ESET Smart Security Premium

Användarhandbok

Klicka här för att visa hjälpversionen av detta dokument

Digital Security
Progress. Protected.

ESET Smart Security Premium har utvecklats av ESET, spol. s r.o.

För mer information besök https://www.eset.com.

Teknisk support: https://support.eset.com

REV. 2024-04-12

ESET Smart Security Premium

ESET Smart Security Premium representerar ett nytt förhållningssätt till integrerad datasäkerhet. Den senaste versionen av ESET LiveGrid®-genomsökningsmotorn, kombinerat med våra skräddarsydda moduler Brandvägg och Antispam, använder snabbhet och noggrannhet för att skydda datorn. Resultatet är ett intelligent system som är oupphörligen vaksamt mot attacker och skadlig programvara som kan utgöra en fara för din dator.

ESET Smart Security Premium är en komplett säkerhetslösning som kombinerar maximalt skydd och minimal systembelastning. Vår avancerade teknik som använder artificiell intelligens för att förhindra infiltration av virus, spionprogram, trojaner, maskar, reklamprogram, rootkits och andra hot utan att minska systemets prestanda eller störa din dator.

Funktioner och fördelar

Omformat användargränssnitt	Användargränssnittet i den här versionen har omformats avsevärt och förenklats baserat på resultat från testning av användarvänlighet. All GUI-text och alla meddelanden har granskats noga och gränssnittet har nu stöd för språk som skrivs från höger till vänster, som hebreiska och arabiska. Onlinehjälpen är nu integrerad i ESET Smart Security Premium och har supportinnehåll som uppdateras dynamiskt.
Mörkt läge	Ett tillägg som hjälper dig att snabbt byta skärm till ett mörkt tema. Du kan välja önskat färgschema i Element i användargränssnittet.
Skydd mot virus och spionprogram	Identifierar och rensar proaktivt kända och okända virus, maskar, trojaner och rootkits. Avancerad heuristik varnar även för inte tidigare känd skadlig kod och skyddar dig mot okända hot och neutraliserar dem innan de hinner göra skada. Webbåtkomstskydd och skydd mot nätfiske övervakar kommunikationen mellan webbläsare och fjärrservrar (inklusive SSL). Skydd av e-postklient kontrollerar e-postkommunikation genom IMAP(S)- och POP3(S)-protokollen.
Regelbundna uppdateringar	Regelbunden uppdatering av detekteringsmotorn (som tidigare kallades virussignaturdatabas) och programmodulerna är det bästa sättet att säkerställa maximal skyddsnivå för datorn.
ESET LiveGrid® (molngenererat rykte)	Det går att kontrollera ryktet för processer och filer som körs direkt i ESET Smart Security Premium.
Enhetskontroll	Söker automatiskt igenom USB-flashenheter, minneskort och CD/DVD. Blockerar flyttbara medier baserat på mediatyp, tillverkare, storlek och andra attribut.
HIPS-funktion	Det går att anpassa systemets beteende i större detalj. Ange regler för systemregistret, aktiva processer och program och finjustera säkerhetsinställningarna.
Spelläge	Skjuter upp alla popup-fönster, uppdateringar och andra systemintensiva aktiviteter för att spara systemresurser för spel och andra aktiviteter i helskärmsläge.

Funktioner i ESET Smart Security Premium

Säkra banktjänster och surfning	Säkra banktjänster och surfning tillhandahåller en säkrad webbläsare som används när du öppnar nätslussar för bank- och betalning för att säkerställa att alla webbtransaktioner sker i en pålitlig och säker miljö.
Stöd för nätverkssignaturer	Nätverkssignaturer möjliggör snabb identifiering och blockerar skadlig trafik till och från användares enheter, till exempel botar och kryphålspaket. Funktionen kan ses som en förbättring av Botnätsskydd.
Intelligent brandvägg	Förhindrar obehörig åtkomst till datorn och missbruk av dina personliga data.

Skräppostskydd av e-postklient	Spam utgör upp till 50 procent av all e-postkommunikation. Skräppostskydd för e-postklient skyddar mot det här problemet.
Stöldskydd	Stöldskydd utökar användarens säkerhet i händelse av förlorad eller stulen dator. När du installerar ESET Smart Security Premium och Stöldskydd, så listas enheten i webbgränssnittet. Med webbgränssnittet kan du hantera Stöldskydd-konfigurationen och administrera Stöldskydd-funktioner på din enhet.
Föräldrakontroll	Skyddar din familj från potentiellt stötande webbinnehåll genom att blockera olika webbplatskategorier.
Password Manager	Password Manager som skyddar och lagrar dina lösenord och personuppgifter.
Secure Data	Med Secure Data kan du kryptera data på datorn och flyttbara enheter för att förhindra missbruk av privat, konfidentiell information.
ESET LiveGuard	Identifierar och stoppar aldrig tidigare sedda hot och bearbetar information för framtida identifiering.

Det måste finnas ett aktivt abonnemang för att ESET Smart Security Premium-funktionerna ska fungera. Vi rekommenderar att du förnyar ditt abonnemang flera veckor innan abonnemanget ESET Smart Security Premium upphör.

Nyheter

Nyheter i ESET Smart Security Premium 17.1

- Små förbättringar av Network Inspector
- Små förbättringar av Säkra banktjänster och surfning
- ESET LiveGuard – skicka dokumenten är nu aktiverat som standard
- Andra mindre buggfixar och förbättringar

Så här inaktiverar du **Visa meddelanden om nyheter**:
1. Öppna Avancerade inställningar > **Meddelanden** > **Meddelanden på skrivbordet**.
2. Klicka på **Redigera** bredvid **Meddelanden på skrivbordet**.
3. Avmarkera kryssrutan för **Visa meddelanden om nyheter** och klicka på **OK**.
För mer information om meddelanden läser du avsnittet Meddelanden.

Du hittar en detaljerad lista över ändringar i ESET Smart Security Premium i ändringsloggar för ESET Smart Security Premium.

Vilken produkt har jag?

ESET erbjuder flera lager av säkerhet med nya produkter – från en kraftfull och snabb antiviruslösning till en heltäckande säkerhetslösning med minimal systempåverkan:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

- **ESET Security Ultimate**

Om du vill se vilken produkt du har installerad öppnar du programmets huvudfönster, så visas produktens namn överst i fönstret (se artikeln i kunskapsbasen).

I tabellen nedan visas vilka funktioner respektive produkt har.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekteringsmotor	✔	✔	✔	✔
Avancerad maskininlärning	✔	✔	✔	✔
Kryphålsblockering	✔	✔	✔	✔
Skydd mot skriptbaserade attacker	✔	✔	✔	✔
Skydd mot nätfiske	✔	✔	✔	✔
Webbåtkomstskydd	✔	✔	✔	✔
HIPS (inklusive Skydd mot ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Brandvägg		✔	✔	✔
Network Inspector		✔	✔	✔
Webbkameraskydd		✔	✔	✔
Skydd mot nätverksattacker		✔	✔	✔
Botnetsskydd		✔	✔	✔
Säkra banktjänster och surfning		✔	✔	✔
Webbläsarsekretess och säkerhet		✔	✔	✔
Föräldrakontroll		✔	✔	✔
Stöldskydd		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Vissa av produkterna ovan kanske inte är tillgängliga på ditt språk eller i din region.

Systemkrav

Om ESET Smart Security Premium ska fungera optimalt ska systemet uppfylla följande krav på maskin- och programvara:

Processorer som stöds

Intel eller AMD-processor, 32-bitars (x86) med SSE2-instruktionsuppsättning eller 64-bitars (x64), 1 GHz eller högre
ARM64-baserad processor, 1 GHz eller högre

Operativsystem som stöds

Microsoft® Windows® 11

Microsoft® Windows® 10

Stöd för Azure Code Signing måste installeras på alla Windows-operativsystem för att installera eller uppgradera ESET-produkter som har släppts efter juli 2023. Mer information.

Försök att alltid hålla operativsystemet uppdaterat.

Krav för ESET Smart Security Premium-funktioner

Se systemkraven för specifika ESET Smart Security Premium-funktioner i tabellen nedan:

Funktion	Krav
Intel® Threat Detection Technology	Se de processorer som stöds.
Säkra banktjänster och surfning	Se de webbläsare som stöds.
Transparent bakgrund	Windows 10 version RS4 och senare.
Specialiserad rensning	Icke-ARM64-baserad processor.
Systemrensare	Icke-ARM64-baserad processor.
Kryphålsblockering	Icke-ARM64-baserad processor.
Djup beteendegranskning	Icke-ARM64-baserad processor.

Övrigt

En internetanslutning krävs för att aktivering och uppdatering av ESET Smart Security Premium ska fungera ordentligt.

Två antivirusprogram som körs samtidigt på en enhet orsakar oundvikliga systemresurskonflikter, till exempel att sakta ner systemet så att det blir oanvändbart.

Inaktuell version av Microsoft Windows

Problem

- Du vill installera den senaste versionen av ESET Smart Security Premium på en dator med Windows 7, Windows 8 (8.1) eller Windows Home Server 2011
- ESET Smart Security Premium visar ett fel **Föråldrat operativsystem** under installationen

Information

Den senaste versionen av ESET Smart Security Premium kräver operativsystemen Windows 10 eller Windows 11.

Lösning

Följande lösningar är tillgängliga:

Uppgradera till Windows 10 eller Windows 11

Uppgraderingsprocessen är relativt enkel, och i många fall kan den genomföras utan att du förlorar dina filer. Innan du uppgraderar till Windows 10:

1. Säkerhetskopiera viktiga data.

2. Läs Microsofts vanliga frågor om uppgradering till Windows 10 eller vanliga frågor om uppgradering till Windows 11 och uppdatera ditt Windows-operativsystem.

Installera ESET Smart Security Premium version 16.0

Om du inte kan uppgradera Windows ska du installera ESET Smart Security Premium version 16.0. Ytterligare information finns i onlinehjälpen för ESET Smart Security Premium version 16.0.

Skydd

När du använder datorn, särskilt när du surfar på Internet, bör du komma ihåg att inget antivirussystem i världen fullständigt kan eliminera risken för infiltreringar och fjärrattacker. För att uppnå maximalt skydd och bekvämlighet är det viktigt att använda antiviruslösningen på ett korrekt sätt och följa några praktiska regler:

Uppdatera regelbundet

Enligt statistik från ESET LiveGrid® skapas tusentals nya unika infiltreringar varje dag. De kan ta sig förbi befintliga säkerhetsåtgärder och berika sina författare, allt på andra användares bekostnad. Specialisterna i ESET:s forskningslabb analyserar dagligen dessa hot. De utvecklar och släpper uppdateringar så att användarnas skyddsnivå hela tiden höjs. För att säkerställa att uppdateringarna för maximal effekt är det viktigt att uppdateringarna är korrekt inställda på systemet. Ytterligare information om konfigurering av uppdateringar finns i kapitlet Uppdateringsinställningar.

Hämta säkerhetskorrigeringsfiler

Författarna till skadlig programvara utnyttjar ofta olika sårbarheter i systemet så att spridningen av skadlig kod blir effektivare. Med detta i åtanke letar programvaruföretag noga efter nya sårbarheter i sina program så att de kan släppa säkerhetsuppdateringar som regelbundet eliminerar potentiella hot så snart en sårbarhet har påvisats. Det är viktigt att hämta dessa säkerhetsuppdateringar så snart de släpps. Microsoft Windows och webbläsare som Internet Explorer är två exempel på program för vilka säkerhetsuppdateringar släpps regelbundet.

Säkerhetskopiera viktiga data

Författare till skadlig programvara bryr sig vanligtvis inte om användarnas behov och skadliga program leder ofta

till att operativsystemet helt slutar fungera och att viktiga data går förlorade. Det är viktigt att regelbundet säkerhetskopiera viktiga och känsliga data till en extern källa som en DVD-skiva eller en extern hårddisk. Detta gör det mycket snabbare och enklare att återställa data om datorn eller systemet slutar fungera.

Genomsök regelbundet datorn efter virus

Identifiering av fler kända och okända virus, maskar, trojaner och rootkit hanteras av skyddsmodulen för realtidsövervakning av filsystemet. Detta innebär att varje gång du öppnar en fil, genomsöks den efter skadlig kod. Vi rekommenderar att du kör en fullständig genomsökning av datorn åtminstone en gång per månad, eftersom skadlig kod ändras och detekteringsmotorn uppdateras varje dag.

Följ grundläggande säkerhetsregler

Detta är den viktigaste och mest effektiva regeln av alla – var alltid försiktig! Idag kräver många infiltreringar att användaren reagerar innan de körs och sprids. Om du är försiktig innan du öppnar nya filer sparar du mycket tid och kraft som annars skulle gå åt till att rensa bort infiltreringar. Här är några praktiska riktlinjer:

- Besök inte misstänkta webbplatser med flera popup-fönster och blinkande annonser.
- Var försiktig när du installerar gratisprogram, codec-paket o.s.v. Använd endast säkra program och besök endast säkra webbplatser.
- Var försiktig när du öppnar bifogade filer i e-postmeddelanden, särskilt om meddelandet har skickats till många mottagare eller kommer från en okänd avsändare.
- Använd inte ett administratörskonto för dagligt arbete med datorn.

Hjälpsidor

Välkommen till användarguiden för ESET Smart Security Premium. Denna information bekantar dig med produkten och hjälper dig att göra datorn säkrare.

Komma igång

Innan du börjar använda ESET Smart Security Premium kan du läsa om olika typer av detekteringar och fjärrattacker du kan träffa på när du använder datorn. Vi har även sammanställt en lista över nya funktioner i ESET Smart Security Premium.

Börja med att installera ESET Smart Security Premium. Om du redan har ESET Smart Security Premium installerat läser du Arbeta med ESET Smart Security Premium.

Använda ESET Smart Security Premium hjälpsidor

Onlinehjälpen är indelad i olika kapitel och kapitelavsnitt. Tryck på **F1** i ESET Smart Security Premium om du vill visa information om det fönster som för närvarande är öppet.

I programmet går det att söka efter ett hjälpavsnitt med hjälp av nyckelord eller söka i innehållet genom att skriva ord eller fraser. Skillnaden mellan dessa två metoder är att ett nyckelord kan vara logiskt relaterat till hjälpsidor som inte innehåller det specifika nyckelordet någonstans i texten. Om du söker efter ord och fraser genomsöks innehållet i alla sidor och sidorna där det aktuella ordet eller frasen ingår i texten visas.

För enhetlighet och tydlighet baseras den terminologi som används i guiden på ESET Smart Security Premium-användargränssnittet. Dessutom markeras avsnitt som är särskilt intressanta eller viktiga med en enhetlig uppsättning symboler.

Anmärkningarna är endast korta observationer. De går att hoppa över, men kan ge värdefull information om till exempel specifika funktioner eller länkar till ett relaterat ämne.

Detta kräver din uppmärksamhet och bör inte hoppas över. Vanligen innehåller avsnittet information som inte är strikt nödvändig att veta, men som ändå är viktig.

Detta är information som kräver extra uppmärksamhet och försiktighet. Varningar är avsedda att hindra dig från att begå potentiellt skadliga misstag. Läs och förstå texten, eftersom den handlar om mycket känsliga systeminställningar eller olika risker.

Detta är ett användningsfall eller ett praktiskt exempel som gör det lättare att förstå hur en viss funktion kan användas.

Konvention	Innebörd
Fet stil	Namn på objekt i gränssnittet, till exempel rutor och alternativknappar.
Kursiv stil	Platshållare för informationen du tillhandahåller. Till exempel innebär filnamn eller sökväg att du skriver den faktiska sökvägen eller namnet på en fil.
`Courier New`	Kodexempel eller kommandon.
Hyperlänk	Ger snabb och smidig åtkomst till korshänvisade avsnitt eller externa webbsidor. Hyperlänkar är markerade i blått och kan vara understrukna.
%ProgramFiles%	Den Windows-systemkatalog där program installerade i Windows finns.

Onlinehjälpen är den primära källan till hjälpinnehåll. Den senaste versionen av onlinehjälpen visas automatiskt när du har en fungerande internetanslutning.

Installation

Det finns flera sätt att installera ESET Smart Security Premium på din dator. Installationssätten kan variera beroende på land och distributionssätt:

- Installerare – hämtas från ESET-webbplatsen eller CD/DVD. Installationspaketet är gemensamt för alla språk (välj önskat språk). Installeraren är en liten fil; ytterligare filer som krävs för att installera ESET Smart Security Premium hämtas automatiskt.

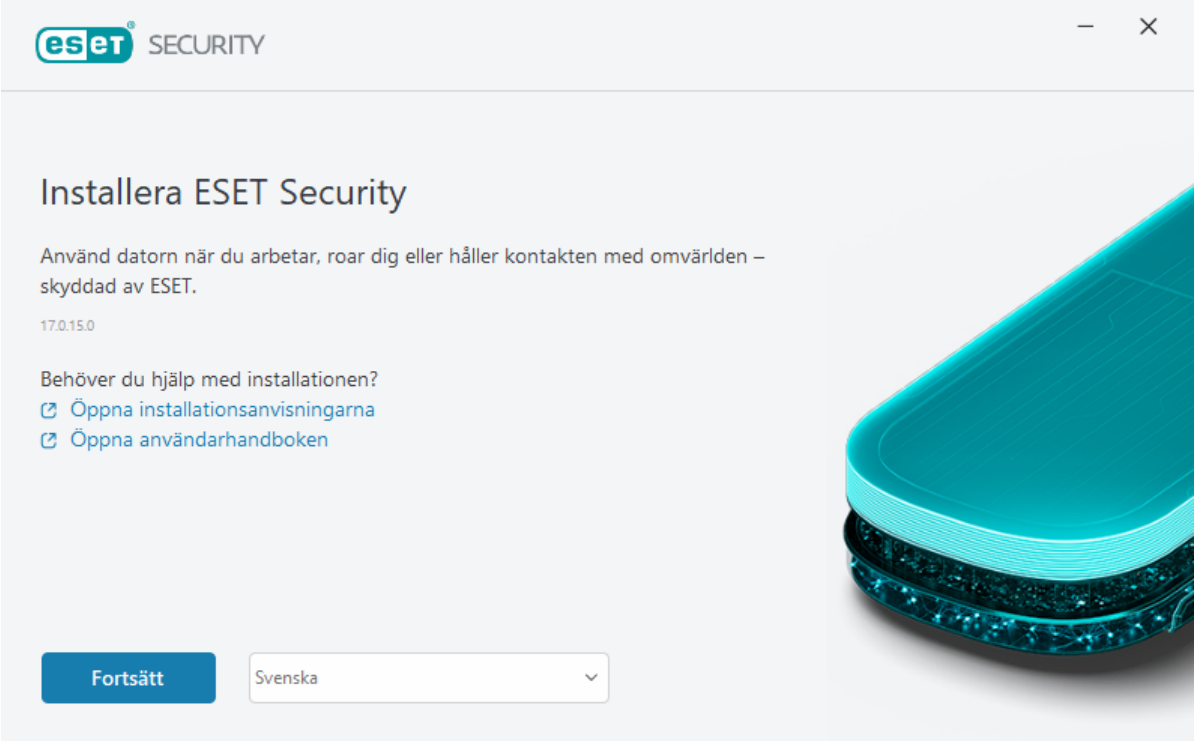
- Offlineinstallation – använder en .exe-fil som är större än installerarfilen och ingen internetanslutning eller ytterligare filer krävs för att slutföra installationen.

Kontrollera att inga andra antivirusprogram är installerade på datorn innan du installerar ESET Smart Security Premium. Om två eller fler antiviruslösningar är installera på en dator kan de komma i konflikt med varandra. Det rekommenderas att du avinstallerar alla andra antivirusprogram på datorn. Se vår artikel i ESET kunskapsbas för en lista med avinstallationsverktyg för vanliga antivirusprogram (finns på engelska och flera andra språk).

Live installer

När du har hämtat installationspaketet Installerare ska du dubbelklicka på installationsfilen och följa instruktionerna i installationsguiden.

För den här typen av installation måste du anslutas till Internet.



1. Välj önskat språk i listrutan och klicka på **Fortsätt**.

Om du installerar en senaste version över den föregående versionen med lösenordskyddade inställningar, så skriver du ditt lösenord. Du kan konfigurera inställningslösenordet i åtkomstinställningarna.

2. Välj dina inställningar för följande funktioner, läs licensavtalet för slutanvändare och sekretesspolicyn och klicka på **Fortsätt** eller klicka på **Tillåt alla och fortsätt** om du vill aktivera alla funktioner:

- ESET LiveGrid®-feedbacksystem
- Potentiellt oönskade program
- Program för en bättre kundupplevelse

Genom att klicka på **Fortsätt** eller **Tillåt alla och fortsätt** godkänner du licensavtalet för slutanvändare och bekräftar sekretesspolicyn.

3. Om du vill aktivera, hantera och visa enhetens säkerhet med hjälp av ESET HOME ansluter du enheten till ESET HOME-kontot. Klicka på **Hoppa över inloggning** om du vill fortsätta utan att ansluta till ESET HOME. Du kan ansluta enheten till ditt ESET HOME-konto senare.

4. Om du fortsätter utan att ansluta till ESET HOME väljer du ett aktiveringsalternativ. Om du installerar en senaste version över den föregående anges **aktiveringsnyckel** automatiskt.

5. Installationsguiden fastställer vilken ESET-produkt som är installerad baserat på ditt abonnemang. Den version som har flest säkerhetsfunktioner är alltid förvald. Klicka på **Ändra produkt** om du vill installera en annan version av ESET-produkten. Klicka på **Fortsätt** för att starta installationsprocessen. Denna kan ta en stund.

Om det finns några rester (filer eller mappar) från ESET-produkter som avinstallerats tidigare uppmanas du att tillåta att de tas bort. Klicka på **Installera** för att fortsätta.

6. Klicka på **Klart** för att stänga installationsguiden.

Felsökning för installation.

När produkten har installerats och aktiverats börjar modulerna hämtas. Skyddet initieras och det är inte säkert att alla funktioner fungerar förrän hämtningen är klar.

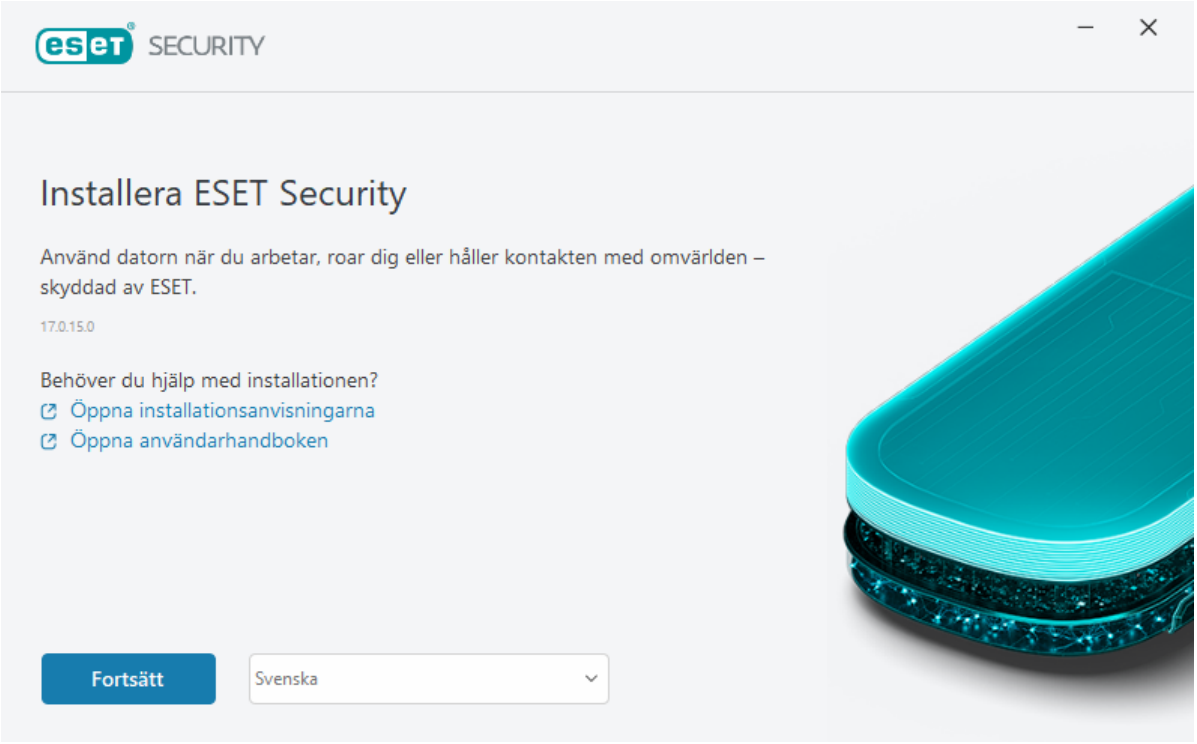
Offline-installation

Ladda ned och installera din ESET Windows-hemprodukt med offlineinstalleraren (.exe) nedan. Välj vilken version av ESET:s produkt för hemmet som ska hämtas (32-bitars, 64-bitars eller ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
64-bitars nedladdning 32-bitars nedladdning ARM-nedladdning	64-bitars nedladdning 32-bitars nedladdning ARM-nedladdning	64-bitars nedladdning 32-bitars nedladdning ARM-nedladdning	64-bitars nedladdning 32-bitars nedladdning ARM-nedladdning

Om du har en aktiv internetanslutning installerar du ESET-produkten med en installerare.

När du startar offlineinstalleraren (.exe) tar installationsguiden dig igenom installationen.



1. Välj önskat språk i listrutan och klicka på **Fortsätt**.

Om du installerar en senaste version över den föregående versionen med lösenordskyddade inställningar, så skriver du ditt lösenord. Du kan konfigurera inställningslösenordet i åtkomstinställningarna.

2. Välj dina inställningar för följande funktioner, läs licensavtalet för slutanvändare och sekretesspolicyn och klicka på **Fortsätt** eller klicka på **Tillåt alla och fortsätt** om du vill aktivera alla funktioner:

- ESET LiveGrid®-feedbacksystem
- Potentiellt oönskade program
- Program för en bättre kundupplevelse

Genom att klicka på **Fortsätt** eller **Tillåt alla och fortsätt** godkänner du licensavtalet för slutanvändare och bekräftar sekretesspolicyn.

3. Klicka på **Hoppa över inloggning**. När du har en internetanslutning kan du ansluta enheten till ditt ESET HOME-konto.

4. Klicka på **Hoppa över aktivering**. ESET Smart Security Premium måste aktiveras efter installationen för att fungera fullt ut. Produktaktivering kräver en aktiv internetanslutning.

5. Installationsguiden visar vilken ESET-produkt som kommer att installeras baserat på den nedladdade offlineinstalleraren. Klicka på **Fortsätt** för att starta installationsprocessen. Denna kan ta en stund.

Om det finns några rester (filer eller mappar) från ESET-produkter som avinstallerats tidigare uppmanas du att tillåta att de tas bort. Klicka på **Installera** för att fortsätta.

6. Klicka på **Klart** för att stänga installationsguiden.

Felsökning för installation.

