

ESET NOD32 Antivirus 3.0

Integrerte komponenter:

ESET NOD32 Antivirus

ESET NOD32 Antispyware

Brukerveiledning



vi beskytter din digitale verden

innhold

ESET NOD32 Antivirus 3.0

Copyright © 2008 ved ESET, spol. s r. o.

ESET NOD32 Antivirus er utviklet av ESET, spol. s r.o.
Hvis du vil ha mer informasjon, går du til www.eset.com.
Med enerett. Ingen deler av denne dokumentasjonen kan kopieres, lagres i et gjenfinningssystem eller overføres helt eller delvis, elektronisk, mekanisk, fotokopiert, registrert, skannet eller på annen måte, uten skriftelig tillatelse fra utvikleren.

ESET, spol. s r.o. forbeholder seg retten til å endre programvaren som er beskrevet, uten å gi beskjed på forhånd.

Brukerstøtte for hele verden: www.eset.eu/support
Brukerstøtte for Nord-Amerika: www.eset.com/support

REV.20080709-001

1. ESET NOD32 Antivirus 3.0	4
1.1 Hva er nytt	4
1.2 Systemkrav	4
2. Installasjon.....	5
2.1 Vanlig installasjon.....	5
2.2 Egendefinert installasjon	6
2.3 Bruk av opprinnelige innstillinger	7
2.4 Oppgi brukernavn og passord	7
2.5 Datamaskinskanning etter behov.....	8
3. Veiledning for nybegynnere	9
3.1 Introduksjon til brukergrensesnittet – moduser	9
3.1.1 Kontrollere driften av systemet.....	9
3.1.2 Hva må gjøres hvis programmet ikke fungerer riktig	9
3.2 Oppsett for oppdatering	10
3.3 Oppsett av proxy-server	10
3.4 Beskyttelse av innstillinger	10
4. Arbeide med ESET NOD32 Antivirus.....	12
4.1 Virus- og spywarebeskyttelse	12
4.1.1 Filsystembeskyttelse i sanntid	12
4.1.1.1 Kontrolloppsett	12
4.1.1.1.1 Skanning av media	12
4.1.1.1.2 Skanning utløst av hendelse	12
4.1.1.1.3 Kontroll av nyopprettede filer	12
4.1.1.1.4 Avansert oppsett	12
4.1.1.2 Rensenivåer	12
4.1.1.3 Når konfigurasjon av beskyttelsen i sanntid må endres	13
4.1.1.4 Kontrollere beskyttelse i sanntid	13
4.1.1.5 Hva må gjøres hvis beskyttelsen i sanntid ikke fungerer	13
4.1.2 E-postbeskyttelse	13
4.1.2.1 Kontroll av POP3	13
4.1.2.1.1 Kompatibilitet	13
4.1.2.2 Integrasjon med Microsoft Outlook, Outlook Express, Windows Mail.....	14
4.1.2.2.1 Legge ved merkningsmeldinger til en e-posttekst	14
4.1.2.3 Fjerne infiltrasjoner.....	14
4.1.3 Beskyttelse for nettilgang.....	14
4.1.3.1 HTTP	15
4.1.3.1.1 Blokkerte/ekskluderte adresser	15
4.1.3.1.2 Nettlesere	15
4.1.4 Datamaskinskanning	16
4.1.4.1 Type skanning.....	16
4.1.4.1.1 Standardskanning	16
4.1.4.1.2 Egendefinert skanning	16
4.1.4.2 Skann mål	16
4.1.4.3 Skanneprofiler	16
4.1.5 Oppsett av parametere for ThreatSense-motor	17
4.1.5.1 Objektoppsett	17
4.1.5.2 Alternativer	17
4.1.5.3 Rensing.....	18
4.1.5.4 Filendelser.....	18
4.1.6 En infiltrasjon er oppdaget	18
4.2 Oppdatering av programmet.....	19
4.2.1 Oppsett for oppdatering	19
4.2.1.1 Oppdater profiler	19
4.2.1.2 Avansert oppsett for oppdatering	20
4.2.1.2.1 Oppdateringsmodus	20
4.2.1.2.2 Proxy-server	20
4.2.1.2.3 Koble til LAN	21
4.2.1.2.4 Opprette oppdateringskopier – Speil.....	21
4.2.1.2.4.1 Oppdatering fra speilet	22
4.2.1.2.4.2 Feilsøking av oppdateringsproblemer med speil.....	23
4.2.2 Slik lager du oppdateringsoppgaver	23

4.3	Planlegger	23
4.3.1	Formålet med å planlegge oppgaver	23
4.3.2	Opprette nye oppgaver	23
4.4	Karantene	24
4.4.1	Legge filer i karantene	24
4.4.2	Gjenopprette fra karantene	24
4.4.3	Sende inn en fil fra karantene	24
4.5	Loggfiler	25
4.5.1	Loggvedlikehold	25
4.6	Bruker grensesnitt	25
4.6.1	Varsler og meldinger	26
4.7	ThreatSense.Net	26
4.7.1	Mistenkelige filer	27
4.7.2	Statistikk	27
4.7.3	Innsending	28
4.8	Ekstern administrering	28
4.9	Lisens	28
5.	Avansert bruker	30
5.1	Oppsett av proxy-server	30
5.2	Eksportere/importere innstillinger	30
5.2.1	Eksporter innstillinger	30
5.2.2	Importer innstillinger	30
5.3	Kommandolinje	30
6.	Ordliste	32
6.1	Typer infiltrasjoner	32
6.1.1	Virus	32
6.1.2	Ormer	32
6.1.3	Trojanske hester	32
6.1.4	Rootkits	32
6.1.5	Adware	32
6.1.6	Spyware	33
6.1.7	Potensielt usikre programmer	33
6.1.8	Potensielt uønskede programmer	33

1. ESET NOD32 Antivirus 3.0

ESET NOD32 Antivirus 3.0 er oppfølgeren til det prisbelønte produktet ESET NOD32 Antivirus 2.[®]. Det benytter skannehastigheten og presisjonen til ESET NOD32 Antivirus, som oppnås ved hjelp av den nyeste versjonen av skannemotoren ThreatSense[®].

De implementerte avanserte teknikkene er i stand til proaktivt å blokkere virus, spyware, trojanske hester, ormer, adware og rootkits uten at systemhastigheten reduseres eller at du blir forstyrret når du arbeider eller spiller på datamaskinen.

1.1 Hva er nytt

Våre eksperters lange utviklingserfaring gir seg til kjenne i den helt nye arkitekturen til ESET NOD32 Antivirus-programmet som garanterer maksimal beskyttelse med minimale systemkrav.

■ Antivirus og antispysware

Denne modulen er bygd på skanningskjernen ThreatSense[®], som for første gang ble brukt i det prisbelønte NOD 32 Antivirus-systemet. ThreatSense[®]-kjernen er optimalisert og forbedret med den nye ESET NOD32 Antivirus-arkitekturen.

Funksjon	Beskrivelse
Forbedret rensing	Antivirussystemet renser og sletter nå på en intelligent måte de fleste oppdagede infiltreringer uten krav til brukerinnblanding.
Bakgrunnsskannemodus	Skanning av datamaskinen kan startes i bakgrunnen uten at det reduserer ytelsen.
Mindre oppdateringsfiler	Optimaliseringsprosesser i kjernen gjør at størrelsen på oppdateringsfilene er mindre enn i versjon 2.7. Beskyttelsen av oppdateringsfilene mot skade er forbedret.
Beskyttelse av populære e-postklienter	Det er nå mulig å skanne innkommende e-post ikke bare i MS Outlook, men også i Outlook Express og Windows Mail.
En rekke andre mindre forbedringer	– Direkte tilgang til filsystemer gir høy hastighet og produksjon. – Blokkering av tilgang til infiserte filer. – Optimalisert for Windows Sikkerhetssenter, inkludert Vista.

1.2 Systemkrav

For at ESET NOD32 Antivirus skal fungere på best mulig måte, må systemet oppfylle følgende krav til maskinvare og programvare:

ESET NOD32 Antivirus:

Windows 2000, XP	400 MHz 32-biters/64-biters (x86/x64) 128 MB RAM systemminne 35 MB ledig plass Super VGA (800 × 600)
Windows Vista	1 GHz 32-biters/64-biters (x86/x64) 512 MB RAM systemminne 35 MB ledig plass Super VGA (800 × 600)

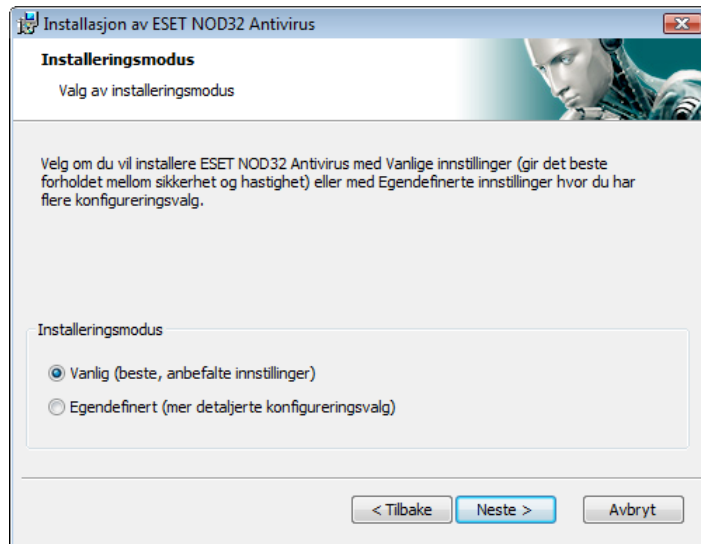
ESET NOD32 Antivirus Business Edition:

Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32-biters/64-biters (x86/x64) 128 MB RAM systemminne 35 MB ledig plass Super VGA (800 × 600)
Windows Vista, Windows Server 2008	1 GHz 32-biters/64-biters (x86/x64) 512 MB RAM systemminne 35 MB ledig plass Super VGA (800 × 600)

2. Installasjon

Etter at produktet er kjøpt, kan installasjonsprogrammet til ESET NOD32 Antivirus lastes ned fra ESETs nettsted som en msi-pakke. Start installasjonsprogrammet, og la installasjonsveviseren føre deg gjennom det grunnleggende oppsettet. Disse to typene installasjon er tilgjengelige med oppsett på forskjellige detaljnivåer:

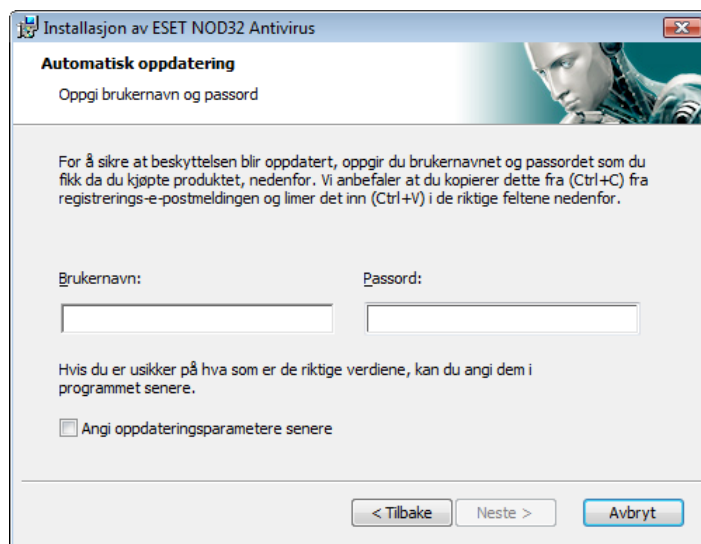
1. Vanlig installasjon
2. Egendefinert installasjon



2.1 Vanlig installasjon

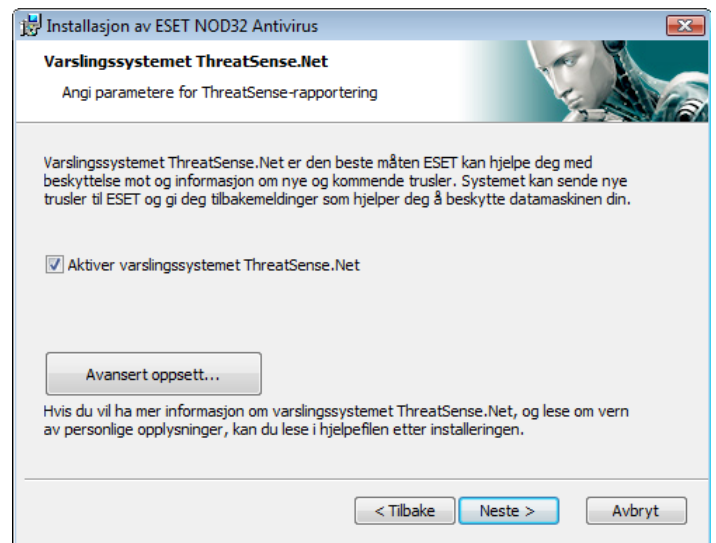
Vanlig installasjon egner seg for brukere som vil installere ESET NOD32 Antivirus med standardinnstillingene. Standardinnstillingene i programmet gir maksimalt beskyttelsesnivå. Det er nyttig for brukere som ikke ønsker å konfigurere detaljerte innstillinger.

Det første (meget viktige) trinnet er å oppgi brukernavn og passord slik at programmet kan oppdateres automatisk. Uten dette kan ikke programmet gi deg konstant beskyttelse.



Oppgi informasjon i feltene **Brukernavn** og **Passord**, dvs. de godkjenningsdataene du mottok da du kjøpte eller registrerte produktet. Hvis du ikke har brukernavn og passord tilgjengelig nå, velger du alternativet **Angi oppdateringsparametere senere**. Du kan skrive inn godkjenningsdataene direkte i programmet når som helst.

Det neste trinnet i installasjonen er konfigurering av varslingsystemet ThreatSense.Net. Varslingssystemet ThreatSense.Net hjelper deg med å sikre at ESET alltid er informert om nye infiltreringer slik at det raskt kan beskytte systemet ditt. Systemet tillater innsending av nye trusler til ESETs viruslaboratorium, hvor de blir analysert, behandlet og lagt til i virussignaturlaboratorbasene.



Det er standard at **Aktiver varslingsystemet ThreatSense.Net** er avmerket, slik at denne funksjonen er aktivert. Klikk **Avansert oppsett...** hvis du vil endre detaljerte innstillinger for innsending av mistenkelige filer.

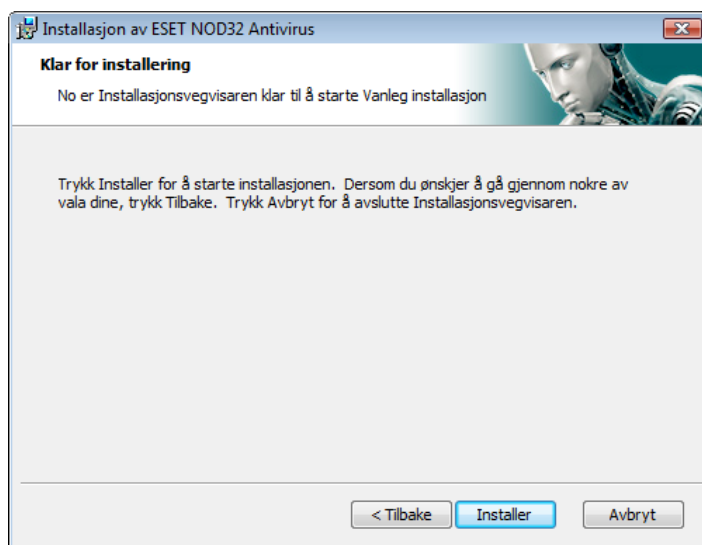
Det neste trinnet i installasjonen er å konfigurere **Gjenkjenning av mulig uønskede programmer**. Potensielt uønskede programmer er ikke nødvendigvis ment å skulle skade, men de kan ofte påvirke operativsystemet på en negativ måte.

Disse programmene følger ofte med andre programmer, og det kan være vanskelig å legge merke til dem under installasjonen. Selv om det som regel vises en melding under installasjonen, kan disse programmene enkelt bli installert uten at du godkjenner det.



Velg alternativet **Aktiver gjenkjenning av potensielt uønskede programmer**, for å la ESET NOD32 Antivirus gjenkjenne denne truseltypen (anbefalt).

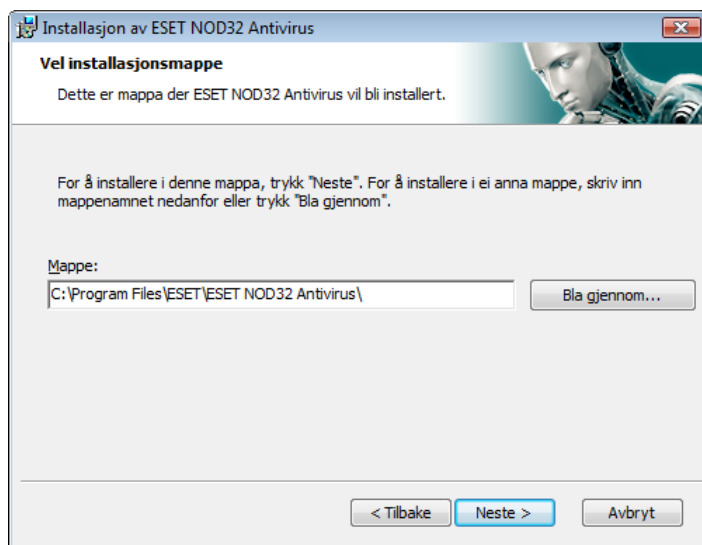
Det siste trinnet i Vanlig installasjon er å bekrefte installasjonen ved å klikke **Installer**.



2.2 Egendefinert installasjon

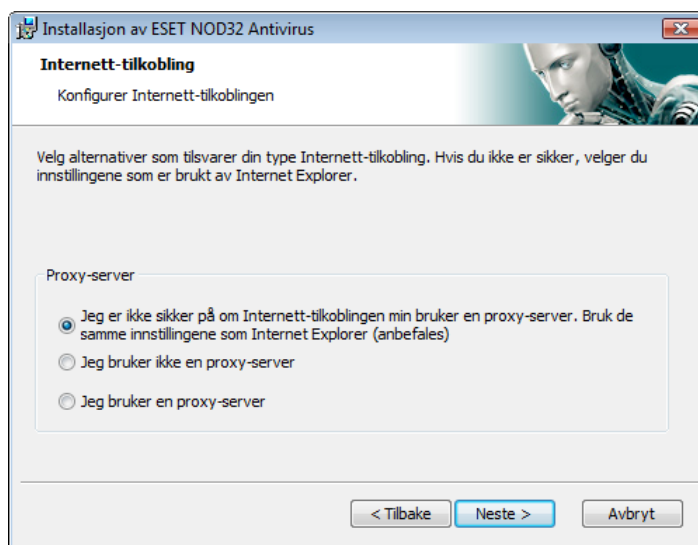
Egendefinert installasjon er beregnet på brukere som har erfaring med å fininnstille programmer, og som ønsker å endre avanserte innstillinger under installasjonen.

Det første trinnet er å velge hvor installasjonen skal plasseres. Det er standard at programmet installeres i C:\Program Files\ESET\ESET Smart Security\. Klikk **Bla gjennom...** hvis du vil endre plassering (anbefales ikke).

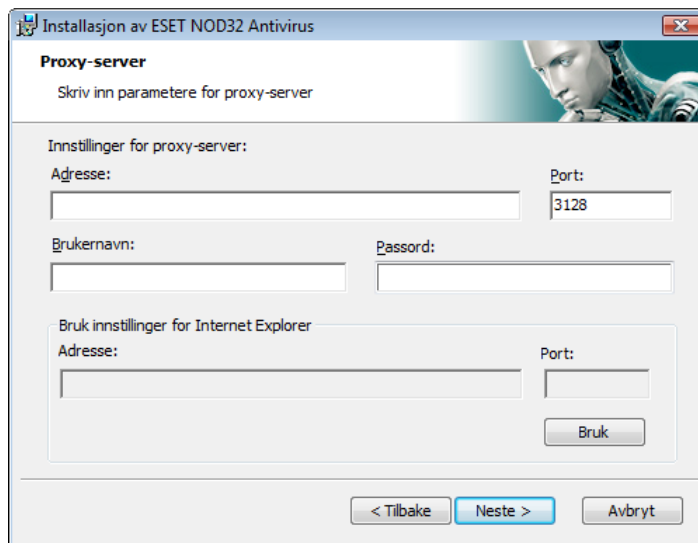


Deretter velger du **Skriv inn brukernavn og passord**. Dette trinnet er det samme som for Vanlig installasjon. (Se side 5.)

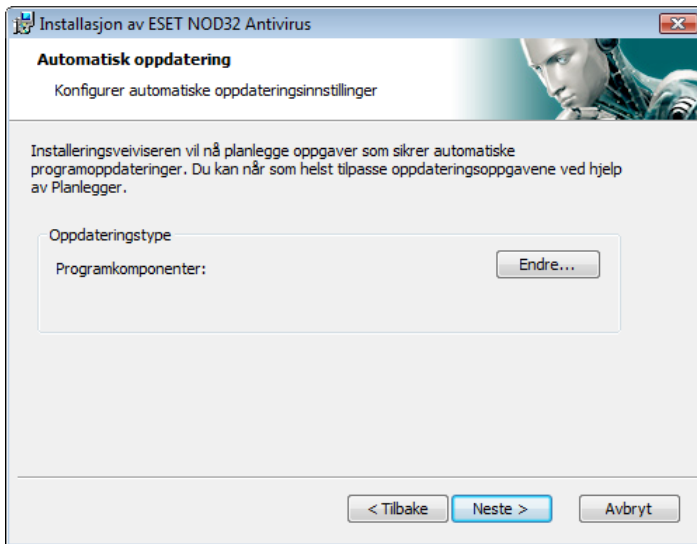
Når du har oppgitt brukernavn og passord, klikker du **Neste** slik at **Konfigurer Internett-tilkoblingen** vises.



Hvis du bruker en proxy-server, må den være korrekt konfigurert for at virussignaturoppdateringer skal fungere riktig. Hvis du ikke vet om du bruker en proxy-server for tilkobling til Internett, beholder du standardinnstillingen **Jeg er ikke sikker på om Internett-tilkoblingen min bruker en proxy-server. Bruk de samme innstillingene som Internet Explorer** og klikk **Neste**. Hvis du ikke bruker en proxy-server, velger du tilsvarende alternativ.

