ESET NOD32 ANTIVIRUS 9

Brukerhåndbok

(beregnet for produktversjon 9.0 og høyere)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / XP

Klikk her for å laste ned den nyeste versjonen av dette dokumentet

ESET NOD32 ANTIVIRUS

Internasjonal kundestøtte: www.eset.com/support

REV. 10/6/2015

Innhold

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus representerer en ny tilnærming til virkelig integrert datamaskinsikkerhet. Den nyeste versjonen av ThreatSense®-skannemotoren gjør bruk av fart og presisjon for å holde datamaskinen trygg. Resultatet er et intelligent system som konstant er på vakt overfor angrep og skadelig programvare som kan true datamaskinen.

ESET NOD32 Antivirus er en komplett sikkerhetsløsning som kombinerer maksimal beskyttelse og et minimalt systemavtrykk. Vår avanserte teknologi tar i bruk kunstig intelligens for å forhindre infiltrering av virus, spyware, trojanske hester, ormer, adware, rootkits og andre trusler – uten å redusere systemytelsen eller føre til forstyrrelser på datamaskinen.

Funksjoner og fordeler

Nytt designet brukergrensesnitt	Brukergrensesnittet i versjon 9 har blitt betydelig redesignet og forenklet basert på resultatene fra brukertesting. All(e) grensesnittekst og varslinger har blitt nøye gjennomgått og grensesnittet støtter nå høyre-til-venstre-språk som hebraisk og arabisk. **Elektronisk hjelp** er nå integrert i ESET NOD32 Antivirusog tilbyr dynamisk støtteinnhold.
Virus- og spywarebeskyttelse	Oppdager og renser proaktivt de mest kjente og ukjente virusene, ormene, trojanerne og rootkit-ene. **Avansert heuristikk** oppdagelsesteknologi flagger til og med skadevare som aldri før har blitt sett og beskytter deg dermed fra ukjente trusler, som blir nøytralisert før de kan gjøre skade. **Beskyttelse for nettilgang** og **Anti-Phishing** skjer ved overvåkning av kommunikasjonen mellom nettlesere og eksterne servere (inkludert SSL). **E-postklientbeskyttelse** gir kontroll over e-postkommunikasjon mottatt gjennom protokollene POP3(S) og IMAP(S).
Vanlige oppdateringer	Regelmessig oppdatering av virussignaturdatabasen og programmodulene er den beste måten å sørge for maksimalt sikkerhetsnivå på datamaskinen din.
ESET LiveGrid® (Skybasert omdømme)	Du kan kontrollere omdømmet til prosesser og filer som kjører, direkte fra ESET NOD32 Antivirus.
Enhetskontroll	Skanner automatisk alle USB-minnepinner, minnekort og CD-er/DVD-er. Blokkerer flyttbare medier basert på type medium, fabrikant, størrelse og andre attributter.
HIPS-funksjonalitet	Du kan i stor grad tilpasse oppførselen til systemet – angi regler for systemregisteret, aktive prosesser og programmer og finjustere sikkerhetsinnstillingene dine.
Spillmodus	Utsetter alle pop-up-vinduer, oppdateringer eller andre systemintensive aktiviteter for å fokusere systemressurser på spilling og andre fullskjermsaktiviteter.

En aktiv lisens er nødvendig for at funksjonene til ESET NOD32 Antivirus kan brukes. Det anbefales at du fornyer lisensen din flere uker før lisensen for ESET NOD32 Antivirus utløper.

1.1 Hva er nytt i versjon 9

ESET NOD32 Antivirus versjon 9 inneholder følgende forbedringer:

- **Nytt designet brukergrensesnitt** – Det grafiske brukergrensesnittet til ESET NOD32 Antivirus har blitt fullstendig omformet for å gi bedre synlighet og en mer intuitiv brukeropplevelse. Grensesnittet støtter nå høyre-til-venstre-språk som hebraisk og arabisk. **Elektronisk hjelp** er nå integrert i ESET NOD32 Antivirusog tilbyr dynamisk støtteinnhold.
- **Raskere og mer pålitelig installasjon** – Omfatter en første skanning som starter automatisk innen 20 minutter etter installasjon eller omstart.

Flere detaljer om nye funksjoner i ESET NOD32 Antivirus finner du i følgende ESET kunnskapsbase-artikkel:
Hva er nytt i ESET Smart Security 9 og ESET NOD32 Antivirus 9?

1.2 Systemkrav

For å oppnå en sømløs drift av ESET NOD32 Antivirus, 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/Home Server 2003 SP2 32-bit/Home Server 2011 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 ThreatSense blir tusenvis av nye, unike infiltrasjoner opprettet hver dag for å forbigå eksisterende sikkerhetstiltak og gi skaperne fortjeneste - på brukernes kostnad. Spesialistene ved ESETs forskningslaboratorium 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. Installasjon

ESET NOD32 Antivirus kan installeres på datamaskinen din på flere måter. Installasjonsmetodene kan variere avhengig av land og distribusjonsmetode:

- Live-installasjonsprogrammet kan lastes ned fra ESETs nettside. Installasjonspakken er universal for alle språk (velg ønsket språk). Selve Live-installasjonsprogrammet er en liten fil; ytterligere filer som er nødvendige for å installere ESET NOD32 Antivirus, lastes ned automatisk.

- Frakoblet installasjon – Denne installasjonstypen brukes når du installerer produktet fra en CD/DVD. Den bruker en *.msi*-fil som er større enn filen til Live-installasjonsprogrammet, og krever ingen tilkobling til Internett eller ytterligere filer for å fullføre installasjonen.

Viktig: Forsikre deg om at ingen andre virusprogrammer er installert på datamaskinen før du installerer ESET NOD32 Antivirus. 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).

2.1 Live-installasjonsprogram

Når du har lastet ned installasjonspakken *Live-installasjonsprogram*, dobbeltklikker du installasjonsfilen og følger trinn-for-trinn-instruksjonene i vinduet til installasjonsprogrammet.

Viktig: For denne typen installasjon må du være tilkoblet Internett.

Velg ønsket språk fra rullegardinmenyen og klikk **Neste**. Det kan ta noe tid å laste ned installasjonsfilene.

Etter at du har godtatt **Lisensavtalen for sluttbrukere**, blir du bedt om å konfigurere **ESET LiveGrid®**. ESET LiveGrid® bidrar til å sikre at ESET er umiddelbart og kontinuerlig informert om nye trusler, slik at vi kan beskytte våre kunder. Systemet tillater innsending av nye trusler til ESETs forskningslaboratorium, hvor de blir analysert, behandlet og lagt til i virussignaturdatabasen.

Jeg vil ta del i ESET LiveGrid® (anbefalt) er som standard valgt, noe som aktiverer denne funksjonen.

Det neste trinnet i installasjonen er å konfigurere oppdagelse av potensielt uønskede programmer. Potensielt uønskede programmer er ikke nødvendigvis skadelige, men kan ha negativ innvirkning på atferden til operativsystemet. Du finner mer informasjon i kapittelet Potensielt uønskede programmer.

Klikk **Installer** for å starte installasjonsprosessen.

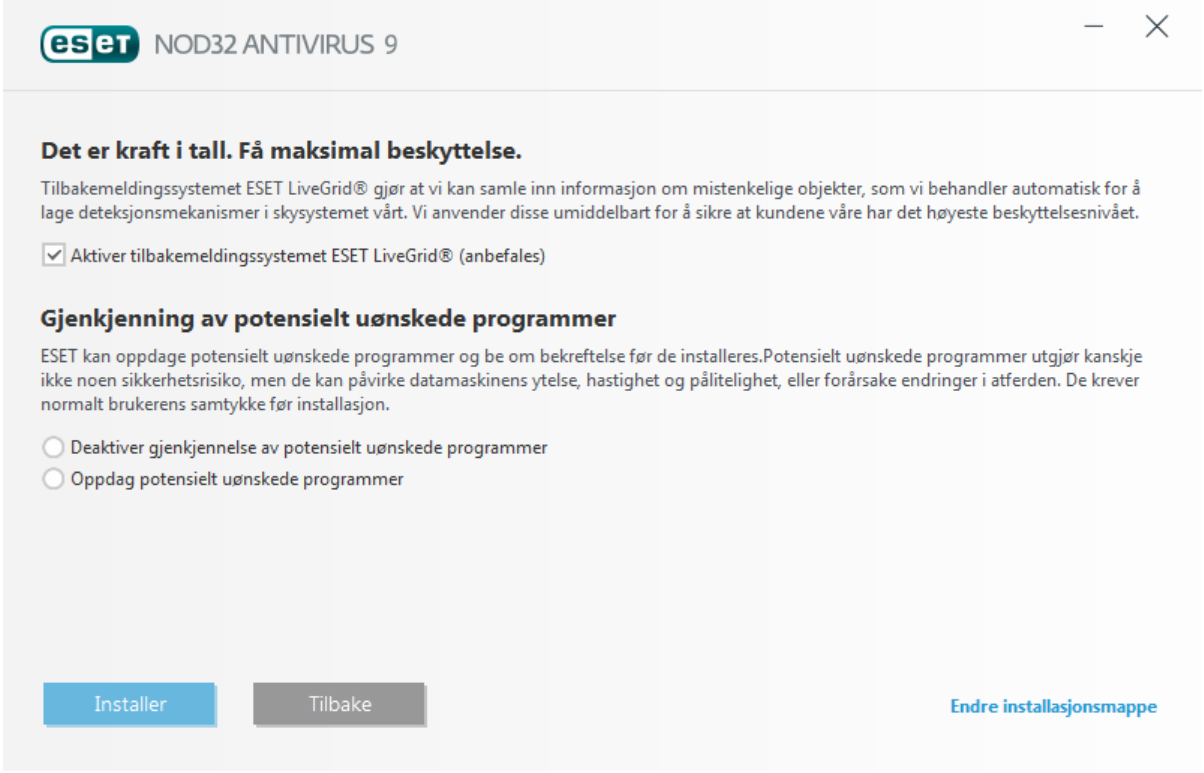
2.2 Frakoblet installasjon

Når du har startet pakken for frakoblet installasjon (.msi), vil installasjonsveiviseren ta deg gjennom installasjonsprosessen.

Først kontrollerer programmet om det finnes en nyere versjon av ESET NOD32 Antivirus tilgjengelig. Hvis det blir funnet en nyere versjon, får du en melding om det på første trinn i installasjonsprosessen. Hvis du valgte alternativet **Last ned og installer ny versjon**, blir den nye versjonen lastet ned, og installasjonen fortsetter. Denne avkrysningsboksen er barre synlig når det finnes en nyere versjon enn den du installerer.

Deretter vil lisensavtalen for sluttbrukere bli vist. Les avtalen og klikk **Godta** for å bekrefte at du godtar lisensavtalen for sluttbrukere. Installasjonen fortsetter når du har godtatt avtalen.

For mer informasjon om installasjonstrinn, **ThreatSense** og **Oppdagelse av potensielt uønskede programmer** følger du instruksjonene i den tidligere nevnte delen (se "Live installer").



2.2.1 Tilleggsinnstillinger

Du blir bedt om å velge plassering for installasjonen når du har valgt **Avanserte innstillinger**. Som standard blir programmet installert i følgende katalog:

C:\Program Files\ESET\ESET NOD32 Antivirus

Klikk **Bla gjennom...** hvis du vil endre denne plasseringen (anbefales ikke).

Klikk **Neste** for å konfigurere Internett-tilkoblingen. Hvis du bruker en proxy-server, må den være riktig konfigurert for at oppdateringene av virussignaturer skal fungere. 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**.

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**. I feltet **Port** kan du angi porten der proxy-serveren godtar tilkoblinger (standard er 3128). Hvis proxy-serveren krever godkjenning, må du oppgi gyldig **brukernavn** og **passord** for å få tilgang til proxy-serveren. Du kan også kopiere innstillingene til proxy-serveren fra Internet Explorer hvis du ønsker. Hvis du vil gjøre det, klikker du **Bruk** og bekrefter valget.

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**.

MERKNAD: Etter en programkomponentoppdatering kreves vanligvis omstart. Vi anbefaler å velge alternativet **Start om nødvendig datamaskinen på nytt uten å varsle**.

Neste installasjonsvindu viser alternativet 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 NOD32 Antivirus. Når begge passordfeltene samsvarer, klikker du **Neste** for å fortsette.

For å fullføre de neste installasjonstrinnene, **ThreatSense** og **Oppdagelse av potensielt uønskede programmer**, følger du instruksjonene i delen Live-installasjonsprogram (se "Live-installasjonsprogram").

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** i vinduet **Klar til å installere** for å fullføre installasjonen.

2.3 Vanlige installasjonsproblemer

Hvis problemet oppstår under installasjon, kan du se listen over vanlige installasjonsfeil og løsninger for å finne en løsning på problemet.

2.4 Produktaktivering

Etter at 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.):

- Hvis du har kjøpt produktet i en pakke i en butikk, aktiverer du produktet med en **lisensnøkkel**. Lisensnøkkelen finnes vanligvis inne i eller på baksiden av produktpakken. Lisensnøkkelen må skrives inn som anvist for at aktiveringen skal fungere. Lisensnøkkel – en unik tegnstreng i formatet XXXX-XXXX-XXXX-XXXX-XXXX eller XXXX-XXXXXXXX som brukes til å identifisere lisenseieren og aktivere lisensen.
- Hvis du vil evaluere ESET NOD32 Antivirus før du kjøper det, velger du **Gratis prøvelisens**. Oppgi e-postadresse og land for å aktivere ESET NOD32 Antivirus for et begrenset tidsrom. Du vil motta prøvelisensen på e-post. Prøvelisenser kan bare aktiveres én gang per kunde.
- Hvis du ikke har lisens, men ønsker å kjøpe en, klikker du Kjøp lisens. Dette vil ta deg til nettsiden til din lokale ESET-distributør.

Velg **Aktiver senere** hvis du først vil gjøre en rask vurdering av produktet og ikke vil aktivere det med en gang, eller hvis du vil aktivere produktet senere.

Du kan også aktivere ditt eksemplar av ESET NOD32 Antivirus direkte fra programmet. Høyreklikk ESET NOD32 Antivirus-ikonet i statusfeltet og velg **Aktiver produkt** fra programmenyen.

2.5 Angi lisensnøkkel

For å oppnå optimal funksjonalitet er det viktig at programmet oppdateres automatisk. Dette er bare mulig hvis du tastet inn riktig **lisensnøkkel** i **oppdateringsoppsettet**.

Hvis du ikke har angitt lisensnøkkelen under installasjonen, kan du gjøre det nå. Klikk **Hjelp og støtte** og deretter **Aktiver lisens** og angi lisensdataene som du mottok sammen med ESET sikkerhetsproduktet i vinduet Produktaktivering.

Når du angir **lisensnøkkelen**, er det viktig å skrive den inn nøyaktig som den er skrevet:

- En unik tegnstreng i formatet XXXX-XXXX-XXXX-XXXX-XXXX som brukes til å identifisere lisenseieren og aktivere lisensen.

Vi anbefaler at du kopierer og forbi lisensnøkkelen fra e-postmeldingen med registreringsinformasjon for å sikre nøyaktighet.

2.6 Oppgraderer til en nyere versjon

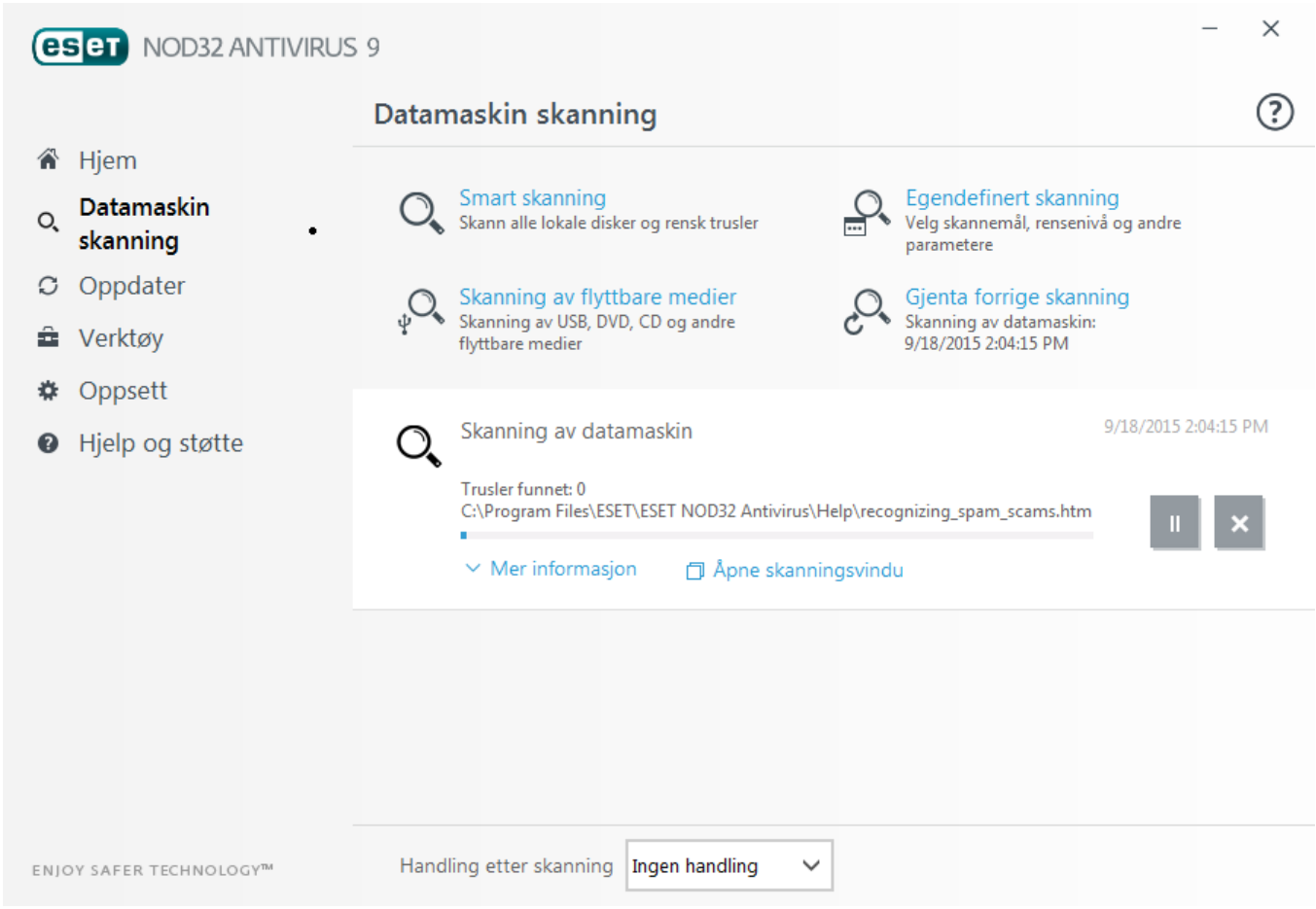
Nye versjoner av ESET NOD32 Antivirus utgis for å levere forbedringer eller reparere problemer som ikke kan ordnes ved automatisk oppdatering av programmodulene. Du kan oppgradere til en nyere versjon på flere måter:

1. Automatisk ved hjelp av en programoppdatering.
   Siden programoppdateringen distribueres til alle brukere og kan ha innvirkning på 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 i hovedprogramvinduet ved å klikke **Se etter oppdateringer** i delen **Oppdater**.
3. Manuelt ved å laste ned og installere en nyere versjon over den forrige.

2.7 Første skanning etter installasjonen

En datamaskinskanning vil begynne 20 minutter etter installasjonen av ESET NOD32 Antivirus, eller en omstart, for å søke etter skadelige koder.

Du kan også starte en datamaskinskanning manuelt fra hovedvinduet ved å klikke på **Datamaskinskanning** > **Skann datamaskinen din**. Se delen Computer scan hvis du ønsker mer informasjon om datamaskinskanning.



3. Veiledning for nybegynnere

Dette kapittelet gir en innledende oversikt over ESET NOD32 Antivirus og produktets grunninnstillinger.

3.1 Programmets hovedvindu

Hovedvinduet i ESET NOD32 Antivirus 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:

Hjem – Gir informasjon om beskyttelsesstatusen til ESET NOD32 Antivirus.

Datamaskinskanning – Konfigurer og start en datamaskinskanning eller opprett en egendefinert skanning.

Oppdatering – Viser informasjon om oppdateringer av virussignaturdatabasen.

Verktøy – gir tilgang til loggfiler, beskyttelsesstatistikk, overvåkingsaktivitet, kjørende prosesser, Planlegger, ESET SysInspector og ESET SysRescue.

Oppsett – Velg dette alternativet for å tilpasse sikkerhetsnivået for datamaskin, Internett.

Hjelp og støtte – gir tilgang til hjelpefiler, ESETs kunnskapsbase, ESETs nettsted og koblinger til å sende en støtteforespørsmål.

Hjem-skjermbildet inneholder informasjon om gjeldende beskyttelsesnivå for datamaskinen. Statusvinduet viser også funksjoner som blir ofte brukt i ESET NOD32 Antivirus. Her finner du også informasjon om den nyeste oppdateringen og programmets utløpsdato.

Det grønne ikonet og den grønne statusen **Maksimal beskyttelse** angir at høyeste sikkerhetsnivå er aktivert.

Hva må gjøres hvis programmet ikke fungerer som det skal?

Hvis en aktivert beskyttelsesmodul fungerer som den skal, vil beskyttelsesstatusikonet være grønt. Et rødt utropstegn eller oransje varselikon betyr at maskinen ikke er maksimalt beskyttet. Det vil vises ytterligere informasjon om beskyttelsesstatusen til hver modul, i tillegg til anbefalte løsninger for å gjenopprette fullstendig beskyttelse under **Hjem**. For å endre statusen til individuelle moduler kan du klikke **Oppsett** og velge ønsket modul.

Det røde ikonet og rød maksimumsbeskyttelse indikerer ikke nødvendigvis kritiske problemer. Denne statusen kan vises av en rekke årsaker. Blant dem er:

- **Produkt ikke aktivert** – Du kan aktivere ESET NOD32 Antivirus på **Hjem** ved å klikke på **Aktiver produkt** eller **Kjøp nå** under beskyttelsesstatus.
- **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 feil innskrevne godkjenningsdata eller feil konfigurerte tilkoblingsinnstillinger.
- **Virus- og spywarebeskyttelse deaktivert** – Du kan reaktivere virus- og spywarebeskyttelsen ved å klikke på **Start alle virus- og spywarebeskyttelsesmoduler**.
- **Lisensen er utløpt** – Dette angis av at ikonet for beskyttelsesstatus blir rødt. Programmet kan ikke oppdateres etter at lisensen er utløpt. Følg instruksjonene i varselvinduet og forny lisensen.

Det oransje ikonet viser begrenset beskyttelse. Det kan for eksempel oppstå et problem med å oppdatere programmet, eller det kan hende at lisensen går snart ut.
Denne statusen kan vises av en rekke årsaker. Blant dem er:

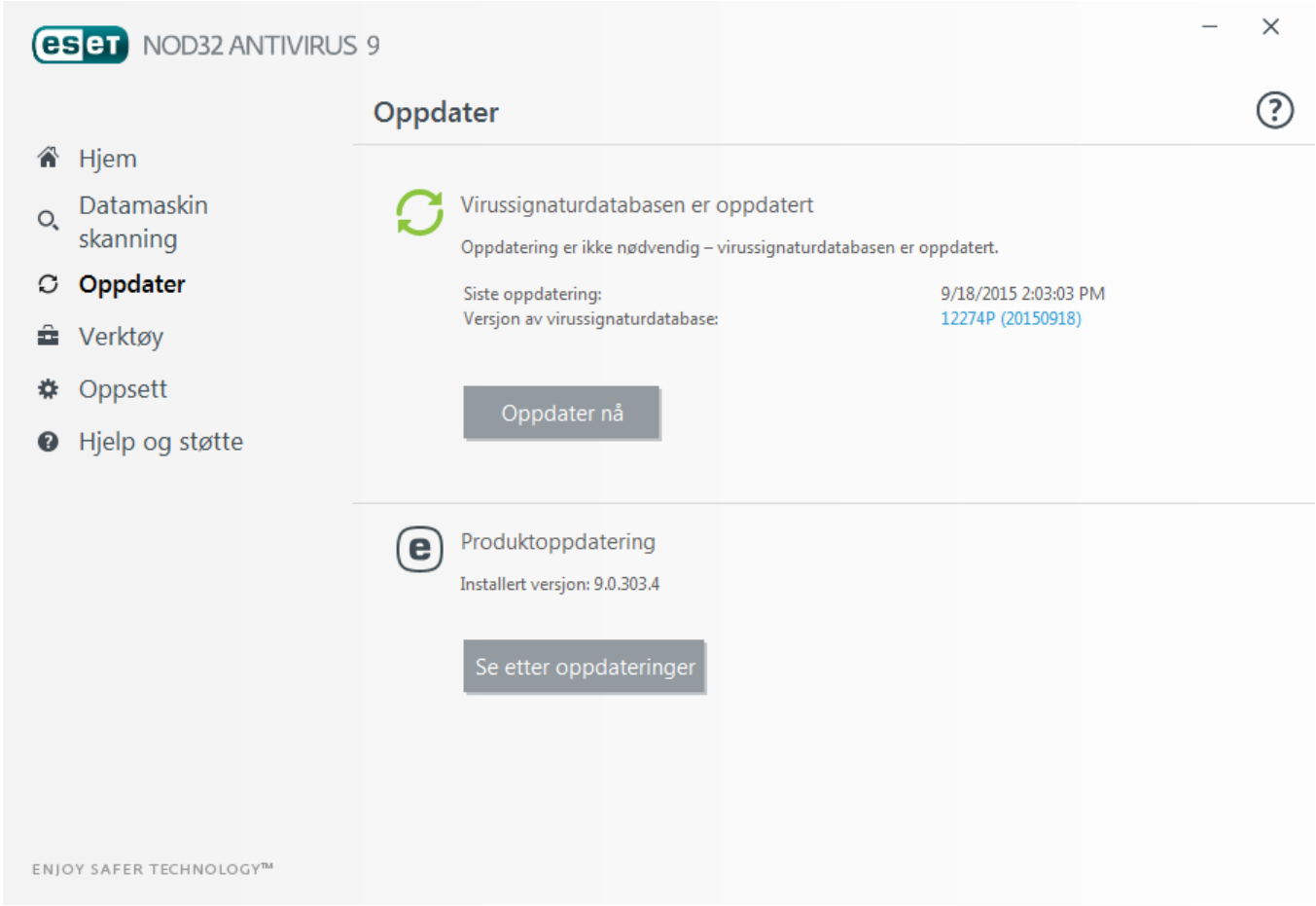
- **Spillmodus aktivert** – Det innebærer en mulig sikkerhetsrisiko å aktivere Spillmodus. Aktivering av denne funksjonen deaktiverer alle popup-vinduer og stopper alle planlagte oppgaver.
- **Lisensen utløper snart** - Dette angis ved at ikonet for beskyttelsesstatus viser et utropstegn ved siden av systemklokken. 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 hjelpefiler eller søke i ESET kunnskapsbase. Du kan sende en forespørsel om støtte hvis du fremdeles trenger hjelp. ESETs brukerstøtte vil raskt gi svar på spørsmålene og hjelpe til med å finne en løsning.

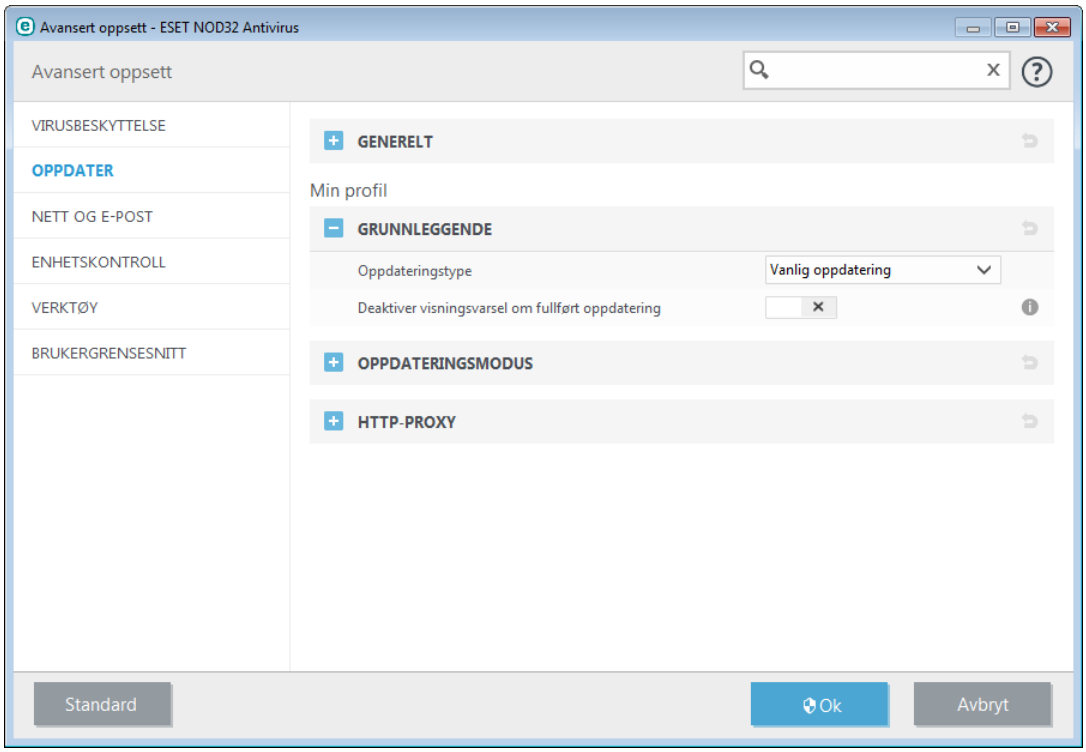
3.2 Oppdateringer

Oppdatering av virussignaturdatabasen og oppdatering av programkomponentene er en viktig del av å beskytte systemet ditt mot skadelig kode. Vær meget oppmerksom på konfigurasjonen og bruken av oppdateringene. Velg **Oppdater** fra hovedmenyen, og klikk deretter **Oppdater virussignaturdatabasen** for å se etter en nyere oppdatering av virussignaturdatabasen.

Hvis brukernavnet og passordet ikke ble oppgitt under aktiveringen av ESET NOD32 Antivirus, blir du bedt om å gjøre det nå.