Uppgradering av abonnemang

Det här meddelandefönstret visas när abonnemanget som används för att aktivera din ESET-produkt har ändrats. Ditt ändrade abonnemang gör att du kan aktivera en produkt med fler säkerhetsfunktioner. Om ingen ändring har utförts kommer ESET Smart Security Premium att visa en aviseringsfönster en gång, kallat **Byt till en produkt med fler funktioner**.

Ja (rekommenderas) – kommer automatiskt att installera produkten med fler säkerhetsfunktioner.

Nej, tack – inga ändringar kommer att göras och meddelandet försvinner permanent.

Om du vill ändra produkten senare, se vår artikel i ESET:s kunskapsbas. Mer information om ESET-abonnemang finns i Vanliga frågor och svar om abonnemang.

I tabellen nedan visas vilka funktioner respektive produkt har.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekteringsmotor	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Avancerad maskininlärning	✔	✔	✔	✔
Kryphålsblockering	✔	✔	✔	✔
Skydd mot skriptbaserade attacker	✔	✔	✔	✔
Skydd mot nätfiske	✔	✔	✔	✔
Webbåtkomstskydd	✔	✔	✔	✔
HIPS (inklusive Skydd mot ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Brandvägg		✔	✔	✔
Network Inspector		✔	✔	✔
Webbkameraskydd		✔	✔	✔
Skydd mot nätverksattacker		✔	✔	✔
Botnetsskydd		✔	✔	✔
Säkra banktjänster och surfning		✔	✔	✔
Webbläsarsekretess och säkerhet		✔	✔	✔
Föräldrakontroll		✔	✔	✔
Stöldskydd		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Uppgradering av produkt

Du har laddat ner en standardinstallerare och beslutat att ändra produkten ska aktiveras eller vill ändra din installerade produkt till en med fler säkerhetsfunktioner.

Byta produkt under installationen.

I tabellen nedan visas vilka funktioner respektive produkt har.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekteringsmotor	✔	✔	✔	✔
Avancerad maskininlärning	✔	✔	✔	✔
Kryphålsblockering	✔	✔	✔	✔
Skydd mot skriptbaserade attacker	✔	✔	✔	✔
Skydd mot nätfiske	✔	✔	✔	✔
Webbåtkomstskydd	✔	✔	✔	✔
HIPS (inklusive Skydd mot ransomware)	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Antispam		✔	✔	✔
Brandvägg		✔	✔	✔
Network Inspector		✔	✔	✔
Webbkameraskydd		✔	✔	✔
Skydd mot nätverksattacker		✔	✔	✔
Botnetsskydd		✔	✔	✔
Säkra banktjänster och surfning		✔	✔	✔
Webbläsarsekretess och säkerhet		✔	✔	✔
Föräldrakontroll		✔	✔	✔
Stöldskydd		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Nedgradering av abonnemang

Det här dialogfönstret visas när abonnemanget som har använts för att aktivera din ESET-produkt har ändrats. Ditt ändrade abonnemang kan endast användas med andra ESET-produkter med färre säkerhetsfunktioner. Produkten har ändrats automatiskt för att förhindra skyddsförlust.

Mer information om ESET-abonnemang finns i Vanliga frågor och svar om abonnemang.

I tabellen nedan visas vilka funktioner respektive produkt har.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekteringsmotor	✔	✔	✔	✔
Avancerad maskininlärning	✔	✔	✔	✔
Kryphålsblockering	✔	✔	✔	✔
Skydd mot skriptbaserade attacker	✔	✔	✔	✔
Skydd mot nätfiske	✔	✔	✔	✔
Webbåtkomstskydd	✔	✔	✔	✔
HIPS (inklusive Skydd mot ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Brandvägg		✔	✔	✔
Network Inspector		✔	✔	✔
Webbkameraskydd		✔	✔	✔
Skydd mot nätverksattacker		✔	✔	✔
Botnetsskydd		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Säkra banktjänster och surfning		✔	✔	✔
Webbläsarsekretess och säkerhet		✔	✔	✔
Föräldrakontroll		✔	✔	✔
Stöldskydd		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Nedgradering av produkt

Produkten du för närvarande har installerad har fler säkerhetsfunktioner än den du är på väg att aktivera. Secure Data och Password Manager ingår inte i den här produkten. Du kommer inte att kunna skapa krypterade filer.

I tabellen nedan visas vilka funktioner respektive produkt har.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Detekteringsmotor	✔	✔	✔	✔
Avancerad maskininlärning	✔	✔	✔	✔
Kryphålsblockering	✔	✔	✔	✔
Skydd mot skriptbaserade attacker	✔	✔	✔	✔
Skydd mot nätfiske	✔	✔	✔	✔
Webbåtkomstskydd	✔	✔	✔	✔
HIPS (inklusive Skydd mot ransomware)	✔	✔	✔	✔
Antispam		✔	✔	✔
Brandvägg		✔	✔	✔
Network Inspector		✔	✔	✔
Webbkameraskydd		✔	✔	✔
Skydd mot nätverksattacker		✔	✔	✔
Botnetsskydd		✔	✔	✔
Säkra banktjänster och surfning		✔	✔	✔
Webbläsarsekretess och säkerhet		✔	✔	✔
Föräldrakontroll		✔	✔	✔
Stöldskydd		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Identity Protection				✔

Felsökning för installation

Om problem uppstår under installationen tillhandahåller installationsguiden en felsökningsfunktion som löser problemet om möjligt.

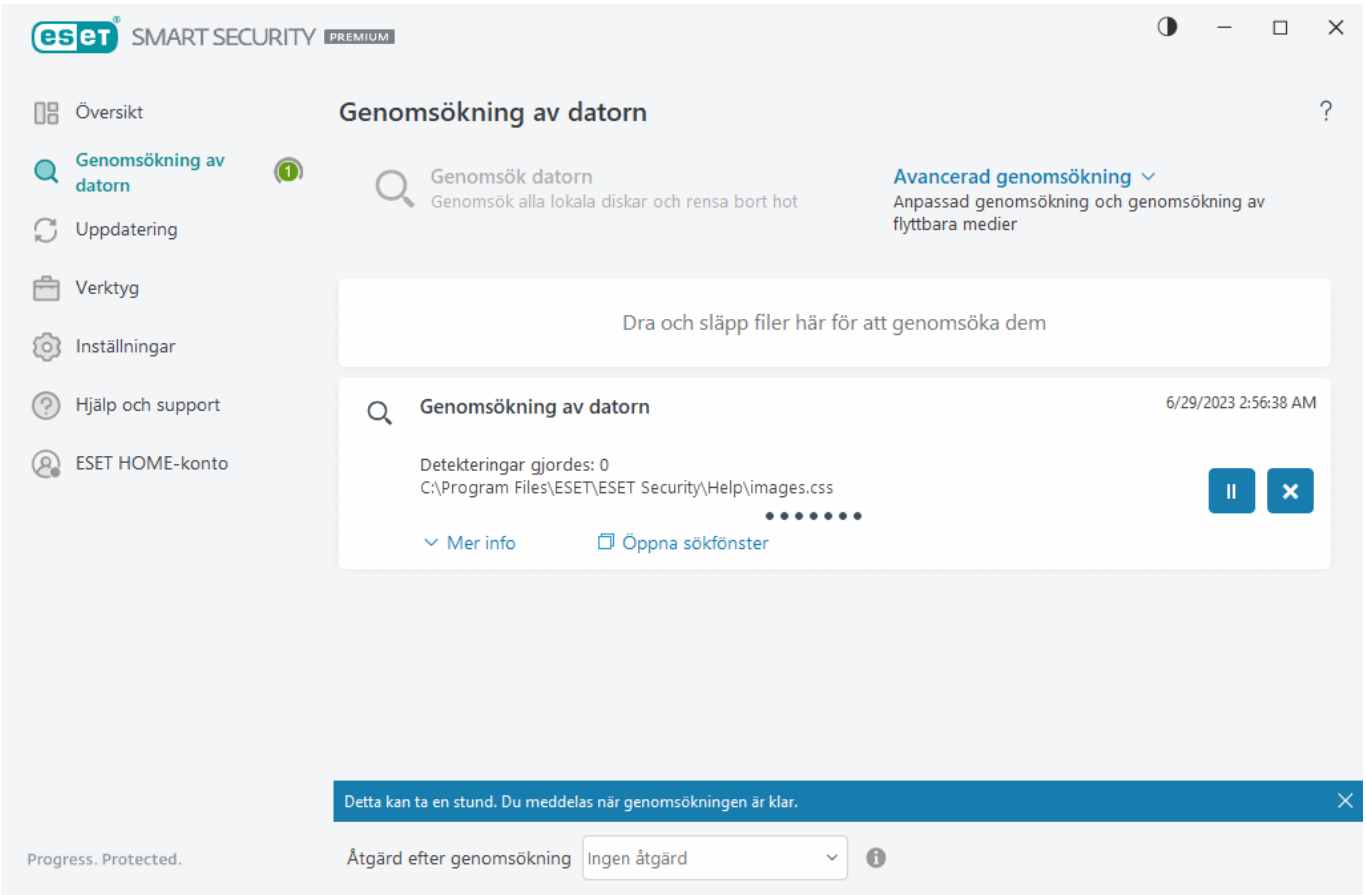
Klicka på **Kör felsökning** för att starta felsökningen. När felsökningen är klar följer du den rekommenderade lösningen.

Om problemet kvarstår kan du se listan över vanliga installationsfel och lösningar.

Första genomsökningen efter installation

När ESET Smart Security Premium installerats startar en datorgenomsökning automatiskt efter den första uppdateringen för att söka efter skadlig kod.

Det går också att starta en datorgenomsökning manuellt från programmets huvudfönster genom att klicka på **Genomsökning av datorn** > **Genomsök datorn**. För mer information om genomsökning av datorn, se Genomsökning av datorn.



Uppgradering till en nyare version

Nya versioner av ESET Smart Security Premium ges ut för att implementera förbättringar eller lösa problem som inte går att åtgärda med automatiska uppdateringar av programmodulerna. Det går att uppdatera till en senare version på flera sätt:

1. Automatiskt genom programuppdatering.
Eftersom programuppdateringen distribueras till alla användare och kan påverka vissa systemkonfigurationer släpps de efter en lång testperiod för att säkerställa att de fungerar med alla tänkbara systemkonfigurationer. Använd en av metoderna nedan om du måste uppgradera till en nyare version omedelbart när den kommer ut.
Se till att du har aktiverat **Uppdateringar av programfunktioner** i Avancerade inställningar > **Uppdatera** > **Profiler** > **Uppdateringar**.

2. Manuellt i programmets huvudfönster genom att klicka på **Leta efter uppdateringar** i avsnittet **Uppdatera**.

3. Manuellt genom att hämta och installera en nyare version över den föregående.

Mer information och illustrerade anvisningar hittar du i:

- Uppdatera ESET-produkter – söka efter de senaste produktmodulerna
- Vilka olika typer av uppdateringar och utgåvor finns det för ESET-produkter?

Automatisk uppgradering av äldre produkt

Din ESET-produktversion stöds inte längre och produkten har uppgraderats till den senaste versionen.

⚠ Vanliga installationsproblem

> ℹ Varje ny version av ESET-produkter har många buggfixar och förbättringar. Befintliga kunder med ett giltigt abonnemang för en ESET-produkt kan uppgradera till den senaste versionen av samma produkt utan kostnad.

Så här avslutar du installationen:

1. Klicka på **Acceptera och fortsätt** att acceptera Licensavtal för slutanvändare och erkänna Sekretesspolicyn. Om du inte samtycker till Licensavtal för slutanvändare klickar du på **Avinstallera**. Du kan inte återgå till den tidigare versionen.

2. Klicka på **Tillåt alla och fortsätt** för att tillåta både ESET LiveGrid®-feedbacksystemet och programmet för en bättre kundupplevelse eller klicka på **Fortsätt** om du inte vill delta.

3. Efter att du aktiverat den nya ESET-produkten med din aktiveringsnyckel kommer översiktssidan att visas. Om din abonnemangsinformation inte hittas fortsätter du med en kostnadsfri provversion. Om ditt abonnemang som används i den tidigare produkten inte är giltigt aktiverar du din ESET-produkt.

4. En omstart av enheten krävs för att slutföra installationen.

ESET Smart Security Premium kommer att installeras

Den här dialogrutan kan visas:

- Under installationsprocessen – klicka på **Fortsätt** för att installera ESET Smart Security Premium.
- När du ändrar ett abonnemang i ESET Smart Security Premium – klicka på **Aktivera** för att ändra abonnemanget och aktivera ESET Smart Security Premium.

Beroende på ditt ESET-abonnemang kan du med alternativet **Ändra produkt** växla mellan Windows-hemprodukter från ESET. Se Vilken produkt har jag? för mer information.

Byt till en annan produktserie

Beroende på ditt ESET-abonnemang kan du växla mellan olika Windows-hemprodukter från ESET. Se Vilken produkt har jag? för mer information.

Registrering

Registrera ditt abonnemang genom att fylla i fälten i registreringsformuläret och klicka på **Aktivera**. Fält markerade som obligatoriska inom parentes måste fyllas i. Informationen kommer endast att användas i ärenden som rör din ESET-abonnemang.

Aktiveringsförlopp

Vänta några sekunder på att aktiveringens slutförs (tiden kan variera beroende på din internetanslutning eller din dator).

Aktivering slutförd

Aktiveringen har slutförts. Följ anvisningarna i guiden efter installationen för att slutföra konfigurationen av ESET Smart Security Premium.

En moduluppdatering startar om några sekunder. Regelbundna uppdateringar av ESET Smart Security Premium börjar omedelbart.

En initial genomsökning startar automatiskt inom 20 minuter efter moduluppdateringen.

> Aktiveringsprocessen kan avbrytas om erbjudandet inte är associerat med ESET HOME. Logga in på ditt ESET HOME-konto eller skapa ett konto.

Nybörjarguide

Detta kapitel ger en inledande översikt över ESET Smart Security Premium och grundinställningarna.

Systemfältsikonen

Vissa av de viktigaste inställningsalternativen och funktionerna är åtkomliga genom att du högerklickar på systemfältsikonen .

Pausa skydd – visar bekräftelsedialogrutan som inaktiverar detekteringsmotorn som skyddar mot skadliga systemangrepp genom att kontrollera filer och webb- och e-postkommunikation. Med rullgardinsmenyn **Tidsintervall** kan du ange hur länge skyddet ska vara inaktiverat.

Pausa brandvägg (tillåt all trafik) – inaktiverar brandväggen. Se Nätverk för mer information.

Blockera all nätverkstrafik – blockerar all nätverkstrafik. Du kan aktivera den igen genom att klicka på **Sluta blockera all nätverkstrafik**.

Avancerade inställningar – öppnar de avancerade inställningarna för ESET Smart Security Premium. För att öppna de avancerade inställningarna från huvudproduktfönstret trycker du på F5 på tangentbordet eller klickar på **Inställningar** > **Avancerade inställningar**.

Loggfiler – loggfilerna innehåller information om viktiga programhändelser som har inträffat och ger en översikt över detekteringar.

Öppna ESET Smart Security Premium – öppnar huvudprogramfönstret för ESET Smart Security Premium.

Återställ fönsterlayout – återställer fönsterlayouten för ESET Smart Security Premium till standardstorlek och standardplacering på bildskärmen.

Färgläge – öppnar inställningar för användargränssnittet där du kan ändra färgen på det grafiska användargränssnittet.

Sök efter uppdateringar – startar en modul- eller produktuppdatering för att säkerställa att du är skyddad. ESET Smart Security Premium söker efter uppdateringar automatiskt flera gånger om dagen.

Om – ger systeminformation och visar den installerade versionen av ESET Smart Security Premium, installerade programmoduler och information om operativsystemet och systemresurserna.

Tangentbordsgenvägar

För bättre navigering i ESET Smart Security Premium kan du använda följande kortkommandon:

Tangentbordsgenvägar	Åtgärd
F1	öppnar hjälpsidorna
F5	öppnar Avancerade inställningar
Uppåtpil/nedåtpil	navigering i rullgardinsmenyer
TAB	gå till nästa gränssnittselement i ett fönster
Shift+TAB	gå till föregående gränssnittselement i ett fönster
ESC	stänger aktiv dialogruta
Ctrl+U	visar information om ESET-abonnemanget och datorn (uppgifter för teknisk support)
Ctrl+R	återställer produktfönstret till standardstorlek och standardplacering på bildskärmen
ALT + vänsterpil	navigera tillbaka
ALT + högerpil	navigera framåt
ALT+Home	navigera hem

Du kan även använda musens bakåt- och framåtknapp för navigering.

Profiler

Profilhanteraren används på två platser i ESET Smart Security Premium – i avsnittet **Genomsökning på begäran** och i avsnittet **Uppdatera**.

Genomsökning av datorn

Det finns fyra fördefinierade genomsökningsprofiler i ESET Smart Security Premium:

- **Smart genomsökning** – Detta är standardprofilen för avancerad genomsökning. Profilen Smart genomsökning använder Smart optimering, som exkluderar som var rena i en tidigare genomsökning och som inte har ändrats sedan dess. Det här möjliggör kortare genomsökningstider med minsta påverkan på systemets säkerhet.

- **Genomsökning av kontextmeny** – Du kan starta en sökning på begäran av valfri fil från kontextmenyn. Med hjälp av genomsökningsprofilen för kontextmenyn kan du definiera en genomsökningskonfiguration som ska användas när du utlöser genomsökningen på detta sätt.

- **Djup genomsökning** – Profilen Djup genomsökning använder inte Smart optimering som standard, därför exkluderas inga filer från genomsökning med den här profilen.

- **Genomsökning av datorn** – Detta är standardprofilen som används för standardgenomsökningen av datorn.

Det går att spara genomsökningsinställningarna för framtida genomsökning. Vi rekommenderar att skapar en profiler (med olika genomsökningsobjekt, genomsökningsmetoder och andra parametrar) för varje regelbunden genomsökning.

Skapa en ny profil genom att öppna Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Genomsökning på begäran** > **Lista över profiler** > **Redigera**. Fönstret **Profilhanteraren** innehåller rullgardinsmenyn **Vald profil** med befintliga genomsökningsprofiler och alternativet att skapa en ny. Du hittar hjälp om hur du skapar en genomsökningsprofil som motsvarar dina behov i avsnittet ThreatSense som innehåller

en beskrivning av varje parameter i genomsökningsinställningen.

> Anta att du vill skapa en egen genomsökningsprofil och konfigurationen **Genomsök datorn** är delvis lämplig, men du vill inte genomsöka internt packade filer eller potentiellt farliga program och dessutom vill du använda **Åtgärda alltid detektering**. Ange namnet på den nya profilen i fönstret **Profilhanteraren** och klicka på **Lägg till**. Välj den nya profilen i listrutan **Vald profil** och justera de återstående parametrarna så att de uppfyller dina krav och klicka på **OK** för att spara den nya profilen.

Uppdatera

Med profilredigeraren i avsnittet för uppdateringsinställningar kan användaren skapa nya uppdateringsprofiler. Skapa och använd dina egna anpassade profiler (dvs. andra profiler än standardprofilen **Min profil**) endast om datorn har flera sätt att ansluta till uppdateringsservrar.

Två profiler kan exempelvis användas av en bärbar dator som normalt ansluts till en lokal server (spegel) i det lokala nätverket, men som hämtar uppdateringar direkt från ESET:s uppdateringsservrar när den inte är ansluten till det lokala nätverket (t.ex. på en affärsresa), den första för anslutning till den lokala servern och den andra för anslutning till ESET:s servrar. När dessa profiler konfigurerats går du till **Verktyg** > **Schemaläggaren** och redigerar parametrarna för uppdateringsaktiviteten. Ange att en av profilerna ska vara primär och den andra sekundär.

Uppdateringsprofil – den uppdateringsprofil som för närvarande används. Om du vill ändra den anger du en annan profil i rullgardinsmenyn.

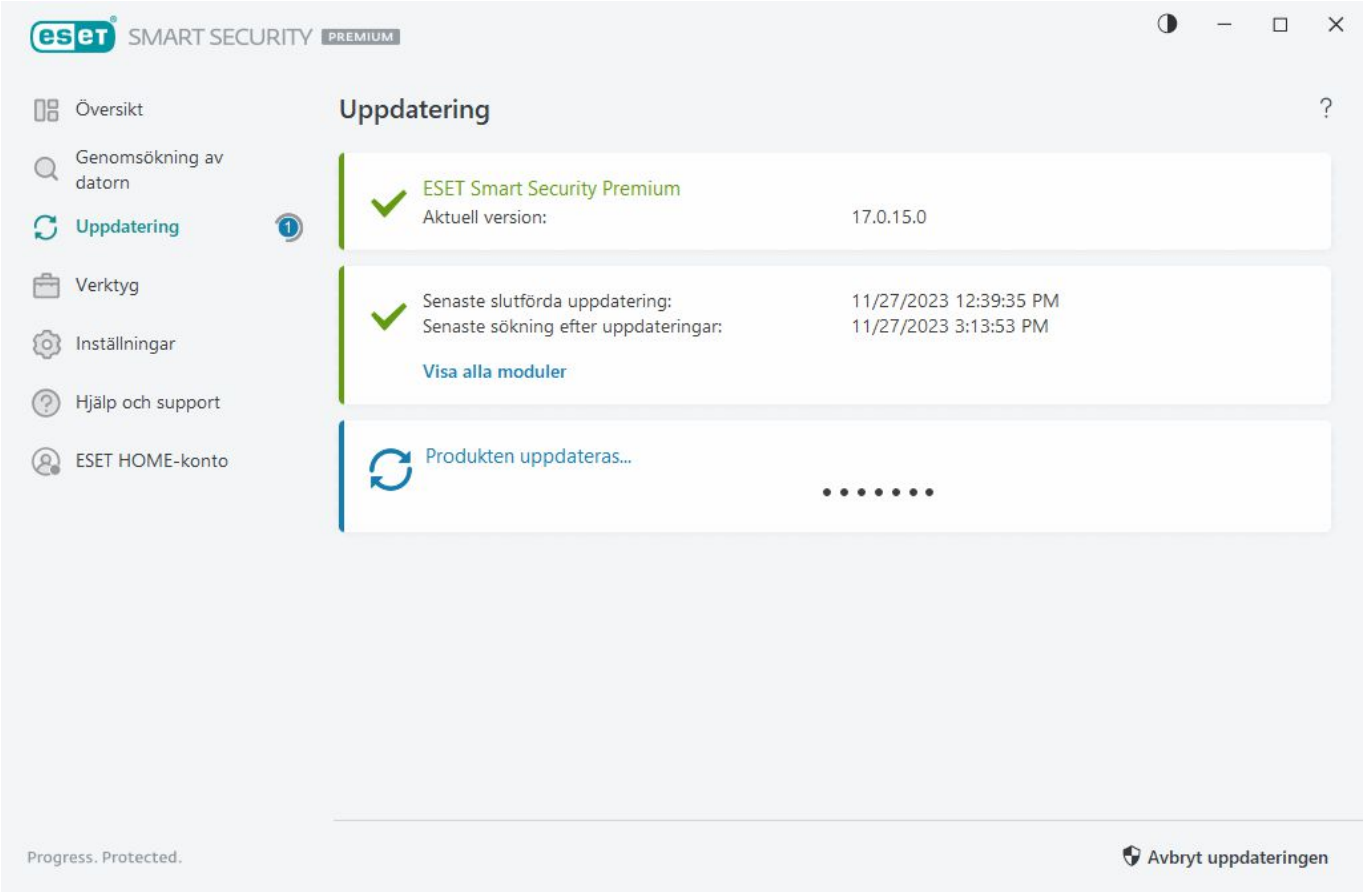
Lista över profiler – skapa nya eller ta bort befintliga uppdateringsprofiler.

Uppdateringar

Regelbunden uppdatering av ESET Smart Security Premium är det bästa sättet att säkerställa maximal säkerhetsnivå på datorn. Uppdateringsmodulen säkerställer att både programmodulerna och systemkomponenterna alltid är uppdaterade.

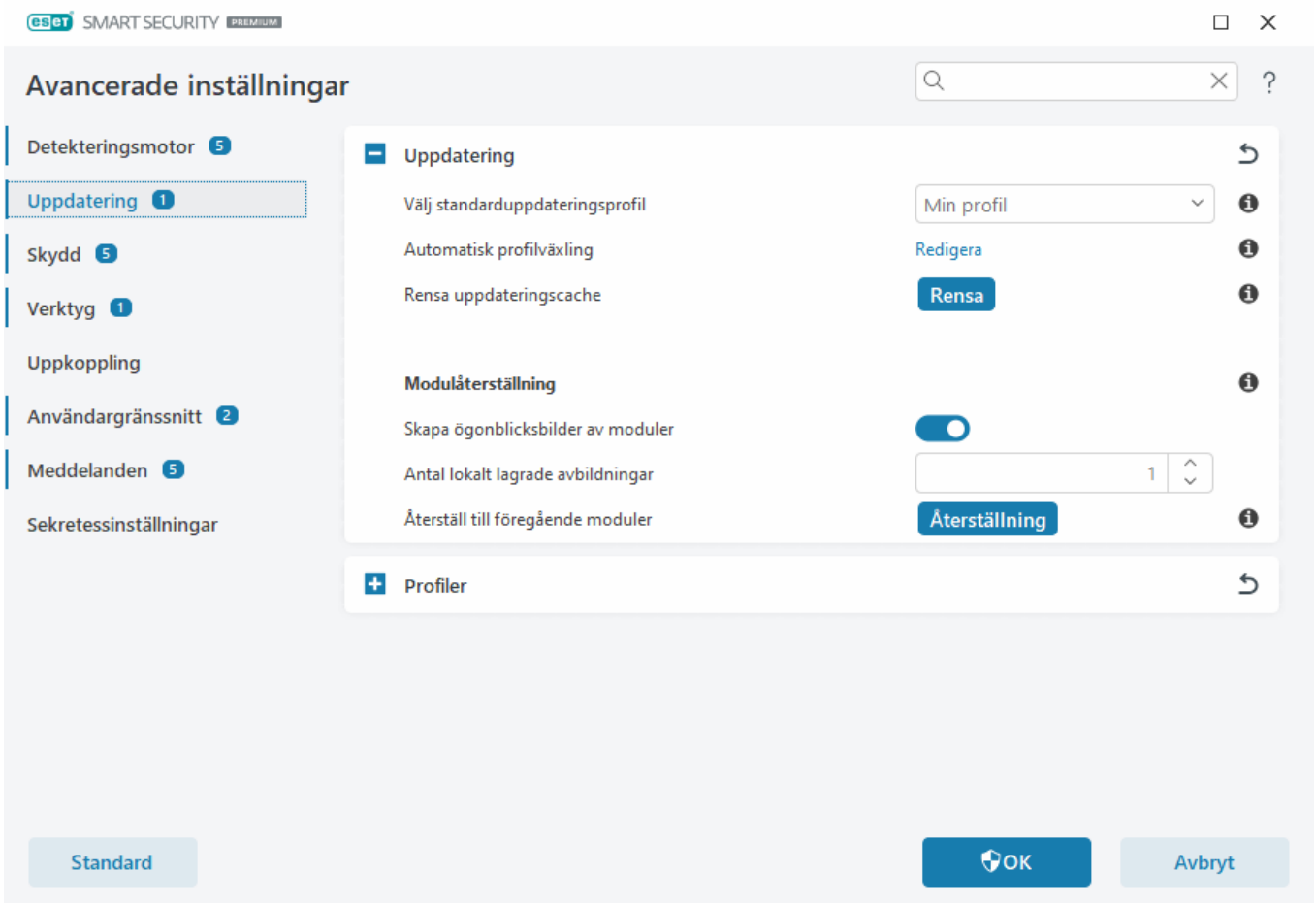
Genom att klicka på **Uppdatering** i programmets huvudfönster går det att visa aktuell uppdateringsstatus, inklusive datum och tid för den senaste uppdateringen och om en uppdatering behövs.

