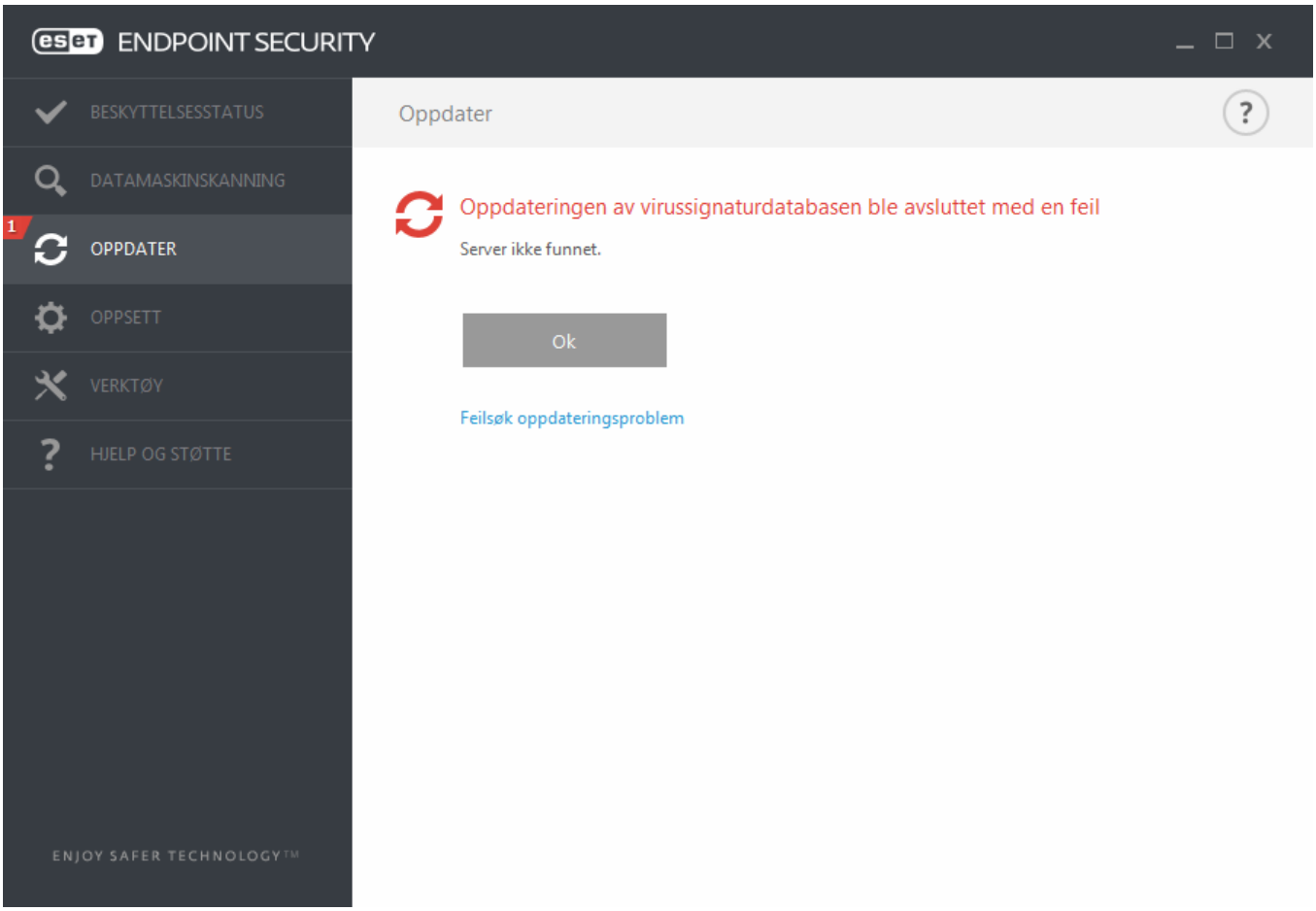
Virussignaturdatabase er utdatert – Denne feilen vil opptre etter flere mislykkede forsøk på å oppdatere virussignaturdatabasen. Vi anbefaler at du kontrollerer oppdateringsinnstillingene. Den vanligste grunnen til denne feilen er feilkonfigurerte tilkoblingsinnstillinger.

Den forrige meldingen er knyttet til de følgende to meldingene **Kunne ikke oppdatere virussignaturdatabasen** om mislykkede oppdateringer:

1. **Ugyldig lisens** – Det er oppgitt feil lisensnøkkel i oppdateringsoppsettet. Vi anbefaler at du kontrollerer godkjenningsdataene dine. Vinduet for Avansert oppsett (klikk **Oppsett** fra hovedmenyen og klikk deretter **Avansert oppsett** eller trykk F5 på tastaturet) inneholder flere oppdateringsalternativer. Klikk på **Hjelp og støtte** > **Håndter lisens** på hovedmenyen for å skrive inn ny lisensnøkkel.



2. **Det oppsto en feil da programmet prøvde å laste ned oppdateringsfiler** - En mulig årsak kan være feil Internett-tilkoblingsinnstillinger. Det anbefales at du kontrollerer Internett-tilkoblingen (for eksempel ved å åpne et vilkårlig nettsted i nettleseren). Hvis nettstedet ikke åpnes, er det sannsynligvis en Internett-tilkobling som ikke er etablert eller tilkoblingsproblemer på tidatamaskinen. Sjekk med Internett-leverandøren (ISP) din om Internett-tilkoblingen din fungerer.



MERKNAD: Hvis du vil ha mer informasjon, kan du gå til ESET Knowledgebase-artikkelen.

3.9.5.1 Oppsett for oppdatering

Alternativene for oppdateringsoppsett er tilgjengelige i treet **Avansert oppsett** (F5) under **Oppdatering** > **Grunnleggende**. Denne delen spesifiserer informasjon om oppdateringskilden, for eksempel oppdateringsservere som brukes og godkjenningsdata for disse serverne.

Generelt

Oppdateringsprofilen som brukes for øyeblikket, vises i rullegardinmenyen **Valgt profil**. For å opprette en ny profil, klikker du **Rediger** ved siden av **Liste over profiler** og klikk deretter **Legg til** og skriv inn ditt eget **Profilnavn**.

Hvis du opplever problemer med en oppdatering når du forsøker å laste ned oppdateringer for virussignaturdatabasen, klikker du på **Slett** for å slette midlertidige oppdateringsfiler/hurtigbuffer.

Varsler for utdatert virussignaturdatabase

Angi maksimal databasealder automatisk – Her kan du angi maksimal tid (i dager) som går før virussignaturdatabase rapporteres som utløpt. Standardverdi er 7.

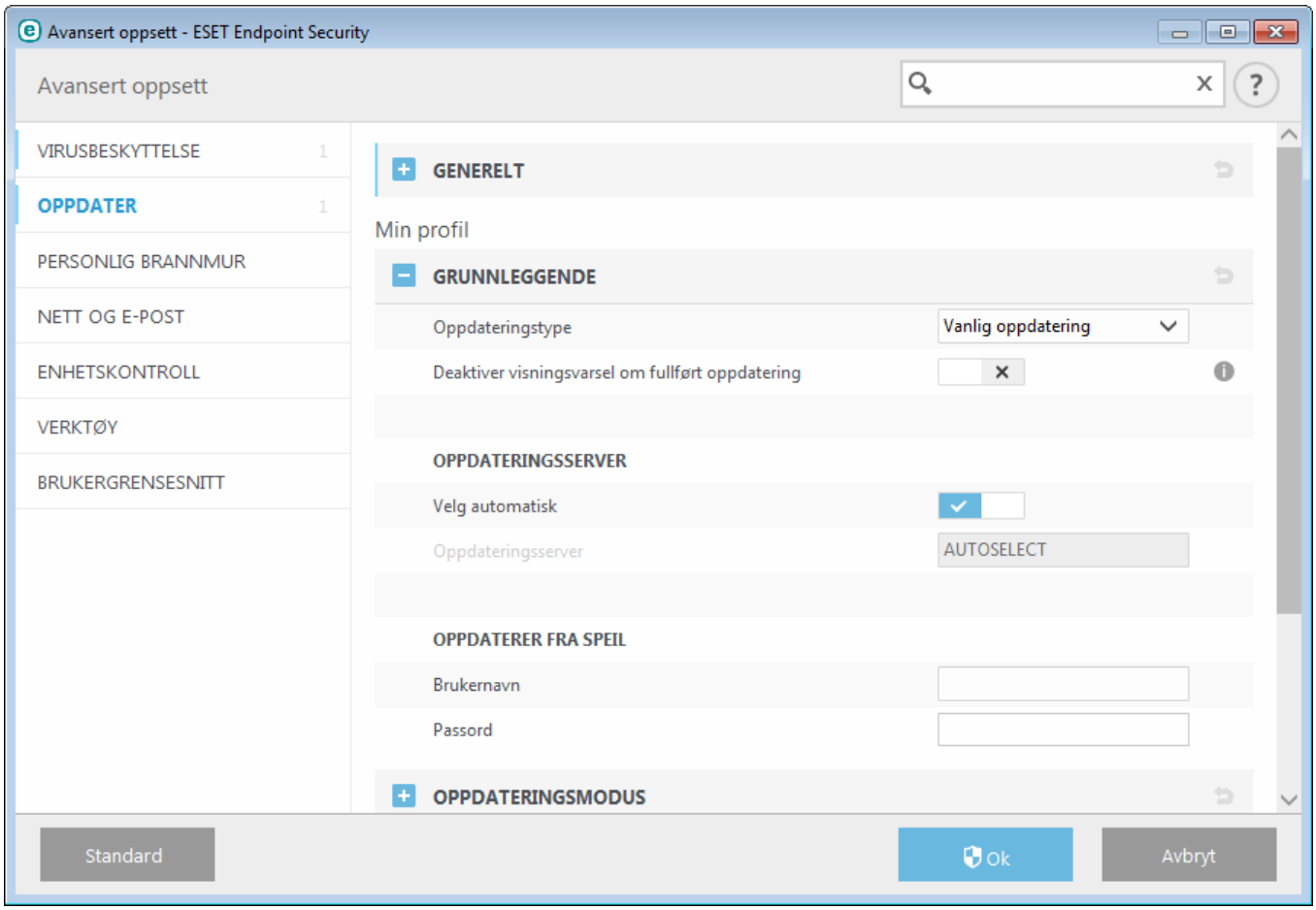
Tilbakerulling

Hvis du mistenker at en ny oppdatering av virusdatabasen og/eller programmoduler kan være ustabil eller skadet, kan du rulle tilbake til forrige versjon og deaktivere eventuelle oppdateringer i en angitt tidsperiode. Alternativt kan du aktivere tidligere deaktiverte oppdateringer hvis du har utsatt dem på ubegrenset tid.

ESET Endpoint Security registrerer avbildninger av virussignaturdatabasen og programmoduler for bruk med

*tilbakerullings*funksjonen. La bryteren **Opprett avbildning av oppdateringsfiler** være aktivert for å opprette avbildninger av virusdatabasen. Feltet **Antall lokalt lagrede avbildninger** definerer antall avbildninger av tidligere virusdatabaser som lagres.

Hvis du klikker **Tilbakestill** (**Avansert oppsett** (F5) > **Oppdater** > **Generelt**), må du velge et tidsintervall fra rullegardinmenyen som viser hvor lenge oppdateringene av virussignaturdatabasen og programmodulene vil være satt på pause.



For at oppdateringer skal lastes ned riktig, er det viktig at du fyller ut alle oppdateringsparameterne riktig. Hvis du bruker en brannmur, må du forsikre deg om at ESET-programmet har tillatelse til å kommunisere med Internett (f.eks. HTTP-kommunikasjon).

Grunnleggende

Ved standard, er **Oppdateringstype** satt til **Vanlig oppdatering** for å sikre at oppdateringsfiler lastes automatisk ned fra den ESET-serveren som har minst nettverkstrafikk. Testoppdateringer (alternativet **Testoppdatering** er oppdateringer som har gjennomgått grundige interne tester og vanligvis vil bli tilgjengelige for alle om kort tid. Du kan dra fordel av å aktivere testoppdateringer ved at du får tilgang til de nyeste oppdagelsesmetodene og løsningene. Det kan imidlertid hende at testoppdateringer ikke er stabile nok hele tiden, og de MÅ IKKE brukes på produksjonsservere og arbeidsstasjoner der maksimal tilgjengelighet og stabilitet er nødvendig. **Forsinket oppdatering** gjør det mulig å oppdatere fra spesielle oppdateringsservere som gir nye versjoner av virusdatabaser en forsinkelse på minst X timer (dette vil si at databasene blir testet i et virkelig miljø og derfor anses som stabile).

Ikke vis melding om gjennomført oppdatering – deaktiverer meldingen i systemstatusfeltet nederst til høyre på skjermen. Det kan være nyttig å velge dette alternativet hvis du kjører et program i fullskjermsmodus, eller hvis du spiller et spill. Vær oppmerksom på at Presentasjonsmodus slår av alle meldinger.

Oppdater fra flyttbart medium – Lar deg oppdatere fra flyttbart medium hvis det inneholder opprettet speil. Når **Automatisk** er valgt, vil oppdateringen kjøre i bakgrunnen. Hvis du vil vise oppdateringsdialoger, velger du **Spør alltid**.

Som standard er menyen **Oppdateringsserver** satt til AUTOMATISK VALG. Oppdateringsserveren er plasseringen hvor oppdateringene er lagret. Hvis du bruker en ESET-server, anbefaler vi at du lar standardalternativet være

markert.

Når du bruker en lokal HTTP-server – også kjent som et speil – må oppdateringsserveren settes opp slik: *http://datamaskinens_navn_eller_IP-adresse:2221.*

Når du bruker en lokal HTTP-server med SSL, må oppdateringsserveren settes opp slik: *https://datamaskinens_navn_eller_IP-adresse:2221.*

Når du bruker en lokal delt mappe, må oppdateringsserveren settes opp slik: *\\datamaskinnavn_eller_dens_IP-adresse\delt_mappe*

Oppdaterer fra speil

Godkjenning for oppdateringsservere er basert på **Lisensnøkkel** og passordet som ble generert og sendt til deg etter at du kjøpte produktet. Når du bruker en lokal speilserver, kan du definere påloggingsinformasjonen som klienter må bruke for å logge seg på speilserveren før du mottar oppdateringer. Standardinnstillingen er at bekreftelse ikke er nødvendig, dvs. at feltene **Brukernavn** og **Passord** er tomme.

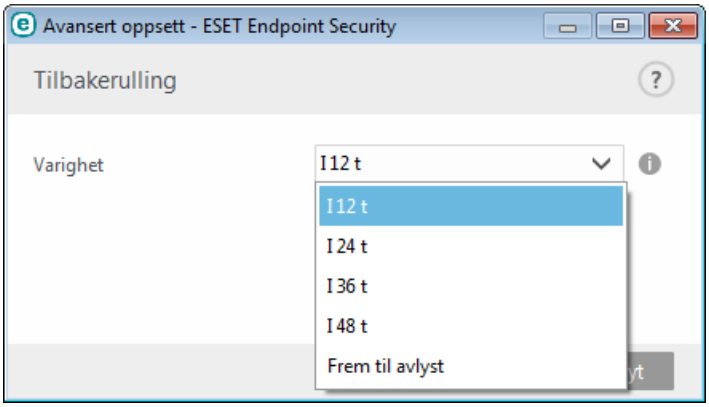
3.9.5.1.1 Oppdateringsprofiler

Oppdateringsprofiler kan opprettes for forskjellige oppdateringskonfigurasjoner og -oppgaver. Det er spesielt nyttig å opprette oppdateringsprofiler for mobile brukere som trenger en alternativ profil for Internett-tilkoblingsegenskaper som regelmessig endres.

Rullegardinmenyen til Valgt profil viser profilen som er valgt for øyeblikket, som standard satt til **Min profil**. For å opprette en ny profil, klikker du **Rediger** ved siden av **Liste over profiler** og klikk deretter **Legg til** og skriv inn ditt eget **Profilnavn**.

3.9.5.1.2 Oppdater gjenoppretting

Hvis du klikker **Tilbakestill** (**Avansert oppsett** (F5) > **Oppdater** > **Profil**), må du velge et tidsintervall fra rullegardinmenyen som viser hvor lenge oppdateringene av virussignaturdatabasen og programmodulene vil være satt på pause.



Velg **Til tilbakekallelse** for å utsette regelmessige oppdateringer inntil du manuelt gjenoppretter oppdateringsfunksjonaliteten. Fordi det utgjør en potensiell sikkerhetsrisiko, anbefaler vi ikke at du velger dette alternativet.

Versjonen av virussignaturdatabasen blir nedgradert til den eldste tilgjengelige og lagret som en avbildning i filsystemet på den lokale datamaskinen.

Eksempel: La nummer 10646 være den nyeste versjonen av virussignaturdatabasen. 10645 og 10643 blir lagret som avbildninger av en virussignaturdatabase. Merk at 10644 ikke er tilgjengelig fordi, for eksempel, datamaskinen var slått av og en nyere oppdatering ble gjort tilgjengelig før 10644 ble lastet ned. Hvis du har angitt 2 i feltet **Antall lokalt lagrede avbildninger** og klikker **Tilbakestill**, blir virussignaturdatabasen (inkludert programmoduler) gjenopprettet til versjonsnummer 10643. Denne prosessen kan ta litt tid. Kontroller om versjonen av virussignaturdatabasen er nedgradert fra hovedvinduet i ESET Endpoint Security i delen oppdater.

3.9.5.1.3 Oppdateringsmodus

Kategorien **Oppdateringsmodus** inneholder alternativer relatert til oppdatering av programkomponenter. Programmet lar deg forhåndsdefinere virkemåte hvis en ny oppdatering til en programkomponent er tilgjengelig.

Oppdateringene av programkomponentene innfører nye funksjoner eller endrer eksisterende funksjoner fra tidligere versjoner. Den kan utføres automatisk uten at brukeren må foreta seg noe, eller du kan velge å bli varslet. Etter at en oppdatering av en programkomponent er installert, er det mulig at du må starte datamaskinen på nytt. I delen **Oppdatering av programkomponent** er tre alternativer tilgjengelig:

- **Spør før nedlasting av programkomponenter** – Standardalternativet. Du blir bedt om å bekrefte eller avvise programkomponentoppdateringer når de blir tilgjengelige.
- **Alltid oppdater programkomponenten** – En oppdatering av programkomponenter blir lastet ned og installert automatisk. Husk at det kan være nødvendig å starte datamaskinen på nytt.
- **Aldri oppdater programkomponenter** – Oppdatering av programkomponenter blir ikke utført. Dette alternativet er egnet for serverinstallasjoner, ettersom servere vanligvis kun startes på nytt når de blir vedlikeholdt.

MERKNAD: Hvilket alternativ som passer best, avhenger av arbeidsstasjonen der innstillingene skal brukes. Vær oppmerksom på at det er forskjeller mellom arbeidsstasjoner og servere – for eksempel kan automatisk omstart av serveren etter en programoppdatering forårsake alvorlig skade.

Hvis alternativet **Spør før nedlasting av oppdatering** er aktivert, vises det en varsling når en ny oppdatering er tilgjengelig.

Hvis størrelsen på oppdateringsfilen er større enn verdien som er angitt i feltet **Spør hvis en oppdateringsfil er større enn (kB)**, vises det en melding.

3.9.5.1.4 HTTP-proxy

Du får tilgang til oppsettalternativene for proxy-servere for en bestemt oppdateringsprofil ved å klikke **Oppdater** i treet for **Avansert oppsett** (F5), og deretter klikke **HTTP-proxy**. Klikk rullegardinmenyen **Proxy-modus** og velg et av følgende alternativer:

- Ikke bruk proxy-server
- Tilkobling gjennom proxy-server
- Bruk globale innstillinger for proxy-server

Hvis du velger alternativet **Bruk globale innstillinger for proxy-server**, brukes proxy-serverkonfigurasjonen som allerede er definert i forgreningen **Verktøy** > **Proxy-server** i treet for avansert oppsett.

Velg alternativet **Ikke bruk proxy-server** for å spesifisere at det ikke skal brukes proxy-server for oppdatering av ESET Endpoint Security.

Alternativet **Tilkobling via proxy-server** skal velges hvis:

- En proxy-server må brukes ved oppdatering av ESET Endpoint Security, og serveren er en annen enn proxy-serveren som er spesifisert i de globale innstillingene (**Verktøy** > **Proxy-server**). I så fall må innstillingene angis her: Adresser for Proxy-server, Port for kommunikasjon (standard 3128 er), pluss Brukernavn og Passord for proxy-serveren, om nødvendig.
- Proxy-serverinnstillingene har ikke blitt spesifisert globalt, men ESET Endpoint Security skal koble seg til en proxy-server ved oppdatering.
- Datamaskinen er koblet til Internett via en proxy-server. Innstillingene hentes fra Internet Explorer under installasjonen av programmet. Hvis innstillingene senere blir endret (for eksempel hvis du bytter Internett-leverandør), må du kontrollere at HTTP-proxyinnstillingene i dette vinduet er korrekte. Ellers kan ikke programmet koble seg til oppdateringsserverne.

Standardinnstillingen for proxy-serveren er **Bruk globale innstillinger for proxy-server**.

MERKNAD: Godkjenningsdata som **Brukernavn** og **Passord** er ment å skulle brukes til å få tilgang til proxy-serveren. Du skal bare fylle ut disse feltene hvis brukernavn og passord er påkrevd. Vær oppmerksom på at disse feltene ikke skal brukes med brukernavnet/passordet for ESET Endpoint Security, og skal bare fylles inn hvis du vet at du trenger

passord for å få tilgang til Internett via en proxy-server.

3.9.5.1.5 Koble til LAN som

Ved oppdatering fra en lokal server med en versjon av Windows NT-operativsystemet, er godkjenning for hver nettverkstilkobling påkrevd som standard.

For å konfigurere en slik konto, velger du fra rullgardinmenyen **Lokal brukertype**:

- **Systemkonto (standard)**,
- **Gjeldende bruker**,
- **Spesifisert bruker**.

Velg **Systemkonto (Standard)** for å bruke systemkontoen til godkjenning. Vanligvis skjer det ingen godkjenningsprosess hvis det ikke er oppgitt godkjenningsdata i hovedoppdateringsoppsettet.

For å sikre at programmet godkjennes med en brukerkonto som er pålogget for øyeblikket velger du **Gjeldende bruker**. Ulempen med denne løsningen er at programmet ikke kan koble til oppdateringsserveren med mindre en bruker er logget på.

Velg **Spesifisert bruker** hvis du vil at programmet skal bruke en spesifisert brukerkonto for godkjenning. Bruk denne metoden når standardtilkoblingen til systemkontoen mislykkes. Vær oppmerksom på at den spesifiserte brukerkontoen må ha tilgang til katalogen med oppdateringsfilene på den lokale serveren. Ellers klarer ikke programmet å opprette en tilkobling og laste ned oppdateringer.

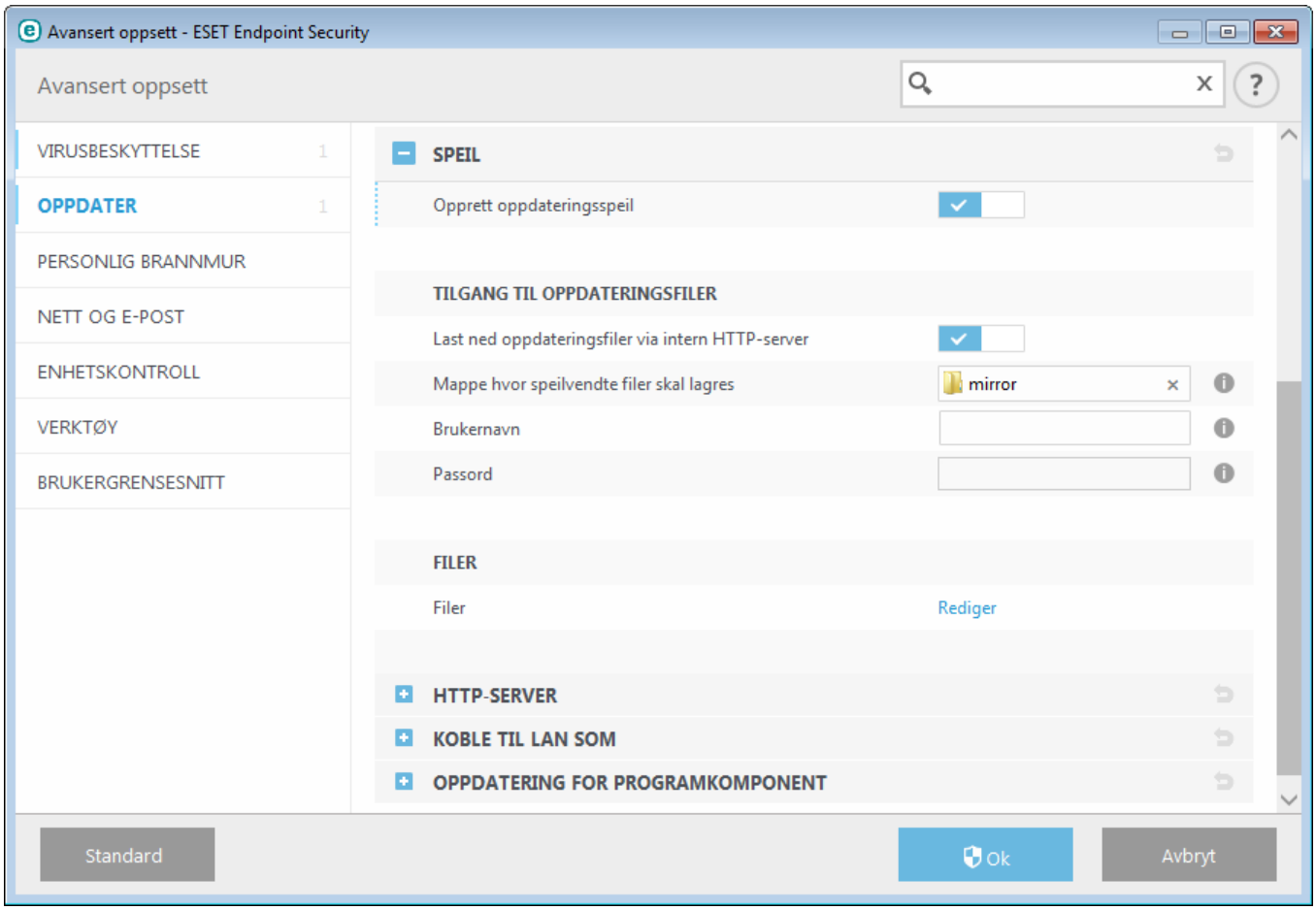
Advarsel: Når et av alternativene **Gjeldende bruker** eller **Spesifisert bruker** er valgt, kan det oppstå en feil når programmets identitet endres til den ønskede brukeren. Vi anbefaler å registrere godkjenningsdataene for LAN i hoveddelen for oppdateringsoppsett. I dette oppdateringsoppsettet skal godkjenningsdata angis som følger: *domenenavn**bruker* (hvis det er en arbeidsgruppe, skriver du *arbeidsgruppenavn**navn*) og passord. Ved oppdatering fra HTTP-versjonen av den lokale serveren er det ikke nødvendig med godkjennelse.

Velg alternativet **Koble fra konto etter oppdatering** for å tvinge frem en frakobling hvis en tilkobling til serveren forblir aktiv også etter at oppdateringene er lastet ned.