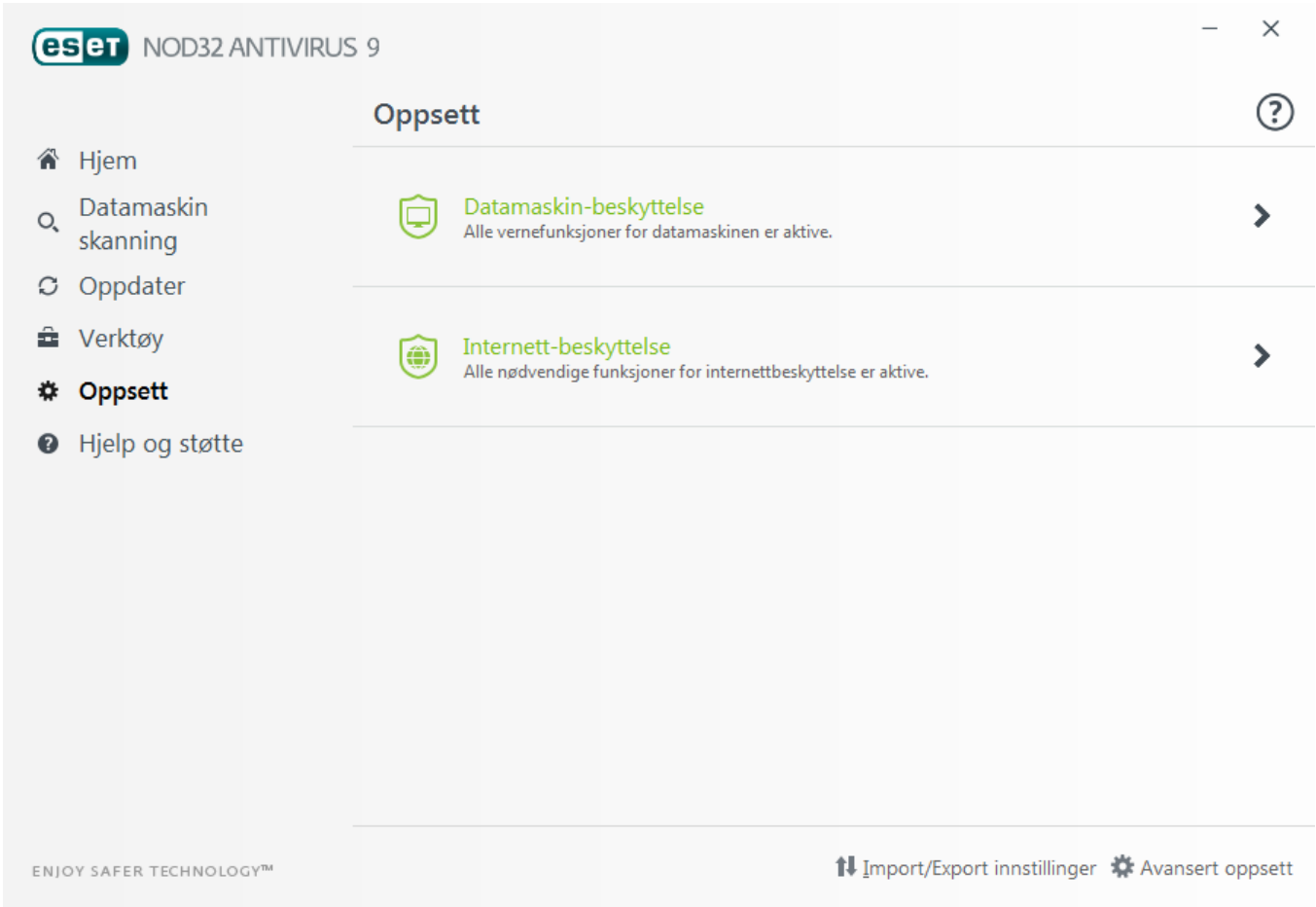


Vinduet for Avansert oppsett (klikk **Oppsett** i hovedmenyen og klikk deretter **Avansert oppsett** eller trykk **F5** på tastaturet) inneholder flere oppdateringsalternativer. Du kan konfigurere avanserte oppdateringsalternativer, for eksempel oppdateringsmodus, proxyservertilgang og LAN-tilkoblinger, ved å klikke på den aktuelle kategorien i vinduet **Oppdater**.



4. Arbeide med ESET NOD32 Antivirus

Med alternativene for oppsett i ESET NOD32 Antivirus kan du justere beskyttelsesnivåene til datamaskinen.



Oppsett-menyen er delt i følgende deler:

Datamaskinbeskyttelse

Internett-beskyttelse

Klikk en komponent for å justere de avanserte innstillingene til den tilsvarende beskyttelsesmodulen.

I oppsett av **Datamaskinbeskyttelse** 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.
- **HIPS** - HIPS-systemet overvåker hendelsene i operativsystemet og reagerer på dem i henhold til et tilpasset sett med regler.
- **Spillmodus** – Aktiverer eller deaktiverer Spillmodus. Du vil få en advarsel (potensiell sikkerhetsrisiko), og hovedvinduet vil bli oransje når Spillmodus er aktivert.

I oppsett av **Internett-beskyttelse** kan du aktivere eller deaktivere følgende komponenter:

- **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.
- **Anti-Phishing-beskyttelse** – Filtrerer nettsteder det mistenkes at distribuerer innhold som er beregnet på å manipulere brukere til å oppgi konfidensiell informasjon.

Når du vil aktivere en deaktivert sikkerhetskomponent på nytt, klikker du glidebryteren så den viser en grønn hake .

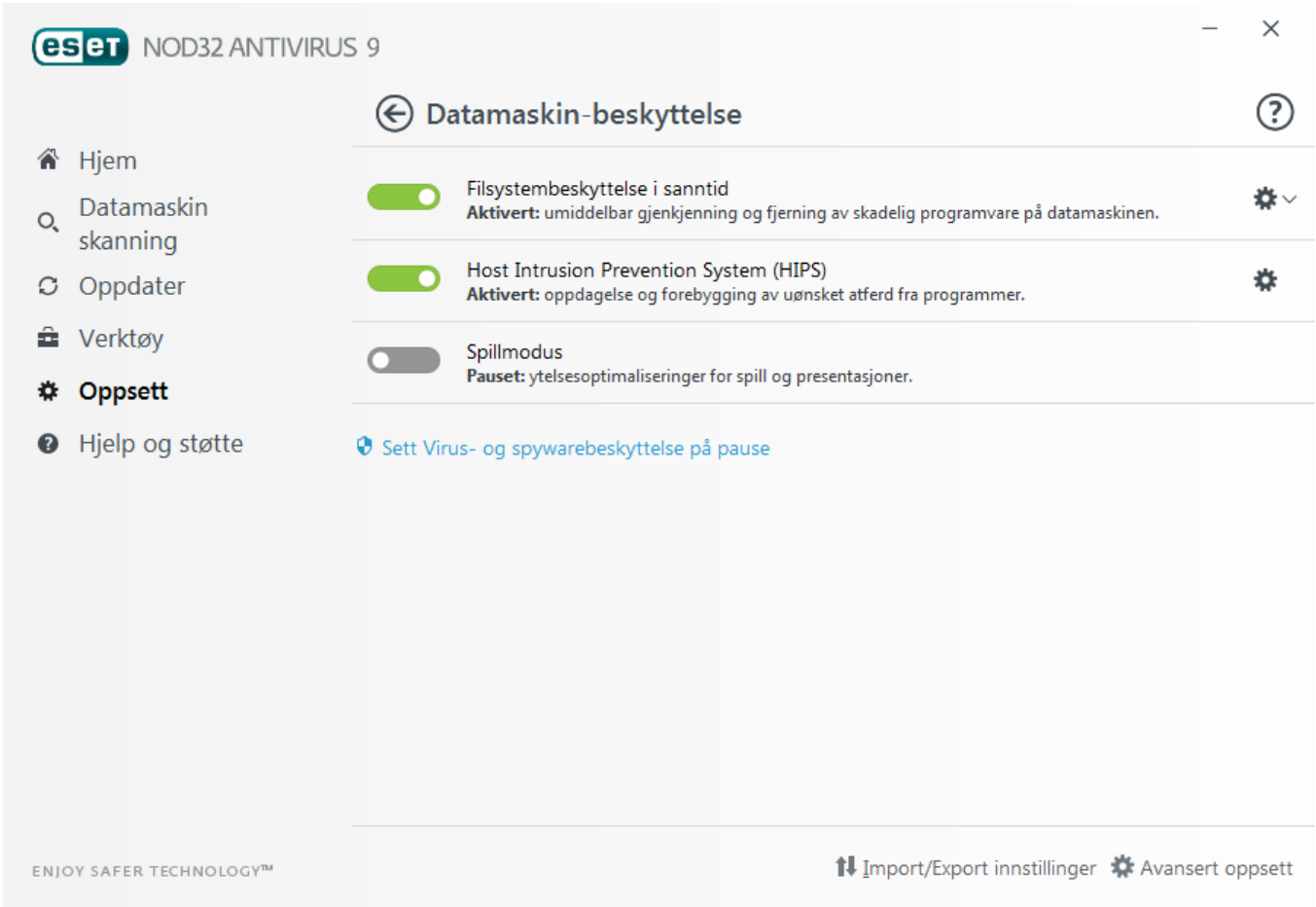
MERKNAD: Ved å deaktivere beskyttelsen på denne måten vil alle deaktiverte beskyttelsesmoduler bli aktivert etter omstart av datamaskinen.

Det er flere alternativer nederst i oppsettvinduet. Bruk koblingen **Avansert oppsett** for å sette opp mer detaljerte parametere for hver modul. Bruk **Importer/eksporter innstillinger** for å laste inn oppsettparametere ved bruk av en *.xml*-konfigureringsfil, eller for å lagre gjeldende oppsettparametere i en konfigureringsfil.

4.1 Datamaskinbeskyttelse

Klikk Datamaskinbeskyttelse fra Oppsett-vinduet for en oversikt over alle beskyttelssmodulene. Hvis du vil deaktivere enkeltmoduler midlertidig, klikker du . Legg merke til at dette kan redusere beskyttelsen av datamaskinen. Klikk ved siden av en beskyttelsesmodul for å få tilgang til avanserte innstillinger for den modulen.

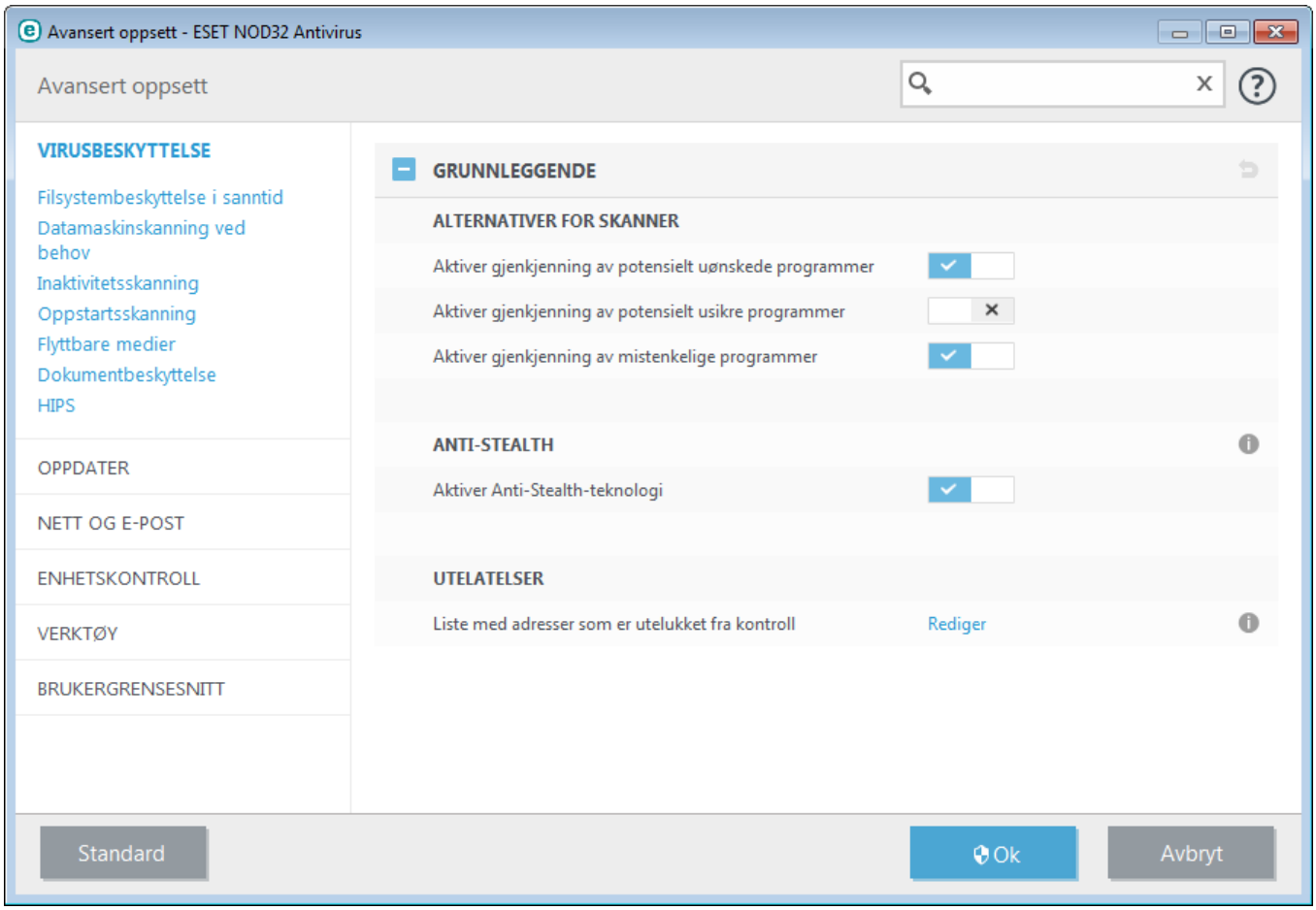
Klikk >Klikk **Rediger utelatelser** ved siden av **Filsystembeskyttelse i sanntid** for å åpne oppsettvinduet for Utelatelse hvor du kan velge å utelate filer og mapper fra skanning.



Deaktiverer Virus- og spywarebeskyttelse midlertidig – Deaktiverer alle virus- og spywarebeskyttelsesmoduler. Når du deaktiverer beskyttelse, vil det åpnes et vindu der du kan bestemme hvor lenge beskyttelsen skal være deaktivert ved bruk av rullgardinmenyen **Tidsintervall**. Klikk **OK** for å bekrefte.

4.1.1 Virusbeskyttelse

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



Alternativer for skanner for alle beskyttelsesmoduler (f.eks. Sanntidsbeskyttelse av filsystemet, Beskyttelse for nettilgang, ...) lar deg aktivere eller deaktivere gjenkjenning av følgende:

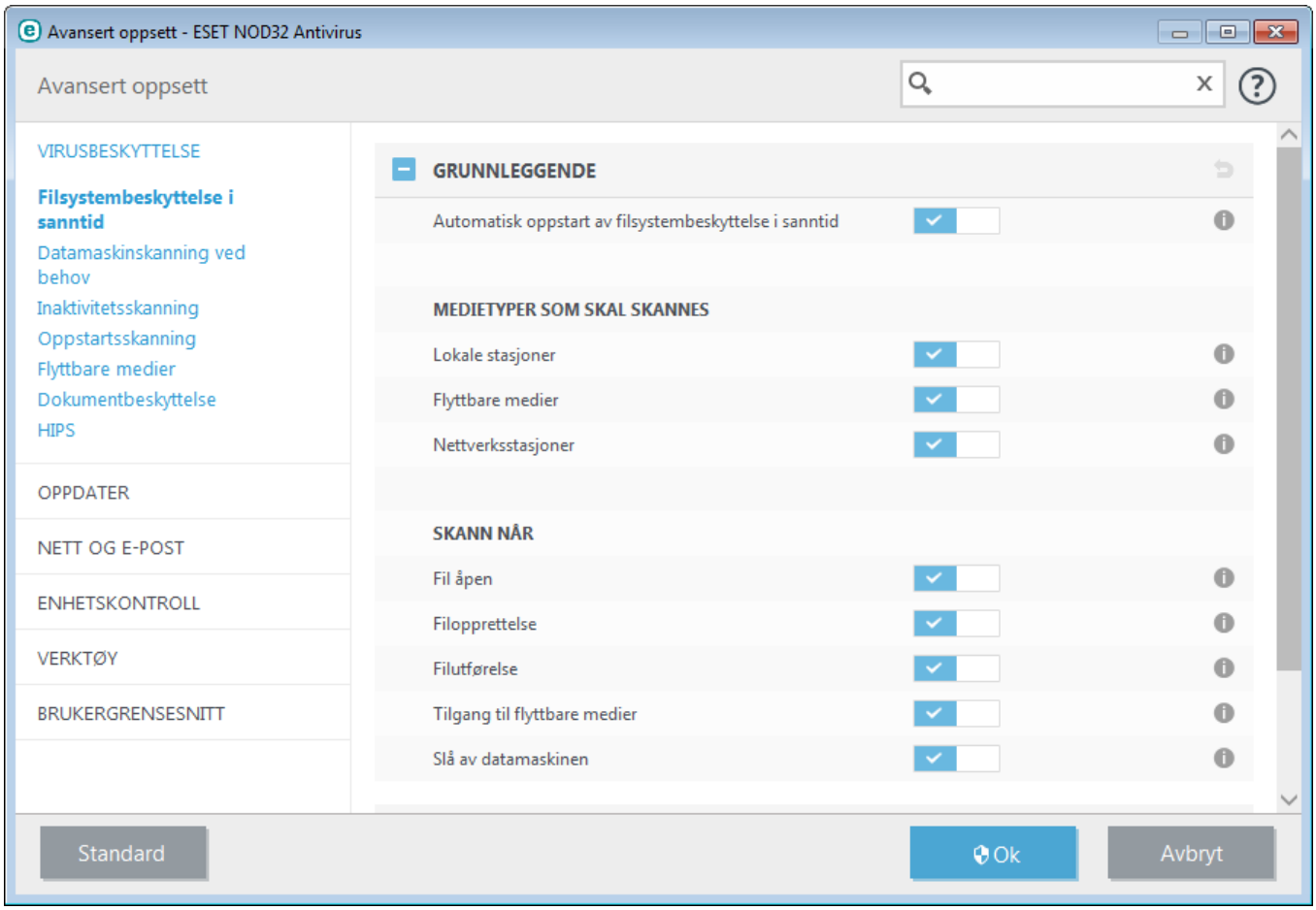
- **Potensielt uønskede programmer** (PUAer) er ikke nødvendigvis ment å være skadelige, men kan påvirke datamaskinens ytelse negativt.
  Du kan lese mer om denne typen programmer i ordlisten.
- **Potensielt usikre programmer** henviser til legitim, kommersiell programvare som har potensial til å bli 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.

Utelatelser gjør det 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 å utelukke et objekt fra skanning se Utelatelser.

4.1.1.1 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 – enhetskontroll av 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 når filer opprettes.
- **Filutførelse** – aktiverer eller deaktiverer skanning ved kjøring av filer.
- **Tilgang til flyttbare medier** – Aktiverer eller deaktiverer skanning som er utløst ved tilgang til spesielle flyttbare medier med lagringsplass.
- **Slå av datamaskinen** – 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**.

4.1.1.1.1 Ytterligere ThreatSense-parametere

Ytterligere ThreatSense-parametere for nylig opprettede og endrede filer

Sannsynligheten for infeksjon i nyopprettede eller endrede filer er høyere enn i eksisterende filer. Derfor kontrollerer programmet disse filene med ekstra skanneparametere. ESET NOD32 Antivirus bruker avansert heuristikk som kan oppdage nye trusler før en oppdatering av virussignaturdatabasen utgis sammen med signaturbaserte skannemetoder. I tillegg til nyopprettede filer skannes også **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**.

Ytterligere ThreatSense-parametere for utførte filer

Avansert heuristikk ved filutførelse – Ved standard, brukes Avansert heuristikk ved filutførelse. Når dette er aktivert, anbefaler vi å la Smartoptimalisering og ESET LiveGrid® være aktivert for å holde systempåkjenning til et minimum.

Avansert heuristikk ved utførelse av filer fra flyttbare medier – Avansert heuristikk emulerer kode i et virtuelt miljø og evaluerer dens oppførsel før koden tillates å kjøre fra flyttbare medier.

4.1.1.1.2 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.

Standardrensing - 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.

4.1.1.1.3 Når skal du endre konfigurasjonen av beskyttelsen i sanntid

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

Når ESET NOD32 Antivirus 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**).

4.1.1.1.4 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

4.1.1.1.5 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 **Datamaskinbeskyttelse** > **Sanntidsbeskyttelse av filsystemet**.

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

Hvis beskyttelsen i sanntid ikke oppdager og renser infiltrasjoner

Forsikre deg om at ingen andre virusprogrammer er installert på datamaskinen. Hvis to virusbeskyttelsesprogrammer er installert 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.

4.1.1.2 Datamaskinskanning

Skanning ved behov er en viktig del av antivirusløsningen. Den brukes til å utføre skanning av filer og mapper på datamaskinen. Fra et sikkerhetsstandpunkt er det viktig at datamaskinskanning ikke bare kjøres når det er mistanke om en infisering, men også 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 når de skrives til disken. Dette kan skje hvis Filsystembeskyttelse i sanntid er deaktivert på dette tidspunktet, virusdatabasen er foreldet eller filen ikke gjenkjennes som virus når den lagres på disken. 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**. **Skann datamaskinen din** skanner systemet raskt uten at du må angi spesifikke skanneparametere. **Egendefinert skanning** lar deg velge mellom forhåndsdefinerte skanneprofiler designet for å fokusere på bestemte plasseringer og lar deg også velge bestemte mål for skanningen.

Skann datamaskinen din

Skann datamaskinen din lar deg raskt starte datamaskinskanning og rense infiserte filer uten at du trenger å foreta

deg noe. Fordelen med Skann datamaskinen din er at den er lett å bruke og ikke krever detaljert skanningskonfigurasjon. Denne skanningen 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 lar deg spesifisere skanneparametere, 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.

Skanning av flyttbare medier

Lignende for å skanne datamaskinen – 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**.

Gjenta siste skanning

Lar deg starte forrige utført skanning raskt ved hjelp av innstillingene for forrige skanning.

Se Skannefremdrift for mer informasjon om skanneprosessen.

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

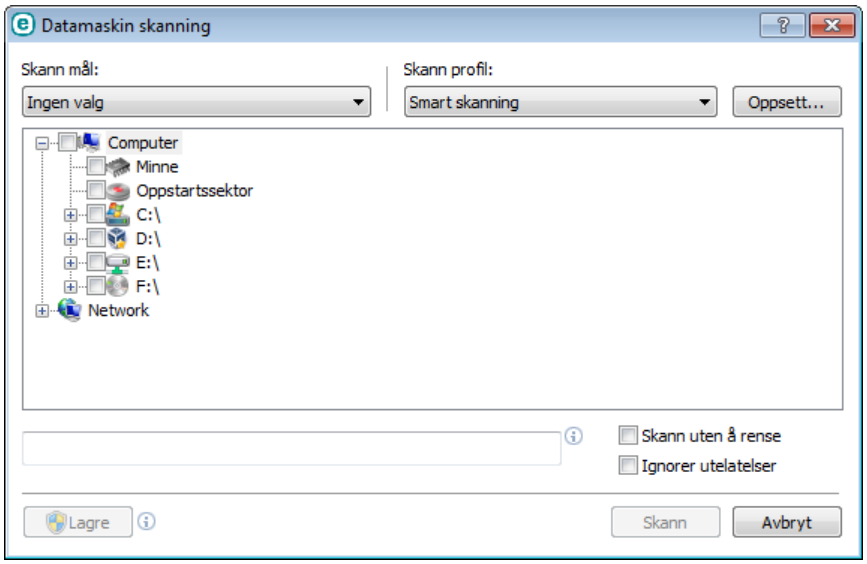
4.1.1.2.1 Oppstartsprogram for egendefinert skanning

Hvis du ikke ønsker å skanne hele disken, men bare et bestemt mål, kan du velge Tilpasset skanning ved å klikke **Datamaskinskanning** > **Tilpasset skanning** og velge et alternativ fra rullegardinmenyen **Skann mål** eller velge bestemte mål fra mappestrukturen (trestrukturen).

I vinduet Skann mål 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...** > **Rensing**. Informasjon om skanningen blir lagret i en skannelogg.

Når **Ignorer utelatelser** er valgt, vil filtypene som tidligere ble utelatt fra skanning skannes uten unntak.

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

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.

4.1.1.2.2 Skannefremdrift

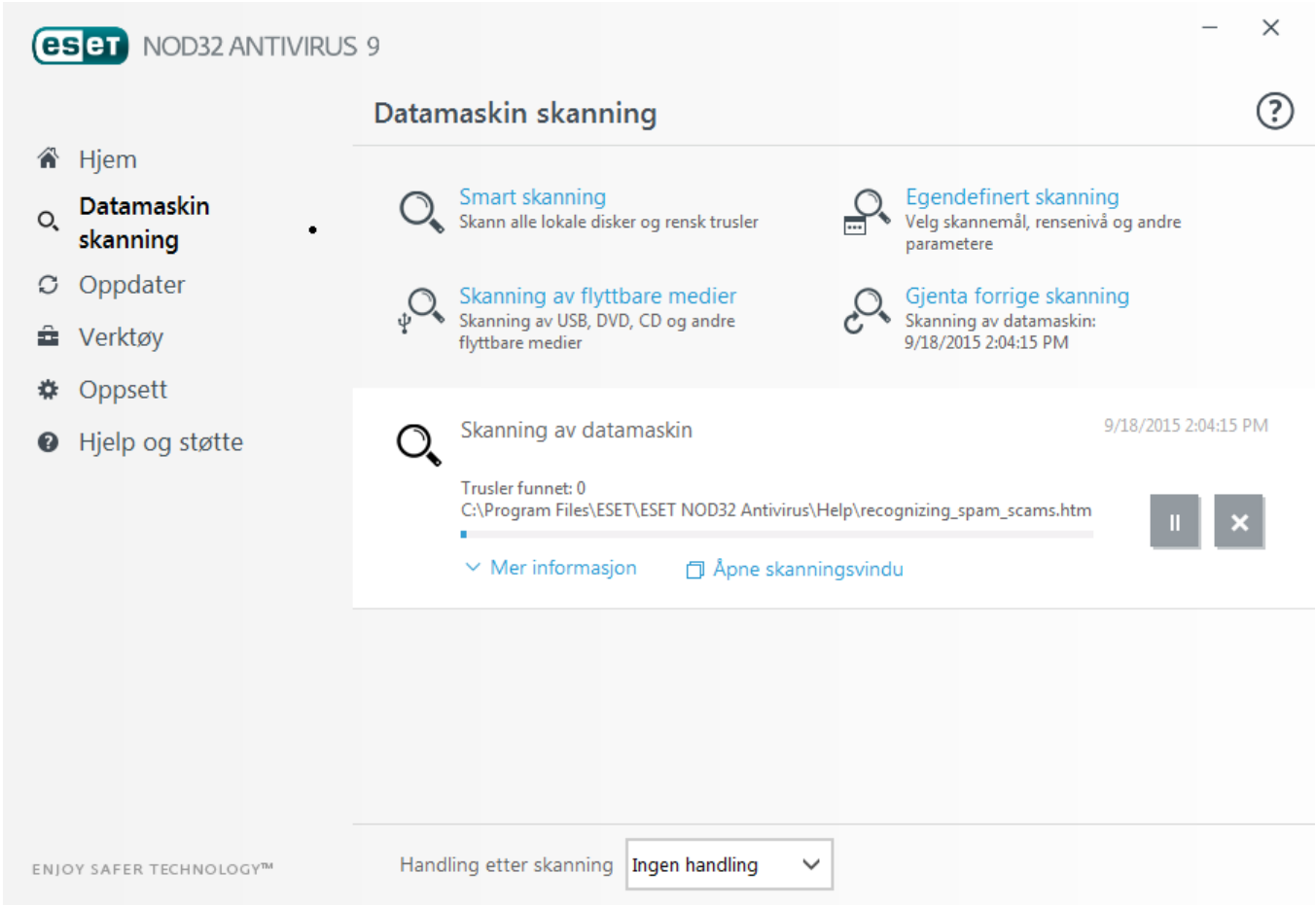
Skannefremdriftsvinduet viser gjeldende status for skanning og informasjon om antall filer funnet med skadelig kode.

MERKNAD: Det er normalt at noen filer, som passordbeskyttede filer eller filer som brukes utelukkende 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 totalt antall skannede filer, trusler som ble funnet og trusler som ble fjernet 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 etter som nye registreringer legges til slik at de nyeste registreringene er synlig.

TIPS:

Klikk på forstørrelsesglasset eller pilen for å se detaljer om den pågående skanningen.
Du kan kjøre en annen, parallell skanning ved å klikke **Skann datamaskinen din** eller **Egendefinert skanning**.



Handling etter skanning – lar deg opprette en planlagt avslutning eller omstart når datamaskinskanningen fullføres. Når skanningen er fullført, vil et bekreftelsesdialogvindu for avslutning åpnes med 60 sekunders tidsavbrudd.

4.1.1.2.3 Skanneprofiler

Du kan lagre dine foretrukne skanneparametre for skanning på 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.

Du oppretter en ny profil ved å åpne vinduet Avansert oppsett (F5) og klikke **Antivirus** > **Datamaskinskanning etter behov** >**Grunnleggende**> **Liste over profiler**. Vinduet **Profilbehandling** inneholder rullegardinmenyen **Valgt profil**, som viser eksisterende skanneprofiler og et alternativ for å opprette en ny. Hvis du vil ha hjelp til å opprette en skanneprofil som er tilpasset ditt behov, kan du se en beskrivelse av hver av parameterne i skanneoppsettet i avsnittet Oppsett av parametere for ThreatSense-motor.

Eksempel: Sett at du vil opprette din egen skanneprofil og konfigurasjonen av **Skann datamaskinen din** 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.

4.1.1.3 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**. For å endre innstillingene, gå til **Verktøy** > **Planlegger** klikk **Kontroll av filer som kjører automatisk ved oppstart** og 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.

4.1.1.3.1 Automatisk filkontroll ved oppstart

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

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 brukt 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.

4.1.1.4 Inaktivitetsskanning

Du kan aktivere skanning i inaktiv tilstand i **Avansert oppsett** under **Antivirus** > **Skanning i inaktiv tilstand** > **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** > **Verktøy** > **ESET LiveGrid®** hvis du ønsker å lagre resultatet av en datamaskinskanning i delen Loggfiler (i hovedprogramvinduet klikker du på **Verktøy** > **Loggfiler** og velger **Datamaskinskanning** fra rullgardinmenyen**Logg**).

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

- Skjermbeskytter
- Datamaskin låst
- Bruker logget av

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

4.1.1.5 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. Det finnes imidlertid tilfeller der du vil kunne ha behov for å ekskludere et objekt, for eksempel store databaseoppføringer som vil gjøre datamaskinen treg ved skanning, eller programvare som er i konflikt med skanningen.