Förutom automatiska uppdateringar kan du klicka på **Sök efter uppdateringar** för att utlösa en manuell uppdatering.



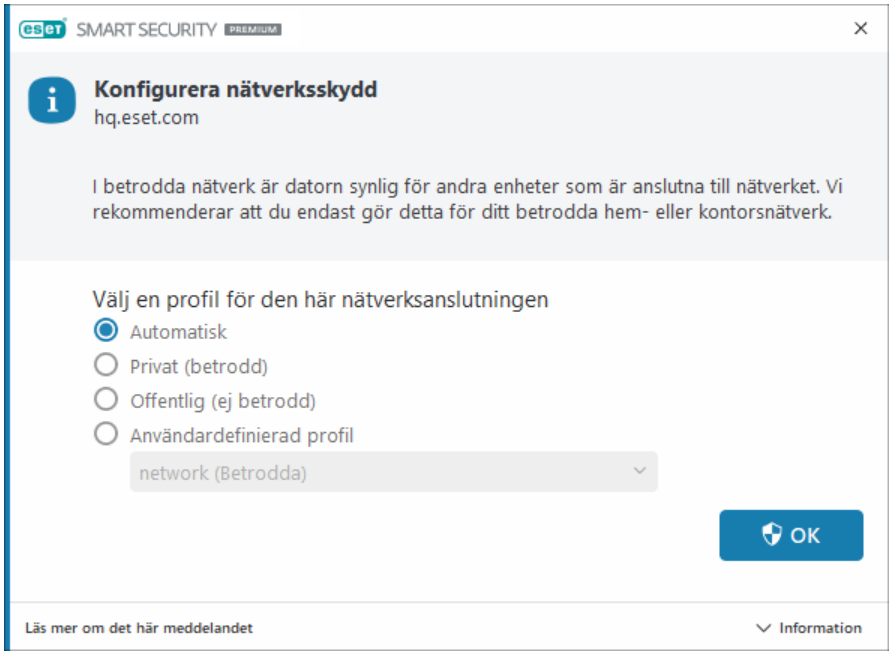
Avancerade inställningar > **Uppdatera** innehåller ytterligare uppdateringsalternativ som uppdateringsläge, proxyserveråtkomst och LAN-anslutningar.

Om det uppstår problem med en uppdatering klickar du på **Rensa** för att rensa uppdateringscachen. Se avsnittet Felsöka meddelandet Moduluppdateringen misslyckades om det fortfarande inte går att uppdatera programmodulerna.



Konfigurera nätverksskydd

Som standard använder ESET Smart Security Premium Windows-inställningar när en ny nätverksanslutning identifieras. Om du vill visa en dialogruta när ett nytt nätverk identifieras ska du ändra Tilldelning av nätverksskyddsprofil till **Fråga**. Konfiguration av nätverksskydd visas varje gång datorn ansluter till ett nytt nätverk.



Du kan välja mellan följande nätverksanslutningsprofiler:

Automatiskt – ESET Smart Security Premium väljer profilen automatiskt baserat på de aktivatorer som har konfigurerats för varje profil.

Privat – för betrodda nätverk (hem- eller kontorsnätverk). Datorn och delade filer som lagras på datorn är synliga för andra nätverksanvändare och systemresurserna är tillgängliga för andra användare i nätverket (åtkomst till delade filer och skrivare är aktiverad, inkommande RPC-kommunikation är aktiverad och fjärrdelning av skrivbord är aktiverad). Vi rekommenderar att du använder den här inställningen när du kommer åt ett säkert lokalt nätverk. Den här profilen tilldelas automatiskt till en nätverksanslutning om den är konfigurerad som ett Domän- eller Privat-närverk i Windows.

Offentligt – för ej betrodda nätverk (offentligt nätverk). Filer och mappar i systemet delas inte med eller är synliga för andra användare i nätverket och delning av systemresurser är inaktiverad. Vi rekommenderar att du använder den här inställningen vid åtkomst till trådlösa nätverk. Den här profilen tilldelas automatiskt till alla nätverksanslutningar som inte är konfigurerade som ett Domän- eller Privat-nätverk i Windows.

Användardefinierad profil – du kan välja en profil som du har skapat på rullgardinsmenyn. Det här alternativet är bara tillgängligt om du har skapat minst en anpassad profil.

⚠ En felaktig nätverkskonfiguration kan innebära en säkerhetsrisk för datorn.

Aktivera Stöldskydd

Under våra dagliga resor mellan hem och arbete eller andra offentliga platser riskerar vi ständigt att tappa bort eller bli bestulna på våra personliga enheter. Stöldskydd är en funktion som utökar användarens säkerhet i händelse av förlorad eller stulen enhet. Med Stöldskydd kan du spåra den saknade enheten och övervaka dess användning genom att söka upp IP-adressen i ESET HOME för att få tillbaka enheten och skydda din personliga data.

Genom att använda moderna tekniker som geografisk IP-adressuppsökning, lagring av webbkamerabild, skydd av användarkonto och enhetsövervakning kan Stöldskydd hjälpa dig och polisen att lokalisera datorn eller enheten om den försvinner eller stjäls. I ESET HOME kan du se vilken aktivitet som äger rum på din dator eller enhet.

Mer information om Stöldskydd i ESET HOME hittar du i ESET HOME-onlinehjälpen.

Stöldskydd kanske inte fungerar korrekt på datorer i domäner på grund av begränsningar i hanteringen av användarkonton.

Om du vill aktivera Stöldskydd och skydda enheten i händelse av förlust eller stöld väljer du något av följande alternativ:

- Klicka på **INSTÄLLNINGAR** bredvid **Stöldskydd** i programmets huvudfönster > **Översikt**.
- Om du ser meddelandet ”Anti-Theft är tillgängligt” i programmets huvudfönster > **Översikt**, klicka på **Aktivera Stöldskydd**.
- I programmets huvudfönster klickar du på **Inställningar** > **Säkerhetsverktyg**. Aktivera växlingsknappen **Stöldskydd** och följ instruktionerna på skärmen.

Om enheten inte är ansluten till ESET HOME måste du:
1. Logga in på ESET HOME-kontot vid aktivering av Stöldskydd.
2. Ange ett enhetsnamn.

Stöldskydd stöder inteMicrosoft Windows Home Server.

När du har aktiverat Stöldskydd kan du optimera enhetens säkerhet i huvudprogramfönstret > **Inställningar** > **säkerhetsverktyg** > **Stöldskydd**.

Föräldrakontroll

Om du redan har aktiverat föräldrakontroll i ESET Smart Security Premium måste du även konfigurera föräldrakontroll för alla relaterade användarkonton.

När föräldrakontrollen är aktiv och användarkonton inte har konfigurerats visar ESET Smart Security Premium meddelandet "Föräldrakontroll ej aktiverad" på skärmen **Översikt**. Klicka på **Ställ in regler** och se avsnittet Föräldrakontroll för mer information.

Produktaktivering

Det går att aktivera produkten på flera sätt. Tillgänglighet för ett visst aktiveringssätt i aktiveringsfönstret kan bero på land och distributionssätt (CD/DVD, ESET webbsida osv.):

- Om du har köpt en förpackad återförsäljarversion av produkten eller har fått ett e-postmeddelande med abonnemangsinformation aktiverar du produkten genom att klicka på **Använd en köpt aktiveringsnyckel**. Aktiveringsnyckeln måste anges för att slutföra aktiveringen. Aktiveringsnyckel– en unik sträng i formatet XXXX-XXXX-XXXX-XXXX-XXXX eller XXXX-XXXXXXXX som används för att identifiera abonnemangsägaren och aktivera abonnemanget. Aktiveringsnyckeln finns normalt inne i eller på baksidan av produktens förpackning.

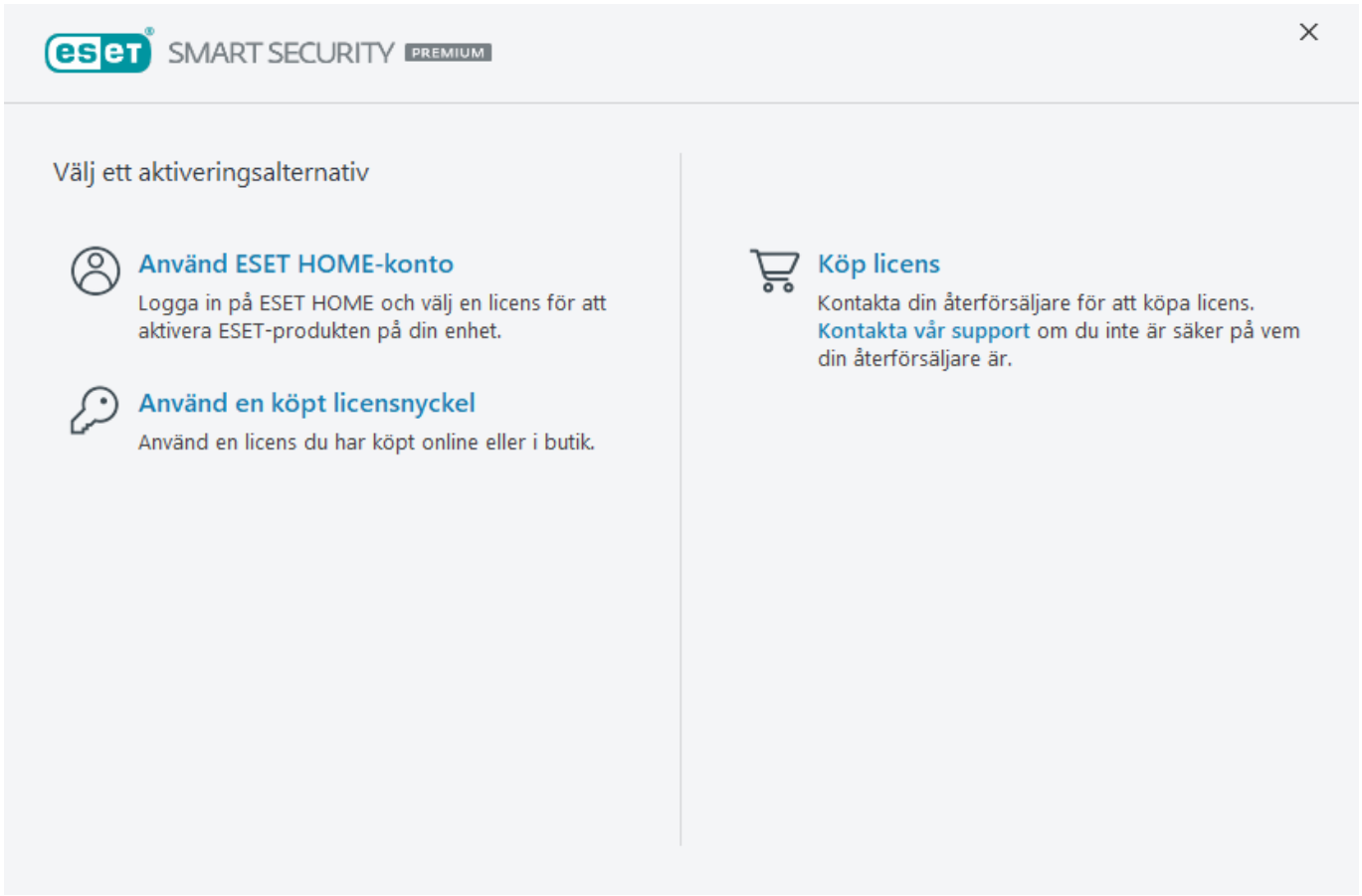
- När du har valt Använd ESET HOME-konto ombeds du att logga in på ditt ESET HOME-konto.

- Om du vill prova ESET Smart Security Premium innan du köper det, välj Gratis utvärdering. Ange din e-postadress och ditt land för att aktivera ESET Smart Security Premium under en begränsad tid. Din kostnadsfria provversion skickas till dig via e-post. Det går endast att aktivera en konstnadsfri provversion per kund.

- Har du inget abonnemang och vill köpa ett, klicka på **Köp abonnemang**. Detta för dig till ESET:s lokala återförsäljares webbplats. Abonnemang på Windows-hemprodukter från ESET är inte kostnadsfria.

Du kan ändra abonnemanget på produkten när som helst. Om du vill göra det klickar du på **Hjälp och support** > **Ändra abonnemang** i programmets huvudfönster. Då visas det offentliga abonnemang-ID:t som behövs för att identifiera abonnemanget för ESET:s support.

Misslyckades produktaktiveringen?



Ange din aktiveringsnyckel under aktiveringen

Automatiska uppdateringar är viktiga för din säkerhet. ESET Smart Security Premium tar endast emot uppdateringar när det aktiverats.

När du anger din **Aktiveringsnyckel** är det viktigt att den anges exakt som den är skriven. Aktiveringsnyckeln är en unik sträng i formatet XXXX-XXXX-XXXX-XXXX-XXXX som används för att identifiera abonnemangsägaren och aktivera abonnemanget.

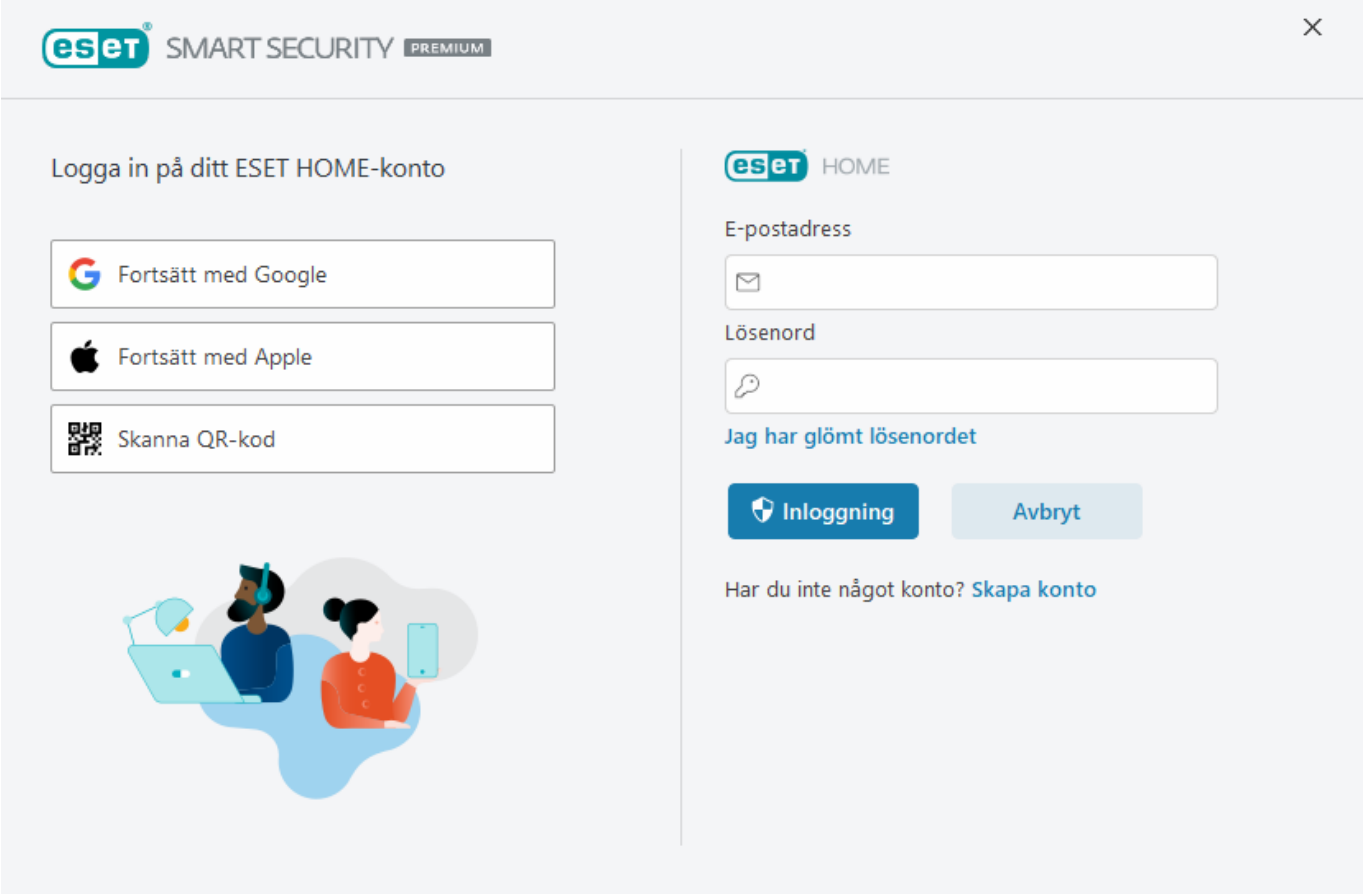
Vi rekommenderar att kopiera och klistra in aktiveringsnyckel från registreringsmeddelandet för noggrannhet.

Om aktiveringsnyckel inte anges efter installationen aktiveras inte produkten. Du kan aktivera ESET Smart Security Premium i huvudprogramfönstret > **Hjälp och support** > **Aktivera abonnemang**.

ESET:s abonnemang för Windows Home-produkter är inte kostnadsfria.

Använd ESET HOME-konto

Anslut din enhet till ESET HOME för att visa och hantera alla dina aktiverade ESET-abonnemang och enheter. Du kan förnya, uppgradera eller utöka abonnemanget och visa viktig information. I ESET HOME-hanteringsportalen eller -mobilappen kan du lägga till olika abonnemang, ladda ned produkter till dina enheter, kontrollera produktens säkerhetsstatus eller dela abonnemang via e-post. Mer information finns i ESET HOME-onlinehjälpen.



När du har valt **Använd ESET HOME-konto** som aktiveringsmetod eller vid anslutning till ESET HOME-konto under installationen:

1. Logga in på ditt ESET HOME konto.

> Om du inte har ett ESET HOME-konto klickar du på **Skapa konto** för att registrera dig eller läser anvisningarna i ESET HOME-onlinehjälpen.
> Om du har glömt ditt lösenord klickar du på **Jag har glömt lösenordet** och följer stegen på skärmen eller läser anvisningarna i ESET HOME-onlinehjälpen.

2. Ange ett **enhetsnamn** för enheten som ska användas i alla ESET HOME-tjänster och klicka på **Fortsätt**.

3. Välj ett abonnemang som ska aktiveras eller lägg till ett nytt abonnemang. Klicka på **Fortsätt** för att aktivera ESET Smart Security Premium.

Aktivera kostnadsfri provversion

För att aktivera provversionen av ESET Smart Security Premium anger du en giltig e-postadress i fälten **E-postadress** och **Bekräfta e-postadress**. Efter aktivering genereras ditt ESET-abonnemang och skickas till din e-postadress. Denna e-postadress används även för meddelanden om produktens utgångsdatum och annan kommunikation med ESET. Den kostndasfria provversionen kan endast aktiveras en gång.

Välj ditt land på rullgardinsmenyn **Land** för att registrera ESET Smart Security Premium hos din lokala leverantör, som ger teknisk support.

Kostnadsfri ESET-aktiveringsnyckel

Abonnemanget på ESET Smart Security Premium är inte gratis.

ESET-aktiveringsnyckel är en unik sekvens med bokstäver och siffror separerade med ett tankstreck som tillhandahålls av ESET för att möjliggöra laglig användning av ESET Smart Security Premium enligt licensavtalet. Varje slutanvändare har endast rätt att använda aktiveringsnyckel i den utsträckning som denne har rätt att använda ESET Smart Security Premium baserat på antalet licenser som har tilldelats av ESET. Aktiveringsnyckeln betraktas som konfidentiell och kan inte delas. Du kan dock dela ett abonnemang med hjälp av ESET HOME.

Det finns källor på internet som kan förse dig med en ”kostnadsfri” ESET-aktiveringsnyckel, men tänk på att:

- Om du klickar på en annons för ett ”gratis ESET-abonnemang” kan du äventyra datorns eller enhetens säkerhet med risk för att de infekteras med skadlig kod. Skadlig kod kan döljas i icke-officiellt webbinnehåll (till exempel videofilmer), webbplatser som tjänar pengar på dina besök och så vidare. Vanligen är dessa en fälla.

- ESET kan inaktivera piratkopierade abonnemang och gör även detta.

- Att ha en piratkopierad aktiveringsnyckel är inte förenligt med licensavtalet för slutanvändare som du måste godkänna för att installera ESET Smart Security Premium.

- Köp endast ESET-abonnemang genom officiella kanaler som till exempel www.eset.com, ESET:s distributörer eller återförsäljare (köp inte abonnemang från icke-officiella webbplatser som till exempel eBay eller delade licenser från tredje part).

- Att hämta en ESET Smart Security Premium kostar inget, men för att kunna aktivera den under installationen krävs en giltig ESET-Aktiveringsnyckel (du kan hämta och installera produkten, men utan aktivering fungerar den inte)

- Dela inte ditt abonnemang på internet eller sociala medier (det kan spridas vidare).

Om du vill identifiera och rapportera ett piratkopierat ESET-abonnemang ska du gå till vår artikel i kunskapsbasen för vägledning.

Om du är osäker på om du vill köpa en ESET-säkerhetsprodukt kan du använda en provversion medan du bestämmer dig:

1. Aktivera ESET Smart Security Premium med en kostnadsfri provversion

2. Delta i ESET:s betaprogram

3. Installera ESET Mobile Security om du använder en mobil enhet med Android – den är ”freemium” (kostnadsfri premium).

Förnya din ESET-produkt om du vill få rabatt/förlänga din licens.

Aktiveringen misslyckades – vanliga scenarier

Om aktiveringen av ESET Smart Security Premium inte lyckas är de vanligaste scenarierna:

- Aktiveringsnyckeln används redan.
- Du har angett en ogiltig aktiveringsnyckel.
- Informationen i aktiveringsformuläret saknas eller är ogiltig.
- Kommunikationen med aktiveringsservern misslyckades.
- Ingen eller inaktiverad anslutning till ESET:s aktiveringsservrar.

Kontrollera att du har angett rätt aktiveringsnyckel och att internetanslutningen är aktiv. Försök att aktivera ESET Smart Security Premium igen. Om du använder ett ESET HOME-konto för aktivering, se ESET HOME Abonnemang och abonnemanshantering – Onlinehjälp.

Om du får ett specifikt felmeddelande (till exempel Avstängt abonnemang eller Abonnemang överanvänds) följer du anvisningarna under abonnemangsstatus.

Om du fortfarande inte kan aktivera ESET Smart Security Premium leder ESET:s felsökning om aktivering dig igenom vanliga frågor, fel och problem med aktivering och licensiering (finns på engelska och flera andra språk).

Abonnemangsstatus

Ditt abonnemang kan ha olika status. Du hittar din abonnemangsstatus i ESET HOME. Information om hur du lägger till ditt abonnemang i ditt ESET HOME-konto finns i Lägga till ett abonnemang.

Om du inte har ett ESET HOME-konto kan du skapa ett nytt ESET HOME-konto.

Om abonnemangstatusen är en annan än **Aktiv** visas ett fel under aktiveringen eller så får du ett meddelande i programmets huvudfönster.

Om du vill inaktivera statusmeddelanden för abonnemang öppnar du Avancerade inställningar > **Meddelanden** > **Programstatusar**. Klicka på **Redigera** bredvid **Programstatusar**, utöka **Licensiering** och avmarkera kryssrutan bredvid det meddelande du vill inaktivera. Att inaktivera meddelandet löser inte problemet.

Se beskrivningar och rekommenderade lösningar för olika abonnemangstatusar i tabellen nedan:

Abonnemangsstatus	Beskrivning	Lösning
Aktiv	Abonnemanget är giltigt och ingen interaktion behövs. ESET Smart Security Premium kan aktiveras och du hittar abonnemanginformationen i programmets huvudfönster > **Hjälp och support**.	
Överanvänds	Fler enheter använder abonnemanget än vad som är tillåtet. Du får ett aktiveringsfel.	Se Aktiveringen misslyckades på grund av överanvänt abonnemang för mer information.

Abonnemangsstatus	Beskrivning	Lösning
Avstängd	Abonnemanget har stängts av på grund av betalningsproblem. Om du vill använda abonnemanget ska du se till att dina betalningsuppgifter i ESET HOME är aktuella eller så kontaktar du abonnemangåterförsäljaren. Du kan få det här felet under aktiveringen eller i huvudprogramfönstret.	Installerad produkt – om du har ett ESET HOME-konto klickar du på **Hantera din abonnemang i ESET HOME** i meddelandet som visas i huvudprogramfönstret och granskar dina betalningsuppgifter. Annars kontaktar du abonnemangsåterförsäljaren. Aktiveringsfel – om du har ett ESET HOME-konto klickar du på **Öppna ESET HOME** i fönstret för aktiveringsfelet och granskar dina betalningsuppgifter. Annars kontaktar du abonnemangsåterförsäljaren.
Har upphört	Abonnemanget har upphört och du kan inte använda abonnemanget för att aktivera ESET Smart Security Premium. Du kan få det här felet under aktiveringen eller i huvudprogramfönstret. Om ESET Smart Security Premium redan är installerad är datorn inte skyddad eller uppdaterad.	Installerad produkt – i meddelandet som visas i programmets huvudfönster klickar du på **Förnya abonnemang** och följer anvisningarna i Hur förnyar jag mitt abonnemang? eller så klickar du på **Aktivera produkt** och väljer aktiveringsmetod. Aktiveringsfel – i fönstret för aktiveringsfel klickar du på **Förnya ditt abonnemang** och följer anvisningarna i Hur förnyar jag mitt abonnemang? eller så skriver du in en ny eller förnyad aktiveringsnyckel och klickar på **Förnya abonnemang**.
Avbruten	Ditt abonnemang har avbrutits av ESET eller av din abonnemangsåterförsäljare.	Om du får ett felmeddelande: Avbrutet abonnemang i programmets huvudfönster eller under aktiveringen och ditt abonnemang ska fungera korrekt, kontakta din abonnemangsåterförsäljare.

Aktiveringen misslyckades på grund av överanvänt abonnemang

Problem

- Ditt abonnemang kanske överanvänds eller uttnyttjas i skadliga syften
- Aktiveringen misslyckades på grund av överanvänt abonnemang

Lösning

Fler enheter använder abonnemanget än vad som är tillåtet. Du kan vara drabbad av piratkopiering eller förfalskning av programvara. Abonnemanget kan inte användas för att aktiva någon annan ESET-produkt. Du kan lösa problemet direkt om du är behörig att hantera abonnemanget på ditt ESET HOME-konto eller om du har köpt abonnemanget från en legitim källa. Om du inte har ett konto än så skapar du ett.