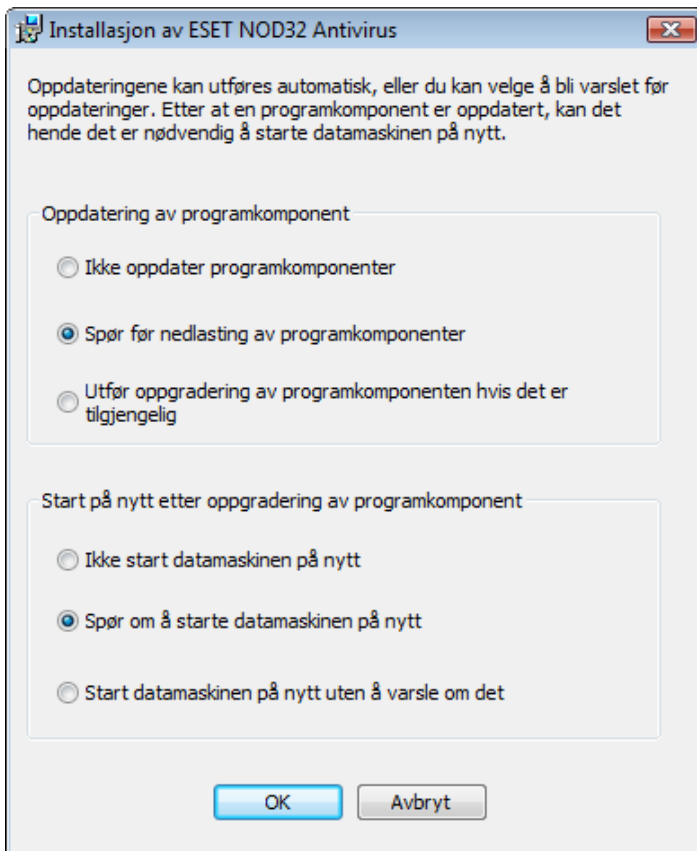


Når du skal konfigurere innstillingene for proxy-serveren, velger du **Jeg bruker en proxy-server** og klikker **Neste**. Legg inn IP- eller URL-adressen til proxy-serveren i feltet **Adresse**. I feltet **Port** angir du den porten som proxy-serveren godtar tilkoblinger via. (Standard er 3128.) Hvis proxy-serveren krever godkjenning, må du oppgi et gyldig brukernavn og passord for å få tilgang til proxy-serveren. Du kan også kopiere innstillingene til proxy-serveren fra Internet Explorer. Hvis du vil gjøre det, klikker du **Bruk** og bekrefter valget.



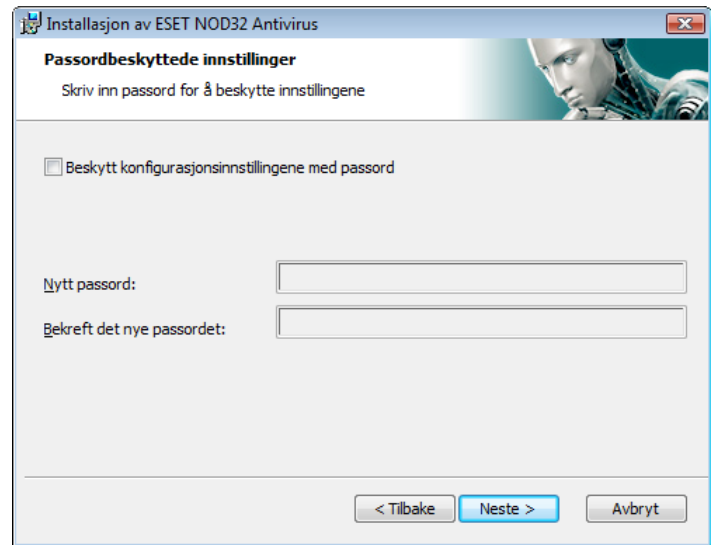
Klikk **Neste** for å gå videre til vinduet **Konfigurer automatiske oppdateringsinnstillinger**. I dette trinnet kan du angi hvordan automatisk oppdatering av programkomponenter skal håndteres av systemet. Klikk **Endre...** hvis du vil gå til de avanserte innstillingene.

Hvis du ikke vil at programkomponentene skal oppdateres, velger du **Aldri oppdater programkomponenter**. Hvis du aktiverer alternativet **Spør før nedlasting av programkomponenter**, vises et bekreftelsesvindu før programkomponenter lastes ned. Hvis du vil aktivere automatisk oppdatering av programkomponenter uten å bli spurt, velger du alternativet **Utfør oppgradering av programkomponenten hvis den er tilgjengelig**.



MERK: Etter at en programkomponent er oppgradert, må vanligvis maskinen startes på nytt. Anbefalt innstilling er: **Start datamaskinen på nytt uten å spørre, om nødvendig**.

Det neste trinnet i installasjonen er å oppgi et passord for å beskytte programparameterne. Velg et passord som du vil beskytte programmet med. Skriv inn passordet på nytt for å bekrefte det.

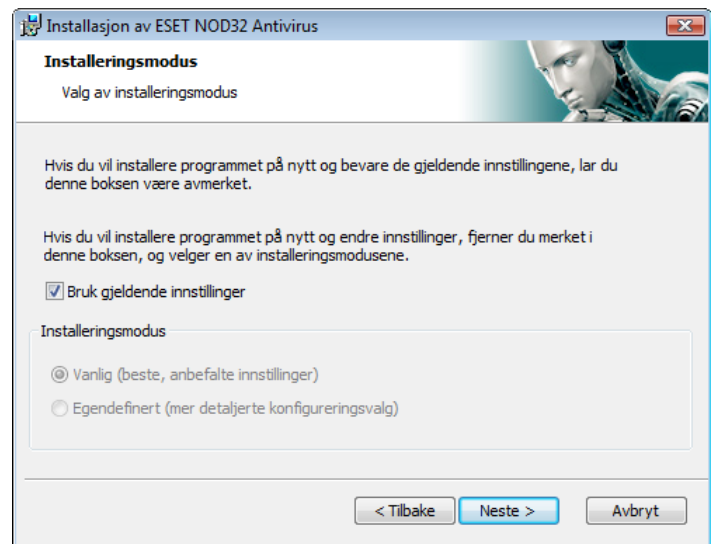


Trinnene **Konfigurering av varslingssystemet ThreatSense** og **Gjenkjenning av mulig uønskede programmer** er de samme som for en vanlig installasjon, og vises ikke her. (Se side 5.)

Det siste trinnet viser et vindu hvor du bekrefter at du vil installere.

2.3 Bruk av opprinnelige innstillinger

Hvis du installerer ESET NOD32 Antivirus på nytt, vises alternativet **Bruk gjeldende innstillinger**. Velg dette alternativet for å overføre oppsettparametere fra den opprinnelige installasjonen til den nye.



2.4 Oppgi brukernavn og passord

For å oppnå optimal funksjonalitet er det viktig at programmet oppdateres automatisk. Dette er bare mulig hvis det blir oppgitt riktig brukernavn og passord i oppsettet for oppdatering.

Hvis du ikke oppgav brukernavn og passord under installasjonen, kan du gjøre det nå. I hovedprogramvinduet velger du **Oppdater** og klikker deretter **Oppsett av brukernavn og passord...** Legg inn dataene du mottok sammen med produktlisensen, i vinduet **Lisensinformasjon**.

Lisensinformasjon

Skriv inn brukernavnet og passordet du mottok da du kjøpte eller registrerte produktet. Vi anbefaler at du kopierer (Ctrl+C) informasjonen fra e-postmeldingen med registreringsinformasjon, og limer den inn (Ctrl+V) i tilhørende felt under.

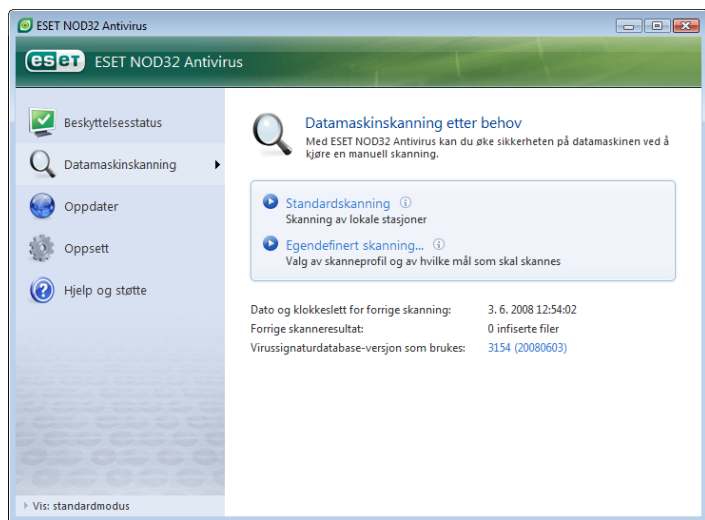
Bruker navn:
EAV-12345678

Passord
••••••••

OK Avbryt

2.5 Datamaskinskanning etter behov

Når du har installert ESET NOD32 Antivirus, bør du umiddelbart skanne datamaskinen for å kontrollere om det er skadelig kode på den. Hvis du vil starte skanning raskt, velger du **Datamaskinskanning** i hovedvinduet og deretter **Standardskanning** i hovedvinduet til programmet. For mer informasjon om datamaskinskanning, kan du lese kapittelet "Datamaskinskanning".



3. Veiledning for nybegynnere

I dette kapittelet får du en innføring i ESET NOD32 Antivirus og grunnleggende innstillinger.

3.1 Introduksjon til brukergrensesnittet – moduser

Hovedvinduet i ESET NOD32 Antivirus er delt inn i to hoveddeler. Den venstre kolonnen gir deg tilgang til den brukervennlige hovedmenyen. I hovedprogramvinduet til høyre blir det hovedsakelig vist informasjon som tilsvarer alternativet som er valgt på hovedmenyen.

Her er en beskrivelse av knappene på hovedmenyen:

Beskyttelsesstatus – gir informasjon om beskyttelsesstatusen til ESET Smart Security på en brukervennlig måte. Hvis Avansert modus er aktivert, vises statusen til alle beskyttelsesmodulene. Klikk en modul hvis du vil se gjeldende status.

Datamaskinskanning – med dette alternativet kan du konfigurere og starte funksjonen Datamaskinskanning etter behov.

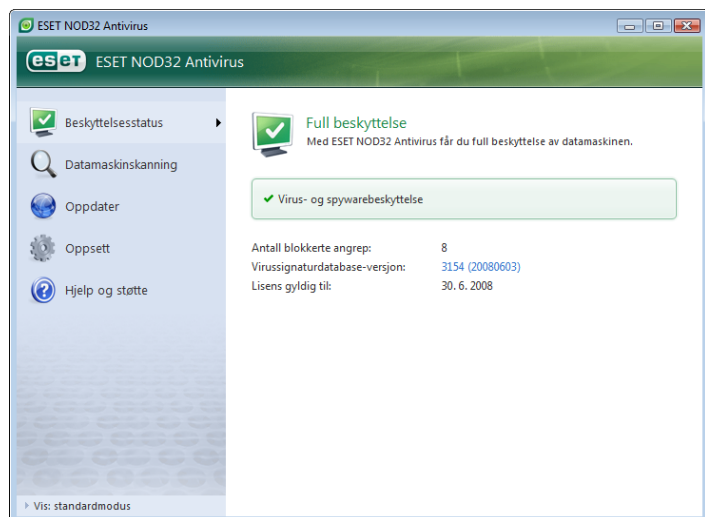
Oppdater – velg dette alternativet for å få tilgang til oppdateringsmodulene som styrer oppdateringene av virussignatordatabasen.

Oppsett – velg dette alternativet hvis du vil justere datamaskinens sikkerhetsnivå. Hvis Avansert modus er aktivert, vises undermenyene for Beskyttelse mot virus og spyware.

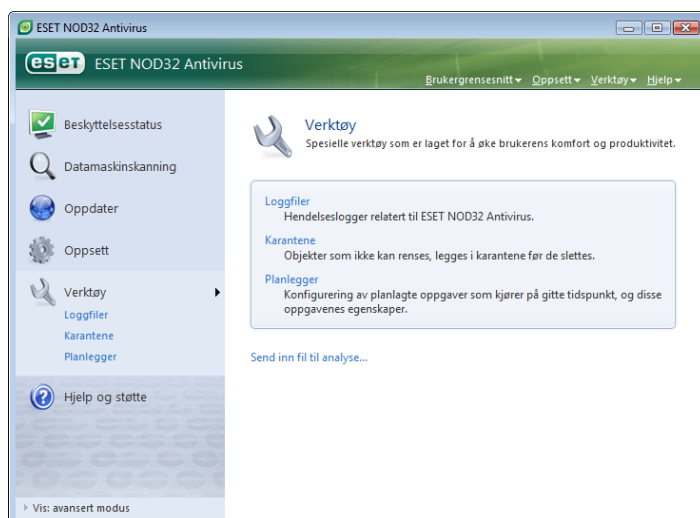
Verktøy – dette alternativet er kun tilgjengelig i Avansert modus. Gir deg tilgang til Loggfiler, Karantene og Planlegger.

Hjelp og støtte – velg dette alternativet for å få tilgang til hjelpefiler, ESETs kunnskapsdatabase, nettstedet til ESET og forespørsel om brukerstøtte.

I brukergrensesnittet til ESET NOD32 Antivirus kan du også veksle mellom modusene Standard og Avansert. Når du skal veksle mellom moduser, går du til koblingen **Vis** nederst i venstre hjørnet av hovedvinduet i ESET NOD32 Antivirus. Klikk denne knappen for å velge ønsket visningsmodus.



Standardmodus gir deg tilgang til funksjoner som er nødvendige for vanlig bruk. Ingen avanserte alternativer vises.

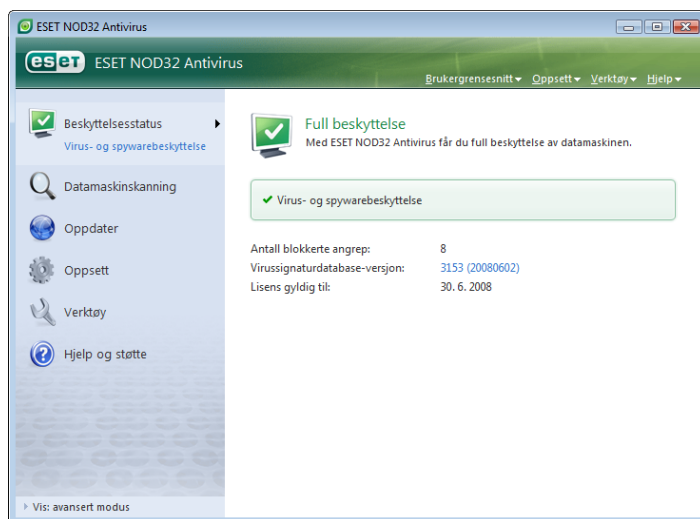


Når du veksler til Avansert modus, legges alternativet **Verktøy** til på hovedmenyen. Med alternativet Verktøy får du tilgang til funksjonene Planlegger og Karantene, og du kan se på loggfilene i ESET NOD32 Antivirus.

MERK: Resten av instruksjonene i denne veiledningen gjelder Avansert modus.

3.1.1 Kontrollere driften av systemet

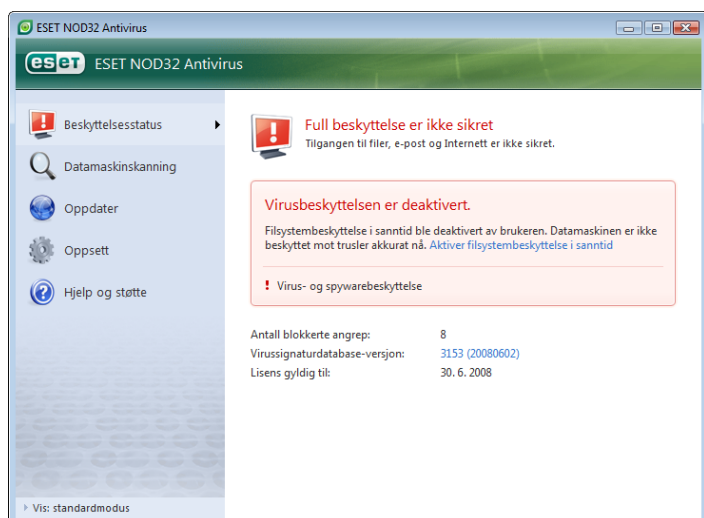
Hvis du vil se **Beskyttelsesstatus**, klikker du dette alternativet øverst på hovedmenyen. Undermenyen **Virus- og spywarebeskyttelse** vises rett under, og en statusoversikt over driften av ESET NOD32 Antivirus vises i hovedprogramvinduet. Klikk Virus- og spywarebeskyttelse og hovedprogramvinduet viser statusen til de individuelle beskyttelsesmodulene



Hvis de aktiverte modulene fungerer riktig, er de merket med en grønn hake. Hvis de ikke fungerer som de skal, vises et rødt utropstegn eller et oransje varslingsikon, og flere opplysninger om modulen vises i den øverste delen av vinduet. Det blir også vist et anbefalt forslag til løsning for modulen. Hvis du vil endre statusen til individuelle moduler, klikker du **Oppsett** på hovedmenyen og deretter ønsket modul.

3.1.2 Hva må gjøres hvis programmet ikke fungerer riktig

Hvis ESET NOD32 Antivirus oppdager et problem i en av beskyttelsesmodulene, blir feilen rapportert i vinduet **Beskyttelsesstatus**. Her blir det også foreslått en mulig løsning.

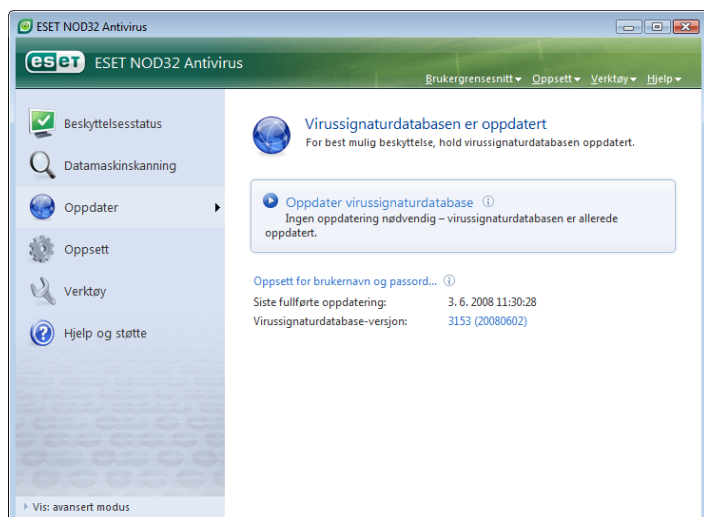


Hvis det ikke er mulig å løse et problem ved hjelp av listen over kjente problemer og løsninger, klikker du **Hjelp og støtte** for å vise hjelpefilene eller søke i kunnskapsdatabasen. Hvis du fremdeles ikke finner en løsning, kan du sende en forespørsel til ESETs brukerstøtte. Basert på denne tilbakemeldingen kan våre spesialister raskt svare på spørsmålene og gi deg gode råd.

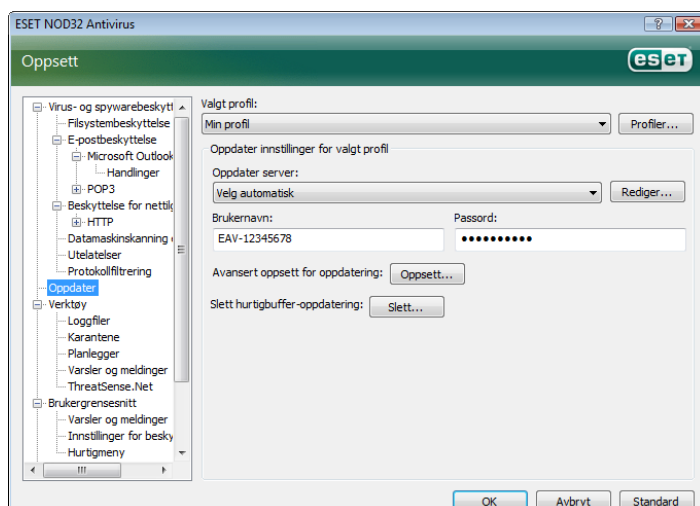
3.2 Oppsett for oppdatering

Oppdatering av virussignatordatabasen og oppdatering av programkomponentene er viktige elementer for å kunne gi deg fullstendig beskyttelse mot skadelig kode. Du bør være spesielt oppmerksom på konfigureringen og bruken av oppdateringene. Velg **Oppdater** på hovedmenyen, og klikk deretter **Oppdater virussignatordatabasen** i hovedprogramvinduet for umiddelbart å sjekke om en nyere databaseoppdatering er tilgjengelig. Ved hjelp av **Oppsett av brukernavn og passord...** vises en dialogboks der du må oppgi brukernavnet og passordet du mottok da du kjøpte programmet.

Hvis du la inn brukernavn og passord under installasjonen av ESET NOD32 Antivirus, vil du ikke få spørsmål om dette nå.

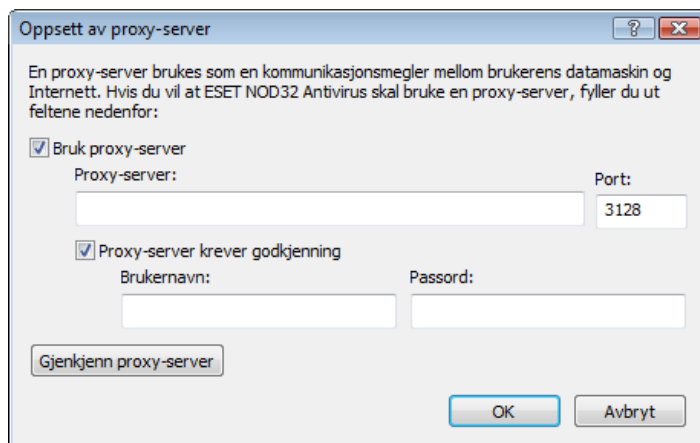


Vinduet **Avansert oppsett** (trykk F5 for å åpne dette) inneholder andre alternativer for detaljert oppdatering. Rullegardinmenyen **Oppdater server:** bør settes til **Velg automatisk**. Når du skal konfigurere avanserte oppdateringsalternativer, for eksempel oppdateringsmodus, proxy-servertilgang, tilgang til oppdateringer på en lokal server og oppretting av virussignaturkopier (ESET NOD32 Antivirus Business Edition), klikker du **Oppsett...**



3.3 Oppsett av proxy-server

Hvis du bruker en proxyserver i tilkoblingen til Internett på et system med ESET Smart Security, må den spesifiseres i Avansert oppsett (F5). Når du vil ha tilgang til konfigurasjonsvinduet **Proxy-server**, klikker du **Diverse > Proxy-server** i treet Avansert oppsett. Merk av for **Bruk proxy-server**, og oppgi IP-adressen og porten til proxy-serveren. Deretter oppgir du godkjenningsdataene.



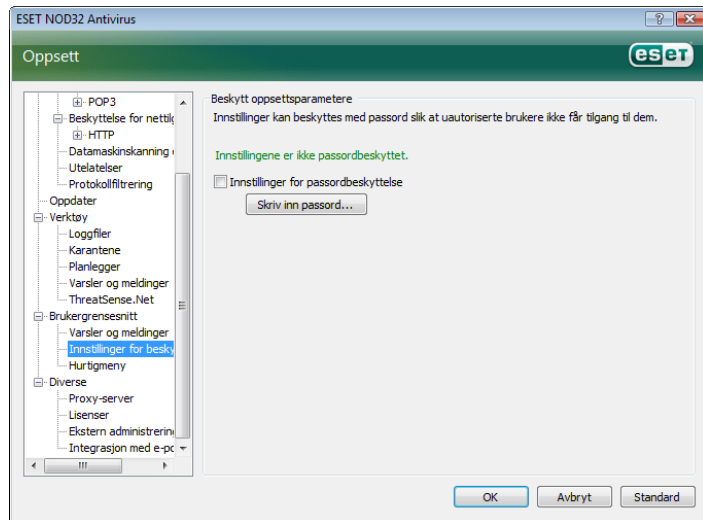
Hvis denne informasjonen ikke er tilgjengelig, kan du forsøke automatisk gjenkjenning av proxy-serverinnstillinger for ESET NOD32 Antivirus, ved å klikke **Gjenkjenn proxy-server**.

MERK: Alternativene for proxy-server for de ulike oppdateringsprofilene kan være forskjellige. Hvis det er tilfellet, konfigurerer du proxy-serveren i det avanserte oppsettet for oppdatering.