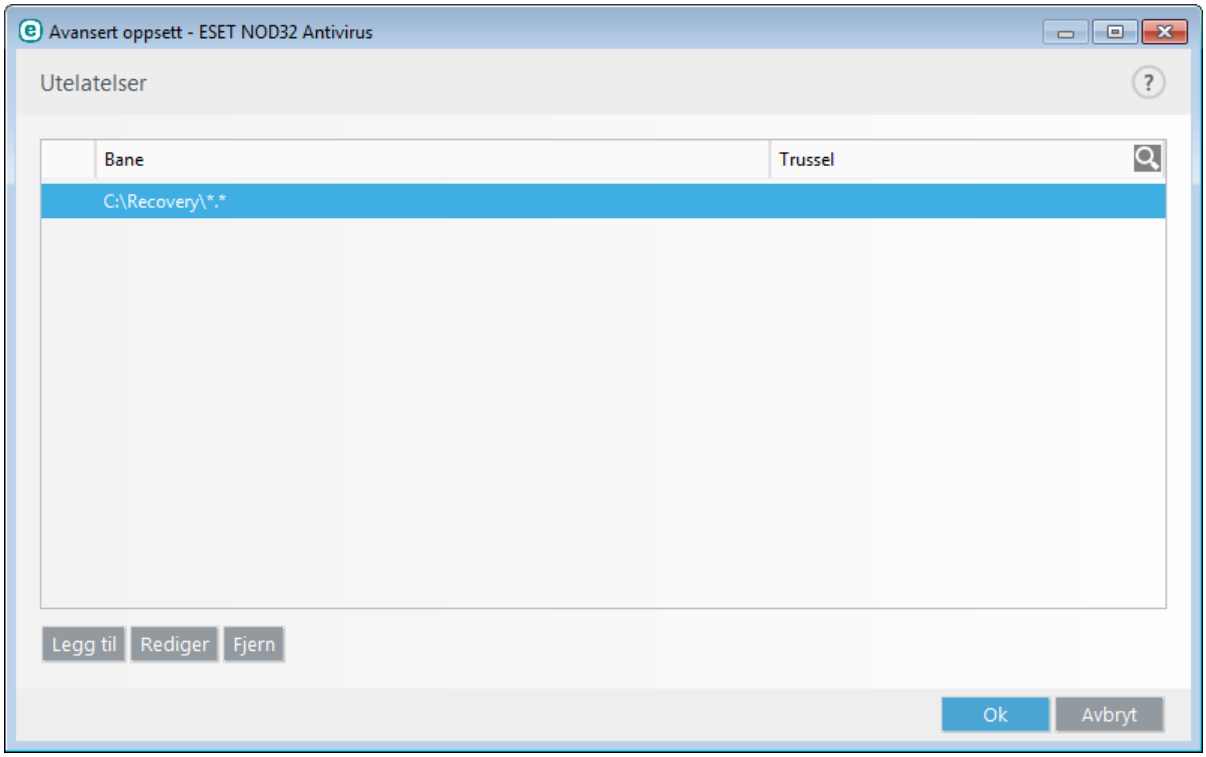
Utelukke et objekt fra skanning:

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 sanntidsbeskyttelse av filsystemet og datamaskinskanning hvis en fil 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 utelatt fil, betyr det at filen ikke er utelatt fullstendig,

bare 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 klikk **Verktøy** > **Karantene** ved å høyreklikke 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.

4.1.1.6 ThreatSense-parametere

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,
- Kombinasjonen av ulike gjenkjenningsmetoder
- Rensingsnivåer osv.

Du kommer inn i oppsettvinduet ved å klikke **ThreatSense-parametere** 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.

Medietyper 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.

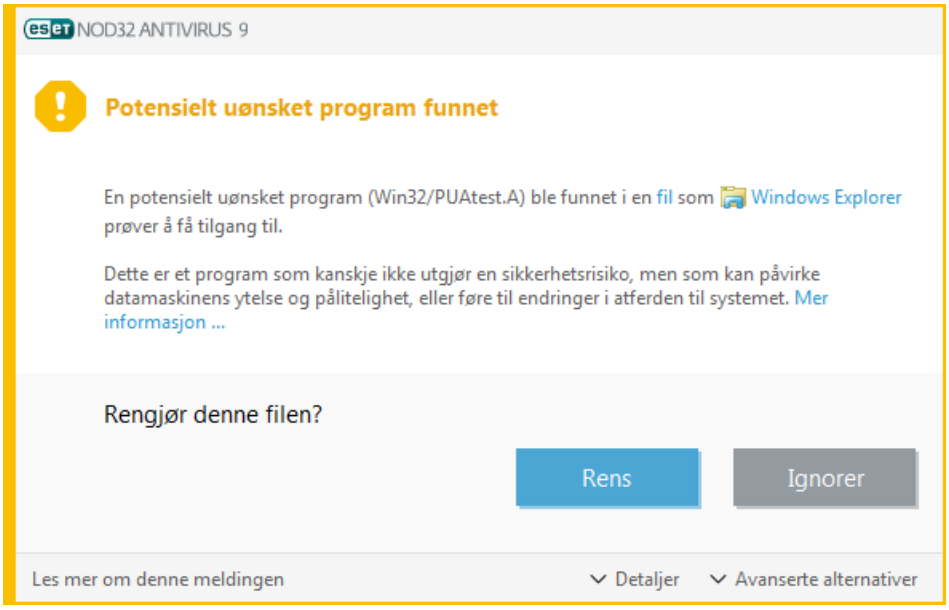
Avansert heuristikk/DNA/Smarte signaturer – Avansert heuristikk består av en unik heuristisk algoritme utviklet av ESET, optimalisert for å gjenkjenne ormer og trojanske hester, og er skrevet i høynivå-programmeringsspråk. Bruk av avansert heuristikk øker ESET-produktenes evne til å gjenkjenne trusler 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.

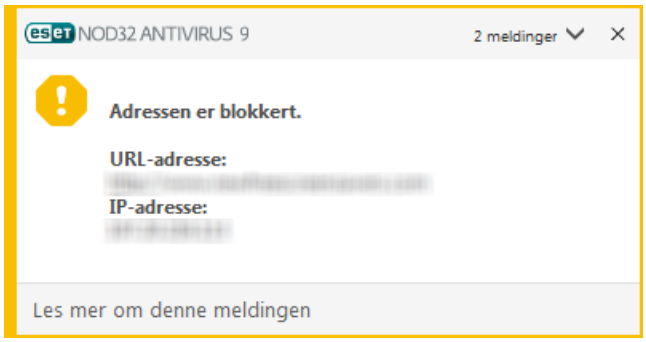
Advarsel – Potensiell trussel funnet

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. **Ignorer**: 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 **Avanserte alternativer** og velg avkrysningsboksen ved siden av **Ekskluder fra gjenkjenning**.

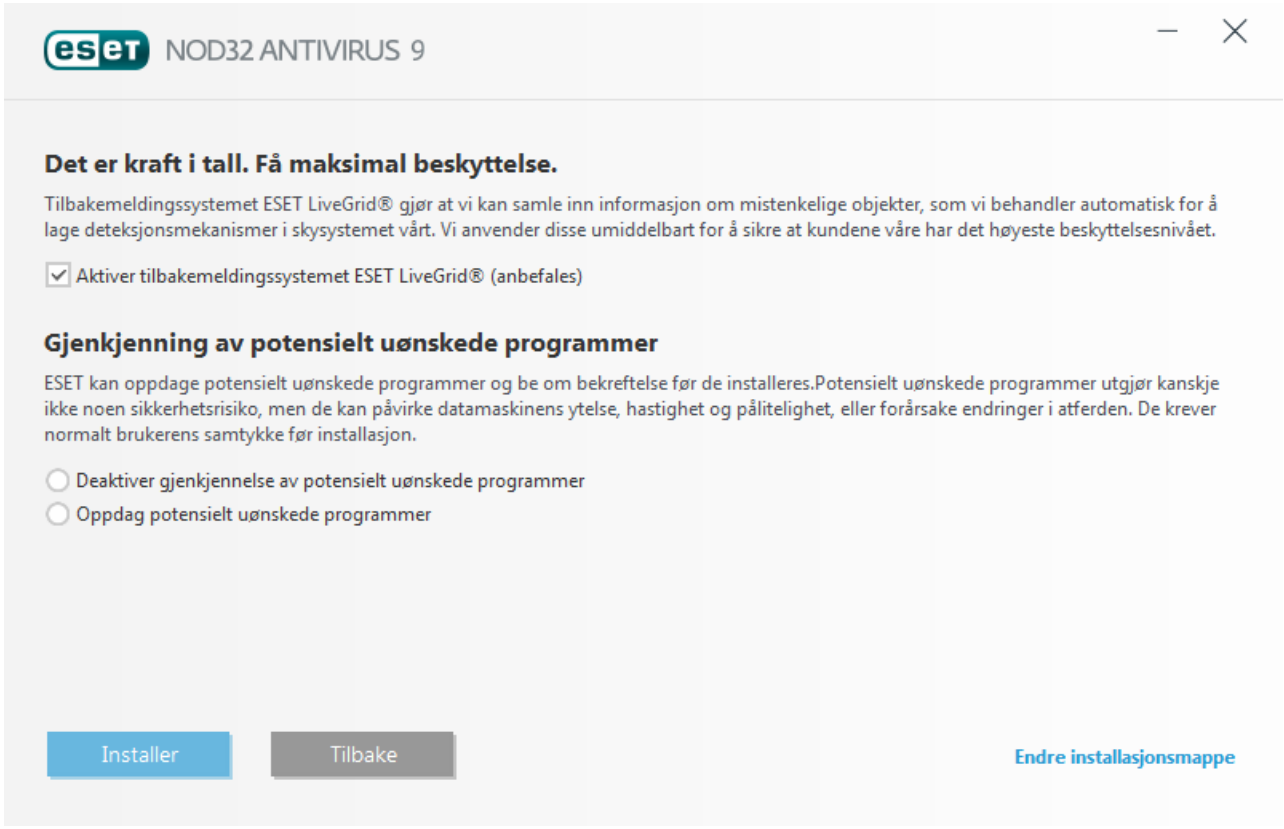


Når et potensielt uønsket program gjenkjennes og det ikke kan rengjøres, vises det et meldingsvindu **Adresse har blitt blokkert** i meldingsområdet nederst til høyre på skjermen. For mer informasjon om denne hendelsen, gå til **Verktøy Loggfiler** > **Filtrerte nettsteder** på hovedmenyen.



Potensielt uønskede programmer – Innstillinger

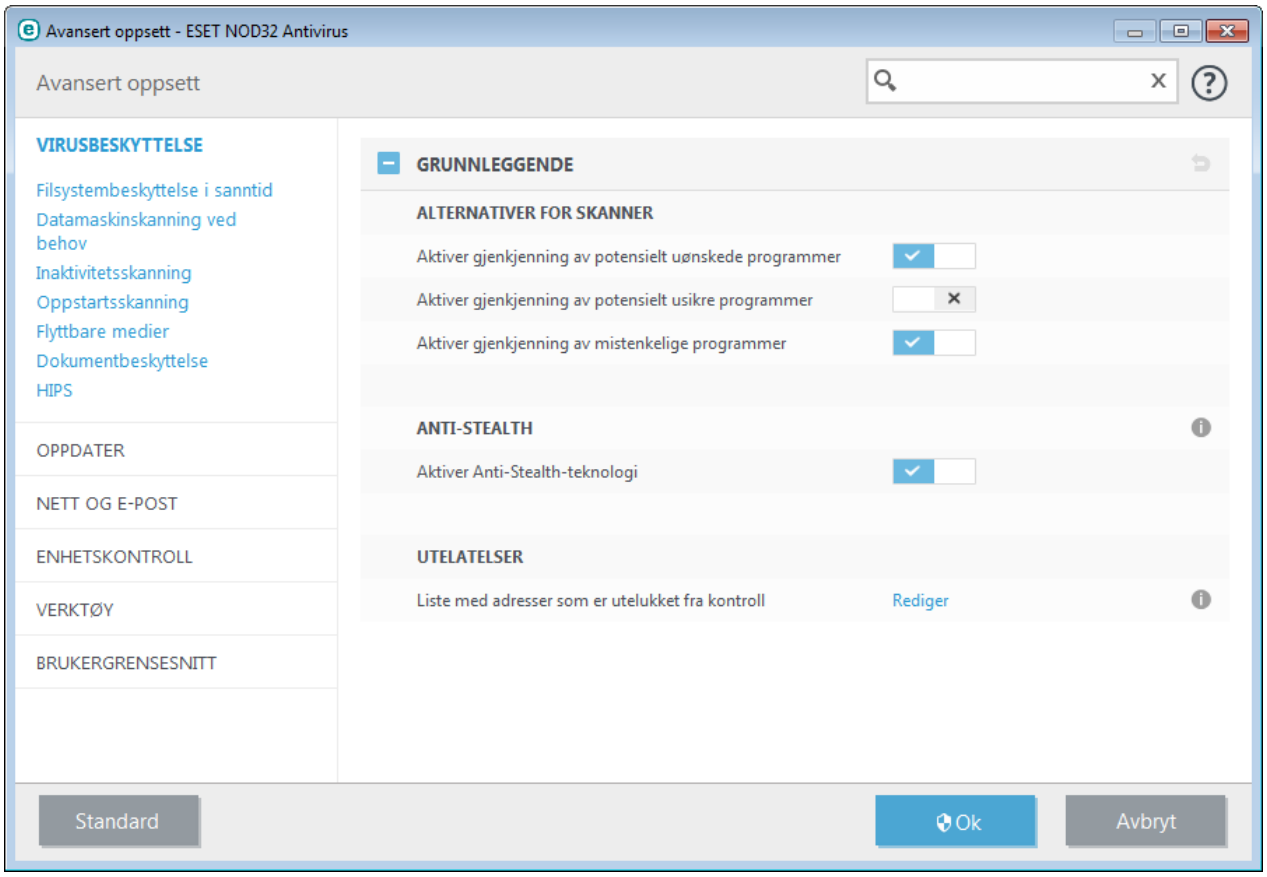
Når du installerer ESET-produktet ditt, kan du velge om du vil aktivere gjenkjenning av potensielt uønskede programmer, som vist nedenfor:



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.

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

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 maksstørrelsen på 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 – Spesifiserer maksimumsdybden på arkivskanning. 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.

4.1.1.6.1 Rensing

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

4.1.1.6.2 Liste med adresser som er utelukket fra kontroll

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.

Som standard blir alle filer skannet, uavhengig av filtype. 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 tillate 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.

4.1.1.7 En infiltrering er gjenkjent

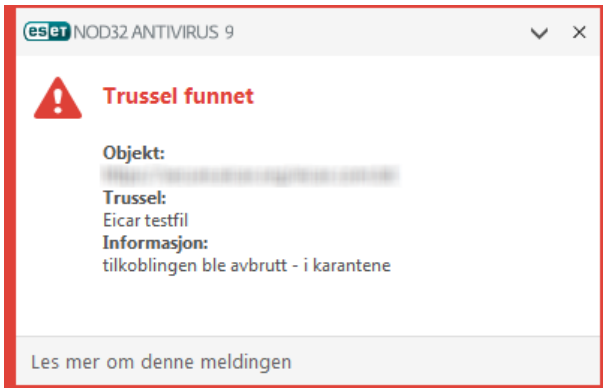
Infiltrasjon kan nå systemet fra forskjellige inngangspunkter, for eksempel nettsider, delte mapper, via e-post eller fra flyttbare enheter (USB, eksterne harddisker, CD-er, DVD-er, disketter osv.).

Standard atferd

Som et generelt eksempel på hvordan infiltrasjoner blir håndtert i ESET NOD32 Antivirus, kan infiltrasjoner oppdages ved hjelp av:

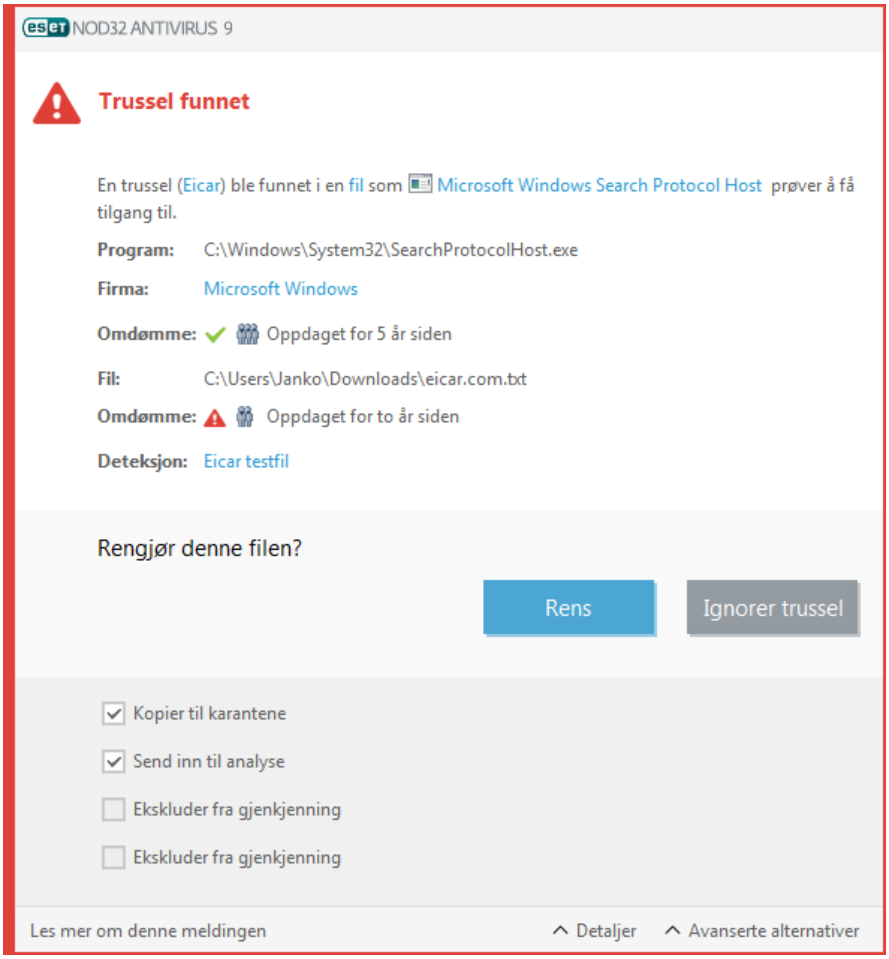
- Filsystembeskyttelse i sanntid
- Beskyttelse for nettilgang
- Beskyttelse for e-postklient
- Datamaskinskanning ved behov

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 Sanntidsbeskyttelse av filsystemet, 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. Velg handling for filene (handlinger angis individuelt for hver av filene i listen), og deretter klikker du **Avslutt**.

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 NOD32 Antivirus og klikk Datamaskinskanning
- Klikk **Skann datamaskinen din** (seDatamaskinskanning for mer informasjon)
- 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.

4.1.1.8 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 endres ved å trykke F5 for å åpne vinduet Avansert oppsett og klikke **Antivirus Dokumentbeskyttelse** i vinduet **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).

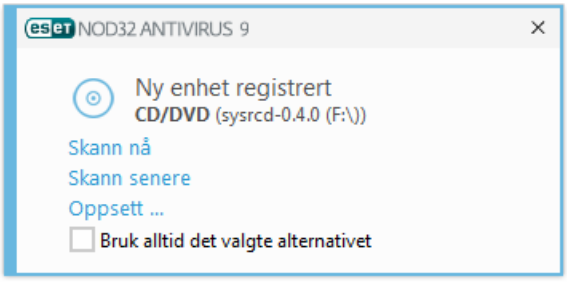
4.1.2 Flyttbare medier

ESET NOD32 Antivirus 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 skanning 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 NOD32 Antivirus Enhetskontroll-funksjonen, som lar deg definere regler for bruk av eksterne enheter på en gitt datamaskin. Mer informasjon om Enhetskontroll finnes i delen Enhetskontroll.

4.1.3 Enhetskontroll

ESET NOD32 Antivirus 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 at brukerne bruker 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

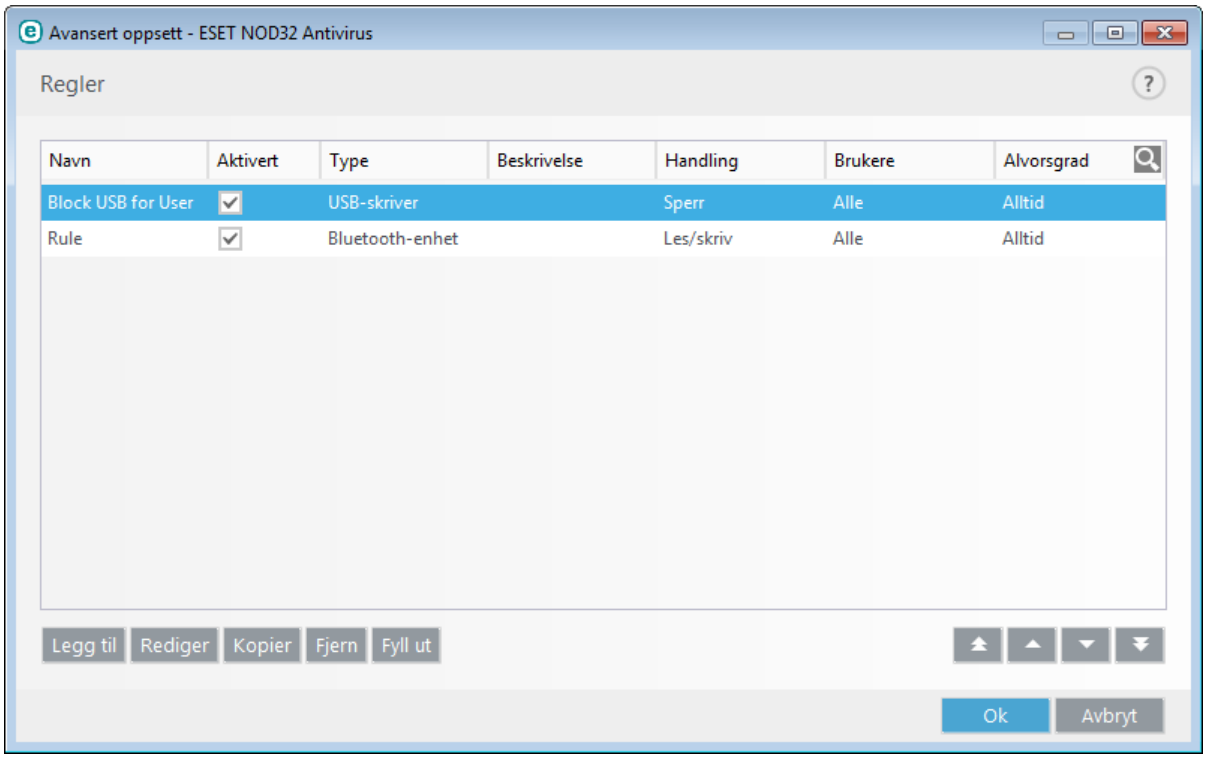
Oppsettsvalgene for enhetskontroll kan endres i **Avansert oppsett** (F5) > **Enhetskontroll**.

Når du slår på bryteren ved siden av **Integrer med system**, aktiveres enhetskontrollfunksjonen i ESET NOD32 Antivirus. 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.

4.1.3.1 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 per bruker eller brukergruppe og baseres på ytterligere parametere 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. Klikk **Kopier** for å opprette en ny regel med forhåndsdefinerte alternativer som brukes for en annen valgt regel. XML-strenger som vises når du klikker en regel, kan kopieres til utklippstavlen eller hjelpe systemansvarlige med å eksportere/importere disse dataene og bruke dem, for eksempel i ESET Remote Administrator.

Trykk CTRL og klikk for å velge flere regler og bruke handlinger på alle de valgte reglene, for eksempel slette eller flytte dem oppover eller nedover på listen. 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.

Kontrollen gjennomføres med regler som er sortert i en rekkefølge som definerer prioriteringen, med regler med høyest prioritet øverst.

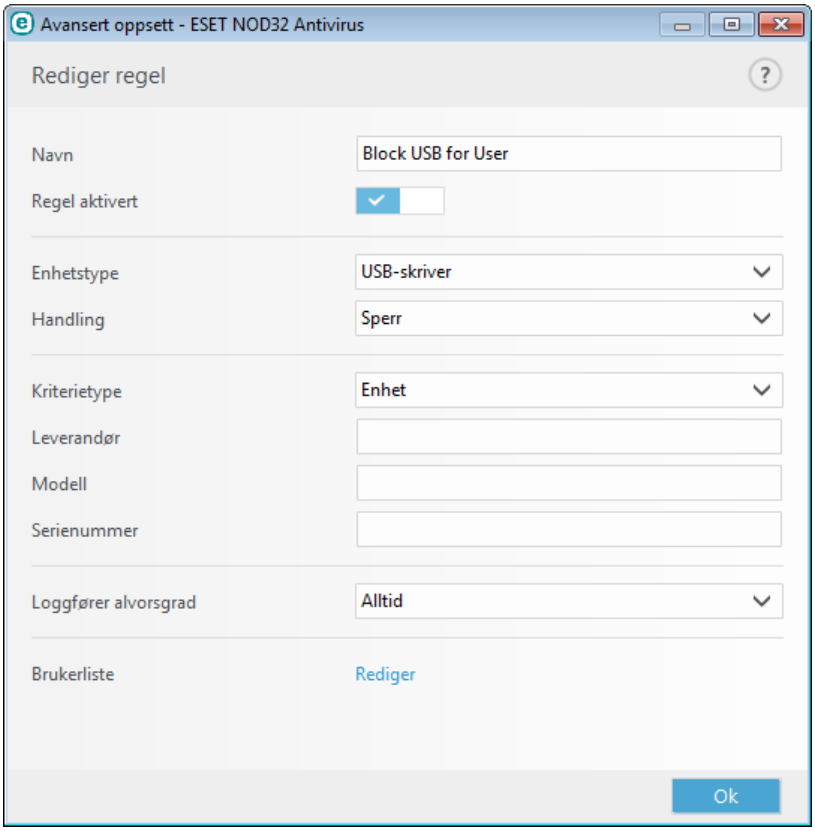
Loggoppføringer kan vises fra hovedvinduet til ESET NOD32 Antivirus i **Verktøy** > **Loggfiler**.

Loggen for enhetskontroll registrerer alle tilfeller der enhetskontroll utløses.

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

4.1.3.2 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.

Loggfører alvorsgrad

ESET NOD32 Antivirus lagrer alle viktige hendelser i en loggfil som du kan vise direkte fra hovedmenyen. Klikk **Verktøy** > **Loggfiler** og velg deretter **Enhetskontroll** på rullegardinmenyen **Logg**.

- **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.

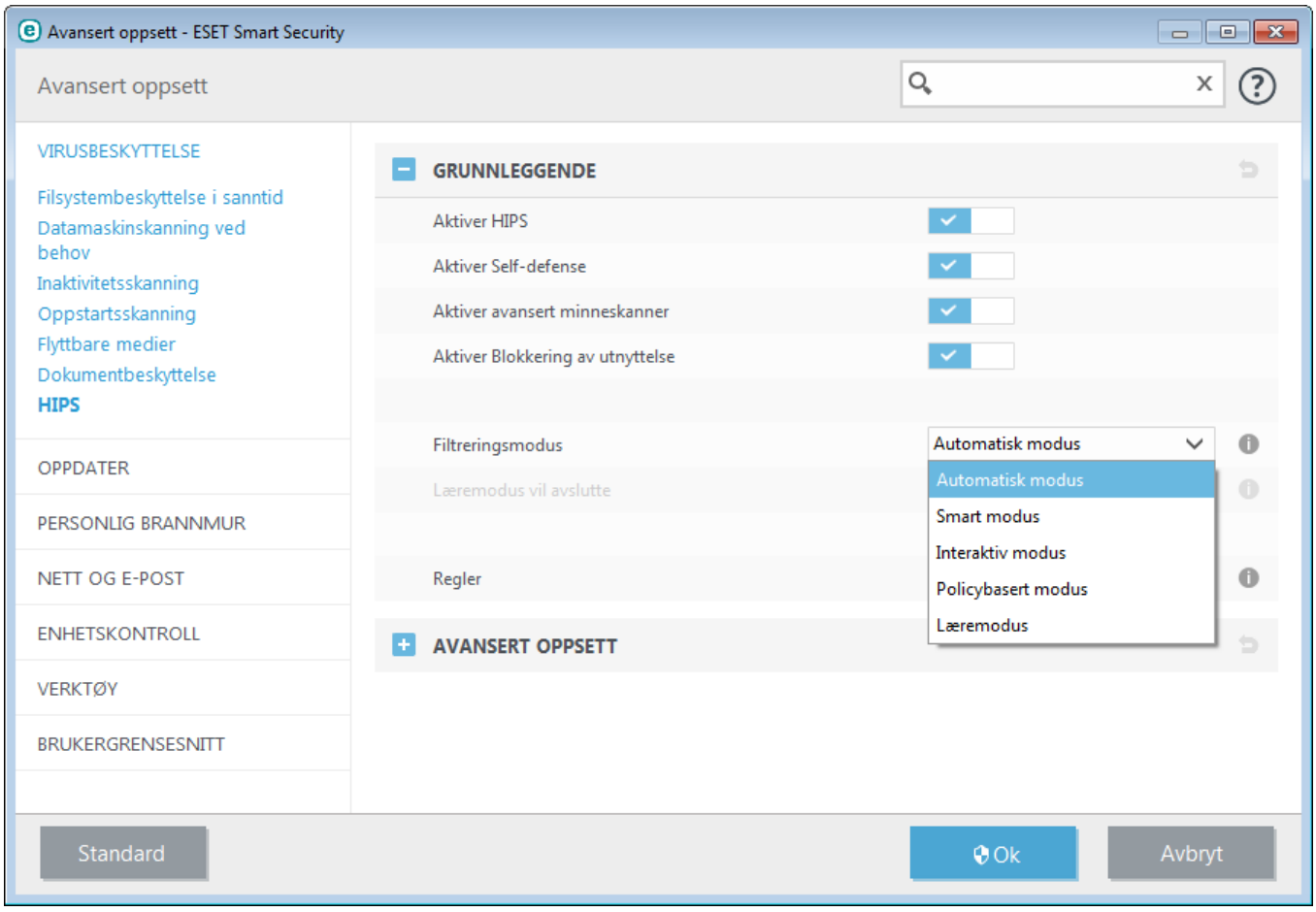
MERK: Alle enheter kan filtreres etter brukerregler, (for eksempel kan ikke bildeenheter gi informasjon om brukere, bare om brukte handlinger).

4.1.4 HIPS

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 NOD32 Antivirus i **Oppsett** > **Datamaskinbeskyttelse**.



ESET NOD32 Antivirus 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 og/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 beskyttelsestypen i glossar.