Om du är en abonnemangsägare och du inte uppmanades att ange din e-postadress:

1. Om du vill hantera ditt ESET-abonnemang öppnar du en webbläsare och går till https://home.eset.com. Besök ESET License Manager och ta bort eller inaktivera klienter. Mer information finns i Så ska du göra om ett abonnemang överanvänds.

2. Om du vill identifiera och rapportera ett piratkopierat ESET-abonnemang ska du gå till vår artikel om att identifiera och rapportera piratkopierade ESET-abonnemang för att få vägledning.

3. Om du är osäker klickar du på **Tillbaka** och kontaktar ESET:s tekniska support via e-post.

Om du inte är abonnemangets ägare ska du kontakta abonnemangsägaren och berätta att du inte kan aktivera ESET-produkten på grund av att abonnemanget överanvänds. Ägaren kan lösa problemet i ESET HOME-portalen.

Om du ombeds att bekräfta din e-postadress (endast flera fall) anger du den e-postadress som används vid köpet eller aktiveringen av ESET Smart Security Premium.

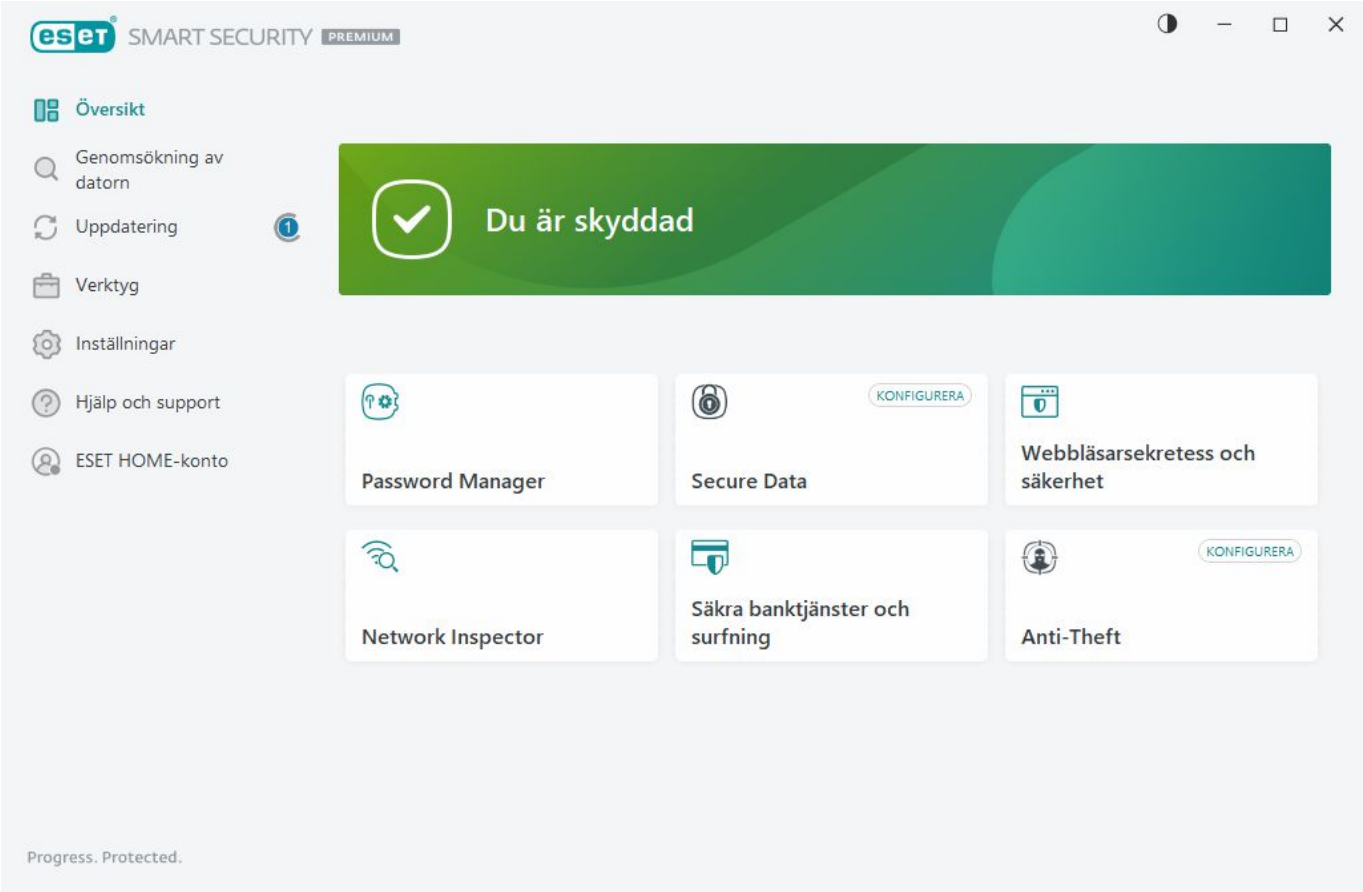
Arbeta med ESET Smart Security Premium

Huvudprogramfönstret för ESET Smart Security Premium är indelat i två delar. Det primära fönstret till höger visar information som motsvarar alternativt som valts i huvudmenyn till vänster.

> **Anvisningar med bilder**
> Se Öppna huvudprogramfönstret för ESET Windows-produkter för illustrerade instruktioner som finns på engelska och flera andra språk.

Du kan välja färgschemat för användargränssnittet för ESET Smart Security Premium i det övre högra hörnet av huvudprogramfönstret. Klicka på ikonen **Färgschema** (ikonen ändras baserat på det valda färgschemat) bredvid ikonen **Minimera** och välj färgschemat i den nedrullningsbara menyn:

- **Samma som systemfärgen** – ställer in färgschemat för ESET Smart Security Premium baserat på operativsystemets inställningar.
- **Mörkt** – ESET Smart Security Premium kommer att ha ett mörkt färgschema (mörkt läge).
- **Ljust** – ESET Smart Security Premium kommer att ha ett vanligt, ljust färgschema.



Huvudmenyns alternativ:

Översikt – ger information om skyddsstatus för ESET Smart Security Premium.

Genomsökning av datorn – konfigurera och starta en genomsökning av datorn eller skapa en anpassad genomsökning.

Uppdatering – visar information om modul- och detekteringsmotoruppdateringar.

Verktyg – ger åtkomst till Network Inspector och andra funktioner som förenklar programadministration och innehåller ytterligare alternativ för avancerade användare.

Inställningar – ger konfigurationsalternativ för skyddsfunktionerna i ESET Smart Security Premium (Datorskydd, Internetskydd, Nätverksskydd och Säkerhetsverktyg) och åtkomst till Avancerade inställningar.

Hjälp och support – visar information om ditt abonnemang, den installerade ESET-produkten och länkar till onlinehjälpen, ESET:s kunskapsbas och teknisk support.

ESET HOME-konto – anslut enheten till ESET HOME eller granska ESET HOME-kontots anslutningsstatus. Använd ESET HOME för att visa och hantera dina Stöldskydd-inställningar och aktiverade ESET-abonnemang och enheter.

Översikt

I fönstret **Översikt** visas information om datorns aktuella skydd tillsammans med snabblänkar till säkerhetsfunktionerna i ESET Smart Security Premium.

Fönstret **Översikt** visar meddelanden med detaljerad information och rekommenderade lösningar för att förbättra säkerheten för ESET Smart Security Premium, aktivera ytterligare funktioner eller säkerställa maximalt

skydd. Om det finns fler meddelanden klickar du på **X meddelanden till** för att visa alla.

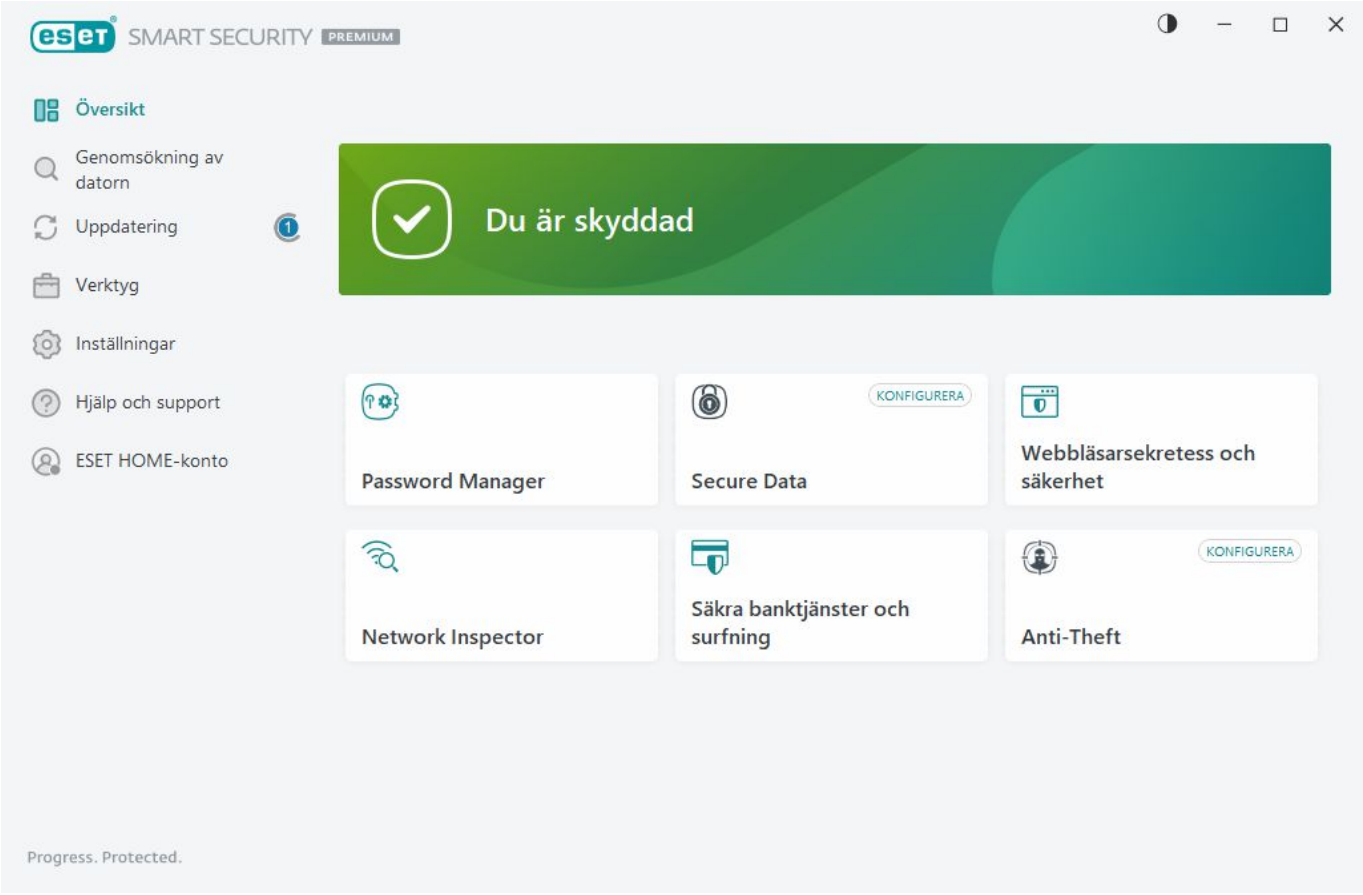
Password Manager – öppnar instruktioner om hur du installerar Password Manager.

Network Inspector – Kontrollera nätverkets säkerhet.

Secure Data – öppnar Säkerhetsverktyg. Klicka på växlingsknappen bredvid **Secure Data** för att aktivera den. Om du redan har aktiverat Secure Data öppnar snabblänken sidan Secure Data.

Säkra banktjänster och surfning – Startar standardwebbläsaren i Windows i ett säkert läge.

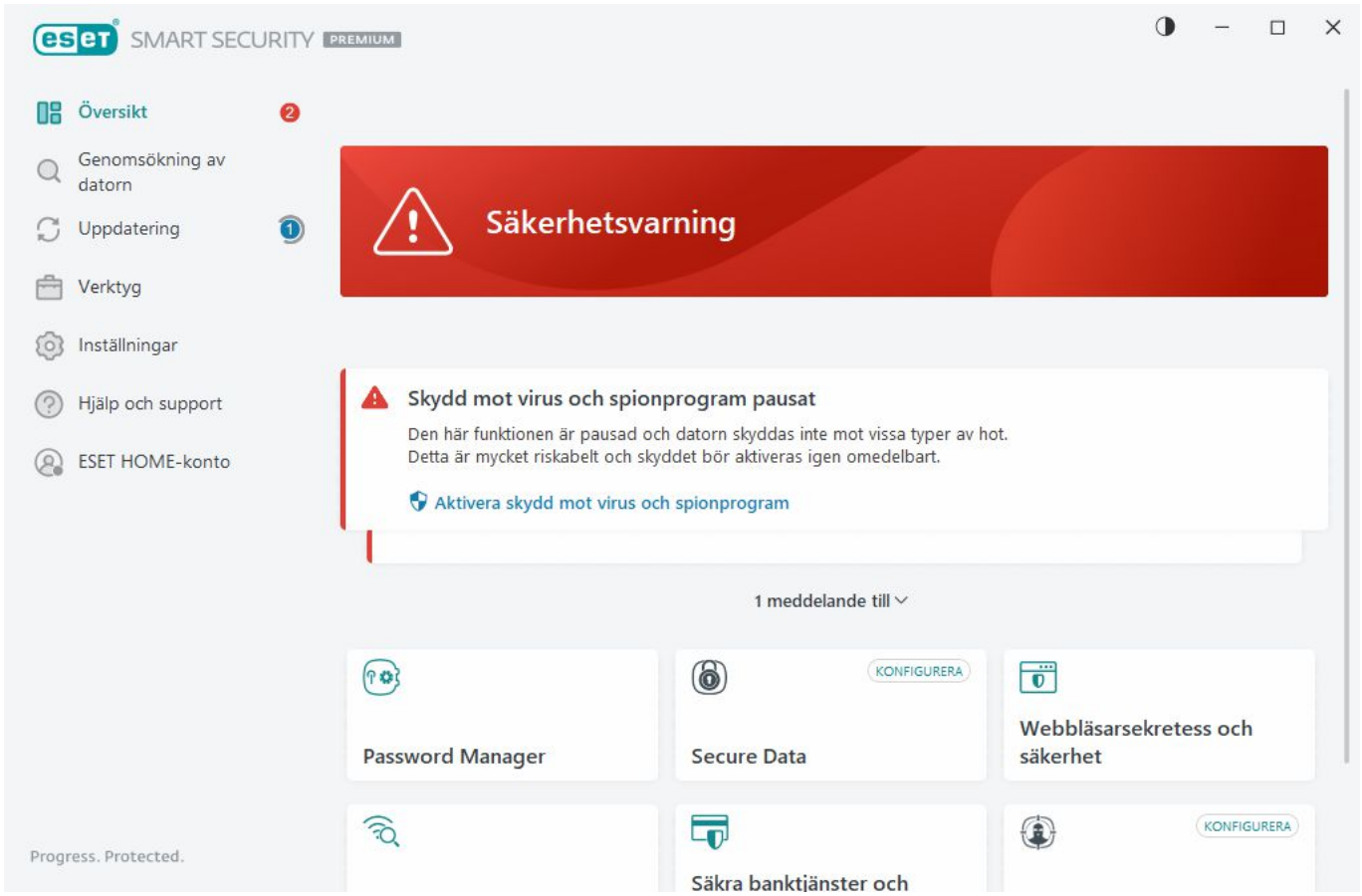
Stöldskydd – startar installationen av Stöldskydd. Om du redan har installerat Stöldskydd öppnar snabblänken sidan Stöldskydd.



Den gröna ikonen och gröna statusen **Du är skyddad** visar att maximalt skydd garanteras.

Vad gör jag om programmet inte fungerar

Om en aktiv skyddsmodul fungerar korrekt är dess skyddsstatusikon grön. Ett rött utropstecken eller en orange meddelandeikon indikerar att maximalt skydd inte är säkerställt. Ytterligare information om skyddsstatus för varje modul, liksom föreslagna lösningar för att återställa fullständigt skydd, visas som ett meddelande i fönstret **Översikt**. Ändra status för enskilda moduler genom att klicka på **Inställningar** och välja önskad modul.



Den röda ikonen och den röda **säkerhetsvarningsstatusen** indikerar kritiska problem. Det finns flera skäl till att denna status kan visas, som till exempel:

- **Produkten är inte aktiverad** eller **Abonnemanget har upphört** – detta indikeras med en röd skyddsstatusikon. Programmet kan inte uppdateras när abonnemanget har upphört. Följ anvisningarna i varningsfönstret för att förnya abonnemanget.
- **Detekteringsmotorn är inaktuell** – detta fel visas efter flera misslyckade försök att uppdatera detekteringsmotorn. Vi rekommenderar att kontrollera uppdateringsinställningarna. Den vanligaste orsaken till detta fel är felaktigt angivna autentiseringsdata eller felaktigt konfigurerade anslutningsinställningar.
- **Skydd av filsystemet i realtid är inaktiverat** – skyddet av filsystemet i realtid har inaktiverats av användaren. Datorn skyddas inte mot vissa hot. Klicka på **Aktivera skydd av filsystemet i realtid** om du vill aktivera funktionen igen.
- **Skydd mot virus och spionprogram inaktiverade** – du kan aktivera skyddet mot virus och spionprogram igen genom att klicka på **Aktivera skydd mot virus och spionprogram**.
- **ESET-brandväggen är inaktiverad** – detta problem indikeras även med ett säkerhetsmeddelande intill objektet **Nätverk** på skrivbordet. Det går att återaktivera nätverksskyddet genom att klicka på **Aktivera brandvägg**.

Den orangea ikonen indikerar begränsat skydd. Det kan exempelvis vara problem med att uppdatera abonnemanget eller så kan abonnemangets utgångsdatum närma sig.
Det finns flera skäl till att denna status kan visas, som till exempel:

- **Stöldskydd optimeringsvarning** – den här enheten är inte optimerad för Stöldskydd. Till exempel kan inte ett fantomkonto (en säkerhetsfunktion som aktiveras automatiskt när en enhet markeras som

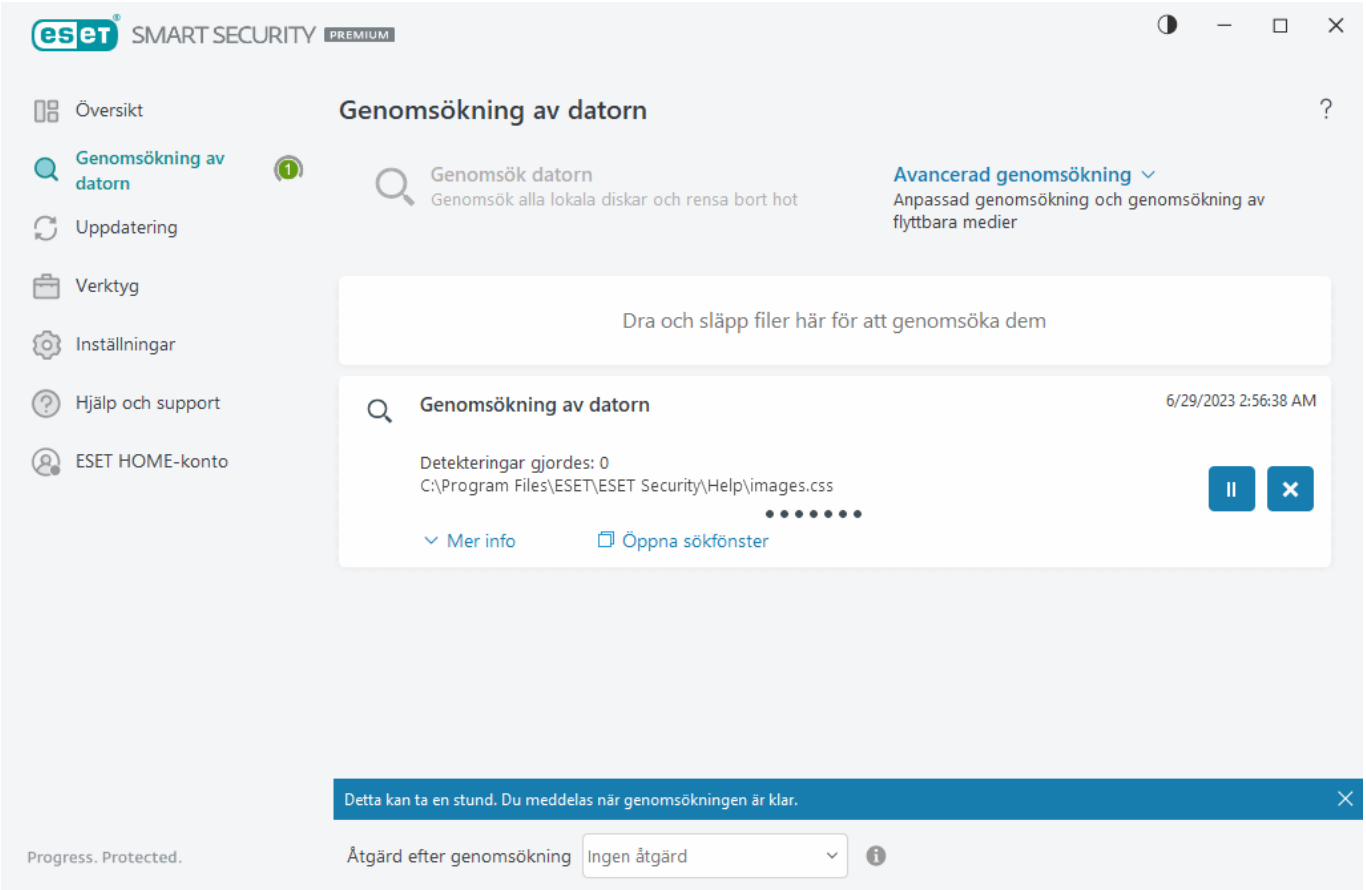
saknad) skapas på datorn. Du kan skapa ett fantomkonto med hjälp av funktionen Optimering i Stöldskydd-webbgränssnittet.

- **Spelläge aktivt** – att aktivera Spelläge är en potentiell säkerhetsrisk. Om denna funktion aktiveras inaktiveras alla meddelande/aviseringsfönster och schemalagda åtgärder stoppas.
- **Abonnemanget upphör snart/Abonnemanget upphör idag** – detta indikeras genom att skyddsstatusikonen och visar ett utropstecken intill systemklockan. När ditt abonnemang har upphört kan programmet inte uppdateras och skyddsstatusikonen blir röd.

Om det inte går att lösa problemet med förslagen, klicka på **Hjälp och support** för att visa hjälpfilerna eller sök i ESET:s kunskapsbas. Om du fortfarande behöver hjälp kan du skicka in en supportfråga. ESET tekniska support svarar snabbt på dina frågor och hjälper dig att hitta en lösning.

Genomsökning av datorn

Skannern utgör en viktig del av virusskyddet. Den används för att göra genomsökningar av filer och mappar på datorn. Av säkerhetsskäl är det mycket viktigt att genomsökningar av datorn utförs regelbundet som en del av rutinåtgärderna för säkerhet, inte endast när en infektion misstänks. Vi rekommenderar att göra regelbundna genomsökningar av systemet för att identifiera virus som inte upptäcks av Skydd av filsystemet i realtid när de skrivs till disk. Detta kan inträffa om skyddet av filsystemet i realtid är inaktiverat vid det tillfället, om detekteringsmotorn är inaktuell eller om filen inte identifieras som ett virus när den sparas till disken.



Det finns två typer av **genomsökning av datorn**. **Genomsök datorn** genomsöker systemet utan att några genomsökningsparametrar anges. **Anpassad genomsökning** (under Avancerad genomsökning) gör det möjligt att välja bland fördefinierade genomsökningsprofiler utformade för specifika platser och att välja specifika genomsökningsobjekt.

Se Genomsökningsförlopp för mer information om genomsökningprocessen.

> Som standard ESET Smart Security Premium försöker automatiskt att rensa eller ta bort detekteringar som hittades under datorgenomsökningen. I vissa fall, om ingen åtgärd kan utföras, får du en interaktiv varning och måste välja en rensningsåtgärd (till exempel ta bort eller ignorera). Om du vill ändra rensningsnivå och för mer detaljerad information, se Rensning. För att granska tidigare genomsökningar, se Loggfiler.

Genomsök datorn

Genomsök datorn startar snabbt en genomsökning av datorn och rensar infekterade filer utan användaråtgärder. Fördelen med **Genomsök datorn** är att den är enkel att använda och inte kräver en noggrann konfiguration av genomsökningen. Genomsökningen kontrollerar alla filer på alla lokala enheter och rensar eller tar bort identifierade infiltrationer. Rensningsnivån är automatiskt inställd på standardvärdet. Se Rensning om du vill ha mer information om olika typer av rensning.

Du kan även använda funktionen **Genomsökning med dra och släpp** för att genomsöka en fil eller mapp manuellt genom att klicka på filen eller mappen, flytta muspekaren till det markerade området med musknappen nedtryckt och sedan släppa den. Därefter flyttas programmet fram till förgrunden.

Följande genomsökningsalternativ är tillgängliga under **Avancerade genomsökningar**:

Anpassad genomsökning

Anpassad genomsökning gör det möjligt att ange genomsökningsparametrar som t.ex. genomsökningsobjekt och metoder. Fördelen med **anpassad genomsökning** är att du kan konfigurera parametrarna i detalj. Konfigurationerna går att spara som användardefinierade genomsökningsprofiler som kan vara användbara om en genomsökning upprepas med samma parametrar.

Genomsökning av flyttbara medier

Liknar **Genomsök datorn** – starta snabbt en genomsökning av flyttbara medier (som t.ex. CD/DVD/USB) som för tillfället är anslutna till datorn. Detta kan vara praktiskt när du ansluter en USB-flashenhet till en dator och vill genomsöka dess innehåll efter potentiella hot.

Denna typ av genomsökning går även att starta genom att klicka på **Anpassad genomsökning**, välja **Flyttbara medier** i listrutan **Genomsökningsobjekt** och klicka på **Genomsök**.

Upprepa senaste genomsökning

Gör att du snabbt kan starta den senast genomförda genomsökningen med samma inställningar som den kördes med.

Med listrutan **Åtgärd efter genomsökning** kan du ange en åtgärd som ska utföras automatiskt när en genomsökning har slutförts:

- **Ingen åtgärd** – ingen åtgärd utförs efter att en genomsökning är klar.
- **Avstängning** – datorn stängs av när en genomsökning är klar.
- **Starta om vid behov** – datorn startas om det bara behövs för att slutföra rensningen av upptäckta hot.

- **Omstart** – alla öppna program stängs och datorn startas om när en genomsökning är klar.

- **Tvinga starta om vid behov** – datorn tvingas att starta om det bara behövs för att slutföra rensningen av upptäckta hot.

- **Tvinga omstart** – tvingar stängning av alla öppna program utan att vänta på användarinteraktion och startar om datorn när en genomsökning är klar.

- **Vänteläge** – sessionen sparas och datorn försätts i vänteläge så att arbetet snabbt kan återupptas.