3.4 Beskyttelse av innstillinger

Innstillingene i ESET NOD32 Antivirus kan være meget viktige for organisasjonens retningslinjer for sikkerhet. Feilaktige endringer kan potensielt sette stabiliteten til og beskyttelsen av systemet i fare. Hvis du vil passordbeskytte oppsettparametrene, går du til hovedmenyen og klikker **Oppsett > Legg inn hele treet for avansert oppsett... > Brukergrensesnitt > Beskyttelse av innstillinger** og klikker **Skriv inn passord...**

Oppgi et passord, bekreft det ved å skrive det inn på nytt og klikk **OK**. Dette passordet må oppgis når du senere skal endre innstillinger i ESET NOD32 Antivirus.



4. Arbeide med ESET NOD32 Antivirus

4.1 Virus- og spywarebeskyttelse

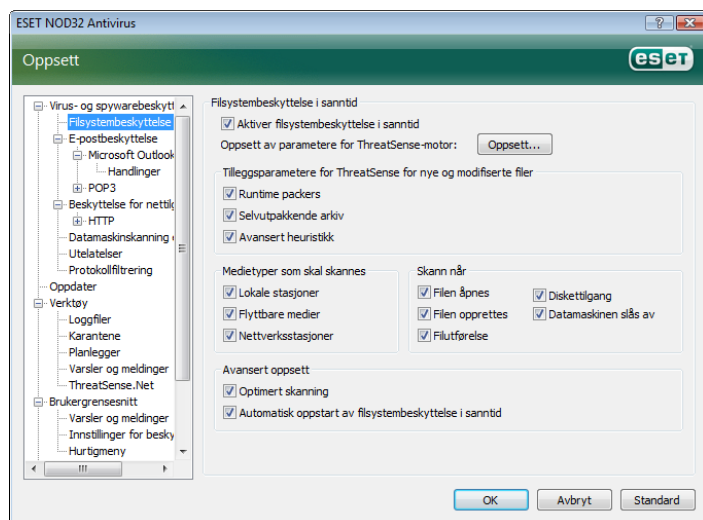
Virusbeskyttelse beskytter mot skadelige systemangrep ved å kontrollere filer, e-postmeldinger og Internett-kommunikasjon. Hvis det oppdages en trussel med skadelig kode, kan virusmodulen eliminere den ved å først blokkere den og deretter rense den, slette den eller legge den i karantene.

4.1.1 Filsystembeskyttelse i sanntid

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

4.1.1.1 Kontrolloppsett

Filsystembeskyttelsen i sanntid kontrollerer alle typer medier, og kontrollen blir utløst av forskjellige hendelser. Kontrollen bruker gjenkjenningsteknologiene til ThreatSense-teknologien (beskrevet i Oppsett av parametere for ThreatSense-motor). Kontrollfunksjonen kan variere for nyopprettede filer og eksisterende filer. For nyopprettede filer er det mulig å bruke et dypere kontrollnivå.



4.1.1.1.1 Skanning av media

Det er standard at alle typer medier blir kontrollert for potensielle trusler.

Lokale stasjoner – kontrollerer alle harddisker på systemet.

Flyttbare medier – disketter, USB-lagringenheter osv.

Nettverksstasjoner – skanner alle nettverksstasjoner.

Vi anbefaler at du beholder standardinnstillingene og bare endrer dem i bestemte tilfeller, for eksempel når skanning av visse medier reduserer dataoverføringshastigheten betydelig.

4.1.1.1.2 Skanning utløst av hendelse

Det er standard at alle filer blir skannet ved åpning, utførelse eller opprettelse. Vi anbefaler at du beholder standardinnstillingene, fordi de gir maksimal beskyttelse i sanntid for datamaskinen.

Alternativet **Disketttilgang** sørger for kontroll av oppstartssektoren på diskett når denne stasjonen brukes. Alternativet **Datamaskinen slås av** sørger for kontroll av oppstartssektorene på harddisken når datamaskinen slås av. Selv om oppstartsvirus er sjeldne i dag, anbefaler vi at du lar disse alternativene være aktivert, ettersom det fremdeles er mulighet for infisering av et oppstartsvirus fra alternative kilder.

4.1.1.3 Kontroll av nyopprettede filer

Sannsynligheten for infisering i nyopprettede filer er betydelig større enn i eksisterende filer. Dette er grunnen til at programmet kontrollerer disse filene med flere skanningsparametere. Sammen med vanlige signaturbaserte skannemetoder brukes avansert heuristikk, som forbedrer gjenkjenningsskanningsfrekvensen betydelig. I tillegg til nyopprettede filer skannes også selvutpakkende filer (SFX) og runtime packers (internt komprimerte kjørbare filer).

4.1.1.4 Avansert oppsett

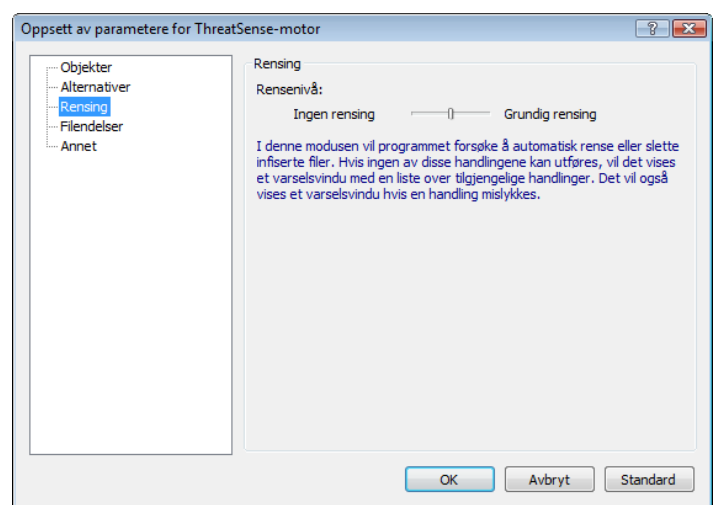
For å få minimalt systemavtrykk ved bruk av beskyttelse i sanntid, skannes ikke filer som allerede er skannet (med mindre de har blitt endret). Filer blir skannet igjen umiddelbart etter hver oppdatering av virussignaturdatabasen. Denne virkemåten konfigureres ved hjelp av alternativet **Optimert skanning**. Hvis den deaktiveres, blir alle filer skannet hver gang de åpnes.

Det er standard at beskyttelse i sanntid startes når operativsystemet startes, og skanner uten å forstyrre. I spesielle tilfeller (for eksempel hvis det er en konflikt med en annen sanntidsskanner) kan beskyttelsen i sanntid avsluttes ved å deaktivere alternativet **Automatisk oppstart av systembeskyttelse i sanntid**.

4.1.1.2 Rensenivåer

Beskyttelsen i sanntid har tre rensnivåer. (Du får tilgang ved å klikke **Oppsett...** i delen **Filsystembeskyttelse i sanntid** og deretter klikke grenen **Rensing**.)

- Det første nivået viser et varselvindu med tilgjengelige alternativer for hver infiltrasjon som oppdages. Brukeren må velge en handling for hver enkelt infiltrasjon. Dette nivået er utformet for mer avanserte brukere som vet hva de skal gjøre med hver type infiltrasjon.
- Mellomnivået velger og utfører automatisk en forhåndsdefinert handling (avhengig av type infiltrasjon). Gjenkjenning og sletting av en infisert fil blir varslet med en informasjonsmelding i det nedre høyre hjørnet av skjermen. Imidlertid blir ikke en automatisk handling utført hvis infiltrasjonen er plassert i et arkiv som også inneholder rene filer, og blir ikke utført for objekter som ikke har en forhåndsdefinert handling.
- Det tredje nivået er det mest "aggressive" – alle infiserte objekter blir renset. Ettersom dette nivået potensielt kan føre til tap av gyldige filer, anbefaler vi at det bare brukes i spesielle situasjoner.



4.1.1.3 Når konfigurasjon av beskyttelsen i sanntid må endres

Beskyttelsen i sanntid er den viktigste komponenten når det gjelder å opprettholde et sikkert system. Du må derfor være forsiktig når du endrer parameterne. Vi anbefaler at du endrer parameterne for sanntidsbeskyttelse bare i spesielle tilfeller. Eksempler på slike tilfeller kan være at den kommer i konflikt med et bestemt program, eller sanntidsskanningen i et annet antivirusprogram.

Når du har installert ESET NOD32 Antivirus, er alle innstillingene optimalisert for å gi deg det høyeste nivået av systemsikkerhet. Hvis du vil gjenopprette standardinnstillingene, klikker du **Standard** i vinduet **Filsystembeskyttelse i sanntid (Avansert oppsett > Antivirus og antispyware > Filsystembeskyttelse i sanntid)**.

4.1.1.4 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 helt 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 eicar.com er tilgjengelig for nedlastning på <http://www.eicar.org/download/eicar.com>

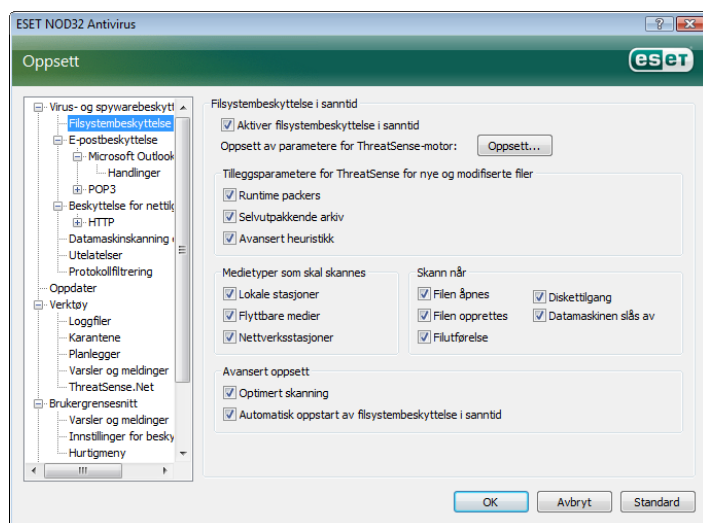
4.1.1.5 Hva må gjøres hvis beskyttelsen i sanntid ikke fungerer

I neste kapittel 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-utslittet ble deaktivert av en bruker, må den aktiveres på nytt. Du aktiverer beskyttelsen i sanntid på nytt ved å gå til **Oppsett > Virus- og spywarebeskyttelse** og klikke **Aktiver** i delen **Filbeskyttelse i sanntid** i hovedvinduet.

Hvis beskyttelsen i sanntid ikke startes når systemet starter, er det sannsynligvis fordi alternativet **Automatisk oppstart av filsystembeskyttelse i sanntid** er deaktivert. For å aktivere dette alternativet går du til **Avansert oppsett (F5)** og klikker **Systembeskyttelse i sanntid** i treet Avansert oppsett. I delen **Avansert oppsett** nederst i vinduet, må du forsikre deg om at det er merket av for **Automatisk oppstart av filsystembeskyttelse i sanntid**.



Beskyttelsen i sanntid oppdager ikke og renser ikke infiltrasjoner

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

Beskyttelsen i sanntid starter ikke

Hvis beskyttelsen i sanntid ikke starter når systemet starter (og alternativet **Automatisk oppstart av filsystembeskyttelse i sanntid** er aktivert), kan det være på grunn av konflikter med andre programmer. Hvis dette er tilfelle, kontakter du ESETs brukerstøttespesialister.

4.1.2 E-postbeskyttelse

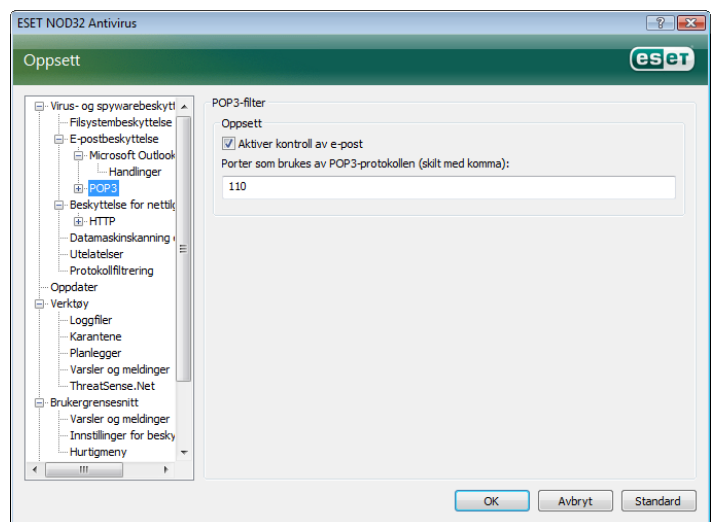
E-postbeskyttelse gir kontroll over e-postkommunikasjon mottatt via POP3-protokollen. Med plugin-programmet for Microsoft Outlook gir ESET NOD32 Antivirus kontroll over all kommunikasjon fra e-postklienten (POP3, MAPI, IMAP, HTTP). Ved undersøkelse av innkommende meldinger bruker programmet alle avanserte skannemetoder i ThreatSense-skannemotoren. Dette betyr at gjenkjenning av skadelige programmer finner sted selv før de blir sammenliknet med virussignatordatabasen. Skanning av kommunikasjon med POP3-protokoll er ikke avhengig av e-postklienten som blir brukt.

4.1.2.1 Kontroll av POP3

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.

Modulen som gir denne kontrollen, blir automatisk startet når operativsystemet starter og er deretter aktiv i minnet. For at modulen skal fungere korrekt må du forsikre deg om at den er aktivert. Kontroll av POP3 blir utført automatisk uten at e-postklienten må konfigureres på nytt. Standardinnstillingen er at all kommunikasjon via port 110 blir skannet, men andre kommunikasjonsporter kan legges til ved behov. Portnumre må skilles med komma.

Kryptert kommunikasjon blir ikke kontrollert.



4.1.2.1.1 Kompatibilitet

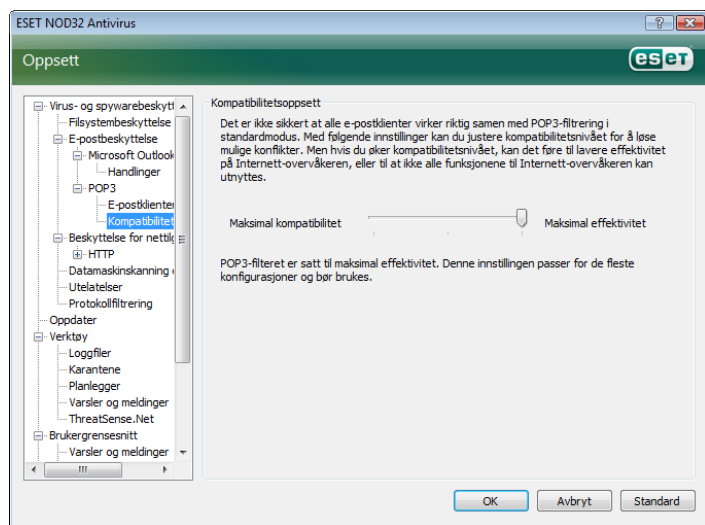
I noen e-postprogrammer kan du oppleve problemer med POP3-filtrering (Hvis du for eksempel mottar meldinger med en treg Internett-tilkobling, kan det oppstå tidsavbrudd på grunn av kontrollen). Hvis dette er tilfelle, kan du prøve å endre måten kontrollen blir utført på. Reduksjon av kontrollnivået kan øke hastigheten til renseprosessen. Hvis du vil justere kontrollnivået for POP3-filtrering, går du til **Virus- og spywarebeskyttelse > E-postbeskyttelse > POP3 > Kompatibilitet**.

Hvis **Maksimal effektivitet** er aktivert, blir infiltrasjoner fjernet fra infiserte meldinger og informasjon om infiltrasjonen blir satt inn før det opprinnelige e-postnettet. (Alternativene **Slett** eller **Rens** må

være aktivert, eller **Grundig rensing** eller **Standard** rensenivå må være aktivert.)

Middels kompatibilitet endrer måten meldinger blir mottatt på. Meldinger blir gradvis sendt til e-postklienten – etter at den siste delen av meldingen er overført, blir den skannet etter infiltrasjoner. Imidlertid øker infeksjonsrisikoen med dette kontrollnivået. Nivået på rensing og håndteringen av markeringsmeldinger (varselmeldinger som er lagt til emnelinjen og e-postteksten i e-postmeldinger) er identiske med innstillingen for maksimal effektivitet.

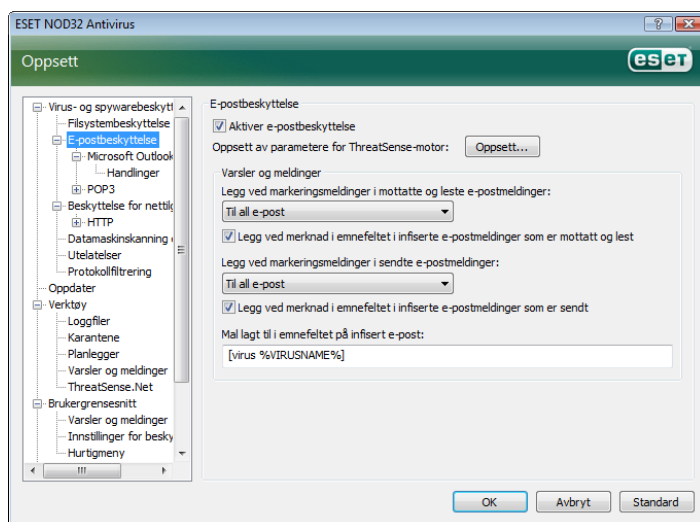
Med nivået **Maksimal kompatibilitet** blir brukeren advart med et varselvindu som rapporterer om en infisert melding. Det blir ikke lagt til informasjon om infiserte filer i emnelinjen eller i e-postteksten i mottatte meldinger, og infiltrasjoner blir ikke fjernet automatisk. Sletting av infiltrasjoner må utføres av brukeren fra e-postklienten.



4.1.2.2 Integrasjon med Microsoft Outlook, Outlook Express, Windows Mail

Integrasjon av ESET NOD32 Antivirus med e-postklienter øker nivået på aktiv beskyttelse mot skadelig kode i e-postmeldinger. Hvis e-postklienten din støttes, kan denne integrasjonen aktiveres i ESET Smart Security. Hvis integrasjon er aktivert, blir verktøylinjen ESET NOD32 Antivirus satt direkte inn i e-postklienten. Dermed er det mulig å få en mer effektiv beskyttelse av e-post. Integrasjonsinnstillingene er tilgjengelige ved hjelp av **Oppsett > Legg inn hele treet for avansert oppsett... > Diverse > Integrasjon med e-postklienter**. I dette dialogvinduet kan du aktivere integrasjon med støttede e-postklienter. E-postklienter som for tiden støttes, inkluderer Microsoft Outlook, Outlook Express og Windows Mail.

E-postbeskyttelse startes ved å merke av for **Aktiver e-postbeskyttelse** i **Avansert oppsett (F5) > Virus- og spywarebeskyttelse > E-postbeskyttelse**.



4.1.2.2.1 Legge ved markeringsmeldinger til en e-posttekst

Hver e-postmelding som blir kontrollert av ESET NOD32 Antivirus, kan markeres ved å legge til en markeringsmelding i emnet eller e-postteksten. Denne funksjonen øker troverdigheten for adressaten, og hvis en infiltrasjon oppdages, gir den verdifull informasjon om trusselnivået til en gitt e-post/avsender.

Alternativene for denne funksjonaliteten er tilgjengelige via **Avansert oppsett > Beskyttelse mot virus og spyware > E-postbeskyttelse**. I programmet kan du velge **Legg ved markeringsmelding i mottatt og lest e-post**, eller **Legg ved markeringsmelding i sendt e-post**. Brukeren kan også bestemme om markeringsmeldinger skal legges ved alle e-postmeldinger, eller bare infiserte e-postmeldinger, eller om de ikke skal legges ved i det hele tatt.

Med ESET NOD32 Antivirus kan brukerne også legge ved meldinger til det opprinnelige emnet i infiserte meldinger. For å aktivere vedlegg til emner velger du alternativene **Legg ved merknad i emnefeltet i infiserte e-poster som er mottatt og lest** og **Legg ved merknad i emnefeltet i infiserte e-poster som er sendt**.

Innholdet i meldingene kan endres i Mal-feltet som er lagt til i emnet i infisert e-post. Endringene som er nevnt ovenfor, kan bidra til å automatisere prosessen med å filtrere infisert e-post, ettersom du kan filtrere e-postmeldinger med et bestemt emne (hvis e-postklienten støtter det) til en egen mappe.

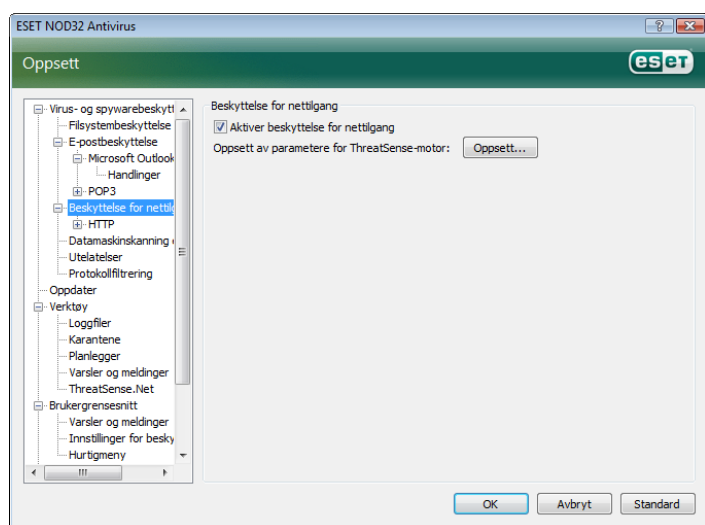
4.1.2.3 Fjerne infiltrasjoner

Hvis en infisert e-postmelding mottas, vises et varselvindu. Varselvinduet viser avsenderens navn, e-postmeldingen og navnet på infiltrasjonen. I den nedre delen av vinduet vises alternativene **Rens**, **Slett** og **Avslutt** som er tilgjengelige for det oppdagede objektet. I nesten alle tilfeller anbefaler vi at du velger enten **Rens**, eller **Slett**. I spesielle situasjoner, når du ønsker å motta den infiserte filen, velger du **Avslutt**. Hvis **Grundig rensing** er aktivert, vises et informasjonsvindu uten alternativer for infiserte objekter.

4.1.3 Beskyttelse for nettilgang

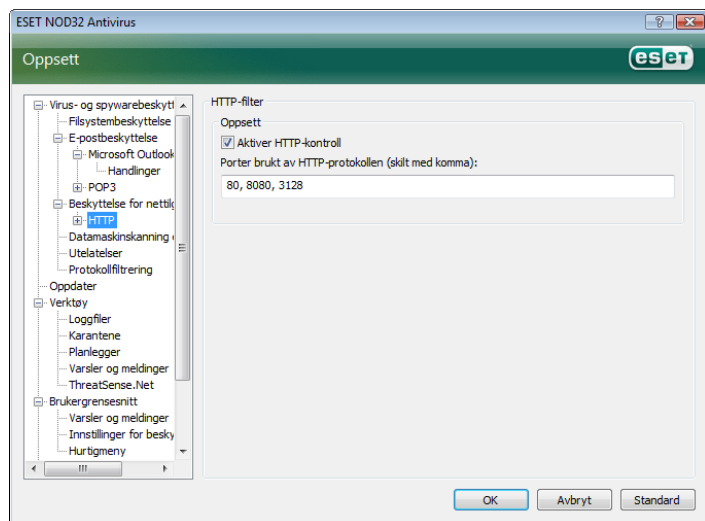
Internett-tilkobling er en standardfunksjon på PC. Dessverre har det også blitt det viktigste mediet for å overføre skadelig kode. På grunn av dette er det svært viktig at du tenker gjennom hvordan du beskytter nettilgangen din. Vi anbefaler sterkt at alternativet **Aktiver beskyttelse for nettilgang** er aktivert. Dette alternativet finner du

under **Avansert oppsett (F5) > Virus- og spywarebeskyttelse > Beskyttelse for nettilgang**.