Filtreringen kan gjøres i en av fire moduser:

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

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

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

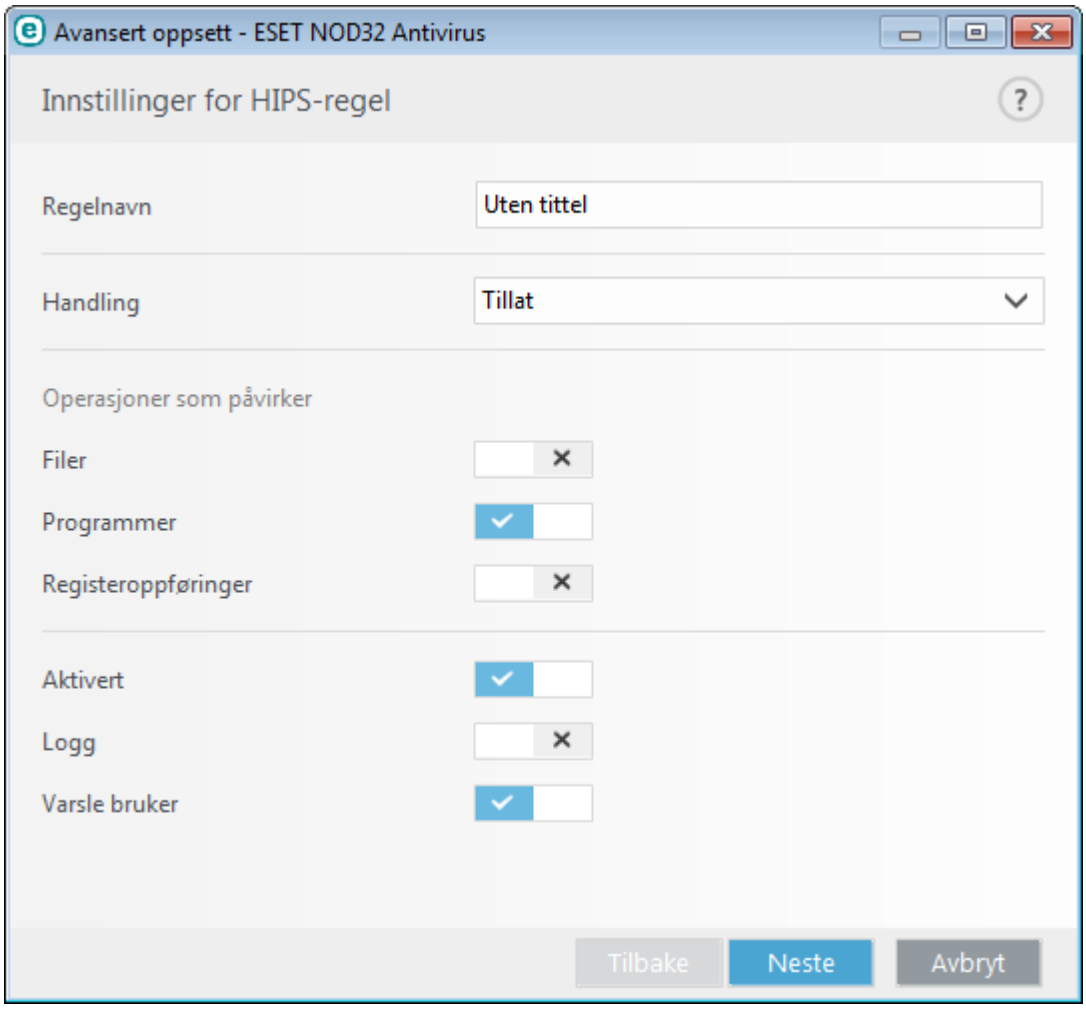
Policybasert modus – Operasjoner blokkeres.

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.

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.



4.1.4.1 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.

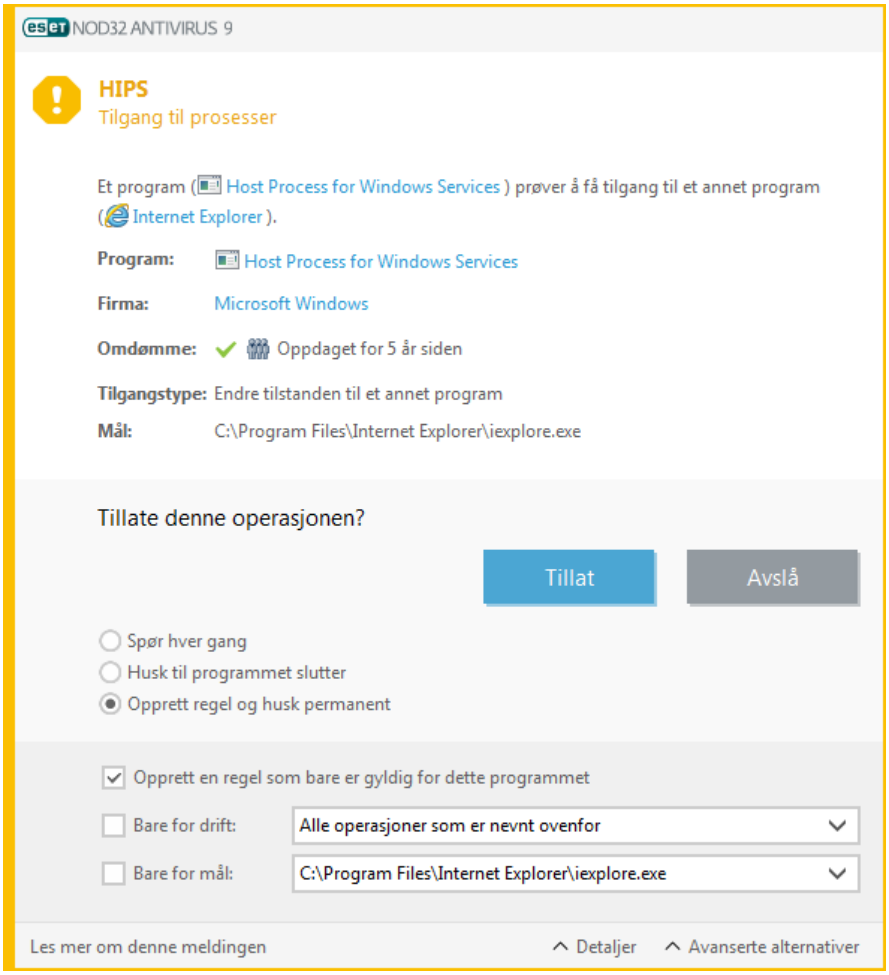
Logg alle blokkerte operasjoner – Alle blokkerte operasjoner vil bli skrevet til HIPS-loggen.

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.

4.1.4.2 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 **Detaljer**. 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 til programmet slutter 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.

4.1.5 Spillmodus

Spillmodus 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. Spillmodus kan også brukes under presentasjoner som ikke kan bli avbrutt av antivirusaktivitet. Når denne funksjonen aktiveres, deaktiveres alle popup-vinduer, og aktiviteten til planleggerfunksjonen stoppes fullstendig. Systembeskyttelsen kjører fortsatt i bakgrunnen, men brukeren behøver ikke å gripe inn.

Du kan aktivere eller deaktivere Spillmodus i programmets hovedvindu i **Oppsett** > **Datamaskinbeskyttelse** ved å klikke eller ved siden av **Spillmodus**. Å aktivere Spillmodus 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 **Spillmodus aktivert** i oransje.

Du kan aktivere Spillmodus i Avansert oppsett-treet (F5) ved å utvide **Datamaskin**, klikke **Spillmodus** og markere boksen ved siden av **Aktiver Spillmodus**.

Merk av for **Aktiver Spillmodus automatisk ved kjøring av programmer i fullskjermmodus** i Avansert oppsett (F5) for å aktivere Spillmodus når du starter et fullskjermprogram, og avslutte det automatisk når du avslutter programmet.

Merk av for **Deaktiver spillmodus automatisk etter** og definere tidsperioden før Spillmodus deaktiveres automatisk.

4.2 Internett-beskyttelse

Nett- og e-postkonfigurering finner du i ruten **Oppsett** ved å klikke **Internett-beskyttelse**. Herfra får du tilgang til mer detaljerte programinnstillinger.

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

Klikk for å åpne nett/e-post/anti-phishing i Avansert oppsett.

Beskyttelse for e-postklient gir kontroll over e-postkommunikasjon som mottas gjennom POP3- og IMAP-protokollene. Med plugin-programmet for e-postklienten gir ESET NOD32 Antivirus deg kontroll over all kommunikasjon til og fra e-postklienten (POP3, MAPI, IMAP, HTTP).

Anti-Phishing-beskyttelse lar deg blokkere nettsider som er kjent for å distribuere phishing-innhold. Vi anbefaler på det sterkeste at du lar Anti-Phishing være aktivert.

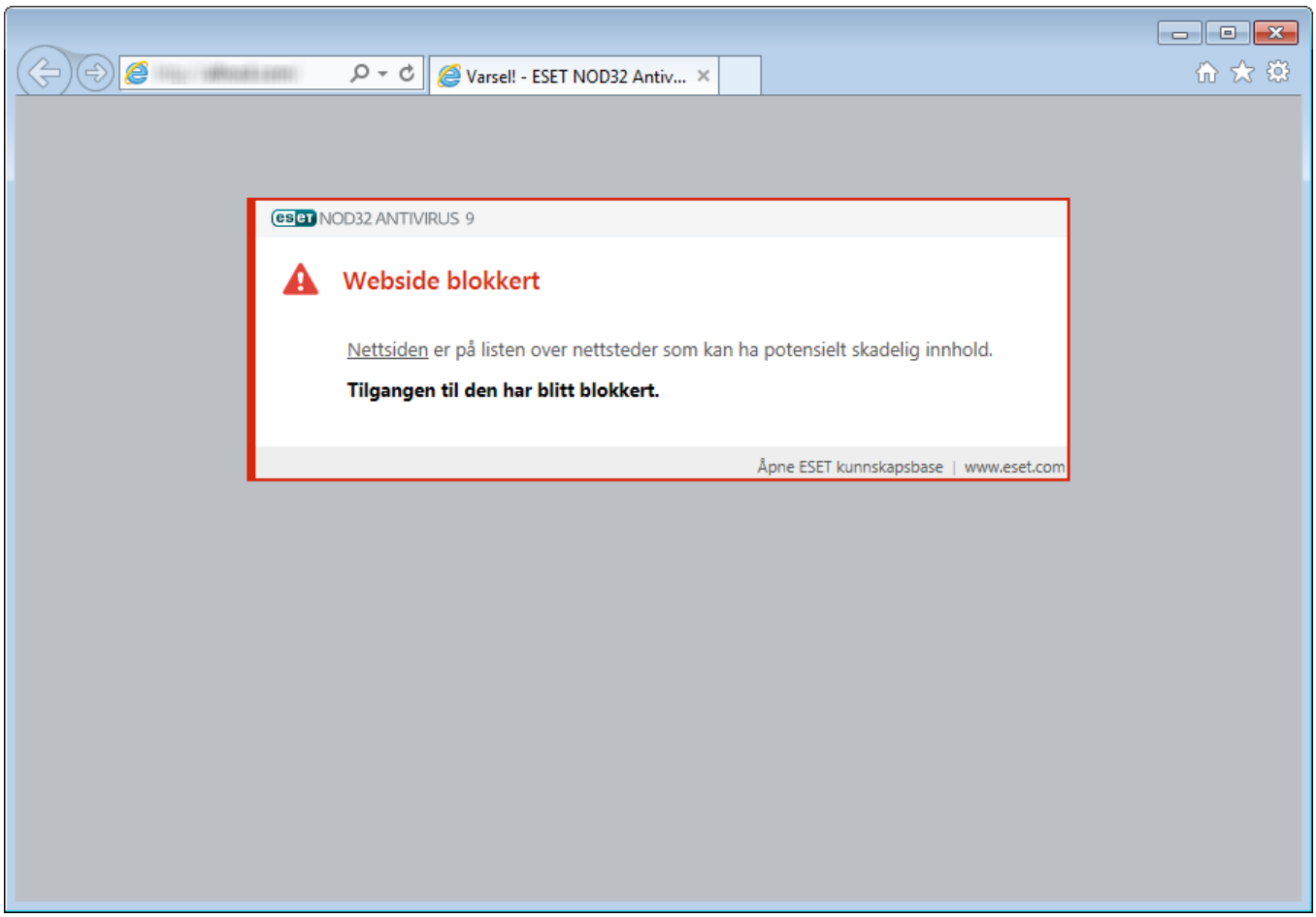
Du kan deaktivere nett/e-post/anti-phishing for nett-/e-post-beskyttelse midlertidig ved å klikke  .

4.2.1 Beskyttelse for nettilgang

Internett-tilkobling er en standardfunksjon på en PC. 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 Beskyttelse for nettilgang aktiveres. Du får tilgang til dette alternativet fra hovedvinduet i ESET NOD32 Antivirus ved å navigere til **Oppsett** >**Internett-beskyttelse** > **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**– Lar deg angi HTTP-adresser som du vil blokkere, tillate eller utelukke fra kontroll.
- **ThreatSense-parametere** – Avansert oppsett for virusskanner – lar deg konfigurere innstillinger for typer objekter som skal skannes (e-poster, arkiver, osv.), gjenkjenningsmetoder for Beskyttelse for nettilgang, osv.

4.2.1.1 Grunnleggende

Aktivere Beskyttelse for nettilgang – Når dette alternativet er deaktivert, vil ikke Beskyttelse for nettilgang og Anti-Phishing-beskyttelse være garantert.

MERKNAD: Vi anbefaler sterkt at du lar dette alternativet være aktivert.

4.2.1.2 Nettprotokoller

Som standard er ESET NOD32 Antivirus konfigurert til å overvåke HTTP-protokollen som brukes av de fleste nettlesere.

Oppsett av HTTP-skanner

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

Oppsett av HTTPS-skanner

ESET NOD32 Antivirus støtter også HTTPS-protokollkontroll. HTTPS-kommunikasjon bruker en kryptert kanal til å overføre informasjon mellom server og klient. ESET NOD32 Antivirus 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. Du aktiverer skanning av kryptert kommunikasjon og viser skanneroppsettet ved å navigere til SSL/TILS i Avansert oppsett, klikke **Nett og e-post** > **SSL/TLS** og aktivere alternativet **Aktiver SSL/TLS-protokollfiltrering**.

4.2.1.3 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.

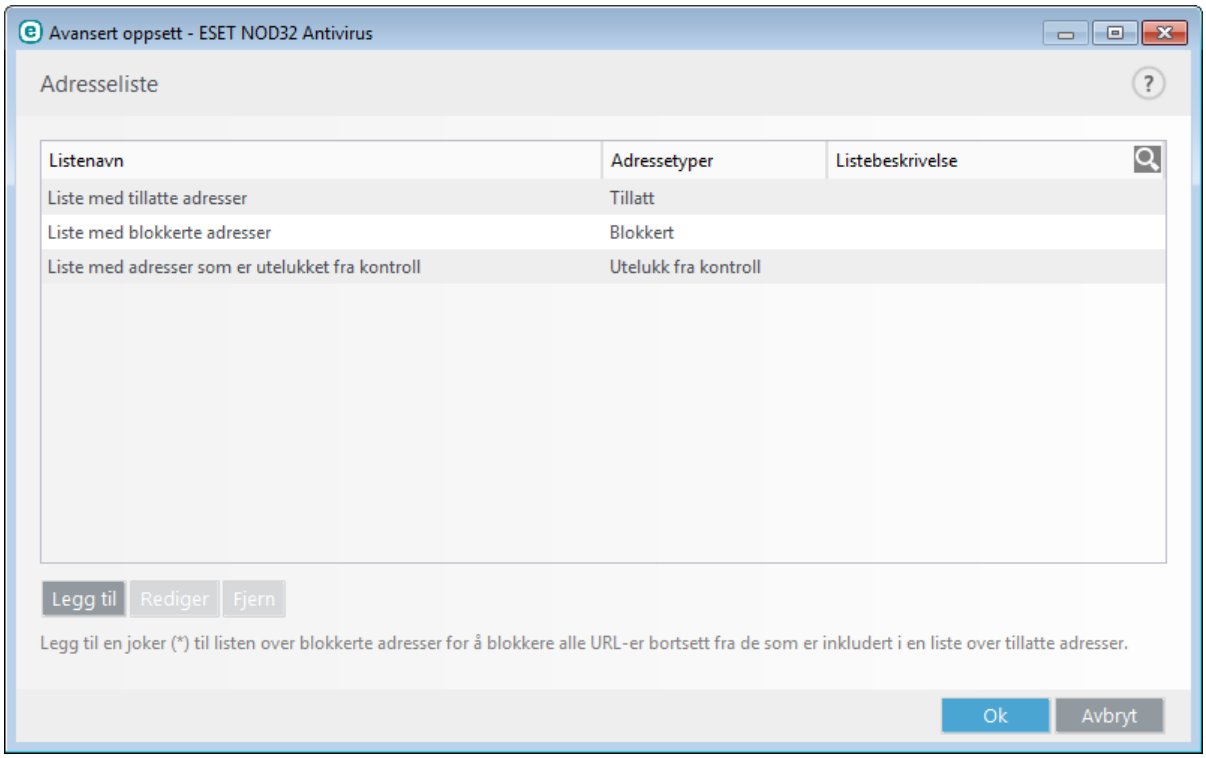
Aktiver SSL-protokollfiltrering må være valgt hvis du vil filtrere HTTPS-adresser i tillegg til HTTP-nettsider. Hvis ikke vil bare domenene til HTTPS-sidene du har besøkt bli lagt til. Den fullstendige URL-en blir altså ikke lagt til.

Hvis du legger til en URL-adresse i **Liste med adresser som er utelukket fra filtrering**, utelukkes adressen fra skanning. Du kan også tillate eller blokkere bestemte adresser ved å legge dem til i **Liste med tillatte adresser** eller **Liste med blokkerte adresse**.

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**.

Spesialsymbolene * (stjerne) og ? (spørsmålstegn) kan brukes i lister. Stjernen erstatter en tegnstreng, og spørsmålstegnet erstatter et symbol. 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 velge **Liste aktiv**. Hvis du ønsker å få beskjed når en adresse fra den gjeldende listen skrives inn, velger du **Varsle under søk**.

TIPS: Med URL-adressebehandling kan du også blokkere eller tillate åpning av spesifikke filtyper under Internett-søk. Hvis du for eksempel ikke vil at kjørbare filer skal åpnes, velger du listen hvor du vil blokkere disse filene i rullegardinmenyen og skriver inn masken "**.exe".



Kontrollelementer

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.

Fjern – Fjerner eksisterende lister. Er bare tilgjengelig for lister som ble opprettet med **Legg til**, ikke standardlistene.

4.2.2 Beskyttelse for e-postklient

4.2.2.1 E-postklienter

Integrasjon av ESET NOD32 Antivirus 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 NOD32 Antivirus. Hvis integrasjon aktiveres, settes verktøylinjen for ESET NOD32 Antivirus 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

Mottatt e-post – Slår av og på kontroll av mottatte meldinger.
Sent e-post – Slår av og på kontroll av sendte meldinger.
Lest e-post – Slår av og på kontroll av leste meldinger.

Handling som skal utføres på infisert e-post

Ingen handling – Programmet gjenkjenner infiserte vedlegg, men lar e-postmeldingene forbli urørt uten å utføre noen handlinger.
Slett e-post– Programmet varsler brukeren om infiltrering(er) 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 – Spesifiser den tilpassede mappen der du ønsker å flytte infiserte e-poster til når disse oppdages.

Gjenta skanning etter oppdatering – Slår av og på ny skanning etter at virussignaturdatabasen er oppdatert.

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

4.2.2.2 E-postprotokoller

Protokollene IMAP og POP3 er de mest brukte protokollene for mottak av e-postkommunikasjon i et e-postklientprogram. Internet Message Access Protocol (IMAP) er en annen Internett-protokoll for henting av e-post. IMAP har enkelte fordeler fremfor POP3, for eksempel at flere klienter kan koble seg til samme postboks samtidig og at informasjon om meldingsstatus beholdes, for eksempel om meldingen har blitt lest, svart på eller slettet. ESET NOD32 Antivirus beskytter disse protokollene, uavhengig av hvilken e-postklient som brukes, og uten at det er nødvendig å konfigurere e-postklienten på nytt.

Beskyttelsesmodulen som gir denne kontrollen, startes automatisk når operativsystemet starter og er deretter aktiv i minnet. IMAP-protokollkontroll utføres automatisk uten at det er nødvendig å konfigurere e-postklienten på nytt. Som standard skannes all kommunikasjon via port 143, men andre kommunikasjonsporter kan legges til ved behov. Flere portnumre må skilles med komma.

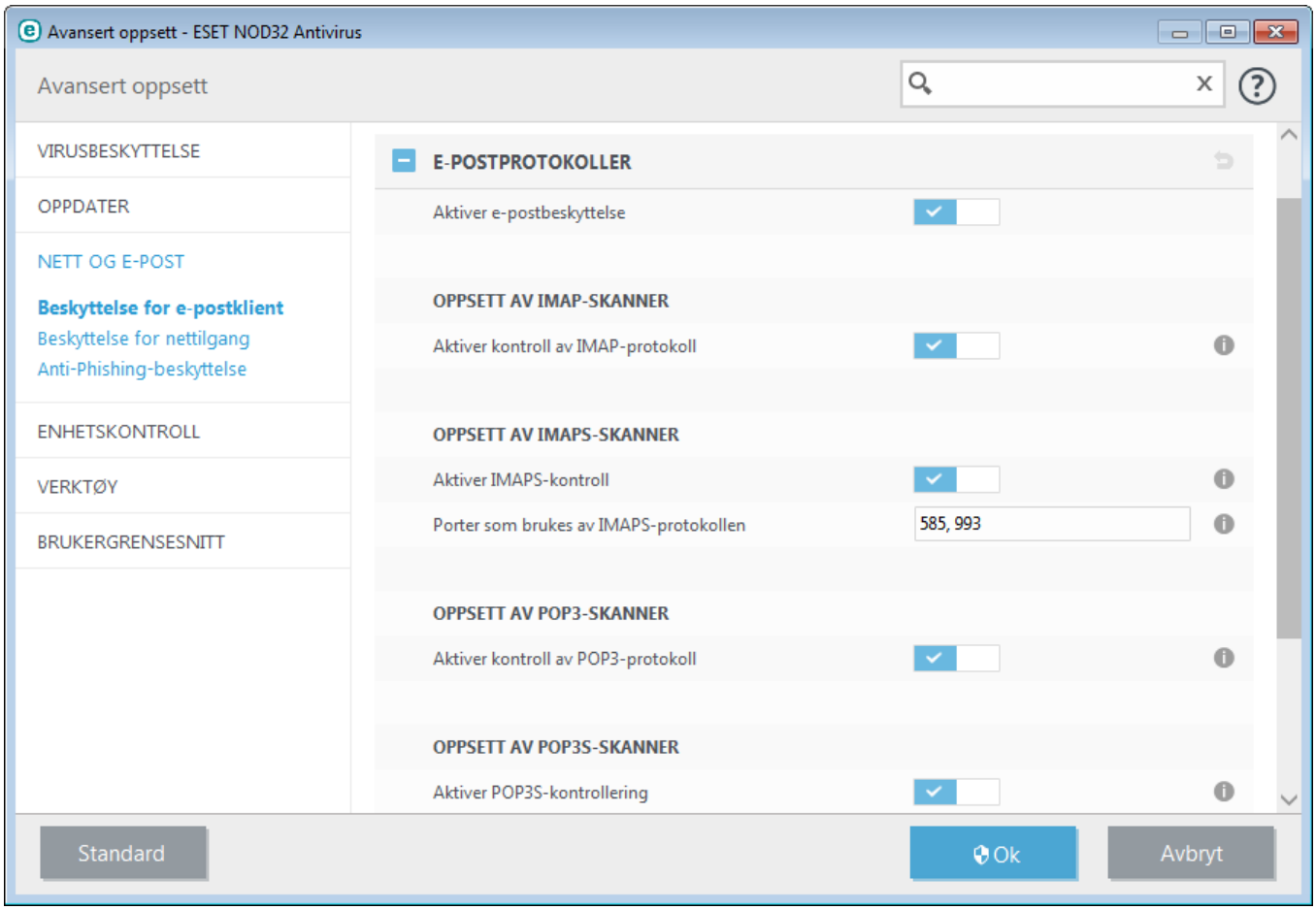
Du kan konfigurere protokollkontroll for IMAP/IMAPS og POP3/POP3S i Avansert oppsett. Du åpne denne innstillingen ved å utvide **Nett og e-post** > **Beskyttelse for e-postklient** > **E-postprotokoller**.

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 som brukes av IMAP/POP3-protokollen** for alle programmene, og alle porter skannes for programmer som er markert som Nett og e-post-klienter.

ESET NOD32 Antivirus støtter også skanning av protokollene IMAPS og POP3S, som bruker en kryptert kanal til å overføre informasjon mellom server og klient. ESET NOD32 Antivirus 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. Du aktiverer skanning av kryptert kommunikasjon og viser skanneroppsettet ved å navigere til SSL/TILS i Avansert oppsett, klikke **Nett og e-post** > **SSL/TLS** og aktivere alternativet **Aktiver SSL/TLS-protokollfiltrering**.



4.2.2.3 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 NOD32 Antivirus 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 finner du i **Avansert oppsett** under **Nett og e-post** > **Beskyttelse for e-postklient** > **Varsler og meldinger**.

ThreatSense-parameter – Avansert oppsett av virusskanner gjør at du kan konfigurere for eksempel skannemål, gjenkjenningsmetoder, osv. Klikk for å vise 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**, **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.

4.2.2.4 Integrasjon med e-postklienter

Integrasjon av ESET NOD32 Antivirus 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 NOD32 Antivirus. Hvis integrasjon aktiveres, settes verktøylinjen for ESET NOD32 Antivirus rett inn i e-postklienten, slik at e-postbeskyttelsen blir mer effektiv. Integrasjonsinnstillingene er tilgjengelige i **Oppsett** > **Åpne avansert oppsett ...** > **Nett og e-post** > **Beskyttelse for e-postklient** > **Integrasjon med e-postklienter**.

E-postklienter som støttes for øyeblikket, er Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. Du finner en komplett liste over e-postklienter som støttes, inkludert versjoner, i følgende artikkel i ESETs kunnskapsbase.

Merk av for **Deaktiver kontroll ved endringer i innboksens innhold** hvis du opplever at systemet fungerer tregt når du arbeider med e-postklienten. Dette kan skje når du laster ned e-post fra Kerio Outlook Connector Store.

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

4.2.2.4.1 Konfigurasjon av beskyttelse for e-postklient

Modulen Beskyttelse for e-postklient støtter følgende e-postklienter: 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.

4.2.2.5 POP3-/POP3S-filter

POP3-protokollen er den mest brukte protokollen for mottak av e-postkommunikasjon i et e-postklientprogram. ESET NOD32 Antivirus beskytter denne protokollen, uavhengig av hvilken e-postklient som brukes.

Beskyttelsesmodulen som gir denne kontrollen, startes automatisk når operativsystemet starter og er deretter aktiv i minnet. For at modulen skal fungere korrekt må du forsikre deg om at den er aktivert - POP3-protokollkontroll blir utført automatisk uten at det er nødvendig å konfigurere e-postklienten på nytt. Standardinnstillingen er at all kommunikasjon på port 110 blir skannet, men andre kommuniksjonsporter kan legges til ved behov. Flere portnumre må skilles med komma.

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

I denne delen kan du konfigurere POP3- og POP3S-protokollkontroll.

Aktiver kontroll av e-post - Hvis dette alternativet er aktivert, blir all trafikk gjennom POP3 overvåket for skadelig programvare.

Porter som brukes av POP3s-protokoll - En liste over porter som brukes av POP3-protokollen (standardporten er 110).

ESET NOD32 Antivirus støtter også POP3S-protokollkontroll. Denne typen kommunikasjon bruker en kryptert kanal til å overføre informasjon mellom server og klient. ESET NOD32 Antivirus kontrollerer kommunikasjonen som bruker krypteringsmetodene SSL (Secure Socket Layer) og TLS (Transport Layer Security).

Ikke bruk POP3S-kontroll - Kryptert kommunikasjon kontrolleres ikke.

Bruk POP3S-protokollkontroll for valgte porter - Merk av for dette alternativet hvis du vil aktivere POP3S-kontroll bare for portene som er definert i **Porter som brukes av POP3s-protokoll**.

Porter som brukes av POP3s-protokoll - En liste over POP3s-porter som skal kontrolleres (standardporten er 995).

4.2.3 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/tls), går du til **Nett og e-post** > **SSL/TLS**.

Aktiver filtrering av programprotokollinnhold – kan brukes til å deaktivere protokollfiltrering. Legg merke til at mange ESET NOD32 Antivirus-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.

4.2.3.1 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.

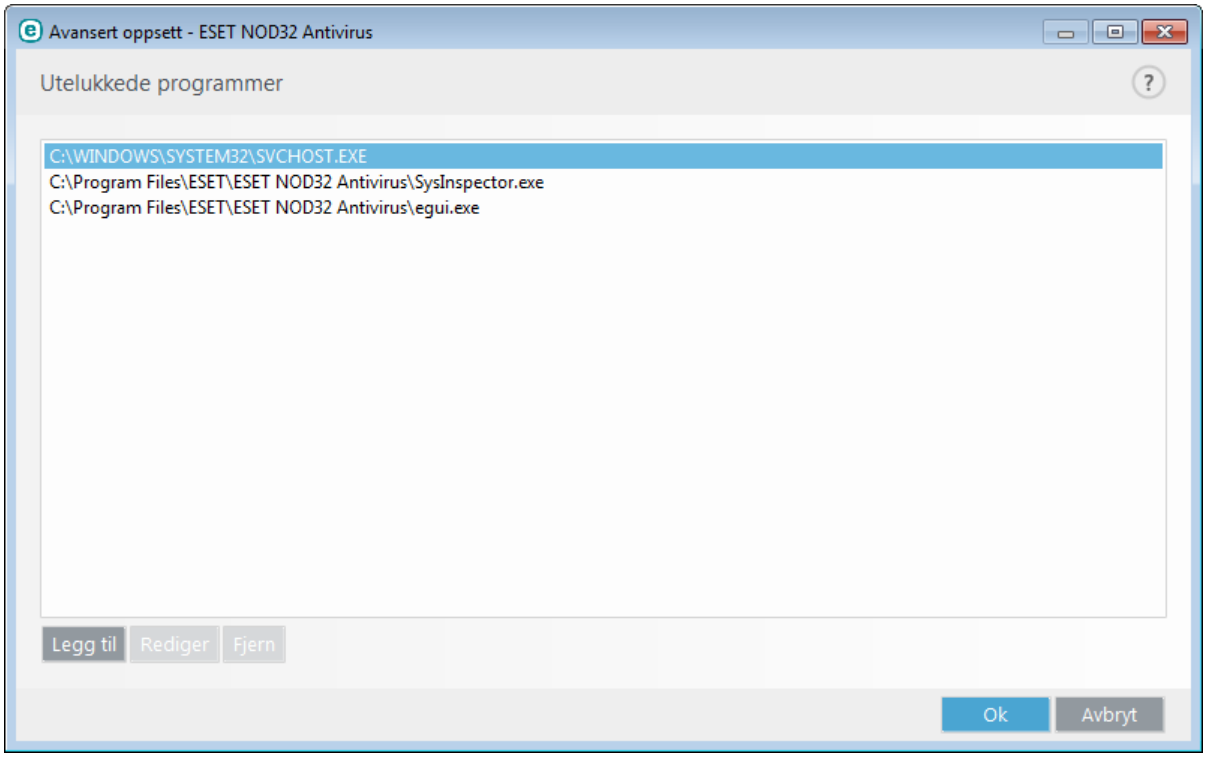
På grunn av den store mengden skadelig kode som sirkulerer på Internett, er sikker bruk av Internett et svært viktig aspekt ved beskyttelse av datamaskiner. Svakheter i nettlesere og falske koblinger fører til at skadelig kode kommer ubemerket inn i systemet, og det er grunnen til ESET NOD32 Antivirus fokuser på nettlesersikkerhet. Hvert enkelt program som bruker nettverket, kan merkes som en nettleser. Boksene har to tilstander:

- **Deaktivert** - Kommunikasjonen til programmer filtreres bare for spesifiserte porter.
- **Aktivert** - Kommunikasjonen filtreres alltid (selv om en annen port er angitt).