- **Viloläge** – allt i RAM-minnet flyttas till en speciell fil på hårddisken. Datorn stängs av, men återgår till sitt föregående tillstånd nästa gång den startas.

> Åtgärderna **Vänteläge** eller **Viloläge** är tillgängliga baserat på operativsystemets inställningar för ström och vänteläge på datorn eller datorns/den bärbara datorns funktioner. Tänk på att en dator i vänteläge fortfarande är i drift. Grundläggande funktioner körs fortfarande och kraft förbrukas när datorn körs på batteridrift. För att spara batterikraft, exempelvis på resor utanför kontoret, rekommenderas alternativet Viloläge.

Den valda åtgärden startas efter att alla genomsökningar som körs har slutförts. När du väljer **Avstängning** eller **Omstart** visas en bekräftelsedialogruta med en nedräkning på 30 sekunder (klicka på **Avbryt** om du vill inaktivera den begärda åtgärden).

> Vi rekommenderar att en genomsökning av datorn görs minst en gång i månaden. Det går att konfigurera genomsökning som en schemalagd aktivitet i **Verktyg** > **Schemaläggaren**. Schemalägga en veckovis genomsökning av datorn

Starta anpassad genomsökning

Om du vill genomsöka arbetsminne, nätverk eller vissa delar av en disk istället för hela disken kan du göra en anpassad genomsökning. I så fall klickar du på **Avancerade genomsökningar** > **Anpassad genomsökning** och markerar specifika mål i trädstrukturen.

Det går att välja en profil på rullgardinsmenyn **Profil** som ska användas vid genomsökning av specifika målobjekt. Standardprofilen är **Smart genomsökning**. Det finns ytterligare tre fördefinierade genomsökningsprofiler kallade **Djup genomsökning**, **Genomsökning av kontextmeny** och **Genomsökning av datorn**. Dessa genomsökningsprofiler använder olika ThreatSense-parametrar. De tillgängliga alternativen beskrivs i Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Genomsökning på begäran** > ThreatSense.

Mapp(träd)strukturen innehåller även specifika genomsökningsmål.

- **Arbetsminne** – söker igenom alla processer och data som för närvarande används av arbetsminnet.

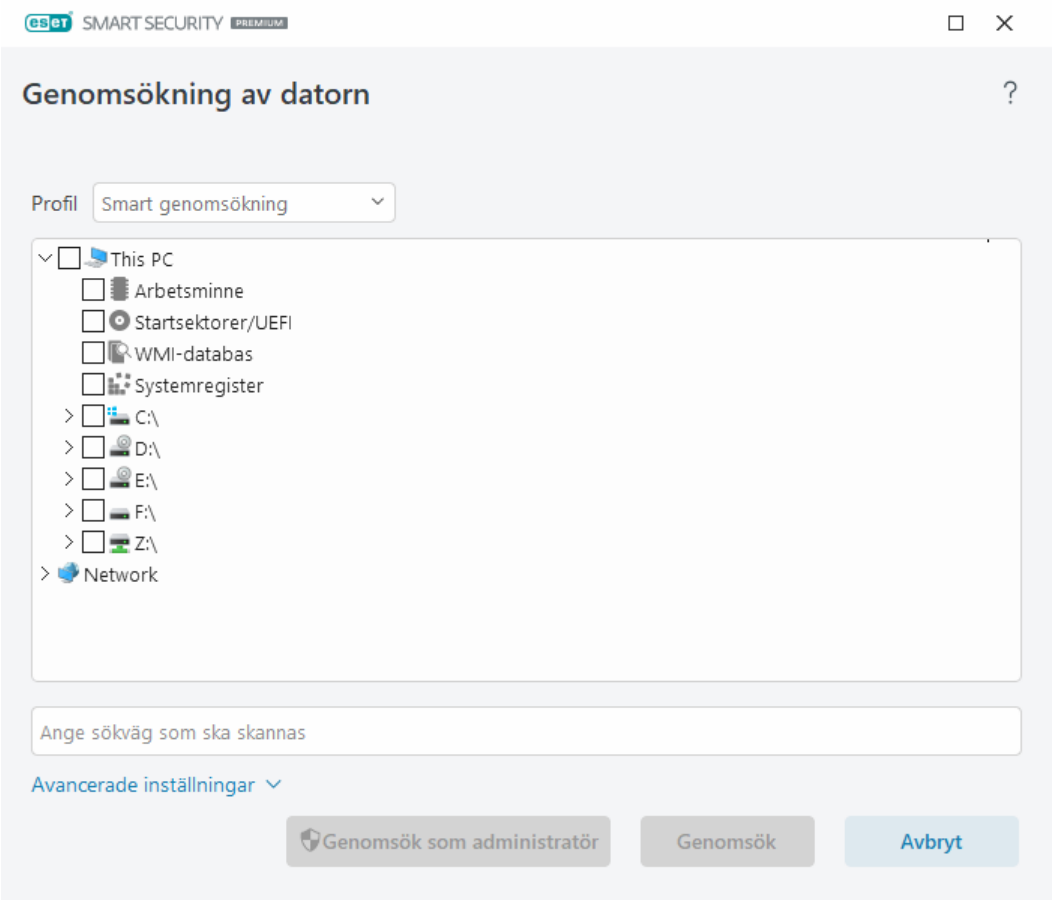
- **Startsektorer/UEFI** – genomsöker startsektorerna och UEFI efter skadlig kod. Läs mer om UEFI-skannern i ordlistan.

- **WMI-databas** – söker igenom hela Windows Management Instrumentation (WMI)-databasen, alla namnrymder, alla klassinstanser och alla egenskaper. Söker efter referenser till infekterade filer eller skadlig kod inbäddad som data.

• **Systemregistret** – söker igenom hela systemregistret, alla nycklar och undernycklar. Söker efter referenser till infekterade filer eller skadlig kod inbäddad som data. När detekteringarna rensas finns referensen kvar i registret så att ingen viktig data går förlorad.

Om du snabbt vill navigera till ett genomsökningsmål (fil eller mapp) skriver du dess sökväg i textfältet under trädstrukturen. Sökvägen är skiftlägeskänslig. Om du vill inkludera målet i genomsökningen markerar du dess kryssruta i trädstrukturen.

> **Schemalägga en veckovis genomsökning av datorn**
> Om du vill schemalägga en regelbunden aktivitet läser du kapitlet Schemalägga en veckovis genomsökning av datorn.



Du kan konfigurera rensningsparametrar för genomsökningen i Avancerade inställningar > **Detekteringsmotor** > **Genomsökning efter skadlig kod** > **Genomsökning på begäran** > **ThreatSense** > **Rensning**. Om du vill göra en genomsökning utan rensning klickar du på **Avancerade inställningar** och väljer **Genomsök utan rensning**. Genomsökningshistoriken sparas i genomsökningsloggen.

När **Ignorera exkluderingar** väljs genomsöks filerna med ändelser som tidigare exkluderades från genomsökning utan undantag.

Klicka på **Genomsökning** för att köra genomsökningen med inställda anpassade parametrar.

Genomsök som administratör gör det möjligt att utföra genomsökningen med administratörskontot. Använd den här funktionen om den aktuella användaren inte har behörighet till filerna som ska genomsökas. Den här knappen inte är tillgänglig om den aktuella användaren inte kan anropa UAC-åtgärder som administratör.

> Du kan visa loggen för genomsökning av datorn när en genomsökning är klar genom att klicka på Visa logg.

Genomsökningsförlopp

Fönstret genomsökningsförlopp visar aktuell status för genomsökningen och information om antalet filer som innehåller skadlig kod.

Det är normalt att en del filer, som lösenordsskyddade filer eller filer som endast används av systemet (typiskt *pagefile.sys* och vissa loggfiler) inte går att genomsöka. Du hittar mer information i vår artikel i kunskapsbasen.

Schemalägga en veckovis genomsökning av datorn

Om du vill schemalägga en regelbunden aktivitet läser du kapitlet Schemalägga en veckovis genomsökning av datorn.

Genomsökningsförlopp – förloppsindikatorn visar status för den pågående genomsökningen.

Mål – namn på det objekt som skannas just nu och dess plats.

Inträffade detekteringar – visar totalt antal genomsökta filer, upptäckta hot och rensade hot under en genomsökning.

Klicka på Mer info för att visa följande information:

- **Användare** – namnet på användarkontot som startade genomsökningen.
- **Genomsökta objekt** – antal redan genomsökta objekt.
- **Varaktighet** – förfluten tid.

Paus-ikon – pausar en genomsökning.

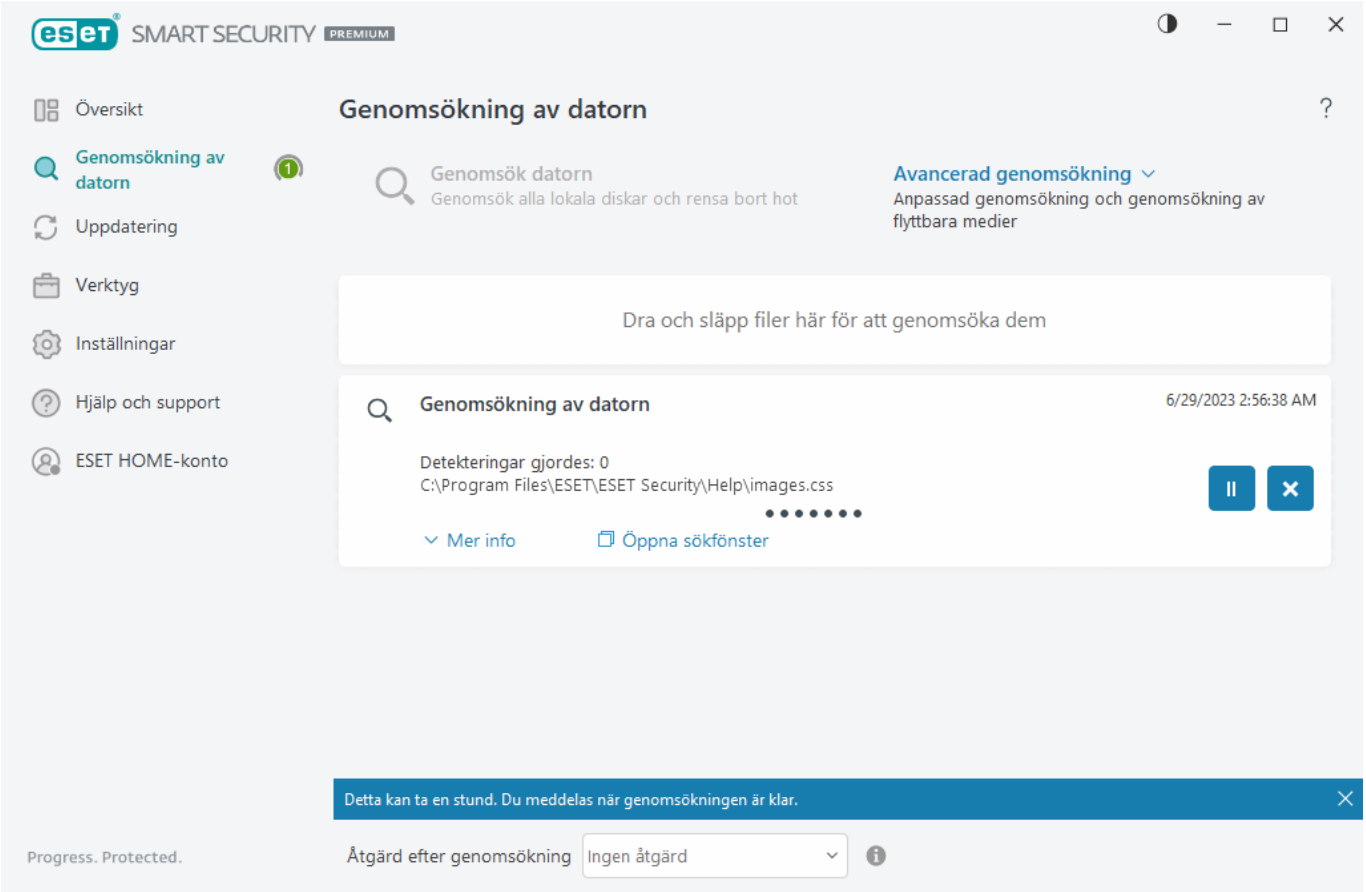
Fortsätt-ikon – det här alternativet visas när genomsökningen pausas. Klicka på ikonen för att fortsätta genomsökningen.

Stopp-ikon – avslutar genomsökningen.

Klicka på **Öppna genomsökningsfönstret** för att öppna Logg för genomsökning av datorn med mer information om genomsökningen.

Bläddra i genomsökningsloggen – om aktiverad bläddrar genomsökningsloggen ned automatiskt när nya poster läggs till så att de senaste är synliga.

Klicka på skärmförstoraren eller pilen för att visa information om genomsökningen som för närvarande äger rum. Det går att köra en parallell genomsökning genom att klicka på **Genomsök datorn** eller **Avancerade genomsökningar** > **Anpassad genomsökning**.



Med listrutan **Åtgärd efter genomsökning** kan du ange en åtgärd som ska utföras automatiskt när en genomsökning har slutförts:

- **Ingen åtgärd** – ingen åtgärd utförs efter att en genomsökning är klar.
- **Avstängning** – datorn stängs av när en genomsökning är klar.
- **Starta om vid behov** – datorn startas om det bara behövs för att slutföra rensningen av upptäckta hot.
- **Omstart** – alla öppna program stängs och datorn startas om när en genomsökning är klar.
- **Tvinga starta om vid behov** – datorn tvingas att starta om det bara behövs för att slutföra rensningen av upptäckta hot.
- **Tvinga omstart** – tvingar stängning av alla öppna program utan att vänta på användarinteraktion och startar om datorn när en genomsökning är klar.
- **Vänteläge** – sessionen sparas och datorn försätts i vänteläge så att arbetet snabbt kan återupptas.
- **Viloläge** – allt i RAM-minnet flyttas till en speciell fil på hårddisken. Datorn stängs av, men återgår till sitt föregående tillstånd nästa gång den startas.

Åtgärderna **Vänteläge** eller **Viloläge** är tillgängliga baserat på operativsystemets inställningar för ström och vänteläge på datorn eller datorns/den bärbara datorns funktioner. Tänk på att en dator i vänteläge fortfarande är i drift. Grundläggande funktioner körs fortfarande och kraft förbrukas när datorn körs på batteridrift. För att spara batterikraft, exempelvis på resor utanför kontoret, rekommenderas alternativet Viloläge.

Den valda åtgärden startas efter att alla genomsökningar som körs har slutförts. När du väljer **Avstängning** eller **Omstart** visas en bekräftelsedialogruta med en nedräkning på 30 sekunder (klicka på **Avbryt** om du vill inaktivera den begärda åtgärden).

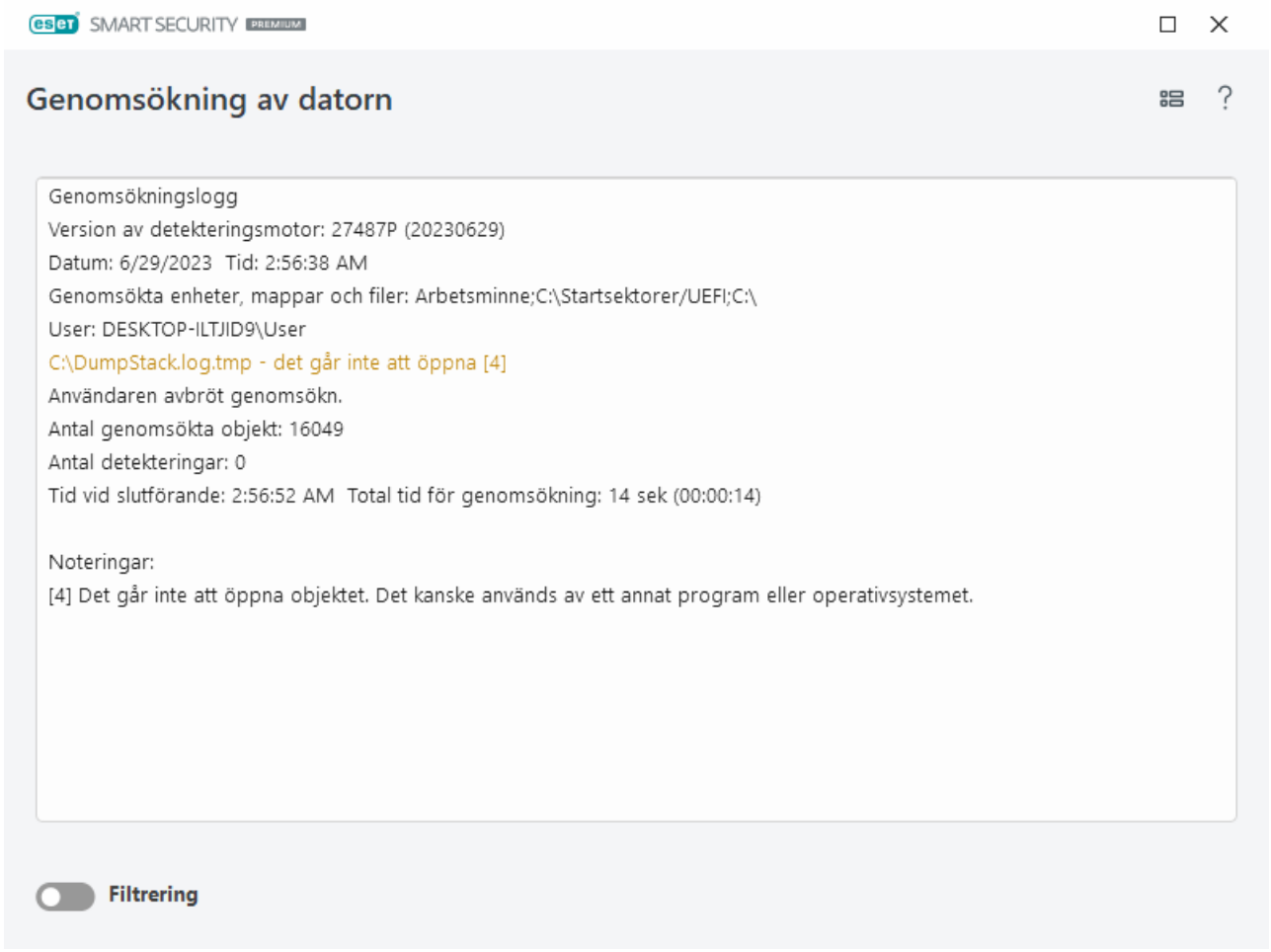
Genomsökningslogg av datorn

Du kan visa detaljerad information relaterad till en specifik genomsökning i Loggfiler. Genomsökningsloggen innehåller följande information:

- Version av detekteringsmotor
- Startdatum och -tid
- Lista över genomsökta enheter, mappar och filer
- Namn på schemalagd genomsökning (endastschemalagd genomsökning)
- Användare som startade genomsökningen.
- Genomsökningsstatus
- Antal genomsökta objekt
- Antal hittade detekteringar
- Tid vid slutförande
- Total tid för genomsökning

> En ny start av en schemalagd genomsökningsaktivitet för datorn hoppas över om samma schemalagda aktivitet som kördes tidigare fortfarande körs. Den överhoppade schemalagda genomsökningsaktiviteten skapar en genomsökningslogg för datorn med 0 genomsökta objekt och statusen **Genomsökningen startade inte eftersom den föregående genomsökningen fortfarande kördes**.

För att hitta tidigare genomsökningsloggar väljer du **Verktyg** > **Loggfiler** på programmets huvudfönster. I listrutan väljer du **Genomsökning av datorn** och dubbelklickar på önskad post.



Mer information om poster med "det går inte att öppna", ”fel vid öppning" och/eller "arkivet är skadat" finns i vår artikel i ESET:s kunskapsbas.

Klicka på växlingsknappen **Filtrering** för att öppna fönstret Loggfiltrering där du kan förfina sökningen med egna villkor. Om du vill öppna kontextmenyn högerklickar du på en viss loggpost:

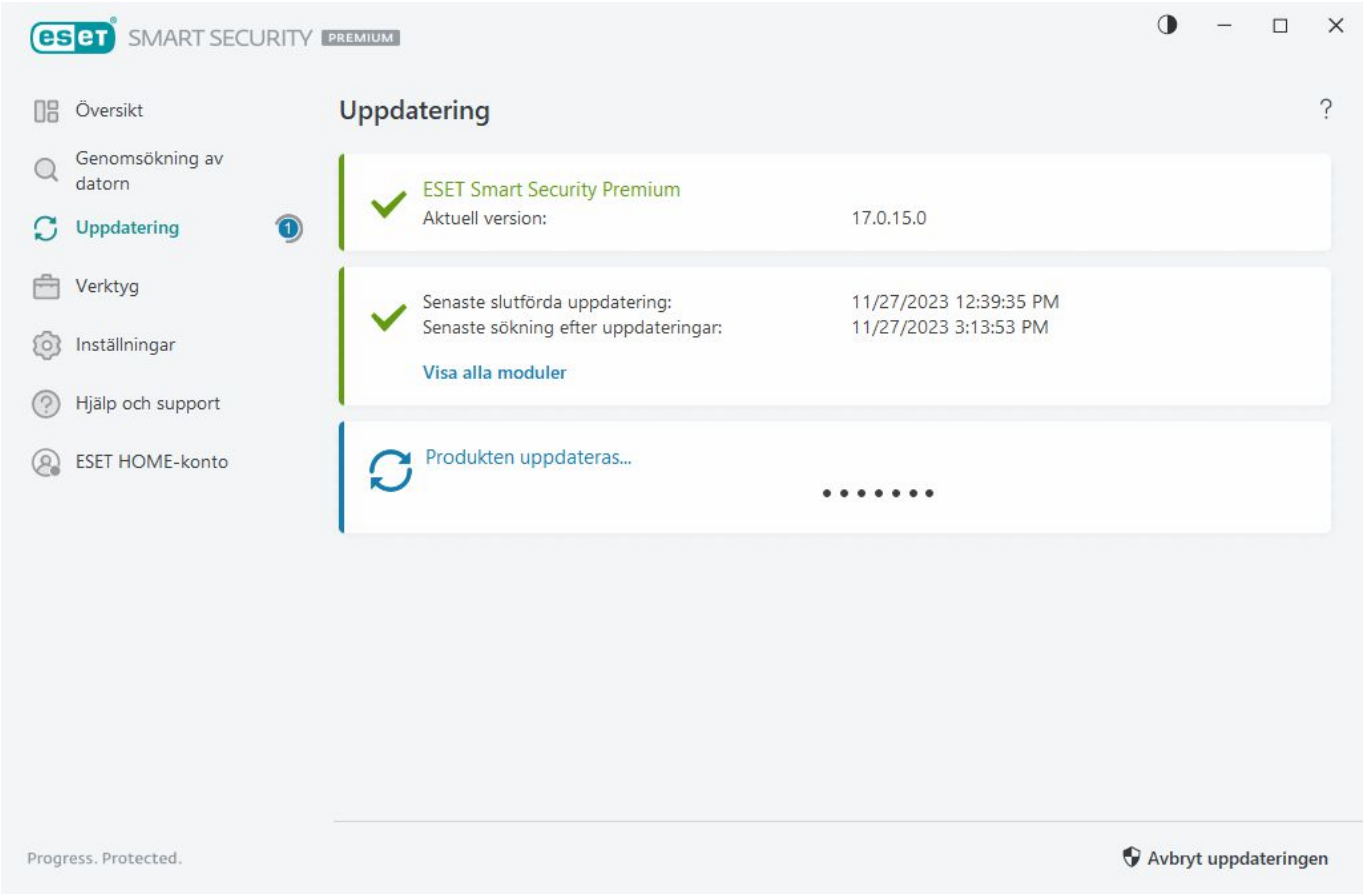
Åtgärd	Användning
Filtrera samma poster	Aktiverar loggfiltreringen. Loggen visar endast poster av samma typ som den valda.
Filtrera	Med det här alternativet öppnas fönstret Loggfiltrering, där du kan ange villkor för specifika loggposter. Genväg: `Ctrl+Shift+F`
Aktivera filter	Aktiverar filterinställningarna. Om du aktiverar filtret för första gången måste du ange inställningarna och fönstret Loggfiltrering öppnas.
Inaktivera filter	Stänger av filtret (samma som att klicka på reglaget nederst).
Kopiera	Kopierar den eller de valda posterna till Urklipp. Genväg: `Ctrl+C`
Kopiera alla	Kopierar alla poster i fönstret.
Exportera	Exporterar den eller de valda posterna till en XML-fil.
Exportera alla	Med det här alternativet exporteras alla poster i fönstret till en XML-fil.
Detekteringsbeskrivning	Öppnar ESET Threat Encyclopedia, som innehåller detaljerad information om farorna med och symptomen på den markerade infiltrationen.

Uppdatera

Regelbunden uppdatering av ESET Smart Security Premium är det bästa sättet att säkerställa maximal säkerhetsnivå på datorn. Uppdateringsmodulen säkerställer att både programmodulerna och systemkomponenterna alltid är uppdaterade.

Genom att klicka på **Uppdatering** i programmets huvudfönster går det att visa aktuell uppdateringsstatus, inklusive datum och tid för den senaste uppdateringen och om en uppdatering behövs.

Förutom automatiska uppdateringar kan du klicka på **Sök efter uppdateringar** för att utlösa en manuell uppdatering. Regelbunden uppdatering av programmoduler och komponenter är avgörande för att bibehålla ett heltäckande skydd mot skadlig kod. Var noggrann angående konfiguration och användning av produktmodulerna. Produkten måste aktiveras med aktiveringsnyckeln för att få uppdateringar. Om du inte gjorde det här under installationen måste du aktivera ESET Smart Security Premium för att få åtkomst till ESET:s uppdateringsservrar. Din aktiveringsnyckel skickades i ett e-postmeddelande från ESET efter ditt köp av ESET Smart Security Premium.



Aktuell version – visar numret på den version av produkten som för närvarande är installerad.

Senaste slutförd uppdatering – visar datumet för den senaste slutförda uppdateringen. Ser du inte närliggande datum är det möjligt att produktmodulerna inte är aktuella.

Senaste slutförd sökning efter uppdateringar – visar datumet för den senaste slutförda sökningen efter uppdateringar.