4.1.3.1 HTTP

Den primære funksjonen til beskyttelse for nettilgang er å overvåke kommunikasjon mellom nettlesere og eksterne servere, i henhold til reglene for HTTP-protokollen (HTTP = Hypertext Transfer Protocol). Det er standard at ESET NOD32 Antivirus er konfigurert til å bruke HTTP-standardene i de fleste nettlesere. Imidlertid kan oppsettsalternativene for kontroll av HTTP delvis endres i delen **Beskyttelse for nettilgang > HTTP**. I vinduet **Oppsett for HTTP-filer** kan du aktivere, eller deaktivere kontroll av HTTP med alternativet **Aktiver HTTP-kontroll**. Du kan også definere portnumre som brukes av systemet for HTTP-kommunikasjon. Det er standard at portnumrene 80, 8080 og 3128 benyttes. HTTP-trafikk via enhver port kan automatisk oppdages og skannes ved å legge til flere portnumre, som skilles med komma.

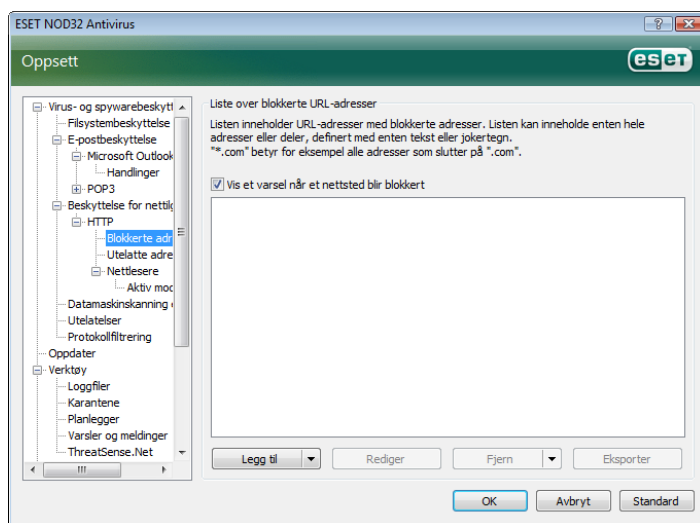


4.1.3.1.1 Blokkerte/ekskluderte adresser

Med oppsett for kontroll av HTTP kan du opprette brukerdefinerte lister over URL-adresser (URL = Uniform Resource Locator) av typen **Blokkerte adresser** og **Ekskluderte adresser**.

Begge dialogvinduer inneholder knappene **Legg til**, **Rediger**, **Fjern** og **Eksporter**, som du kan bruke til å administrere og vedlikeholde lister over spesifiserte adresser på en enkel måte. Hvis en adresse som blir forespurt av brukeren, er inkludert i listen over blokkerte adresser, er det ikke mulig å få tilgang til adressen. På den annen side gis det tilgang til adresser i listen over ekskluderte adresser uten kontroll av skadelig kode. I begge lister kan spesialsymbolene * (asterisk) og ? (spørsmålstegn) brukes. Asterisken erstatter en tegnstring,

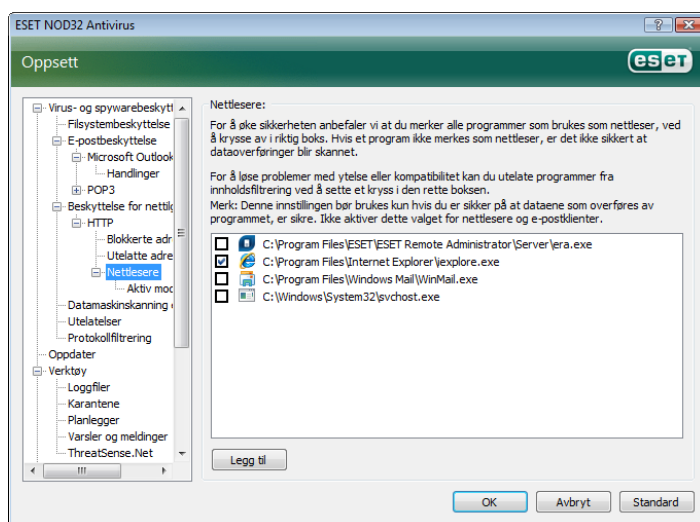
og spørsmålstegnet erstatter et symbol. Vær spesielt nøye når du spesifiserer ekskluderte adresser, ettersom listen bare skal inneholde klarerte og trygge adresser. På samme måte er det nødvendig å forsikre seg om at tegnene * og ? blir brukt korrekt i denne listen.



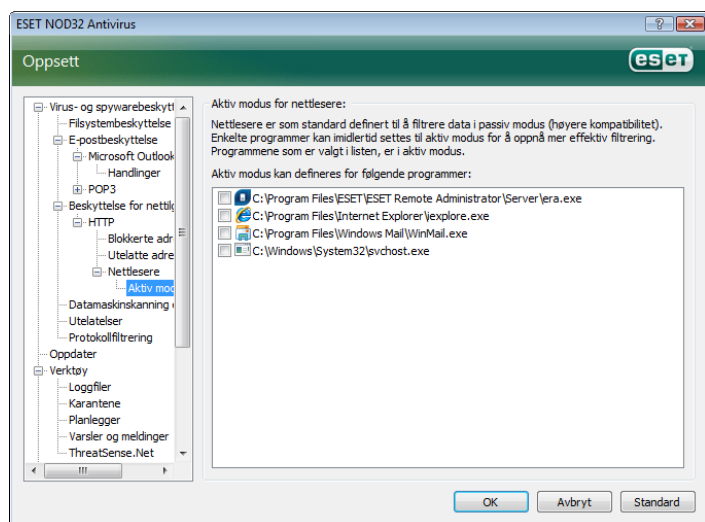
4.1.3.1.2 Nettlesere

ESET NOD32 Antivirus inneholder også funksjonen **Nettlesere**, som kan brukes til å definere om det valgte programmet er en nettleser eller ikke. Hvis et program er markert som en nettleser av brukeren, blir all kommunikasjon fra dette programmet overvåket uavhengig av hvilke portnumre som er involvert i kommunikasjonen.

Nettleserfunksjonen fullfører kontrollfunksjonen for HTTP, ettersom kontroll av HTTP bare finner sted på forhåndsdefinerte porter. Imidlertid benytter mange Internett-tjenester dynamisk endring av eller ukjente portnumre. For å veie opp for dette kan nettleserfunksjonen etablere kontroll av portkommunikasjon uavhengig av tilkoblingsparametrene.



Listen over programmer som er markert som nettlesere er tilgjengelig direkte fra undermenyen **Nettlesere**, i grenen **HTTP**. Denne delen inneholder også undermenyen **Aktiv modus** som definerer kontrollmodus for nettlesere. **Aktiv modus** er nyttig fordi den undersøker overført data i sin helhet. Hvis den ikke er aktivert, blir kommunikasjon av programmer overvåket gradvis i grupper. Dette reduserer effektiviteten til dataverifiseringsprosessen, men det gir også høyere kompatibilitet for programmene på listen. Hvis det ikke oppstår problemer under bruk, anbefaler vi at du aktiverer aktiv kontrollmodus ved å merke boksen ved siden av ønsket program.



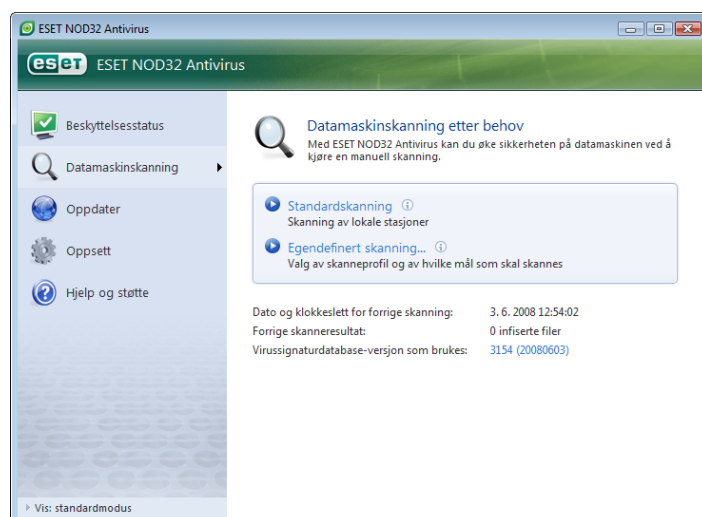
4.1.4 Datamaskinskanning

Hvis du mistenker at datamaskinen er infisert (den oppfører seg unormalt), kjører du en datamaskinskanning for å søke etter infiltrasjoner på datamaskinen. For å være på den sikre siden er det viktig at datamaskinskanning ikke bare kjøres når det er mistanke om en infisering, men jevnlig som en del av rutinemessige sikkerhetstiltak. Jevnlig skanning oppdager infiltrasjoner som ikke ble oppdaget av skanningen i sanntid, på tidspunktet de ble lagret på disken. Dette kan skje hvis skanning i sanntid var deaktivert på infeksjonstidspunktet, eller hvis virussignatordatabasen er foreldet.

Vi anbefaler at du kjører en skanning- minst én eller to ganger i måneden. Skanning kan konfigureres som en planlagt oppgave ved hjelp av **Verktøy > Planlegger**.

4.1.4.1 Type skanning

To typer er tilgjengelige. **Standardskanning** skanner systemet raskt uten behov for ytterligere konfigurering av skanneparametrene. **Egendefinert skanning...** lar brukeren velge forhåndsdefinerte skanneprofiler, i tillegg til å velge objekter fra trestrukturen.



4.1.4.1.1 Standardskanning

Standardskanning er en brukervennlig metode som lar brukeren raskt starte datamaskinskanning og rense infiserte filer uten brukerhandling. De viktigste fordelene er enkel bruk uten detaljert skanningskonfigurering. Standardskanningen kontrollerer alle filer på lokale stasjoner og renser, eller sletter automatisk oppdagede infiltrasjoner. Oppryddingsnivået blir automatisk stilt inn på standardverdien. For mer detaljert informasjon om typer rensing, se Rensing (på side 18).

Standardskanningsprofilen er utformet for brukere som ønsker å skanne datamaskinen raskt og enkelt. Den tilbyr en effektiv skanne- og renseløsning uten en omfattende konfigurasjonsprosess.

4.1.4.1.2 Egendefinert skanning

Egendefinert skanning er en optimal løsning hvis du vil spesifisere skanneparametrene, for eksempel mål som skal skannes, og skannemetoder. Fordelen med Egendefinert skanning er muligheten til å konfigurere parametrene detaljert. Konfigurasjonene kan lagres til egendefinerte skanneprofiler, som kan være nyttige hvis skanningen utføres gjentatte ganger med de samme parametrene.

For å velge mål som skal skannes, bruker du rullegardinmenyen i funksjonen for hurtigvalg av mål, eller velger mål fra trestrukturen som inneholder en liste over alle tilgjengelige enheter på datamaskinen. Videre kan du velge mellom tre rensenivåer ved å klikke **Oppsett... > Rensing**. Hvis du bare er interessert i å skanne systemet uten å gjøre noe mer, merker du av for **Skann uten å rense**.

Datamaskinskanning ved hjelp av Egendefinert skanning er egnet for erfarne brukere med tidligere erfaring med virusprogrammer.

4.1.4.2 Skann mål

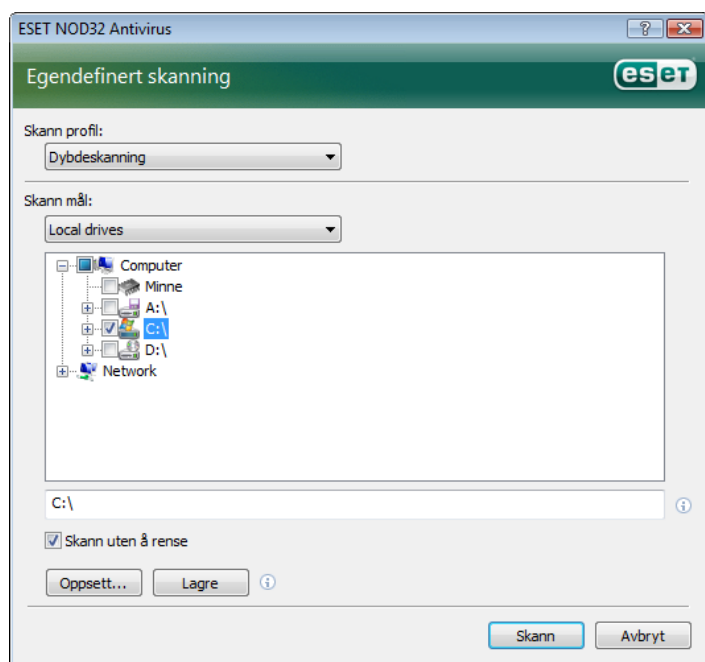
Ved hjelp av rullegardinmenyen Skann mål velger du filer, mapper og enheter (stasjoner) som skal skannes for virus.

Med alternativet for hurtigskanning av mål kan du velge følgende mål:

Lokale stasjoner – kontrollerer alle harddisker på systemet.

Flyttbare medier – disketter, USB-lagringseenheter, CD/DVD.

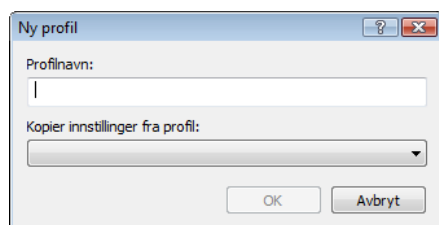
Nettverksstasjoner – alle nettverksstasjoner.



Du kan også oppgi et mål for skanning mer presist ved å angi banen til mappen eller filen(e) du vil inkludere i skanningen. Velg mål fra trestrukturen med liste over alle enheter som er tilgjengelige på datamaskinen.

4.1.4.3 Skanneprofiler

Foretrukne skanneparametere for datamaskinen kan lagres i profiler. Fordelen med å opprette skanneprofiler er at de kan brukes jevnlig for skanning i fremtiden. Vi anbefaler at du oppretter så mange profiler (med forskjellige mål for skanning, skannemetoder og andre parametere) som brukeren jevnlig benytter.



For å opprette en ny profil som kan brukes gjentatte ganger for fremtidige skanninger, går du til **Avansert oppsett (F5) > Datamaskinskanning etter behov**. Klikk **Profiler...** på høyre side for å vise listen over eksisterende skanneprofiler og alternativet for å opprette en ny profil. Det påfølgende **Oppsett av parametere for ThreatSense-motor** beskriver hvert parameter for oppsett for skanning. Dette vil hjelpe deg med å opprette en skanneprofil som dekker behovene dine.

Eksempel:

Anta at du vil opprette din egen skanneprofil, og at konfigurasjonen som er tildelt profilen **Smart skanning**, er delvis egnet. Du vil imidlertid ikke skanne runtime packers eller potensielt usikre programmer, og du vil bruke **Grundig rensing**. Klikk **Legg til...** i vinduet **Konfigurasjonsprofiler**. Oppgi navnet på den nye profilen i feltet **Profilnavn**, og velg **Smart skanning** på rullegardinmenyen **Kopier innstillinger fra profil**: rullegardinmeny. Deretter endrer du resten av parametrene etter behov.

4.1.5 Oppsett av parametere for ThreatSense-motor

ThreatSense er navnet på teknologien som består av komplekse metoder for gjenkjenning av trusler. Denne teknologien er proaktiv, noe som betyr at den gir beskyttelse også de første timene en ny trussel spres. Den benytter en kombinasjon av flere metoder (kodeanalyse, kodeemulering, generiske signaturer, virussignaturer) som jobber sammen slik at systemsikkerheten blir betydelig forbedret. Skannemotoren er i stand til å kontrollere flere datastrømmer samtidig, noe som øker effektiviteten og gjenkjenningssmengden. ThreatSense-teknologien eliminerer også rootkits på riktig måte.

Med oppsettalternativene for ThreatSense-teknologien kan du angi disse skanneparametrene:

- Filtyper og filendelser som skal skannes
- Kombinasjonen av ulike gjenkjenningsmetoder
- Rensenivåer osv.

Når du skal bruke oppsettvinduet, klikker du **Oppsett...**, som finnes i alle oppsettvinduer til alle modulene som bruker ThreatSense-teknologi (se nedenfor). Det kan være nødvendig med ulike sikkerhetsscenarier for ulike konfigurasjoner. ThreatSense kan konfigureres individuelt for følgende beskyttelsesmoduler:

- Filsystembeskyttelse i sanntid
- Filkontroll ved systemstart
- E-postbeskyttelse
- Beskyttelse for nettilgang
- Datamaskinskanning etter behov

ThreatSense-parametere kan enkelt optimaliseres for hver modul, men hvis du endrer dem, kan dette påvirke systemdriften betydelig. Hvis du for eksempel endrer parametere slik at runtime packers alltid skal skannes, eller aktiverer avansert heuristikk i beskyttelsesmodulen for filsystemet i sanntid, kan det føre til et langsommere system (normalt blir bare nyopprettede filer skannet ved hjelp av disse metodene). Vi anbefaler derfor at du ikke endrer standard ThreatSense-parametere i noen moduler, bortsett fra i Datamaskinskanning.

4.1.5.1 Objektoppsett

I delen **Objekter** kan du definere hvilke datamaskinkomponenter og filer som skal skannes for infiltrasjoner.

Minne – skanner etter trusler som angriper minnet til systemet.

Oppstartssektorer – skanner oppstartssektorer for virus i hovedoppstartsregisteret.

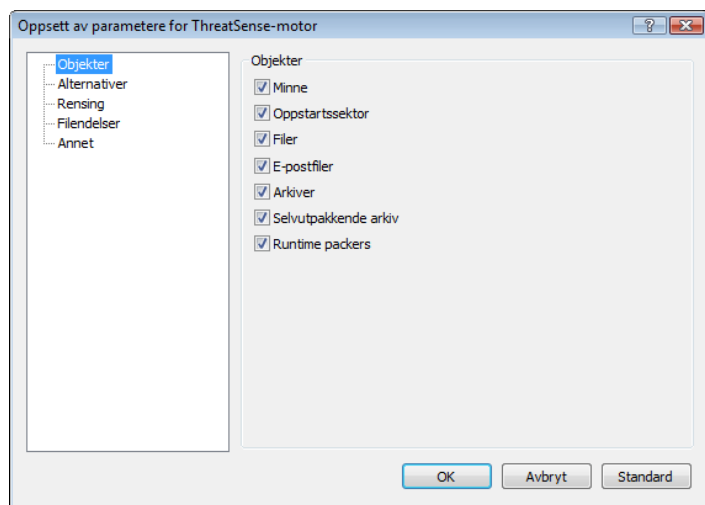
Filer – skanner alle vanlige filtyper (programmer, bilder, lyd- og videofiler, databasefiler osv.).

E-postfiler – skanner spesielle filer som inneholder e-postmeldinger.

Arkiver – skanner filer som er komprimert i arkiver (RAR, ZIP, ARJ, TAR osv.).

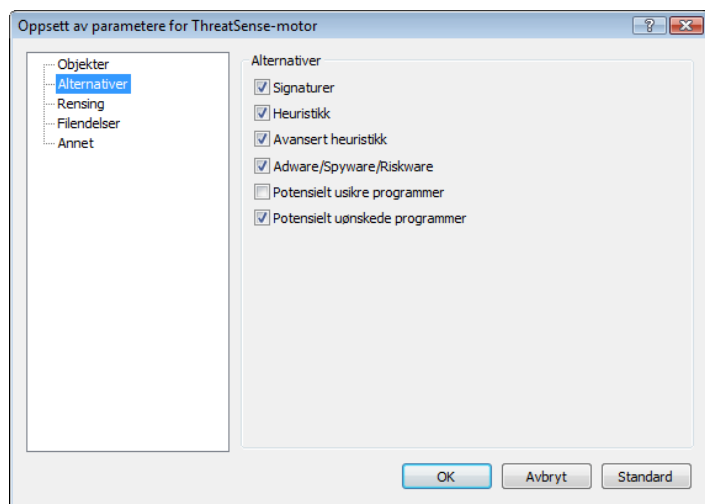
Selvutpakkende arkiver – skanner filer som ligger i selvutpakkende-arkivfiler, som vanligvis har filendelsen EXE.

Runtime packers – runtime packers (til forskjell fra standard arkivtyper) dekomprimeres i minnet, i tillegg til standard static packers (UPX, yoda, ASPack, FGS osv.).



4.1.5.2 Alternativer

I delen **Alternativer** kan brukeren velge metoder som skal brukes ved skanning av systemet etter infiltrasjoner. Følgende alternativer er tilgjengelige:



Signaturer – Signaturer kan nøyaktig og pålitelig oppdage og identifisere infiltrasjoner etter navn ved hjelp av virussignaturer.

Heuristikk – Heuristikk er en algoritme som analyserer (den skadelige) aktiviteten til programmer. Hovedfordelen med heuristisk gjenkjenning er muligheten til å oppdage ny, skadelig programvare som ikke tidligere eksisterte, eller som ikke er inkludert i listen over kjente virus (virussignatordatabase).

Avansert heuristikk – Avansert heuristikk utgjør en unik heuristisk algoritme utviklet av ESET som er optimert for å oppdage dataormer og trojanske hester skrevet i programmeringsspråk på høyt nivå. Takket være avansert heuristikk blir gjenkjennelsesintelligensen til programmet betydelig høyere.

Adware/Spyware/Riskware – denne kategorien inkluderer programvare som samler forskjellig sensitiv informasjon om brukere uten deres samtykke. Denne kategorien inkluderer også programvare som viser markedsføringsmateriale.

Potensielt usikre programmer – potensielt usikre programmer er klassifisering brukt for kommersiell, legitim programvare. Den inkluderer programmer som eksterne tilgangsværktøy, som er grunnen til at dette alternativet er deaktivert som standardinnstilling.

Potensielt uønskede programmer – potensielt uønskede programmer er ikke nødvendigvis ment å skulle skade, men de kan påvirke ytelsen til datamaskinen på en negativ måte. Slike programmer krever vanligvis godkjenning ved installasjon. Hvis de er til stede på datamaskinen, oppfører systemet seg annerledes (sammenlignet med tilstanden før installasjon). De mest betydelige endringene inkluderer uønskede popup-vinduer, aktivering og kjøring av skjulte prosesser, økt bruk av systemressurser, endringer i søkeresultater og programmer som kommuniserer med eksterne servere.

4.1.5.3 Rensing

Renseinnstillingene avgjør skannerens funksjon under rensingen av infiserte filer. Dette er de tre nivåene for rensing:

Ingen rensing

Infiserte filer blir ikke renses automatisk. Programmet viser et varselvindu og lar brukeren velge en handling.