3.9.5.1.6 Speil

Med ESET Endpoint Security kan du opprette kopier av oppdateringsfiler som kan brukes til å oppdatere andre arbeidsstasjoner i nettverket. Opprettelse av *«speil»* – en kopi av oppdateringsfilene i et LAN-miljø er praktisk, siden oppdateringsfilene ikke trenger å lastes ned fra leverandørens oppdateringsserver gjentatte ganger av hver arbeidsstasjon. Oppdateringene lastes ned til en lokal speilserver, og deretter distribueres de til alle arbeidsstasjonene. Dermed hindres en mulig risiko for overbelastning av nettverket. Når klientarbeidsstasjoner oppdateres fra en speilserver, optimaliseres belastningsfordelingen i nettverket, og man sparer båndbredde for Internett-tilgang.

Konfigurasjonsalternativer for den lokale speilserveren er tilgjengelig i Avansert oppsett under **Oppdater**. For å gå inn på denne delen, trykk på **F5** for å gå inn på Avansert oppsett, klikk på **Oppdater** og velg fanen **Speil**.



For å opprette et speil på en klients arbeidsstasjon, aktiver **Opprett oppdateringsspeil**. Når du velger dette alternativet, aktiveres andre alternativer for speilkonfigurasjon, for eksempel måten man får tilgang til oppdateringsfiler på og oppdateringsbanen til speilede filer.

Tilgang til oppdateringsfiler

Last ned oppdateringsfiler via intern HTTP-server – Hvis dette er aktivert, kan du enkelt få tilgang til oppdateringsfiler via HTTP uten å måtte oppgi brukernavn og passord.

MERKNAD: Windows XP Service Pack 2 eller nyere bruker HTTP-server.

Metodene som brukes til å få tilgang til Speil-serveren er beskrevet i detalj i avsnittet Oppdatering fra speilet. Det er to grunnleggende måter å få tilgang til speilet på – mappen med oppdateringsfiler kan presenteres som en delt nettverksmappe eller klienter kan få tilgang til speilet på en HTTP-server.

Mappen som er dedikert til lagring av oppdateringsfiler for speilet, er definert i delen **Mappe hvor speilede filer skal lagres**. Klikk **Mappe** for å finne en mappe på den lokale datamaskinen eller en delt nettverksmappe. Hvis godkjenning kreves for den angitte mappen, angis godkjenningsdata i feltene **Brukernavn** og **Passord**. Hvis den valgte målmappen ligger på en nettverksdisk som kjører operativsystemet Windows NT/2000/XP, må angitt brukernavn og passord ha skrivetilgang til den valgte mappen. Brukernavnet og passordet skal angis med formatet *Domene/Bruker* eller *Arbeidsgruppe/Bruker*. Husk å bruke riktig passord for brukernavnet som oppgis.

Filer – Når speilet skal konfigureres, kan du også angi for hvilke språkversjoner du vil laste ned oppdateringskopier. Valgte språk må støttes av speilserveren brukeren har konfigurert.

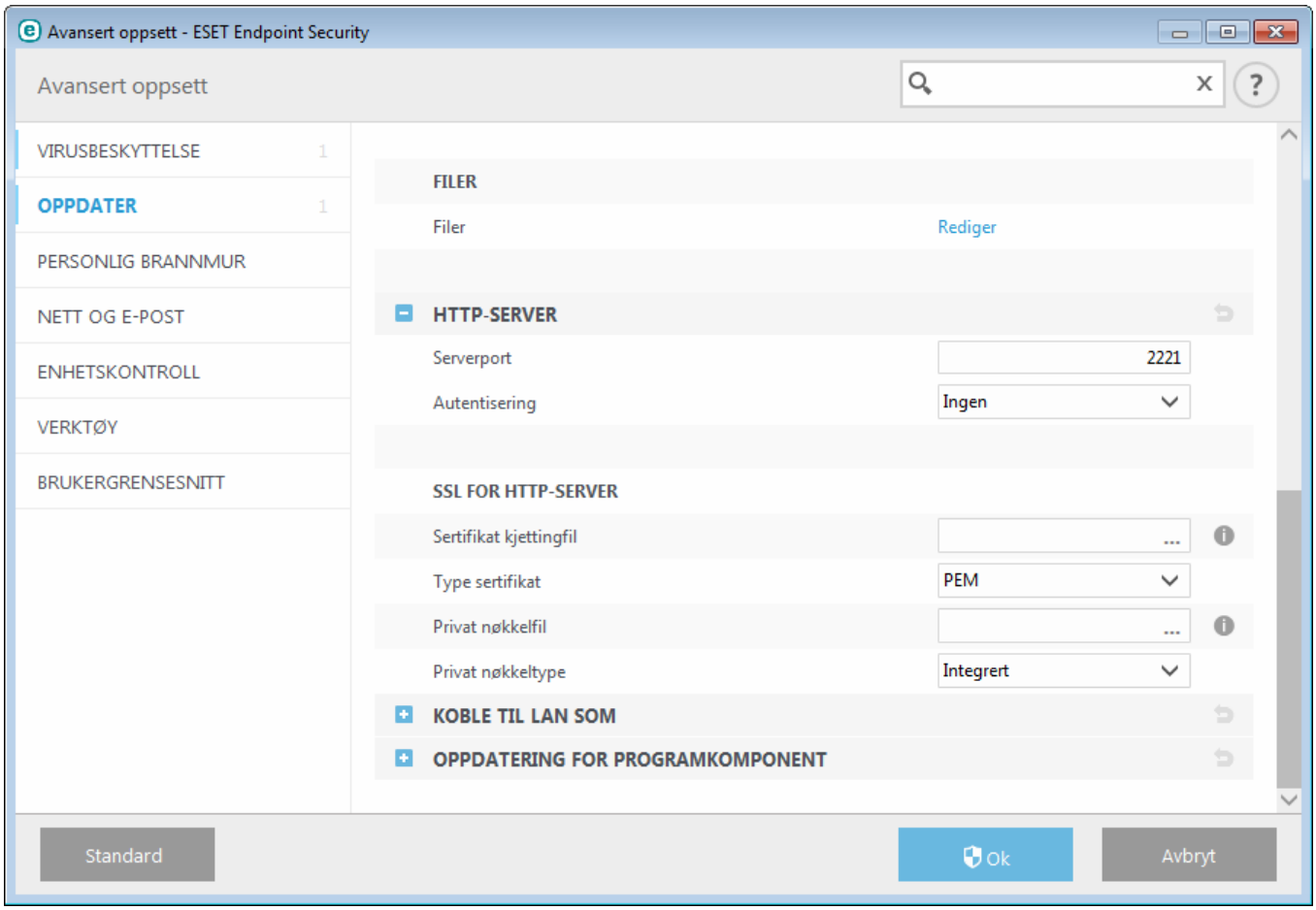
HTTP-server

Serverport – Serverporten er som standard satt til 2221.

Godkjenning – Definerer godkjenningsmetoden som skal brukes for tilgang til oppdateringsfilene. Følgende alternativer er tilgjengelige: **Ingen**, **Grunnleggende** og **NTLM**. Velg **Grunnleggende** for å bruke base64-kryptering med grunnleggende autentisering av brukernavn og passord. Alternativet **NTLM** gir kryptering med en trygg krypteringsmetode. Autentiseringen bruker brukeren som er opprettet på arbeidsstasjonen og som deler oppdateringsfilene. Standardinnstillingen er **Ingen**, noe som gir tilgang til oppdateringsfilene uten behov for

autentisering.

Legg ved **Sertifikat kjettingfil** eller generer et selvsignert sertifikat hvis du vil kjøre HTTP-serveren med støtte for HTTPS (SSL). Følgende sertifikattyper er tilgjengelige: ASN, PEM og PFX. For ytterligere sikkerhet, kan du bruke HTTPS-protokollen til å laste ned oppdateringsfiler. Det er nesten umulig å spore dataoverføringer og påloggingsinformasjon med denne protokollen. Alternativet **Privat nøkkeltype** er satt til **Integrert** som standardinnstilling, og derfor er **Privatnøkkelfil**-alternativet er deaktivert som standard). Dette betyr at den private nøkkelen er en del av den valgte sertifikatkjettingfilen.



Koble til LAN som

Lokal brukertype – Innstillingene **Systemkonto (standard)**, **Gjeldende bruker** og **Spesifisert bruker** finner du i de korresponderende rullegardinmenyene. Innstillingene **Brukernavn** og **Passord** er valgfrie. Se Koble til LAN som.

Velg **Koble fra konto etter oppdatering** for å tvinge frem en frakobling hvis en tilkobling til serveren forblir aktiv etter at oppdateringene er lastet ned.

Oppdatering av programkomponent

Automatisk oppdatering av komponent – Lar brukeren installere nye funksjoner og oppdateringer for eksisterende funksjoner. En oppdatering kan utføres automatisk uten at brukeren må foreta seg noe, eller du kan velge å bli varslet. Etter at en oppdatering av en programkomponent er installert, er det mulig at du må starte datamaskinen på nytt.

Oppdater komponenter nå – Oppdaterer programkomponentene til den nyeste versjonen.

3.9.5.1.6.1 Oppdatering fra speilet

Det finnes to grunnleggende metoder for å konfigurere et speil, som er et repositorium der klienter kan laste ned oppdateringsfiler. Mappen med oppdateringsfiler kan presenteres som en delt nettverksmappe eller som en HTTP-server.

Tilgang til speilet med en intern HTTP-server

Denne konfigurasjonen er standardkonfigurasjonen som er angitt i den forhåndsdefinerte programkonfigurasjonen. For å gi tilgang til speilet med bruk av HTTP-serveren, går du til **Avansert oppsett**> **Oppdater** > **Speil** og velg **Opprett oppdateringsspeil**.

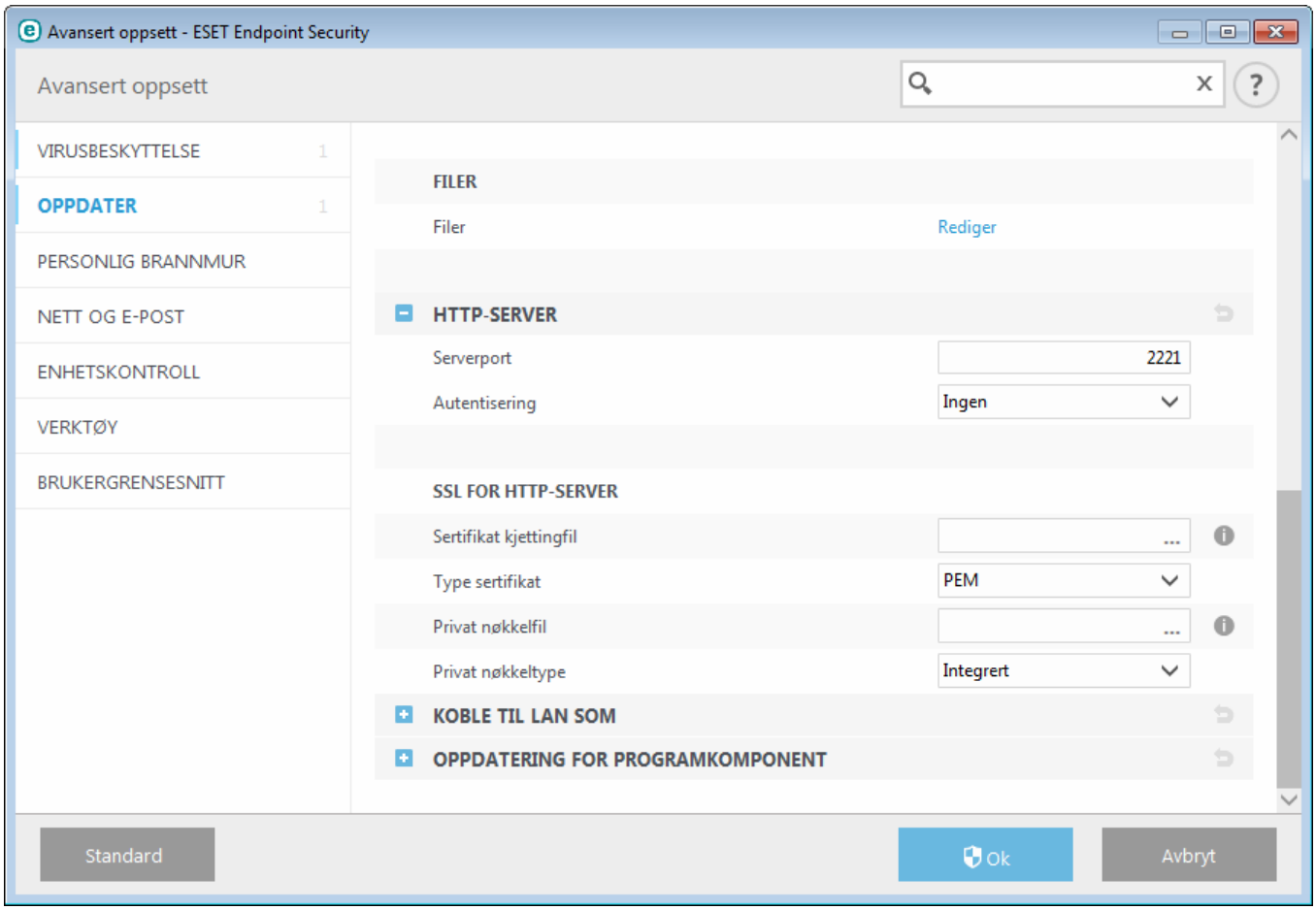
I seksjonen **HTTP-server i kategorien Speil** kan du spesifisere **Serverport** som HTTP-serveren skal lytte til, i tillegg til typen **Godkjenning** som brukes av HTTP-serveren. Serverporten er som standard satt til **2221**. Alternativet **Autentisering** definerer godkjenningsmetoden som skal brukes for tilgang til oppdateringsfilene. Følgende alternativer er tilgjengelige: **Ingen**, **Grunnleggende** og **NTLM**. Velg **Grunnleggende** for å bruke base64-kryptering med grunnleggende autentisering av brukernavn og passord. Alternativet **NTLM** gir kryptering med en trygg krypteringsmetode. Autentiseringen bruker brukeren som er opprettet på arbeidsstasjonen og som deler oppdateringsfilene. Standardinnstillingen er **Ingen**, noe som gir tilgang til oppdateringsfilene uten behov for autentisering.

Advarsel: Hvis du vil gi tilgang til oppdateringsfiler via HTTP-serveren, må speilmappen være på samme datamaskin som ESET Endpoint Security-forekomsten som oppretter den.

SSL for HTTP-server

Legg ved **Sertifikat kjettingfil** eller generer et selvsignert sertifikat hvis du vil kjøre HTTP-serveren med støtte for HTTPS (SSL). Følgende sertifikattyper er tilgjengelige: **PEM, PFX** og **ASN**. For ytterligere sikkerhet, kan du bruke HTTPS-protokollen til å laste ned oppdateringsfiler. Det er nesten umulig å spore dataoverføringer og påloggingsinformasjon med denne protokollen. **Privat nøkkeltype** er satt til **Integrert** som standard. Dette betyr at den private nøkkelen er en del av den valgte sertifikatkjettingfilen.

MERKNAD: Feilen **Ugyldig brukernavn og/eller passord** vises i oppdateringsvinduet på hovedmenyen etter flere mislykkede forsøk på å oppdatere virussignaturdatabasen fra speilet. Vi anbefaler at du går til **Avansert oppsett** > **Oppdater** > **Speil** og kontrollerer brukernavn og passord. Den vanligste grunnen til denne feilen er feil innskrevne godkjenningsdata.



Etter at Speil-serveren er konfigurert, må du legge til den nye oppdateringsserveren på klientarbeidsstasjoner. Gjør dette ved å følge fremgangsmåten under:

- Gå inn på **Avansert oppsett** (F5) og klikk på **Oppdater** > **Grunnleggende**.
- Deaktiver **Velg automatisk** og legg til en ny server i feltet **Oppdateringsserver** ved å bruke ett av følgende formater:
  http://IP_adresse_til_din_server:2221
  https://IP_address_of_your_server:2221 (hvis SSL brukes)

Tilgang til speilet via systemressurser

Først må du opprette en delt mappe på en lokal stasjon eller nettverksstasjon. Når du oppretter mappen for speilet, må du gi *skrivetilgang* til brukeren som skal lagre oppdaterte filer i mappen, og *lesetilgang* til alle brukere som skal oppdatere ESET Endpoint Security fra speilmappen.

Deretter konfigurerer du tilgang til speilet i **Avansert oppsett** > **Oppdater** > **Speil** ved å deaktivere **>Last ned oppdateringsfiler via intern HTTP-server**. Dette alternativet er aktivert som standard i programinstallasjonspakken.

Hvis den delte mappen ligger på en annen datamaskin i nettverket, må du angi godkjenningsdata for tilgang til den andre datamaskinen. Du angir godkjenningsdata ved å åpne ESET Endpoint Security **Avansert oppsett** (F5) og klikke **Oppdater** > **Koble til LAN som**. Dette er den samme innstillingen som brukes til oppdatering, som beskrevet i avsnittet Koble til LAN som.

Etter at speilkonfigurasjonen er fullført, fortsetter du med arbeidsstasjonene og angir *UNC**PATH* som oppdateringsserver ved å følge trinnene nedenfor:

1. Åpne ESET Endpoint Security **Avansert oppsett** og klikk **Oppdater** > **Grunnleggende**.
2. Klikk feltet **oppdateringsserver** og legg til en ny server ved bruk av *UNC**PATH*-formatet.

MERKNAD: For oppdateringene skal fungere riktig, må banen til speilmappen være angitt som en UNC-bane. Oppdateringer fra tilordnede stasjoner vil kanskje ikke fungere.

Den siste delen styrer programkomponenter (PCU-er). Som standard er nedlastede programkomponenter klargjort

for å kopiere til lokal speilserver. Hvis **Oppdatering for programkomponent** er valgt, trenger du ikke å klikke **Oppgrader komponenter** fordi filene kopieres automatisk til den lokale speilserveren når de er tilgjengelige. Se Oppdateringsmodus hvis du ønsker mer informasjon om oppdatering av programkomponenter.

3.9.5.1.6.2 Feilsøking av oppdateringsproblemer med speil

I de fleste tilfeller blir problemer som oppstår under oppdatering fra en speilserver, forårsaket av noe av følgende: feil angivelse av alternativer for speilmappe, feil autentiseringsdata til speilmappen, feil konfigurasjon av lokale arbeidsstasjoner som prøver å laste ned oppdateringsfiler fra speilet, eller en kombinasjon av årsakene over. Under gir vi en oversikt over de vanligste problemene som kan oppstå ved oppdatering fra speilet:

ESET Endpoint Security rapporterer om feil ved tilkobling til speilserveren – Sannsynligvis forårsaket av feil angivelse av oppdateringsserveren (feil nettverksbane til speilmappen) som den lokale arbeidsstasjonen laster ned oppdateringer fra. Bekreft mappen ved å klikke **Start**-menyen i Windows, klikke **Kjør**, angi mappenavnet og klikke **OK**. Innholdet i mappen skal vises.

ESET Endpoint Security krever et brukernavn og passord – sannsynligvis forårsaket av feil godkjenningsdata (brukernavn og passord) i oppdateringsdelen. Brukernavnet og passordet brukes til å gi tilgang til oppdateringsserveren som programmet oppdateres fra. Forsikre deg om at autentiseringsdataene er riktige og angitt i riktig format. Eksempler er *Domene/Brukernavn*, eller *Arbeidsgruppe/Brukernavn*, pluss de tilhørende passordene. Hvis speilserveren er tilgjengelig for "Alle", må du være klar over at dette ikke betyr at alle brukere får tilgang. "Alle" betyr ikke alle uautoriserte brukere, det betyr bare at mappen er tilgjengelig for alle brukerne av domenet. Brukerne må derfor oppgi brukernavn og passord i oppsettdelen av oppdateringen, selv om mappen er tilgjengelig for "Alle".

ESET Endpoint Security rapporterer en feil ved tilkobling til speilserveren – kommunikasjon på porten som er definert for tilgang til HTTP-versjonen av speilet, er blokkert.

3.9.5.2 Slik lager du oppdateringsoppgaver

Oppdateringer kan aktiveres manuelt ved å klikke **Oppdater virussignaturdatabase** i hovedvinduet som vises etter å ha klikket **Oppdater** i hovedmenyen.

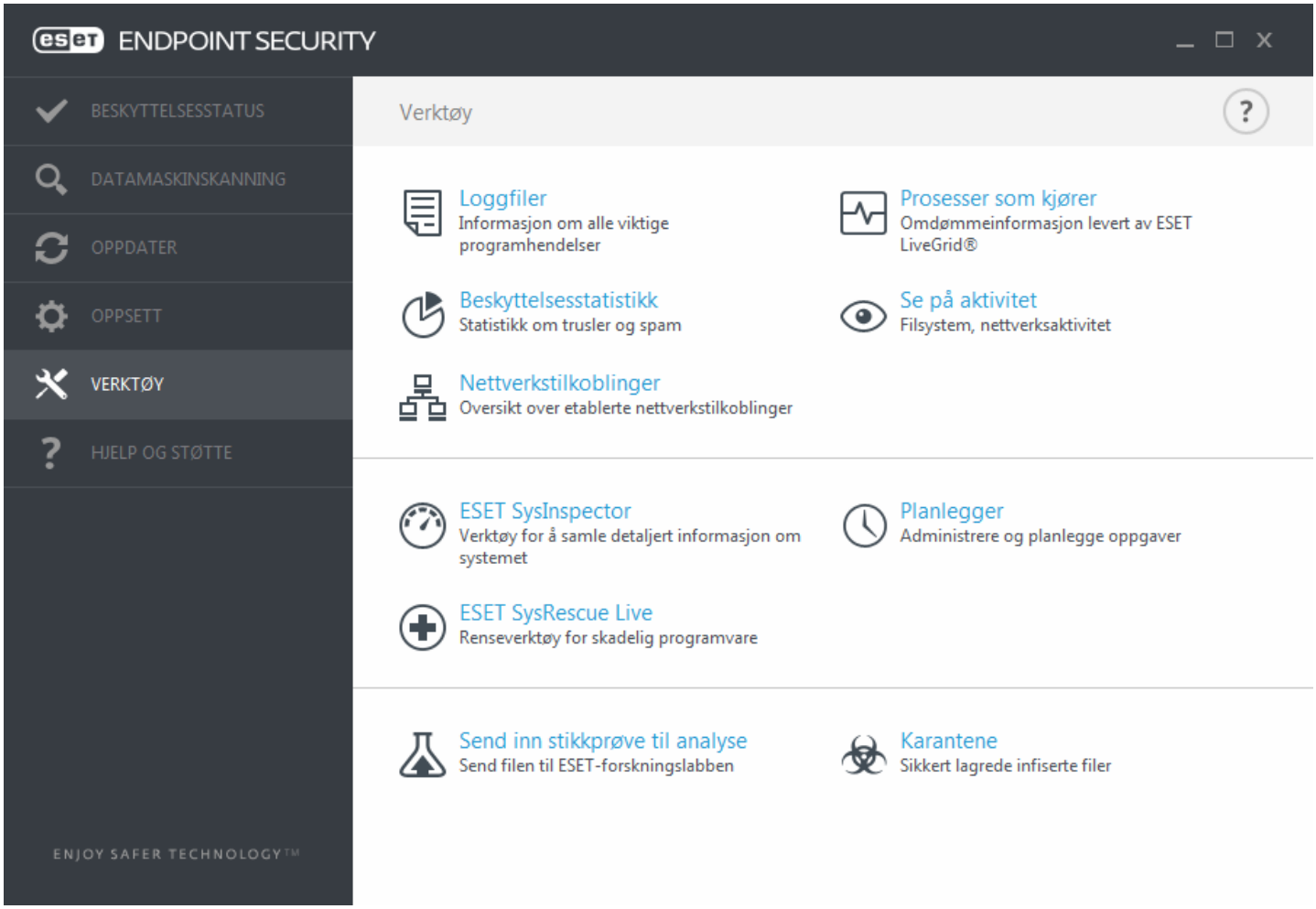
Oppdateringer kan også kjøres som planlagte oppgaver. Klikk **Verktøy** > **Planlegger** for å konfigurere en planlagt oppgave. Som standard er følgende oppgaver aktivert i ESET Endpoint Security :

- **Vanlig automatisk oppdatering**
- **Automatisk oppdatering etter oppringt tilkobling**
- **Automatisk oppdatering etter brukerpålogging**

Hver oppdateringsoppgave kan endres etter dine behov. I tillegg til standardiserte oppdateringsoppgaver kan du opprette nye oppdateringsoppgaver med en brukerdefinert konfigurasjon. Hvis du vil vite mer om hvordan du oppretter og konfigurerer oppdateringsoppgaver, kan du se Planlegger.

3.9.6 Verktøy

Verktøy-menyen inneholder moduler som bidrar til å forenkle programadministrasjon og inneholder ytterligere alternativer for avanserte brukere.



Denne menyen inneholder følgende verktøy:

- Loggfiler
- Beskyttelsesstatistikk
- Se på aktivitet
- Prosesser som kjører (hvis ESET Live Grid er aktivert i ESET Endpoint Security)
- Planlegger
- Karantene
- Nettverkstilkoblinger (ved er aktivert i ESET Endpoint Security)
- ESET SysInspector

Send fil til analyse – Lar deg sende en mistenkelig fil til analyse ved ESETs forskningslaboratorium. Dialogvinduet som vises når du klikker dette alternativet, er beskrevet under innsending av fil til analyse.

ESET SysRescue – Omdirigerer deg til ESET SysRescue Live-siden, der du kan laste ned ESET SysRescue Live-bildet eller Live CD/USB Creator til operativsystem med Microsoft Windows.

3.9.6.1 Loggfiler

Loggfiler inneholder informasjon om viktige programhendelser som har skjedd, og gir en oversikt over trusler som er oppdaget. Logger er et viktig verktøy ved systemanalyse, trusseloppdagelse og feilsøking. Loggføring utføres aktivt i bakgrunnen uten at brukeren trenger å foreta seg noe. Informasjonen registreres basert på gjeldende innstillinger for loggdetaljnivå. Det er mulig å vise tekstmeldinger og logger direkte i ESET Endpoint Security-miljøet. Det er også arkivere loggfiler.