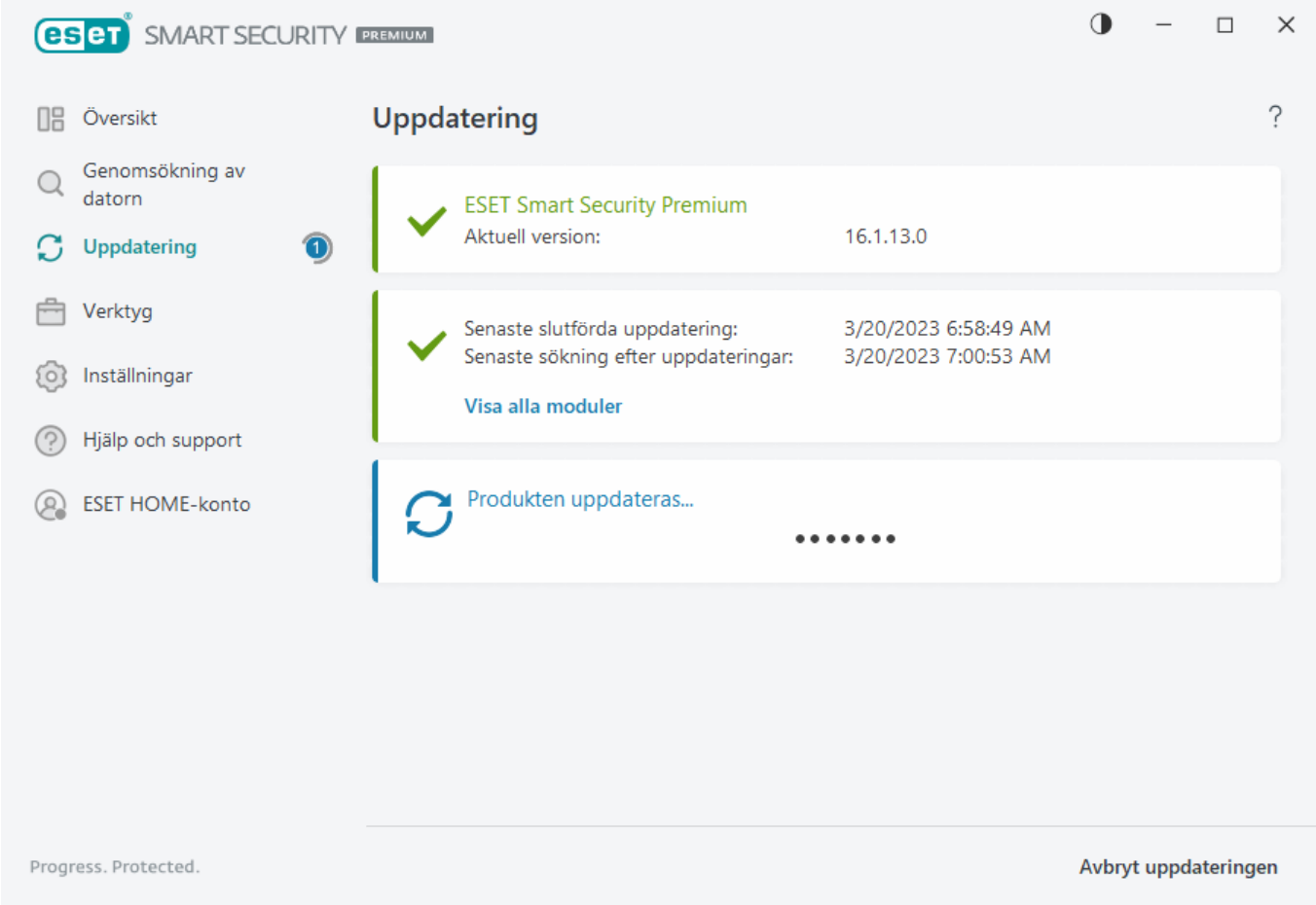
Visa alla moduler – visar listan med installerade programmoduler.

Klicka på **Sök efter uppdateringar** för att leta efter den senaste tillgängliga versionen av ESET Smart Security

Premium.

Uppdateringsprocessen

När du har klickat på **Leta efter uppdateringar** startas hämtningen. En förloppsindikator och den kvarvarande hämtningstiden visas. Klicka på **Avbryt** om du vill avbryta uppdateringen.



Normalt visar en grön bock i fönstret **Uppdatering** att programmet är aktuellt. Om det inte finns en grön bock är programmet inaktuellt och mer sårbart för infektion. Uppdatera programmodulerna så snart som möjligt.

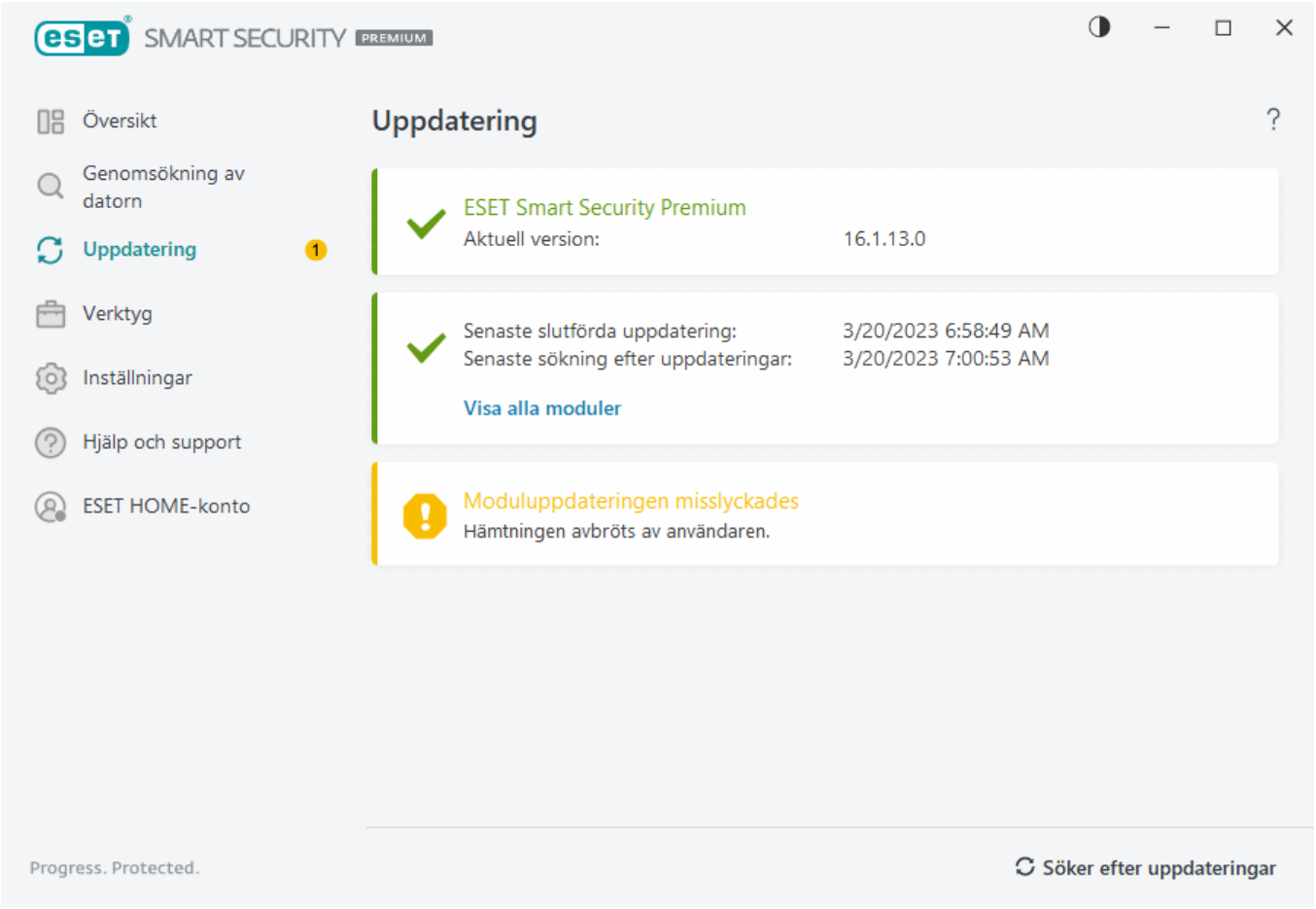
Misslyckad uppdatering

Om du får ett meddelande om en misslyckad moduluppdatering kan det bero på följande problem:

1. **Ogiltigt abonnemang** – Abonnemanget som används för aktivering är ogiltigt eller har upphört. Klicka på **Hjälp och support** > **Ändra abonnemang** i programmets huvudfönster och aktivera produkten.

2. **Ett fel uppstod när uppdateringsfiler skulle hämtas** – detta kan bero på felaktiga inställningar för Internetanslutningen. Vi rekommenderar att du kontrollerar Internetanslutningen genom att öppna en helt annan webbsida i webbläsaren. Om webbplatsen inte öppnar är det troligt att en Internetanslutning inte upprättats eller att din dator har anslutningsproblem. Kontrollera med din Internetleverantör om du har en

aktiv Internetanslutning.



Du måste starta om datorn efter uppdatering av ESET Smart Security Premium till en nyare produktversion för att säkerställa att alla programmoduler har uppdaterats korrekt. Det är inte nödvändigt att starta om datorn efter vanliga moduluppdateringar.

Mer information finns i Felsöka meddelandet Moduluppdateringen misslyckades.

Dialogfönster – omstart krävs

En omstart av datorn krävs efter uppdatering av ESET Smart Security Premium till en ny version. Nya versioner av ESET Smart Security Premium utfärdas för att implementera förbättringar eller åtgärda problem som automatiska uppdateringar av programmoduler inte kan lösa.

Den nya versionen av ESET Smart Security Premium kan installeras automatiskt, baserat på dina programuppdateringsinställningar, eller manuellt genom att ladda ned och installera en nyare version jämfört med den föregående.

Klicka på **Starta om nu** för att starta om datorn. Om du planerar att starta om datorn senare klickar du på **Påminn mig senare**. Senare kan du starta om datorn manuellt från avsnittet **Översikt** i huvudprogramfönstret.

Skapa uppdateringsaktiviteter

Uppdateringar utlöses manuellt genom att klicka på **Leta efter uppdateringar** i fönstret som öppnas när du klickat på **Uppdatera** på huvudmenyn.

Det går även att köra uppdateringar som schemalagda aktiviteter. Konfigurera en schemalagd aktivitet genom att klicka på **Verktyg** > **Schemaläggaren**. Som standard är följande uppdateringsaktiviteter aktiverade i ESET Smart Security Premium:

- **Vanlig automatisk uppdatering**
- **Automatisk uppdatering efter inloggning**

Varje uppdateringsaktivitet går att ändra för att uppfylla dina behov. Förutom standardaktiviteterna går det även att skapa nya uppdateringsaktiviteter med en användardefinierad konfiguration. Mer information om att skapa och konfigurera uppdateringsaktiviteter finns i avsnittet Schemaläggaren.

Verktyg

Verktygsmenyn innehåller funktioner som erbjuder ytterligare säkerhet och hjälper till att förenkla administrationen av ESET Smart Security Premium. Följande verktyg är tillgängliga:

 Loggfiler

 Processer som körs (om ESET LiveGrid® aktiverats i ESET Smart Security Premium)

 Säkerhetsrapport

 Nätverksanslutningar (om brandväggen aktiverats i ESET Smart Security Premium)

 ESET SysInspector

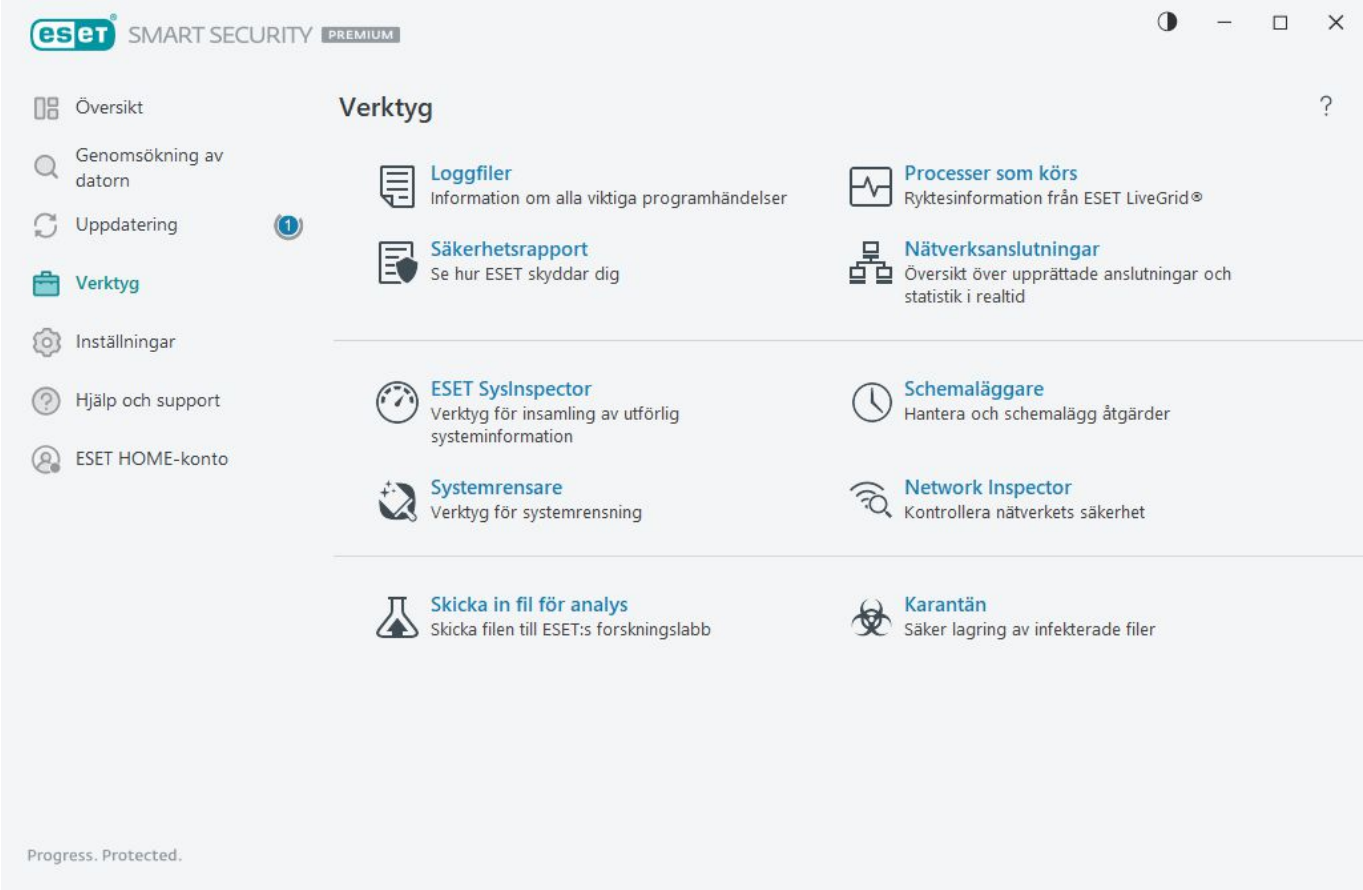
 Schemaläggare

 Systemrensare

 Network Inspector

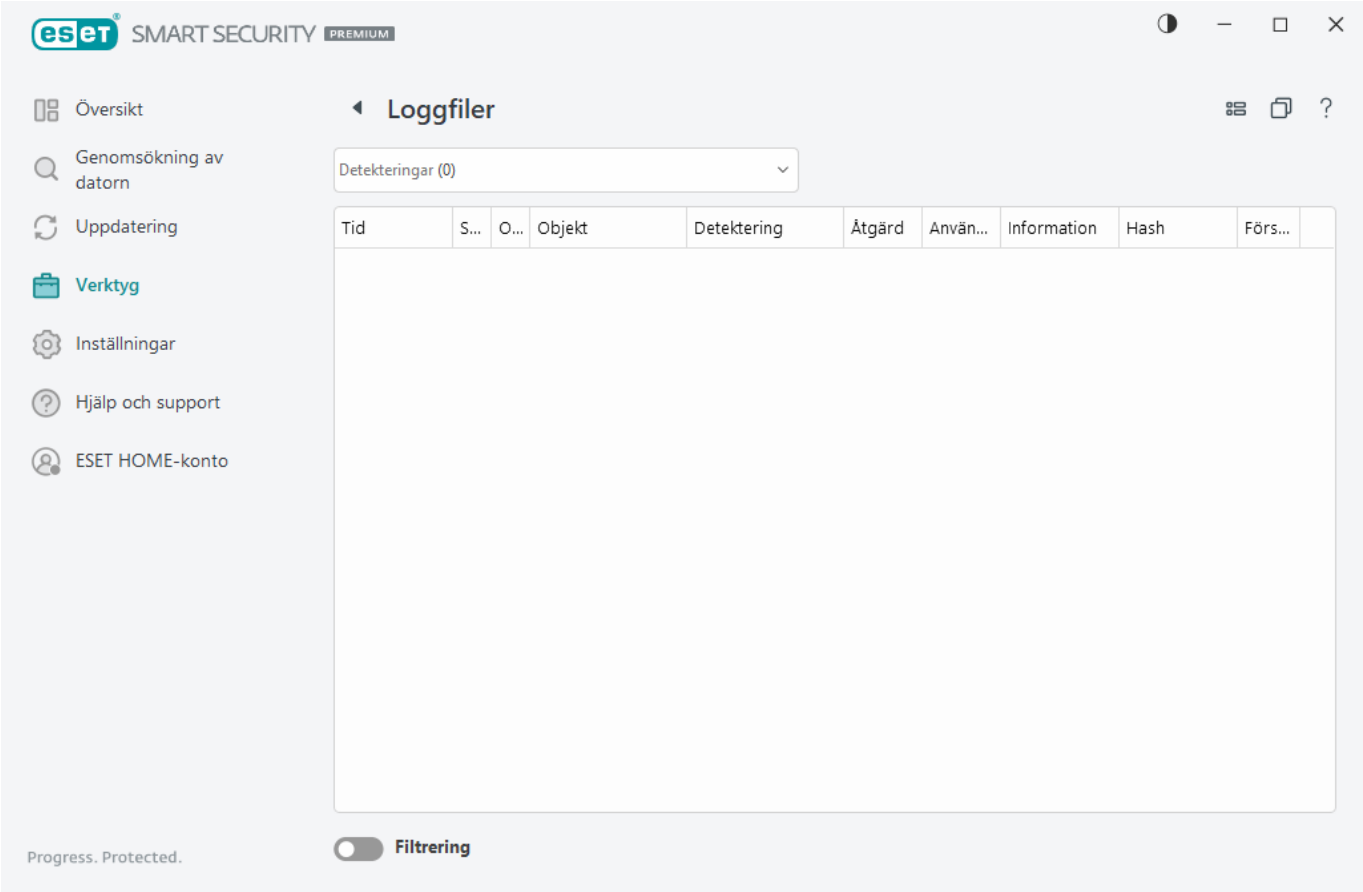
 Skicka prov för analys (kanske inte är tillgängligt baserat på din konfiguration av ESET LiveGrid®).

 Karantän



Loggfiler

Loggfiler innehåller information om viktiga programhändelser som har inträffat och ger en översikt över upptäckta hot. Loggning utgör ett viktigt verktyg vid systemanalys, hotdetektering och felsökning. Loggning sker aktivt i bakgrunden utan att användaren behöver göra något. Informationen som sparas baseras på loggens aktuella utförlighetsinställningar. Det är möjligt att visa textmeddelanden och loggar direkt från ESET Smart Security Premium-miljön, såväl som att arkivera loggar.



Loggfilerna finns tillgängliga från programmets huvudfönster genom att klicka på **Verktyg** > **Loggfiler**. Välj önskad loggtyp i rullgardinsmenyn Logg.

- **Detekteringar** – i den här loggen sparas detaljerad information om detekteringar och infiltreringar som har upptäckts av ESET Smart Security Premium. Logginformationen innehåller tiden för upptäckt, skannertyp, objekttyp, objektets plats, detekteringens namn, vidtagen åtgärd, namnet på den användare som var inloggad vid den tidpunkt då infiltreringen upptäcktes, hash och första förekomst. Dubbelklicka på loggposten för att visa detaljerna i ett separat fönster. Ej rensade infiltrationer markeras alltid med röd text på ljusröd bakgrund, rensade infiltrationer markeras med gul text på vit bakgrund. Ej rensade potentiella osäkra program markeras med gul text på vit bakgrund.

- **Händelser** – alla viktiga åtgärder som utförs av ESET Smart Security Premium sparas i händelseloggen. I händelseloggen finns information om händelser och fel som uppstått i programmet. Det är utformat för systemadministratörer och användare för att lösa problem. Informationen i loggfiler hjälper ofta till att hitta en lösning på ett problem i programmet.

- **Genomsökning av datorn** – resultatet av alla slutförda genomsökningar visas i detta fönster. Varje rad motsvarar en enskild genomsökning av datorn. Dubbelklicka på en post för att visa information om respektive genomsökning av datorn.

- **Skickade filer** – Innehåller poster för de prover som har skickats till ESET LiveGuard.

- **HIPS** – innehåller poster för specifika HIPS-regler som är markerade för registrering. Protokollet visar programmet som utlöste åtgärden, resultatet (om regeln tilläts eller var förbjuden) och regelns namn.

- **Webbläsarskydd** – innehåller poster över ej verifierade/ej betrodda filer som läses in i webbläsaren.

- **Nätverksskydd** – loggen för nätverksskydd visar alla fjärrattacker som upptäckts av brandväggen, skyddet

mot nätverksattacker (IDS) och botnetskyddet. Här finns information om alla attacker mot datorn. Kolumnen Händelse visar de identifierade attackerna. Kolumnen Källa berättar mer om angriparen. Kolumnen Protokoll avslöjar attackens kommunikationsprotokoll. Analys av loggen för nätverksskydd kan hjälpa till att identifiera systeminfiltrationsförsök i tid för att förhindra obehörig åtkomst till systemet. För mer information om nätverksattacker, se IDS och avancerade alternativ.

- **Filtrerade webbplatser** – den här listan är användbar om du vill visa en lista över webbplatser som har blockerats av Webbåtkomstskydd eller Föräldrakontroll. Varje logg innehåller tid, URL-adress, användare och program som upprättat en anslutning till en viss webbplats.

- **Skräppostskydd av e-postklient** – innehåller poster relaterade till e-postmeddelanden märkta som spam.

- **Föräldrakontroll** – visar webbsidor blockerade eller tillåtna av Föräldrakontroll. Kolumnerna Matchningstyp och Matchningsvärden visar hur filtreringsreglerna tillämpades.

- **Enhetskontroll** – innehåller poster med flyttbara medier eller enheter som anslutits till datorn. Endast enheter med respektive enhetskontrollregler registreras i loggfilen. Om regeln inte motsvarar en ansluten enhet skapas inte en loggpost för en ansluten enhet. Det går även att visa information såsom enhetstyp, serienummer, leverantörsnamn och mediastorlek (om tillgängligt).

- **Webbkameraskydd** – innehåller poster om program som blockerats av webbkameraskyddet.

Välj innehållet i en logg och tryck på **CTRL + C** om du vill kopiera det till Urklipp. Håll ned **CTRL** eller **SHIFT** om du vill välja flera poster.

Klicka på  **Filtrering** för att öppna fönstret Loggfiltrering där filtreringskriterier kan anges.

Högerklicka på en viss post om du vill öppna kontextmenyn. Följande alternativ är tillgängliga i kontextmenyn:

- **Visa** – visar mer utförlig information om den valda loggen i ett nytt fönster.

- **Filtrera samma poster** – aktivera detta filter för att endast visa poster av samma typ (diagnostik, varningar, ...).

- **Filtrera** – när du klickar på det här alternativet kan du ange filtreringsvillkor för specifika loggposter i fönstret Loggfiltrering.

- **Aktivera filter** – aktiverar filterinställningarna.

- **Inaktivera filter** – rensar alla inställningar i filtret (enligt beskrivning ovan).

- **Kopiera/kopiera alla** – kopierar information om de markerade posterna.

- **Kopiera cell** – kopierar innehållet i den högerklickade cellen.

- **Ta bort/Ta bort alla** – tar bort de valda posterna eller alla visade poster. Denna åtgärd kräver administratörsbehörighet.

- **Exportera/Exportera alla** – exporterar information om de valda posterna eller alla poster i XML-format.

- **Sök/Sök nästa/Sök föregående** – när du klickar på det här alternativet kan du ange filtreringsvillkor för att markera den specifika posten med hjälp av fönstret Loggfiltrering.

• **Beskrivning av detektering** – öppnar ESET Threat Encyclopedia, som innehåller detaljerad information om farorna med och symptomen på den registrerade infiltrationen.

• **Skapa exkludering** – skapa ett nytt exkluderingsundantag med hjälp av en guide (ej tillgänglig för detektering av skadlig kod).

• **Lägg till i listan över tillåtna webbläsarskydd**– öppnar fönstret Lista över tillåtna webbläsarskydd och lägger till objektet i listan.

Loggfiltrering

Klicka på **Filtrering** i **Verktyg** > **Loggfiler** för att ange filtreringskriterier.

Loggfiltreringsfunktionen hjälper dig att hitta den information du letar efter, särskilt när det finns många poster. Med den kan du begränsa antalet loggposter om du till exempel letar efter en viss typ av händelse, status eller tidsperiod. Du kan filtrera loggposter genom att ange vissa sökalternativ. Endast poster som är relevanta (enligt dessa sökalternativ) visas i fönstret Loggfiler.

Skriv det aktuella sökordet i fältet **Sök text**. Använd listrutan **Sök i kolumner** för att förfina sökningen. Välj en eller flera poster i listrutan **Posttyper**. Ange vilken **tidsperiod** du vill visa resultat inom. Du kan även använda fler sökalternativ, till exempel **Matcha endast hela ord** eller **Skiftlägeskänslig**.

Sök text

Skriv en sträng (ett ord eller en del av ett ord). Endast poster som innehåller strängen visas. Andra poster utesluts.

Sök i kolumner

Välj vilka kolumner du vill ska tas med i sökningen. Du kan kontrollera en eller flera kolumner när du söker.

Posttyper

Välj en eller flera posttyper i listrutan:

• **Diagnostik** – loggar information som behövs för att fininställa programmet och alla poster ovan.

• **Informativ** – loggar alla informationsmeddelanden, inklusive framgångsrika uppdateringar och alla poster ovan.

• **Varningar** – registrerar kritiska fel och varningsmeddelanden.

• **Fel** – fel som ”Fel när filen hämtades” och kritiska fel registreras.

• **Kritiska** – loggar endast kritiska fel (fel vid start av antivirusskyddet

Tidsperiod

definiera tidsperioden för vilken du vill visa resultat.

- **Inte angivet** (standard) – ingen tidsperiod används, utan hela loggen söks igenom.
- **Senaste dagen**
- **Senaste veckan**
- **Senaste månaden**
- **Tidsperiod** – du kan ange den exakta tidsperioden (Från: och Till:) för att endast visa posterna inom den angivna tidsperioden.

Matcha endast hela ord

Markera kryssrutan om du vill söka efter hela ord för mer exakta resultat.

Skiftlägeskänslig

Aktivera det här alternativet om det är viktigt att gemener eller versaler används vid filtreringen. När du har konfigurerat filtrerings-/sökalternativen klickar du på **OK** för att visa filtrerade loggposter eller **Sök** för att börja söka. Loggfilerna söks igenom uppifrån och ned, med början från den aktuella positionen (den markerade posten). Sökningen stoppas när den första matchande posten hittas. Tryck på **F3** för att söka efter nästa post eller högerklicka och välj **Sök** för att förfina sökalternativen.

Processer som körs

Processer som körs visar program eller processer som körs på datorn och håller ESET omedelbart och kontinuerligt informerad om nya infiltrationer. ESET Smart Security Premium ger detaljerad information om processer som körs för att skydda användare med ESET LiveGrid®-teknik.