4.2.3.2 Utelukkede programmer

Du kan utelukke kommunikasjon for spesifikke nettverksfølsomme programmer fra innholdsfiltrering, ved å velge dem i listen. HTTP-/POP3-/IMAP-kommunikasjon for de valgte programmene kontrolleres ikke for trusler. Vi anbefaler at dette bare brukes for programmer som ikke fungerer som de skal når kommunikasjonen kontrolleres.

Programmer og tjenester som kjører, blir tilgjengelige her automatisk. Klikk **Legg til** for å legge til et program manuelt hvis det ikke vises i protokollfiltreringslisten.

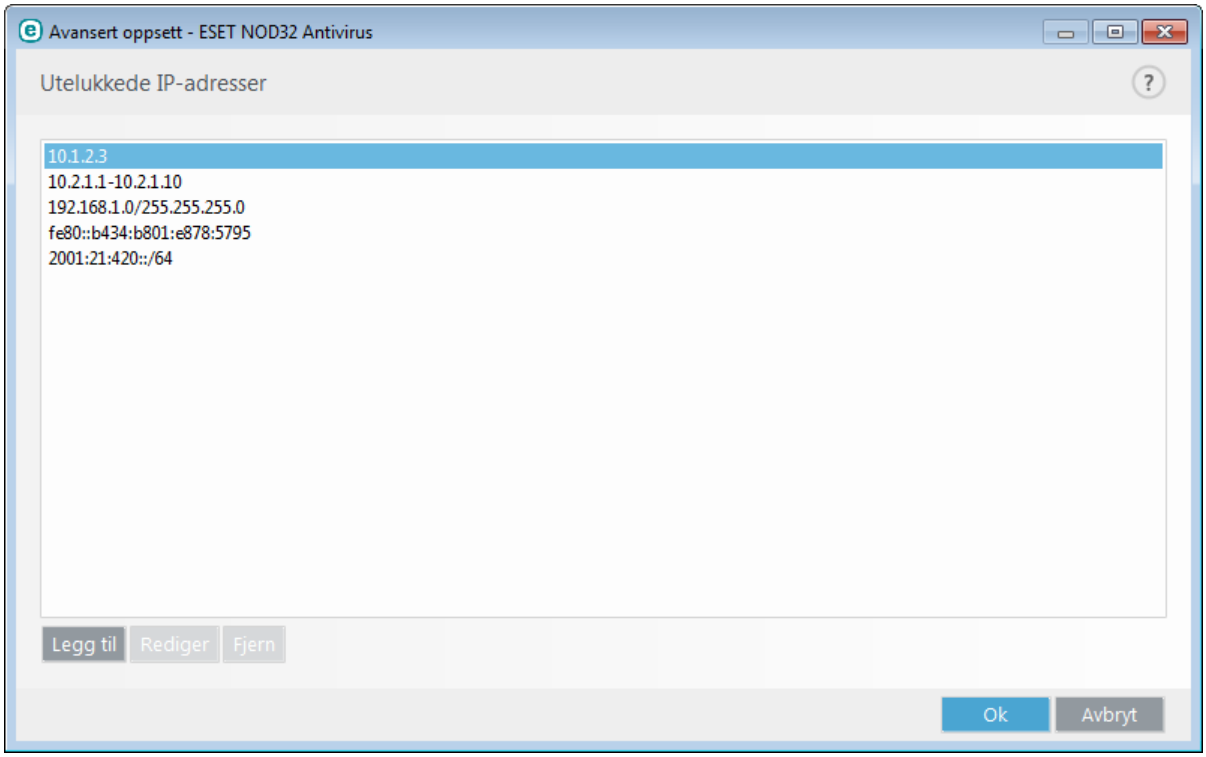


4.2.3.3 Utelukkede IP-adresser

Oppføringene i 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.

Klikk **Legg til** for å utelukke en IP-adresse/adresseområde/delnett til et eksternt punkt som ikke vises i protokollfiltreringslisten.

Klikk **Fjern** for å fjerne de valgte oppføringene fra listen.



4.2.3.3.1 Legg til IPv4-adresse

Dette lar deg legge til en IP-adresse/adresseområde/delnett til et eksternt punkt som regelen skal gjelde for. Internet Protocol versjon 4 er den eldste versjonen, men fremdeles den mest brukte.

En enkelt adresse - Legger til IP-adressen til en individuell datamaskin som regelen skal gjelde for (for eksempel *192.168.0.10*).

Adresseområde - Skriv inn den første og siste IP-adressen for å angi IP-området (for flere datamaskiner) som regelen skal gjelde for, (for eksempel *192.168.0.1* til *192.168.0.99*).

Delnett – Delnett (en gruppe med datamaskiner) defineres av en IP-adresse og -maske.

255.255.255.0 er for eksempel nettverksmasken for prefikset *192.168.1.0/24*, det vil si adresseområdet *192.168.1.1* til *192.168.1.254*.

4.2.3.3.2 Legg til IPv6-adresse

Dette alternativet lar deg legge til en IPv6-adresse/delnett til et eksternt punkt som regelen skal gjelde for. Dette er den nyeste versjonen av Internet Protocol, og vil erstatte den eldre versjon 4.

En enkelt adresse – Legger til IP-adressen til en enkelt datamaskin som regelen skal gjelde for, for eksempel *2001:718:1c01:16:214:22ff:fec9:ca5*).

Delnett – Delnett (en gruppe med datamaskiner) defineres av en IP-adresse og -maske (for eksempel: *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

ESET NOD32 Antivirus 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 – Standard modus vil bare skanne passende programmer slik som nettlesere og e-postklienter. Du man overstyre den ved å velge programmer som du vil skanne kommunikasjon for.

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.

Policymodus – 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.

Liste med SSL-filtrert programmer – Lar deg tilpasse atferden til ESET NOD32 Antivirus for spesifikke programmer.

Liste med kjente sertifikater – Lar deg tilpasse atferden til ESET NOD32 Antivirus for spesifikke SSL-sertifikater.

Ekskluder informasjon som sikres med EV-sertifikater (Extended Validation) –Når dette alternativet aktiveres, vil kommunikasjon med denne typen SSL-sertifikat bli utelukket fra kontroll. EV SSL-sertifikater (Extended Validation) sikrer at du faktisk er inne på din egen nettside og ikke en falskt nettside som ser helt identisk ut (vanlig for phishing-sider).

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

Rotsertifikat

Legg til rotsertifikatet i kjente nettlesere – 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). Når det aktiveres vil ESET NOD32 Antivirus 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.

4.2.3.4.1 Sertifikater

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 (f.eks. 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.

I noen tilfeller kan ikke sertifikatet verifiseres ved hjelp av lageret for klarerte rotsertifiseringsinstanser (f.eks. VeriSign). Dette betyr at sertifikatet er selvsignert av noen (for eksempel administratoren for en nettserver eller et lite selskap), 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. En dialogboks for valg av handling åpnes. Der kan du markere sertifikatet som klarert eller utelukket. Hvis sertifikatet ikke finnes i TRCA-listen, er vinduet rødt. Hvis sertifikatet er i TRCA-listen, vil vinduet bli grønt.

Du kan aktivere alternativet **Blokker kommunikasjon som bruker sertifikatet** for alltid å avslutte krypterte tilkoblinger til nettstedet som bruker det ubekreftede sertifikatet.

Hvis sertifikatet er ugyldig eller skadet, betyr det at sertifikatet har utløpt eller ble selvsignert ved en feil. I så fall anbefaler vi at du blokkerer kommunikasjonen som bruker sertifikatet.

4.2.3.4.2 Liste med kjente sertifikater

Listen med kjente sertifikater kan brukes til å tilpasse atferden til ESET NOD32 Antivirus 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 – Navn på sertifikatet.

Sertifikatutsteder – Navn på sertifikatutsteder.

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

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** hvis du vil avslutte uten å lagre.

4.2.3.4.3 Liste med SSL-filtrert programmer

Liste med SSL-filtrerte programmer kan brukes til å tilpasse atferden til ESET NOD32 Antivirus for spesifikke programmer, og til å huske valgte handlinger hvis **Interaktiv modus** er valgt i **filtreringsmodus for SSL-protokoll**. Listen kan vises og redigeres i **Avansert oppsett** (F5) > **Nett og e-post** > **SSL** > **Liste med SSL-filtrerte programmer**.

Vinduet **Liste med SSL-filtrert programmer** består av:

Kolonner

Program – Navn på programmet.

Skanningshandling – Velg **Skanning** eller **Ignorere** for å skanne eller ignorere kommunikasjon. 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 – Legg til filtrert program.

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** hvis du vil avslutte uten å lagre.

4.2.4 Anti-Phishing-beskyttelse

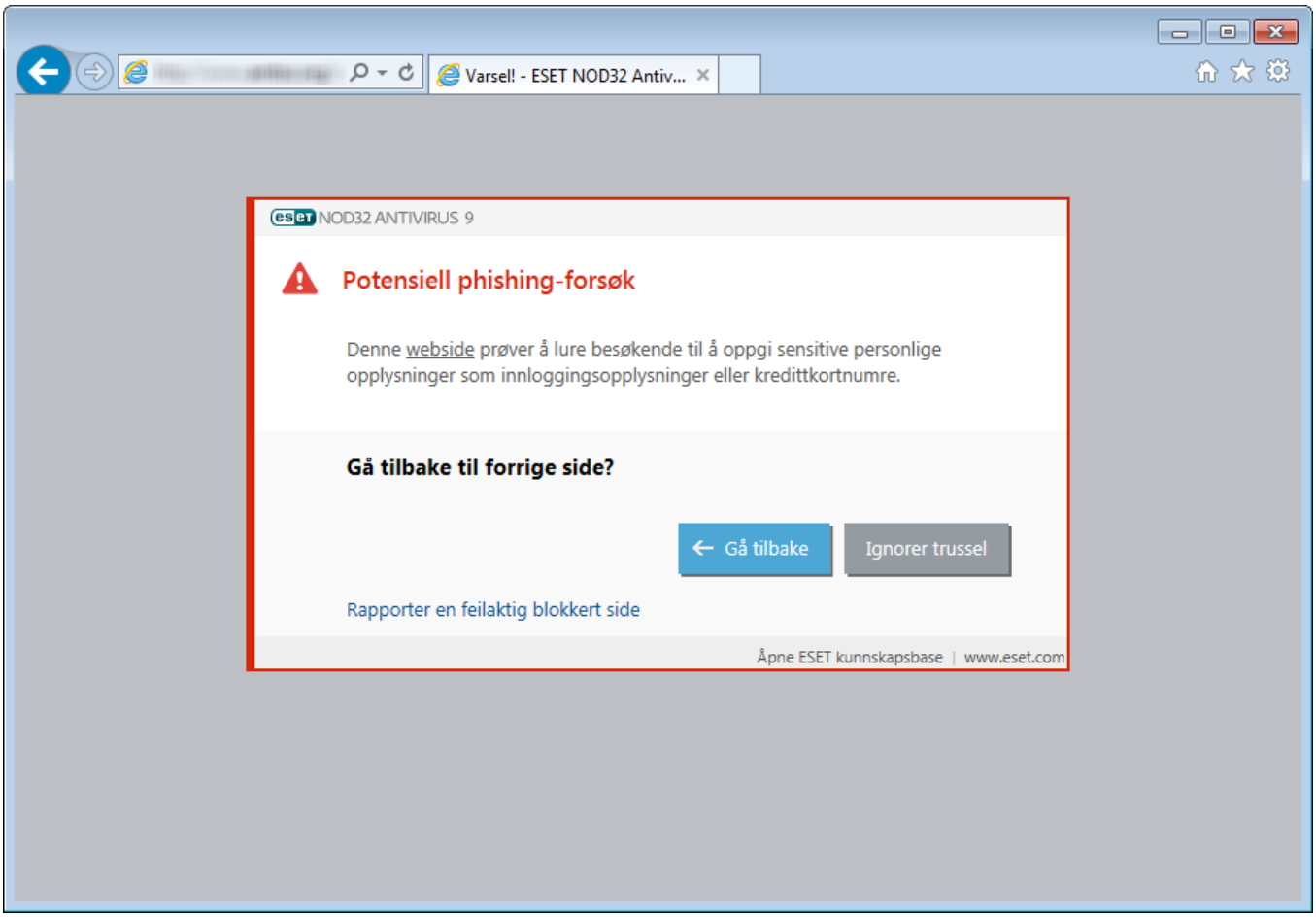
Begrepet phishing definerer en kriminell handling som bruker sosial manipulering for å få andre til å oppgi ellers hemmelig informasjon. Phishing brukes ofte for å få tilgang til sensitivt materiale som f.eks. bankkontonumre, PIN-koder osv. Du kan lese mer om denne aktiviteten i ordlisten. ESET NOD32 Antivirus 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 NOD32 Antivirus. 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 NOD32 Antivirus.

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 **Ignorer trussel** (anbefales ikke).



MERK: 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 rapportere en feilaktig blokkert side.

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.).

4.3 Oppdatere programmet

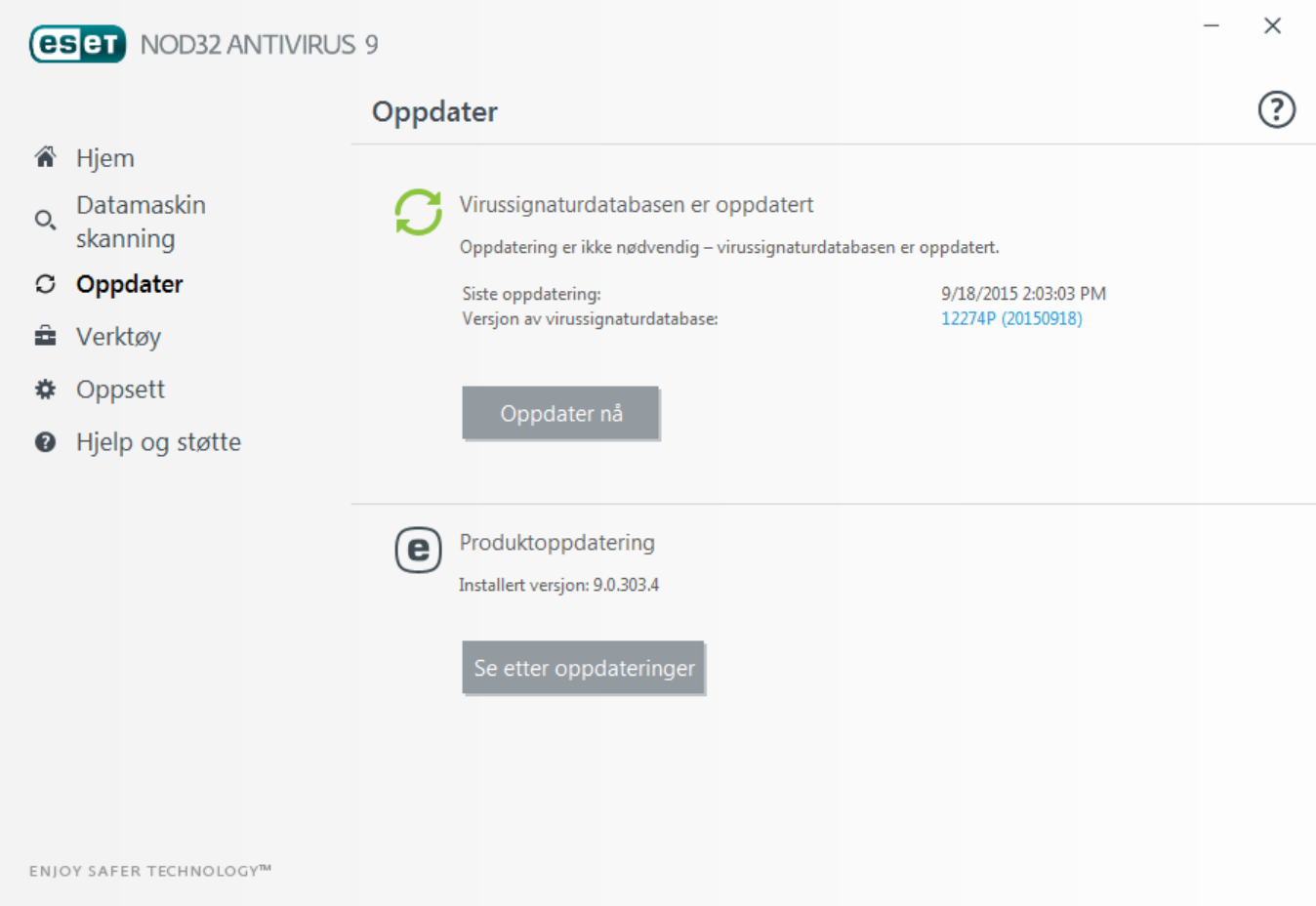
Regelmessig oppdatering av ESET NOD32 Antivirus er den beste måten å sikre maksimalt sikkerhetsnivå for datamaskinen. Oppdateringsmodulen har to metoder for å sikre at programmet alltid er oppdatert, ved å oppdatere virussignaturdatabasen og ved å oppdatere systemkomponentene.

Du kan klikke **Oppdater** i hovedvinduet for å vise 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 til automatiske oppdateringer kan du klikke på **Oppdater nå**. Da utløser du en oppdatering manuelt. 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. Du må aktivere produktet ditt ved bruk av lisensnøkkel for å motta oppdateringer. Hvis du ikke gjorde dette under

installasjonen, kan du skrive inn lisensnøkkelen for å aktivere produktet under oppdateringen for å få tilgang til ESETs oppdateringsservere.

MERKNAD: ESET sender deg en lisensnøkkel på e-post etter at du har kjøpt ESET NOD32 Antivirus.



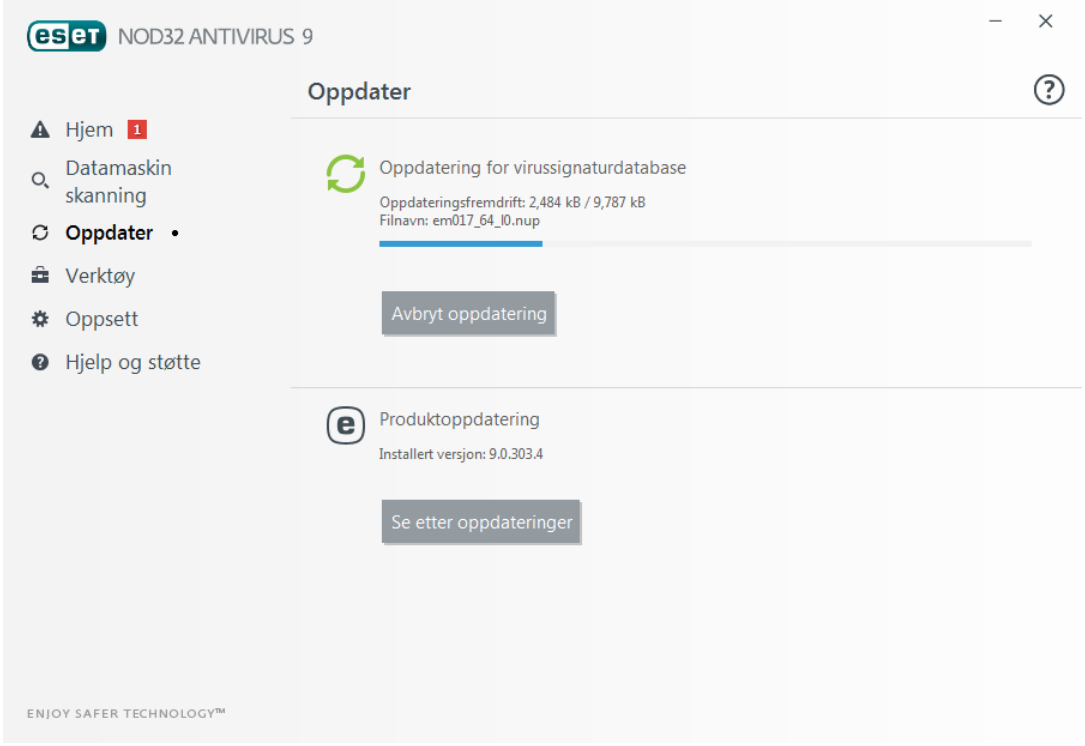
Siste fullførte oppdatering - viser dato for siste oppdatering. Hvis du ikke ser en nylig dato, kan det hende at virussignaturdatabasen din ikke er nylig oppdatert.

Virussignaturdatabaseversjon – Virussignaturdatabasenummeret, som også er en aktiv kobling til ESETs nettsted. Klikk for å vise en liste over alle signaturer som er lagt til i en bestemt oppdatering.

Klikk **Se etter oppdateringer** for å finne siste tilgjengelige versjon av ESET NOD32 Antivirus.

Oppdateringsprosessen

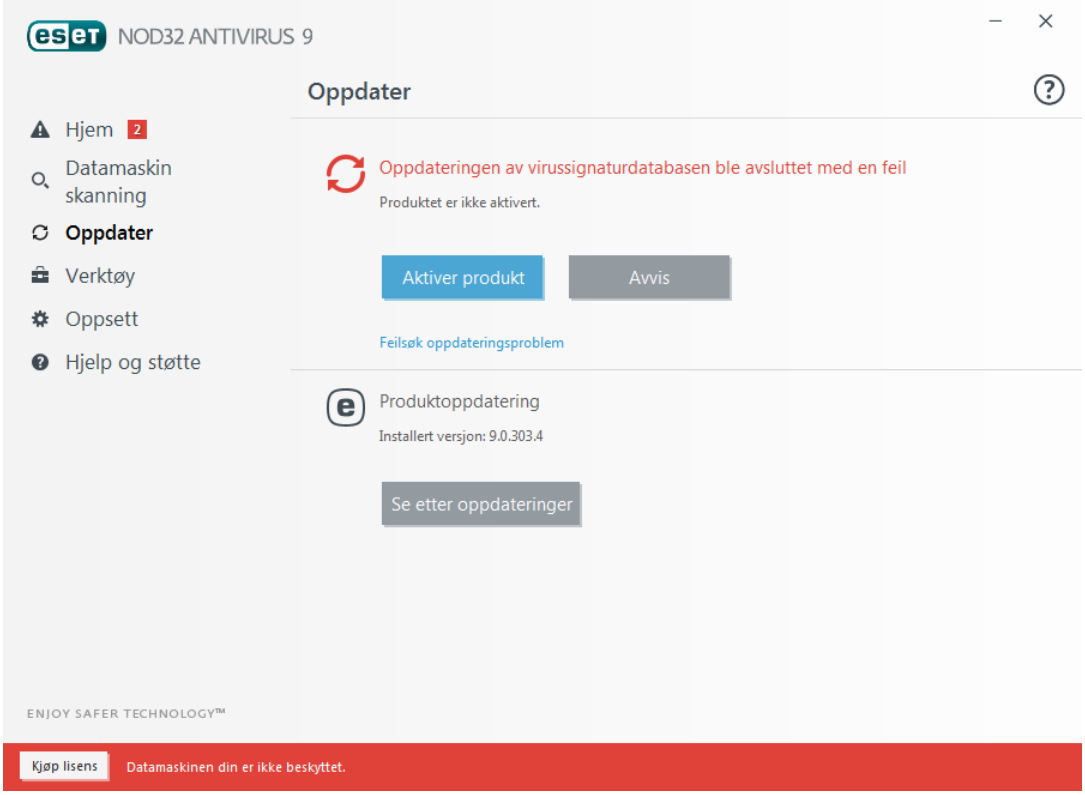
Nedlastingen begynner når du klikker **Oppdater nå**. En fremdriftslinje for nedlastingen og gjenstående tid vises. Hvis du vil avbryte oppdateringen, klikker du **Avbryt oppdatering**.



Viktig: Under normale omstendigheter, 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. Ellers vises en av de følgende meldingene:

Den forrige varslingen 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** > **Endre lisens** på hovedmenyen for å skrive inn ny lisensnøkkel.
2. **Det oppsto en feil da programmet prøvde å laste ned oppdateringsfiler** – Dette kan skyldes 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.

4.3.1 Oppdatere innstillinger

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**.

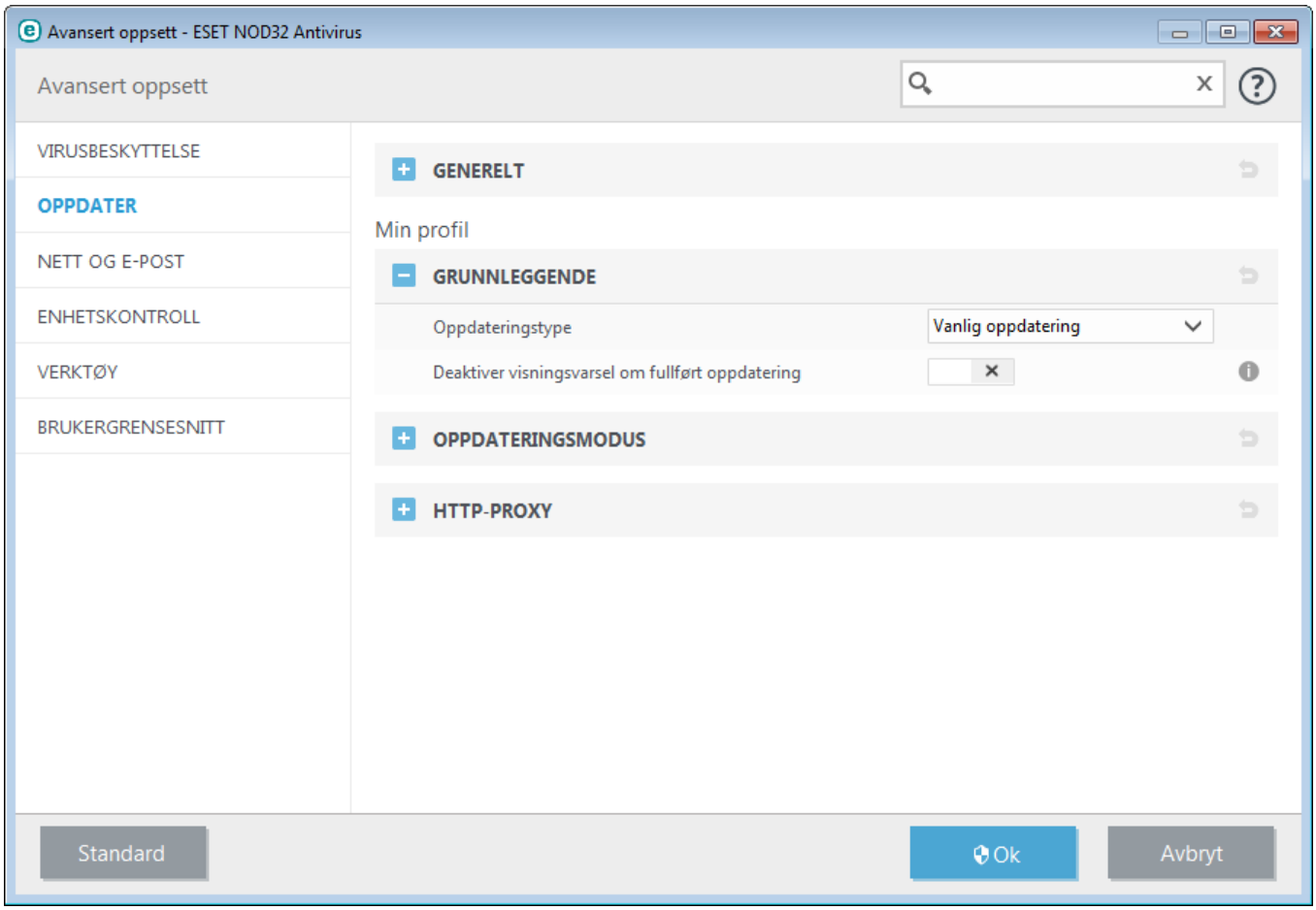
Hvis du opplever problemer med en oppdatering når du forsøker å laste ned oppdateringer for virussignaturdatabasen, klikker du på **Slett** for å slette midlertidige oppdateringsfiler/hurtigbuffer.

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 NOD32 Antivirus 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.

Deaktiver visningsvarsel om fullført oppdatering – Deaktiverer meldingen i systemstatusfeltet nederst til høyre på skjermen. Det kan være nyttig å velge dette alternativet hvis du kjører et program i fullskjermmodus, eller hvis du spiller et spill. Vær oppmerksom på at Presentasjonsmodus slår av alle meldinger.

4.3.1.1 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 først **Profiler ...**. Deretter klikker du **Legg til ...** og angir ditt eget **Profilnavn**. Når du oppretter en ny profil, kan du kopiere innstillinger fra en eksisterende profil ved å velge den fra rullegardinmenyen**Kopier innstillinger fra profil**.

4.3.1.2 Avansert oppsett for oppdatering

Du ser Avansert oppsett for oppdatering ved å klikke **Oppsett ...**. Avansert oppsett for oppdatering inkluderer konfigurering av **Oppdateringsmodus**, **HTTP Proxy** og **LAN**.

4.3.1.2.1 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. Etter at en oppdatering av en programkomponent er installert, er det mulig at du må starte datamaskinen på nytt.

Programoppdatering – Når dette er aktivert, utføres hver programkomponentoppgradering automatisk og i stillhet uten full programoppdatering.

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.

4.3.1.2.2 HTTP-proxy

Du får tilgang til oppsettalternativene for proxy-servere for en bestemt oppdateringsprofil ved å klikke **Oppdater** i treet **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 NOD32 Antivirus.