Loggfiler er tilgjengelige fra hovedvinduet ved å klikke **Verktøy** > **Loggfiler**. Velg ønsket loggtype fra rullegardinmenyen **Logg**. Følgende loggtyper er tilgjengelige:

- **Oppdagede trusler** – Trusselloggen tilbyr detaljert informasjon om infiltrasjoner oppdaget av ESET Endpoint Security-moduler. Informasjonen inkluderer tidspunkt for oppdagelse, navn på infiltrasjon, plassering, utført handling og navn på brukeren som var pålogget på tidspunktet da infiltrasjonen ble oppdaget. Dobbeltklikk en loggoppføring for å vise detaljert innhold i et separat vindu.
- **Hendelser** – Alle viktige handlinger som utføres av ESET Endpoint Security, registreres i hendelsesloggene. Hendelsesloggen inneholder informasjon om hendelser og feil som har oppstått i programmet. Den er utformet for å hjelpe systemadministratorer og brukere med å løse problemer. Ofte kan informasjon som finnes her, hjelpe deg med å finne en løsning på et problem som oppstår i programmet.
- **Datamaskinskanninger** – Alle skanneresultater vises i dette vinduet. Hver linje tilsvarer en enkel datakontroll. Dobbeltklikk en oppføring for å vise detaljer om den respektive skanningen.
- **HIPS** – Inneholder poster med bestemte regler som er merket for registrering. Protokollen viser programmet som kalte opp operasjonen, resultatet (om regelen var tillatt eller forbudt) og navnet på den opprettede regelen.
- **Personlig brannmur** – Brannmurloggen viser alle eksterne angrep oppdaget av den personlige brannmuren. Her finner du informasjon om alle angrep mot datamaskinen. Kolonnen *Hendelse* viser de oppdagede angrepene. Kolonnen *Kilde* forteller deg mer om angriperen. Kolonnen *Protokoll* avslører kommunikasjonsprotokollen brukt til angrepet. Analyse av brannmurloggen kan hjelpe deg med å oppdage systeminfiltrasjonsforsøk i tide til å forhindre uautorisert tilgang til systemet. Hvis du ønsker mer informasjon om nettverksangrep, se IDS og avanserte alternativer.
- **Filtrerte nettsteder** – Denne listen er nyttig hvis du ønsker å se en liste over nettsteder som har blitt blokkert av Beskyttelse for nettilgang eller Nettkontroll. I disse loggene kan du se tidspunktet, URL-en, brukeren og programmet som åpnet en tilkobling til det aktuelle nettstedet.
- **Spambeskyttelse** – Inneholder poster knyttet til e-postmeldinger som var merket som spam.
- **Nettkontroll** – Viser sperrede eller tillatte URL-adresser og detaljer om hvordan de er kategorisert. Kolonnen *Utført handling* forteller deg hvordan filtreringsreglene ble anvendt.
- **Enhetskontroll**– Inneholder poster med flyttbare medier eller enheter som var tilkoblet datamaskinen. Bare enheter med en enhetskontrollregel vil bli registrert i loggfilen. Hvis regelen ikke stemmer overens med en tilkoblet enhet, blir det ikke opprettet noen loggoppføring for en tilkoblet enhet. Her finner du også detaljer som enhetstype, serienummer, forhandlernavn og mediestørrelse (hvis tilgjengelig).

Informasjonen som vises i hvert av avsnittene, kan kopieres til utklippstavlen (tastatursnarvei **Ctrl+C)** ved å velge oppføringen og klikke **Kopier**. **CTRL-** og **SHIFT**-tastene kan brukes til å velge flere oppføringer.

Klikk **Filtrering** for å åpne vinduet **Loggfiltrering** der du kan definere filtreringskriterier.

Du kan vise hurtigmenyen ved å høyreklikke på en bestemt post. Følgende alternativer er tilgjengelige i hurtigmenyen:

- **Vis** – Viser mer detaljert informasjon om den valgte loggen i et nytt vindu.
- **Filtrer samme oppføringer** – Etter aktivering av dette filteret vil du bare se postene av samme type (diagnostikk, advarsler, ...).
- **Filtrer .../Finn ...** – Når du klikker på dette alternativet, kan du bruke vinduet Søk i logg til å definere filtreringskriterier for spesifikke loggoppføringer.
- **Aktiver filter** – Aktiverer filterinnstillinger.
- **Deaktiver filter** – Fjerner alle filterinnstillingene (som beskrevet over).
- **Kopier/Kopier alle** – Kopierer informasjon om alle postene i vinduet.
- **Slett/Slett alle** – Sletter valgt(e) post(er) eller alle postene som vises - denne handlingen krever administratorrettigheter.
- **Eksporter ...** – eksporterer informasjon om posten(e) i XML-format.
- **Eksporter alle ...** – Eksporterer informasjon om alle postene i XML-format.
- **Rulle logg** – La dette alternativet være aktivert for å automatisk rulle gamle logger og se aktive logger i vinduet **Loggfiler**.

3.9.6.1.1 Søk i logg

Logger lagrer informasjon om viktige systemhendelser. Loggfiltreringsfunksjonen gjør at du kan vise oppføringer om en bestemt hendelsestype.

Skriv inn søkeordet i feltet **Finn tekst**. Hvis du ønsker å søke på ordet i bestemte kolonner, endrer du filteret i rullegardinmenyen **Søk i kolonner**.

Oppføringstyper – Velg én eller flere oppføringstyper fra rullegardinmenyen:

- **Diagnostisering** – logger informasjon som trengs for å finjustere programmet og alle postene over.
- **Informative** – registrerer informative meldinger, inkludert vellykkede oppdateringsmeldinger, pluss alle registreringene ovenfor.
- **Advarsler** – logger alle kritiske feil og varselsmeldinger.
- **Feil** – feil som f.eks. "Feil under nedlasting av fil" og kritiske feil logges.
- **Kritisk** – logger bare kritiske feil (feil som starter virusbeskyttelse, innebygd brannmurosv...).

Tidsperiode – Definer tidsperioden som du ønsker at resultatene skal vises fra.

Bare finn hele ord – Velg denne avmerkingsboksen hvis du ønsker å søke etter bestemte hele ord og få mer presise resultater.

Skill mellom store og små bokstaver – Aktiver dette alternativet hvis det er viktig for deg å bruke store eller små bokstaver ved filtrering.

Søk oppover – Søkeresultater som er høyere i dokumentet vises først.

3.9.6.2 Oppsett av proxy-server

I store LAN-nettverk kan datamaskinens tilkobling til Internett gå via en proxy-server. Hvis dette er tilfelle, må følgende innstillinger defineres. Ellers kan ikke programmet oppdateres automatisk. I ESET Endpoint Security er oppsett av proxy-server tilgjengelig i to ulike deler i treet for avansert oppsett.

For det første kan innstillingene for proxy-servere konfigureres i **Avansert oppsett** under **Verktøy** > **Proxy-server**. Når du angir proxy-server på dette nivået, definerer du globale proxy-serverinnstillinger for hele ESET Endpoint Security. Parameterne her benyttes av alle modulene som krever tilkobling til Internett.

Når du skal angi innstillinger for proxy-server på dette nivået, velger du avmerkingsboksen **Bruk proxy-server** og skriver inn adressen til proxy-serveren i **Proxy-server**-feltet sammen med **port**-nummeret til proxy-serveren.

Hvis kommunikasjon med proxy-serveren krever godkjenning, velger du avmerkingsboksen **Proxy-serveren krever godkjenning** og skriver inn gyldig **Brukernavn** og **Passord** i de respektive feltene. Klikk **Gjenkjenn** hvis du vil gjenkjenne og sette inn proxy-serverinnstillingene automatisk. Parameterne som er angitt i Internet Explorer, kopieres.

MERKNAD: Du må manuelt oppgi brukernavn og passord i innstillingene **Proxy-serveren**.

Innstillinger for proxy-server kan også defineres i det avanserte oppdateringsoppsettet (**Avansert oppsett**> **Oppdater** > **HTTP Proxy** ved å velge **Tilkobling gjennom proxy-server** fra rullegardinmenyen **Proxy-modus**). Denne innstillingen gjelder for den angitte oppdateringsprofilen og anbefales for bærbare datamaskiner som ofte mottar virussignaturdatabaser fra eksterne plasseringer. Se delen Avansert oppsett for oppdatering hvis du vil ha mer informasjon om denne innstillingen.

3.9.6.3 Planlegger

Planlegger administrerer og starter planlagte oppgaver med forhåndsdefinert konfigurasjon og forhåndsdefinerte egenskaper.

Du går inn i planleggeren fra hovedmenyen for ESET Endpoint Security ved å klikke **Verktøy** > **Planlegger**. **Planlegger** inneholder en liste over alle planlagte oppgaver og konfigurasjonsegenskaper som forhåndsdefinert dato, klokkeslett og skanneprofil som benyttes.

Planleggeren kan planlegge følgende oppgaver: oppdatering av virussignaturdatabase, skanneoppgaver, filkontroll ved systemstart og loggvedlikehold. Du kan legge til eller slette oppgaver direkte fra hovedvinduet til Planlegger (click **Legg till oppgave** eller **Slett** nederst). Høyreklikk hvor som helst i Planleggervinduet for å utføre følgende handlinger: vise detaljert informasjon, utføre oppgaven umiddelbart, legge til en ny oppgave og slette en eksisterende oppgave. Bruk avmerkingsboksene på begynnelsen av hver oppføring for å aktivere/deaktivere oppgavene.

Som standard vises følgende planlagte oppgaver i **Planlegger**:

- **Loggvedlikehold**
- **Vanlig automatisk oppdatering**
- **Automatisk oppdatering etter oppringt tilkobling**
- **Automatisk oppdatering etter brukerpålogging**
- **Automatisk filkontroll ved oppstart** (etter brukerpålogging)
- **Automatisk filkontroll ved oppstart** (etter en vellykket oppdatering av virussignaturdatabasen)
- **Automatisk førstegangsskanning**

Du kan redigere konfigurasjonen av en eksisterende planlagt oppgave (både standard og brukerdefinert) ved å høyreklikke oppgaven og klikke **Rediger ...**, eller ved å velge oppgaven du vil endre, og klikke **Rediger ...**.

Legge til en ny oppgave

1. Klikk **Legg til oppgave** nederst i vinduet.
2. Skriv inn navnet på oppgaven.

3. Velg den ønskede oppgaven fra rullegardinmenyen:

- **Kjør eksternt program** – Planlegger kjøring av et eksternt program.
- **Vedlikehold av logg** – Loggfiler inneholder også rester av slettede poster. Denne oppgaven optimerer poster i loggfiler regelmessig for å arbeide effektivt.
- **Filkontroll ved systemstart** – kontrollerer filer som har lov til å kjøre ved systemstart eller pålogging.
- **Opprett en datamaskinskanning** – oppretter en ESET SysInspector-datamaskinavbildning – samler detaljert informasjon om systemkomponenter (f.eks. drivere, programmer) og vurderer risikonivået for hver komponent.
- **Datamaskinskanning ved forespørsel** – Utfører en datamaskinskanning av filene og mappene på datamaskinen din.
- **Første skanning** – Som standard 20 minutter etter installasjon eller omstart, gjennomføres en datamaskinskanning som en lavprioritet-oppgave.
- **Oppdater** – Planlegger en oppdateringsoppgave ved å oppdatere virussignaturdatabasen og ved å oppdatere programmoduler.

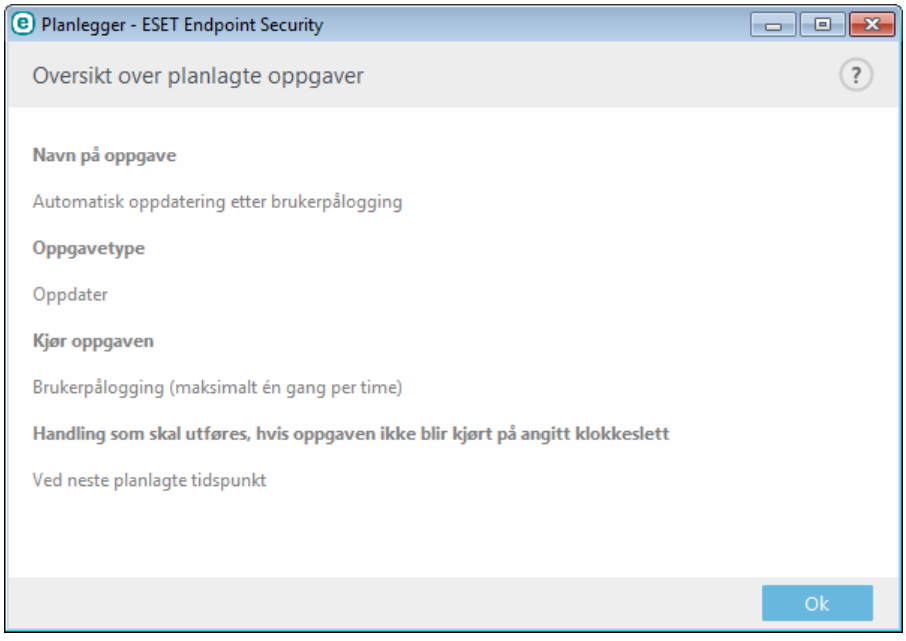
4. Slå på bryteren **Aktivert** hvis du vil aktivere oppgaven (du kan gjøre dette senere ved å merke av / fjerne merket i avkrysningsboksen i listen over planlagte oppgaver), klikk **Neste** og velg et av følgende alternativer:

- **En gang** – Oppgaven blir utført på forhåndsdefinert dato og tidspunkt.
- **Gjentatte ganger** – Oppgaven blir utført med angitt tidsintervall (i timer).
- **Daglig** – Oppgaven blir kjørt hver dag på angitt tidspunkt.
- **Ukentlig** – Oppgaven blir utført på angitt dag og tidspunkt.
- **Utløst av handling** – Oppgaven utføres på en angitt hendelse.

5. Velg **Hopp over oppgave hvis datamaskinen kjører på batteri** for å begrense systemressursene mens en laptop kjører på batteristrøm. Oppgaven vil kjøre på datoen og klokkeslettet som er angitt i **Oppgaveutførelse**-feltene. Hvis oppgaven ikke kan kjøres på forhåndsdefinert tidspunkt, kan du angi når den skal utføres igjen:

- **På neste planlagte tidspunkt**
- **Så snart som mulig**
- **Umiddelbart, hvis tiden fra forrige utførelse overskrider en angitt verdi** (intervallen kan defineres ved bruk av rulleboksen **Tid fra siste utførelse**)

Du kan gjennomgå den planlagte oppgaven når du høyreklikker og klikker **Vis oppgavedetaljer**.



3.9.6.4 Beskyttelsesstatistikk

Du kan vise en graf med statistiske data knyttet til ESET Endpoint Securitys beskyttelsesmoduler ved å klikke **Verktøy** > **Beskyttelsesstatistikk**. Velg ønsket beskyttelsesmodul fra rullegardinmenyen **Statistikk** for å vise den tilsvarende grafen med forklaringer. Hvis du holder musepekeren over et element i forklaringene, vises bare dataene for det aktuelle elementet i grafen.

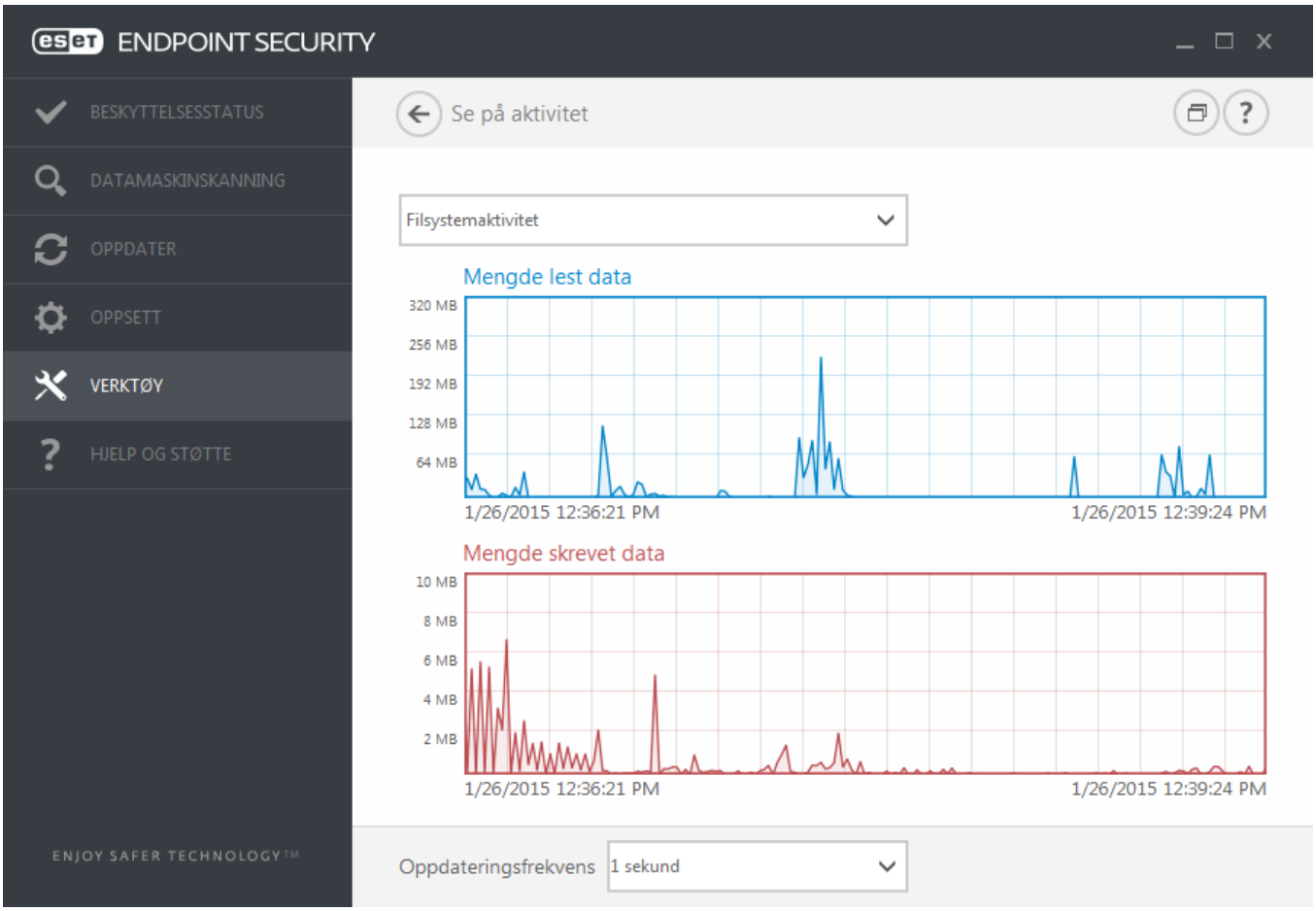
Følgende statistikkgrafer er tilgjengelige:

- **Virus- og spywarebeskyttelse** – Viser antall infiserte og rensede objekter.
- **Filsystembeskyttelse** – Viser bare objekter som er lest eller skrevet til filsystemet.
- **Beskyttelse for e-postklient** – Viser bare objekter som er sendt eller mottatt av e-postklienter.
- **Beskyttelse for nettilgang og anti-phishing** – Viser bare objekter som er lastet ned av nettlesere.
- **Spambeskyttelse for e-postklient** – Viser historikk for antispamstatistikk siden forrige oppstart.

Ved siden av de statistiske grafene, kan du se det totale antallet skannede objekter, infiserte objekter, rensede objekter og antall rene objekter. Klikk **Tilbakestill** for å fjerne statistikkinformasjonen eller **Tilbakestill alle** for å slette eller fjerne alle eksisterende data.

3.9.6.5 Se på aktivitet

Hvis du vil vise gjeldende **Filsystemaktivitet** i en graf, klikker du **Verktøy** > **Se på aktivitet**. Under grafen finnes det en tidslinje som viser filsystemaktiviteter i sanntid, basert på en valgt tidsperiode. For å endre tidsrommet, velg fra rullgardinmenyen **Oppdateringsfrekvens**.



Følgende alternativer er tilgjengelige:

- **Trinn: 1 sekund** – Grafen oppdateres hvert sekund og tidslinjen dekker de siste 10 minuttene.
- **Trinn: 1 minutt (siste 24 timer)** – Grafen oppdateres hvert minutt og tidslinjen dekker de siste 24 timene.
- **Trinn: 1 minutt (siste måned)** – Grafen oppdateres hver time og tidslinjen dekker den siste måneden.
- **Trinn: 1 time (valgt måned)** – Grafen oppdateres hver time og tidslinjen dekker de siste X valgte månedene.

Den vertikale aksen i **Graf for** filsystemaktivitet representerer leste data (blått) og skrevne data (rødt). Begge verdier gis i kB (kilobyte), MB eller GB. Hold pekeren over leste eller skrevne data i forklaringene under grafen for å vise data kun for denne aktivitetstypen.

Du kan også velge **Nettverksaktivitet** fra rullegardinmenyen. Grafen og alternativene for **Filsystemaktivitet** og **Nettverksaktivitet** er identiske, bortsett fra at i den sistnevnte vises mengden mottatte data (rødt) og mengden sendte data (blått).

3.9.6.6 ESET SysInspector

ESET SysInspector er et program som kontrollerer datamaskinen grundig, samler inn detaljert informasjon om systemkomponenter, for eksempel installerte drivere og programmer, nettverkstilkoblinger eller viktige registerregistreringer, og vurderer risikonivået for hver komponent. Denne informasjonen kan bidra til å finne årsaken til mistenkelig systemoppførsel, som kan skyldes inkompatibel program- og maskinvare eller skadelig programvare.

SysInspector-vinduet viser følgende informasjon om opprettede logger:

- **Klokkeslett**– Tidspunktet da loggen ble opprettet.
- **Kommentar**– En kort kommentar.
- **Bruker**– Navnet på brukeren som opprettet loggen.
- **Status** – Status for loggopprettelse.

Følgende handlinger er tilgjengelige:

- **Åpne** – Åpner opprettet logg. Du kan høyreklikke en gitt loggfil og velge **Vis** fra hurtigmenyen.
- **Sammenlign** – Sammenlikner to eksisterende logger.
- **Opprett ...** – Oppretter en ny logg. Vent til ESET SysInspector er ferdig (loggstatus vises som Opprettet) før du prøver å få tilgang til loggen.
- **Slett** – fjerner de(n) valgte loggen(e) fra listen.

Etter at du har høyreklikket én eller flere valgte loggfiler, er følgende alternativer tilgjengelig fra hurtigmenyen:

- **Vis** – Åpner den valgte loggen i ESET SysInspector (samme funksjon som å dobbeltklikke en logg).
- **Sammenlign** – Sammenlikner to eksisterende logger.
- **Opprett ...** – Oppretter en ny logg. Vent til ESET SysInspector er ferdig (loggstatus vises som Opprettet) før du prøver å få tilgang til loggen.
- **Slett alle**– Sletter alle logger.
- **Eksporter...** – Eksporterer loggen til en *.xml*-fil eller zippet *xml*.

3.9.6.7 ESET Live Grid

ESET Live Grid er et avansert tidligvarslingssystem mot oppståtte trusler basert på omdømme. Det hjelper med å oppdage nylig oppståtte trusler basert på omdømme og forbedre skanneytelsen ved å bruke en hvitliste. ESET-viruslabben bruker sanntidsstreaming av trusselrelatert informasjon fra skyen for å holde forsvaret oppdatert på et konstant beskyttelsesnivå. Brukere kan sjekke omdømmet til aktive prosesser og filer direkte fra programmets grensesnitt eller fra kontekstmenyen, og få tilleggsinformasjon fra ESET Live Grid. Velg et av følgende alternativer når du installerer ESET Endpoint Security:

1. Du kan bestemme deg for å ikke aktivere ESET Live Grid. Du vil ikke miste noe av funksjonaliteten i programvaren, men ESET Endpoint Security kan i enkelte tilfeller reagere raskere på nye trusler enn oppdateringen av virussignaturdatabasen.
2. Du kan konfigurere ESET Live Grid til å sende inn anonym informasjon om nye trusler og om hvor den nye trusselkoden ligger. Denne filen kan sendes til ESET for detaljert analyse. Ved å studere disse truslene kan ESET oppdatere sine trusselgjenkjenningsprosesser.

ESET Live Grid samler inn informasjon om datamaskinen som er relatert til nyoppdagede trusler. Denne informasjon kan inneholde en prøve eller en kopi av filen som trusselen ble oppdaget i, banen til den filen, filnavnet, dato og tidspunkt, prosessen som trusselen viste seg i på datamaskinen og informasjon om datamaskinens operativsystem.

Standardinnstillingen er at ESET Endpoint Security sender mistenkelige filer til ESETs viruslaboratorium for detaljert

analyse. Bestemte filtyper, for eksempel *.doc* eller *.xls*, utelukkes alltid. Du kan også legge til andre filtyper hvis det er spesielle filer som du eller organisasjonen din vil unngå å sende inn.

ESET Live Grid-omdømmesystem tilbyr skybaserte hvite- og svartelister. Hvis du vil vise innstillinger for ESET Live Grid, trykker du **F5** for å gå inn i Avansert oppsett og utvider deretter **Verktøy** > **ESET Live Grid**.

Aktiver ESET Live Grid omdømmesystem (anbefalt) – ESET Live Grid omdømmesystem forbedrer effektiviteten til ESET sine løsninger for anti-malware ved å sammenligne skannede filer mot en database med hvit- og svartelistede elementer i skyen.

Send inn anonym statistikk – Gi ESET tillatelse til å samle informasjon om nylig oppdagede trusler. Dette kan for eksempel være trusselnavn, dato og klokkeslett for oppdagelse, oppdagelsesmetode og tilknyttede metadata, produktversjon- og konfigurasjon, samt informasjon om systemet.

Send inn filer – Mistenkelige filer som minner om infiltreringer gjennom deres innhold eller opptreden vil sendes inn til ESET for analyse, via ESET Live Grid-teknologi.

Velg **Aktiver logging** hvis du vil opprette en hendelseslogg som registrerer innsending av filer og statistisk informasjon. Dette aktiverer logging til Hendelsesloggen ved sending av filer og statistikk.

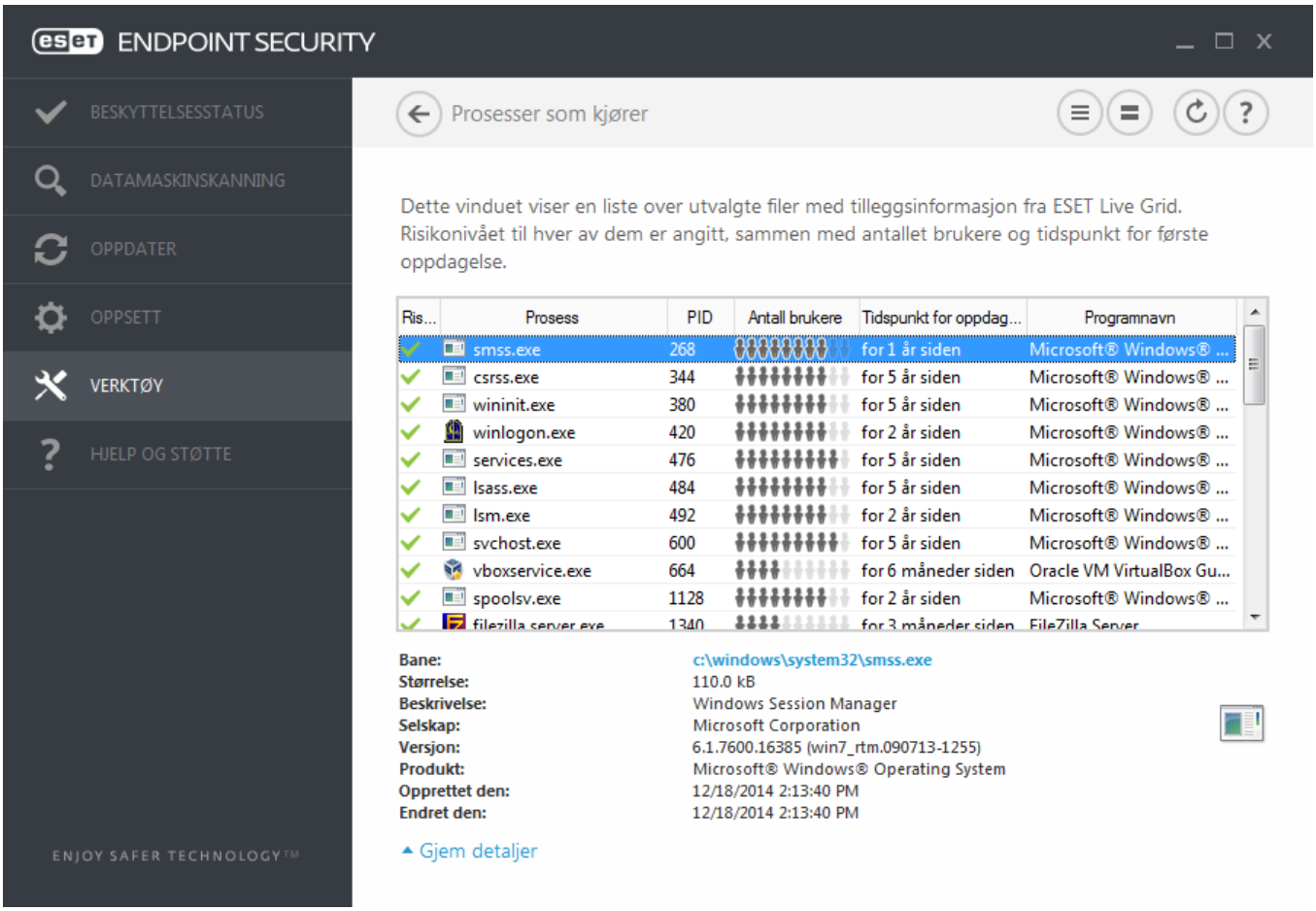
E-postadresse for kontakt (valgfritt) – E-postadressen din kan bli inkludert i mistenkelige filer, og kan brukes til å ta kontakt med deg hvis det trengs mer informasjon for analysen. Vær oppmerksom på at du ikke vil få svar fra ESET med mindre det er behov for flere opplysninger.