Standardnivå

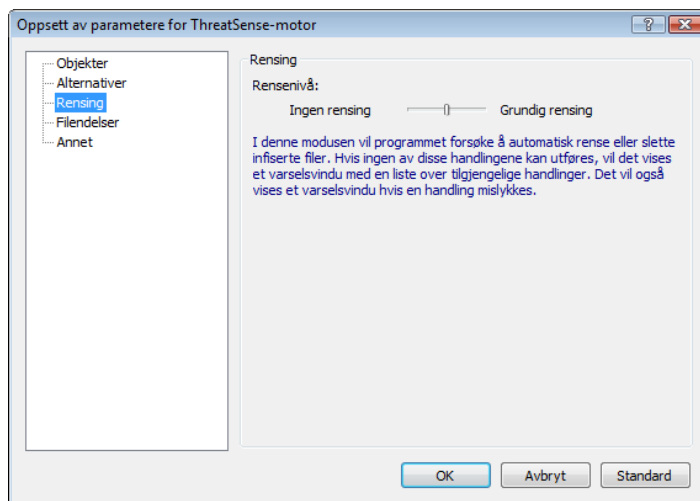
Programmet vil forsøke å renses automatisk eller slette en infisert fil. Hvis det ikke er mulig å velge korrekt handling automatisk, vil programmet tilby flere oppfølgingshandlinger. Valget av oppfølgingshandlinger vil også vises hvis en forhåndsdefinert handling ikke kunne fullføres.

Grundig rensing

Programmet renser eller sletter alle infiserte filer (inkludert arkiver). De eneste unntakene er systemfiler. Hvis det ikke er mulig å renses dem, får brukeren velge handling i et varselvindu.

Advarsel:

I Standard-modus blir hele arkivfilen slettet bare hvis alle filene i arkivet er infisert. Hvis arkivet også inneholder legitime filer, blir det ikke slettet. Hvis en infisert arkivfil blir oppdaget under grundig rensing, blir hele arkivet slettet, selv om det inneholder rene filer.



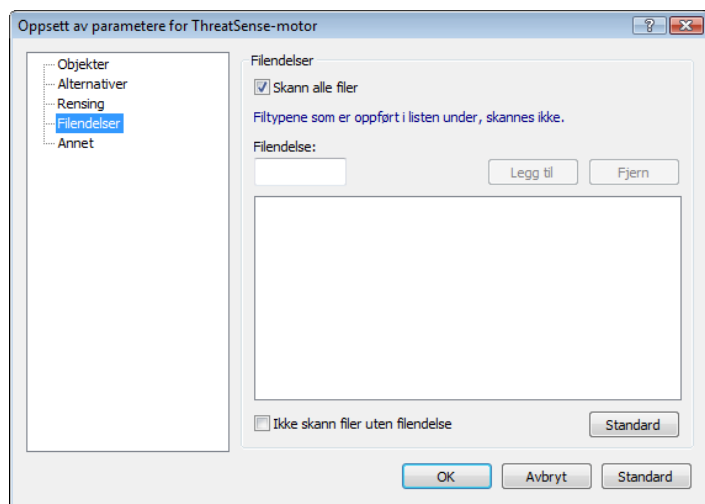
4.1.5.4 Filendelser

En filendelse er en del av filnavnet som er skilt ut med punktum. Filendelsen definerer type fil og innholdet i den. I denne delen av oppsettet av parametere for ThreatSense kan du definere hvilke filtyper som skal skannes.

Det er standard at alle filer skannes uavhengig av filendelse. Alle filendelser kan legges til listen over filer som skal utelates ved skanning. Hvis det ikke er merket av for **Skann alle filer**, blir alle filendelser som blir skannet vist i listen. Ved å bruke **Legg til** og **Fjern** kan du aktivere eller begrense skanning av ønskede endelser.

Hvis du vil aktivere skanning av filer uten endelse, velger du **Skann filer uten filendelse**.

Utelatelse av filer fra skanning har et formål hvis skanning av bestemte filtyper hindrer programmet i å bruke endelsene til å kjøre riktig. Det anbefales for eksempel å utelate endelsene edb, eml og tmp, ved bruk av MS Exchange Server.



4.1.6 En infiltrasjon er oppdaget

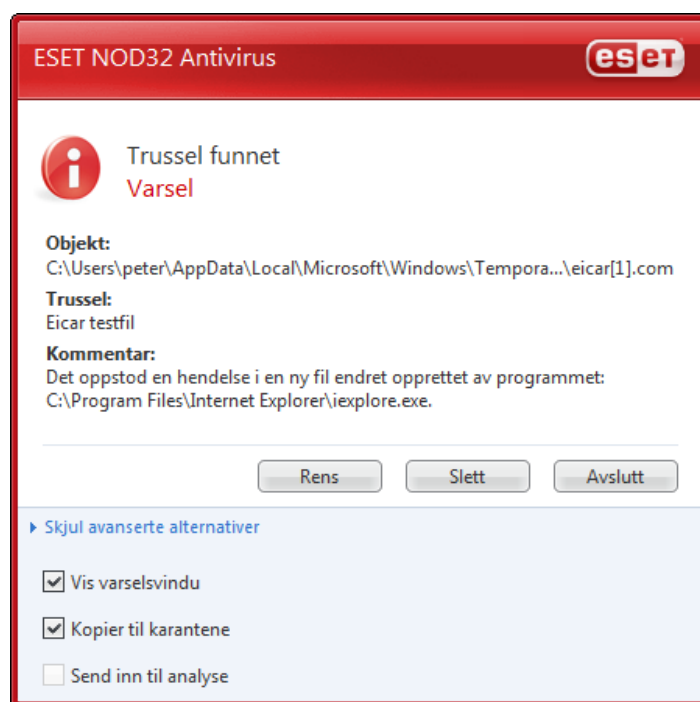
Infiltrasjon kan nå systemet fra forskjellige inngangspunkter, for eksempel nettsider, delte mapper, via e-post eller fra flyttbare dataenheter (USB, eksterne harddisker, CD-er, DVD-er, disketter osv.).

Hvis datamaskinen viser tegn på 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 **Standardskanning** (For mer informasjon, se Standardskanning).
- Etter at skanningen er fullført, kan du gjennomgå loggen for antall skannede, infiserte og rensede filer.

Hvis du bare vil skanne en bestemt del av harddisken klikker du **Egendefinert skanning** og velger målene som skal skannes for virus.

Som et generelt eksempel på hvordan infiltrasjoner blir håndtert i ESET Smart Security, kan du anta at en infiltrasjon blir oppdaget av filsystemovervåkning i sanntid, som bruker standard rensenivå. Den vil prøve å rense eller slette filen. Hvis det ikke er en forhåndsdefinert handling som skal utføres av beskyttelsesmodulen i sanntid, blir du alltid bedt om å velge et alternativ i et varselvindu. Vanligvis er alternativene **Rens**, **Slett** og **Avslutt** tilgjengelige. Det anbefales ikke å velge **Avslutt**, siden den infiserte filen / infiserte filer da ikke blir håndtert. Unntaket er når du er sikker på at filen er sikker og har blitt oppdaget ved en feil.



Rense og slette

Bruk rensing hvis en rensert fil har blitt angrepet av et virus som har festet skadelig kode til den rensede filen. Hvis dette er tilfellet, vil den først prøve å rense den infiserte filen for å gjenopprette den til opprinnelig 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 oppdaget etter at den er sluppet (vanligvis etter at systemet er startet på nytt).

Slette filer i arkiver

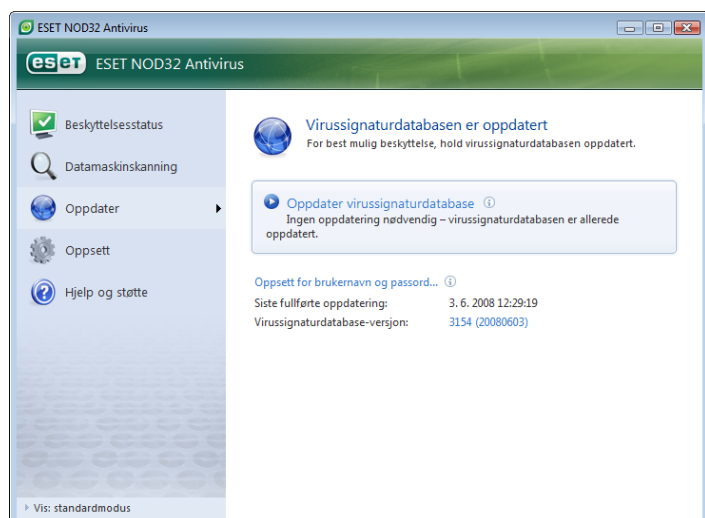
I standard rensmodus blir hele arkivet slettet, kun hvis det inneholder infiserte filer og ingen rene filer. Det vil si at arkivene ikke blir slettet hvis de også inneholder sikre, rene filer. Du må imidlertid utvise forsiktighet når du utfører en skanning av typen Grundig rensing. Med Grundig rensing blir arkivet slettet hvis det inneholder minst én infisert fil, uavhengig av statusen til de andre filene i arkivet.

4.2 Oppdatering av programmet

Jevnlig oppdatering av systemet er helt nødvendig for å få maksimalt sikkerhetsnivå med ESET Smart Security. Oppdateringsmodulen sikrer at programmet alltid er oppdatert. Dette gjøres på to måter – ved å oppdatere virussignaturdatabasen, og ved å oppdatere alle systemkomponentene.

Informasjon om gjeldende oppdateringsstatus finner du ved å klikke **Oppdater**, inkludert gjeldende versjon av virussignaturdatabasen og om en oppdatering er nødvendig. I tillegg er alternativet for å aktivere oppdateringsprosessen umiddelbart – **Oppdater virussignaturdatabasen** – tilgjengelig, sammen med grunnleggende alternativer for oppsett for oppdatering, for eksempel brukernavn og passord for å få tilgang til ESETs oppdateringsservere.

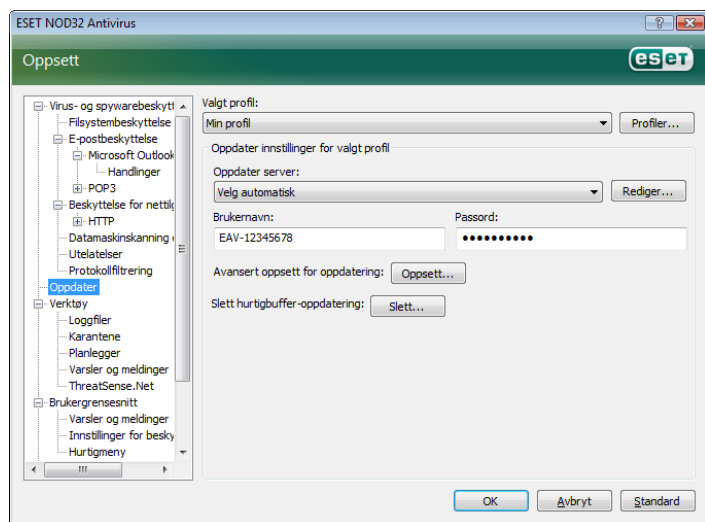
Informasjonsvinduet inneholder også informasjon, for eksempel dato og klokkeslett for forrige oppdatering og nummeret på virussignaturdatabasen. Denne numeriske angivelsen er en aktiv kobling til ESETs nettsted, med en oversikt over alle signaturer som er lagt til etter den forrige oppdateringen.



MERK: Brukernavn og passord fås fra ESET etter kjøp av ESET Smart Security.

4.2.1 Oppsett for oppdatering

Delen for oppdateringsoppsett spesifiserer informasjon om oppdateringskilden, for eksempel oppdateringsservere og godkjenningsdata for disse serverne. Det er standard at feltet **Oppdater server:** er satt til **Velg automatisk**. Denne verdien sikrer at oppdateringsfilene blir automatisk lastet ned fra ESET-serveren med minst nettverkstrafikk. Alternativene for oppsett for oppdatering er tilgjengelig i treet **Avansert oppsett (F5)** under **Oppdater**.



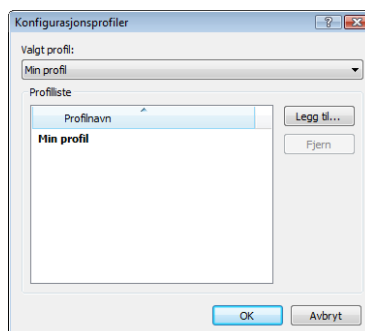
Listen over eksisterende oppdateringsservere er tilgjengelig via rullegardinmenyen **Oppdater server:** Hvis du vil legge til en ny oppdateringsserver, klikker du **Rediger...** i delen **Oppdater innstillinger for valgt profil** og klikker deretter **Legg til**.

Godkjenning for oppdateringsservere gis etter angivelse av brukernavnet og passordet som ble generert og sendt til brukeren av ESET etter kjøp av produktlisensen.

4.2.1.1 Oppdater profiler

For de forskjellige oppdateringskonfigurasjonene kan du opprette brukerdefinerte oppdateringsprofiler som kan brukes til en bestemt oppdateringsoppgave. Det er spesielt nyttig å opprette forskjellige oppdateringsprofiler for mobile brukere, ettersom egenskapene til Internett-tilkoblingen endres med jevne mellomrom. Ved å endre oppdateringsoppgaven kan mobile brukere spesifisere at hvis det ikke er mulig å oppdatere programmet med konfigurasjonen som er angitt i **Min profil**, blir oppdateringen utført med en alternativ profil.

Rullegardinmenyen **Valgt profil** viser den gjeldende profilen. Det er standard at denne oppføringen er satt til **Min profil**. Hvis du vil opprette en ny profil, klikker du først **Profiler...** Deretter klikker du **Legg til...**, og skriver inn ditt eget **Profilnavn**. Når du oppretter en ny profil, kan du kopiere innstillinger fra en eksisterende profil ved å velge den på rullegardinmenyen **Kopier innstillinger fra profil:**



I oppsettet av profilen kan du angi hvilken oppdateringsserver programmet skal koble seg til og laste ned oppdateringer fra. Du kan velge en server fra listen over tilgjengelige servere, eller du kan legge til en ny server. Listen over eksisterende oppdateringsservere er tilgjengelig via rullegardinmenyen **Oppdater server:** For å legge til en ny oppdateringsserver, klikker du **Rediger...** i delen **Oppdater innstillinger for valgt profil** og klikker deretter **Legg til**.

4.2.1.2 Avansert oppsett for oppdatering

Hvis du vil se **Avansert oppsett for oppdatering**, klikker du **Oppsett...** Alternativene for avansert oppsett for oppdatering inkluderer konfigurasjon av **Oppdateringsmodus**, **HTTP-proxy**, **LAN** og **Spill**.

4.2.1.2.1 Oppdateringsmodus

Kategorien **Oppdateringsmodus** inneholder alternativer som gjelder oppdatering av programkomponenter.

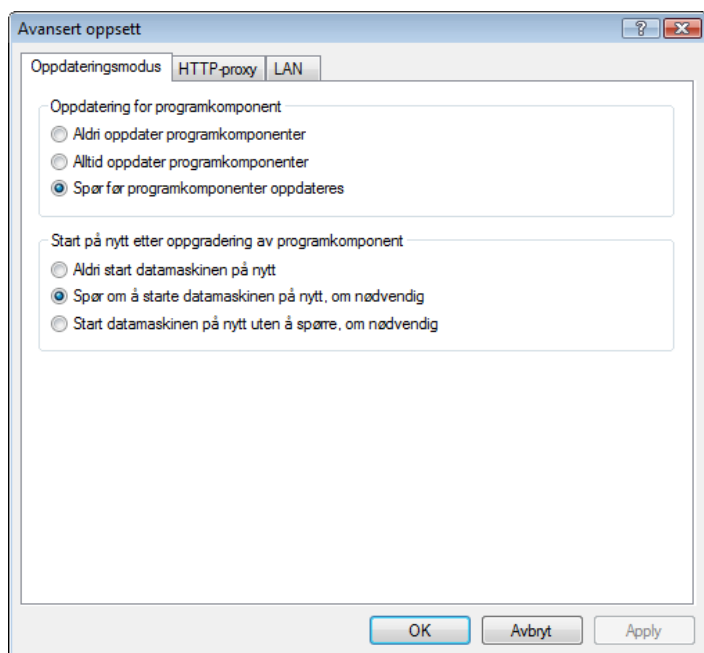
I delen **Oppdatering av programkomponent** er disse tre alternativene tilgjengelige:

- **Aldri oppdater programkomponenter**
- **Alltid oppdater programkomponenter**
- **Spør før nedlasting av programkomponenter**

Ved å velge alternativet **Aldri oppdater programkomponenter** sikrer du at nye oppdateringer av programkomponenter fra ESET ikke blir lastet ned, og at ingen programkomponenter oppdateres på den aktuelle arbeidsstasjonen. Alternativet **Alltid oppdater programkomponenter** betyr at komponenter blir oppdatert hver gang en ny oppdatering er tilgjengelig på ESETs oppdateringsservere, og at programkomponenter blir oppgradert til den nedlastede versjonen.

Velg det tredje alternativet, **Spør før nedlasting av programkomponenter** hvis du vil at programmet skal be brukeren om å bekrefte nedlasting av oppdaterte programkomponenter når slike oppdateringer blir tilgjengelige. I slike tilfeller vises et dialogvindu med informasjon om de tilgjengelige oppdateringene og mulighet til å bekrefte eller avslå nedlasting. Hvis du bekrefter, blir oppdateringer lastet ned og nye programkomponenter blir installert.

Standardalternativet for oppdatering av programkomponenter er **Spør før nedlasting av programkomponenter**.



Etter at en programkomponent er oppdatert, må systemet startes på nytt for å få full funksjonalitet i alle moduler. I delen **Start på nytt etter oppgradering av programkomponent** kan du velge ett av følgende tre alternativer:

- **Aldri start datamaskinen på nytt**
- **Spør om å starte datamaskinen på nytt, om nødvendig**
- **Start datamaskinen på nytt uten å varsle om det**

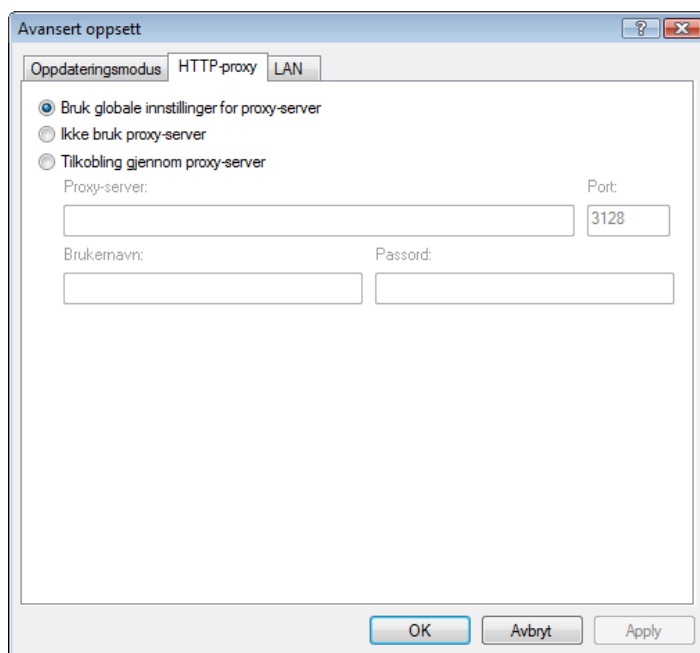
Standardalternativet for å starte på nytt er **Spør om å starte datamaskinen på nytt, om nødvendig**. Hvilket alternativ for oppdatering av programkomponenter i kategorien **Oppdateringsmodus** som er best, avhenger av hver enkelt arbeidsstasjon, ettersom det er dem innstillingene gjelder for. Vær oppmerksom på at det er forskjell på arbeidsstasjoner og servere – for eksempel kan automatisk omstart av serveren etter en programoppdatering forårsake alvorlig skade.

4.2.1.2.2 Proxy-server

Slik får du tilgang til oppsettalternativene for proxy-server for en gitt oppdateringsprofil: Klikk **Oppdater** i treet Avansert oppsett (F5), og klikk deretter **Oppsett...** til høyre for **Avansert oppsett for oppdatering**. Klikk kategorien **HTTP-proxy**, og velg ett av tre følgende alternativer:

- **Bruk globale innstillinger for proxy-server**
- **Ikke bruk proxy-server**
- **Tilkobling via proxy-server** (tilkobling definert av egenskapene til tilkoblingen)

Hvis du velger alternativet **Bruk globale innstillinger for proxy-server**, benyttes konfigurasjonsalternativene for proxy-server som er spesifisert i grenen **Diverse > Proxy-server** i treet Avansert oppsett.



Velg alternativet **Ikke bruk proxy-server** hvis du ikke vil at det skal benyttes proxy-server for oppdatering av ESET Smart Security.

Velg alternativet **Tilkobling gjennom proxy-server** hvis det skal benyttes en proxy-server for oppdatering av ESET NOD32 Antivirus, og den ikke er identisk med proxy-serveren som er spesifisert i de globale innstillingene (**Diverse > Proxy-server**). Hvis det er tilfellet, må innstillingene angis her: Adressen til proxy-serveren i feltet **Proxy-server**, kommunikasjonsporten i feltet **Port**, samt **Brukernavn** og **Passord** for proxy-serveren hvis det er nødvendig.

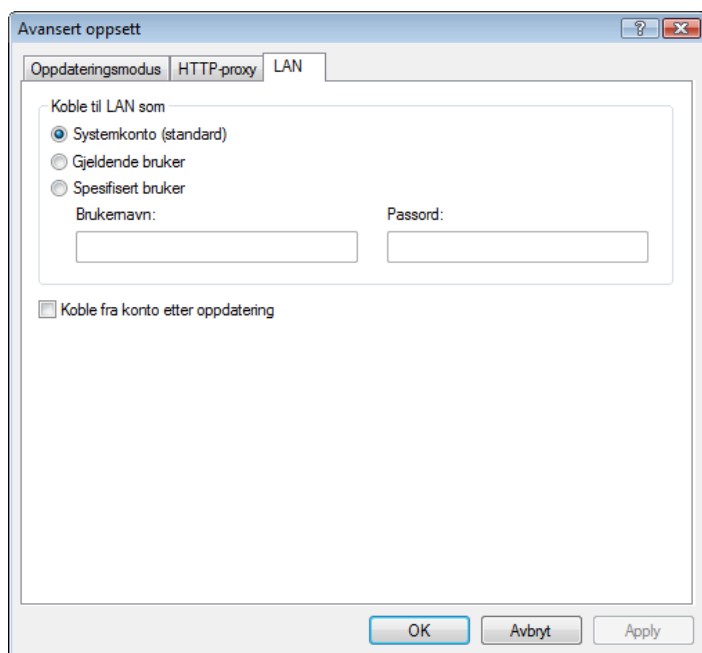
Dette alternativet bør også velges hvis innstillingene for proxy-server ikke ble angitt globalt, og ESET NOD32 Antivirus isteden skal koble til en proxy-server for å hente oppdateringer.

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

4.2.1.2.3 Koble til LAN

Ved oppdatering fra en lokal server med NT-basert operativsystem, er det standard at godkjenning for hver nettskilkobling er påkrevd. I de fleste tilfeller har ikke en lokal systemkonto tilstrekkelige tilgangsrettigheter til Speil-mappen. (Denne mappen inneholder kopier av oppdateringsfiler.) Hvis dette er tilfellet, skriver du inn brukernavnet og passordet i delen for oppdateringsoppsett eller angir en eksisterende konto som programmet kan bruke for å få tilgang til oppdateringsserveren (Speil).

Hvis du skal konfigurere en slik konto, klikker du kategorien **LAN**. I delen **Koble til LAN som** finner du alternativene **Systemkonto (standard)**, **Gjeldende bruker** og **Spesifisert bruker**.