Rykte – i de flesta fall tilldelar ESET Smart Security Premium med hjälp av ESET LiveGrid®-teknik risknivåer till objekt (filer, processer, registernycklar, osv.) med hjälp av ett antal heuristiska regler så att egenskaperna för varje objekt granskas och risken för skadlig aktivitet utvärderas. Baserat på heuristiken kan objekt tilldelas en risknivå från 1 – Okej (grönt) till 9 – Riskfyllt (rött).

Process – avbildningsnamn för programmet eller processen som för närvarande körs på datorn. Det går även att använda Windows Aktivitetshanterare för att visa alla processer som körs i datorn. Det går att öppna Aktivitetshanteraren genom att högerklicka på ett tomt utrymme på aktivitetsfältet och sedan klicka **Aktivitetshanteraren** eller genom att trycka på **Ctrl**+**Skift**+**Esc** på tangentbordet.

Kända program markerade som Okej (gröna) är definitivt rena (vitlistade) och undantas från genomsökning.

PID – processidentifieringsnumret kan användas som en parameter i olika funktionsanrop, till exempel för att justera processens prioritet.

Antal användare – antalet användare som använder ett visst program. Denna information samlas in med ESET LiveGrid®-teknik.

Identifieringstid – tiden sedan programmet identifierades av ESET LiveGrid®-tekniken.

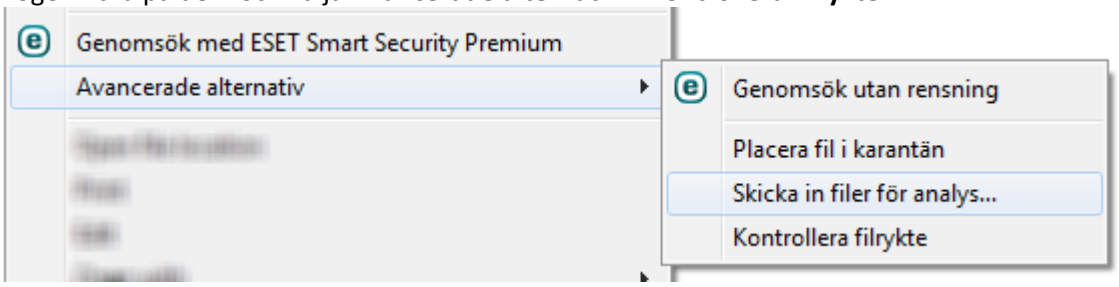
Ett program markerat som Okänd (orange) är inte nödvändigtvis skadlig programvara. Det är ofta ett nytt program. Om du inte är säker på filen kan du skicka in filen för analys till ESET:s forskningslabb. Om filen visar sig vara ett skadligt program läggs dess detektering till i en kommande uppdatering.

Programnamn – namnet på ett visst program eller viss process.

Klicka på ett program om du vill visa följande information om det:

- **Sökväg** – platsen för programmet på din dator.
- **Storlek** – filstorlek i antingen kB (kilobyte) eller MB (megabyte).
- **Beskrivning** – filens egenskaper som de beskrivs av operativsystemet.
- **Företag** – namnet på försäljaren eller programprocessen.
- **Version** – information från programmets utgivare.
- **Produkt** – programmets namn och/eller affärsnamn.
- **Skapad/ändrad** – datum och tidpunkt för skapande (ändring).

Det går även att kontrollera ryktet hos filer som inte är program/processer som körs. Gör det genom att högerklicka på dem och välja **Avancerade alternativ** > **Kontrollera filrykte**.



Säkerhetsrapport

Den här funktionen ger en översikt över statistiken för följande kategorier:

- **Webbsidor blockerade** – visar antalet blockerade webbsidor (svartlistade webbadresser för potentiellt oönskade program, hackad router, IP-adress eller certifikat).
- **Infekterade e-postobjekt blockerade** – visar antalet infekterade e-postobjekt som har detekterats.
- **Webbsidor i Föräldrakontroll blockerade** – visar antalet blockerade webbsidor i Föräldrakontroll.
- **Potentiellt oönskade program blockerade** – visar antalet potentiellt oönskade program (PUA).
- **Skräppost detekterad** – visar antalet detekterade skräppostmeddelanden.
- **Blockerad åtkomst till webbkameran** – visar antalet blockerade åtkomster till webbkameran.
- **Dokument genomsökta** – visar antalet genomsökta dokumentobjekt.
- **Genomsökta appar** – visar antalet genomsökta körbara filobjekt.
- **Övriga genomsökta objekt** – visar antalet övriga genomsökta objekt.
- **Genomsökta webbsideobjekt** – visar antalet genomsökta webbsideobjekt.
- **E-postobjekt genomsökta** – visar antalet genomsökta e-postobjekt.
- **Filer analyserade av ESET LiveGuard** – Visar antalet prover som analyserats av ESET LiveGuard.

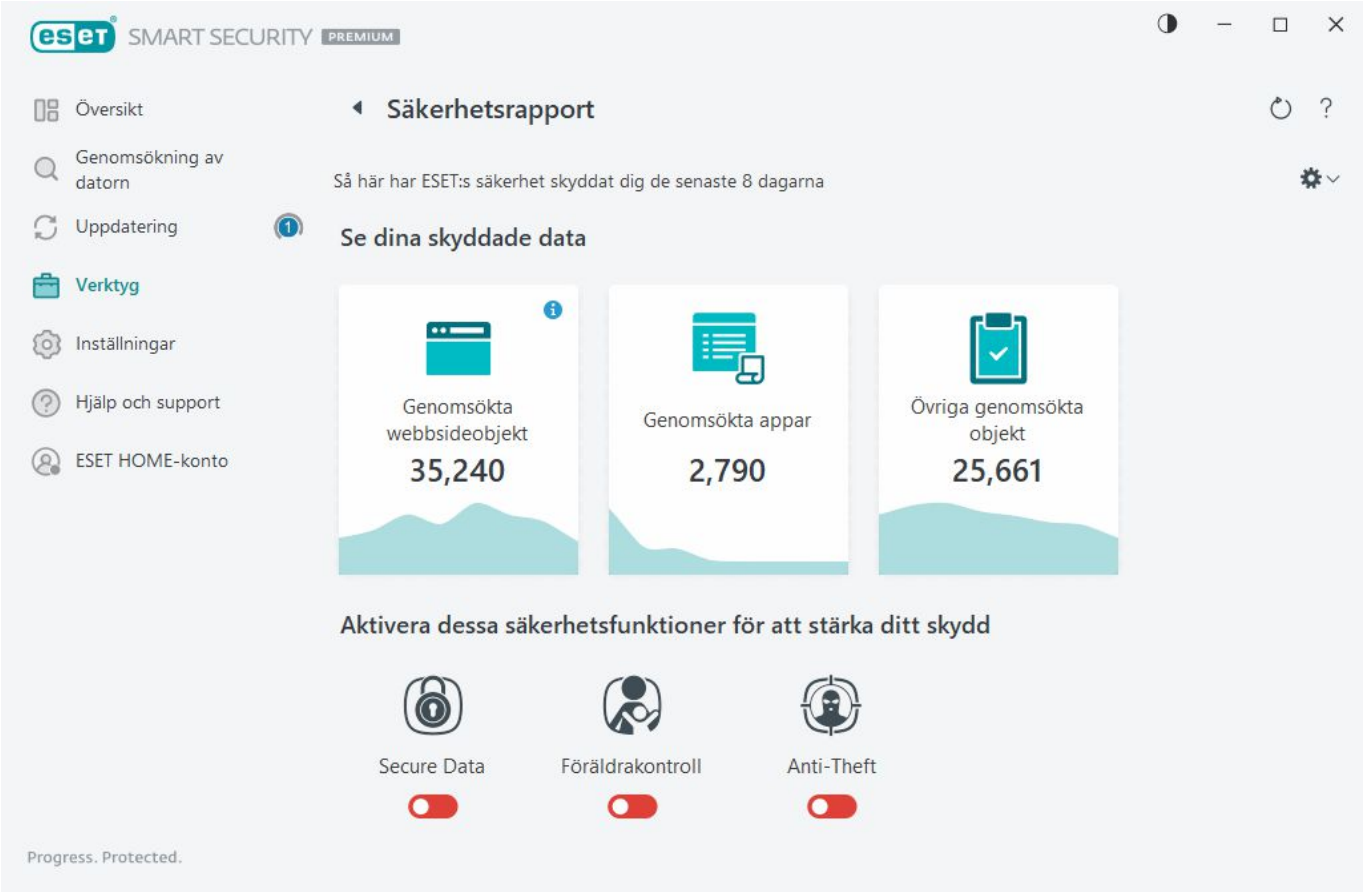
Ordningen för dessa kategorier baseras på det numeriska värdet från högsta till lägsta. Kategorier med nollvärden visas inte. Klicka på **Visa mer** om du vill utöka och visa dolda kategorier.

I den sista delen av säkerhetsrapporten går det att aktivera följande funktioner:

- ESET LiveGuard
- Secure Data
- Föräldrakontroll
- Stöldskydd

När funktionen har aktiverats visas den inte längre som inaktiv i säkerhetsrapporten.

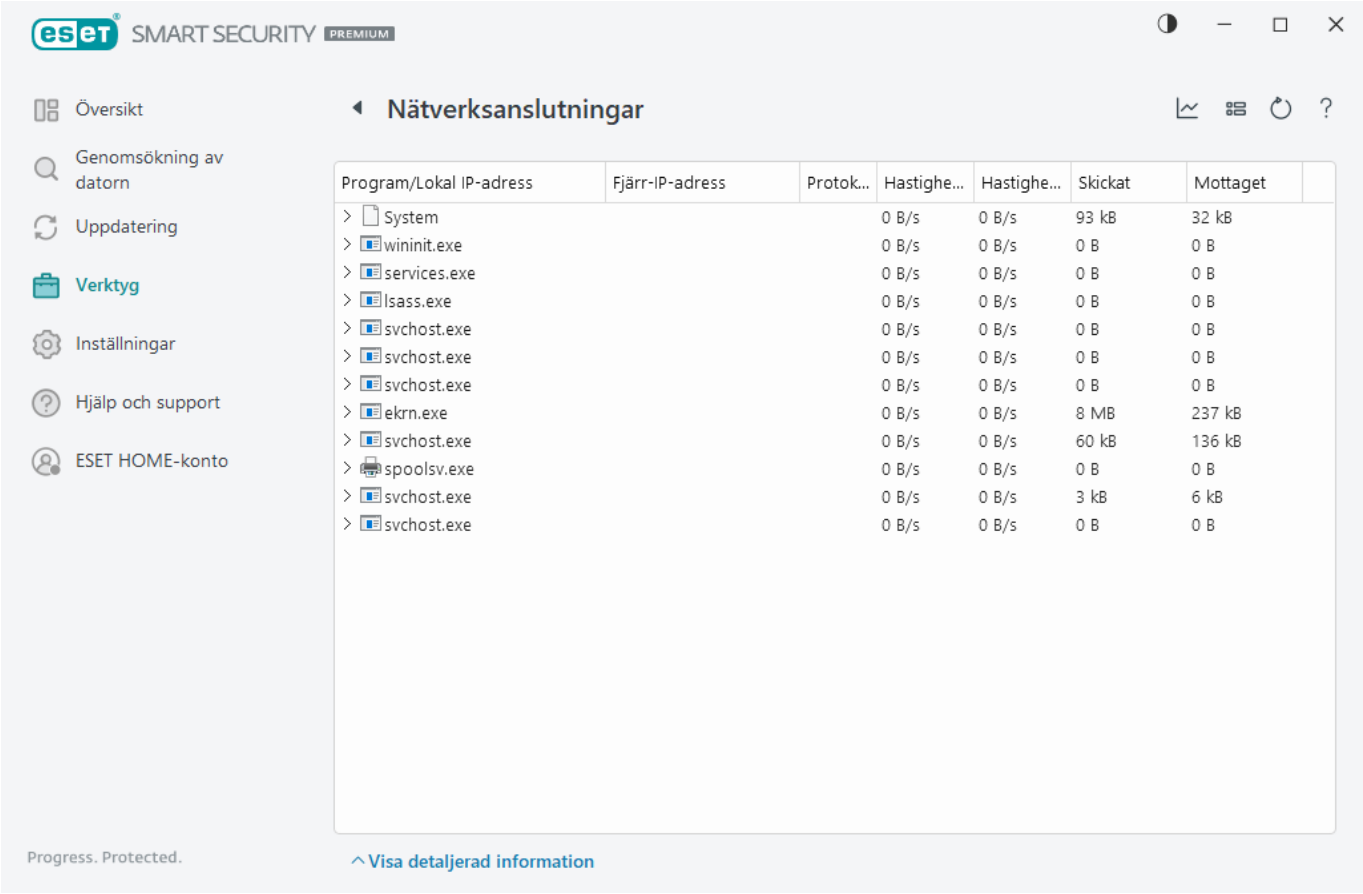
Genom att klicka på kugghjulet uppe till höger kan du **aktivera/inaktivera meddelanden med säkerhetsrapporter** eller välja om data ska visas för de senaste 30 dagarna eller sedan produkten aktiverades. Om ESET Smart Security Premium installerades för mindre än 30 dagar sedan kan endast antal dagar sedan installationen väljas. Standardinställningen är 30-dagarsperiod.



Med **Återställ data** rensas all statistik och befintliga data för säkerhetsrapporten tas bort. Den här åtgärden måste bekräftas om inte alternativet **Fråga innan statistik återställs** har avmarkerats i Avancerade inställningar > **Meddelanden** > **Interaktiva varningar** > **Bekräftelsemeddelanden** > **Redigera**.

Nätverksanslutningar

I Nätverksanslutningar visas en lista över aktiva och väntande anslutningar. Detta hjälper dig att kontrollera alla program som upprättar utgående anslutningar.



Klicka på diagramikonen för att öppna Nätverksaktivitet.

Den första raden visar namnet på programmet och dataöverföringshastigheten. Visa en lista över anslutningar gjorda av programmet (samt mer detaljerad information) genom att klicka på **+**.

Kolumner

Program/lokalt IP – namnet på programmet, lokala IP-adresser och kommunikationsportar.

Fjärr-IP – IP-adress och portnummer för en viss fjärrdator.

Protokoll – använt överföringsprotokoll.

Hastighet upp/Hastighet ned – aktuell hastighet på utgående och inkommande data.

Skickat/Mottaget – mängd data som överförts inom anslutningen.

Visa detaljerad information – välj det här alternativet om du vill visa detaljerad information om vald anslutning.

Högerklicka på en anslutning för att se ytterligare alternativ som innefattar:

Matcha värdnamn – om möjligt visas alla nätverksadresser i DNS-format, inte i IP-adressformat med siffror.

Visa endast TCP-anslutningar – listan visar endast anslutningar som tillhör protokollsviten TCP.

Visa anslutningar som lyssnar – markera det här alternativet för att enbart visa anslutningar där ingen kommunikation har upprättats men där systemet har öppnat en port och inväntar anslutning.

Visa anslutningar inom datorn – markera det här alternativet om du endast vill visa anslutningar där fjärrsidan är ett lokalt system, så kallade localhost-anslutningar.

Uppdateringshastighet – välj frekvensen för uppdatering av de aktiva anslutningarna.

Uppdatera nu – uppdaterar fönstret **Nätverksanslutningar**.

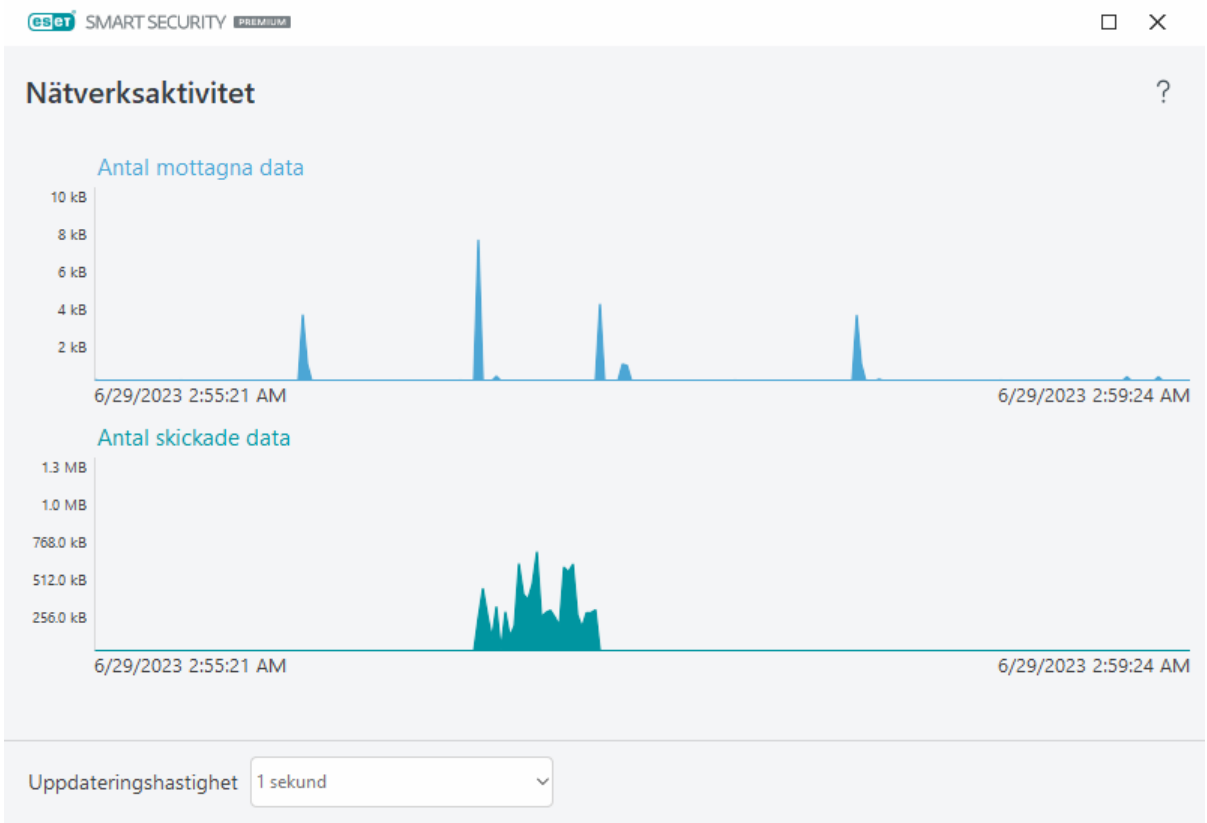
Följande alternativ är endast tillgängliga om du klickar på ett program eller en process, inte på en aktiv anslutning:

Neka temporärt kommunikation för processen – avvisar aktuella anslutningar för det angivna programmet. Om en ny anslutning upprättas använder brandväggen en fördefinierad regel. Du hittar en beskrivning av inställningarna i avsnittet Brandväggsregler.

Tillåt temporärt kommunikation för processen – tillåter aktuella anslutningar för det angivna programmet. Om en ny anslutning upprättas använder brandväggen en fördefinierad regel. Du hittar en beskrivning av inställningarna i avsnittet Brandväggsregler.

Nätverksaktivitet

Om du vill visa den aktuella **nätverksaktiviteten** i diagramform klickar du på **Verktyg** > **Nätverksanslutningar** och klickar på diagramikonen . Längst ned i diagrammet finns en tidslinje som registrerar nätverksaktivitet i realtid baserat på det valda tidsintervallet. Om du vill ändra tidsintervallet väljer du det tillämpliga värdet på listrutan **Uppdateringsfrekvens**.



Följande alternativ finns tillgängliga:

- **1 sekund** – grafen uppdateras varje sekund och tidslinjen täcker de senaste 4 minuterna.
- **1 minut (senaste 24 timmarna)** – grafen uppdateras varje minut och tidslinjen täcker de senaste 24 timmarna.
- **1 timme (senaste månaden)** - grafen uppdateras varje timme och tidslinjen täcker den senaste månaden.

Diagrammets lodräta axel representerar mängden mottagen eller skickad data. Håll musen över diagrammet för att se den exakta mängden mottagen/skickad data vid en viss tidpunkt.

ESET SysInspector

ESET SysInspector är ett program som grundligt undersöker din dator, samlar detaljerad information om systemkomponenter, som t.ex. drivrutiner och program, nätverksanslutningar eller viktiga registerposter och utvärderar risknivån för varje komponent. Informationen kan hjälpa till att fastställa orsaken till misstänkta systemfunktioner som kan ha uppstått på grund av inkompatibla program- eller maskinvaror eller infektion av skadlig programvara. Mer information om hur du använder ESET SysInspector finns i ESET SysInspector-onlinehjälpen.

I ESET SysInspector-fönstret visar följande information om loggar:

- **Tid** – tiden då loggen skapades.
- **Kommentar** – en kort kommentar.
- **Användare** – namnet på användaren som skapade loggen.
- **Status** – status för loggskapande.

Följande åtgärder finns tillgängliga:

- **Visa** – öppnar den valda inloggningen i ESET SysInspector. Du kan även högerklicka på en viss loggfil och välja **Visa** på kontextmenyn.
- **Skapa** – skapar en ny logg. Vänta tills ESET SysInspector har genererats (statusen **Skapad**) innan du försöker komma åt loggen. Loggen sparas i C:\ProgramData\ESET\ESET Security\SysInspector.
- **Ta bort** – tar bort vald eller valda loggar från listan.

Följande objekt är tillgängliga på kontextmenyn när en eller flera loggfiler väljs:

- **Visa** – öppnar markerad logg i ESET SysInspector (samma funktion som att dubbelklicka på en logg).
- **Skapa** – skapar en ny logg. Vänta tills ESET SysInspector har genererats (statusen **Skapad**) innan du försöker komma åt loggen.
- **Ta bort** – tar bort vald eller valda loggar från listan.
- **Ta bort alla** – tar bort alla loggar.

- **Exportera...** – exporterar loggen till en .xml-fil eller zippad .xml.

Schemaläggare

Schemaläggaren hanterar och startar schemalagda aktiviteter med fördefinierade inställningar och egenskaper.

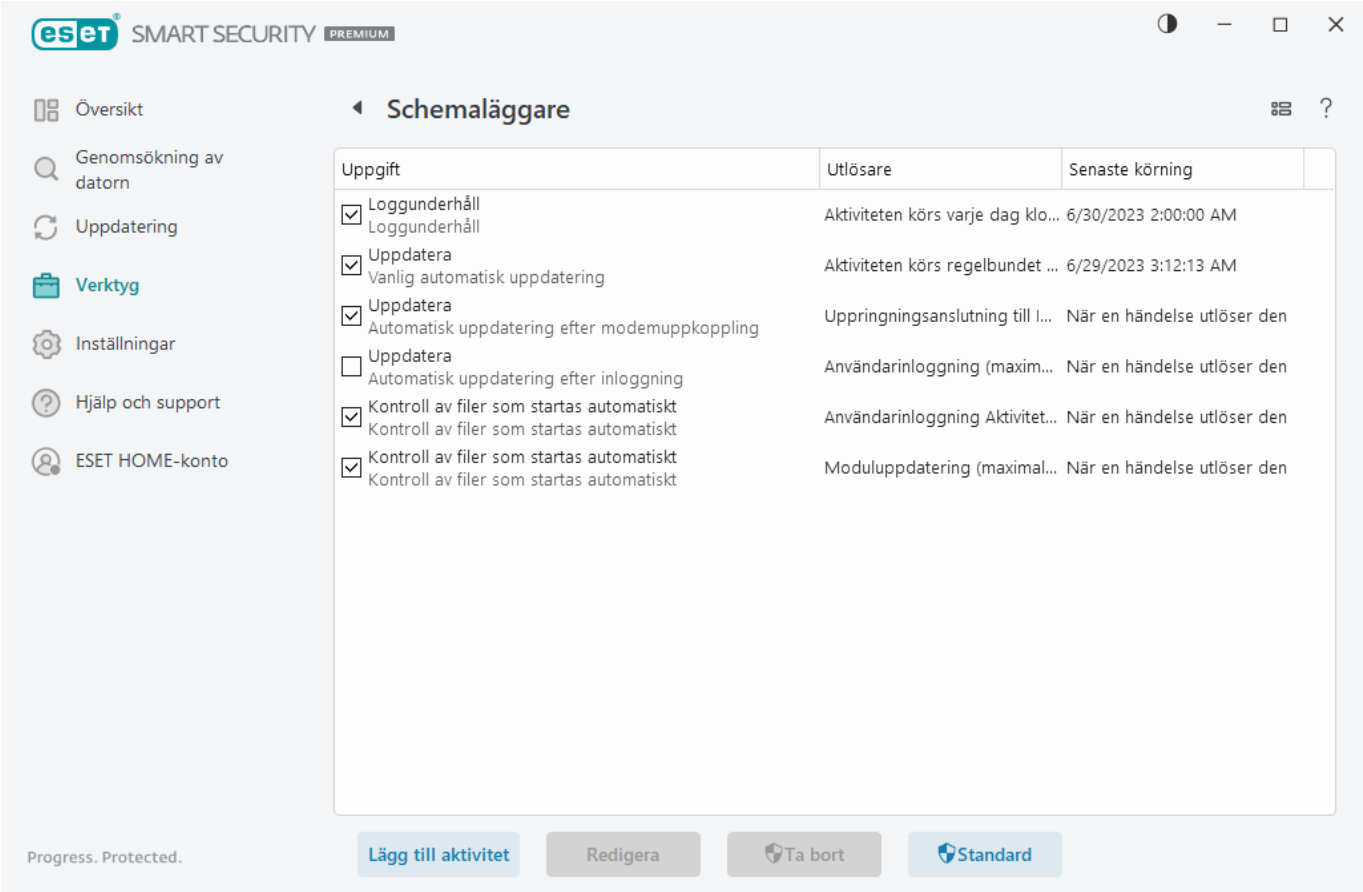
Schemaläggaren är tillgänglig från ESET Smart Security Premium-programmets huvudfönster genom att klicka på **Verktyg** > **Schemaläggaren**. **Schemaläggaren** innehåller en lista med alla schemalagda aktiviteter och konfigurationsegenskaper som t.ex. förinställt datum, tid och använd genomsökningsprofil.

Schemaläggaren används för att schemalägga följande aktiviteter: uppdatera moduler, genomsökning, kontroll av systemstartfiler och underhåll av loggfiler. Det går att lägga till eller ta bort aktiviteter direkt i Schemaläggarens huvudfönster (klicka på **Lägg till aktivitet** eller **Ta bort** längst ned). Det går att återställa listan med schemalagda uppgifter till standardvärdena och ta bort alla ändringar genom att klicka på **Standard**. Du kan utföra följande åtgärder genom att högerklicka var som helst i Schemaläggarens fönster: visa detaljerad information, utföra aktiviteten omedelbart, lägga till en ny aktivitet eller ta bort en befintlig aktivitet. Aktivera/inaktivera aktiviteterna med hjälp av kryssrutorna i början av varje post.

Som standard visas följande schemalagda aktiviteter i **Schemaläggaren**:

- **Loggunderhåll**
- **Vanlig automatisk uppdatering**
- **Automatisk uppdatering efter inloggning**
- **Kontroll av filer som startas automatiskt** (när användaren loggat in)
- **Kontroll av filer som startas automatiskt** (efter uppdatering av detekteringsmotorn)

Redigera konfigurationen för en befintlig schemalagd aktivitet (både standard och användardefinierad) genom att högerklicka på aktiviteten och klicka på **Redigera** eller markera den aktivitet du vill ändra och klicka på **Redigera**.