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

- En proxy-server må brukes ved oppdatering av ESET NOD32 Antivirus, 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: **Proxy-**serveradresse, **kommunikasjonsport** (3128 som standard), samt**Brukernavn** og **Passord** for proxy-serveren, hvis det kreves.
- Proxy-serverinnstillingene har ikke blitt spesifisert globalt, men ESET NOD32 Antivirus 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 NOD32 Antivirus, og skal bare fylles inn hvis du vet at du trenger passord for å få tilgang til Internett via en proxy-server.

4.3.1.2.3 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 alternativet **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.

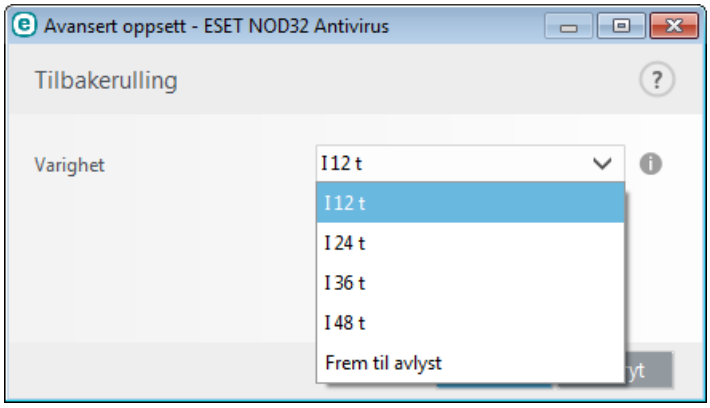
Velg alternativet **Koble fra konto etter oppdatering** for å tvinge frem en frakobling hvis en tilkobling til serveren forblir aktiv også etter at oppdateringene er lastet ned.

4.3.2 Oppdater gjenoppretting

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 NOD32 Antivirus registrerer avbildninger av virussignaturdatabasen og programmoduler for bruk med *tilbakerullings*funksjonen. La boksen **Opprett avbildning av oppdateringsfiler** være merket av for å opprette avbildninger av virusdatabasen. Feltet **Antall lokalt lagrede avbildninger** definerer antall avbildninger av tidligere virusdatabaser som lagres.

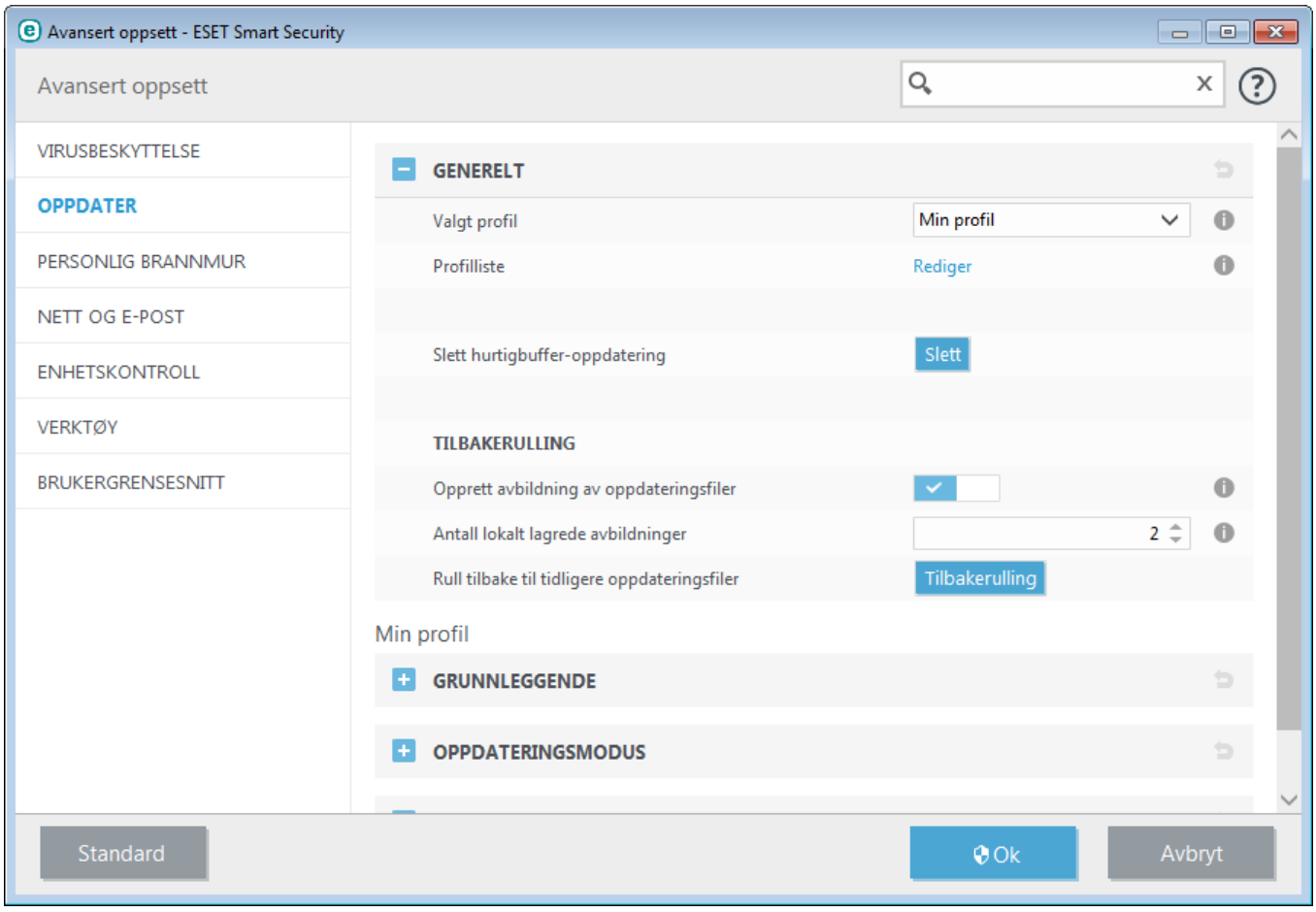
Hvis du klikker **Tilbakestill** (**Avansert oppsett** (F5) > **Oppdater** > **Avansert**), må du velge et tidsintervall fra rullegardinmenyen **Opphev oppdateringer** som viser hvor lenge oppdateringene av virussignaturdatabasen og programmodulene vil være satt på pause.



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.

Hvis en tilbakerulling utføres, endres knappen **Tilbakestill** til **Tillat oppdateringer**. Ingen oppdateringer vil være tillatt for tidsintervallet valgt i rullegardinmenyen **Opphev oppdateringer**. Versjonen av virussignaturdatabasen blir nedgradert til den eldste tilgjengelige og lagret som en avbildning i filsystemet på den lokale datamaskinen.



Eksempel: La nummer 6871 være den nyligste versjonen av virussignaturdatabasen. 6870 og 6868 blir lagret som avbildninger av en virusdatabase. Merk at 6869 ikke er tilgjengelig fordi, for eksempel, datamaskinen var slått av og en nyere oppdatering ble gjort tilgjengelig før 6869 ble lastet ned. Hvis du har angitt 2 i feltet **Antall lokalt lagrede avbildninger** og klikker **Tilbakestill**, blir virussignaturdatabasen (inkludert programmoduler) gjenopprettet til versjonsnummer 6868. Denne prosessen kan ta litt tid. Kontroller om versjonen av virussignaturdatabasen er nedgradert fra hovedvinduet i ESET NOD32 Antivirus i delen Oppdater.

4.3.3 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 NOD32 Antivirus :

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

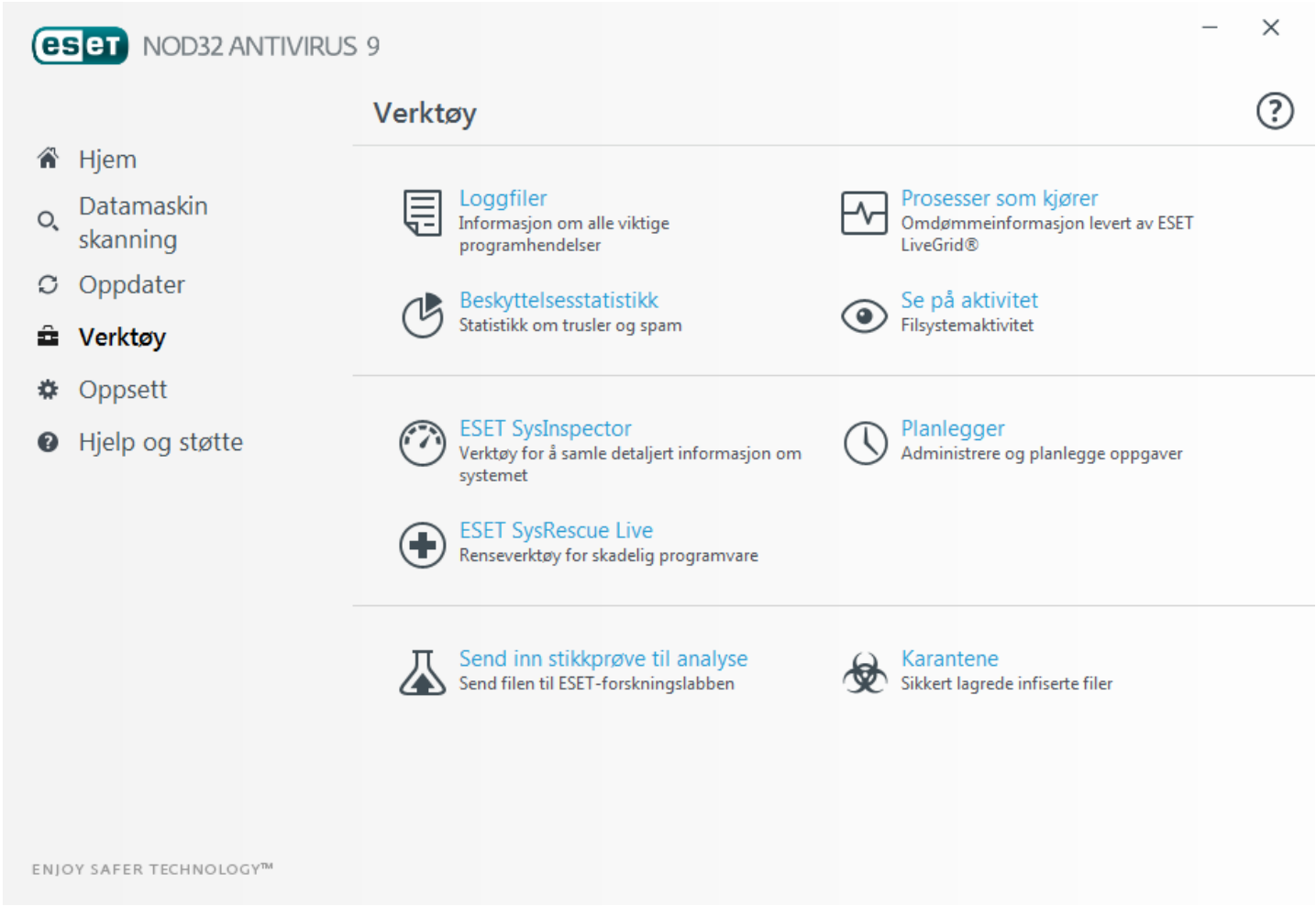
Hver oppdateringsoppgave kan endres etter dine behov. I tillegg til standardiserte oppdateringsoppgaver kan du opprette nye oppdateringsoppgaver med en brukerdefinert konfigurasjon. Hvis du vil vite mer om hvordan du oppretter og konfigurerer oppdateringsoppgaver, kan du se Planlegger.

4.4 Verktøy

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

4.4.1 Verktøy i ESET NOD32 Antivirus

Den/Det **Verktøy** menyen inneholder moduler for enklere programadministrasjonen og tilleggsalternativer for avanserte brukere.



Denne menyen inneholder følgende verktøy:

 Loggfiler

 Beskyttelsesstatistikk

 Se på aktivitet

 Kjørende prosesser (hvis ThreatSense er aktivert i ESET NOD32 Antivirus)

 ESET SysInspector

 ESET SysRescue Live – 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.

 Planlegger

 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 i denne delen.

 Karantene

MERKNAD: ESET SysRescue er kanskje ikke tilgjengelig for Windows 8 i eldre versjoner av ESET-sikkerhetsprodukter. I så tilfelle, anbefaler vi at du oppgraderer produktet ditt eller oppretter en ESET SysRescue-disk i en annen versjon av Microsoft Windows.

4.4.1.1 Loggfiler

Loggfiler inneholder informasjon om viktige programhendelser som har skjedd, og gir en oversikt over trusler som er oppdaget. Loggføring 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 NOD32 Antivirus-miljøet, samt arkivere logger.

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

- **Gjenkjente trusler** – Trusselloggen gir detaljert informasjon om infiltrasjoner som gjenkjennes av ESET NOD32 Antivirus . Logginformasjon 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 NOD32 Antivirus, registreres i hendelsesloggene. Hendelsesloggen inneholder informasjon om hendelser og feil som har oppstått i programmet. Den er utformet for at systemadministratorer og brukere skal kunne løse problemer. Ofte kan informasjon som finnes her, hjelpe deg med å finne en løsning på et problem som oppstår i programmet.
- **Datamaskinskanning** - Resultater fra alle fullførte manuelle eller planlagte skanninger 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 HIPS-regler som er merket for registrering. Protokollen viser programmet som utløste operasjonen, resultatet (om regelen var tillatt eller forbudt) og navnet på den opprettede regelen.
- **Filtrerte nettsteder** - Denne listen er nyttig hvis du ønsker å se en liste over nettsteder som har blitt blokkert av Beskyttelse for nettilgang. I disse loggene kan du se tidspunktet, URL-adressen, brukeren og programmet som opprettet en tilkobling til det aktuelle nettstedet.
- **Enhetskontroll** – Inneholder poster med flyttbare medier eller enheter som var tilkoblet datamaskinen. Bare enheter med respektiv 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 ved å velge oppføringen og bruke tastatursnarveien **Ctrl+C.** Tastene **Ctrl** og **Shift** kan brukes til 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.
- **Filter 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.
- **Eksport ...** – 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**.

4.4.1.1.1 Loggfiler

Loggkonfigurasjonen for ESET NOD32 Antivirus er tilgjengelig fra hovedvinduet for programmet. Klikk **Oppsett** > **Åpne avansert oppsett...** > **Verktøy** > **Loggfiler**. I Logger-delen kan du definere hvordan loggene administreres. Programmet sletter automatisk gamle logger for å spare plass på harddisken. Du kan angi følgende alternativer for loggfiler:

Laveste detaljnivå for logging - Angir det laveste detaljnivået for hendelser som skal logges.

- **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 for eksempel *"Feil ved nedlasting av fil"* og kritiske feil blir registrert.
- **Kritisk** - Logger bare kritiske feil (feil som starter Antivirus-beskyttelse osv...).

Loggoppføringer som er eldre enn antall dager som er spesifisert i feltet **Slett automatisk poster som er eldre enn (dager)**, slettes automatisk.

Optimaliser loggfiler automatisk - Hvis det er merket av for dette, defragmenteres loggfilene automatisk hvis prosentverdien er høyere enn verdien som er spesifisert i feltet **Hvis antall ubrukte oppføringer overskrider (%)**.

Klikk **Optimaliser nå** for å starte defragmenteringen av loggfilene. Alle tomme loggoppføringer fjernes under denne prosessen, slik at ytelsen og hastigheten ved behandling av loggene forbedres. Denne forbedringen ser man særlig hvis loggene inneholder et stort antall oppføringer.

Aktiver tekstprotokoll aktiverer lagring av logger i et alternativt filformat i tillegg til standard loggfiler:

- **Målkatalog** – Katalogen der loggfiler skal lagres (gjelder bare for Tekst/CSV). Hver loggseksjon har en egen fil med et forhåndsdefinert navn (for eksempel *virlog.txt* for **Trusler som er oppdaget** i loggfiler, hvis du lagrer logger med et filformat med ren tekst).

- **Type** – Hvis du velger **Tekst**-filformat, lagres logger i en tekstfil, mens data skilles etter kategorier. Det samme gjelder for det kommaseparerte **CSV**-filformatet. Hvis du velger **Hendelse**, lagres logger i Windows Event-loggen (kan vises ved bruk av Event Viewer i kontrollpanelet) i motsetning til filen.

Slette alle loggfiler – sletter alle lagrede logger som på gjeldende tidspunkt er valgt i rullegardinmenyen **Type**. Det vises en varsling om at loggene ble slettet.

MERKNAD: For å hjelpe med å løse problemer raskere, kan ESET noen ganger be deg om å oppgi logger fra datamaskinen din. ESET Log Collector gjør det enkelt for det å samle sammen informasjonen som trengs. Hvis du vil ha mer informasjon om ESET Log Collector, kan du gå til artikkelen ESET-kunnskapsbase.

4.4.1.1.2 Microsoft NAP

NAP (Network Access Protection) er en Microsoft-teknologi for å kontrollere nettverkstilgang til en datavert basert på vertens systemtilstand. Med NAP kan systemadministratorer i organisasjonens datanettverk definere policyer for krav til systemtilstand.

NAP (Network Access Protection) er laget for å hjelpe administratorer å vedlikeholde helsen til datamaskinene på nettverket. Dette hjelper i sin tur med å vedlikeholde den generelle integriteten til nettverket. Den er ikke laget for å beskytte et nettverk mot ondsinnede brukere. Hvis for eksempel en datamaskin har all(e) programvaren og konfigurasjonene som kreves av policyen for nettverkstilgang, regnes datamaskinen for å være sunn eller godkjent, og vil dermed bli gitt riktig tilgang til nettverket. NAP hinder ikke en uautorisert bruker med en godkjent datamaskin i å laste opp et ondsinnet program til nettverket eller foreta andre former for upassende atferd.

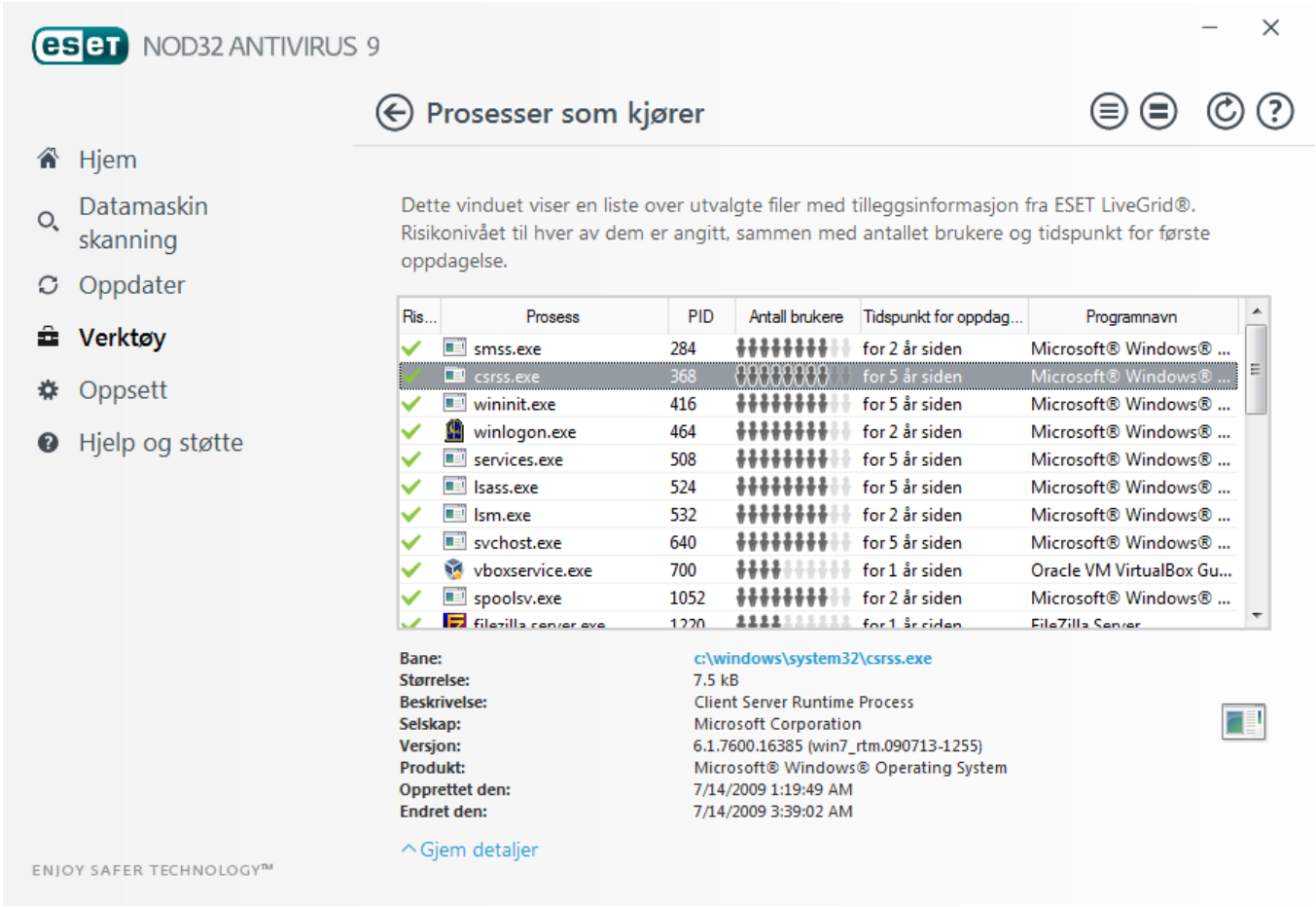
NAP gjør det mulig for administratorer å opprette og fremtvinge helsepolicyer for datamaskiner som er koblet til bedriftsnettverket. Policyene styrer både de installerte programvarekomponentene og systemkonfigurasjonene. Datamaskiner som er koblet til nettverket, slik som bærbare datamaskiner, arbeidsstasjoner eller andre slike enheter evalueres opp mot de konfigurerte helsekravene.

Helsekravene inkluderer:

- Brannmur er aktivert,
- Et virusprogram er installert,
- Virusprogrammet er oppdatert,
- Automatisk Windows Update er aktivert, osv.

4.4.1.2 Prosesser som kjører

Kjørende prosesser viser hvilke programmer eller prosesser som kjører på datamaskinen, og holder ESET umiddelbart og fortløpende informert om nye infiltrasjoner.ESET NOD32 Antivirus gir detaljert informasjon om prosesser som kjører, for å beskytte brukere med ThreatSense-teknologi.



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+Skift+Esc på tastaturet.

Risikonivå – Som regel tilordner ESET NOD32 Antivirus og ThreatSense-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).

MERKNAD: Kjente programmer som er merket som OK (grønt), er avgjort rene (hvitelistet) og vil bli utelatt fra skanning, da dette vil forbedre skannehastigheten til datamaskinskanning etter behov eller beskyttelsen av sanntidsfiler på datamaskinen.

Antall brukere - Antall brukere som bruker et gitt program. Denne informasjonen er samlet inn med ThreatSense-teknologi.

Tidspunkt for oppdagelse - Tidsperioden siden programmet ble oppdaget av ThreatSense-teknologi.

MERKNAD: Når et program er merket som Ukjent (oransje) sikkerhetsnivå, er det ikke nødvendigvis skadelig programvare. Vanligvis er det bare et nytt program. Hvis du ikke er sikker på filen, kan du sende filen til ESETs forskningslaboratorium for analyse. Hvis det viser seg at filen er et skadelig program, blir gjenkjenningen av dette lagt til i en av de kommende oppdateringene.

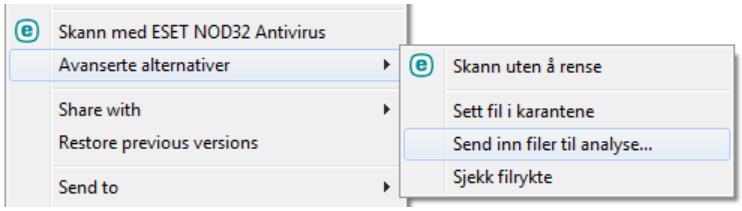
ProgramnavnApplication name - Gitt navn på et program eller en prosess.

Åpne i nytt vindu – Informasjonen om prosessene som kjører, blir åpnet i et nytt vindu.

Klikk på et gitt program nederst for å vise følgende informasjon nederst i vinduet:

- **Fil** - Plasseringen av et program på datamaskinen.
- **Filstørrelse** – Filstørrelse i b (byte).
- **Filbeskrivelse** - Filegenskaper basert på beskrivelsen fra operativsystemet.
- **Firmanavn** - Navn på leverandør eller programprosess.
- **Filversjon** - Informasjon fra utgiveren av programmet.
- **Produktnavn** - Programnavn og/eller forretningsnavn.

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 ThreatSense**.



4.4.1.3 Beskyttelsesstatistikk

Du kan vise en graf med statistiske data knyttet til ESET NOD32 Antiviruss beskyttelsesmoduler ved å klikke **Verktøy** > **Beskyttelsesstatistikk**. Velg ønsket bekyttelsesmodul 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.

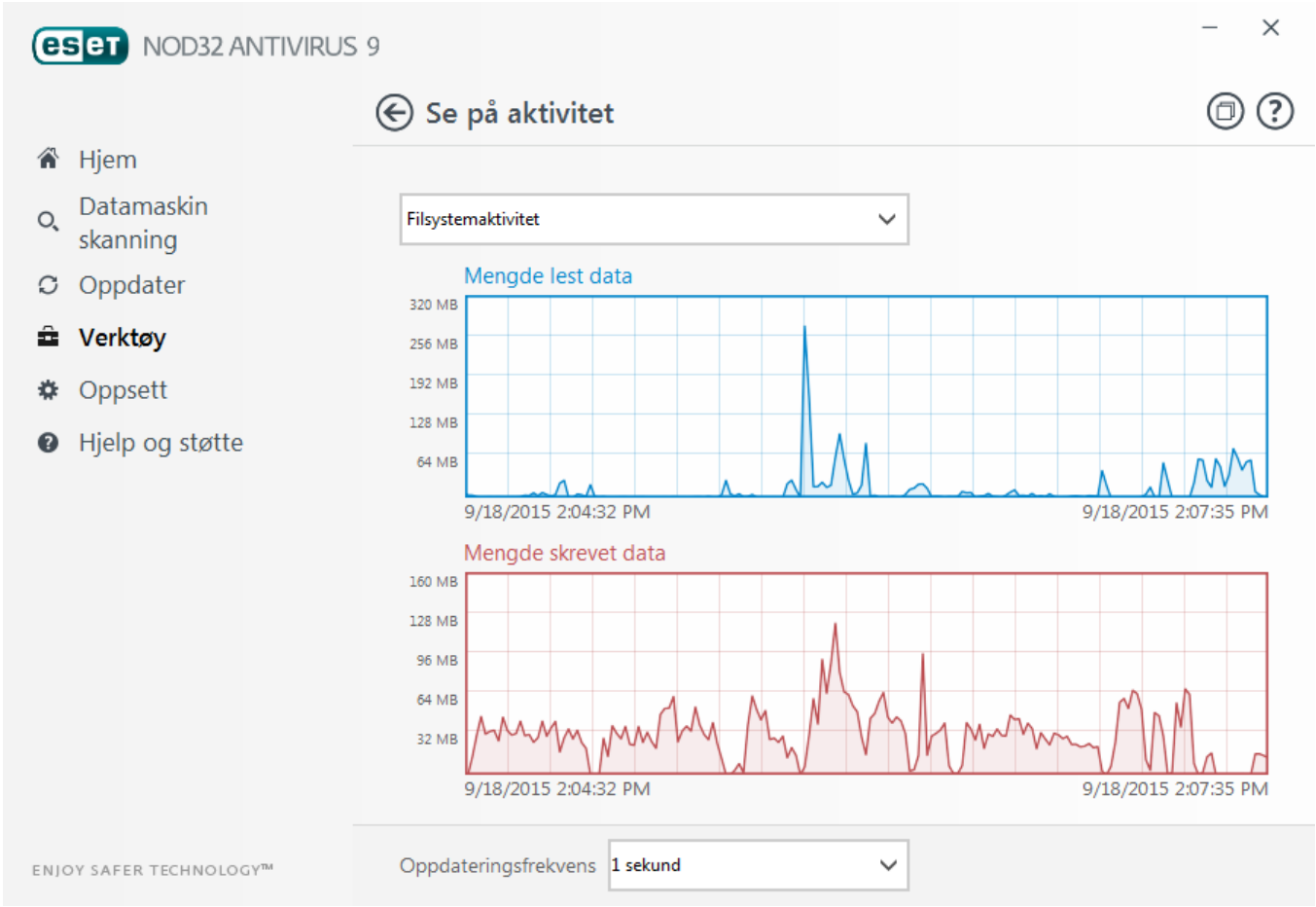
Følgende statistikkgrafer er tilgjengelige:

- **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.

Under statistikkdiagrammene kan du se totalt antall skannede objekter, sist skannet objekt og tidspunktet for statistikken. Klikk **Tilbakestill** for å fjerne all statistikkinformasjon.

4.4.1.4 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 time (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.

4.4.1.5 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*-fil.

4.4.1.6 Planlegger

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

Du går inn i planleggeren fra hovedmenyen for ESET NOD32 Antivirus 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 (klikk **Legg til...** 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**
- **Regelmessig kontroll for nyeste produktversjon** (se Oppdateringsmodus)
- **Automatisk filkontroll ved oppstart** (etter brukerpålogging)
- **Automatisk filkontroll ved oppstart** (etter vellykket oppdatering av virussignaturdatabasen)
- **Automatisk førstegangs skanning**

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 på listen.
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 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.