Unntak – Unntaksfilteret gjør det mulig å utelate bestemte filer/mapper fra innsendingen (det kan for eksempel være nyttig å utelate filer som kan ha konfidensiell informasjon, for eksempel dokumenter eller regneark). Filer som finnes her, blir aldri sendt til ESETs laboratorier for analyse, selv om de inneholder mistenkelig kode. De vanligste filtypene er utelatt som standard (.doc, osv.). Du kan legge til flere filer i listen over utelatte filer hvis du ønsker det.

Hvis du har brukt ESET Live Grid før, men deaktivert den, kan det fortsatt være datapakker som kan sendes. Selv etter deaktivering vil slike pakker bli sendt til ESET. Straks all gjeldende informasjon er sendt, vil ingen flere pakker bli opprettet.

3.9.6.8 Prosesser som kjører

Omdømmet til kjørende prosesser viser hvilke programmer eller prosesser som kjører på datamaskinen, og holder ESET umiddelbart og fortløpende informert om nye infiltrasjoner. ESET Endpoint Security gir detaljert informasjon om prosesser som kjører, for å beskytte brukere med ESET Live Grid-teknologi aktivert.



Risikonivå – Som regel tilordner ESET Endpoint Security og ESET Live Grid-teknologi risikonivå til objekter (filer, prosesser, registernøkler osv.) ved hjelp av en rekke heuristiske regler som undersøker egenskapene til hvert objekt og deretter vekter potensialet for skadelig aktivitet. Basert på denne heuristikken blir objektene tilordnet et risikonivå fra 1 – OK (grønt) til 9 – Risikofylt (rødt).

Prosess – Bildenavn på programmet eller prosessen som i øyeblikket kjører på datamaskinen. Du kan også bruke Windows Oppgavebehandling til å vise alle prosesser som kjører på datamaskinen. Du kan også åpne Oppgavebehandling ved å høyreklikke et tomt område på oppgavelinjen og velge Oppgavebehandling, eller ved å trykke **Ctrl**+**Shift**+**Esc** på skrivebordet.

PID – Er en ID for prosesser som kjører i Windows-operativsystemer.

MERKNAD: Kjente programmer som er merket OK (grønt), er avgjort rene (hvitelistet) og vil bli utelatt fra skanning, da dette vil forbedre skannehastigheten til datamaskinskanning etter behov eller Filsystembeskyttelse i sanntid på datamaskinen.

Antall brukere – Antall brukere som bruker et gitt program. Denne informasjonen er samlet inn med ESET Live Grid-teknologi.

Tidspunkt for oppdagelse – Tidsperioden siden programmet ble oppdaget av ESET Live Grid-teknologi.

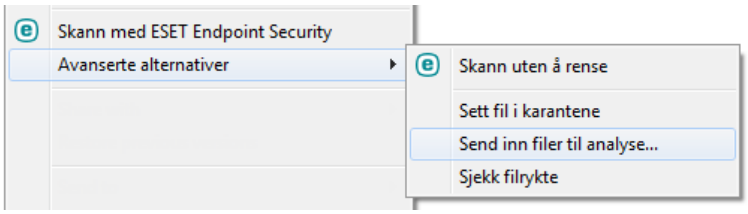
Merk: Når et program er merket som Ukjent (oransje) sikkerhetsnivå, er det ikke nødvendigvis skadelig programvare. Vanligvis er det bare et nytt program. Hvis du er usikker på filen, kan du bruke funksjonen Sende inn fil til analyse for å sende filen til ESETs viruslaboratorium. Hvis det viser seg at filen er et skadelig program, blir gjenkjenningen av dette lagt til i en av de kommende oppdateringene i virussignaturdatabasen.

Programnavn – Gitt navn på et program eller en prosess.

Klikk på et gitt program nederst for å vise følgende informasjon nederst i vinduet:

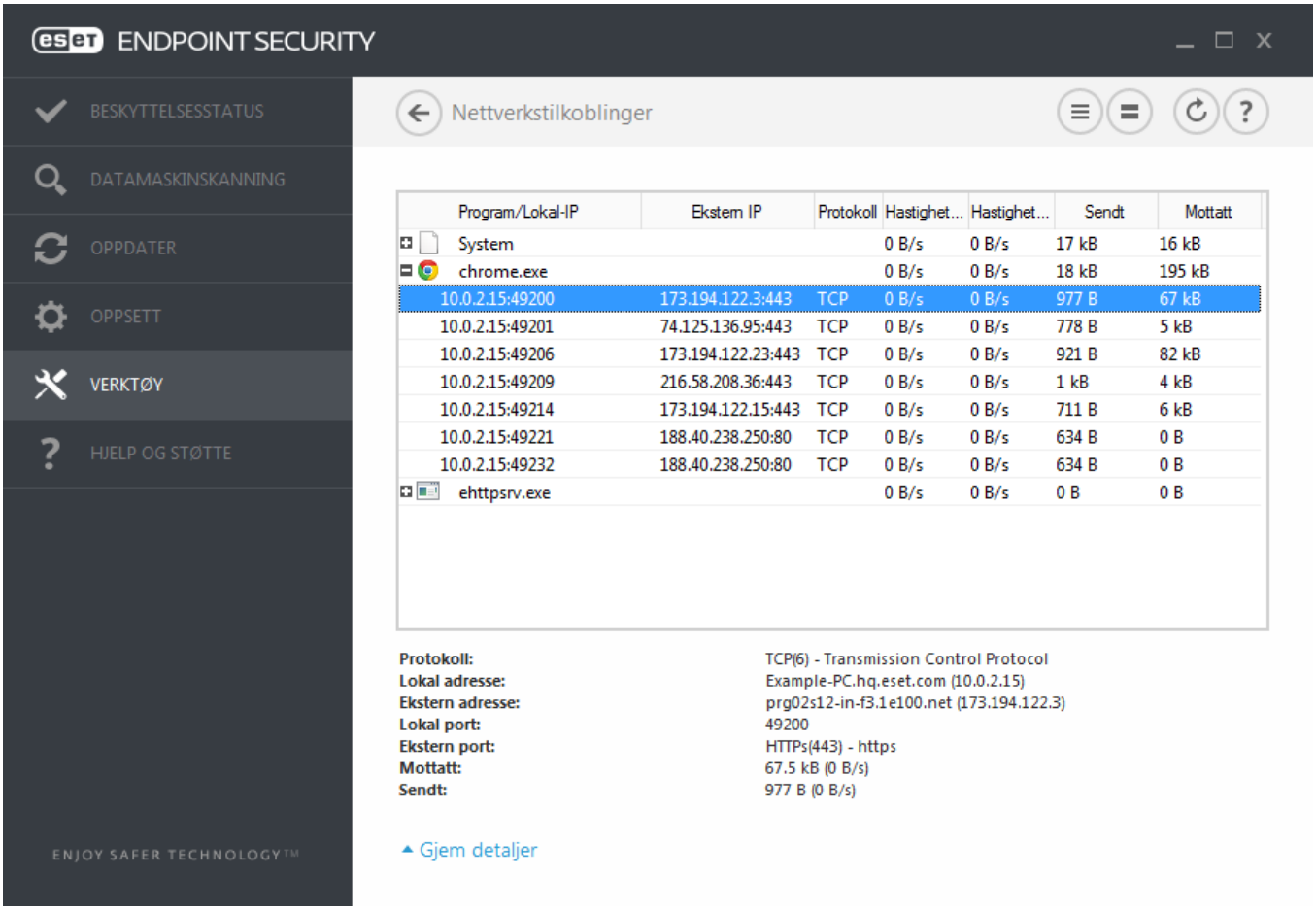
- **Bane** – Plassering av et program på datamaskinen.
- **Størrelse** – Filstørrelse enten i kB (kilobyte) eller MB (megabyte).
- **Beskrivelse** – Filegenskaper basert på beskrivelsen fra operativsystemet.
- **Selskap** – Navn på leverandør eller søkeprosess.
- **Versjon** – Informasjon fra utgiveren av programmet.
- **Produkt** – Programnavn og/eller forretningsnavn.
- **Opprettet på** – Dato og klokkeslett da programmet ble opprettet.
- **Opprettet på** – Siste dato og klokkeslett da programmet ble opprettet.

MERKNAD: Omdømme kan også kontrolleres på filer som ikke opptrer som kjørende programmer/prosesser – merk de filene du vil kontrollere, høyreklikk dem og velg **Avanserte alternativer** > **Kontroller filomdømme ved hjelp av ESET Live Grid** fra hurtigmenyen.



3.9.6.9 Nettverkstilkoblinger

I delen Nettverkstilkoblinger vises en liste over aktive og ventende tilkoblinger. Dette hjelper deg med å kontrollere alle programmer som etablerer utgående tilkoblinger.



Programnavnet og dataoverføringshastigheten står på den første linjen. Hvis du vil vise listen over programtilkoblinger (samt mer detaljert informasjon), klikker du **+**.

Kolonner

Program/lokal IP – Navn på program, lokal IP-adresse og kommunikasjonsporter.

Ekstern IP – IP-adresse og portnummer til en bestemt ekstern datamaskin.

Protokoll – Overføringsprotokoll brukt.

Opp-hastighet/Ned-hastighet – Gjeldende hastighet på utgående og innkommende data.

Sendt/Mottatt – Mengden data som er utvekslet i tilkoblingen.

Vis detaljer – Velg dette alternativet for å vise detaljert informasjon om den valgte tilkoblingen.

Velg et/en program eller IP-adresse i Nettverkstilkoblinger og høyreklikk på det for å åpne hurtigmenyen med følgende struktur:

Løs vertsnavn – Hvis det er mulig, blir alle nettverksadresser vist i DNS-format, ikke i det numeriske IP-adresseformatet.

Vis bare TCP-tilkoblinger – Listen viser bare tilkoblinger som tilhører TCP-protokollen.

Vis lyttende tilkoblinger – Velg dette alternativet for bare å vise tilkoblinger der det for tiden ikke er etablert kommunikasjon, men der systemet har åpnet en port og venter på tilkobling.

Vis tilkoblinger i datamaskinen – Velg dette alternativet for bare å vise tilkoblinger der den eksterne siden er et lokalt system – såkalte *localhost*-tilkoblinger.

Høyreklikk på en tilkobling for å vise ytterligere alternativer, inkludert:

Avslå kommunikasjon for tilkoblingen – Terminerer den etablerte kommunikasjonen. Dette alternativet er bare tilgjengelig etter at du har klikket på den aktive tilkoblingen.

Oppdateringshastighet – Angi hvor ofte de aktive tilkoblingene skal oppdateres.

Oppdater nå – Laster inn nettverkstilkoblingsvinduet på nytt.

De følgende alternativene er bare tilgjengelig etter at du har klikket på et program eller en prosess, ikke på en aktiv tilkobling:

Avslå kommunikasjon midlertidig for prosessen – Avviser gjeldende tilkoblinger for det aktuelle programmet. Hvis en ny tilkobling blir etablert, bruker brannmuren en forhåndsdefinert regel. Du finner en beskrivelse av innstillingene i delen Regler og soner.

Tillat kommunikasjon midlertidig for prosessen – Tillater gjeldende tilkoblinger for det aktuelle programmet. Hvis en ny tilkobling blir etablert, bruker brannmuren en forhåndsdefinert regel. Du finner en beskrivelse av innstillingene i delen Regler og soner.

3.9.6.10 Innsending av filer for analyse

Med dialogboksen for innsending av prøver kan du sende en fil eller et område til analyse hos ESET. Du finner den under **Verktøy** > **Send inn fil til analyse**. Hvis du finner en fil på maskinen eller et nettsted som oppfører seg mistenkelig, kan du sende den inn til ESETs viruslaboratorium for analyse. Hvis det viser seg at filen er et skadelig program eller at nettstedet er skadelig, blir gjenkjenningen av dette lagt til i en av de kommende oppdateringene.

Du kan også sende inn filen via e-post. Hvis du foretrekker denne muligheten, pakker du filen(e) med WinRAR/ZIP, beskytter arkivet med passordet "infected" og sender det til samples@eset.com. Husk å bruke et beskrivende emne og legge ved så mye informasjon som mulig om filen (for eksempel hvilket nettsted du lastet den ned fra).

MERKNAD: Før du sender inn en prøve til ESET, må du kontrollere at den oppfyller ett eller flere av følgende kriterier:
- filen eller nettstedet gjenkjennes overhodet ikke
- filen blir feilaktig oppfattet som en trussel

Du vil ikke få svar hvis det ikke er nødvendig å innhente mer informasjon for analysen.

Velg beskrivelsen fra rullegardinmenyen **Grunn til innsending av filen** som passer best med meldingen din:

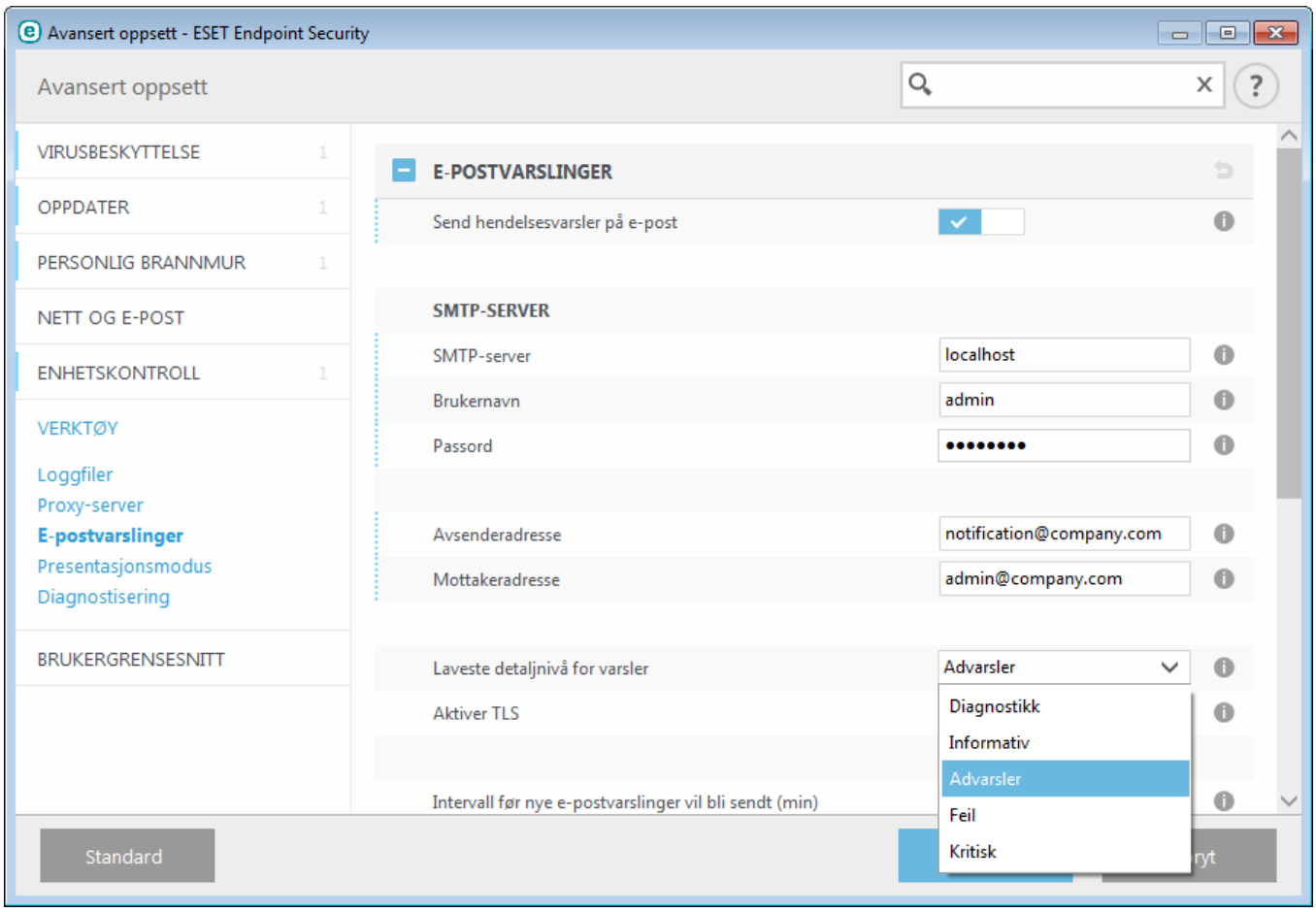
- **Mistenkelig fil**
- **Mistenkelig område** (et nettsted som er infisert av skadevare),
- **Falsk positiv fil** (fil som gjenkjennes som infisert, men som ikke er infisert),
- **Falskt positivt område**
- **Annet**

Fil/Nettsted – banen til filen eller nettstedet du har tenkt å sende inn.

E-postadresse for kontakt – E-postadressen for kontakt sendes sammen med mistenkelige filer til ESET og kan brukes til å kontakte deg hvis det er nødvendig å innhente flere opplysninger for analysen. Det er valgfritt å oppgi en e-postadresse for kontakt. Du får ikke svar fra ESET med mindre vi trenger mer informasjon, ettersom serverne våre mottar titusenvis av filer hver dag, noe som gjør det umulig å svare på alle innsendelser.

3.9.6.11 E-postvarslinger

ESET Endpoint Security kan automatisk sende e-postvarslinger hvis en hendelse med det valgte detaljnivået oppstår. Aktiver **Send hendelsesvarslinger via e-post** for å aktivere e-postvarslinger.



SMTP-server

SMTP-server – SMTP-serveren som brukes til å sende varsler (f.eks. *smtp.provider.com:587*, forhåndsdefinert port er 25).

MERKNAD: SMTP-servere med TLS-kryptering støttes av ESET Endpoint Security.

Brukernavnog **passord** – Hvis SMTP-serveren krever godkjenning, må disse feltene fylles ut med gyldig brukernavn og passord for å få tilgang til SMTP-serveren.

Avsenderadresse – Dette feltet angir avsenderadressen som blir vist overskriften i e-postvarslinger.

Mottakeradresse – Dette feltet angir mottakeradressen som blir vist overskriften i e-postvarslinger.

Fra rullegardinmenyen **Vis laveste detaljnivå for hendelser** kan du velge det laveste alvorlighetsnivået for visning av varsler og meldinger.

- **Diagnostisering** – logger informasjon som trengs for å finjustere programmet og alle postene over.
- **Informativ** – registrerer informative meldinger, inkludert vellykkede oppdateringsmeldinger, pluss alle registreringene ovenfor.
- **Advarsler** – logger alle kritiske feil og varselsmeldinger (antistealth kjører ikke ordentlig eller oppdatering mislyktes).
- **Feil** – Feil (dokumentbeskyttelse ikke startet) og kritiske feil vil bli registrert.
- **Kritisk** – logger bare kritiske feil feil som starter virusbeskyttelse eller infisert system.

Aktiver TLS – Aktiver sending av varsler og varslingsmeldinger som støttes av TLS-kryptering.

Intervall før nye e-postvarslinger vil bli sendt (min) – Intervall i minutter før nye e-postvarslinger vil bli sendt. Sett denne verdien til 0 hvis du vil sende varslingene umiddelbart.

Sendt hver varsling i en separat e-post – Når dette er aktivert, vil mottakeren motta en ny e-post for hver enkelt varsling. Dette kan føre til at mottakeren mottar et stort antall e-postmeldinger i løpet av en kort tidsperiode.

Meldingsformat

Format på hendelsesmeldinger – Formatet på hendelsesmeldinger som vises på eksterne datamaskiner.

Format på trussels- og varselsmeldinger: – Trusselvarsler og varslingsmeldinger har et forhåndsdefinert standardformat. Du bør ikke endre dette formatet. Det kan imidlertid finnes tilfeller (hvis du for eksempel har et automatisert behandlingssystem for e-post) hvor du trenger å endre meldingsformatet.

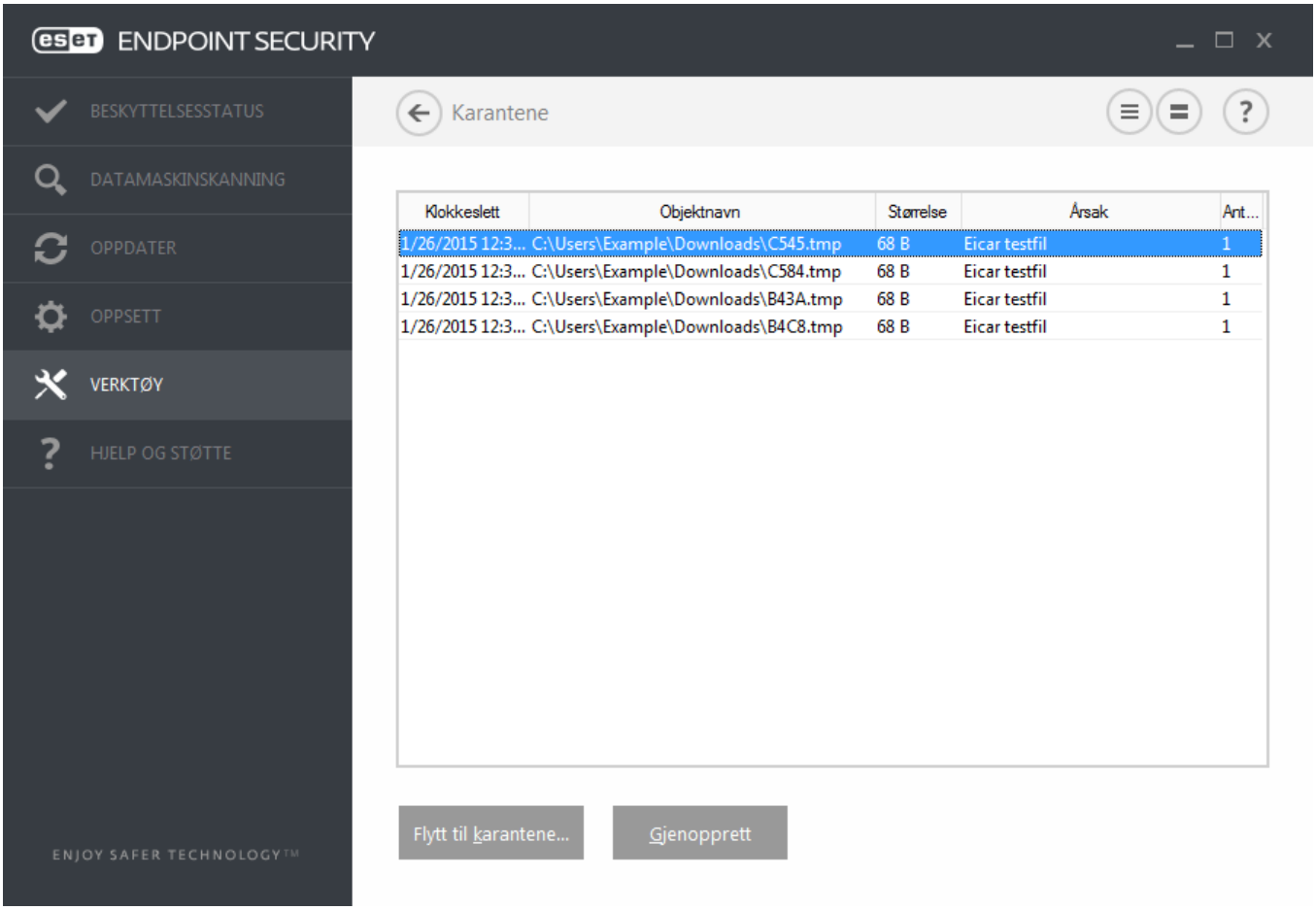
Bruk lokale bokstaver – Konverterer en e-postmelding til ANSI-kode, basert på de regionale innstillingene i Windows (f.eks. windows-1250). Hvis du ikke merker av for dette alternativet, blir meldinger konvertert til og kodet i ACSII 7-biter (f.eks. vil "á" bli endret til "a", og ukjente tegn til "?").

Bruk lokal koding av skrifttegn – Kildekoden i e-postmeldingen blir kodet til QP-format (Quoted-printable), som bruker ASCII-tegn og kan overføre spesielle nasjonale tegn på riktig måte i e-post med 8-biters format (áéíóú).

3.9.6.12 Karantene

Hovedfunksjonen til karantenen er å lagre infiserte filer på en trygg måte. Filer bør legges i karantene hvis de ikke kan renses, hvis det ikke er trygt eller anbefalt å slette dem eller hvis de blir feilaktig gjenkjent av ESET Endpoint Security.

Du kan velge å legge en hvilken som helst fil i karantene. Dette anbefales hvis en fil oppfører seg mistenkelig, men ikke oppdages av virusskanneren. Filer som er lagt i karantene, kan sendes til ESETs viruslaboratorium for analyse.



Filer som er lagret i karantenemappen, kan vises i en tabell som viser dato og tidspunkt for karantenen, banen til den opprinnelige plasseringen av den infiserte filen, størrelse i byte, årsak (f.eks. objekt lagt til av bruker) og antall trusler (f.eks. hvis et arkiv inneholder flere infiltrasjoner).

Sette filer i karantene

ESET Endpoint Security legger automatisk slettede filer i karantene (hvis du ikke har deaktivert dette alternativet i varselvinduet). Hvis du vil, kan du sette en hvilken som helst mistenkelig fil i karantene manuelt ved å klikke **Sett fil i karantene**. Den opprinnelige filen blir fjernet fra den opprinnelige plasseringen. Hurtigmenyen kan også brukes til dette formålet. Høyreklikk i **Karantene**-vinduet og velg **Sett fil i karantene**.

Gjenopprette fra karantene

Filer som er satt i karantene, kan også gjenopprettes til sin opprinnelige plassering. For å gjenopprette en fil i karantene, høyreklikk Karantene-vinduet og velg **Gjenopprett** på hurtigmenyen. Hvis en fil er merket som potensielt uønsket program, blir alternativet **Gjenopprett og utelat fra skanning** også tilgjengelig. Hurtigmenyen har også alternativet **Gjenopprett til ...**, som lar deg gjenopprette en fil til en annen plassering enn den filen ble slettet fra.