Velg alternativet **Systemkonto** hvis du vil bruke systemkontoen til godkjenning. Vanligvis skjer det ingen godkjenningsprosess hvis det ikke er oppgitt godkjenningsdata i hovedoppdateringsoppsettet.

For å sikre at programmet godkjenner seg selv med en gjeldende pålogget brukerkonto, 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.

Standardalternativet for LAN-tilkobling er **Systemkonto**.

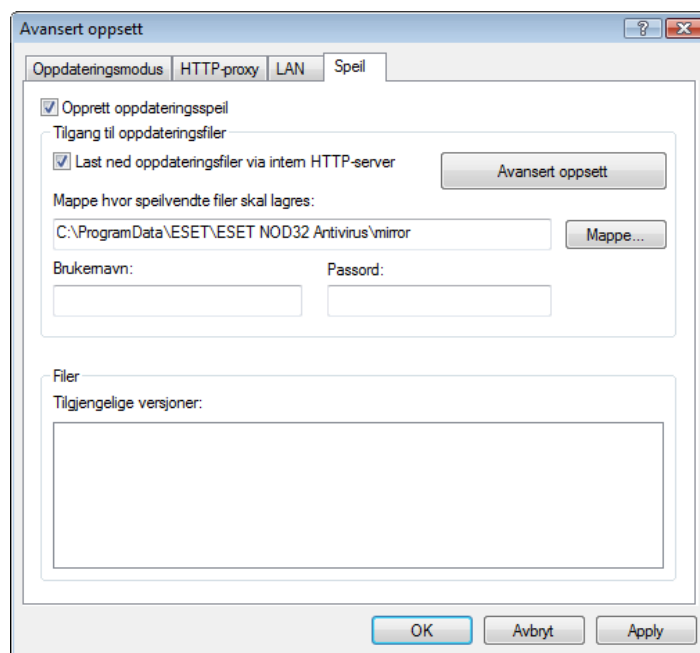
Advarsel:

Når enten **Gjeldende bruker** eller **Spesifisert bruker** er aktivert, kan det oppstå en feil ved endring av programmets identitet til den ønskede brukeren. Dette er grunnen til at vi anbefaler å legge inn godkjenningsdata for LAN i hovedoppdateringsoppsettet. I denne delen for oppdateringsoppsett skal godkjenningsdata angis som følger: domene_navn\bruker (hvis det er en arbeidsgruppe skriver du inn arbeidsgruppe_navn\navn) og brukerens passord. Ved oppdatering fra HTTP-versjonen av den lokale serveren er det ikke nødvendig med godkjenning.

4.2.1.2.4 Opprette oppdateringskopier – Speil

Med ESET NOD32 Antivirus Business Edition kan du opprette kopier av oppdateringsfiler som kan brukes til å oppdatere andre arbeidsstasjoner i nettverket. Oppdatering av klientarbeidsstasjoner fra en speilserver optimaliserer belastningsbalansen i nettverket og sparer båndbredde for Internett-tilgang.

Konfigurasjonsalternativene til den lokale speilserveren er tilgjengelige (etter å ha lagt inn en gyldig lisensnøkkel i Lisensbehandling, som er plassert i delen Avansert oppsett i ESET Smart Security Business Edition) i delen **Avansert oppsett for oppdatering**: (Du får tilgang til denne delen ved å trykke F5 og klikke **Oppdater** i treet Avansert oppsett. Klikk **Oppsett...** ved siden av **Avansert oppsett for oppdatering**, og velg kategorien **Speil**.)



Det første trinnet for å konfigurere speilserveren er å merke av for **Opprett oppdateringsspeil**. Når du merker dette alternativet, aktiveres andre alternativer for speilkonfigurasjon, som tilgangsmetode til oppdateringsfiler og oppdateringsbanen til speilede filer.

Metodene for aktivisering av speilservere er beskrevet detaljert i det neste kapittelet "Varianter av tilgang til speil". I denne omgangen kan du merke deg at det er to grunnleggende varianter av tilgang til speil – mappen med oppdateringsfiler kan presenteres av et speil som en delt nettverksmappe, eller som et speil på en HTTP-server.

Mappen som er dedikert til lagring av oppdateringsfiler for speilet, er definert i delen **Mappe hvor speilede filer skal lagres**. Klikk **Mappe...** for å bla gjennom en ønsket mappe på den lokale datamaskinen eller en delt nettverksmappe. Hvis det er nødvendig med godkjenning for den angitte mappen, må godkjenningsdata angis i feltene **Brukernavn** og **Passord**. Brukernavn og passord skal angis i formatet *Domene/Bruker* eller *Arbeidsgruppe/Bruker*. Husk å bruke riktig passord for brukernavnet som oppgis.

Når du angir detaljert speilkonfigurasjon, kan du også angi hvilken språkversjon du vil laste ned oppdateringskopier til. Oppsett for språkversjoner er tilgjengelig i delen **Filer - Tilgjengelige versjoner**.

4.2.1.2.4.1 Oppdatering fra speilet

Det er to grunnleggende måter å konfigurere speilet på – mappen med oppdateringsfiler kan presenteres som et speil av en delt nettverksmappe, eller som et speil av en HTTP-server.

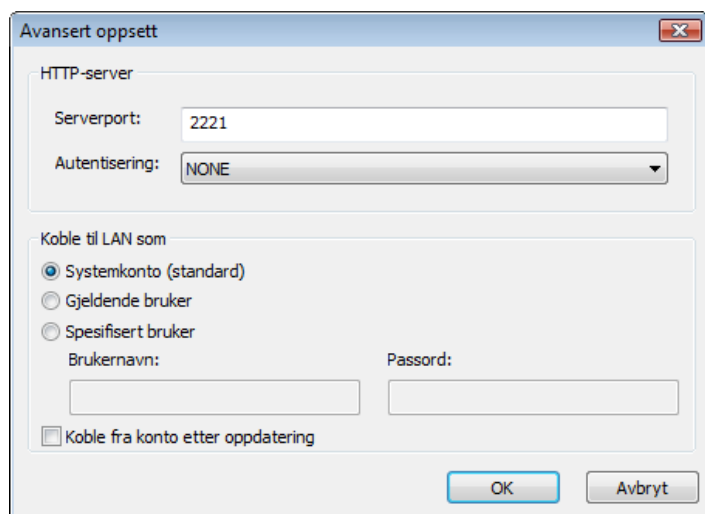
Tilgang til speilet med en intern HTTP-server

Dette er standardkonfigurasjonen som er spesifisert i den forhåndsdefinerte programkonfigurasjonen. For å gi tilgang til speilet ved hjelp av HTTP-serveren, går du til **Avansert oppsett for oppdatering** (kategorien **Speil**) og velger alternativet **Opprett oppdateringsspeil**.

I delen **Avansert oppsett** i kategorien **Spil** kan du angi hvilken **Serverport** HTTP-serveren skal lytte til, i tillegg til typen **Autentisering** HTTP-serveren skal bruke. Det er standard at serverporten er satt til verdien **2221**. Alternativet **Autentisering** definerer godkjenningssmetoden som blir brukt for å få tilgang til oppdateringsfilene. Følgende alternativer er tilgjengelige: **INGEN**, **Grunnleggende** og **NTLM**. Velg **Grunnleggende** for å bruke base64-kryptering med grunnleggende godkjenning av brukernavn og passord. Alternativet **NTLM** gir kryptering med en trygg krypteringsmetode. Brukeren som er opprettet på arbeidsstasjonen og som deler oppdateringsfilene, benyttes til godkjenning. Standardinnstillingen er **INGEN**, noe som gir tilgang til oppdateringsfilene uten behov for godkjenning.

Advarsel:

Hvis du vil tillate tilgang til oppdateringsfiler via HTTP-serveren, må spillmappen og ESET NOD32 Antivirus-eksemplaret som oppretter den, være på samme datamaskin.



Etter at konfigureringen av speilet er fullført, går du til arbeidsstasjonene og legger til en ny oppdateringsserver i formatet **http://IP_adresse_til_din_server:2221**. For å gjøre dette, følger du disse trinnene:

- Åpne **Avansert oppsett** for ESET NOD32 Antivirus, og klikk grenen **Oppdater**.
- Klikk **Rediger...** til høyre for rullegardinmenyen **Oppdater server**, og legg til en ny server med følgende format: **http://IP_adresse_til_din_server:2221**
- Velg denne nyopprettede serveren fra listen over oppdateringsservere.

Tilgang til speilet via systemdeler

Først må du opprette en delt mappe på en lokal stasjon eller nettverksstasjon. Når du oppretter mappen for speilet, må du gi skrivetilgang til brukeren som skal lagre oppdateringsfiler i mappen og lesetilgang til alle brukere som skal oppdatere ESET NOD32 Antivirus fra spillmappen.

Deretter konfigurerer du tilgang til speilet i delen **Avansert oppsett for oppdatering** (kategorien **Spil**) ved å deaktivere alternativet **Last ned oppdateringsfiler via intern HTTP-server**. Det er standard at dette alternativet er aktivert i programinstallasjonspakken.

Hvis den delte mappen ligger på en annen datamaskin i nettverket, må du angi godkjenningsdata for å få tilgang til den andre datamaskinen. Når du skal angi godkjenningsdata, åpner du Avansert oppsett (F5) i ESET NOD32 Antivirus og klikker grenen **Oppdater**. Klikk **Oppsett...** og deretter kategorien **LAN**. Denne innstillingen er den samme som for oppdatering, som er beskrevet i kapitlet "Koble til LAN".

Etter at speilkonfigurasjonen er fullført, fortsetter du med arbeidsstasjonene og angir **\\UNC\BANE** som oppdateringsserver. Du fullfører denne operasjonen ved hjelp av følgende trinn:

- Åpne Avansert oppsett i ESET NOD32 Antivirus, og klikk **Oppdater**.
- Klikk **Rediger...** ved siden av oppdateringsserveren, og legg til en ny server med formatet **\\UNC\BANE**.
- Velg denne nyopprettede serveren fra listen over oppdateringsservere.

MERK: For at alt skal fungere riktig, må banen til spillmappen være angitt som en UNC-bane. Det er ikke sikkert at oppdateringer fra nettverksstasjonene vil fungere.

4.2.1.2.4.2 Feilsøking av oppdateringsproblemer med spil

Avhengig av hvilken metode som er brukt til å få tilgang til spillmappen, kan det oppstå forskjellige typer problemer. I de fleste tilfeller blir problemer som oppstår under en oppdatering fra en speilserver, forårsaket av en eller flere av følgende faktorer: Feil angivelse av alternativer for spillmappe, feil godkjenningsdata til spillmappen, feil konfigurering på lokale arbeidsstasjoner som prøver å laste ned oppdateringsfiler fra speilet, eller en kombinasjon av årsakene. Her gir vi en oversikt over de vanligste problemene som kan oppstå ved oppdatering fra speilet:

- **ESET NOD32 Antivirus rapporterer en feil ved tilkobling til speilserveren** – sannsynligvis forårsaket av feil angivelse av oppdateringsserveren (feil nettverksbane til spillmappen) som den lokale arbeidsstasjonen laster ned oppdateringer fra. Hvis du vil kontrollere banen, klikker du **Start** og deretter **Kjør** i Windows, skriver inn mappenavnet og klikker **OK**. Innholdet i mappen skal vises.
- **ESET NOD32 Antivirus krever brukernavn og passord** – sannsynligvis forårsaket av feil angivelse av godkjenningsdata (brukernavn og passord) i oppdateringsdelen. Brukernavn og passord brukes for å gi tilgang til oppdateringsserveren som programmet oppdateres fra. Forsikre deg om at godkjenningsdataene er riktige og angitt i riktig format. For eksempel *Domenet/brukernavn* eller *Arbeidsgruppe/brukernavn* sammen med riktig passord for brukernavnet. Hvis speilserveren er tilgjengelig for "Alle", må du være klar over at dette ikke betyr at en hvilken som helst bruker får tilgang. "Alle" betyr ikke uautoriserte brukere, det betyr bare at mappen er tilgjengelig for alle brukerne av domenet. Brukerne må oppgi brukernavn og passord i delen for oppdateringsoppsett, selv om mappen er tilgjengelig for "Alle".
- **ESET NOD32 Antivirus rapporterer en feil ved tilkobling til speilserveren** – kommunikasjon via porten som er definert for tilgang til HTTP-versjonen av speilet, er blokkert.

4.2.2 Slik lager du oppdateringsoppgaver

Oppdateringer kan utløses manuelt ved å klikke **Oppdater virussignatordatabase** i informasjonsvinduet som vises etter at du har klikket **Oppdater** på hovedmenyen.

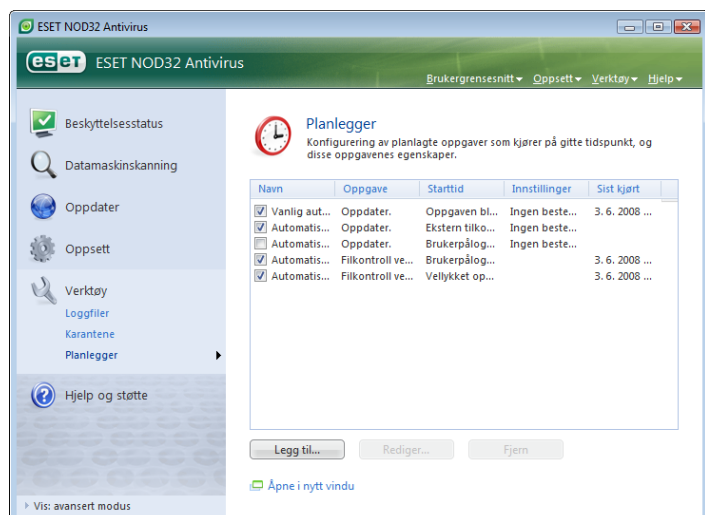
Oppdateringer kan også kjøres som planlagte oppgaver. Du konfigurerer en planlagt oppgave ved å klikke **Verktøy > Planlegger**. Det er standard at følgende oppgaver blir aktivert i ESET Smart Security:

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

Hver av oppdateringsoppgavene som er nevnt ovenfor, kan endres slik at de dekker dine behov. I tillegg til å bruke de standardiserte oppdateringsoppgavene, kan du opprette nye oppdateringsoppgaver med en brukerdefinert konfigurasjon. For mer detaljert informasjon om hvordan du oppretter og konfigurerer oppdateringsoppgaver, les kapittelet "Planlegger".

4.3 Planlegger

Planlegger er tilgjengelig hvis Avansert modus i ESET NOD32 Antivirus er aktivert. Du finner **Planlegger** under **Verktøy** på hovedmenyen i ESET NOD32 Antivirus. Planlegger inneholder en liste over alle planlagte oppgaver og tilhørende konfigurasjonsegenskaper, for eksempel forhåndsdefinert dato, klokkeslett og brukt skanneprofil.



Standardinnstillingen viser følgende planlagte oppgaver i **Planlegger**:

- **Vanlig automatisk oppdatering**
- **Automatisk oppdatering etter oppringt tilkobling**
- **Automatisk oppdatering etter brukerpålogging**
- **Automatisk filkontroll ved oppstart etter at brukeren har logget seg på**
- **Automatisk filkontroll ved oppstart etter en vellykket oppdatering av virussignatordatabasen**

Når du skal redigere konfigurasjonen til en allerede planlagt oppgave (enten standard eller brukerdefinert), høyreklikker du oppgaven og klikker **Rediger...** eller velger oppgaven du ønsker å endre, og klikker **Rediger...**

4.3.1 Formålet med å planlegge oppgaver

I Planlegger administreres og startes planlagte oppgaver med forhåndsdefinert konfigurasjon og forhåndsdefinerte egenskaper. Konfigurasjonen og egenskapene inneholder informasjon, som dato og klokkeslett, i tillegg til angitte profiler som skal brukes til å utføre oppgaven.

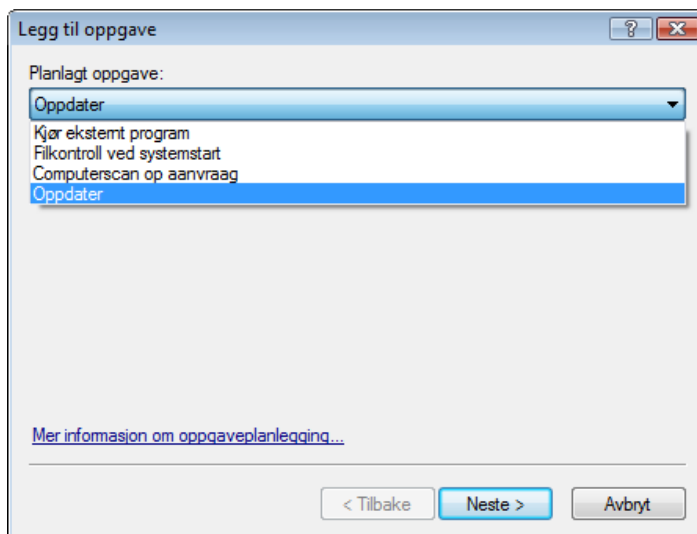
4.3.2 Opprette nye oppgaver

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

- **Kjør eksternt program**
- **Loggvedlikehold**
- **Filkontroll ved systemstart**

■ Datamaskinskanning etter behov

■ Oppdater



Ettersom **Datamaskinskanning etter behov** og **Oppdater** er de mest brukte planlagte oppgavene, vil vi forklare hvordan du legger til en ny oppdateringsoppgave.

På rullegardinmenyen **Planlagt oppgave:** velger du **Oppdater**. Klikk **Neste**, og skriv inn navnet på oppgaven i feltet **Navn på oppgave**. Velg hvor ofte oppgaven skal utføres. Følgende alternativer er tilgjengelige: **En gang**, **Gjentatte ganger**, **Daglig**, **Ukentlig** og **Utløst av handling**. Du kan du velge mellom ulike oppdateringsparametere på bakgrunn av hvilket valg du har angitt. Deretter definerer du hva som skal skje hvis oppgaven ikke kan utføres eller fullføres til planlagt tid. Følgende tre alternativer er tilgjengelige:

- Vent til neste planlagte tidspunkt
- Kjør oppgaven så snart som mulig
- Kjør oppgaven umiddelbart hvis tiden siden forrige utførelse overskrider angitt intervall. (Intervall kan defineres umiddelbart ved hjelp av rulleboksen Oppgaveintervall.)

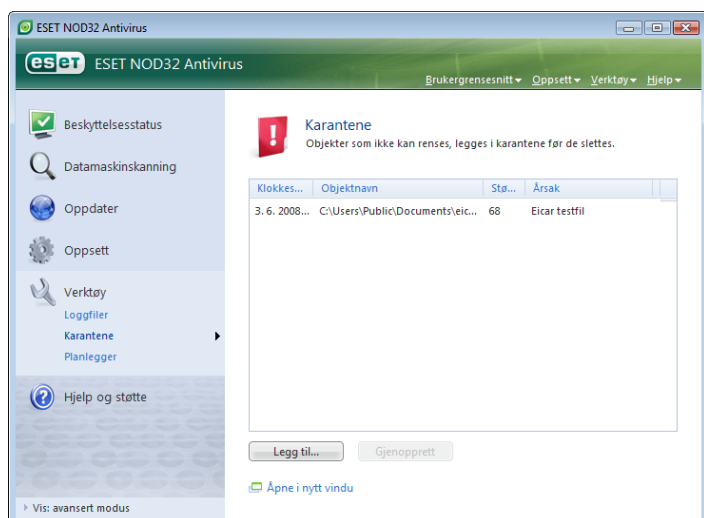
I neste trinn vises et sammendragsvindu med informasjon om den gjeldende planlagte oppgaven. Alternativet **Kjør oppgave med bestemte parametere** må aktiveres automatisk. Klikk **Fullfør**.

Et dialogvindu vises der du kan velge profilene som skal brukes til den planlagte oppgaven. Her kan du angi en primær og alternativ profil, som blir brukt hvis oppgaven ikke kan utføres med den primære profilen. Bekreft ved å klikke OK i vinduet **Oppdater profiler**. Den nye planlagte oppgaven blir lagt til listen over gjeldende planlagte oppgaver.

4.4 Karantene

Hovedoppgaven 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 er feilaktig gjenkjent av ESET Smart Security.

Brukeren kan velge å legge en hvilken som helst fil i karantene. Dette anbefales hvis en fil oppfører seg mistenkelig, men ikke oppdages av viruskanneren. Filer som er lagt i karantene, kan sendes til ESETs viruslaboratorier for analyse.



Filer som er lagret i karanteneappen, kan vises i en tabell som viser dato og klokkeslett for karantenen, banen til den opprinnelige plasseringen av den infiserte filen, størrelse i byte, årsak (**lagt til av bruker...**), og antall trusler (for eksempel hvis det er et arkiv som inneholder flere infiltrasjoner).

4.4.1 Legge filer i karantene

Programmet legger automatisk slettede filer i karantene (hvis du ikke har avbrutt dette alternativet i varselvinduet). Hvis du vil, kan du manuelt legge mistenkelige filer i karantene ved å klikke **Legg til...** Hvis dette gjøres, blir ikke den opprinnelige filen fjernet fra den opprinnelige plasseringen. Hurtigmenyen kan også brukes til dette formålet – høyreklikk i karantenevinduet, og velg **Legg til...**

4.4.2 Gjenopprette fra karantene

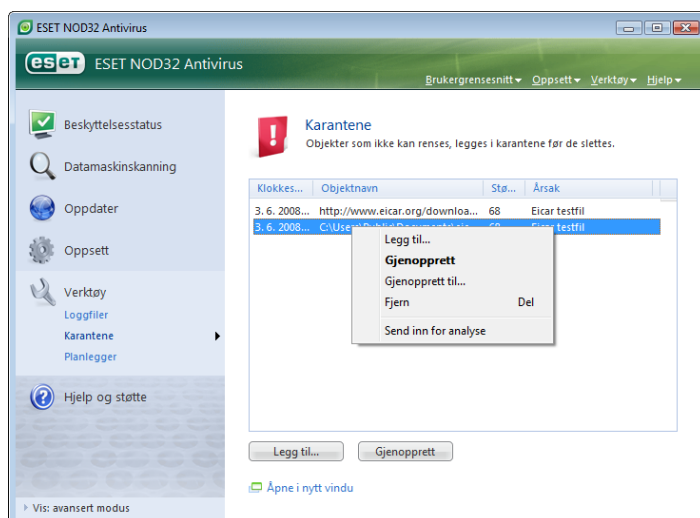
Filer som er lagt i karantene, kan også gjenopprettes til den opprinnelige plasseringen. Bruk funksjonen **Gjenopprett** til dette formålet. Funksjonen er tilgjengelig fra hurtigmenyen ved å høyreklikke en fil i karantenevinduet. På hurtigmenyen finner du også alternativet **Gjenopprett til**, som du kan bruke til å gjenopprette en fil til en annen plassering enn den plasseringen filen ble slettet fra.

MERK:

Hvis programmet ved en feiltakelse legger en harmløs fil i karantene, kan du utelate filen fra skanning etter gjenoppretting og sende filen til ESETs brukerstøtte.

4.4.3 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 evaluert som infisert (for eksempel ved heuristisk analyse av koden) og deretter lagt i karantene, ber vi deg om å sende filen til ESETs viruslaboratorium. Når du skal sende inn en fil som ligger i karantene, høyreklikker du filen og velger **Send inn til analyse** fra hurtigmenyen.