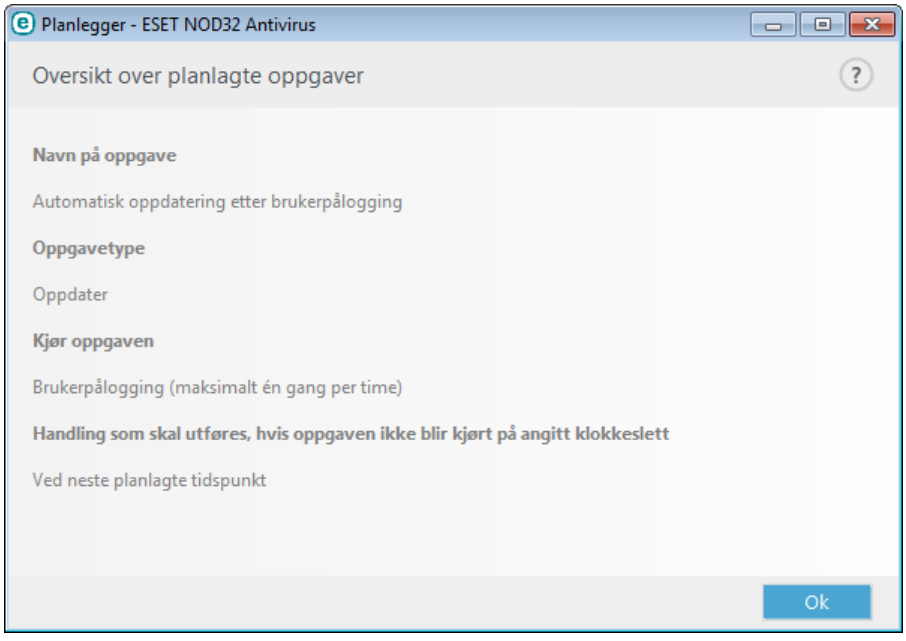
4. Slå på bryteren **Aktivert** hvis du vil aktivere oppgaven (du kan gjøre dette senere ved å merke av / fjerne merket i avkrysningsboksen i listen over planlagte oppgaver), klikk **Neste** og velg et av følgende alternativer:

- **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 kjørt 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:

- **Ved 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**)

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



4.4.1.7 ESET SysRescue

ESET SysRescue er et verktøy som gjør det mulig å opprette en oppstartbar disk som inneholder én av ESET Security-løsningene – ESET NOD32 Antivirus, ESET Smart Security eller visse serverorienterte produkter. Hovedfordelen med ESET SysRescue er at ESET Security-løsningen kjøres uavhengig av vertsoperativsystemet med direkte tilgang til disken og filsystemet. Det er derfor mulig å fjerne infiltrasjoner som ellers ikke ville være mulige å slette, f.eks. når operativsystemet kjører osv.

4.4.1.8 ESET LiveGrid®

ESET LiveGrid® (bygget på ESET sitt ThreatSense.Net avanserte varslingssystem) bruker data som ESET-brukere har sendt inn fra over hele verden og sender den til ESET forskningslaboratorium. Ved å gi mistenkelige prøver og metadata fra naturen, lar ESET LiveGrid® oss reagere umiddelbart på behovene til kundene våre og gjør at ESET kan reagere på de siste truslene. Les mer om ESET LiveGrid® i glossar.

Brukeren kan sjekke omdømmet til aktive prosesser og filer direkte fra programmets grensesnitt eller fra kontekstmenyen, og få tilleggsinformasjon fra ESET LiveGrid®. Du har to alternativer:

1. Du kan velge ikke å aktivere ESET LiveGrid®. Du vil ikke miste noe av funksjonaliteten i programvaren, men ESET NOD32 Antivirus kan i enkelte tilfeller reagere raskere på nye trusler enn oppdateringen av virussignaturdatabasen når ESET Live Grid er aktivert.
2. Du kan konfigurere ESET LiveGrid® 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 LiveGrid® 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.

Som standard er ESET NOD32 Antivirus konfigurert til å sende inn mistenkelige filer til ESETs trussellaboratorium 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 LiveGrid®s oppsettmeny har flere alternativer for å aktivere/deaktivere ESET LiveGrid®, som styrer innsendingen av mistenkelige filer og anonym statistikk til ESETs laboratorier. Det er tilgjengelig fra treet for avansert oppsett, under **Verktøy** > **ESET LiveGrid®**.

Aktiver ESET LiveGrid® omdømmesystem (anbefalt) – ESET LiveGrid® 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 LiveGrid® 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.

4.4.1.8.1 Mistenkelige filer

Kategorien **Filer** i avansert oppsett for ESET LiveGrid® gjør det mulig å konfigurere hvordan trusler sendes til analyse ved ESETs forskningslaboratorium.

Hvis du finner en mistenkelig fil, kan du sende den inn til ESETs forskningslaboratorium. Hvis det er et skadelig program, blir gjenkjenningen av programmet lagt til i neste virussignaturoppdatering.

Utelatelsesfilter - Med utelatelsesfilteret kan du utelate enkelte filer og mapper fra innsending. Filer som finnes her, blir aldri sendt til ESETs forskningslaboratorium for analyse, selv om de inneholder mistenkelig kode. Det kan for eksempel være nyttig å utelate filer som kan inneholde konfidensiell informasjon, som dokumenter og regneark. De vanligste filtypene er utelatt som standard (.doc, osv.). Du kan legge til flere filer i listen over utelatte filer hvis du ønsker det.

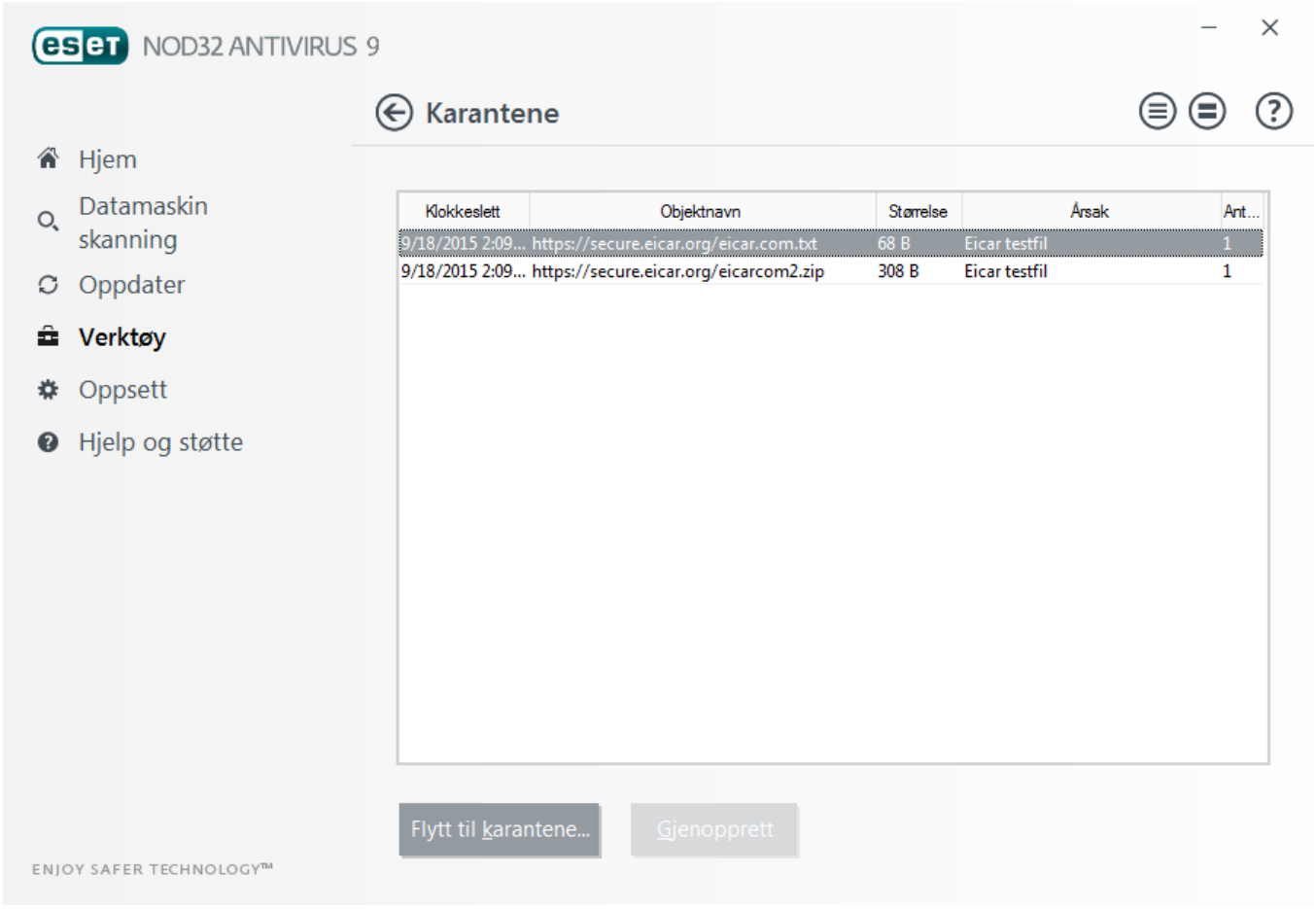
E-postadresse for kontakt (valgfritt) - E-postadressen din kan bli inkludert i mistenkelige filer, og kan brukes til å ta kontakt med deg hvis det trengs mer informasjon for analysen. Vær oppmerksom på at du ikke vil få svar fra ESET med mindre det er behov for flere opplysninger.

Velg **Aktiver logging** hvis du vil opprette en hendelseslogg som registrerer innsending av filer og statistisk informasjon. Dette aktiverer logging tilHendelsesloggen ved sending av filer og statistikk.

4.4.1.9 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 NOD32 Antivirus.

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 forskningslaboratorium 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 NOD32 Antivirus setter 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...**. Hvis dette gjøres, blir ikke den opprinnelige filen 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. Bruk funksjonen **Gjenopprett** til dette formålet. Funksjonen er tilgjengelig fra hurtigmenyen ved å høyreklikke en gitt fil i vinduet Karantene. Hvis en fil er merket som potensielt uønskede programmer, blir alternativet **Gjenopprett og utelat fra skanning** aktivert. Du kan lese mer om denne programtypen i ordlisten. Hurtigmenyen har også alternativet **Gjenopprett til...**, som lar deg gjenopprette en fil til en annen plassering enn den filen ble slettet fra.

MERKNAD: Hvis programmet ved en feiltakelse setter 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 infisert (for eksempel ved heuristisk analyse av koden) 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.

4.4.1.10 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 NOD32 Antivirus 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 NOD32 Antivirus. 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.

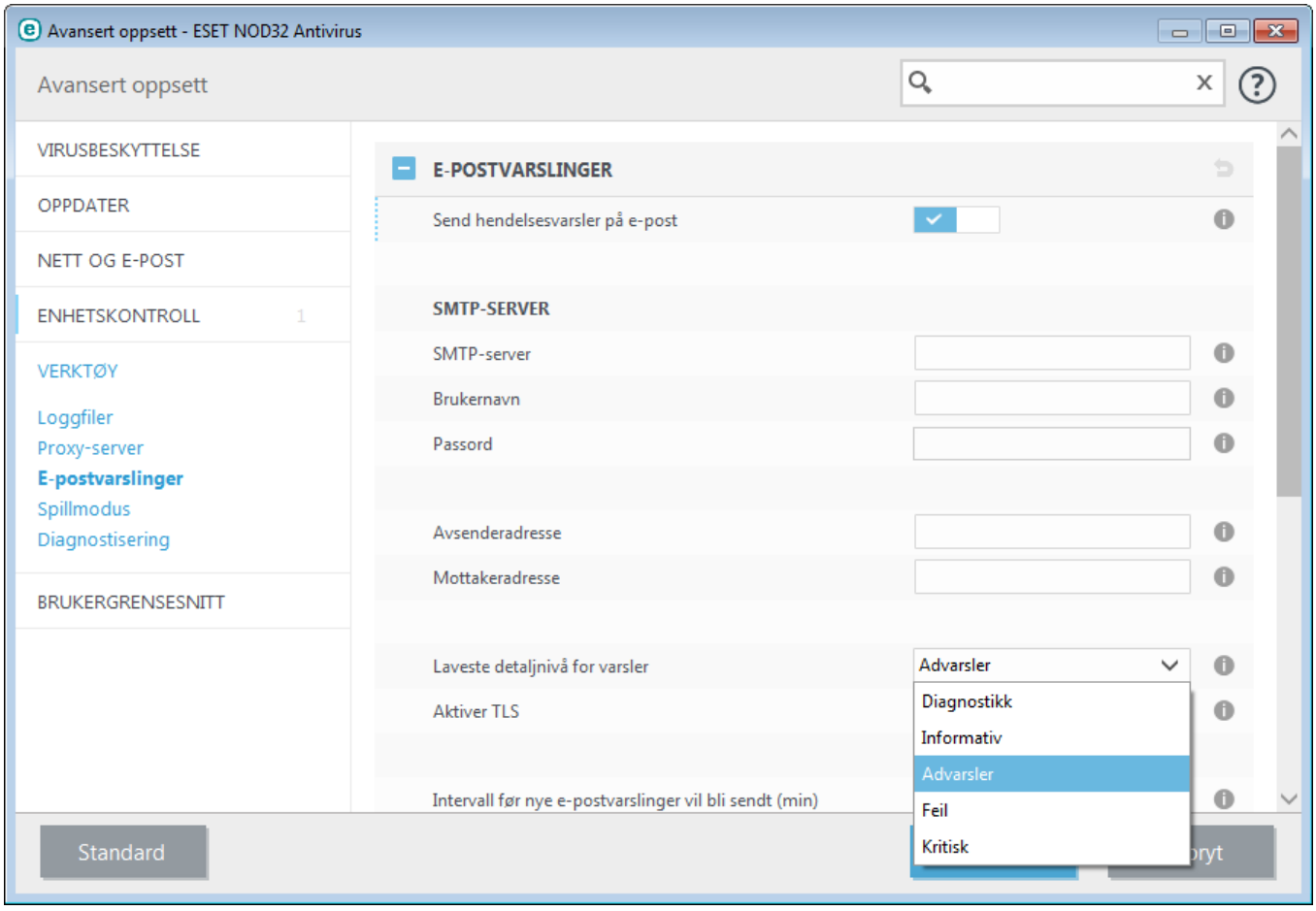
Hvis kommunikasjon med proxy-serveren krever godkjenning, velger du avmerkingsboksen **Proxy-serveren krever godkjenning** og skriver inn gyldig **Brukernavn** og **Passord** i de respektive feltene. Klikk **Gjenkjenn** hvis du vil gjenkjenne og sette inn proxy-serverinnstillingene automatisk. Parametrene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

MERK: 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.

4.4.1.11 E-postvarslinger

ESET NOD32 Antivirus kan automatisk sende e-postvarslinger hvis en hendelse med det valgte detaljnivået oppstår. Aktiver **Send hendelsesvarsler på e-post** for å aktivere varslinger.



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 NOD32 Antivirus.

Brukernavn og **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 avsenderadressen som blir vist i 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 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).

4.4.1.11.1 Meldingsformat

Her kan du sette opp formatet på hendelsesmeldinger som vises på eksterne datamaskiner.

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.

Nøkkelord (strenger skilt med %-tegn) blir i meldingen erstattet med den faktiske informasjonen. Følgende nøkkelord kan brukes:

- **%TimeStamp%** – dato og klokkeslett for hendelsen
- **%Scanner%** – den aktuelle modulen
- **%ComputerName%** – navnet på datamaskinen der varselet oppstod
- **%ProgramName%** – programmet som genererte varselet
- **%InfectedObject%** – navn på infisert fil, melding, osv.
- **%VirusName%** – identifikasjon av infeksjonen
- **%ErrorDescription%** – beskrivelse av en hendelse som ikke er virusrelatert

Nøkkelordene **%InfectedObject%** og **%VirusName%** brukes bare i trusseladvarselsmeldinger, og **%ErrorDescription %** brukes bare i hendelsesmeldinger.

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).

4.4.1.12 Velg prøve for analyse

Med dialogboksen for innsending av filer kan du sende en fil eller et område til analyse hos ESET. Du finner den under **Verktøy** > **Send inn stikkprøve til analyse**. Hvis du finner en fil på maskinen eller et nettsted som oppfører seg mistenkelig, kan du sende den inn til ESETs forskningslaboratorium 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 fil til ESET, må du kontrollere at den oppfyller ett eller flere av følgende kriterier:
- filen 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.

4.4.1.13 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 NOD32 Antivirus 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.

4.5 Brukergrensesnitt

I delen **Brukergrensesnitt** kan du konfigurere atferden til programmets grafiske brukergrensesnitt (GUI).

Med Grafikk-verktøyet kan du justere programmets utseende og effektene som brukes.

Ved å konfigurere Varsler og meldinger kan du endre atferden til trusselvarsler og systemmeldinger. Disse kan konfigureres etter behov.

Hvis du velger å ikke vise enkelte meldinger, vises de i delen Skjulte meldingsvinduer. Her kan du kontrollere statusen til meldingene, se mer informasjon om dem eller fjerne dem fra vinduet.

For at sikkerhetsprogramvaren skal kunne levere maksimal sikkerhet, kan du forhindre uautoriserte endringer ved å beskytte innstillingene med et passord ved hjelp av verktøyet Oppsett av tilgang.

Hurtigmenyen vises når et objekt høyreklikkes. Bruk dette verktøyet til å integrere kontrollelementene i ESET NOD32 Antivirus med hurtigmenyen.

4.5.1 Brukergrensesnittelementer

Alternativene for konfigurasjon av brukergrensesnittet i ESET NOD32 Antivirus 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 NOD32 Antivirus.

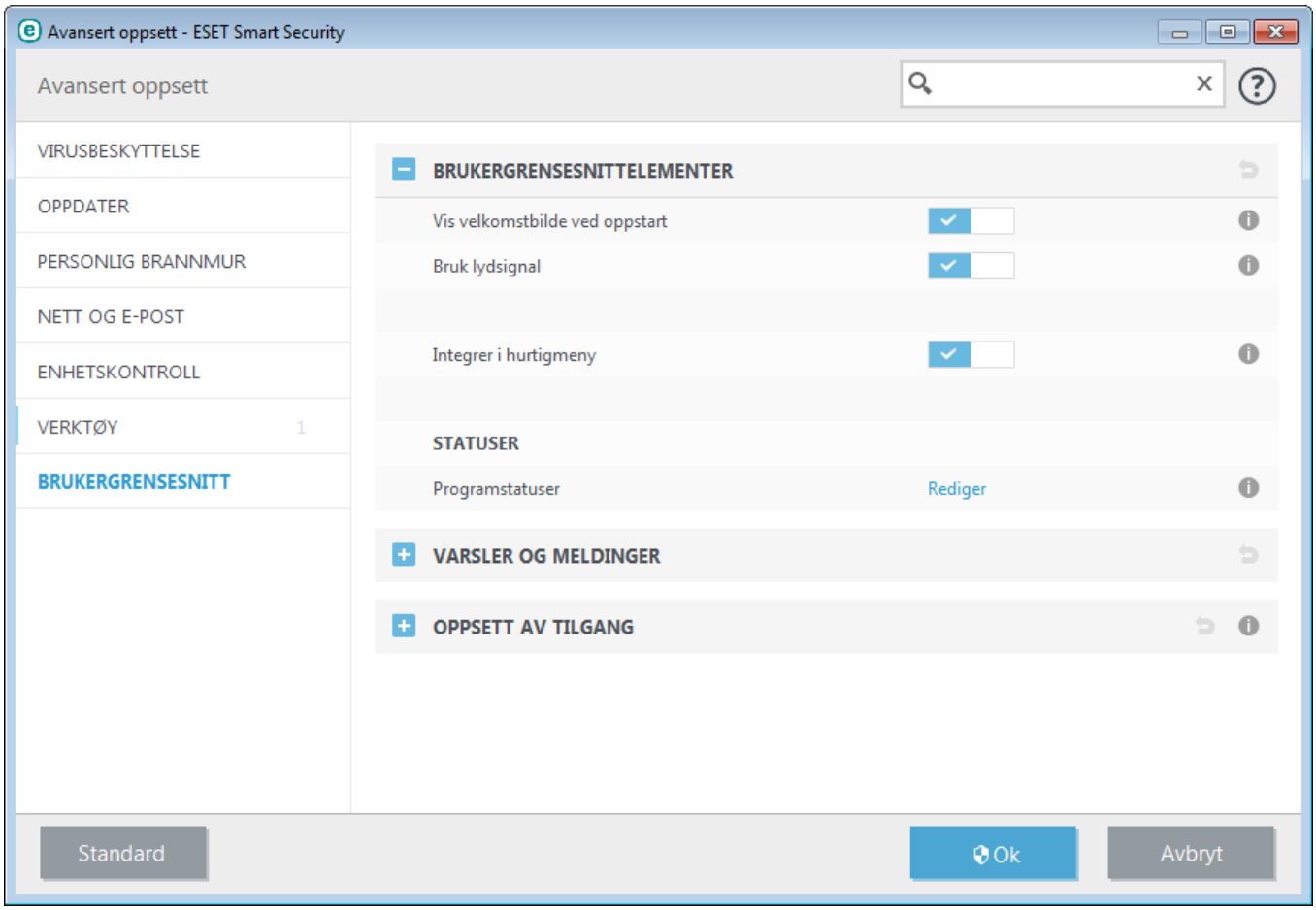
Hvis du vil deaktivere velkomstbildet i ESET NOD32 Antivirus, fjerner du avmerkingen ved **Vis velkomstbilde ved oppstart** .

For at ESET NOD32 Antivirus 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 NOD32 Antivirus med hurtigmenyen.

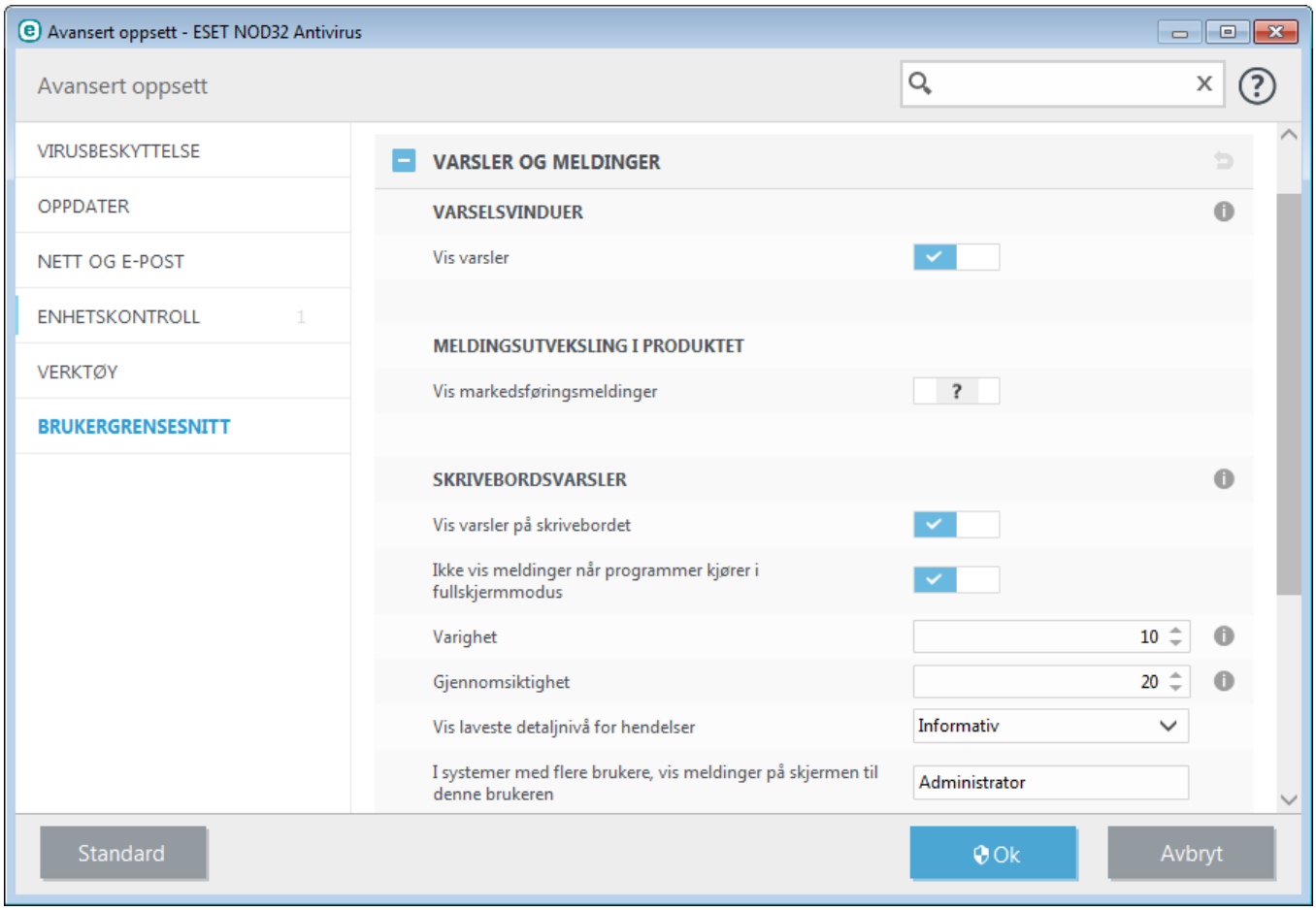
Statuser

Programstatuser – Klikk **Rediger**-knappen for å administrere (deaktivere) statuser i **Beskyttelsesstatus**-panelet i hovedmenyen.


Avansert oppsett - ESET Smart Security
Avansert oppsett
VIRUSBESKYTTELSE
OPPDATER
PERSONLIG BRANNMUR
NETT OG E-POST
ENHETSKONTROLL
VERKTØY
BRUKERGRENSESNITT
BRUKERGRENSESNITTELEMENTER
Vis velkomstbilde ved oppstart
Bruk lydsignal
Integrer i hurtigmeny
STATUSER
Programstatuser
Rediger
VARSLER OG MELDINGER
OPPSETT AV TILGANG
Standard
Ok
Avbryt

4.5.2 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 NOD32 Antivirus. Du kan også angi visningstiden og gjennomsiktigheten til systemmeldinger (dette gjelder bare systemer som støtter systemmeldinger).



Varselsvinduer

Hvis du deaktivererer**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).

Meldingsutveksling i produktet

Vis markedsføringsmeldinger – Meldingsutveksling i produktet har blitt utviklet for å informere brukere om ESET-nyheter og annen kommunikasjon. Deaktiver dette alternativet hvis du ikke ønsker å motta markedsføringsmeldinger.

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**.

Aktiver **Ikke vis meldinger når programmer kjører i fullskjermmodus** hvis du vil blokkere alle 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 virusbeskyttelseosv...).

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.

4.5.2.1 Avansert oppsett

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.
- **Informative** - registrerer informative meldinger, inkludert vellykkede oppdateringsmeldinger, pluss alle registreringene ovenfor.
- **Advarsler** - logger alle kritiske feil og varselsmeldinger.
- **Feil** - Feil som for eksempel *"Feil ved nedlasting av fil"* og kritiske feil blir registrert.
- **Kritisk** - Logger bare kritiske feil (feil som starter Antivirus-beskyttelse 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 en bruker som skal motta systemmeldinger og andre meldinger, 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.

4.5.3 Skjulte meldingsvinduer

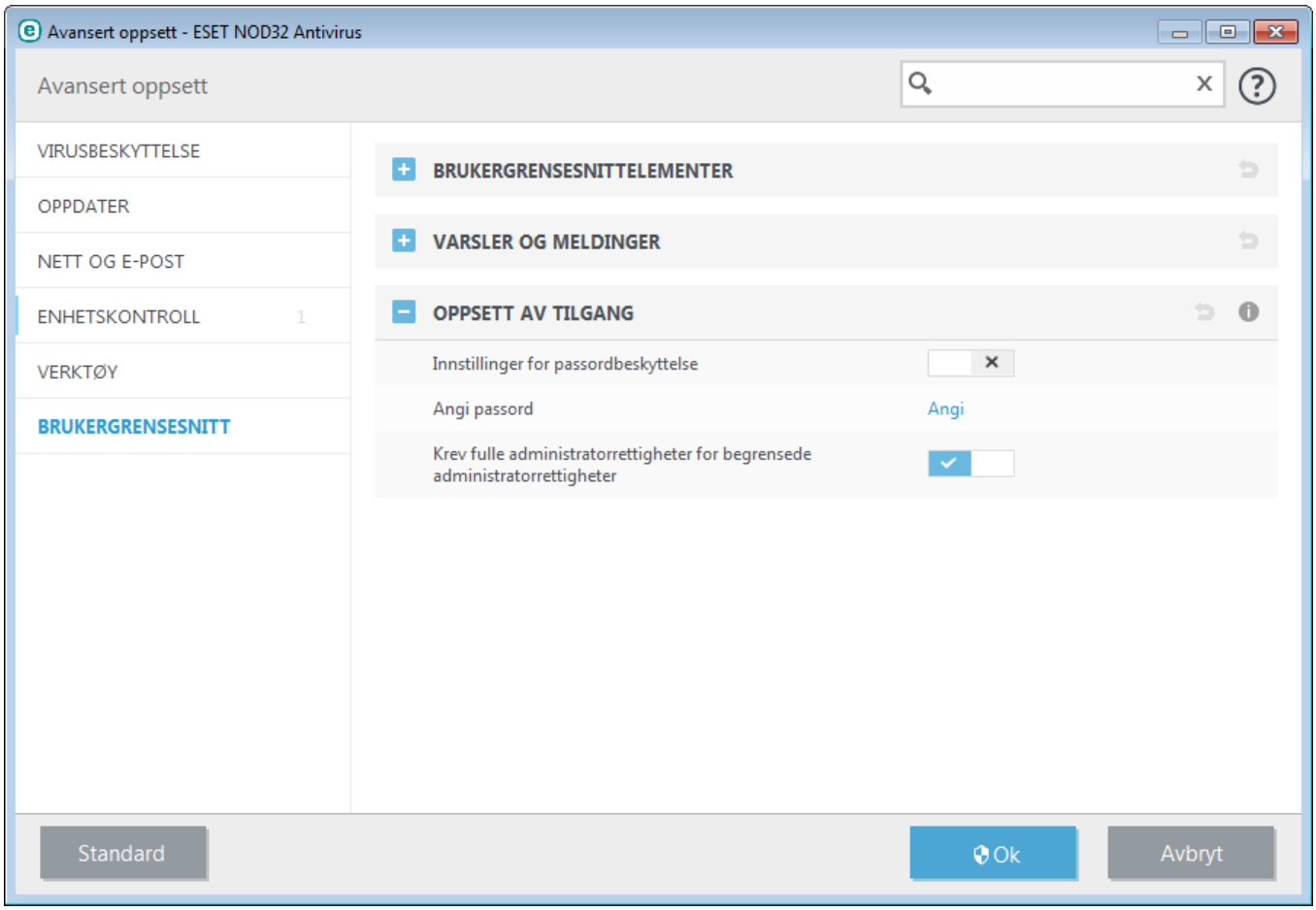
Hvis **Ikke vis denne meldingen igjen** velges for et meldingsvindu (varsel) som tidligere ble vist, vil det havne på listen over skjulte meldingsvinduer. Handlinger som nå utføres automatisk, vises i kolonnen **Bekreft**.

Vis - Viser en forhåndsvisning av meldingsvinduer som inntil videre ikke vises, og som det er konfigurert automatiske handlinger for.

Fjern - Fjerner elementer fra listen **Skjulte meldingsbokser**. Alle meldingsvinduer som fjernes fra listen, vil bli vist igjen.

4.5.4 Oppsett av tilgang

Innstillingene for ESET NOD32 Antivirus er en fundamental del av sikkerheten for systemet ditt. Uautoriserte endringer kan potensielt sette systemets stabilitet og beskyttelse i fare. For å unngå uautorisert endring, kan parameterne for oppsett av ESET NOD32 Antivirus passordbeskyttes.