Slette fra karantene – Høyreklikk på et element og velg **Slette fra Karantene**, eller velg elementet du vil slette og trykk på **Delete** på tastaturet ditt. Du kan også velge flere elementer og slette dem samtidig.

MERKNAD: Hvis programmet ved en feiltakelse legger en harmløs fil i karantene, kan du utelate filen fra skanning etter gjenoppretting og sende filen til ESETs brukerstøtte.

Sende inn en fil fra karantene

Hvis du har lagt en mistenkelig fil som ikke ble gjenkjent av programmet, i karantene, eller hvis en fil ved en feil ble vurdert som en trussel og deretter satt i karantene, ber vi deg om å sende filen til ESETs viruslaboratorium. Når du skal sende inn en fil fra karantene, høyreklikker du filen og velger **Send inn for analyse** fra hurtigmenyen.

3.9.6.13 Microsoft Windows-oppdatering

Oppdateringsfunksjonen i Windows er en viktig komponent som beskytter brukere mot skadelig programvare. Derfor er det viktig å installere oppdateringene fra Microsoft Windows så snart de foreligger. Du vil få beskjed om manglende oppdateringer via ESET Endpoint Security i henhold til det nivået du angir. Du kan velge mellom følgende nivåer:

- **Ingen oppdateringer** – Ingen oppdateringer tilbys for nedlasting.
- **Valgfrie oppdateringer** – Oppdateringer som er merket med lav prioritet og høyere, tilbys for nedlasting.
- **Anbefalte oppdateringer** – Oppdateringer som er merket som vanlige og høyere, tilbys for nedlasting.
- **Viktige oppdateringer** – Oppdateringer som er merket som viktige og høyere, tilbys for nedlasting.
- **Kritiske oppdateringer** – Bare kritiske oppdateringer tilbys for nedlasting.

Klikk **OK** for å lagre endringene. Vinduet for systemoppdateringer vises etter at oppdateringsserveren har bekreftet statusen. Følgelig kan det hende at informasjon om systemoppgraderinger ikke er tilgjengelig umiddelbart etter at endringene er lagret.

3.9.7 Brukergrensesnitt

I delen **Brukergrensesnitt** kan du konfigurere atferden til programmets grafiske brukergrensesnitt (GUI).

Med verktøyet Brukergrensesnittelementer kan du justere programmets utseende og effektene som brukes.

For at sikkerhetsprogramvaren skal kunne levere maksimal sikkerhet kan du forhindre uautoriserte endringer ved hjelp av verktøyet Tilgangsoppsett.

Ved å konfigurere Varsler og meldinger kan du endre atferden til trusselvarsler og systemmeldinger. Disse kan konfigureres etter behov.

Hvis du velger ikke å vise enkelte meldinger, vises de i **Brukergrensesnittelementer** > **Programstatuser**. Her kan du kontrollere statusen til eller fjerne varslingene fra vinduet.

Integrering av hurtigmeny vises når det merkede objekt høyreklikkes. Bruk dette verktøyet til å integrere kontrollelementene i ESET Endpoint Security med hurtigmenyen.

Presentasjonsmodus er nyttig for brukere som ønsker å arbeide med et program uten å bli avbrutt av popup-vinduer, planlagte oppgaver og komponenter som kan belaste prosessoren og minnet.

3.9.7.1 Brukergrensesnittelementer

Alternativene for konfigurasjon av brukergrensesnittet i ESET Endpoint Security gjør det mulig å justere arbeidsmiljøet etter dine spesifikke behov. Disse alternativene er tilgjengelige fra forgreiningen **Brukergrensesnitt** > **Brukergrensesnittelementer** i treet for avansert oppsett av ESET Endpoint Security.

Arbeidsmiljøet kan justeres i delen **Brukergrensesnittelementer**. Klikk rullegardinmenyen **GUI-startmodus** for å velge blant følgende startmoduser for grafisk brukergrensesnitt (GUI):

Full – Hele brukergrensesnittet (GUI) vises.

Minimalt – Det grafiske brukergrensesnittet kjøres, men bare varsler vil vises til brukeren.

Manuell – Ingen varslinger eller varsler vises.

Stille – Verken GUI, ikke varslinger eller varsler vises. Denne modusen kan være nyttig i situasjoner der du kan måtte for bevare systemressurser. Stillemodus kan bare startes av administrator.

MERKNAD: Når Minimal GUI startmodus velges og datamaskinen startes på nytt, vises varslinger, men ikke det grafiske grensesnittet. For å tilbakestille den fulle grafiske brukergrensesnittmodus, kjør Grafisk brukergrensesnitt

på startmenyen under **Alle programmer** > **ESET** > ESET Endpoint Security som administrator, eller du kan gjøre dette via ESET Remote Administrator ved å bruke en policy.

Hvis du vil deaktivere velkomstbildet i ESET Endpoint Security, fjerner du avmerkingen ved **Vis velkomstbilde ved oppstart** .

For at ESET Endpoint Security skal gi et lydsignal når viktige hendelser inntreffer under en skanning, for eksempel når en trussel oppdages eller skanningen er ferdig, velger du **Bruk lydsignal**.

Integrer i hurtigmeny – Integrerer kontrollelementene i ESET Endpoint Security med hurtigmenyen.

Statuser

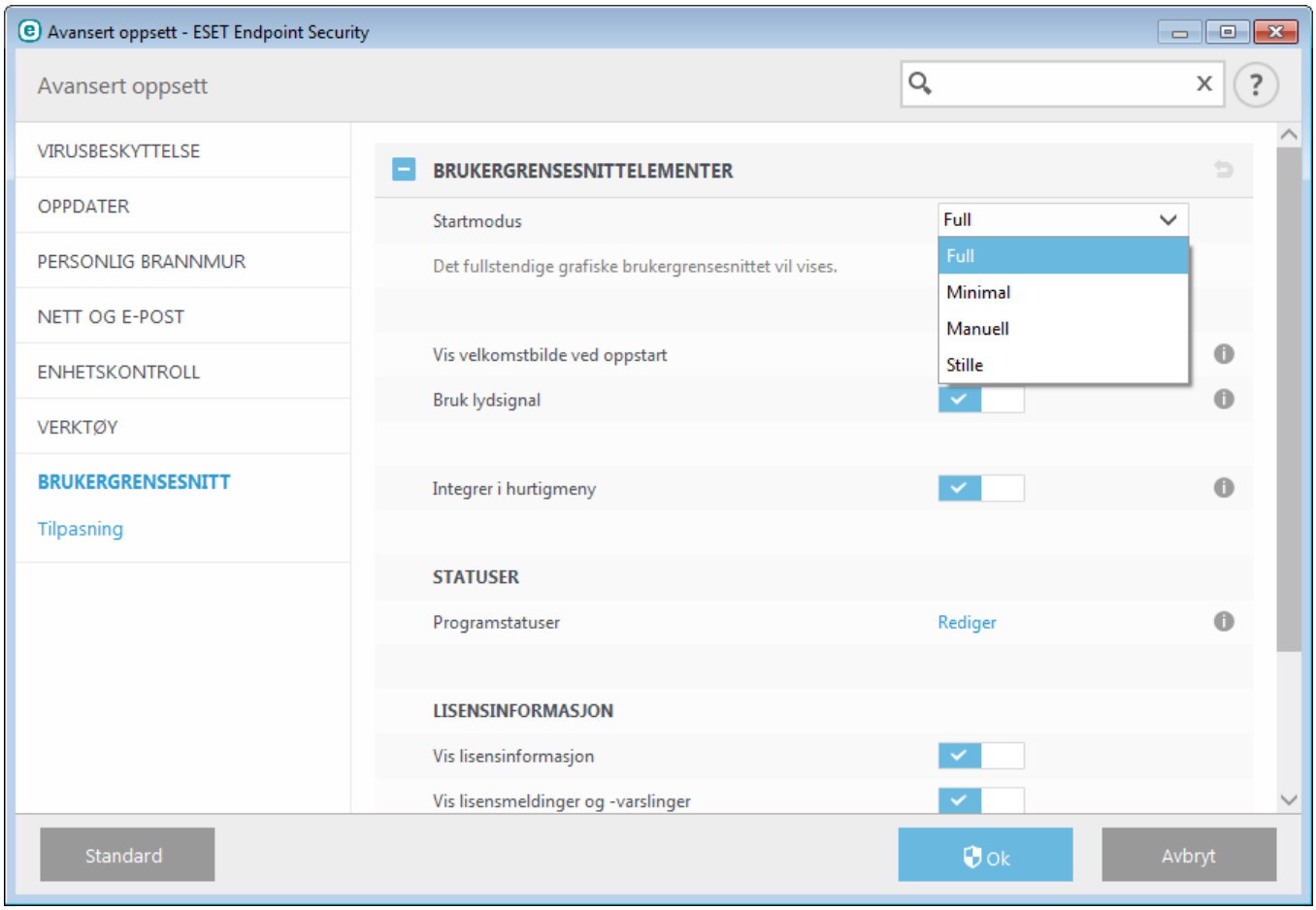
Programstatuser – Klikk **Rediger**-knappen for å administrere (deaktivere) statuser i **Beskyttelsesstatus**-panelet i hovedmenyen.

Lisensinformasjon

Vis lisensinformasjon – Når dette alternativet er deaktivert, vil ikke lisensinformasjonen på skjermbildet **Beskyttelsesstatus** og **Hjelp og støtte** vises.

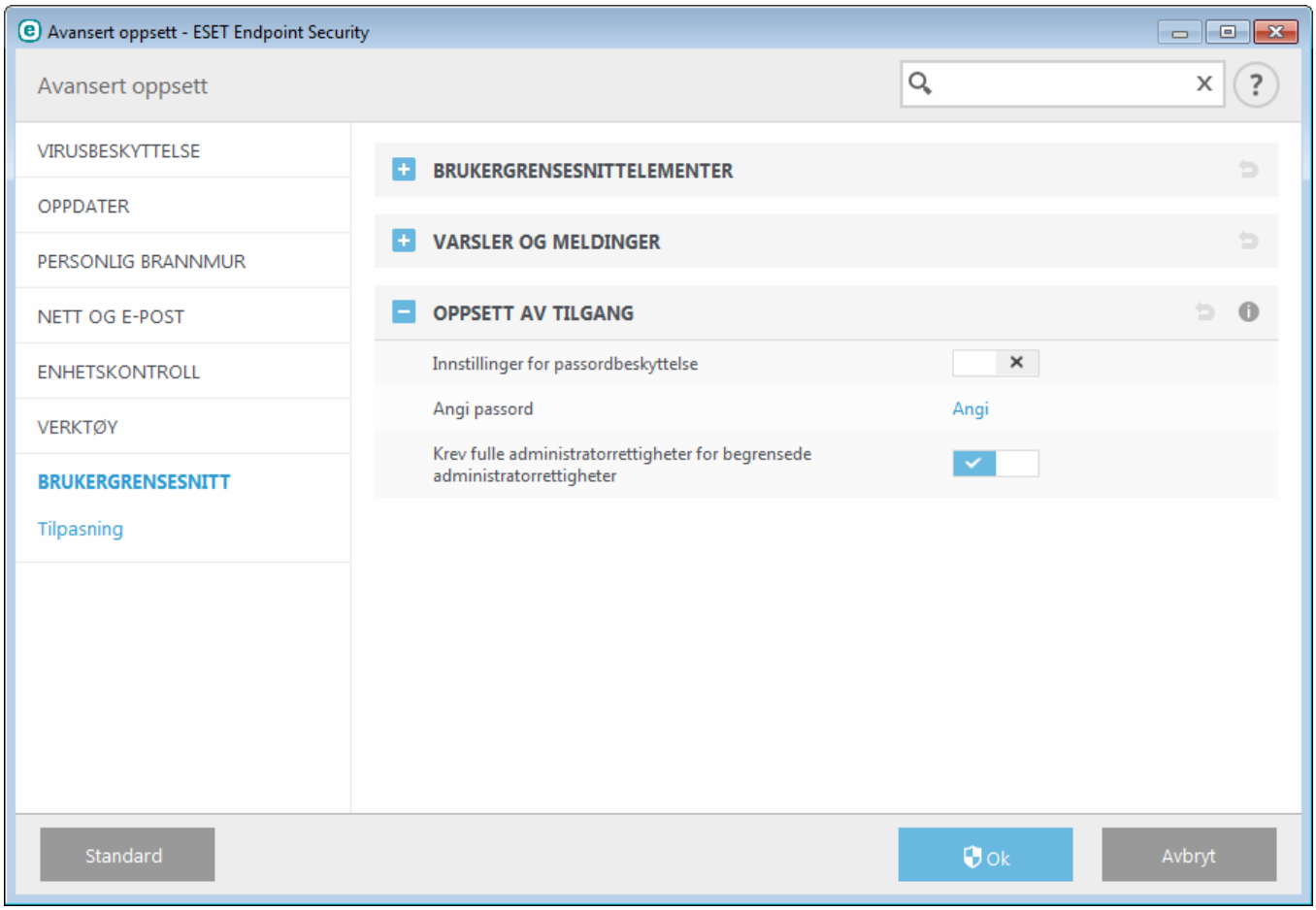
Vis lisensmeldinger og -varslinger – Når dette alternativet er deaktivert, vil meldinger og varslinger bare bli vist når lisensen utløper.

MERKNAD: Lisensinformasjonsinnstillingene anvendes, men er ikke tilgjengelig for ESET Endpoint Security som aktiveres for MSP-lisens.



3.9.7.2 Oppsett av tilgang

For å kunne gi systemet maksimal sikkerhet er det helt avgjørende at ESET Endpoint Security er riktig konfigurert. Feilaktige endringer kan føre til tap av viktige data. For å unngå uautorisert endring, kan parameterne for oppsett av ESET Endpoint Security passordbeskyttelse. Konfigurasjonsinnstillinger for passordbeskyttelse finner du i undermenyen **Oppsett av tilgang** (F5) under **Tilgangsoppsett** > **Brukergrensesnitt**.



Innstillinger for passordbeskyttelse – angi passordinnstillinger. Klikk for å åpne vinduet Oppsett av passord.

Klikk **Still inn** for å angi eller endre et passord for å beskytte oppsettsparametrene.

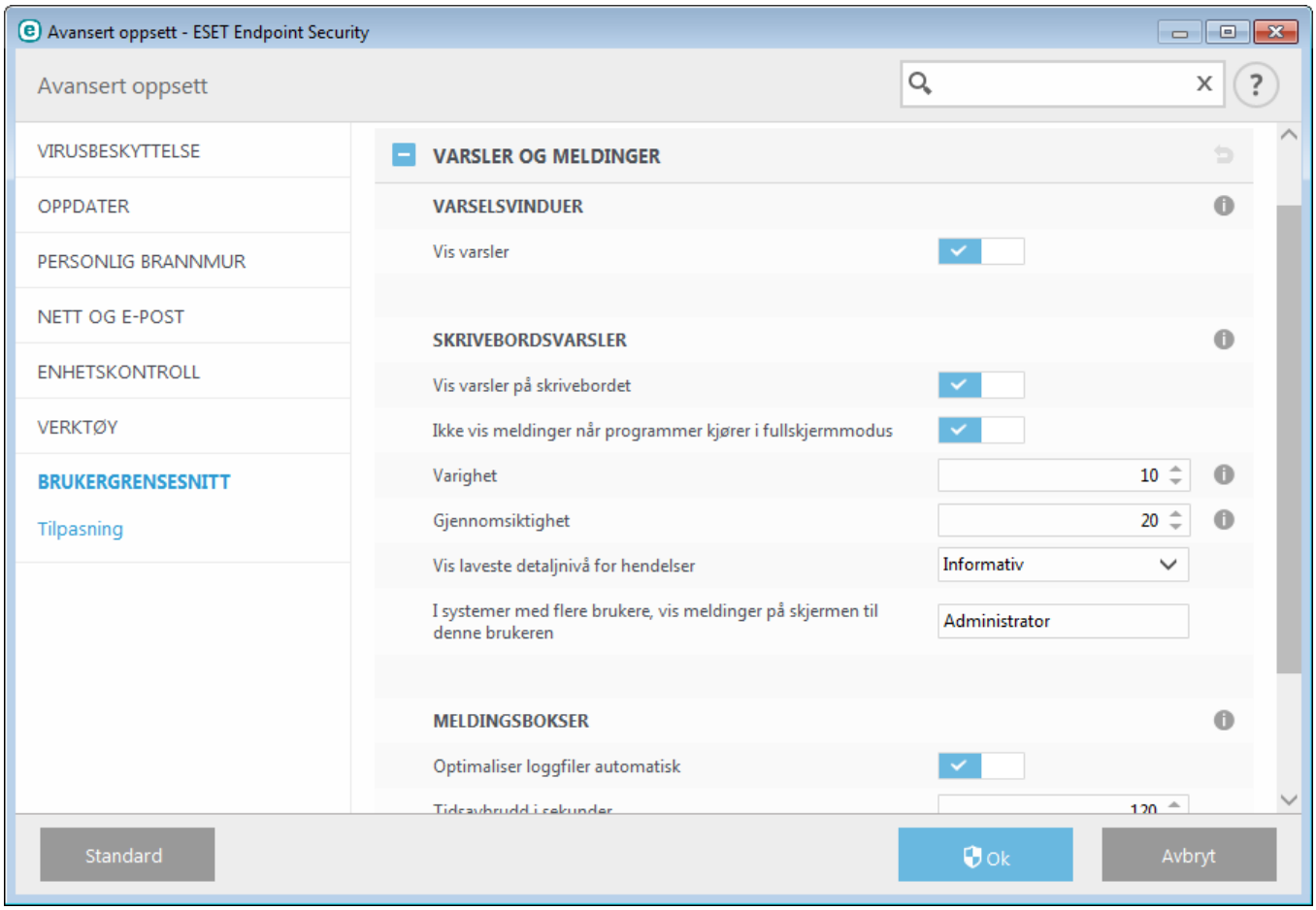
Krev fulle administratorrettigheter for begrensede administratorrettigheter – Velg dette alternativet for å be gjeldende bruker (hvis han/hun ikke har administratorrettigheter) om å skrive inn brukernavn og passord for administrator når de endrer bestemte systemparametere (ligner brukerkontokontroll i Windows Vista). Dette gjelder bl.a. deaktivering av beskyttelsesmoduler eller brannmuren.

Kun for Windows XP:

Krev administratorrettigheter (system uten UAC-støtte) – Aktiver dette alternativet for at ESET Endpoint Security skal be om administratorinformasjon.

3.9.7.3 Varsler og meldinger

I delen **Varsler og meldinger** under **Brukergrensesnitt** kan du konfigurere hvordan trusselvarsler og systemmeldinger (for eksempel meldinger om vellykkede oppdateringer) håndteres av ESET Endpoint Security. Du kan også angi visningstiden og gjennomsiktigheten til systemmeldinger (dette gjelder bare systemer som støtter systemmeldinger).



Varselsvinduer

Hvis du deaktiverer **Vis varsler**, vil det ikke bli vist noen varselvinduer. Dette passer bare i et begrenset antall spesielle situasjoner. For de fleste brukere anbefaler vi å beholde standardalternativet (aktivert).

Skrivebordsvarsler

Varsler på skrivebordet og tipsbobler er til informasjon og krever ingen handling fra brukeren. De vises i systemstatusfeltet nederst til høyre på skjermen. Hvis du vil aktivere visning av varsler på skrivebordet, velger du **Vis varsler på skrivebordet**. Slå på bryteren **Ikke vis varsler når programmer kjører i fullskjermmodus** hvis du vil blokkere all ikke-interaktive varsler. Du kan endre mer detaljerte alternativer, f.eks. visningstiden for skrivebordsvarsler og vindusgjennomsiktigheten nedenfor.

Med rullegardinmenyen **Vis laveste detaljnivå for hendelser** kan du velge alvorlighetsnivå for visning av varsler og meldinger. Følgende alternativer er tilgjengelige:

- **Diagnostisering** – Logger informasjon som trengs for å finjustere programmet og alle postene over.
- **Informative** – Registrerer informative meldinger, inkludert vellykkede oppdateringsmeldinger, pluss alle registreringene ovenfor.
- **Advarsler** – Logger alle kritiske feil og varselsmeldinger.
- **Feil** – Feil som f.eks. "Feil under nedlasting av fil" og kritiske feil logges.
- **Kritisk** – Logger bare kritiske feil (feil som starter virusbeskyttelse , innebygd brannmur, osv ...).

Den siste funksjonen i denne delen gjør det mulig å konfigurere målet for meldinger i et flerbrukersystem. Feltet **I systemer med flere brukere, vis meldinger på skjermen til denne brukeren** angir hvilken bruker som skal motta

systemvarsler og andre varsler, på systemer som tillater at flere brukere er tilkoblet samtidig. Dette vil vanligvis være en systemansvarlig eller en nettverksansvarlig. Dette alternativet er spesielt nyttig for terminalservere hvis alle systemmeldinger sendes til den systemansvarlige.

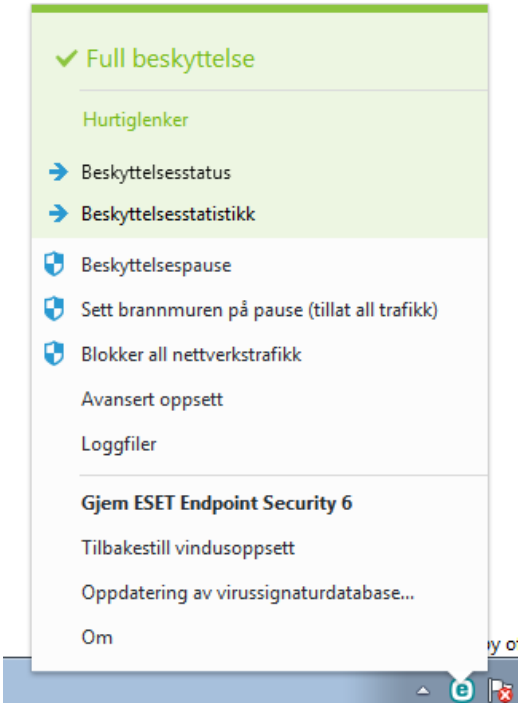
Meldingsbokser

Hvis du vil lukke popup-vinduer automatisk etter en bestemt tid, velger du alternativet **Lukk meldingsvinduer automatisk**. Hvis vinduet ikke lukkes manuelt, lukkes varselvinduet automatisk når den angitte tidsperioden utløper.

Bekreftelsesmeldinger – viser en liste med bekreftelsesmeldinger som du kan velge å vise eller ikke vise.

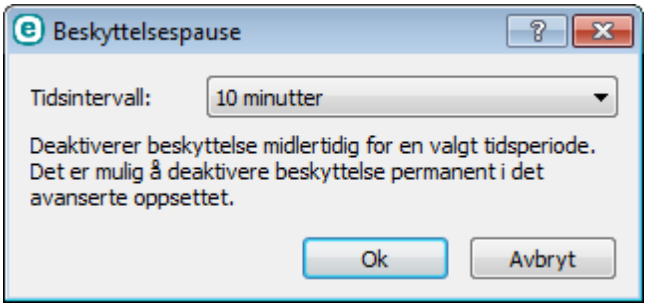
3.9.7.4 Ikonet i systemstatusfeltet

Du får tilgang til noen av de viktigste oppsettsalternativene og funksjonene ved å høyreklikke ikonet i statusfeltet .



Blokker nettverk – Personlig brannmur vil blokkere all utgående/innkommende nettverks- og Internett-trafikk.

Sett beskyttelse på pause – Viser bekreftelsesdialogboksen som deaktiverer Virus- og spywarebeskyttelse, som beskytter mot skadelige systemangrep ved å kontrollere filer, nett- og e-postkommunikasjon.



Rullegardinmenyen **Tidsintervall** representerer tidsperioden når all spambeskyttelse vil være deaktivert.

Sett brannmuren (Tillat all trafikk) på – Setter brannmuren over i en inaktiv tilstand. Se Nettverk for mer informasjon.

Blokker all nettverkstrafikk – Blokkerer all nettverkstrafikk. Du kan aktivere den på nytt ved å klikke **Stopp blokkering av all nettverkstrafikk**.

Avansert oppsett – Velg dette alternativet for å vise treet **Avansert oppsett**. Du kan også gå inn på Avansert oppsett

ved å trykke F5-tasten eller navigere til **Oppsett** > **Avansert oppsett**.

Loggfiler – Loggfiler inneholder informasjon om viktige programhendelser som har skjedd, og gir en oversikt over trusler som er oppdaget.

Skjul ESET Endpoint Security – Skjuler ESET Endpoint Security vinduet fra skjermen.

Tilbakestill vindusoppsett – Tilbakestiller vinduet til ESET Endpoint Security til standardstørrelsen og -plasseringen på skjermbildet.

Oppdatering av virussignaturdatabase – Starter oppdateringen av virussignaturdatabasen for å sikre beskyttelsesnivået mot skadelig kode.

Om – Gir systeminformasjon, detaljer om den installerte versjonen av ESET Endpoint Security og de installerte systemkomponentene samt utløpsdatoen for lisensen. Informasjon om operativsystemet ditt og systemressurser er tilgjengelig nederst på siden.

3.9.7.5 Hurtigmeny

Hurtigmenyen vises når et objekt høyreklikkes (fil). Menyen inneholder alle handlinger som kan utføres på et objekt.

Det er mulig å integrere kontrollelementene i ESET Endpoint Security med hurtigmenyen. Oppsettalternativer for denne funksjonaliteten er tilgjengelige i treet for avansert oppsett under **Brukergrensesnitt** > **Brukergrensesnitt**.

Integrer i hurtigmeny– Integrerer kontrollelementene i ESET Endpoint Security med hurtigmenyen.

3.10 Erfaren bruker

3.10.1 Profilbehandling

Profilbehandling brukes på to steder i ESET Endpoint Security – i avsnittet **Datamaskinskanning ved forespørsel** og i avsnittet **Oppdater**.

Datamaskinskanning ved behov

Du kan lagre dine foretrukne skanneparametere for skanning på et senere tidspunkt. Vi anbefaler at du oppretter en forskjellig profil (med forskjellige mål for skanning, skannemetoder og andre parametere) for hver skanning som brukes jevnlig.

Når du skal opprette en ny profil, åpner du vinduet for Avansert oppsett (F5) og klikker på **Antivirus** > **Datamaskinskanning ved behov** og deretter **Rediger** ved siden av **Liste over profiler**. Rullegardinmenyen **Valgt profil** som viser eksisterende skanneprofiler. Hvis du vil ha hjelp til å opprette en skanneprofil som er tilpasset ditt behov, finner du en beskrivelse av hver av parameterne i skanneoppsettet i delen Oppsett av parametere for ThreatSense-motor.

Eksempel: Sett at du vil opprette din egen skanneprofil og konfigurasjonen av Smart skanning egner seg delvis, men du vil ikke skanne kjøretidspakker eller potensielt usikre programmer, og du vil bruke **Grundig rensing**. Skriv inn navnet på den nye profilen i vinduet **Profilbehandling** og klikk **Legg til**. Velg den nye profilen din fra rullegardinmenyen **Valgt profil** og juster de gjenværende parameterne etter behov og klikk **OK** for å lagre den nye profilen din.

Oppdater

Profilredigering i delen Oppsett for oppdatering lar brukere opprette nye profiler. Opprett og bruk dine egne profiler (en annen enn standardprofilen **Min profil**) bare hvis datamaskinen din benytter flere former for tilkobling for å oppdatere servere.