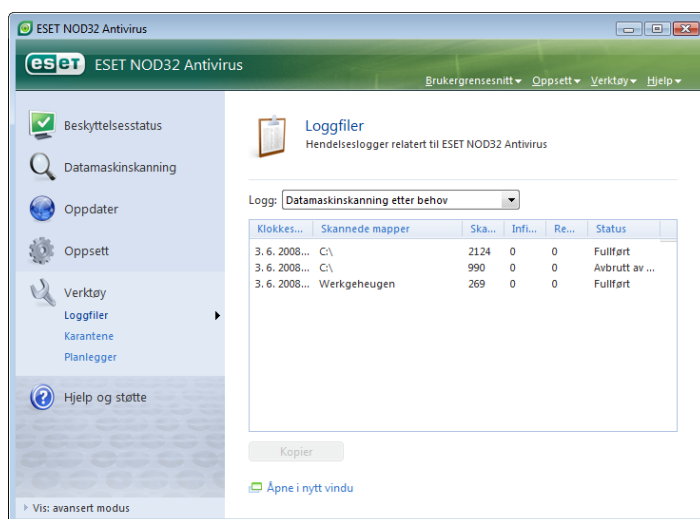


4.5 Loggfiler

Loggfilene inneholder informasjon om alle viktige programhendelser som har skjedd, og gir en oversikt over trusler som er oppdaget. Loggføring er et viktig verktøy ved systemanalyse, trusselgjenkjenning og feilsøking. Loggføring utføres aktivt i bakgrunnen uten at brukeren trenger å foreta seg noe. Informasjon registreres basert på gjeldende innstillinger for detaljnivå i loggen. Det er mulig å se tekstmeldinger, logger og arkivlogger direkte fra ESET NOD32 Antivirus-miljøet.

Loggfiler er tilgjengelige fra hovedvinduet i ESET NOD32 Antivirus ved å klikke **Verktøy > Loggfiler**. Velg ønsket loggtype ved hjelp av rullegardinmenyen **Logg**: øverst i vinduet. Følgende loggtyper er tilgjengelige:

1. **Trusler som er oppdaget** – bruk dette alternativet til å vise all informasjon om hendelser som gjelder oppdagelse av infiltrasjoner.
2. **Hendelser** – dette alternativet er utformet for å hjelpe systemadministratorer og brukere med å løse problemer. Alle viktige handlinger som blir utført av ESET NOD32 Antivirus, blir registrert i hendelseslogger.
3. **Datamaskinskanning etter behov** – resultatene fra alle fullførte skanninger vises i dette vinduet. Dobbeltklikk en oppføring hvis du vil se detaljert informasjon om en skanningen etter behov.

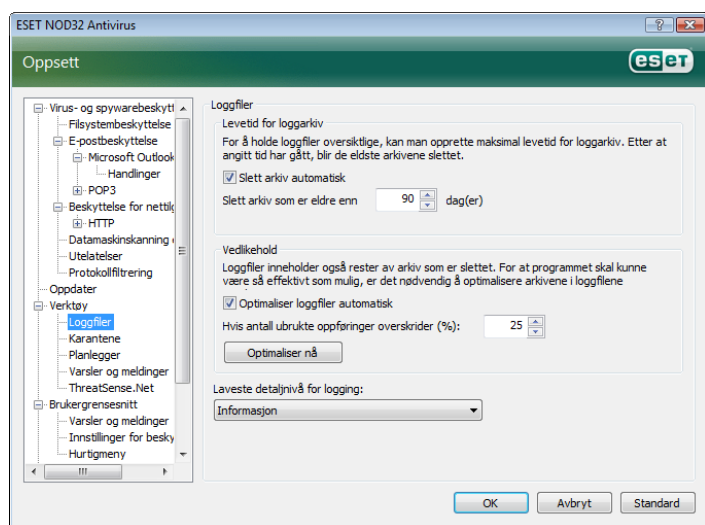


I hver del kan den viste informasjonen kopieres direkte til utklippstavlen ved å merke de ønskede oppføringene og klikke **Kopier**. Når du skal velge flere oppføringer, kan du bruke CTRL- og SKIFT-tastene.

4.5.1 Loggvedlikehold

Du finner loggkonfigurasjon for ESET NOD32 Antivirus i hovedprogramvinduet. Klikk **Oppsett > Legg inn hele treet for avansert oppsett...** > **Verktøy > Loggfiler**. Du kan angi følgende alternativer for loggfiler:

- **Slett arkiv automatisk:** Loggoppføringer som er eldre enn angitt antall dager, blir automatisk slettet.
- **Optimaliser loggfiler automatisk:** Aktiverer automatisk defragmentering av loggfiler hvis den angitte prosentandelen av ubrukte oppføringer er overskredet.
- **Laveste detaljnivå for logging:** Angir detaljnivået for logger. Alternativer som er tilgjengelig:
 - **Kritiske feil** – logger alle kritiske feil (feil som starter virusbeskyttelsen osv.)
 - **Feil** – bare meldinger av typen "Feil under nedlasting av fil" blir registrert, pluss kritiske feil.
 - **Advarsler** – logger alle kritiske feil og varselmeldinger.
 - **Informasjonsarkiv** – registrerer alle informasjonsmeldinger, inkludert meldinger om vellykkede oppdateringer og alle loggene ovenfor.
 - **Diagnosearkiv** – logger all informasjon som er nødvendig for fininnstilling- av programmet, og alle loggene ovenfor.



4.6 Brukergrensesnitt

Du kan endre konfigurasjonsalternativene for brukergrensesnittet i ESET NOD32 Antivirus for å få et arbeidsmiljø som er tilpasset dine behov. Disse konfigurasjonsalternativene er tilgjengelige fra grenen **Brukergrensesnitt** i treet Avansert oppsett i ESET NOD32 Antivirus.

I delen **Brukergrensesnittelementer** kan brukere bytte til Avansert modus om de ønsker det. Avansert modus viser flere detaljerte innstillinger og flere av kontrollene i ESET Smart Security.

Alternativet **Grafisk brukergrensesnitt** bør deaktiveres hvis de grafiske elementene reduserer ytelsen til maskinen, eller forårsaker andre problemer. Det kan også være at det grafiske grensesnittet bør slås av for svaksynte brukere, fordi det kan komme i konflikt med spesialprogrammer som brukes til lesing av tekst på skjermen.

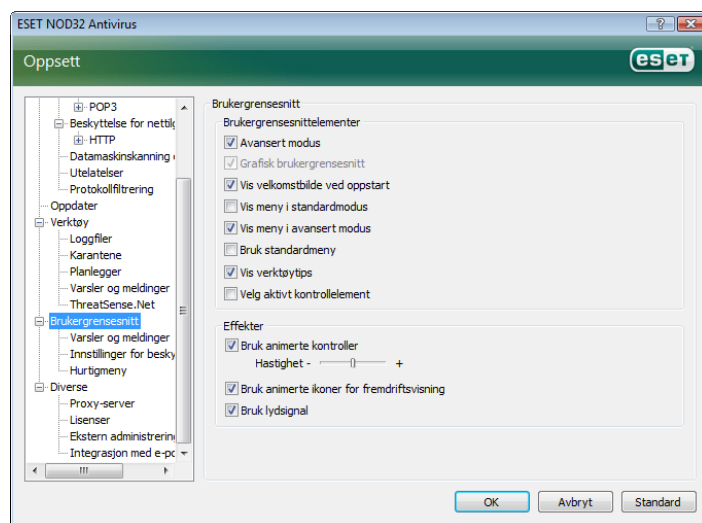
Hvis du vil deaktivere velkomstbildet i ESET NOD32 Antivirus, deaktiverer du alternativet **Vis velkomstbilde ved oppstart**.

Øverst i hovedprogramvinduet i ESET NOD32 Antivirus finner du en standardmeny som du kan aktivere eller deaktivere basert på alternativet **Bruk standardmeny**.

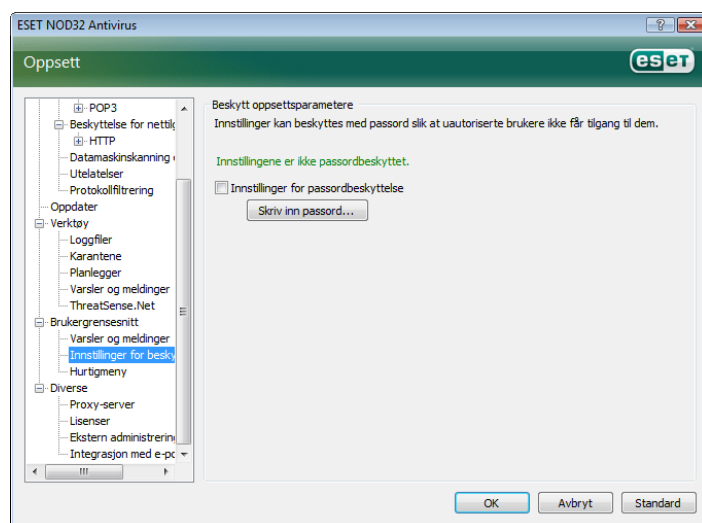
Hvis alternativet **Vis verktøytips** er aktivert, vises en kort beskrivelse av alle alternativene når musepekeren plasseres over alternativet. Med alternativet **Velg aktivt kontrollelement** markerer systemet elementer som er under det aktive området til musepekeren. Det markerte elementet blir aktivert ved et museklikk.

Hvis du vil redusere eller øke hastigheten til animerte effekter, velger du alternativet **Bruk animerte kontroller** og flytter glidebryteren **Hastighet** mot venstre eller høyre.

Hvis du vil aktivere bruken av animerte ikoner for å vise fremdriften til ulike operasjoner, merker du av for **Bruk animerte ikoner...** Hvis du vil at programmet skal avgi en varsellyd når en viktig hendelse finner sted, velger du alternativet **Bruk lydsignal**.



Funksjonen **Brukergrensesnitt** inneholder også muligheten til å passordbeskytte oppsettparametrene i ESET NOD32 Antivirus. Dette alternativet finner du på undermenyen **Beskyttelse av innstillinger** under **Brukergrensesnitt**. For at programmet skal kunne beskytte systemet ditt maksimalt, er det helt avgjørende at det er riktig konfigurert. Feilaktige endringer kan føre til tap av viktige data. Hvis du vil angi et passord som beskytter oppsettparametrene, klikker du **Skriv inn passord...**



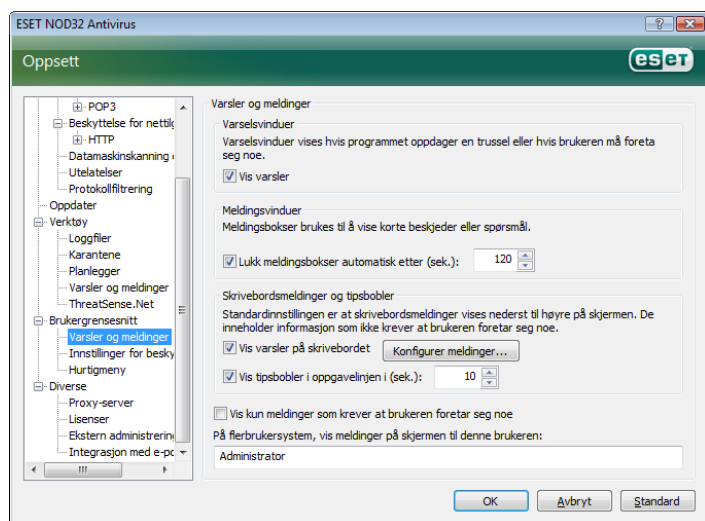
4.6.1 Varsler og meldinger

I delen **Oppsett av varsler og meldinger** under **Brukergrensesnitt** kan du konfigurere hvordan varselmeldinger og systemmeldinger skal behandles i ESET Smart Security.

Det første elementet er **Vis varsler**. Hvis du deaktiverer dette alternativet, vil det ikke bli vist noen varselvinduer. Dette passer bare i helt spesielle situasjoner. For de fleste brukere anbefaler vi at standardinnstillingen (aktivert) benyttes for dette alternativet.

Hvis du vil lukke popup-vinduer automatisk etter en bestemt tid, velger du alternativet **Lukk meldingsbokser automatisk etter (sek.)**. Hvis varselvinduer ikke lukkes manuelt av brukeren, blir de lukket automatisk etter at den angitte tiden har utløpt.

Meldinger på skrivebordet og tipsbøler er kun til informasjon og krever ingen handling fra brukeren. De vises i meldingsområdet nederst i høyre hjørne på skjermen. Hvis du vil aktivere visning av varsler på skrivebordet, velger du alternativet **Vis varsler på skrivebordet**. Du kan endre mer detaljerte alternativer – visningstiden for skrivebordsmeldinger og vindusgjennomsiktigheten – ved å klikke **Konfigurer meldinger...** Hvis du vil se hvordan varslene ser ut, klikker du **Forhåndsvisning**. Hvis du vil konfigurere hvor lenge tipsbølene skal vises, går du til alternativet **Vis tipsbøler i oppgavelinjen i (sek.)**.



I den nedre delen av oppsettvinduet **Varsler og meldinger** finnes alternativet **Vis kun meldinger, som krever at brukeren foretar seg noe**. Med dette alternativet kan du slå av og på visning av varsler og meldinger som ikke krever at brukeren foretar seg noe. Den siste funksjonen i denne delen spesifiserer adresser for meldinger i et flerbrukersystem.

I feltet **På flerbrukersystem, vis meldinger på skjermen til denne brukeren:** kan du definere hvem som skal motta viktige meldinger fra ESET Smart Security. Dette vil normalt være en systemansvarlig eller en nettverksansvarlig. Dette alternativet er spesielt nyttig for terminalservere hvis alle systemmeldinger sendes til den systemansvarlige.

4.7 ThreatSense.Net

Varslingssystemet ThreatSense.Net er et verktøy som kontinuerlig og umiddelbart informerer ESET om nye infiltrasjoner. Varslingssystemet ThreatSense.Net for toveistrafikk har ett mål – å forbedre beskyttelsen som vi kan tilby deg. Den beste måten å sikre at vi ser nye trusler så snart de vises, er å "koble oss" til så mange av våre kunder som mulig og bruke dem som trusselspeidere. Du har disse to alternativene:

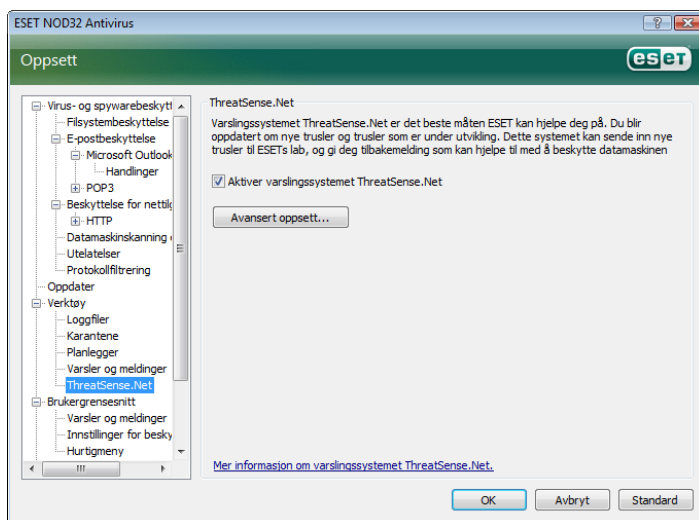
- Du kan bestemme deg for ikke å aktivere varslingssystemet ThreatSense.Net. Du mister ikke funksjonalitet i programvaren, og du får fremdeles den beste beskyttelsen som vi kan tilby.

- Du kan konfigurere varslingssystemet til å sende inn anonym informasjon om nye trusler og hvor den nye trusselkoden ligger, i en enkelt fil. Denne filen kan sendes til ESET for detaljert analyse. Ved å studere disse truslene kan ESET oppdatere sine muligheter for trusselgjenkjenning. Varslingssystemet ThreatSense.Net samler inn informasjon om datamaskinen din som er knyttet til nyoppdagede trusler. Denne informasjonen kan inkludere et eksempel eller en kopi av filen som trusselen ble oppdaget i, banen til den filen, filnavnet, informasjon om dato og klokkeslett, prosessen som trusselen viste seg i på datamaskinen, og informasjon om datamaskinens operativsystem. Noe av denne informasjonen kan inneholde personlig informasjon om brukeren av datamaskinen, for eksempel brukernavn i en katalogbane. Et eksempel på filinformasjonen som blir sendt inn, er tilgjengelig her.

Selv om det er en mulighet for at dette noen ganger kan overføre noe informasjon om deg eller datamaskinen til ESETs trussellaboratorium, blir ikke denne informasjonen brukt til andre formål enn å hjelpe oss med å reagere på nye trusler så raskt som mulig.

Standardinnstillingen er at ESET NOD32 Antivirus spør før det sender mistenkelige filer til ESETs trussellaboratorium for analyse. Du bør merke deg at filer med bestemte filendelser, for eksempel doc og xls, alltid er utelatt fra innsending hvis det oppdages en trussel i dem. Du kan også legge til andre filendelser hvis det er spesielle filer som du eller organisasjonen din vil unngå å sende inn.

Oppsettet av ThreatSense.Net er tilgjengelig fra treet Avansert oppsett under **Verktøy > ThreatSense.Net**. Merk av for **Aktiver varslingssystemet ThreatSense.Net**. Dermed kan du aktivere og deretter klikke **Avansert oppsett...**

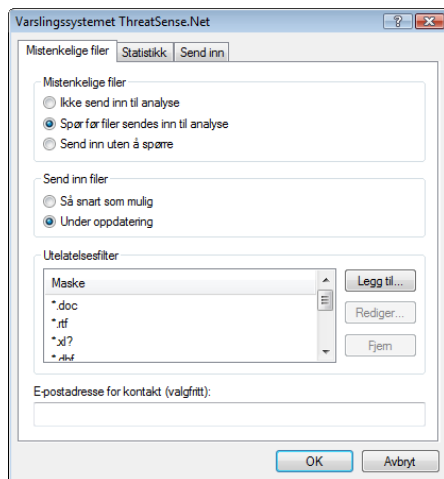


4.7.1 Mistenkelige filer

I kategorien **Mistenkelige filer** kan du konfigurere hvordan trusler skal sendes til ESETs viruslaboratorium for analyse.

Hvis du har funnet en mistenkelig fil, kan du sende den inn til ESETs viruslaboratorium for analyse. Hvis det viser seg å være et skadelig program, blir gjenkjenningen av dette lagt til i neste virussignaturoppdatering.

Innsending av filer kan utføres automatisk uten at du blir spurt. Hvis du velger dette alternativet, blir mistenkelige filer sent inn i bakgrunnen. Hvis du vil vite hvilke filer som er sendt inn til analyse, og bekrefte innsendingen, velger du alternativet **Spør før innsending**.



Hvis du ikke vil sende inn noen filer, velger du **Ikke send inn til analyse**. Vær oppmerksom på at hvis du velger ikke å sende inn noen filer til analyse, påvirker det ikke innsending av statistisk informasjon til ESET. Statistisk informasjon konfigureres i en egen oppsettdel som beskrives i neste kapittel.

Send inn filer

Mistenkelige filer blir sendt til ESETs viruslaboratorium for analyse så snart som mulig. Dette alternativet anbefales hvis du har en permanent Internett-tilkobling, og mistenkelige filer kan sendes inn uten forsinkelse. Det andre alternativet er å sende inn mistenkelige filer ved å velge **Under oppdatering**. Hvis du velger dette alternativet, bli mistenkelige filer samlet og lastet opp til varslingssystemserverne under en oppdatering.

Utelatelsesfilter

Det er ikke nødvendig å sende inn alle filer til analyse. Hvis du bruker utelatelsesfiltret, kan du utelate enkelte filer og mapper fra innsending. Det kan for eksempel være fornuftig å utelate filer som kan inneholde konfidensiell informasjon, for eksempel dokumenter og regneark. De vanligste filtypene er utelatt som standard (Microsoft Office, OpenOffice). Listen over utelatte filer kan utvides hvis det er ønskelig.

E-postadresse for kontakt

E-postadressen for kontakt sendes sammen med mistenkelige filer til ESET. Adressen kan brukes til å kontakte deg hvis det er nødvendig å innhente flere opplysninger om sendte filer, til analysen. Legg merke til at du ikke vil få svar fra ESET hvis det ikke er nødvendig med flere opplysninger.

4.7.2 Statistikk

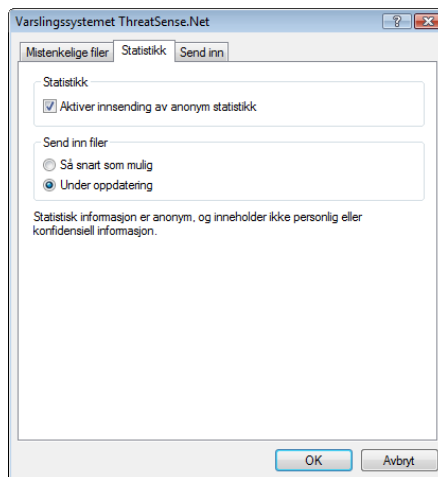
Varslingssystemet ThreatSense.Net samler inn informasjon om datamaskinen din som er knyttet til nyoppdagede trusler. Denne informasjonen kan omfatte navnet på infiltreringen, opplysninger om dato og klokkeslett da trusselen ble oppdaget, versjonen av ESET NOD32 Antivirus, informasjon om datamaskinens operativsystem og plasseringsinnstillingen. Statistikken leveres normalt til ESETs servere én eller to ganger daglig.

Her er et eksempel på en innsendt statistikkpakke:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

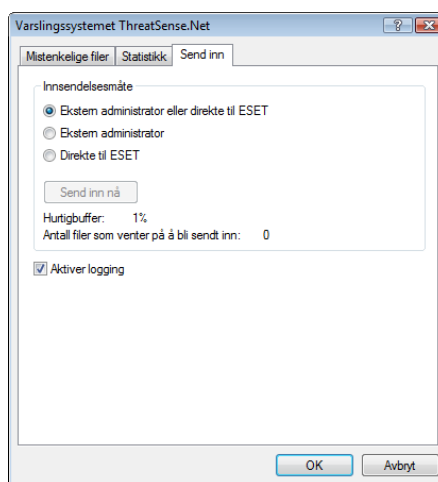
Send inn filer

I delen **Send inn filer** kan du definere når den statistiske informasjonen skal sendes inn. Hvis du velger **Så snart som mulig**, blir statistisk informasjon sendt inn så snart som mulig etter at den er opprettet. Denne innstillingen passer hvis du har en permanent Internett-tilkobling. Hvis du velger **Under oppdatering**, blir statistisk informasjon beholdt og sendt inn samlet under neste oppdatering.



4.7.3 Innsending

I denne delen kan du velge om filer og statistisk informasjon skal sendes inn ved hjelp av ESET Ekstern administrator eller direkte til ESET. Hvis du vil være sikker på at mistenkelige filer og statistisk informasjon blir levert til ESET, velger du alternativet **Ekstern administrator eller direkte til ESET**. Hvis du velger dette alternativet, blir alle filer og all statistikk sendt med alle tilgjengelige hjelpemidler. Når mistenkelige filer sendes inn ved hjelp av Ekstern administrator, sendes filer og statistikk til serveren for ekstern administrering. Dette sikrer videresending til ESETs viruslaboratorier. Hvis du har valgt alternativet **Direkte til ESET**, blir alle mistenkelige filer og all statistisk informasjon sendt til ESETs viruslaboratorium direkte fra programmet.