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.

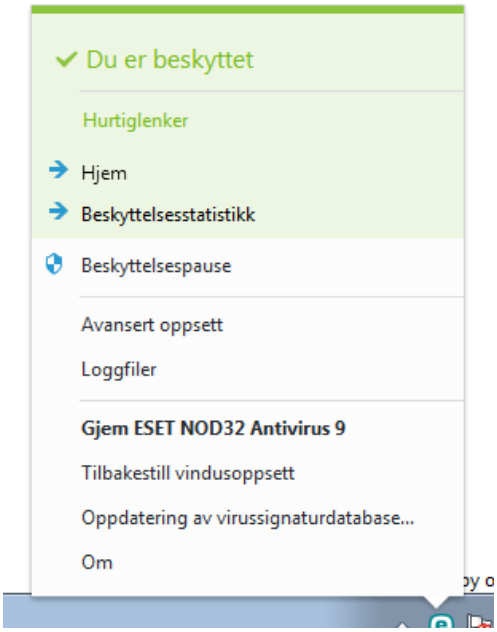
Krev fulle administratorrettigheter for begrensede administratorrettigheter – Velg dette alternativet for å be gjeldende bruker (hvis han/hun ikke har administratorrettigheter) om å skrive inn brukernavn og passord for administrator når de endrer bestemte systemparametre (ligner brukerkontokontroll (UAC) i Windows Vista og Windows 7). Slike endringer inkluderer det å deaktivere beskyttelsesmoduler. På Windows XP-systemer hvor UAC ikke kjører vil brukere ha alternativet **Krev administratorrettigheter (system uten UAC-støtte)** tilgjengelig.

Kun for Windows XP:

Krev administratorrettigheter (system uten UAC-støtte) – Aktiver dette alternativet for at ESET NOD32 Antivirus skal be om administratorinformasjon.

4.5.5 Programmeny

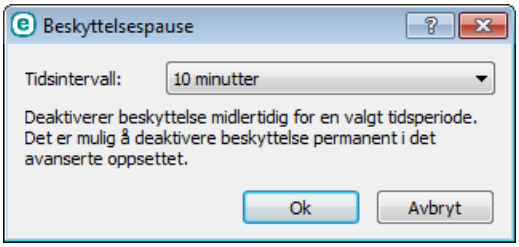
Du får tilgang til noen av de viktigste oppsettsalternativene og funksjonene ved å høyreklikke ikonet i statusfeltet .



Hurtiglenker – viser de mest brukte delene av ESET NOD32 Antivirus. Du kan få rask tilgang til disse fra programmenyen.

Beskyttelsespause – Viser bekreftelsesdialogboksen som deaktiverer Virus- og spywarebeskyttelse, som beskytter mot skadelige systemangrep ved å kontrollere filer, Internett- og e-postkommunikasjon.

Rullegardinmenyen **Tidsintervall** representerer tidsperioden når all spambeskyttelse vil være deaktivert.



Avansert oppsett – Velg dette alternativet for å vise treet **Avansert oppsett**. Du kan også åpne Avansert oppsett på andre måter: ved å trykke på F5 eller navigere til **Oppsett** > **Avansert oppsett**.

Loggfiler - Loggfiler inneholder informasjon om viktige programhendelser som har inntruffet, og gir en oversikt over trusler som er oppdaget.

Skjul ESET NOD32 Antivirus – Skjuler ESET NOD32 Antivirus-vinduet fra skjermen.

Tilbakestill vindusoppsett - Tilbakestiller vinduet til ESET NOD32 Antivirus til standardstørrelsen og -plasseringen på skjermbildet.

Aktiver produktet ditt... - Velg dette alternativet hvis du enda ikke har aktivert ESET-sikkerhetsproduktet ditt eller for å oppgi produktaktiveringsinformasjonen på nytt etter å ha fornyet lisensen.

Oppdatering av virussignaturdatabase – Starter oppdateringen av virussignaturdatabasen for å sikre beskyttelsesnivået mot skadelig kode.

Om - Gir systeminformasjon, detaljer om den installerte versjonen av ESET NOD32 Antivirus og de installerte systemkomponentene. Her kan du også se lisensens utløpsdato og informasjon om operativsystemet og systemressurser.

4.5.6 Hurtigmeny

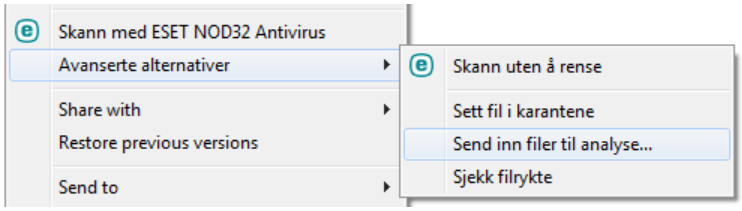
Hurtigmenyen vises når et objekt høyreklikkes. Menyen inneholder alle handlinger som kan utføres på et objekt.

Det er mulig å integrere kontrollelementene i ESET NOD32 Antivirus med hurtigmenyen. Du finner mer informasjon om oppsettalternativene for denne funksjonaliteten i treet for avansert oppsett i delene **Brukergrensesnitt** og **Hurtigmeny**.

Integrer i hurtigmeny – Integrerer kontrollelementene i ESET NOD32 Antivirus med hurtigmenyen.

Følgende alternativer er tilgjengelige i rullegardinmenyen **Menytype**:

- **Full (skann først)** – Aktiverer alle hurtigmenyvalgene; hovedmenyen vil vise **Skann uten rensing medESET NOD32 Antivirus** som det første valget og **Skann og rens** som andre nivås elementet.
- **Full (rens først)** - Aktiverer alle hurtigmenyvalgene; hovedmenyen vil vise **Skann med ESET NOD32 Antivirus** som det første valget og **Skann uten rensing** som andre nivås elementet.



- **Kun skann** - Kun **Skann uten rensing med ESET NOD32 Antivirus** vil vises i hurtigmenyen.
- **Kun opprydding** - Kun **Skann med ESET NOD32 Antivirus** vil vises i hurtigmenyen.

5. Erfaren bruker

5.1 Profilbehandling

Profilbehandling brukes på to steder i ESET NOD32 Antivirus – i avsnittet **Datamaskinskanning ved forespørsel** og i avsnittet **Oppdater**.

Datamaskinskanning

Du kan lagre dine foretrukne skanneparametre for skanning på 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.

Du oppretter en ny profil ved å åpne vinduet Avansert oppsett (F5) og klikke **Antivirus** > **Datamaskinskanning etter behov** >**Grunnleggende**> **Liste over profiler**. Vinduet **Profilbehandling** inneholder rullegardinmenyen **Valgt profil**, som viser eksisterende skanneprofiler og et alternativ for å opprette en ny. Hvis du vil ha hjelp til å opprette en skanneprofil som er tilpasset ditt behov, kan du se en beskrivelse av hver av parameterne i skanneoppsettet i avsnittet Oppsett av parametere for ThreatSense-motor.

Eksempel: Sett at du vil opprette din egen skanneprofil og konfigurasjonen av **Skann datamaskinen din** 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.

Legg til... - Oppretter nye oppdateringsprofiler.

Den nedre delen av vinduet viser en liste over eksisterende profiler.

5.2 Hurtigtaster

Følgende hurtigtaster kan brukes til å forenkle navigasjonen i ESET-sikkerhetsproduktet:

F1	åpner hjelpesider
F5	åpner Avansert oppsett
Opp/ned	navigasjon i produkter gjennom elementer
-	skjuler trenodene Avansert oppsett
TAB	flytter markøren i et vindu
Esc	lukker det aktive dialogvinduet

5.3 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 NOD32 Antivirus. Klikk rullegardinmenyen ved siden av **Dumptype** og velg et av følgende alternativer:

- Velg **Deaktiver** (standard) for å deaktivere funksjonen.
- **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 programmet 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 tidligere 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.

5.4 Importer og eksporter innstillinger

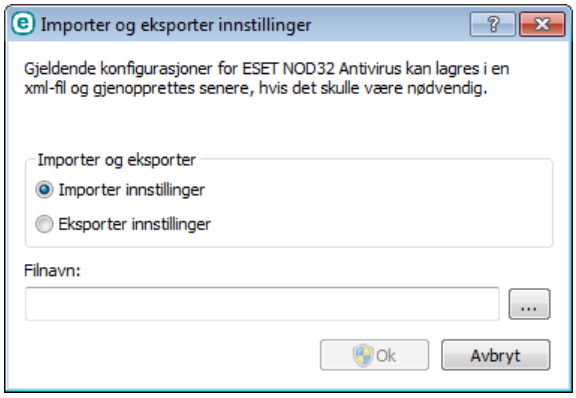
Du kan importere eller eksportere en tilpasset .xml-konfigurasjonsfil for ESET NOD32 Antivirus fra menyen **Oppsett**.

Import og eksport av konfigurasjonsfiler er nyttig hvis du må sikkerhetskopiere den gjeldende konfigurasjonen til ESET NOD32 Antivirus 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 programmets hovedvindu klikker du **Oppsett** > **Importer og 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 programmets hovedvindu klikker du **Oppsett** > **Importer og 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.



5.5 Gjenkjenning av inaktiv tilstand

Innstillingene for gjenkjenning av inaktiv tilstand konfigureres i **Avansert oppsett** under **Verktøy** > **Gjenkjenning av inaktiv tilstand**. Disse innstillingene definerer en utløser for Inaktivitetsskanning når:

- skjermspareren kjører,
- datamaskinen er låst,
- en bruker logger seg av.

Bruk avmerkingsboksene for hver enkelt tilstand for å aktivere eller deaktivere utløserne for gjenkjenning av inaktiv tilstand.

5.6 ESET SysInspector

5.6.1 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 NOD32 Antivirus.

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.

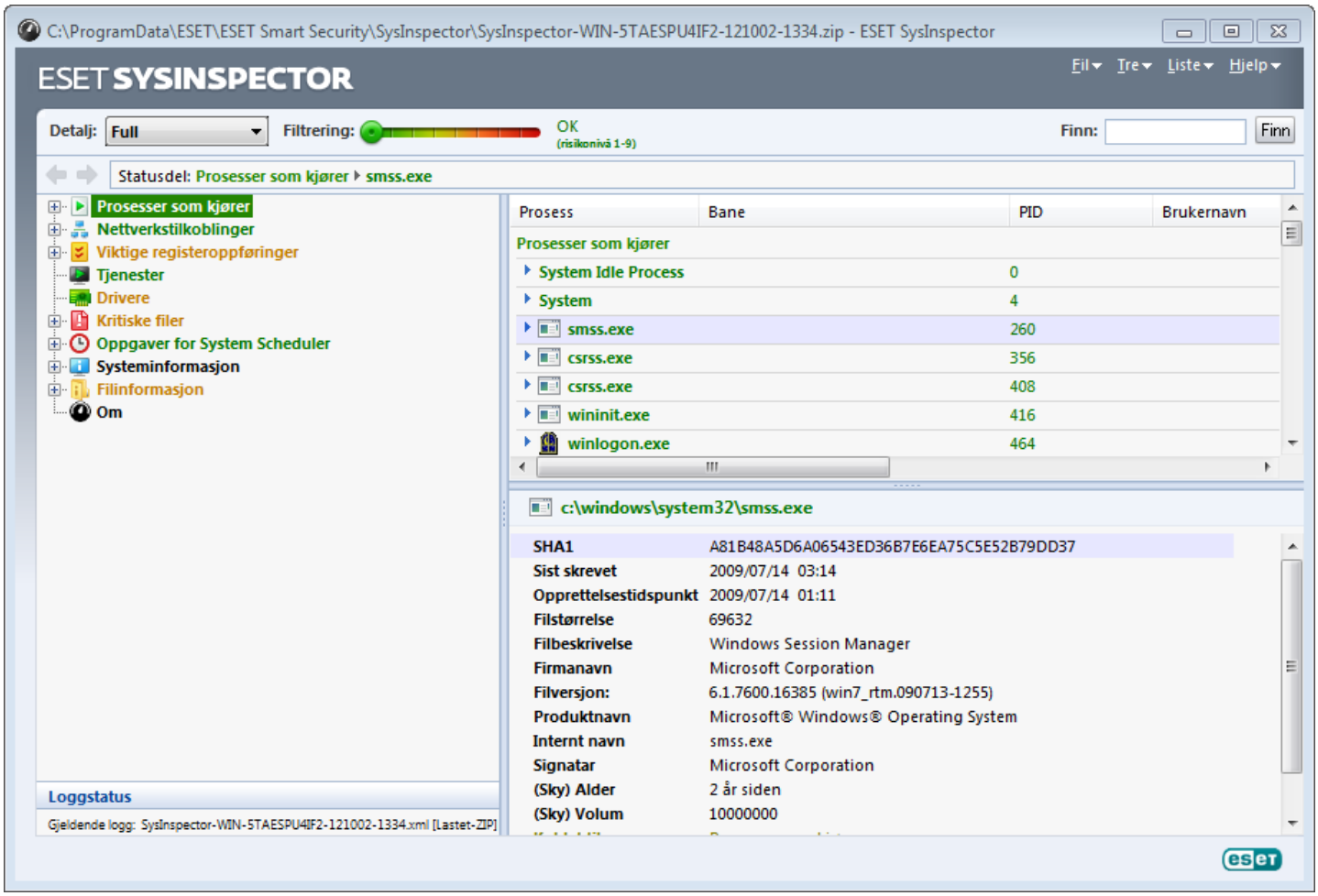
5.6.1.1 Starter ESET SysInspector

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 NOD32 Antivirus**).

Vent mens programmet inspiserer systemet ditt. Dette kan ta opptil flere minutter.

5.6.2 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.).



5.6.2.1 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.

5.6.2.2 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.

5.6.2.2.1 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

5.6.2.3 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.

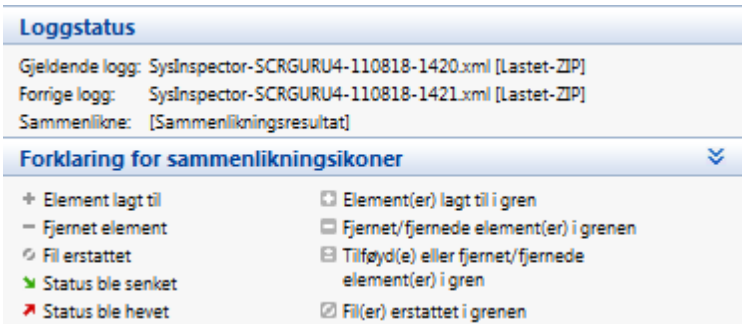
MERKNAD: Du sammenligner to loggfiler ved å klikke **Fil** > **Lagre logg** for å lagre som en ZIP-fil. Begge filene blir da lagret. Hvis du åpner denne filen senere, sammenliknes automatisk loggene den inneholder.

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

5.6.3 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).

5.6.4 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.

5.6.4.1 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.

5.6.4.2 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.

10) Planlagt oppgaver

Denne delen inneholder informasjon om planlagte oppgaver.

Eksempel:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.6.4.3 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.

5.6.5 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.

Eksempel:

Windows 2000 inkluderer HyperTerminal-programmet plassert i *C:\Program Files\Windows NT*. Den kjørbare hovedfilen i programmet er ikke digitalt signert, men ESET SysInspector merker den som en fil signert av Microsoft. Grunnen til dette er en referanse i *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* som peker på *C:\Program Files\Windows NT\hypertrm.exe* (den kjørbare hovedfilen i HyperTerminal-programmet) og *sp4.cat* er digitalt signert av Microsoft.

5.6.6 ESET SysInspector som en del av ESET NOD32 Antivirus

Når du vil åpne ESET SysInspector-delen i ESET NOD32 Antivirus, 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).

5.7 Kommandolinje

Antivirusmodulen til ESET NOD32 Antivirus 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.

6. Ordliste

6.1 Typer infiltreringer

En infiltrering er skadelig programvare som prøver å få tilgang til og/eller skade brukerens datamaskin.

6.1.1 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 forskningslaboratorium 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.

6.1.2 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.

6.1.3 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.

6.1.4 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 NOD32 Antivirus brukere har fordelen med Anti-Stealth-teknologien som også kan oppdage og fjerne aktive rootkits.

6.1.5 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.

6.1.6 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.

6.1.7 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.

6.1.8 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 NOD32 Antivirus 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.

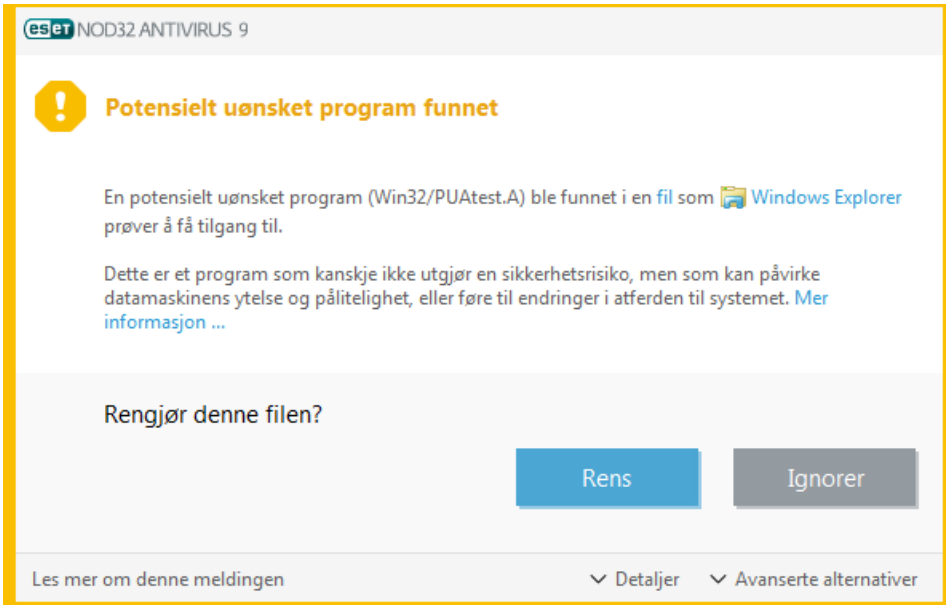
6.1.9 Potensielt uønskede programmer

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.

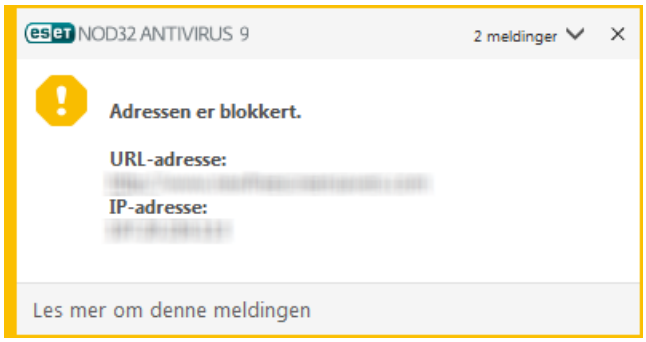
Advarsel – Potensiell trussel funnet

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. **Ignorer**: 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 **Avanserte alternativer** og velg avkrysningsboksen ved siden av **Ekskluder fra gjenkjenning**.

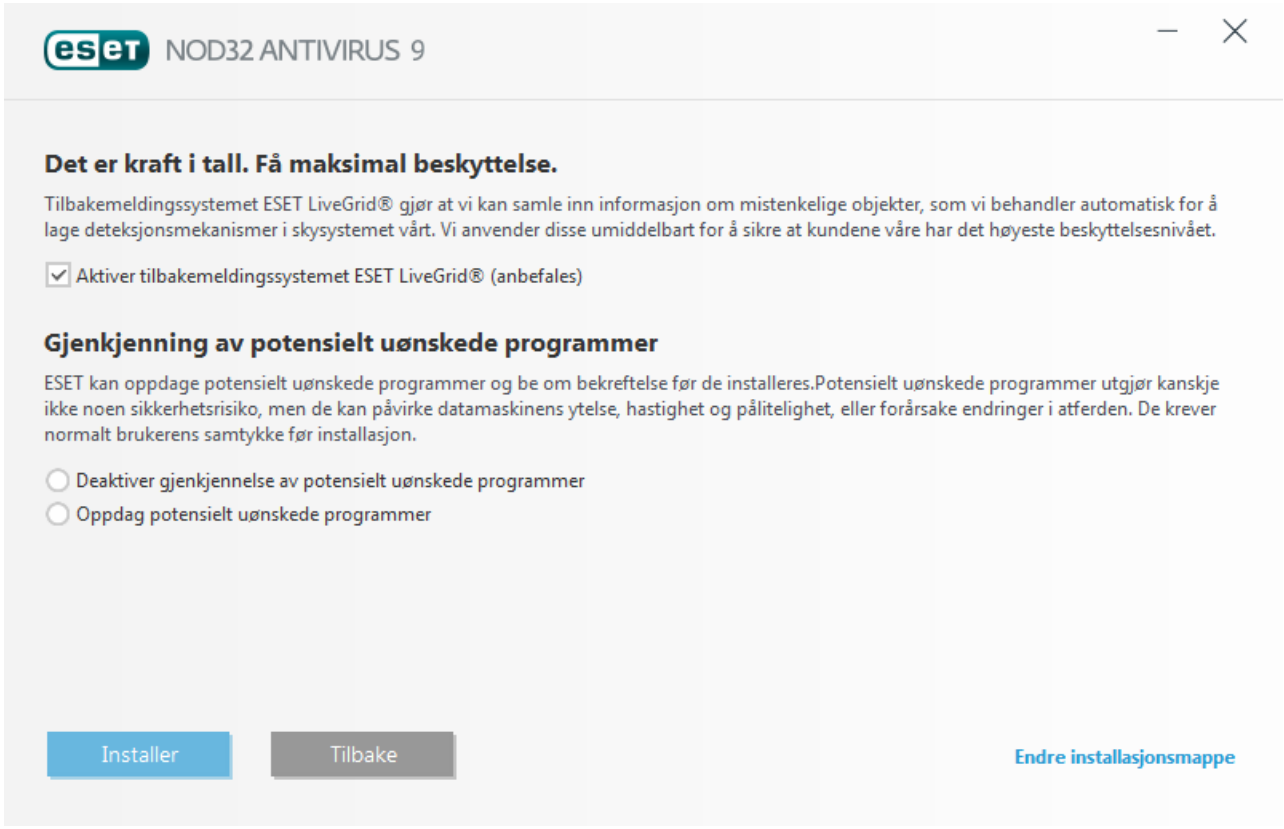


Når et potensielt uønsket program gjenkjennes og det ikke kan rengjøres, vises det et meldingsvindu **Adresse har blitt blokkert** i meldingsområdet nederst til høyre på skjermen. For mer informasjon om denne hendelsen, gå til **Verktøy Loggfiler** > **Filtrerte nettsteder** på hovedmenyen.



Potensielt uønskede programmer – Innstillinger

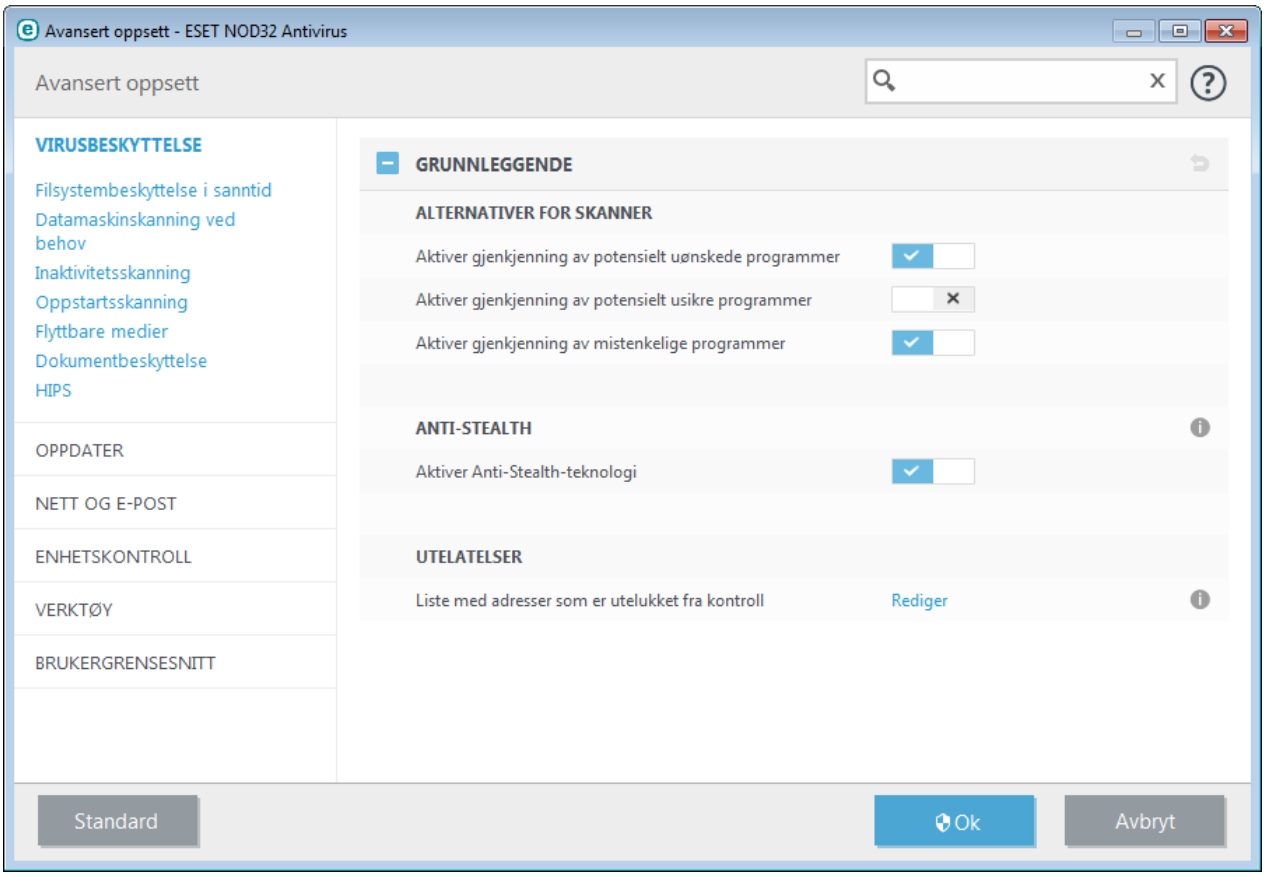
Når du installerer ESET-produktet ditt, kan du velge om du vil aktivere gjenkjenning av potensielt uønskede programmer, som vist nedenfor:



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.

6.2 ESET-teknologi

6.2.1 Blokkering av utnyttelse

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. Den fungerer ved å overvåke oppførselen til prosesser og se etter mistenkelig aktivitet som kan indikere en utnyttelse.

Når Blokkering av utnyttelse identifiserer en mistenkelig prosess, kan den stoppe prosessen umiddelbart og registrere data om trusselen, som deretter sendes til ThreatSense skysystemet. Denne informasjonen behandles av ESETs forskningslaboratorium 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).

6.2.2 Avansert minneskanner

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 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 blokkering av utnyttelse, er den avanserte minneskanneren 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, men i tilfeller der andre oppdagelsesteknikker mislykkes gir den et ekstra lag av sikkerhet.

6.2.3 ESET LiveGrid®

Bygget på ThreatSense.Net® sitt avanserte varslingssystem – ESET LiveGrid® 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 LiveGrid® 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 LiveGrid®-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 der 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 brukerens datamaskin via oppdatert virusdatabase (som skjer flere ganger om dagen).

6.2.4 Java blokkering av utnyttelse

Java blokkering av utnyttelse er en utvidelse av den eksisterende beskyttelsen 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 dem på andre lag (URL-blokkering, filnedlasting, osv.).

6.3 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

6.3.1 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.

6.3.2 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.

6.3.3 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.

6.3.4 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.

7. 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 NOD32 Antivirus
Fjerne virus fra PC-en
Hvordan opprette en ny oppgave i Planlegger
Planlegge en skanningsoppgave (hver 24.time)

Prøv å søke på hjelpesidene til ESET NOD32 Antivirus hvis problemet ikke finnes i oversikten over hjelpesider ovenfor.

Hvis du ikke finner løsningen på problemet/spørsmålet ditt på hjelpsidene, kan du prøve vår jevnlig oppdaterte ESET-kunnskapsdatabase på Internett. Koblinger til vår mest populære kunnskapsbaseartikler er tatt med nedenfor. De hjelper deg med å løse vanlige problemer:

Jeg mottok en aktiveringsfeilmelding da jeg installerte ESET-produktet mitt. Hva betyr det?
Hvordan angir jeg brukernavn og passord i ESET Smart Security/ESET NOD32 Antivirus?
Jeg mottar melding om at ESET-installasjonen ble avsluttet for tidlig
Hva må jeg gjøre når jeg har fornyet lisensen? (Hjemmebrukere)
Hva skjer hvis jeg endrer e-postadresse?
Slik startes Windows i Sikkermodus eller Sikkermodus med nettverk

Du kan om nødvendig kontakte brukerstøtte med spørsmål eller problemer. Kontaktskjemaet finner du i fanen **Hjelp og støtte** under ESET NOD32 Antivirus.

7.1 Oppdatere ESET NOD32 Antivirus

ESET NOD32 Antivirus kan oppdateres enten manuelt eller automatisk. Oppdateringen startes ved å klikke **Oppdater virussignaturdatabasen** i seksjonen **Oppdater**.

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).

7.2 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 **Skann datamaskinen din** 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, klikker du **Egendefinert skanning** og angir målene som skal skannes etter virus.

Se vår regelmessig oppdaterte ESET Kunnskapsbaseartikkel for mer informasjon.

7.3 Hvordan opprette en ny oppgave i Planlegger

Når du skal opprette en ny oppgave i **Verktøy** > **Planlegger**, klikker du **Legg til** eller høyreklikker og velger **Legg til ...** i hurtigmenyen. Fem typer planlagte oppgaver er tilgjengelig:

- **Kjør eksternt program** - Planlegger kjørinig 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 én av de mest brukte planlagte oppgavene, vil vi forklare hvordan du legger til en ny oppdateringsoppgave:

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:

- **Ved 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 (timer)**)

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.

7.4 Planlegge en ukentlig datamaskinskanning

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. Se våre hjelpesider for mer detaljerte instruksjoner.

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 **Ukentlig** for oppgavehyppighet.
4. Angi dagen og tidspunktet når oppgaven skal utføres.
5. Velg **Kjør oppgaven så snart som mulig** for å utføre oppgaven senere, dersom den planlagte utførelsen av en eller annen grunn ikke starter (hvis f.eks. datamaskinen var avslått).

6. Gjennomgå sammendraget av den planlagte oppgaven, og klikk **Fullfør**.
7. Velg **Lokale stasjoner** fra fra rullegardinmenyen **Mål**.
8. Klikk **Fullfør** for å ta i bruk oppgaven.