For eksempel kan en bærbar datamaskin som vanligvis er tilkoblet en lokal server (Mirror) i det lokale nettverket, men laster ned oppdateringer direkte fra ESET oppdaterings-servere når den er koblet fra det lokale nettverket (forretningsreise), benytte to profiler: den første til å koble seg til den lokale serveren, og den andre for å koble seg til ESET-servere. Når disse profilene er konfigurert, navigerer du til **Verktøy** > **Planlegger** og redigerer parameterne for oppdateringsoppgaven. Angi én profil som primær og den andre som sekundær.

Valgt profil – oppdateringsprofilen som er i bruk. For å endre den velger du en profil fra rullegardinmenyen.

Liste over profiler – Opprett nye eller fjern eksisterende oppdateringsprofiler.

3.10.2 Diagnostisering

Diagnostisering leverer programkrasjdumper for ESET-prosessene (f.eks. *ekrn*). Hvis et program krasjer, genereres det en dump. Dette kan hjelpe utviklerne med å feilsøke og løse ulike problemer i ESET Endpoint Security. Klikk rullegardinmenyen ved siden av **Dumptype** og velg et av følgende alternativer:

- Velg **Deaktiver** (standard) for å deaktivere denne verdien.
- **Mini** – registrerer det minste settet med nyttig informasjon som kan bidra til å finne ut hvorfor programmet krasjet. Denne typen dumpfil kan være nyttig når du har begrenset med plass. Men på grunn av den begrensede informasjonen vil feil som ikke ble direkte forårsaket av tråden som kjørte på problemtidspunktet, kanskje ikke bli oppdaget gjennom en analyse av filen.
- **Full** – registrerer alt innholdet i systemminnet når et program stopper uventet. En komplett minnedump kan inneholde data fra prosesser som kjørte mens minnedumpen ble innhentet.

Aktiver avansert logging Protokollfiltrering – Registrer alle data som passerer gjennom Protokollfiltreringen i PCAP-format for å hjelpe utviklerne å finne og løse problemer knyttet til Protokollfiltreringen.

Loggfiler kan finnes i:
C:\ProgramData\ESET\ESET Smart Security\Diagnostics i Windows Vista og senere operativsystemer og *C:\Documents and Settings\All Users\...* i eldre versjoner av Windows.

Målkatalog– Katalogen der dumpen genereres når programmet krasjer.

Åpne diagnostikkmappe – Klikk **Åpne** for å åpne denne katalogen i et nytt *Windows utforsker*-vindu.

3.10.3 Importer og eksporter innstillinger

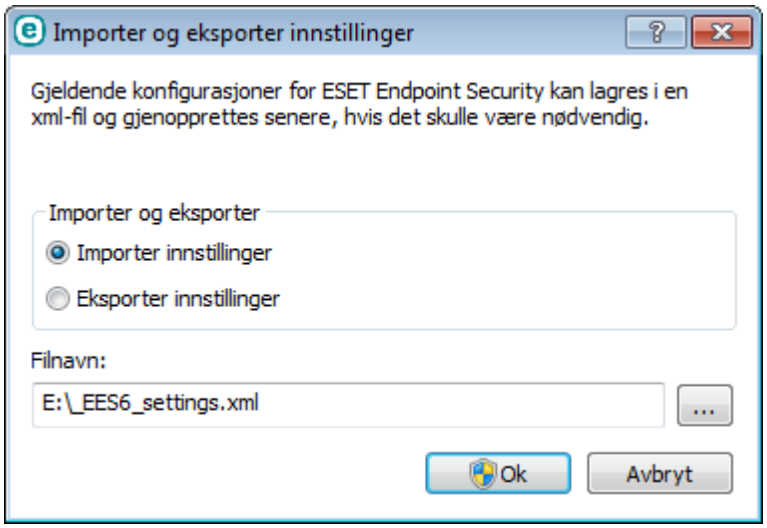
Du kan importere eller eksportere en tilpasset .xml-konfigurasjonsfil for ESET Endpoint Security fra menyen **Oppsett**.

Import og eksport av konfigurasjonsfiler er nyttig hvis du må sikkerhetskopiere den gjeldende konfigurasjonen til ESET Endpoint Security for bruk på et senere tidspunkt. Eksportinnstillingene er også praktisk for brukere som vil bruke sin foretrukne konfigurasjon på flere systemer. De kan enkelt importere en *.xml*-fil for å overføre disse innstillingene.

Det er ganske enkelt å importere en konfigurasjon. I hovedprogramvinduet klikker du **Oppsett** > **Importer/eksporter innstillinger**, og velger deretter **Importer innstillinger**. Skriv inn filnavnet på konfigurasjonsfilen, eller klikk på knappen **...** for å lete etter konfigurasjonsfilen du vil importere.

Trinnene for å eksportere en konfigurasjon er ganske like. I hovedprogramvinduet klikker du **Oppsett** > **Importer/eksporter innstillinger**. Velg **Eksporter innstillinger**, og skriv inn filnavnet på konfigurasjonsfilen (dvs. *export.xml*). Bruk nettleseren til å velge en plassering på datamaskinen der du vil lagre konfigurasjonsfilen.

MERKNAD: Hvis du ikke har tilstrekkelige rettigheter til å skrive den eksporterte filen til den spesifiserte mappen, kan du bli møtt med en feilmelding.



3.10.4 Kommandolinje

Antivirusmodulen til ESET Endpoint Security kan startes via kommandolinjen - manuelt (med kommandoen "ecls") eller med en seriell fil ("bat"). Bruk av ESET-kommandolinjeskanner:

```
ecls [ALTERNATIVER..] FILER..
```

Følgende parametere og brytere kan brukes når du kjører skanning ved behov fra kommandolinjen:

Alternativer

/base-dir=MAPPE	last inn moduler fra MAPPE
/quar-dir=MAPPE	karantenemappe
/exclude=MASKE	ekskluder filer som samsvarer med MASKE fra skanning
/subdir	skann undermapper (standard)
/no-subdir	ikke skann undermapper
/max-subdir-level=NIVÅ	maksimalt undernivå for mapper i mapper som skal skannes
/symlink	følg symbolske koblinger (standard)
/no-symlink	hopp over symbolske koblinger
/ads	skann ADS (standard)
/no-ads	ikke skann ADS
/log-file=FIL	logg utdata til FIL
/log-rewrite	overskriv utdatafil (standard - legg ved)
/log-console	logg utdata til konsoll (standard)
/no-log-console	ikke logg utdata til konsoll
/log-all	logg også rene filer
/no-log-all	ikke logg rene filer (standard)
/aind	vis aktivitetsindikator
/auto	skann og rens alle lokale stasjoner automatisk

Alternativer for skanner

/files	skann filer (standard)
/no-files	ikke skann filer
/memory	skann minne
/boots	skann oppstartssektorer
/no-boots	ikke skann oppstartssektorer (standard)
/arch	skann arkiver (standard)

/no-arch	ikke skann arkiver
/max-obj-size=STØRRELSE	skann kun filer som er mindre enn STØRRELSE megabyte (standard 0 = ubegrenset)
/max-arch-level=NIVÅ	maksimalt undernivå for arkiver i arkiver (dybdearkiver) som skal skannes
/scan-timeout=GRENSE	ikke skann arkiv i mer enn GRENSE sekunder
/max-arch-size=STØRRELSE	skann filene i et arkiv hvis de er mindre enn STØRRELSE (standard 0 = ubegrenset)
/max-sfx-size=STØRRELSE	skann kun filene i et selvutpakkende arkiv hvis de er mindre enn STØRRELSE megabyte (standard 0 = ubegrenset)
/mail	skann e-postfiler (standard)
/no-mail	ikke skann e-postfiler
/mailbox	skann postbokser (standard)
/no-mailbox	ikke skann postbokser
/sfx	skann selvutpakkende arkiver (standard)
/no-sfx	ikke skann selvutpakkende arkiver
/rtp	skann runtime packers (standard)
/no-rtp	ikke skann runtime packers
/unsafe	skann etter potensielt usikre programmer
/no-unsafe	ikke skann etter potensielt usikre programmer (standard)
/unwanted	skann etter potensielt uønskede programmer
/no-unwanted	ikke skann etter potensielt uønskede programmer (standard)
/mistenkelig	skann etter mistenkelige programmer (standard)
/ikke mistenkelig	ikke skann etter mistenkelige programmer
/pattern	bruk signaturer (standard)
/no-pattern	ikke bruk signaturer
/heur	aktiver heuristikk (standard)
/no-heur	deaktiver heuristikk
/adv-heur	aktiver Avansert heuristikk (standard)
/no-adv-heur	deaktiver Avansert heuristikk
/ext=FILTYPER	skann kun FILTYPER, adskilt med kolon
/ext-exclude=FILTYPER	utelat FILTYPER, adskilt med kolon, fra skanning
/clean-mode=MODUS	bruk rensemodusen MODUS for infiserte objekter Følgende alternativer er tilgjengelige: • ingen – Ingen automatisk rensing vil skje. • standard (standardverdi) – ecls.exe vil forsøke å rense eller slette infiserte filer automatisk. • streng – ecls.exe vil forsøke å rense eller slette infiserte filer automatisk uten at brukeren må foreta seg noe (du vil ikke bli spurt før filene er slettet). • grundig – ecls.exe vil slette filer uten å forsøke å rense dem uavhengig av hvilken fil det er snakk om. • slett – ecls.exe vil slette filer uten å forsøke å rense dem, men vil ikke slette sensitive filer som f.eks. Windows-systemfiler.
/quarantine	kopier infiserte filer (hvis de renses) til Karantene (supplerer handlingen som blir utført under rensing)
/no-quarantine	ikke kopier infiserte filer til Karantene

Generelle alternativer

/help	vis hjelpefil og avslutt
/version	vis versjonsinformasjon og avslutt
/preserve-time	bevar tidsmerket for forrige tilgang

Avslutningskoder

0	ingen trusler funnet
1	trussel funnet og renset
10	noen filer kunne ikke skannes (kan være trusler)
50	trussel funnet
100	feil

MERKNAD: Avslutningskoder større enn 100 betyr at filen ikke ble skannet og dermed kan være infisert.

3.10.5 Gjenkjenning av inaktiv tilstand

Innstillingene for gjenkjenning av inaktiv tilstand konfigureres i **Avansert oppsett** under **Antivirus** > **Skanning i inaktiv tilstand** > **Gjenkjenning av inaktiv tilstand**. Disse innstillingene definerer en utløser for Inaktivitetsskanning når:

- skjermspareren kjører,
- datamaskinen er låst,
- en bruker logger seg av.

Bruk bryterne for hver enkelt tilstand for å aktivere eller deaktivere utløserne for gjenkjenning av inaktiv tilstand.

3.10.6 ESET SysInspector

3.10.6.1 Innføring i ESET SysInspector

Programmet ESET SysInspector foretar en grundig kontroll av datamaskinen og viser en omfattende oversikt over dataene som er innsamlet. Informasjon om hvilke drivere og programmer som er installert, nettverkstilkoblinger og viktige registeroppføringer kan hjelpe deg med å undersøke mistenkelig systemoppførsel og finne ut om den skyldes inkompatibel program- og maskinvare eller at maskinen er infisert av skadelig programvare.

Du kan få tilgang til ESET SysInspector på to måter: Fra den integrerte versjonen i ESET Security eller ved å laste ned den frittstående versjonen (SysInspector.exe) gratis fra ESET's nettsted. Begge versjoner er identiske i funksjon og har samme programmkontroller. Den eneste forskjellen er hvordan utdataene blir administrert. Både den frittstående og den integrerte versjonen lar deg eksportere systemavbildninger til en *.xml*-fil og lagre dem på disk. Den integrerte versjonen lar deg imidlertid også lagre systemavbildninger direkte i **Verktøy** > **ESET SysInspector** (unntatt ESET Remote Administrator). Du finner mer informasjon i delen ESET SysInspector som en del av ESET Endpoint Security.

Beregn noe tid til at ESET SysInspector skanner datamaskinen din. Det kan ta fra 10 sekunder til noen minutter, avhengig av maskinvarekonfigurasjon, operativsystem og antall programmer installert på datamaskinen.

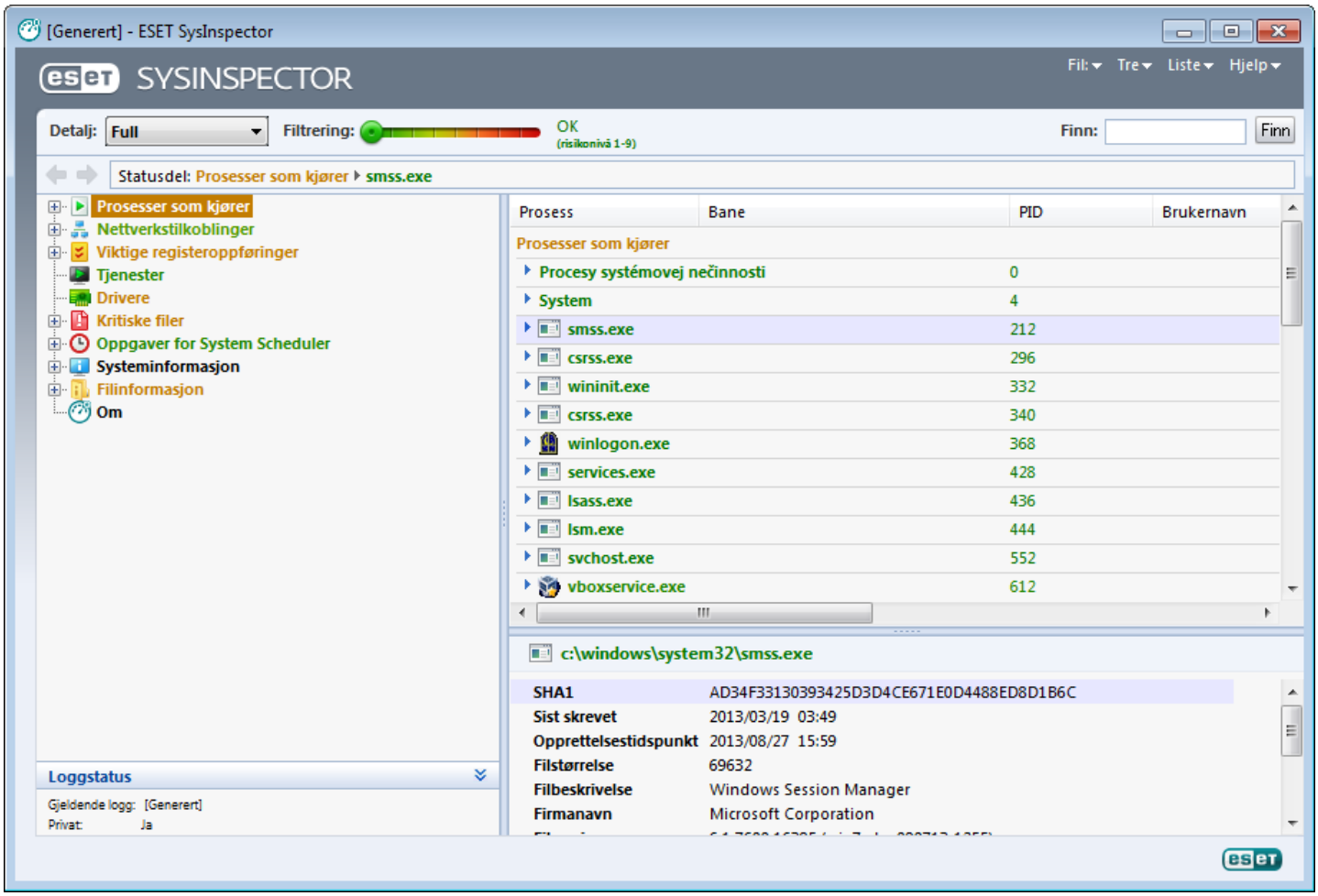
3.10.6.1.1 Starter ESET SysInspector

For å starte ESET SysInspector, kjører du ganske enkelt det kjørbare programmet *SysInspector.exe* som du laster ned fra ESETs nettsted. Hvis du allerede har et av ESET Security-produktene installert, kan du kjøre ESET SysInspector direkte fra startmenyen (klikk **Programmer** > **ESET** > **ESET Endpoint Security**).

Vent mens programmet inspiserer systemet ditt. Dette kan ta opptil flere minutter.

3.10.6.2 Brukergrensesnitt og bruk av programmet

For å gjøre det oversiktlig er hovedprogramvinduet delt inn i fire deler - Programkontroller øverst i hovedprogramvinduet, Navigasjon-vinduet til venstre, Beskrivelse-vinduet til høyre og Detaljer-vinduet nederst til høyre i hovedprogramvinduet. Avsnittet Loggstatus lister opp basisparametrene i en logg (filter brukt, filtertype, er loggen et resultat av en sammenligning, osv.).



3.10.6.2.1 Programkontroller

Denne delen beskriver alle programkontrollene som er tilgjengelige i ESET SysInspector.

Fil

Når du klikker **Fil**, kan du lagre systemstatusen for senere undersøkelser eller åpne en tidligere lagret logg. For publiseringsformål anbefaler vi at du genererer en logg **Egnet for sending**. I denne formen sender loggen ut følsom informasjon (navn på gjeldende bruker, datamaskinnavn, domenenavn, gjeldende brukerrettigheter, miljøvariabler osv.).

MERKNAD: Du kan åpne tidligere lagrede ESET SysInspector-rapporter ved å dra og slippe dem i hovedprogramvinduet.

Tre

Gjør det mulig å utvide eller lukke alle noder og eksportere utvalgte deler til tjenesteskript.

Liste

Inneholder funksjoner for enklere navigering i programmet samt andre funksjoner, for eksempel å finne informasjon på Internett.

Hjelp

Inneholder informasjon om programmet og funksjonene.

Informasjon

Denne innstillingen påvirker informasjonen som vises i hovedprogramvinduet for å gjøre det lettere å arbeide med informasjonen. I Grunnleggende modus har du tilgang til informasjon som brukes til å finne løsninger på vanlige problemer i systemet. I Middels modus viser programmet mindre brukte detaljer. I Full modus viser ESET SysInspector all informasjon som trengs for å kunne løse spesifikke problemer.

Filtrering

Elementfiltrering brukes til å finne mistenkelige filer eller registeroppføringer i systemet. Ved å justere glidebryteren kan du filtrere elementer etter risikonivå. Hvis glidebryteren står helt til venstre (risikonivå 1), vises alle elementene. Når du flytter glidebryteren mot høyre, filtrerer programmet vekk alle elementer som er mindre farlige enn gjeldende risikonivå. Da vises bare elementer som er mer mistenkelige enn det viste nivået. Hvis glidebryteren står helt til høyre, viser programmet bare elementer man vet er skadelige.

Alle elementer som er merket som risiko 6 til 9, kan utgjøre en sikkerhetsrisiko. Hvis du ikke bruker noen sikkerhetsløsning fra ESET, anbefaler vi at du skanner systemet med ESET Online Scanner hvis ESET SysInspector har funnet et slikt element. ESET Online Scanner er en gratis tjeneste.

MERKNAD: Du kan raskt fastsette risikonivået til et element ved å sammenlikne fargen på elementet med fargen på risikonivå-glidebryteren.

Sammenlikne

Når du sammenlikner to logger, kan du velge om du vil vise alle postene, vise bare poster som er lagt til, vise bare poster som er fjernet, eller vise bare poster som er erstattet.

Finn

Du kan bruke Søk til å finne et bestemt element etter navn eller en del av navnet. Søkeresultatene vises i Beskrivelse-vinduet.

Retur

Ved å klikke på tilbake- eller foroverpilen kan du gå tilbake til tidligere vist informasjon i Beskrivelse-vinduet. Du kan bruke tilbaketasten og mellomromstasten i stedet for å klikke deg frem og tilbake.

Statusdel

Viser gjeldende node i Navigasjon-vinduet.

Viktig: Elementer som er uthevet i rødt, er ukjente. Det er derfor programmet markerer dem som potensielt farlige. Hvis et element er rødt, betyr det ikke automatisk at du kan slette filen. Før du sletter filer må du forvisse deg om at de virkelig er farlige eller unødvendige.

3.10.6.2.2 Navigere i ESET SysInspector

ESET SysInspector deler ulike typer informasjon inn i en rekke grunndeler som kalles noder. Du kan finne flere detaljer ved å utvide nodene i undernoder. Når du skal åpne eller skjule en node, dobbeltklikker du nodenavnet, eller klikker ⊞ eller ⊟ ved siden av nodenavnet. Når du går gjennom trestrukturen av noder og undernoder i Navigasjon-vinduet, kan du finne ulike detaljer for hver node i Beskrivelse-vinduet. Hvis du går gjennom elementene i Beskrivelse-vinduet, kan det vises ytterligere informasjon om hvert element i Detaljer-vinduet.

Det følgende er beskrivelser av hovednodene i Navigasjon-vinduet og relatert informasjon i vinduene Beskrivelse og Detaljer.

Prosesser som kjører

Denne noden inneholder informasjon om programmer og prosesser som kjører når rapporten genereres. I Beskrivelse-vinduet kan du finne ytterligere detaljer for hver prosess, for eksempel dynamiske biblioteker som

brukes av prosessen, og deres plassering i systemet, navnet på programleverandøren og filens risikonivå.

Informasjon-vinduet inneholder tilleggsinformasjon for elementer som er valgt i Beskrivelse-vinduet, for eksempel filstørrelse eller firkanttegn.

MERKNAD: Et operativsystem består av en rekke viktige kjernekomponenter som kjører hele tiden og sørger for grunnleggende og nødvendige funksjoner for brukerprogrammene. I noen tilfeller vises slike prosesser i ESET SysInspector med en filbane som starter med \??\. Disse symbolene forhåndsoptimaliserer prosessene. De er trygge å bruke for systemet.

Nettverkstilkoblinger

Beskrivelse-vinduet inneholder en liste over prosesser og programmer som kommuniserer i nettverket ved å bruke protokollen som er valgt i Navigasjon-vinduet (TCP eller UDP), og den eksterne adressen som programmet er tilkoblet. Du kan også sjekke IP-adressene til DNS-servere.

Informasjon-vinduet inneholder tilleggsinformasjon for elementer som er valgt i Beskrivelse-vinduet, for eksempel filstørrelse eller firkanttegn.

Viktige registeroppføringer

Inneholder en liste over valgte registeroppføringer som ofte er relatert til ulike systemproblemer, for eksempel de som spesifiserer oppstartsprogrammer, nettleserhjelperobjekter (BHO) osv.

I Beskrivelse-vinduet kan du finne ut hvilke filer som er knyttet til bestemte registeroppføringer. Du kan se flere detaljer i Detaljer-vinduet.

Tjenester

Beskrivelse-vinduet inneholder en liste over filer som er registrert som Windows-tjenester. Du kan kontrollere hvordan tjenesten skal starte og vise spesifikke detaljer om filen, i Detaljer-vinduet.

Drivere

En liste over drivere som er installert i systemet.

Kritiske filer

Beskrivelse-vinduet viser innholdet av kritiske filer som er knyttet til operativsystemet Microsoft Windows.

Oppgaver for System Scheduler

Inneholder en liste over oppgaver som utløses av Windows Task Scheduler til bestemte tider/intervaller.

Systeminformasjon

Inneholder detaljert informasjon om maskinvare og programvare samt informasjon om miljøvariabler, brukerrettigheter og systemhendelseslogger.

Filinformasjon

En liste over viktige systemfiler og andre filer i Programfiler-mappen. Du kan finne ytterligere informasjon om filene i vinduene Beskrivelse og Detaljer.

Om

Informasjon om ESET SysInspector-versjon og listen over programmoduler.

3.10.6.2.2.1 Hurtigtaster

Hurtigtaster du kan bruke når du arbeider med ESET SysInspector, inkluderer:

Fil

Ctrl+O	åpner eksisterende logg
Ctrl+S	lagrer opprettede logger

Genererer

Ctrl+G	genererer en standardavbildning av datamaskinstatusen
Ctrl+H	genererer en avbildning av datamaskinstatusen som også kan logge sensitiv informasjon

Elementfiltrering

1, O	ok, elementer på risikonivå 1-9 vises
2	ok, elementer på risikonivå 2-9 vises
3	ok, elementer på risikonivå 3-9 vises
4, U	ukjent, elementer på risikonivå 4-9 vises
5	ukjent, elementer på risikonivå 5-9 vises
6	ukjent, elementer på risikonivå 6-9 vises
7, B	risikofylt, elementer på risikonivå 7–9 vises
8	risikofylt, elementer på risikonivå 8–9 vises
9	risikofylt, elementer på risikonivå 9 vises
-	reduserer risikonivået
+	øker risikonivået
Ctrl+9	filtreringsmåte, likt nivå eller høyere
Ctrl+0	filtreringsmåte, kun likt nivå

Vis

Ctrl+5	vis etter forhandler, alle forhandlere
Ctrl+6	vis etter forhandler, bare Microsoft
Ctrl+7	vis etter forhandler, alle andre forhandlere
Ctrl+3	viser alle detaljer
Ctrl+2	viser noen detaljer
Ctrl+1	grunnleggende visning
Tilbaketast	går ett trinn tilbake
Mellomromst ast	går ett trinn frem
Ctrl+W	utvider tre
Ctrl+Q	skjuler tre

Andre kontroller

Ctrl+T	går til den opprinnelige plasseringen til elementet etter valg i søkeresultater
Ctrl+P	viser grunnleggende informasjon om et element
Ctrl+A	viser all informasjon om et element
Ctrl+C	kopierer treet til gjeldende element
Ctrl+X	kopierer elementer
Ctrl+B	finner informasjon om valgte filer på Internett
Ctrl+L	åpner mappen hvor den valgte filen ligger
Ctrl+R	åpner den tilhørende oppføringen i verktøyet for registerredigering
Ctrl+Z	kopierer banen til en fil (hvis elementet er knyttet til en fil)
Ctrl+F	går til søkefeltet
Ctrl+D	lukker søkeresultatene
Ctrl+E	kjøre tjenesteskript

Sammenlikner

Ctrl+Alt+O	åpner opprinnelig logg / sammenlikningslogg
Ctrl+Alt+R	avbryter sammenlikning
Ctrl+Alt+1	viser alle elementer
Ctrl+Alt+2	viser bare tilføyde elementer, loggen vil vise elementene i gjeldende logg
Ctrl+Alt+3	viser bare fjernede elementer, loggen vil vise elementene i forrige logg
Ctrl+Alt+4	viser bare utskiftede elementer (inkl. filer)
Ctrl+Alt+5	viser bare forskjeller mellom logger
Ctrl+Alt+C	viser sammenlikning
Ctrl+Alt+N	viser gjeldende logg
Ctrl+Alt+P	åpner forrige logg

Diverse

F1	viser hjelp
Alt+F4	lukker programmet
Alt+Shift+F4	lukker programmet uten å spørre
Ctrl+I	loggstatistikk

3.10.6.2.3 Sammenlikne

Sammenlign-funksjonen lar brukeren sammenligne to eksisterende logger. Resultatet av funksjonen er et sett elementer som ikke finnes i begge loggene. Dette er nyttig hvis du vil ha oversikt over endringer i systemet, et nyttig verktøy for gjenkjenning av skadelig kode.

Etter at det er startet, oppretter programmet en ny logg som vises i et nytt vindu. Klikk **Fil** > **Lagre logg** hvis du vil lagre en logg i en fil. Loggfiler kan åpnes og gjennomgås på et senere tidspunkt. Hvis du vil åpne en eksisterende logg, klikker du **Fil** > **Åpne logg**. ESET SysInspectorviser alltid én logg om gangen i hovedprogramvinduet.