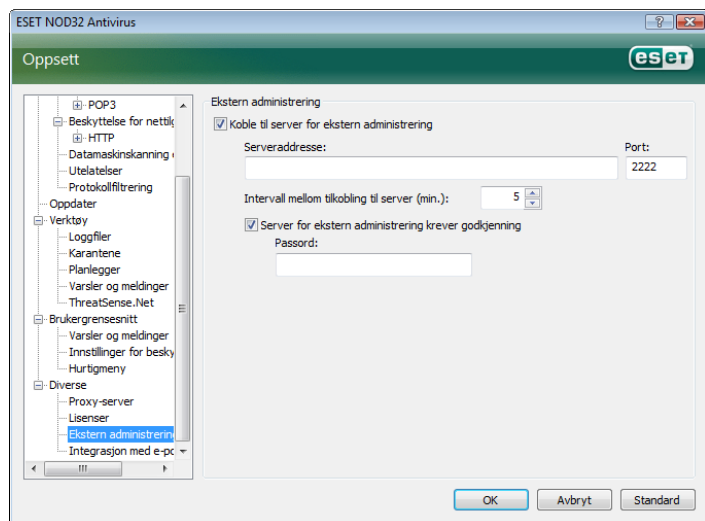
Når du har filer som venter på å bli sendt inn, er knappen **Send inn nå** aktivert i dette oppsettvinduet. Klikk denne knappen hvis du vil sende inn filer og statistisk informasjon med en gang.

Merk alternativet **Aktiver logging** for å aktivere registrering av innsending av filer og statistisk informasjon. Etter hver innsending av en mistenkelig fil eller statistisk informasjon, blir det opprettet en post i hendelsesloggen.

4.8 Ekstern administrering

Ekstern administrering er et kraftig verktøy for å vedlikeholde retningslinjer for sikkerhet og for å få oversikt over den generelle sikkerhetshåndteringen i nettverket. Ekstern administrering er spesielt nyttig for større nettverk. Ekstern administrering gir ikke bare økt sikkerhetsnivå, men det gjør også ESET NOD32 Antivirus enklere å bruke på klientarbeidsstasjoner.

Oppsettalternativene for Ekstern administrering er tilgjengelige fra hovedprogramvinduet i ESET NOD32 Antivirus. Klikk **Oppsett > Legg inn hele treet for avansert oppsett... > Diverse > Ekstern administrering**.



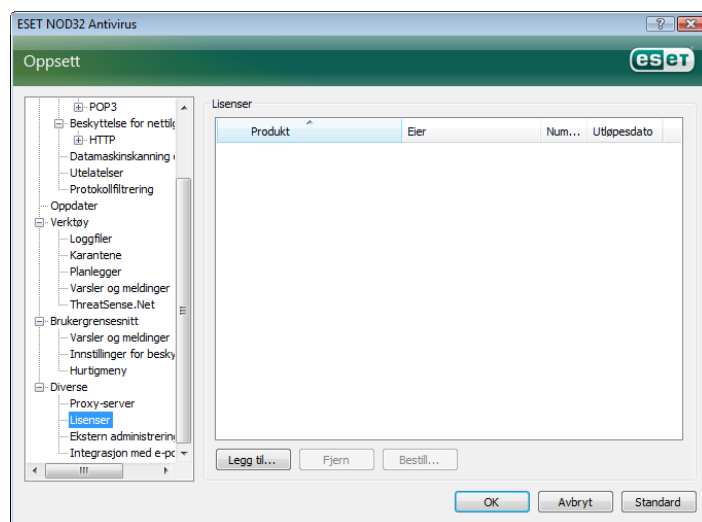
I oppsettsvinduet kan du aktivere modus for ekstern administrering. Dette oppnår du ved først å velge **Koble til server for ekstern administrering**. Du får deretter tilgang til de andre alternativene som er beskrevet nedenfor:

- **Serveradresse** – nettverksadressen til serveren, der serveren for ekstern administrering er installert.
- **Port** – dette feltet inneholder en forhåndsdefinert serverport som brukes til tilkobling. Vi anbefaler at du beholder den forhåndsdefinerte portinnstillingen 2222.
- **Intervall mellom tilkobling til server (min.)** – dette angir hvor ofte ESET NOD32 Antivirus vil koble til serveren for ekstern administrering for å sende data. Med andre ord blir informasjonen sendt etter tidsintervallene som er definert her. Hvis 0 er angitt, blir informasjon sendt hvert 5. sekund.
- **Server for ekstern administrering krever godkjenning** – du kan angi et passord for tilkobling til serveren for ekstern administrering.

Klikk **OK** hvis du vil bekrefte endringene og ta i bruk innstillingene. ESET NOD32 Antivirus bruker disse innstillingene til å koble til den eksterne serveren.

4.9 Lisens

Ved hjelp av grenen **Lisenser** kan du administrere lisensnøkler for ESET NOD32 Antivirus og andre ESET-produkter. Når du har kjøpt produktet, får du lisensnøklerne, brukernavn og passord. Hvis du vil legge til eller fjerne en lisensnøkkel, klikker du den tilsvarende knappen i lisensbehandlingsvinduet. Lisensbehandling er tilgjengelig fra treet Avansert oppsett under **Diverse > Lisenser**.



Lisensnøkkelen er en tekstfil som inneholder følgende opplysninger om det kjøpte produktet: eier, antall lisenser og utløpsdato.

I vinduet Lisensbehandling kan du laste opp og se på innholdet i en lisensnøkkel ved hjelp av **Legg til...** Opplysningene blir vist i Lisensbehandling. Hvis du vil slette lisensfiler fra listen, klikker du **Fjern**.

Hvis en lisensnøkkel har utløpt og du vil kjøpe en fornyet utgave, klikker du **Bestill...**, – slik at du kommer til vår butikk på Internett.

5. Avansert bruker

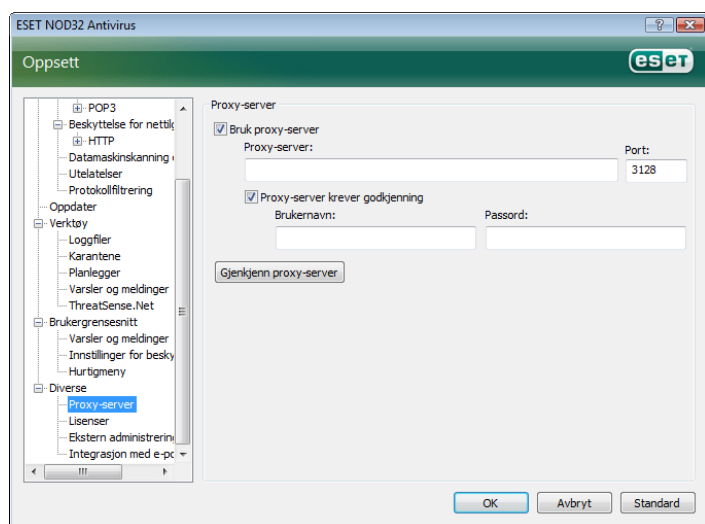
I dette kapittelet beskrives funksjonene i ESET NOD32 Antivirus, som kan være nyttige for mer avanserte brukere. Oppsettsalternativene for disse funksjonene er bare tilgjengelige i Avansert modus. Hvis du vil bytte til Avansert modus, klikker du **Bytt til avansert modus** nederst i venstre hjørnet av hovedvinduet, eller trykker CTRL + M på tastaturet.

5.1 Oppsett av proxy-server

I ESET Smart Security er oppsett av proxy-server tilgjengelig i to ulike deler i treet Avansert oppsett.

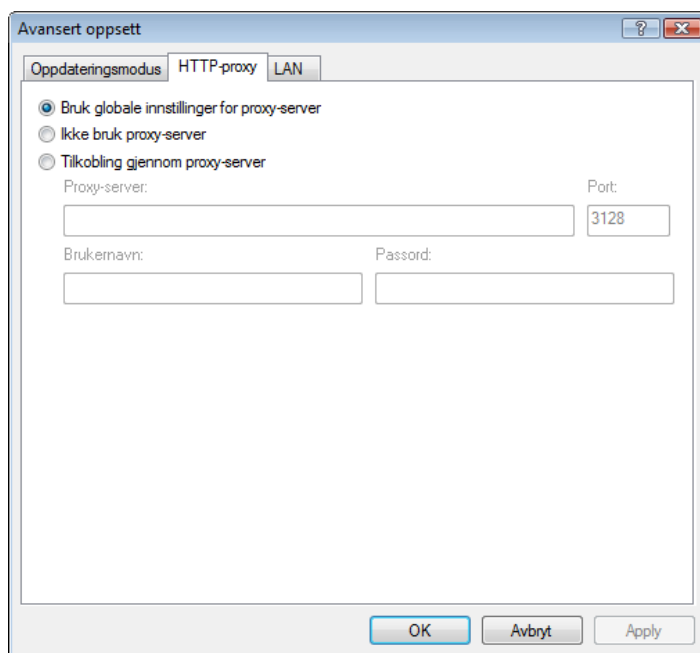
For det første kan innstillinger for proxy-server konfigureres under **Diverse > Proxy-server**. Hvis du angir proxy-serveren på dette nivået, defineres globale innstillinger for proxy-server for hele ESET Smart Security. Disse parameterne blir brukt av alle modulene som krever tilkobling til Internett.

Hvis du vil angi innstillinger for proxy-server for dette nivået, merker du av for **Bruk proxy-server** og oppgir deretter adressen til proxy-serveren i feltet **Proxy-server**: Angi også portnummeret til proxy-serveren i feltet **Port**.



Hvis kommunikasjon med proxy-serveren krever godkjenning, merker du av for **Proxy-server krever godkjenning** og oppgir gyldig informasjon i feltene **Brukernavn** og **Passord**. Klikk **Gjenkjenn proxy-server** for automatisk å gjenkjenne og sette inn innstillinger for proxy-server. Parameterne som er angitt i Internet Explorer, blir kopiert. Vær oppmerksom på at denne funksjonen ikke henter godkjenningsdata (brukernavn og passord). Disse må oppgis av brukeren.

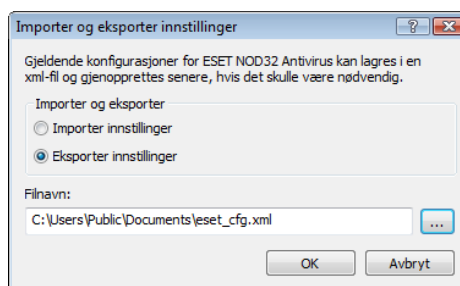
Innstillinger for proxy-server kan også angis i **Avansert oppsett for oppdatering** (grenen **Oppdater** i treet Avansert oppsett). Denne innstillingen gjelder en gitt oppdateringsprofil og anbefales for bærbare datamaskiner, fordi disse maskinene ofte mottar virussignaturoppdateringer fra andre plasseringer. Hvis du vil ha mer informasjon om denne innstillingen, går du til del 4.4 "Oppdatering av programmet".



5.2 Eksportere/importere innstillinger

Eksport og import av gjeldende konfigurasjon av ESET NOD32 Antivirus er tilgjengelig under **Oppsett** i Avansert modus.

Filtypen xml benyttes til både eksport og import. Eksport og import er nyttig hvis du trenger å sikkerhetskopiere gjeldende konfigurasjon av ESET NOD32 Antivirus slik at du kan bruke den senere (uansett grunn). Eksportinnstillingene er også nyttige for de som ønsker å bruke favorittkonfigurasjonen av ESET NOD32 Antivirus på flere systemer. De trenger bare å importere xml-filen.



5.2.1 Eksporter innstillinger

Det er veldig enkelt å eksportere konfigurasjon. Hvis du vil lagre gjeldende konfigurasjon av ESET Smart Security, klikker du **Oppsett > Importer og eksporter innstillinger...** Velg alternativet **Eksporter innstillinger**, og oppgi navnet på konfigurasjonsfilen. Bruk nettleseren til å velge en plassering på datamaskinen der du vil lagre konfigurasjonsfilen.

5.2.2 Importer innstillinger

Trinnene for å importere en konfigurasjon er veldig like. Velg **Importer og eksporter innstillinger** og deretter **Importer innstillinger**. Klikk ..., og bla gjennom etter konfigurasjonsfilen du ønsker å importere.

5.3 Kommandolinje

Antivirusmodulen til ESET NOD32 Antivirus kan startes fra kommandolinjen – manuelt (med kommandoen "ecls") eller med en seriell fil ("bat").

Følgende parametere og brytere kan brukes når du kjører skanning ved behov fra kommandolinjen:

Generelle alternativer:

- hjelp vis hjelp og avslutt
- version vis opplysninger om versjon og avslutt
- base-dir = MAPPE last inn moduler fra MAPPE
- quar-dir = MAPPE sett MAPPE i karantene
- aind vis aktivitetsindikator
- auto skanner alle harddisker i rensemodus

Mål:

- files skann filer (standard)
- no-files ikke skann filer
- boots skann oppstartssektorer (standard)
- no-boots ikke skann oppstartssektorer
- arch skann arkiver (standard)
- no-arch ikke skann arkiver
- max-archive-level = NIVÅ maksimalt NIVÅ for arkivnesting
- scan-timeout = GRENSE skann arkiver i maksimalt GRENSE sekunder. Hvis skannetiden når denne grensen, vil skanningen av arkivet stoppe, og skanningen fortsetter med neste fil.
- max-arch-size=STØRRELSE skann kun de første STØRRELSE-bytene i arkivene (standard 0 = ubegrenset)
- mail skann e-postfiler
- no-mail ikke skann e-postfiler
- sfx skann selv-utpakkende arkiver
- no-sfx ikke skann selv-utpakkende arkiver
- rtp skann runtime packers
- no-rtp ikke skann runtime packers
- exclude = MAPPE utelat MAPPE fra skanning
- subdir skann undermapper (standard)
- no-subdir ikke skann undermapper
- max-subdir-level = NIVÅ maksimalt neste NIVÅ for undermappe (standard 0 = ubegrenset)
- symlink følg symbolske koblinger (standard)
- no-symlink hopp over symbolske koblinger
- ext-remove = FILENDELSE utelat FILENDELSE, som er skilt med kolon, fra skanning
- ext-exclude = FILENDELSE

Metoder:

- adware skann etter Adware/Spyware/Riskware
- no-adware ikke skann etter Adware/Spyware/Riskware
- unsafe skann etter potensielt usikre programmer
- no-unsafe ikke skann etter potensielt usikre programmer
- unwanted skann etter potensielt uønskede programmer
- no-unwanted ikke skann etter potensielt uønskede programmer
- pattern bruk signaturer
- no-pattern ikke bruk signaturer
- heur aktiver heuristikk
- no-heur deaktivert heuristikk
- adv-heur aktiver avansert heuristikk
- no-adv-heur deaktivert avansert heuristikk

Rensing:

- action = HANDLING utfør HANDLING på infiserte objekter. Tilgjengelige handlinger: none, clean, prompt
- quarantine kopier infiserte filer til Karantene (supplerer HANDLING)
- no-quarantine ikke kopier infiserte filer til Karantene

Logger:

- log-file=FIL logger utdata til FIL
- log-rewrite overskriv utdatafil (standard er tilføy)
- log-all logger også rensefiler
- no-log-all logger ikke rensefiler (standard)

Mulige avslutningskoder for skanningen:

- 0 – ingen trussel funnet
- 1 – trussel funnet, men ikke rens
- 10 – enkelte infiserte filer gjenstår
- 101 – arkivfeil
- 102 – tilgangsfeil
- 103 – intern feil

MERK:

Avslutningskoder som er større enn 100, betyr at filen ikke ble skannet og dermed kan være infisert.

6. Ordliste

6.1 Typer infiltrasjoner

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

6.1.1 Virus

Et datamaskinvirus er en infiltrering som ødelegger eksisterende filer på datamaskinen din. Datavirus har fått navnet sitt etter biologiske virus, fordi de bruker liknende metoder for å spre seg fra én maskin til en annen.

Datavirus angriper hovedsakelig kjørbare filer og dokumenter. Når de skal formere seg, fester et virus "kroppen" til slutten av en målfil. Dette er kort fortalt hvordan et datavirus fungerer: Etter utførelsen på den infiserte filen, aktiverer viruset seg selv (før originalprogrammet) og utfører sin forhåndsdefinerte oppgave. Kun etter det, kan originalprogrammet kjøre. Et virus kan ikke infisere en datamaskin hvis ikke brukeren selv (enten bevisst eller ubevisst) kjører eller åpner det skadelige programmet.

Datavirus kan være forskjellige når det gjelder aktivitet og alvorlighetsgrad. Noen av dem er svært farlige på grunn av deres evne til å slette filer fra en harddisk. På den annen side er det enkelte virus som ikke forårsaker noen reell skade. De bare irriterer brukeren og viser frem de tekniske kunnskapene de som har laget dem.

Det er viktig å legge merke til at virus (sammenliknet med trojanske hester og spyware) gradvis blir mer og mer sjeldne, fordi de ikke er kommersielt interessante nok for de som skaper skadelig programvare. Ordet "virus" blir også ofte feil brukt for å dekke alle typer infiltreringer. Nå har dette gradvis endret seg, og det nye og mer presise begrepet "malware" (skadelig programvare) blir brukt.

Hvis datamaskinen din er infisert med et virus, er det nødvendig å gjenopprette infiserte filer til den opprinnelige tilstanden – det vil si å rense dem ved hjelp av et antivirusprogram.

Dette er eksempler på virus: OneHalf, Tenga og Yankee Doodle.

6.1.2 Ormer

En dataorm er et program som inneholder skadelig kode som angriper vertsmaskinen, og som sprer seg via et nettverk. Hovedforskjellen mellom et virus og en orm er at ormer har evnen til å reproducere seg selv og flytte seg selv. De er ikke avhengige av vertsfiler (eller oppstartssektorer).

Ormer formerer seg ved hjelp av e-post eller nettverkspakker. De kan dermed deles inn i disse to gruppene:

- **E-post** – sprer seg selv til e-postadressene som blir funnet i brukerens kontaktliste.
- **Nettverk** – utnytter sikkerhetssvakheter i ulike programmer.

Ormer er derfor mye mer levedyktige enn datavirus. Siden de bruker Internett, kan ormer spre seg over hele kloden på bare noen få timer – og i enkelte tilfeller på bare noen minutter. Deres evne til å reproducere seg selv, gjør dem mye farligere enn andre typer skadelig programvare, slik som virus.

En orm som er aktivert i et system, kan skape mange vanskeligheter, blant annet følgende: Den kan slette filer, føre til dårligere systemytelse, og til og med deaktivere enkelte programmer. En dataorm skal fungere som et "transportmiddel" for andre typer infiltreringer.

Hvis datamaskinen din er infisert med en dataorm, anbefaler vi at du sletter infiserte filer, fordi de sannsynligvis inneholder skadelig kode.

Dette er eksempler på velkjente ormer: Lovsan/Blaster, Stration/Warezov, Bagle og Netsky.

6.1.3 Trojanske hester

Trojanske hester er historisk blitt definert som en klasse infiltreringer som forsøker å presentere seg selv som nyttige programmer, og dermed lurer de brukerne til å kjøre dem. Men det er viktig å merke seg at dette tidligere var en riktig definisjon av trojanske hester. Nå har de ikke lenger noen grunn til å komme i forkledning. Deres eneste formål er å infiltrere så enkelt som mulig, og nå sine skadelige mål. En "trojansk hest" har blitt et veldig generelt begrep som beskriver enhver infiltrering, som ikke kommer inn under noen annen bestemt klasse av infiltreringer.

Og fordi dette er en svært vid kategori, blir den ofte delt opp i flere underkategorier. Dette er de mest kjente:

- **Nedlaster** – et skadelig program som er i stand til å laste ned andre infiltreringer fra Internett.
- **Dropper** – en type trojansk hest som er laget for å droppe eller plassere andre typer skadelige programmer på berørte datamaskiner.
- **Bakdør** – et program som kommuniserer med eksterne angripere, og som lar dem få tilgang til et system og ta kontrollen over det.
- **Tastlogger** – (tastetrykk-logger) – et program som registrerer alle tastetrykk fra en bruker og sender informasjonen til eksterne angripere.
- **Oppringer** – oppringere er programmer som er laget for å koble seg til svært dyre telefonnumre. 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.

Trojanske hester ser vanligvis ut som kjørbare filer med filendelsen exe. Hvis en fil på datamaskinen din blir gjenkjent som en trojansk hest, er det lurt å slette den, fordi den høyst sannsynlig inneholder skadelig kode.

Dette er eksempler på velkjente trojanske hester: NetBus, Trojandownloader.Small.ZL, Slapper

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 til å unngå å bli oppdaget av virusprogramvaren. De skjuler prosesser, filer og Windows-registerdata. Derfor er det nesten umulig å oppdage dem med vanlige testteknikker.

Når det gjelder forebygging av rootkit, må du huske at dette er de to nivåene for gjenkjennelse:

1. Når de prøver å få tilgang til et system. De er fremdeles ikke til stede, og er derfor inaktive. De fleste antivirussystemer kan eliminere rootkits på dette nivået (hvis man antar at de faktisk oppdager slike filer som infisert).
2. Når de er skjult for den vanlige testingen. Brukere av ESETs antivirussystem har fordelen av Anti-Stealth-teknologi, som også kan oppdage og eliminere aktive rootkits.

6.1.5 Adware

Adware er en betegnelse på reklamestøttet programvare. Programmer som viser markedsføringsmateriale, plasseres 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, noe som gjør at utviklere kan dekke utviklingskostnadene til sine (vanligvis nyttige) programmer.

Adware i seg selv er ikke farlig – brukere blir bare forstyrret med reklame. Faren ligger i at adware også kan utføre sporingsfunksjoner (som også spyware gjør).

Hvis du bestemmer deg for å bruke et gratisprodukt, bør du være spesielt oppmerksom på installasjonsprogrammet. Installasjonsprogrammer vil mest sannsynlig varsle deg om installasjon av et ekstra adware-program. Du kan ofte avbryte installasjonen og installere programmet uten adware. På den annen side er det noen programmer som ikke kan installeres uten adware, eller som får begrenset funksjonalitet. Dette betyr at adware ofte får tilgang til systemet på en "lovlig" måte, siden brukeren godtar det. I dette tilfellet er det bedre å være føre var.

Hvis det blir oppdaget en adware-fil på datamaskinen din, er det lurt å slette den, fordi den høyst sannsynlig inneholder skadelig 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. Slike programmer 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 utførte 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 informasjonen som hentes, 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. Under installeringen blir brukerne ofte informert 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 antispymware-programmer, men er i realiteten selv spyware.

Hvis det blir oppdaget en spyware-fil på datamaskinen din, er det lurt å slette den, fordi den høyst sannsynlig inneholder skadelig kode.

6.1.7 Potensielt usikre programmer

Det er mange lovlige programmer som har som oppgave å forenkle administreringen av maskiner i nettverk. Men hvis disse programmene kommer på feil hender, kan de bli brukt til skadelige formål. Det er derfor ESET har opprettet denne spesialkategorien. Våre kunder har nå muligheten til å velge om de vil at antivirussystemet skal gjenkjenne slike trusler eller ikke.

"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 (et program 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), kontakter du systemansvarlig eller fjerner programmet.

6.1.8 Potensielt uønskede programmer

Potensielt uønskede programmer er ikke nødvendigvis ment å skulle skade, men de kan påvirke ytelsen til datamaskinen din på en negativ måte. Slike programmer krever vanligvis godkjenning ved installasjon. Hvis de er til stede på datamaskinen, oppfører systemet seg annerledes (sammenlignet med tilstanden før installasjon). Dette er de tydeligste endringene:

- Det blir åpnet nye vinduer du ikke har sett før.
- Aktivering og kjøring av skjulte prosesser.
- Økt bruk av systemressurser.
- Endringer i søkeresultater.
- Programmer kommuniserer med eksterne servere.