Fordelen med å sammenligne to logger er at du kan vise en aktiv logg og en logg som er lagret i en fil. Når du vil sammenligne logger, klikker du **Fil** > **Sammenligne logger** og velger **Velg fil**. Den valgte loggen vil bli sammenliknet med den aktive loggen i hovedprogramvinduene. Sammenligningsloggen vil bare vise forskjeller mellom de to loggene.

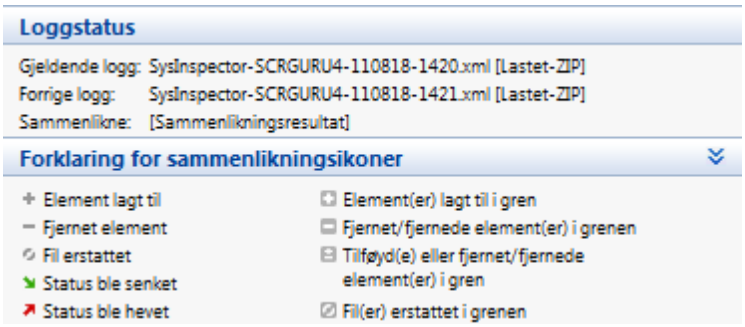
MERKNAD: Du sammenligner to loggfiler ved å klikke **Fil** > **Lagre logg** for å lagre som en ZIP-fil. Begge filene blir da lagret. Hvis du åpner denne filen senere, sammenliknes automatisk loggene den inneholder.

Ved siden av de viste elementene viser ESET SysInspector symboler som identifiserer forskjellene mellom de sammenliknede loggene.

Beskrivelse av symboler som kan vises ved siden av elementer:

- + ny verdi, ikke til stede i den forrige loggen
- trestrukturdelen inneholder nye verdier
- – fjernet verdi, til stede bare i den forrige loggen
- trestrukturdelen inneholder fjernede verdier
- verdi / filen er endret
- trestrukturdelen inneholder modifiserte verdier / filer
- risikonivået har sunket / det var høyere i den forrige loggen
- risikonivået har økt / det var lavere i den forrige loggen

Forklaringsdelen som vises nederst til venstre, inneholder alle symbolene og viser også navnene på loggene som sammenliknes.



Enhver sammenlikningslogg kan lagres i en fil og åpnes senere.

Eksempel

Generer og lagre en logg, som registrerer originalinformasjon om systemet, i en fil med navnet forrige.xml. Etter at det er gjort endringer i systemet, åpner du ESET SysInspector og lar den generere en ny logg. Lagre den i en fil med navnet *gjeldende.xml*.

Når du vil spore endringer mellom de to loggene, klikker du **Fil** > **Sammenligne logger**. Programmet vil opprette en sammenlikningslogg som viser forskjellene mellom loggene.

Samme resultat kan oppnås ved at du skriver følgende på kommandolinjen:

SysIsnpector.exe current.xml previous.xml

3.10.6.3 Kommandolinjeparametre

ESET SysInspector støtter rapportgenerering fra kommandolinjen ved hjelp av disse parametrene:

/gen	genererer en logg direkte fra kommandolinjen uten å kjøre GUI
/privacy	genererer en logg uten følsom informasjon
/zip	lagre loggen i komprimert zip-arkiv
/silent	ikke vis fremdriftsvindu ved generering av logg fra kommandolinjen
/blank	start ESET SysInspector uten å generere/laste loggen

Eksempler

Bruk:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Hvis du vil laste en bestemt logg direkte inn i nettleseren, bruker du: *SysInspector.exe .\clientlog.xml*
Hvis du vil generere en logg fra kommandolinjen, bruker du: *SysInspector.exe /gen=.\mynewlog.xml*
Hvis du vil generere en logg uten følsom informasjon direkte i en komprimert fil, bruker du: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Hvis du vil sammenligne to loggfiler og bla gjennom forskjeller, bruker du: *SysInspector.exe new.xml old.xml*

MERKNAD: Hvis navnet på filen/mappen inneholder et mellomrom, må det settes i enkle anførselstegn (omvendt komma).

3.10.6.4 Tjenesteskript

Tjenesteskript er et verktøy som hjelper kunder som bruker ESET SysInspector ved å fjerne uønskede objekter fra systemet på en enkel måte.

Tjenesteskript gjør at brukeren kan eksportere hele ESET SysInspector-loggen eller deler av den. Etter eksport kan du markere uønskede objekter for sletting. Deretter kan du kjøre den modifiserte loggen for å slette markerte objekter.

Tjenesteskript passer for avanserte brukere med erfaring i å løse systemproblemer. Ukvalifiserte endringer kan føre til skade på operativsystemet.

Eksempel

Hvis du mistenker at datamaskinen har fått et virus som ikke er blitt oppdaget av antivirusprogrammet, følger du den trinnvise instruksen nedenfor:

1. Kjør ESET SysInspector for å generere en ny systemavbildning.
2. Velg det første elementet i delen til venstre (i trestrukturen), trykk på Shift og velg det siste elementet for å markere alle elementene.
3. Høyreklikk valgte objekter og velg **Eksporter valgte seksjoner til tjenesteskript**.
4. De valgte objektene vil bli eksportert til en ny logg.
5. Dette er det viktigste trinnet i hele prosedyren: åpne den nye loggen og endre attributtet - til + for alle objekter du vil fjerne. Pass på så du ikke markerer noen viktige operativsystemfiler/-objekter.
6. Åpne ESET SysInspector, klikk **Fil** > **Kjør tjenesteskript** og angi banen til skriptet.
7. Klikk **OK** for å kjøre skriptet.

3.10.6.4.1 Generere tjenesteskript

Når du skal generere et skript, høyreklikker du på et element fra menytreet (i den venstre ruten) i ESET SysInspectors hovedvindu. Fra hurtigmenyen velger du enten **Eksporter alle deler til tjenesteskript** eller **Eksporter utvalgte deler til tjenesteskript**.

MERKNAD: Det er ikke mulig å eksportere tjenesteskriptet når to logger sammenlignes.

3.10.6.4.2 Strukturen i tjenesteskriptet

På den første linjen i skriptets overskrift kan du finne informasjon om motorversjon (ev), GUI-versjon (gv) og Loggversjon (lv). Du kan bruke disse dataene til å spore mulige endringer i .xml-filen som genererer skriptet, og hindre eventuelle inkonsistenser under utføring. Denne delen av skriptet bør ikke endres.

Resten av filen er delt i deler der elementer kan redigeres (angi de som vil bli behandlet av skriptet). Du merker elementer for behandling ved å erstatte tegnet "-" foran et element med tegnet "+". Delene i skriptet er atskilt fra hverandre med en tom linje. Hver del har et nummer og en tittel.

01) Kjøre prosesser

Denne delen inneholder en liste over alle prosesser som kjører i systemet. Hver prosess er identifisert av sin UNC-bane, og dernest av sin CRC16 hash-kode i asterisker (*).

Eksempel:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

I dette eksempelet ble en prosess, module32.exe, valgt (merket av et "+"-tegn). Prosessen vil avsluttes etter utførelse av skriptet.

02) Innlastede moduler

Denne delen lister opp systemmoduler som brukes i øyeblikket.

Eksempel:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

I dette eksempelet var modulen khbekhb.dll merket med en "+". Når skriptet kjører, vil det kjenne igjen prosessene som bruker den bestemte modulen og avslutte dem.

03) TCP-tilkoblinger

Denne delen inneholder informasjon om eksisterende TCP-tilkoblinger.

Eksempel:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Når skripter kjører, vil det finne eieren av socketen i de merkede TCP-tilkoblingene og stoppe socketen, og dermed frigjøre systemressurser.

04) UDP-endepunkter

Denne delen inneholder informasjon om eksisterende UDP-endepunkter.

Eksempel:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Når skripter kjører, vil det isolere eieren av socketen i de merkede UDP-endepunktene og stoppe socketen.

05) DNS-serveroppføringer

Denne delen inneholder informasjon om gjeldende DNS-serverkonfigurering.

Eksempel:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Merkede DNS-serveroppføringer vil bli fjernet når du kjører skriptet.

06) Viktige registeroppføringer

Denne delen inneholder informasjon om viktige registeroppføringer.

Eksempel:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

De merkede oppføringene vil bli slettet, redusert til 0-byteverdier eller tilbakestilt til sine standardverdier etter utføring av skriptet. Handlingen som skal skje med en bestemt oppføring, avhenger av oppføringens kategori og nøkkelverdi i det bestemte registeret.

07) Tjenester

Denne delen lister opp tjenester registrert innenfor systemet.

Eksempel:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

De merkede tjenestene og deres avhengige tjenester vil bli stoppet og avinstallert når skriptet utføres.

08) Drivere

Denne delen lister opp installerte drivere.

Eksempel:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Når du kjører skriptet, stopper de valgte driverne. Merk at noen drivere ikke tillater å bli stoppet.

09) Kritiske filer

Denne delen inneholder informasjon om filer som er kritiske for at operativsystemet skal fungere riktig.

Eksempel:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

De valgte elementene vil enten bli slettet eller tilbakestilt til sine opprinnelige verdier.

3.10.6.4.3 Utføre tjenesteskript

Merk alle ønskede elementer, og lagre og lukk deretter skriptet. Kjør det redigerte skriptet direkte fra ESET SysInspectors hovedvindu ved å velge alternativet **Kjør tjenesteskript** fra Fil-menyen. Når du åpner et skript, vil programmet veilede deg med følgende melding: **Er du sikker på at du vil kjøre tjenesteskriptet "%Scriptname%" ?** Etter at du har bekreftet valget ditt, vises kanskje en annen advarsel som informerer deg om at tjenesteskriptet du prøver å kjøre, ikke er undertegnet. Klikk **Kjør** for å starte skriptet.

Et dialogboksvindu vil bekrefte om kjøringen av skriptet var vellykket.

Hvis skriptet bare kunne behandles delvis, vil et dialogboksvindu med følgende melding vises: **Tjenesteskriptet ble delvis kjørt. Ønsker du å vise feilrapporten?** Velg **Ja** for å vise en kompleks feilrapport som lister opp de operasjonene som ikke ble utført.

Hvis skriptet ikke ble gjenkjent, vil et dialogboksvindu med følgende melding vises: **Det valgte tjenesteskripet er ikke undertegnet. Kjøring av usignerte og ukjente skript kan skade dataene på maskinen din alvorlig. Er du sikker på at du ønsker å kjøre skriptet og gjennomføre handlingene?** Dette skyldes kanskje inkonsistens inne i skriptet (skadet overskrift, ødelagt avsnittstittel, tom linje som mangler mellom delene osv.). Du kan enten åpne skriptfilen på nytt og rette opp feilene inne i skriptet eller opprette et nytt tjenesteskript.

3.10.6.5 Vanlige spørsmål

Kreves det administratorrettigheter for å kunne kjøre ESET SysInspector?

Selv om det ikke kreves administratorrettigheter for å kunne kjøre ESET SysInspector, vil en del av informasjonen som samles inn, bare være tilgjengelig fra en administratorkonto. Hvis du kjører programmet som vanlig bruker eller begrenset bruker, vil det samles inn mindre informasjon om datamaskinmiljøet.

Oppretter ESET SysInspector en loggfil?

ESET SysInspector kan opprette en loggfil med konfigurasjonen til datamaskinen. Hvis du vil lagre en slik fil, klikker du **Fil** > **Lagre logg** i hovedprogramvinduet. Loggfiler lagres i XML-format. Filene lagres som standard i katalogen *%USERPROFILE%\My Documents*, med filnavnkonvensjonen "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Du kan om ønskelig endre loggfilens plassering og navn før du lagrer den.

Hvordan viser jeg ESET SysInspector-loggfilen?

Når du vil vise en loggfil opprettet med ESET SysInspector, kjører du programmet og klikker **Fil** > **Åpne logg** i hovedprogramvinduet. Du kan også dra og slippe filer på ESET SysInspector-programmet. Hvis du ofte har behov for å vise ESET SysInspector-loggfiler, anbefaler vi at du oppretter en snarvei til filen SYSINSPECTOR.EXE på skrivebordet. Da kan du vise loggfilene ved å dra og slippe dem på snarveien. Av sikkerhetsgrunner tillater kanskje ikke Windows Vista/7 dra og slipp mellom vinduer som har forskjellige sikkerhetsinnstillinger.

Er det mulig å skaffe en spesifikasjon av loggfilformatet? Hva med en SDK (programutviklingspakke)?

For tiden finnes det verken en spesifikasjon av loggfilene eller en SDK, noe som skyldes at programmet fortsatt er under utvikling. Når programmet er endelig utgitt, kan det hende at vi gjør dette tilgjengelig, avhengig av kundenes tilbakemeldinger og behov.

Hvordan vurderer ESET SysInspector risikoen knyttet til bestemte objekter?

ESET SysInspector tildeler som regel risikonivå til objekter (filer, prosesser, registernøkler osv.) ved å bruke en rekke heuristiske regler som undersøker egenskapene til hvert objekt og deretter vurderer potensialet for skadelig aktivitet. Basert på denne heuristikken blir objektene tilordnet et risikonivå fra 1 - OK (grønt) til 9 - Risikofylt (rødt). I venstre navigasjonsrute er de ulike delene farget etter det høyeste risikonivået som forekommer blant objektene i den aktuelle delen.

Betyr risikonivå "6 - Ukjent (rødt)" at et objekt er farlig?

Evalueringene til ESET SysInspector garanterer ikke at et objekt er skadelig - denne beslutningen bør tas av en sikkerhetsekspert. Det ESET SysInspector er laget for, er å gi sikkerhetseksperter en rask evaluering slik at de vet hvilke objekter i et system de kanskje vil undersøke nærmere med hensyn til uvanlig oppførsel.

Hvorfor kobler ESET SysInspector seg til Internett når det kjøres?

I likhet med mange andre programmer har ESET SysInspector et "sertifikat" som er signert med en digital signatur som sikrer at programvaren er utgitt av ESET og ikke er endret. For å kunne verifisere sertifikatet kontakter operativsystemet en sertifikatautoritet for å verifisere identiteten til programvareutgiveren. Dette er normal oppførsel for alle digitalt signerte programmer under Microsoft Windows.

Hva er Anti-Stealth-teknologi?

Anti-Stealth-teknologien gir effektiv gjenkjennelse av rootkits.

Hvis systemet angripes av skadelig kode som oppfører seg som en rootkit, kan brukeren være utsatt for tap eller tyveri av data. Uten et spesielt anti-rootkit-verktøy er det nesten umulig å oppdage rootkits.

Hvorfor forekommer det av og til filer merket som "Signert av MS", som samtidig har en annen "Selskapsnavn"-oppføring?

Når ESET SysInspector prøver å identifisere den digitale signaturen til en kjørbar fil, søker det først etter om det finnes en digital signatur innebygd i filen. Hvis det finnes en digital signatur, blir filen validert med den informasjonen. Hvis det ikke finnes en digital signatur, begynner ESI å lete etter den tilsvarende CAT-filen (Sikkerhetskatalog - *%systemroot%\system32\catroot*) som inneholder informasjon om den kjørbare filen som behandles. Hvis den aktuelle CAT-filen blir funnet, vil den digitale signaturen til denne CAT-filen bli brukt i valideringsprosessen for den kjørbare.

Dette er grunnen til at det noen ganger finnes filer merket som "Signert av MS", men som har en annen "Selskapsnavn"-oppføring.

3.10.6.6 ESET SysInspector som en del av ESET Endpoint Security

Når du vil åpne ESET SysInspector-delen i ESET Endpoint Security, klikker du **Verktøy** > **ESET SysInspector**. Administrasjonssystemet i ESET SysInspector-vinduet ligner på det som finnes i datamaskinens skannelogger eller i planlagte oppgaver. Alle operasjoner med systemavbildning – opprette, vise, sammenlikne, fjerne og eksportere – er bare ett eller to klikk unna.

ESET SysInspector-vinduet inneholder grunnleggende informasjon om de opprettede avbildningene, for eksempel opprettingstid, kort kommentar, navn på brukeren som opprettet avbildningen og status på avbildningen.

Når du skal sammenlikne, opprette eller slette avbildninger, bruker du de tilsvarende knappene under avbildningslisten i ESET SysInspector-vinduet. Disse alternativene finner du også på hurtigmenyen. Når du skal vise den valgte systemavbildningen, velger du **Vis** på hurtigmenyen. Når du skal eksportere den valgte avbildningen til en fil, høyreklikker du avbildningen og velger **Eksporter**.

Her er en detaljert beskrivelse av de tilgjengelige alternativene:

- **Sammenlikne** – Gjør det mulig å sammenlikne to eksisterende logger. Den egner seg hvis du ønsker å spore endringer mellom gjeldende logg og en eldre logg. For at dette alternativet skal tre i kraft, må du velge to avbildninger som skal sammenlignes.
- **Opprett...** – Oppretter en ny oppføring. Men først må du lage en kort kommentar om oppføringen. Hvis du vil finne avbildningsfremdriften (av den genererte avbildningen), kan du se kolonnen **Status**. Alle fullførte avbildninger merkes med statusen **Opprettet**.
- **Fjern** – Fjerner oppføringer fra listen.
- **Eksporter...** – Lagrer den valgte oppføringen i en XML-fil (også i en zippet versjon).

3.11 Ordliste

3.11.1 Trusseltyper

En infiltrering er skadelig programvare som prøver å få tilgang til og/eller skade brukerens datamaskin.

3.11.1.1 Virus

Et datavirus er skadelig kode som legges til før eller etter eksisterende filer på datamaskinen din. Virus har fått navnet sitt etter biologiske virus, fordi de bruker liknende metoder for å spre seg fra én datamaskin til en annen. Termen "virus" brukes ofte feilaktig i betydningen en type trussel. Denne bruken blir gradvis mindre vanlig og erstattes av den nye, mer nøyaktige betegnelsen "skadelig programvare".

Datavirus angriper hovedsakelig kjørbare filer og dokumenter. Dette er kort fortalt hvordan et datavirus fungerer: Når en infisert fil kjøres, blir den skadelige koden kalt opp og kjørt før det opprinnelige programmet kjøres. Et virus kan infisere alle filene som gjeldende bruker har skrivetilgang til.

Datavirus kan være forskjellige når det gjelder formål og alvorlighetsgrad. Noen av dem er svært farlige på grunn av deres evne til å slette filer fra en harddisk. På det annen side er det enkelte virus som ikke forårsaker noen skade - de bare irriterer brukeren og viser frem de tekniske ferdighetene til de som har laget dem.

Hvis datamaskinen er infisert med et virus, og det ikke er mulig å rense datamaskinen, kan du sende den til ESETs laboratorium der den vil bli omhyggelig gransket. I visse tilfeller kan infiserte filer endres i så stor grad at det ikke er mulig å rense datamaskinen, og filene må erstattes med en ren kopi.

3.11.1.2 Ormer

En dataorm er et program som inneholder skadelig kode som angriper vertsmaskinen, og som sprer seg via nettverk. Hovedforskjellen mellom et virus og en orm er at ormen har evnen til å spre seg av seg selv. De er ikke avhengig av vertsfiler (eller oppstartssektorer). Ormer sprer seg til e-postadresser i kontaktlisten din eller utnytter sikkerhetssvakheter i nettverksprogrammer.

Ormer er derfor mye mer levedyktige enn datavirus. Fordi Internett er så bredt tilgjengelig, kan ormer spre seg over hele verden i løpet av bare noen få timer, eller til og med minutter etter at de har sluppet fri. Deres evne til å reprodusere seg selv gjør dem mye farligere enn andre typer skadelig programvare.

En orm som er aktivert i et system, kan skape mange vanskeligheter: Den kan slette filer, føre til dårligere systemytelse, og til og med deaktivere programmer. Av natur er en dataorm et slags "transportmiddel" for andre typer infiltreringer.

Hvis datamaskinen din er infisert med en orm, anbefaler vi at du sletter de infiserte filene fordi de sannsynligvis inneholder skadelig kode.

3.11.1.3 Trojanere

Trojanere (trojanske hester) er historisk blitt definert som en klasse trusler som forsøker å fremstå som nyttige programmer, og dermed lurer de brukerne til å kjøre dem.

Fordi trojanere er en svært vid kategori, blir den ofte delt opp i flere underkategorier:

- **Nedlaster** - Skadelige programmer som kan laste ned andre trusler fra Internett.
- **Dropper** - Skadelige programmer som kan legge inn andre typer skadelige programmer på infiserte datamaskiner.
- **Bakdør** - Skadelige programmer som kommuniserer med eksterne angripere og lar dem få tilgang til datamaskinen og ta kontroll over den.
- **Tastelogger** – (tastetrykklogger) - et program som registrerer alle tastetrykk fra brukeren og sender informasjonen til eksterne angripere.
- **Oppringer** – Skadelige programmer beregnet på å koble seg til svært dyre telefonnumre i stedet for brukerens Internett-leverandør. Det er nesten umulig for brukeren å registrere at det blir opprettet en ny tilkobling. Oppringere kan bare skade brukere som benytter oppringt tilkobling med modem, noe som ikke er så vanlig lenger.

Hvis en fil på datamaskinen din blir gjenkjent som en trojaner, anbefaler vi at du sletter den, fordi den høyst sannsynlig inneholder skadelig kode.

3.11.1.4 Rootkits

Rootkits er skadelige programmer som gir Internett-angripere ubegrenset tilgang til et system, mens de skjuler sitt nærvær. Etter å ha fått tilgang til et system (vanligvis ved å utnytte en svakhet i systemet), bruker rootkits funksjoner i operativsystemet for å unngå å bli oppdaget av virusprogramvaren: de skjuler prosesser, filer og Windows-registerdata. Av denne årsak er det nesten umulig å oppdage dem med vanlige testteknikker.

Det finnes to nivåer for gjenkjennelse for å forebygge rootkits:

1. Når de prøver å få tilgang til et system: De er ennå ikke til stede, og er derfor inaktive. De fleste antivirussystemer kan eliminere rootkits på dette nivået (forutsatt at de faktisk gjenkjenner slike filer som infisert).
2. Når de er skjult fra vanlig testing: ESET Endpoint Security brukere har fordelen med Anti-Stealth-teknologien som også kan oppdage og fjerne aktive rootkits.

3.11.1.5 Adware

Adware er en betegnelse på reklamestøttet programvare. Programmer som viser markedsføringsmateriale, faller i denne kategorien. Adware-programmer åpner ofte automatisk et nytt popup-vindu som inneholder reklame i en nettleser, eller endrer nettleserens hjemmeside. Adware følger ofte med gratisprogrammer, slik at utviklere av gratisprogrammer kan dekke utviklingskostnadene til sine (vanligvis nyttige) programmer.

Adware i seg selv er ikke farlig – brukerne blir bare forstyrret med reklame. Faren ligger i at adware også kan utføre sporingsfunksjoner (som spyware gjør).

Hvis du bestemmer deg for å bruke et gratisprodukt, bør du være spesielt oppmerksom på installasjonsprogrammet. Installasjonsprogrammet vil mest sannsynlig varsle deg om installasjon av et ekstra adware-program. Du kan ofte avbryte installasjonen og installere programmet uten adware.

Enkelte programmer kan ikke installeres uten adware, eller de får begrenset funksjonalitet. Dette betyr at adware ofte får tilgang til systemet på en "lovlig" måte, siden brukeren godtar det. I så fall er det best å være føre var. Hvis det gjenkjennes en fil som er adware på datamaskinen, anbefales det å slette den, siden det er høy sannsynlighet for at den inneholder ondsinnet kode.

3.11.1.6 Spyware

Denne kategorien omfatter alle programmer som sender privat informasjon uten at brukeren har gitt samtykke til det, eller er klar over det. Spyware bruker sporingsfunksjoner til å sende forskjellige typer statistiske data, for eksempel en liste over besøkte nettsteder, e-postadresser fra brukerens kontaktliste, eller en liste over registrerte tastetrykk.

De som lager spyware, hevder at disse teknikkene har som mål å finne ut mer om brukernes behov og interesser, slik at man kan skape mer målrettet reklame. Problemet er at det ikke finnes noen klar forskjell på nyttige og skadelige programmer, og ingen kan være sikker på at den hentede informasjonen ikke blir misbrukt. Dataene som hentes ut av spyware-programmer, kan inneholde sikkerhetskoder, PIN-koder, bankkontonumre osv. Spyware er ofte innebygd i gratisversjoner av programvare fra utvikleren, som skal skape inntekt eller sørge for økte muligheter for å få solgt programvaren. Ofte blir brukerne informert under installeringen om at det finnes spyware, slik at de har en mulighet til å oppgradere til en betalt versjon uten spyware.

Eksempler på kjente gratisprodukter som inneholder spyware, er klientprogrammer i P2P-nettverk (node-til-node-nettverk). Spyfalcon eller Spy Sheriff (og mange flere) tilhører en bestemt underkategori av spyware - de ser ut til å være antispyware-programmer, men er i realiteten selv spyware.

Hvis det oppdages en fil som er spyware på datamaskinen, anbefales det å slette den, siden det er høy sannsynlighet for at den inneholder skadelig kode.

3.11.1.7 Pakkere

Pakker er en selvutpakkende kjøretidsfil som kommer med flere typer skadelig programvare i en enkelt pakke.

De vanligste pakkerne er UPX, PE_Compact, PKLite og ASPack. Den samme skadelige programvaren kan oppdages forskjellig når den komprimeres ved bruk av en annen pakker. Pakkere har også muligheten til å få sine "signaturer" til å endre seg over tid, noe som gjør den skadelige programvaren vanskeligere å oppdage og fjerne.

3.11.1.8 Potensielt utrygge programmer

Det er mange lovlige programmer som har som funksjon å forenkle administreringen av maskiner i nettverk. Men i feil hender kan de bli misbrukt til ondsinnede formål. ESET Endpoint Security gir mulighet til å oppdage slike trusler.

Potensielt usikre programmer er en klassifisering som brukes om kommersiell, lovlig programvare. Klassifiseringen inkluderer programmer som for eksempel verktøy for ekstern tilgang, programmer for å knekke passord samt tastlogger (programmer som registrerer alle tastetrykk som foretas av brukeren).

Hvis du oppdager at det kjøres et potensielt usikkert program på maskinen din (og du ikke installerte det), tar du kontakt med den systemansvarlige eller fjerner programmet.

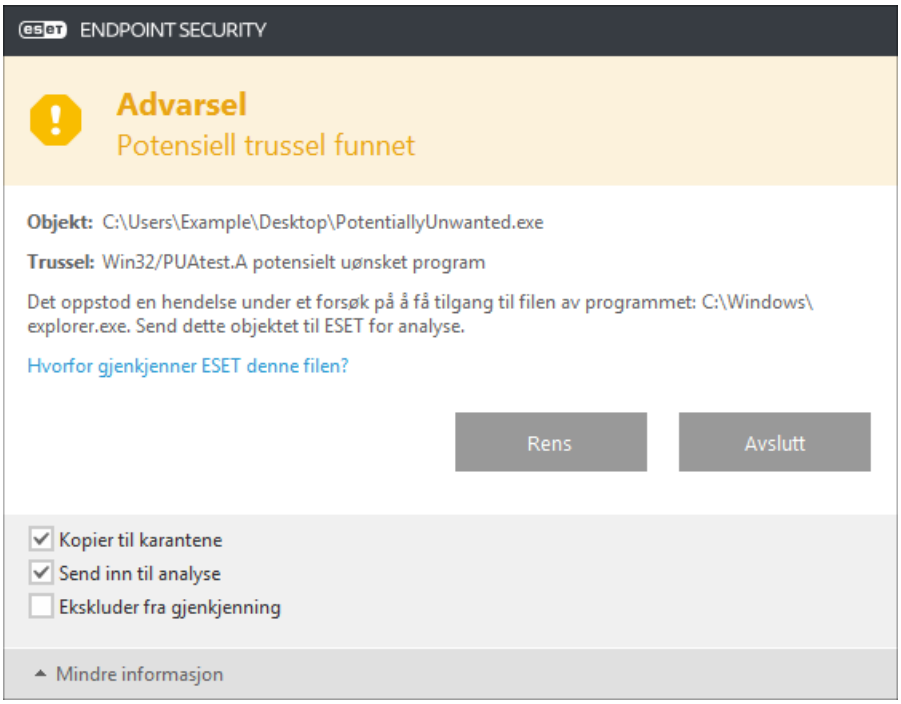
3.11.1.9 Potensielt uønskede programmer

Et potensielt uønsket program er et program som inneholder adware, installerer verktøylinjer, sporer søkeresultater, eller har andre uklare mål. Det er noen situasjoner hvor du kan føle at fordelene med det uønskede programmet oppveier risikoene. Av denne grunnen tildeler ESET slike programmer en lavere risikokategori sammenlignet med andre typer skadelig programvare, slik som trojanske hester og ormer.

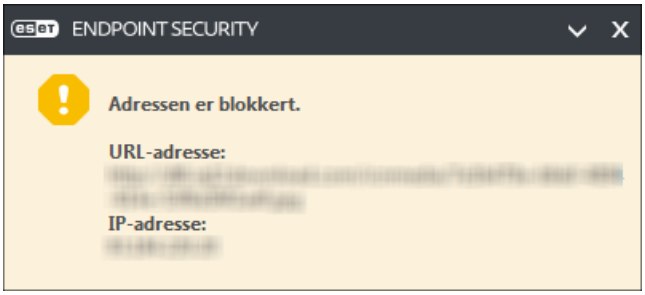
Advarsel – Potensiell trussel funnet

Når et potensielt uønsket program oppdages, vil du kunne velge hvilke handlinger du til utføre:

1. **Rengjøre/Koble fra**: Dette alternativet avslutter handlingen og forhindrer at mulige trusler kommer inn i systemet.
2. **Ingen handling**: Dette alternativet tillater at mulige trusler kommer inn i systemet.
3. For å la programmet kjøre på datamaskinen din i fremtiden uten avbrudd, klikker du på **Mer informasjon/Vis avanserte alternativer** og velg avkrysningsboksen ved siden av **Ekskluder fra gjenkjenning**.

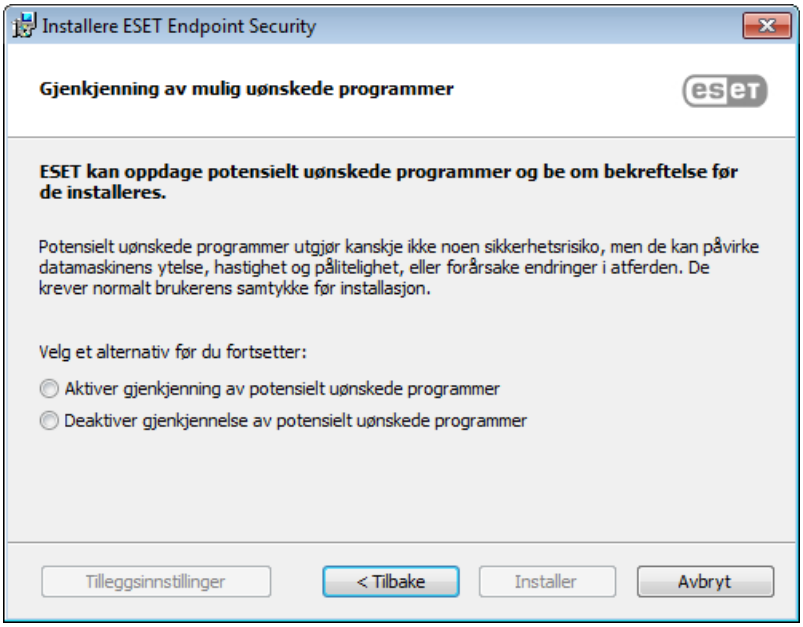


Når et potensielt uønsket program gjenkjennes og det ikke kan rengjøres, vises det et meldingsvindu **Adresse har blitt blokkert** i meldingsområdet nederst til høyre på skjermen. For mer informasjon om denne hendelsen, se **Verktøy** > **Loggfiler** > **Filtrerte nettsteder** på hovedmenyen.



Potensielt uønskede programmer – Innstillinger

Når du installerer ESET-produktet ditt, kan du velge om du vil aktivere gjenkjenning av potensielt uønskede programmer, som vist nedenfor:

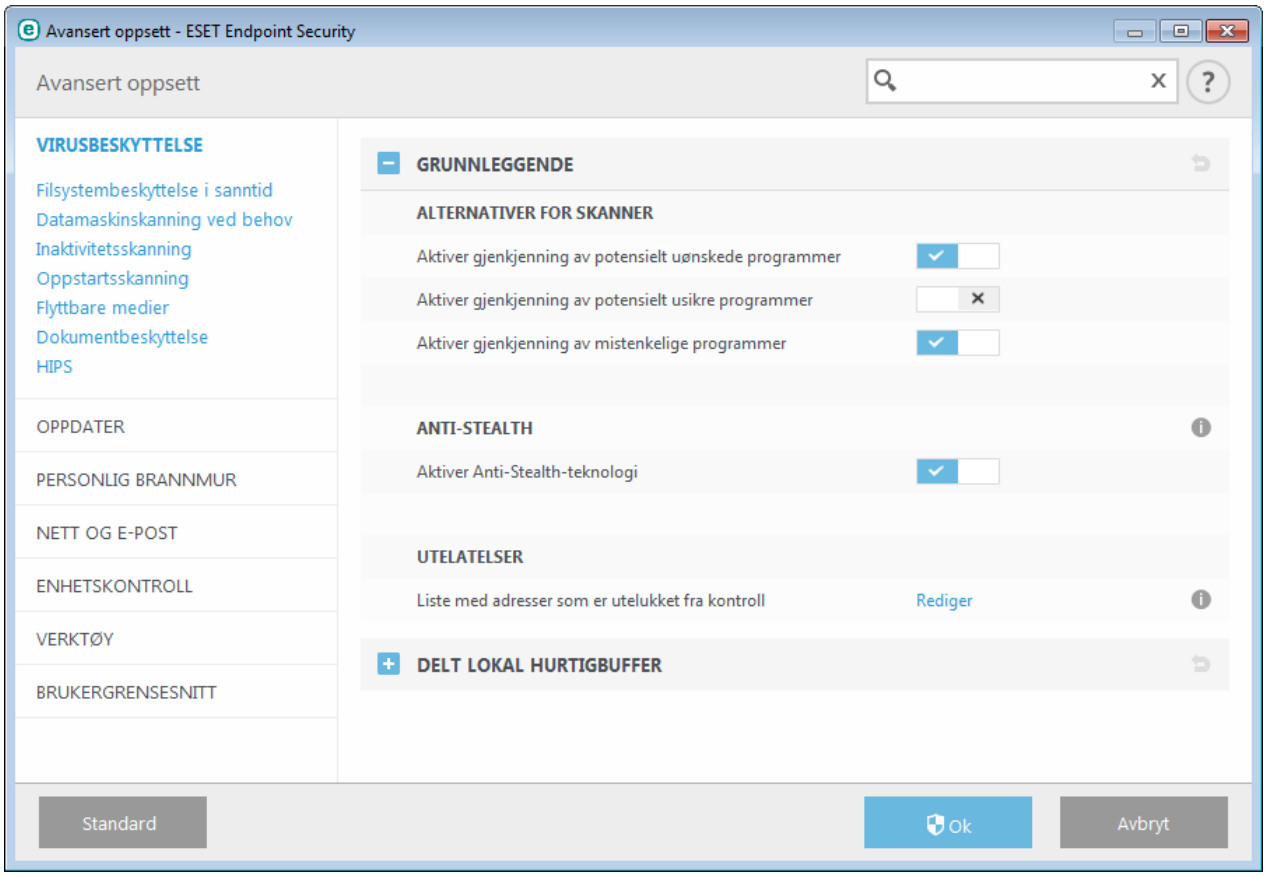


Potensielt uønskede programmer kan installere adware, verktøyslinjer eller inneholde andre uønskede og

usikre programfunksjoner.

Disse innstillingene kan endres i programinnstillinger til enhver tid. For å aktivere eller deaktivere gjenkjennelse av potensielt uønskede, usikre eller mistenkelige programmer, følg disse instruksene:

1. Åpne ditt ESET-produkt. Hvordan åpner jeg ESET-produktet?
2. Trykk på **F5** for å gå inn på **Avansert oppsett**.
3. Klikk **Virusbeskyttelse** og aktiver eller deaktiver alternativene **Aktiver gjenkjenning av potensielt uønskede programmer**, **Aktiver gjenkjenning av potensielt usikre programmer** og **Aktiver gjenkjenning av mistenkelige programmer** alt ettersom du vil. Bekreft ved å klikke **OK**.



Potensielt uønskede programmer – Programvarepakkere

En programvarepakker er en spesiell type programmodifikasjon som brukes av noen nettsteder som tilbyr filhosting. Dette er et tredjeparts verktøy som installerer programmet du ønsket å laste ned, men legger til ekstra programvare, slik som verktøyslinjer eller reklameprogrammer. Den ekstra programvaren kan også gjøre endringer på nettleserens hjemmeside og søkeinnstillinger. Nettsteder for filhosting varsler ofte ikke programvareleverandøren eller nedlastingsmottakeren at endringer har blitt utført, og tillater ikke enkle måter å velge bort modifikasjoner på. Av slike grunner, klassifiserer ESET programvarepakkere som en type potensielt uønsket program som lar brukere godta nedlastingen eller ikke.

Du finner en oppdatert versjon av denne hjelpesiden i denne ESET-kunnskapsbaseartikkelen.

3.11.1.10 Botnet

En bot, eller en nettrobot er en automatisk skadelig programvare som skanner blokker med nettverksadresser og infiserer sårbare datamaskiner. Dette lar hackerne ta kontroll på mange datamaskiner samtidig og gjøre dem om til botter (også kjent som en zombie). Hackere bruker vanligvis botter for å infisere et større antall datamaskiner. Denne store gruppen infiserte datamaskiner kalles et botnet. Når du har et botnet på datamaskinen din, kan det brukes til å distribuere denial of service (tjenestenekt), angrep, proxy og kan også brukes til å utføre automatiske oppgaver over Internett, uten at du vet om det (f.eks. sende spam, virus eller stjele personlig og privat informasjon, slik som bankopplysninger eller kredittkortnummer).

3.11.2 Typer av eksterne angrep

Det er mange spesialteknikker som gjør at angriperne er i stand til å svekke eksterne systemer. Disse er inndelt i flere kategorier.

3.11.2.1 Ormeangrep

En dataorm er et program som inneholder skadelig kode som angriper vertsmaskinen, og som sprer seg via et nettverk. Nettverksormer utnytter sikkerhetssvakheter i ulike programmer. På grunn av tilgjengeligheten til Internett kan de spre seg over hele verden i løpet av noen timer etter at de er utgitt.

De fleste ormeangrep kan forhindres ved å bruke standard sikkerhetsinnstillinger i brannmuren. Det er også viktig å velge beskyttelsestypen **Offentlig nettverk** i offentlige nettverker og sørge for at operativsystemet og programmene dine er oppdatert med de siste sikkerhetsoppdateringene.

3.11.2.2 DoS-angrep

DoS eller *Denial of Service* (tjenestenekt), er et forsøk på å gjøre en datamaskin eller et nettverk utilgjengelig for de tiltenkte brukerne. Kommunikasjonen mellom rammede brukere er hindret og kan ikke lenger fungere på en funksjonell måte. Datamaskiner som utsettes for DoS-angrep, må vanligvis startes på nytt for at de skal fungere som de skal.

I de fleste tilfeller er målene nettservere, og hensikten er å gjøre dem utilgjengelige for brukerne i en bestemt tidsperiode.

3.11.2.3 Portskanning

Portskanning brukes til å bestemme hvilke datamaskinporter som er åpne på en nettverksvertsmaskin. En portskanner er programvare som er utformet for å finne slike porter.

En dataport er et virtuelt punkt som håndterer innkommende og utgående data - dette er viktig fra et sikkerhetsmessig synspunkt. I et stort nettverk kan informasjon samlet inn av portskannere hjelpe med å identifisere potensielle svakheter. Slik bruk er lovlig.

Portskanning blir ofte brukt av hackere som prøver å svekke sikkerheten. Det første trinnet er å sende pakker til hver port. Avhengig av responstypen er det mulig å fastslå hvilke porter som er i bruk. Selve skanningen forårsaker ikke skade, men vær klar over at denne aktiviteten kan avsløre potensielle svakheter og la angripere ta kontroll over eksterne datamaskiner.

Nettverksadministratorer anbefales å blokkere alle ubrukte porter og beskytte de som er i bruk mot uautorisert tilgang.

3.11.2.4 DNS-forgiftning

Ved bruk av DNS-forgiftning (DNS - Domain Name Server), kan hackere lure DNS-serveren til en datamaskin til å tro at de falske dataene de oppgir, er legitime og ekte. Den falske informasjonen hurtigbufres i en bestemt periode, slik at angriperne kan skrive om DNS-svarene til IP-adresser. Som et resultat kan brukere som prøver å få tilgang til nettsider, laste ned datavirus eller -ormer i stedet for det opprinnelige innholdet.

3.11.3 E-post

E-post, eller elektronisk post, er en moderne kommunikasjonsform med mange fordeler. E-post er fleksibel, rask og direkte og spilte en viktig rolle for utbredelsen av Internett tidlig på 1990-tallet.

På grunn av det høye anonymitetsnivået gir dessverre e-post og Internett også rom for ulovlige aktiviteter, for eksempel spamming. Spam omfatter uønsket markedsføring, hoax-meldinger og spredning av skadelig programvare – malware. Problemene og faren for deg økes ved at kostnadene ved å sende spam er minimale, og forfatterne av spam har mange verktøy for å skaffe seg nye e-postadresser. I tillegg gjør også spamvolumet og alle variasjonene det vanskelig å regulere. Jo lenger du bruker en e-postadresse, desto høyere sannsynlighet er det for den havner i en spammotordatabase. Her er noen råd som kan hjelpe deg med å forebygge at du får spam i innboksen:

- Om mulig bør du ikke publisere e-postadressen din på Internett
- Bare gi e-postadressen din til personer du stoler på
- La om mulig være å bruke vanlige aliaser – med mer kompliserte aliaser er sannsynligheten for sporing mindre
- Ikke svar på spam som allerede har havnet i innboksen
- Vær forsiktig når du fyller ut skjemaer på Internett. Vær spesielt oppmerksom på alternativer som "Ja, jeg ønsker å motta informasjon".
- Bruk «spesialiserte» e-postadresser – for eksempel én for arbeid, én for kommunikasjon med venner, osv.
- Bytt e-postadresse fra tid til annen
- Bruk en antispamløsning

3.11.3.1 Markedsføring

Internett-markedsføring er en av de raskest voksende typer markedsføring. De viktigste fordelene er lave kostnader og at metoden er svært direkte. Dessuten leveres meldingene nesten umiddelbart. Mange selskaper bruker e-postmarkedsføringsverktøy for å kommunisere effektivt med nåværende og potensielle kunder.

Denne typen markedsføring er legitim, ettersom brukeren kan være interessert i å motta kommersiell informasjon om noen produkter. Men mange selskaper sender uønskede kommersielle meldinger. I slike tilfeller er ikke e-postmeldingene markedsføring, men spam.

Mengden uønsket e-post har blitt et problem, og ingenting typer på at mengden kommer til å reduseres. Forfattere av uønsket e-post prøver ofte å skjule spam som legitime meldinger.

3.11.3.2 Hoax-meldinger

Hoax-meldinger er feilinformasjon som spres via Internett. Hoax-meldinger sendes vanligvis via e-post eller kommunikasjonsverktøy som ICQ og Skype. Meldingen i seg selv er ofte en vits eller en urban legende.

Hoax-meldinger om datavirus prøver å skape frykt, uvisshet og tvil hos mottakerne, og få dem til å tro at det er et "uoppdagelig virus" som sletter filer og henter frem passord eller utfører annen skadelig aktivitet på maskinen.

Noen hoax-meldinger ber mottakerne om å videresende meldinger til kontaktene sine, slik at hoax-meldingen videreføres. Det finnes hoax-meldinger for mobiltelefoner, meldinger som er bønn om hjelp, tilbud om å få tilsendt penger fra utlandet osv. Det er ofte umulig å fastslå den opprinnelige senderens egentlige hensikt.

Hvis du ser en melding som ber deg om å videresende meldingen til alle du kjenner, kan det godt hende det er en hoax-melding. Det finnes mange nettsteder på Internett som kan bekrefte om en e-postmelding er legitim eller ikke. Før du videresender en e-postmelding du tror at kan være en hoax-melding, bør du utføre et søk på Internett.

3.11.3.3 Phishing

Begrepet phishing definerer en kriminell handling som bruker forskjellige typer sosial manipulering for å få andre til å oppgi ellers hemmelig informasjon. Formålet er å få tilgang til konfidensiell informasjon, for eksempel kontonummer, PIN-koder osv.

Tilgang oppnås vanligvis ved å sende e-postmeldinger som utgir seg for å være fra en pålitelig person eller virksomhet (finansinstitusjon, forsikringsselskap). E-postmeldingen kan se veldig ekte ut, og vil inneholde grafikk og innhold som opprinnelig kommer fra kilden de kopierer. Du blir av forskjellige årsaker (databekreftelse, finansielle operasjoner) bedt om å oppgi personlig informasjon, for eksempel kontonummer, brukernavn og passord. Det er enkelt å stjele og misbruke all slik informasjon, hvis du oppgir den.

Banker, forsikringsselskaper og andre legitime selskaper vil aldri be om brukernavn og passord i en uventet e-postmelding.

3.11.3.4 Gjenkjenne spamsvindel

Det finnes en del generelle kriterier som kan hjelpe deg med å identifisere spam (uønsket e-post) i innboksen. Hvis en melding oppfyller noen av følgende kriterier, er den sannsynligvis en spammelding.

- Avsenderens adresse finnes ikke i kontaktlisten din.
- Du blir tilbudt en stor sum penger, men du må først overføre et mindre beløp.
- Du blir av forskjellige årsaker (databekreftelse, finansielle operasjoner) bedt om å oppgi personlig informasjon, for eksempel kontonummer, brukernavn og passord osv.
- Meldingen er skrevet på et annet språk.
- Du blir bedt om å kjøpe et produkt du ikke er interessert i. Hvis du bestemmer deg for å kjøpe likevel, må du bekrefte at meldingens avsender er en pålitelig leverandør (kontakt den opprinnelige produsenten).
- Noen ord er skrevet feil i et forsøk på å lure spamfilteret. For eksempel «vaigra» i stedet for «viagra» osv.

3.11.3.4.1 Regler

I sammenheng med antispamløsninger og e-postklienter er regler verktøy som styrer e-postfunksjoner. De består av to logiske deler:

1. Betingelse (for eksempel en innkommende melding fra en bestemt adresse)
2. Handling (for eksempel sletting av meldingen, flytte den til en angitt mappe).

Antallet og kombinasjonen av regler varierer med hvilken antispamløsning man bruker. Disse reglene er tiltak mot spam (uønsket e-post). Vanlige eksempler:

- 1. Betingelse: En innkommende e-postmelding inneholder noen av ordene som ofte sees i spammeldinger
  2. Handling: Slette meldingen
- 1. Betingelse: En innkommende e-post inneholder et vedlegg med filendelsen .exe
  2. Handling: Slette vedlegget og levere meldingen i innboksen
- 1. Betingelse: En innkommende melding ankommer fra arbeidsgiveren din
  2. Handling: Flytte meldingen til mappen "Arbeid"

Vi anbefaler at du bruker en kombinasjon av regler i antispamprogrammer for å legge til rette for administrering, og filtrere spam mer effektivt.

3.11.3.4.2 Hviteliste

Generelt sett er en hviteliste en liste over elementer eller personer som er godtatt, eller har fått innvilget tilgangsrettigheter. Begrepet "e-posthviteliste" definerer en liste med kontakter som brukeren vil motta e-postmeldinger fra. Slike hvitelister er basert på nøkkelord som det søkes etter i e-postadresser, domenenavn eller IP-adresser.

Hvis en hviteliste er i "utelukkende modus", vil det ikke bli mottatt meldinger fra andre adresser, domener eller IP-adresser. Hvis en hviteliste ikke er eksklusiv, vil slike meldinger ikke bli slettet, men filtrert på en annen måte.

En hviteliste tar utgangspunkt i det motsatte prinsippet fra en svarteliste. Hvitelister er relativt enkle å administrere i forhold til svartelister. Vi anbefaler at du bruker både hviteliste og svarteliste for å filtrere spam mer effektivt.

3.11.3.4.3 Svarteliste

Svartelisten er en liste over ikke godkjente eller forbudte elementer eller personer. I den virtuelle verden er det en teknikk som tillater mottak av meldinger fra alle brukere som ikke er på en slik liste.

Det finnes to typer svartelister: Svartelister som er opprettet av brukere i antispamprogrammet, og profesjonelle, regelmessig oppdaterte svartelister som opprettes av spesialiserte institusjoner og er tilgjengelige på Internett.

Det er viktig å bruke svartelister til å blokkere spam, men de er vanskelige å vedlikeholde, siden nye elementer som må blokkeres, dukker opp hver dag. Vi anbefaler at du bruker både en hviteliste og en svarteliste for å kunne filtrere spam så effektivt som mulig.

3.11.3.4.4 Unntaksliste

Unntakslisten inneholder vanligvis adresser som kan være misbrukte eller som brukes til å sende spam. E-postmeldinger som mottas fra adresser oppført på unntakslisten, skannes alltid for spam. Som standard inneholder unntakslisten alle e-postadresser fra eksisterende e-postklientkontoer.

3.11.3.4.5 Kontroll på serversiden

Kontroll på serversiden er en teknikk for å identifisere masseutsendte spammeldinger basert på antall mottatte meldinger og reaksjonene til brukerne. Hver melding etterlater et unikt, digitalt "avtrykk" basert på innholdet i meldingen. Det unike ID-nummeret forteller ingen ting om innholdet i e-postmeldingen. To identiske meldinger vil ha identiske avtrykk, mens forskjellige meldinger vil ha forskjellige avtrykk.

Hvis en melding blir merket som spam, blir avtrykket sendt til serveren. Hvis serveren mottar flere identiske avtrykk (som tilhører en bestemt spammelding), blir avtrykket lagret i spamavtrykksdatabasen. Ved skanning av innkommende meldinger sender programmet meldingenes avtrykk til serveren. Serveren returnerer informasjon om hvilke avtrykk som tilsvarer meldinger som allerede er merket som spam av brukerne.

3.11.4 ESET-teknologi

3.11.4.1 Blokkering av utnyttelse

Blokkering av utnyttelse er utviklet for å befeste programmer som utnyttes ofte, som for eksempel nettlesere, PDF-lesere, e-postklienter eller MS Office-komponenter. Den overvåker oppførselen til prosesser og se etter mistenkelig aktivitet som kan indikere en utnyttelse. Den gir et ekstra lag med beskyttelse – ett skritt nærmere angriperne – ved hjelp av teknologi som er betydelig annerledes enn teknikker som fokuserer på å oppdage selve de skadelige filene.

Når Blokkering av utnyttelse identifiserer en mistenkelig prosess, kan den stoppe prosessen umiddelbart og registrere data om trusselen, som deretter sendes til ESET Live Grid skysystemet. Denne informasjonen behandles av ESETs trussellaboratorium og brukes til å gi alle brukere bedre beskyttelse mot ukjente trusler og nulldagstrusler (nylig utgitte skadelig programvare som det ikke finnes en forhåndskonfigurert løsning for).

3.11.4.2 Avansert minneskanner

Avansert minneskanner jobber sammen med blokkeringen av utnyttelse til å gi bedre beskyttelse mot skadelig programvare som er utviklet for å unngå å bli oppdaget av produkter mot skadelig programvare ved bruk av villedning og/eller kryptering. I tilfeller der vanlig emulering eller heuristikk ikke kan oppdage en trussel, er den avanserte minneskanneren i stand til å identifisere mistenkelig oppførsel og skanne trusler når de oppdages i systemminnet. Denne løsningen er effektiv selv mot høyst villedende skadelig programvare. I motsetning til blokkeringen av beskyttelse, er dette en metode som brukes etter utførelse av skadelig programvare. Det er med andre ord en risiko for at noe skadelig programvare kan ha blitt utført før trusselen ble oppdaget. I tilfeller der andre oppdagelsesteknikker mislykkes, gir den imidlertid et ekstra lag av sikkerhet.

3.11.4.3 ESET Live Grid

Bygget på ThreatSense.Net® sitt avanserte varslingssystem – ESET Live Grid bruker data som ESET-brukere har sendt inn fra over hele verden og sender den til ESET viruslaboratorium. Ved å gi mistenkelige prøver og metadata fra naturen, lar ESET Live Grid oss reagere umiddelbart på behovene til kundene våre og gjør at ESET kan reagere på de siste truslene. ESETs forskere på skadelig programvare bruker informasjonen til å skape et nøyaktig bilde av arten og omfanget av globale trusler. Dette gjør det enklere for oss å fokusere på de riktige målene. ESET Live Grid-data spiller en viktig rolle i utformingen av prioriteringer i vår automatiserte behandling.

I tillegg implementerer den et omdømmesystem som bidrar til å forbedre den totale effektiviteten av våre løsninger for skadelig programvare. Når en kjørbar fil eller et arkiv inspiseres på systemet til en bruker, sammenlignes filens/arkivets #-merke mot en database av hvite- og svartelistede elementer. Hvis filen blir funnet i hvitelisten, anses den å være ren og flagges slik at den ekskludere fra fremtidige skanninger. Hvis den er på svartelisten, iverksettes egnede tiltak basert på innholdet i trusselen. Hvis ingen match blir funnet, skannes filen grundig. Filer kategoriseres som trusler eller ikke-trusler basert på denne skanningen. Denne tilnærmingen har en betydelig positiv innvirkning på skanneytelsen.

Dette omdømmesystem muliggjør effektiv oppdagelse av eksempler på skadelig programvare selv før signaturene deres leveres til brukerne ved oppdatere virussignaturdatabasen flere ganger om dagen.

3.11.4.4 Botnet-beskyttelse

Botnet-beskyttelse oppdager skadelig programvare gjennom analyse av nettverkskommunikasjonsprotokollen. Skadelig programvare fra botnet endres ofte i motsetning til nettverksprotokoller, som ikke har blitt endret de siste årene. Denne nye teknologien hjelper ESET med å bekjempe skadelig programvare som prøver å koble datamaskinen din til et botnet-nettverk.

3.11.4.5 Java blokkering av utnyttelse

Java blokkering av utnyttelse er en utvidelse av den eksisterende ESET beskyttelse blokkering av utnyttelse. Den overvåker Java og ser etter oppførsel som tyder på utnyttelse. Blokkerte prøver kan rapporteres til en analytiker for skadelig programvare, slik at de kan opprette signaturer for å blokkere forsøkte Java-utnyttelser på andre lag (URL-blokkering, filnedlasting, osv.).