Lägg till ny aktivitet

1. Klicka på **Lägg till aktivitet** längst ned i fönstret.

2. Namnge aktiviteten.

3. Välj önskad aktivitet på rullgardinsmenyn:

   • **Kör externt program** – schemalägger körning av ett extern program.

   • **Underhåll av loggning** - loggfiler innehåller även rester från borttagna poster. Denna aktivitet optimerar regelbundet posterna i loggfiler för effektiv funktion.

   • **Kontroll av filer som startas automatiskt** – kontrollerar filer som tillåts köra vid systemstart eller inloggning.

   • **Skapa en avbildning av datorns status** – skapar en avbildning av datorn i ESET SysInspector – samlar detaljerad information om systemkomponenter (t.ex. drivrutiner och program) och utvärderar risknivån för varje komponent.

   • **Genomsökning av datorn på begäran** – utför genomsökning av filer och mappar på datorn.

   • **Uppdatering** – schemalägger en uppdateringsaktivitet genom att uppdatera modulerna.

4. Aktivera växlingsknappen bredvid **Aktiverad** om du vill aktivera åtgärden (du kan göra det här senare genom att markera/avmarkera kryssrutan i listan över schemalagda aktiviteter), klicka på **Nästa** och välj något av tidsalternativen:

- **En gång** – aktiviteten utförs vid det datum och den tidpunkt som angetts.
- **Flera gånger** – aktiviteten utförs regelbundet med angivet tidsintervall.
- **Dagligen** – aktiviteten körs varje dag vid den angivna tidpunkten.
- **Varje vecka** – aktiviteten körs angiven dag och tidpunkt.
- **När en händelse utlöser den** – aktiviteten utförs efter en angiven händelse.

5. Välj **Hoppa över aktivitet när datorn körs på batteri** för att minimera systemresurserna när datorns körs på batteri. Aktiviteten körs vid det datum och den tidpunkt som angetts i fältet **Utförande av aktivitet**. Om aktiviteten inte kunde köras vid den förutbestämda tidpunkten, ange när den ska utföras igen:

- **Vid nästa schemalagda tid**
- **Så snart som möjligt**
- **Omedelbart, om tiden sedan den senaste körningen överstiger (timmar)** – representerar den tid som gått sedan den första överhoppade körningen av aktiviteten. Om den här tiden överskrids körs aktiviteten omedelbart. Ställ in tiden med hjälp av snurran nedan.

Om du vill granska schemalagda aktiviteter högerklickar du på uppgiften och klickar på **Visa aktivitetsinformation**.

Alternativ för schemalagd genomsökning

I det här fönstret kan du ange avancerade alternativ för schemalagd genomsökning av datorn.

Om du vill göra en genomsökning utan rensning klickar du på **Avancerade inställningar** och väljer **Genomsök utan rensning**. Genomsökningshistoriken sparas i genomsökningsloggen.

När **Ignorera undantag** väljs genomsöks filerna med ändelser som tidigare undantogs från genomsökning utan undantag.

Med listrutan **Åtgärd efter genomsökning** kan du ange en åtgärd som ska utföras automatiskt när en genomsökning har slutförts:

- **Ingen åtgärd** – ingen åtgärd utförs efter att en genomsökning är klar.
- **Avstängning** – datorn stängs av när en genomsökning är klar.
- **Starta om vid behov** – datorn startas om det bara behövs för att slutföra rensningen av upptäckta hot.
- **Omstart** – alla öppna program stängs och datorn startas om när en genomsökning är klar.
- **Tvinga starta om vid behov** – datorn tvingas att starta om det bara behövs för att slutföra rensningen av upptäckta hot.
- **Tvinga omstart** – tvingar stängning av alla öppna program utan att vänta på användarinteraktion och startar om datorn när en genomsökning är klar.
- **Vänteläge** – sessionen sparas och datorn försätts i vänteläge så att arbetet snabbt kan återupptas.

• **Viloläge** – allt i RAM-minnet flyttas till en speciell fil på hårddisken. Datorn stängs av, men återgår till sitt föregående tillstånd nästa gång den startas.

Åtgärderna **Vänteläge** eller **Viloläge** är tillgängliga baserat på operativsystemets inställningar för ström och vänteläge på datorn eller datorns/den bärbara datorns funktioner. Tänk på att en dator i vänteläge fortfarande är i drift. Grundläggande funktioner körs fortfarande och kraft förbrukas när datorn körs på batteridrift. För att spara batterikraft, exempelvis på resor utanför kontoret, rekommenderas alternativet Viloläge.

Den valda åtgärden startas efter att alla genomsökningar som körs har slutförts. När du väljer **Avstängning** eller **Omstart** visas en bekräftelsedialogruta med en nedräkning på 30 sekunder (klicka på **Avbryt** om du vill inaktivera den begärda åtgärden).

Välj **Genomsökningen kan inte avbrytas** om du vill neka obehöriga användare möjligheten att stoppa åtgärder vidtagna efter en genomsökning.

Välj alternativet **Användaren kan pausa genomsökningen i (min)** om du vill ge begränsade användare möjlighet att pausa genomsökningen av datorn för en viss tidsperiod.

Se även Genomsökningsförlopp.

Översikt över schemalagda aktiviteter

I den här dialogrutan visas utförlig information om den valda schemalagda aktiviteten när du dubbelklickar på en anpassad aktivitet eller högerklickar på en anpassad schemaläggaraktivitet och klickar på **Visa aktivitetsinformation**.

Aktivitetsuppgifter

Skriv in **aktivitetsnamnet**, välj ett av alternativen för **aktivitetstyp** och klicka sedan på **Nästa**:

• **Kör externt program** – schemalägger körning av ett extern program.

• **Underhåll av loggning** - loggfiler innehåller även rester från borttagna poster. Denna aktivitet optimerar regelbundet posterna i loggfiler för effektiv funktion.

• **Kontroll av filer som startas automatiskt** – kontrollerar filer som tillåts köra vid systemstart eller inloggning.

• **Skapa en avbildning av datorns status** – skapar en avbildning av datorn i ESET SysInspector – samlar detaljerad information om systemkomponenter (t.ex. drivrutiner och program) och utvärderar risknivån för varje komponent.

• **Genomsökning av datorn på begäran** – utför genomsökning av filer och mappar på datorn.

• **Uppdatering** – schemalägger en uppdateringsaktivitet genom att uppdatera modulerna.

Aktivitetstid

Aktiviteten utförs regelbundet med angivet tidsintervall. Välj något av följande tidsalternativ:

- **En gång** – aktiviteten utförs endast en gång vid det datum och den tidpunkt som anges.
- **Flera gånger** – aktiviteten utförs regelbundet med angivet intervall (i timmar).
- **Dagligen** – aktiviteten körs varje dag vid den angivna tidpunkten.
- **Varje vecka** – aktiviteten körs en eller flera gånger i veckan, vid angivna dagar och tidpunkter.
- **När en händelse utlöser den** – aktiviteten utförs efter en angiven händelse.

Hoppa över aktivitet när datorn körs på batteri – en aktivitet startas inte om datorn körs på batteri vid tillfället då aktiviteten skulle startas. Detta gäller även datorer som körs på UPS.

Tidpunkt för aktivitet – en gång

Utförande av aktivitet – den angivna aktiviteten kommer endast att utföras en gång vid angivet datum och tid.

Tidpunkt för aktivitet – dagligen

Aktiviteten körs varje dag vid den angivna tidpunkten.

Tidpunkt för aktivitet – veckovis

Aktiviteten körs varje vecka på valda dag(ar) och tid.

Tidpunkt för aktivitet – händelseutlöst

Aktiviteten utlöses av någon av följande händelser:

- **Varje gång datorn startas**
- **Första gången datorn startas varje dag**
- **Fjärranslutning till Internet/VPN**
- **Modulen har uppdaterats**
- **Produkten har uppdaterats**
- **Användarinloggning**
- **Upptäcka hot**

När du schemalägger en aktivitet som utlöses av en händelse kan du ange ett minsta intervall mellan två körningar av aktiviteten. Om du till exempel loggar in på datorn flera gånger om dagen kan du välja 24 timmar, så att aktiviteten utförs vid den första inloggningen för dagen och sedan igen nästa dag.

Överhoppad aktivitet

En aktivitet kan hoppas över om datorn körs på batteri eller är avstängd. Välj när den överhoppade aktiviteten ska köras bland dessa alternativ och klicka på **Nästa**:

- **Vid nästa schemalagda tid** – aktiviteten körs om datorn är påslagen vid nästa schemalagda tidpunkt.
- **Så snart som möjligt** – aktiviteten körs när datorn är påslagen.
- **Omedelbart, om tiden sedan den senaste schemalagda körningen överstiger (timmar)** – representerar den tid som gått sedan den första överhoppade körningen av aktiviteten. Om den här tiden överskrids körs aktiviteten omedelbart.

Omedelbart, om tiden sedan den senaste schemalagda körningen överstiger (timmar) – exempel

En exempeluppgift är inställd på att köras upprepade gånger varje timme. Alternativet **Omedelbart, om tiden sedan den senaste schemalagda körningen överstiger (timmar)** har valts och den överskridna tiden är inställd på två timmar. Uppgiften körs klockan 13:00 och när den är klar datorn försätts datorn i vänteläge:

- Datorn vaknar klockan 15:30. Den första överhoppade körningen av uppgiften var klockan 14:00. Endast 1,5 timmar har gått sedan 14:00, så uppgiften körs klockan 16:00.
- Datorn vaknar klockan 16:30. Den första överhoppade körningen av uppgiften var klockan 14:00. Två och en halv timme har gått sedan 14:00, så uppgiften körs omedelbart.

Aktivitetsuppgifter – uppdatera

Om du vill uppdatera programmet från två uppdateringsservrar måste du skapa två olika uppdateringsprofiler. Om det inte går att hämta uppdateringsfilerna från den första kommer programmet automatiskt att växla till den alternativa servern. Detta kan till exempel vara lämpligt för bärbara datorer som normalt uppdateras från en lokal uppdateringsserver i ett LAN-nätverk, men datorns ägare ansluter ofta till Internet med andra nätverk. Går det inte att hämta den första profilen, hämtar den andra automatiskt uppdateringsfiler från ESET:s uppdateringsservrar.

Aktivitetsuppgifter – kör program

Den här aktiviteten schemalägger körning av ett extern program.

Körbar fil – välj en körbar fil i katalogträdet, klicka på alternativet **...** eller ange sökvägen för hand.

Arbetsmapp – definiera det externa programmet arbetskatalog. Alla temporära filer för vald **Körbar fil** skapas i denna katalog.

Parametrar – programmets kommandoradsparametrar (valfritt).

Klicka på **Slutför** om du vill använda aktiviteten.

Systemrensare

Systemrensaren är ett verktyg som hjälper dig att återställa datorn till ett användbart tillstånd efter att hotet rensats bort. Skadlig kod kan inaktivera systemverktyg som till exempel Registerredigeraren, Aktivitetshanteraren eller Windows-uppdateringar. Systemrensaren återställer systemets standardvärden och inställningar med ett enda klick.

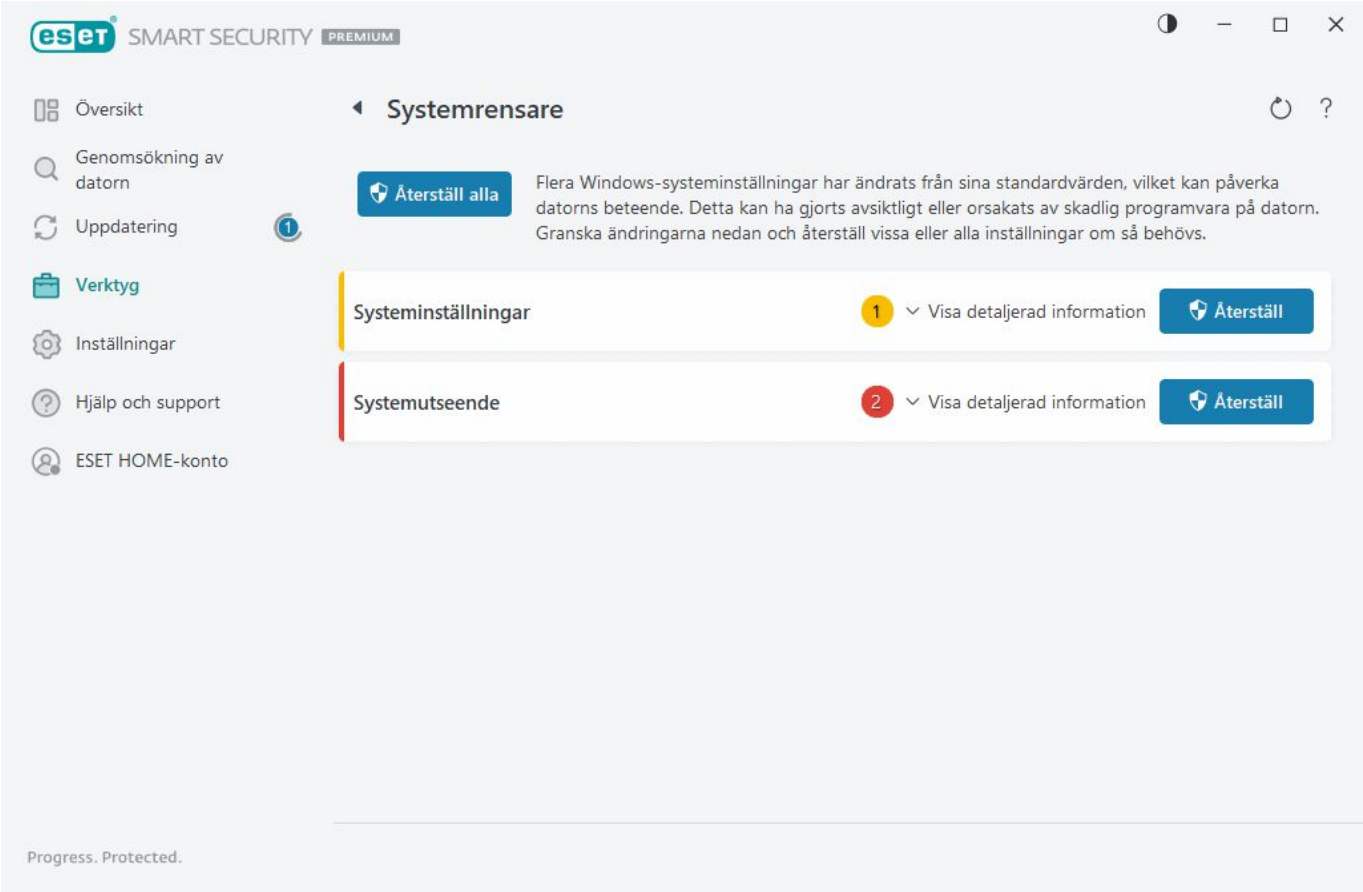
Systemrensaren rapporterar problem utifrån fem inställningskategorier:

- **Säkerhetsinställningar**: ändringar av inställningar som kan göra datorn mer sårbar, till exempel Windows Update
- **Systeminställningar**: ändringar av systeminställningar som kan ändra datorns beteende, till exempel filassociationer
- **Systemutseende**: inställningar som påverkar hur systemet ser ut, till exempel skrivbordets bakgrund
- **Inaktiverade funktioner**: viktiga funktioner och program som kan vara inaktiverade
- **Windows Systemåterställning**: inställningar för Windows Systemåterställning, som används för att återställa datorn till ett tidigare tillstånd

Systemrensning kan begäras:

- när ett hot hittas
- när en användare klickar på **Återställ**

Du kan granska ändringarna och återställningsinställningarna om du vill.



Endast användare med administratörsbehörighet kan utföra åtgärder i systemrensaren.

Network Inspector

Network Inspector kan hjälpa till att identifiera sårbarheter i ditt betrodda nätverk (hem- eller kontorsnätverk) (till exempel öppna portar eller ett svagt routerlösenord). Det innehåller även en lista över anslutna enheter, kategoriserade efter enhetstyp (till exempel skrivare, router, mobil enhet osv.) för att visa vad som är anslutet till ditt nätverk (till exempel spelkonsol, IoT eller andra smarta hemenheter).

Network Inspector hjälper dig att identifiera en routers sårbarheter och stärker skyddet när du ansluter till ett nätverk.

Network Inspector konfigurerar inte om routern åt dig. Utan du behöver göra ändringarna själv i det särskilda routergränssnittet. Routrar för hemmabruk är mycket sårbara för skadlig kod som används för att inleda DDoS-attacker. Om routerlösenordet inte har ändrats från standardvärdet av användaren är det lätt för hackare att lista ut det och sedan logga in på routern för att konfigurera om den eller göra intrång i nätverket.

Vi rekommenderar att du skapar ett starkt lösenord som är tillräckligt långt och innehåller siffror, symboler eller versaler. Om du använder en blandning av olika typer av tecken blir lösenordet svårare att lista ut.

Om nätverket du är ansluten till är konfigurerat som betrott kan du markera nätverket som ”Mitt nätverk”. Klicka på **Markera som ”Mitt nätverk”** för att lägga till taggen Mitt nätverk för nätverket. Taggen visas bredvid nätverket i hela ESET Smart Security Premium för bättre identifiering och säkerhetsöversikt. Klicka på **Avmarkera som ”Mitt nätverk”** om du vill ta bort taggen.

Varje enhet som är ansluten till nätverket visas med grundläggande information i en listvy. Klicka på den specifika

enheten om du vill redigera enheten eller visa detaljerad information om enheten.

I listvyn **Nätverk** kan du filtrera enheter baserat på följande villkor:

- Enheter som är anslutna till ett visst nätverk
- Enheter anslutna till **alla nätverk**
- Okategoriserade enheter

Klicka på enhetsikonen om du vill redigera enheten eller visa utförlig information om enheten. Nyligen anslutna enheter visas närmare routern så att du lätt kan se dem.

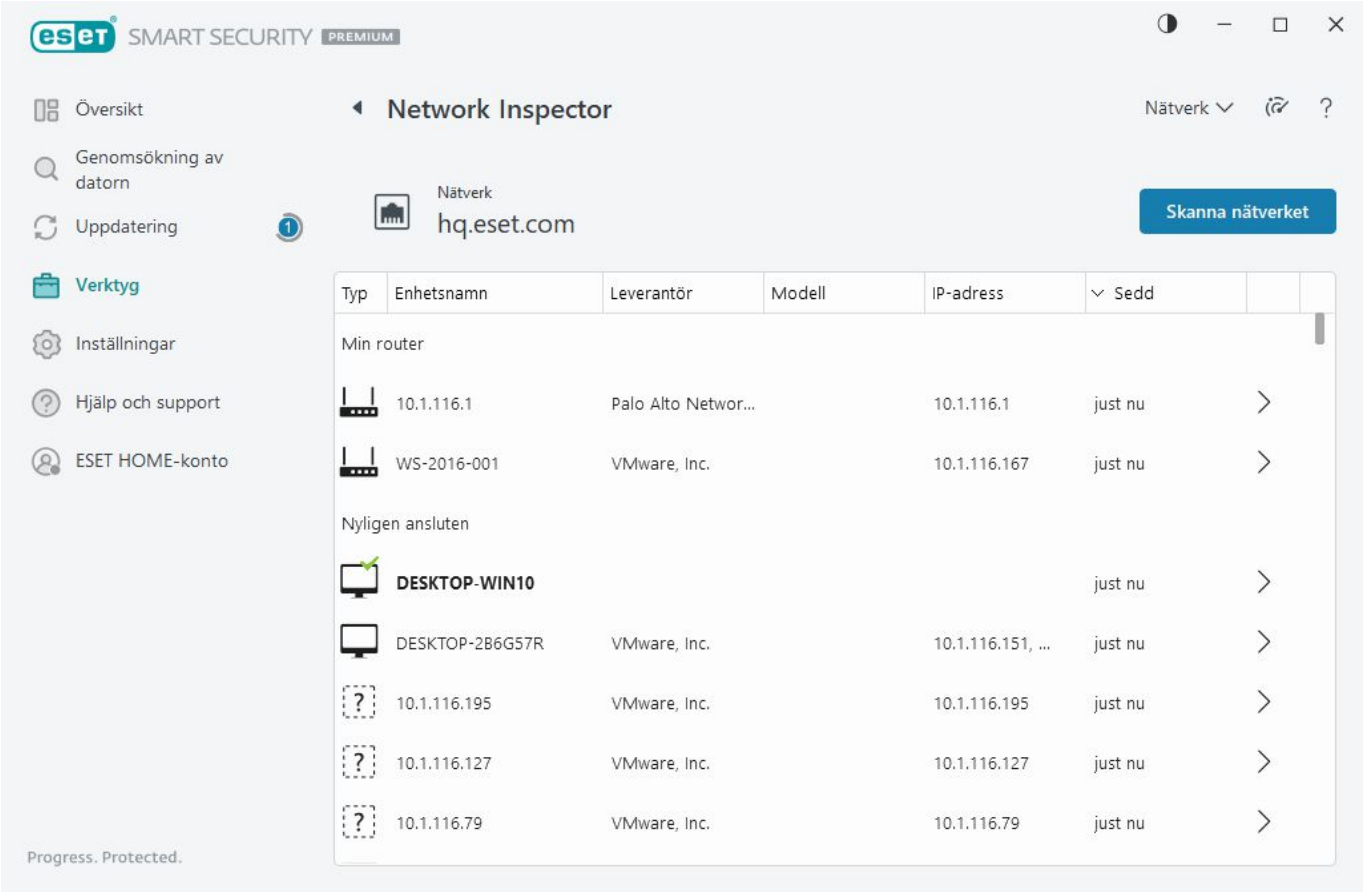
Klicka på kugghjulet ⚙ i det övre högra hörnet för att välja om du vill bli meddelad när en ny enhet upptäcks i nätverket.

Klicka på **Skanna nätverket** om du vill göra en manuell genomsökning av det nätverk du för närvarande är ansluten till. **Skanna nätverket** är endast tillgängligt för ett betrott nätverk. Se Nätverksanslutningsprofiler för att granska eller redigera dina nätverksinställningar.

Följande genomsökningsalternativ finns:

- Genomsök allt
- Genomsök endast router
- Genomsök endast enheter

⚠ Utför endast nätverksgenomsökningar på betrodda nätverk! Det är förenat med risker att göra detta i ej betrott nätverk.



När genomsökningen är klar visas ett meddelande med en länk till grundläggande information om enheten eller så kan du dubbelklicka på den misstänkta enheten i list- eller skrivbordsvyn. Klicka på **Felsök** om du vill se nyligen blockerad kommunikation. Mer information om felsökning av brandväggen.

Det finns två typer av meddelanden som visas av Network Inspector-modulen:

- **Ny enhet ansluten till nätverket** – visas om en okänd enhet ansluts till nätverket medan användaren är ansluten.
- **Nya nätverksenheter hittades** – visas om du återansluter till betrott nätverk och en tidigare okänd enhet nu finns.

Båda aviseringstyperna informerar dig om en obehörig enhet försöker ansluta till ditt nätverk. Klicka på **visa enhet** om du vill visa enhetsuppgifterna.

Vad betyder ikonerna på enheterna i Network Inspector?

	Den gula stjärnikonen anger enheter som är nya i nätverket eller som har upptäckts av ESET för första gången.
	Den gula varningsikonen indikerar att routern kan innehålla sårbarheter. Klicka på ikonen i produkten för mer detaljerad information om problemet.
	Den röda varningsikonen anger för enheter att routern innehåller sårbarheter och kan vara infekterad. Klicka på ikonen i produkten för mer detaljerad information om problemet.
	Den blå ikonen kan visas när ESET-produkten har ytterligare information för routern men inte kräver omedelbar uppmärksamhet eftersom det inte finns några säkerhetsrisker. Klicka på ikonen i produkten för mer detaljerad information.

Nätverksenhet i Network Inspector

Utförlig information om enheten hittar du här, inklusive följande:

- Enhetsnamn
- Enhetstyp
- Sågs senast
- Nätverksnamn
- IP-adress
- MAC-adress
- Operativsystem

Pennikonen indikerar att du kan ändra enhetsnamnet eller enhetstypen.

Ta bort från historiken – ta bort enheten från enhetslistan. Det här alternativet är endast tillgängligt för enheter som inte är anslutna till nätverket just nu.

Följande åtgärder är tillgängliga för varje enhetstyp:

Router

Routerinställningar – du kan komma åt routerinställningarna via webbgränssnittet eller mobilappen, eller genom att klicka på **Öppna routergränssnittet**. Om du har en router som har tillhandahållits av din internetleverantör kan du behöva kontakta dennes support eller routertillverkaren för att lösa upptäckta säkerhetsproblem. Följ alltid säkerhetsföreskrifterna i routerns användarhandbok.
Skydd – Om du vill skydda routern och nätverket mot IT-säkerhetsattacker följer du dessa grundläggande rekommendationer.

Nätverksenhet

Enhetsidentifiering – om du inte är säker på enheten som är ansluten till nätverket kontrollerar du återförsäljarens eller tillverkarens namn under enhetens namn. Det kan hjälpa dig att identifiera vilken slags enhet det är. Du kan ändra enhetens namn för framtida referens.
Koppla från enheten – om du inte är säker på att en ansluten enhet är säker för ditt nätverk eller dina enheter, så hanterar du nätverksåtkomsten för den enheten i routerinställningarna eller ändrar nätverkets lösenord.
Skydd – om du vill skydda enheter mot attacker och skadlig programvara installerar du ett datasäkerhetsskydd på enheten och ser till att alltid hålla operativsystemet och installerad programvara uppdaterade. Anslut inte till Wi-Fi-nätverk utan säkerhet om du vill hålla dig skyddad.

Denna enhet

Den här enheten representerar datorn på nätverket.
Nätverksadaptrar – visar information om nätverksadaptrarna.

Meddelanden | Network Inspector

Nedan följer flera meddelanden som kan visas när ESET Smart Security Premium hittar en sårbarhet i routern. Varje meddelande innehåller en kort beskrivning och en lösning eller åtgärder som bör vidtas för att minimera routerns sårbarhetsrisk. Vi rekommenderar dig att ta kontakt med din routers tillverkare eller din internetleverantör om du inte känner till hur man gör ändringar i routern.

Potentiell sårbarhet hittad
Routern kan innehålla kända sårbarheter som kan göra den enkel att attackera och utnyttja. Uppdatera routerns firmware.

Sårbarhet hittad
Routern innehåller kända sårbarheter som gör den enkel att attackera och utnyttja. Uppdatera routerns firmware.

Hot upptäckt
Routern är infekterad av skadlig kod. Starta om routern och upprepa genomsökningen.

Svagt routerlösenord
Routerns lösenord är svagt och kan enkelt gissas av andra. Byt routerns lösenord.

Skadlig omdirigering av nätverk
Internettrafiken verkar omdirigeras till skadliga webbplatser. Detta kan betyda att routern utsatts för en attack. Ändra routerns DNS-serverinställningar.

Öppna nätverkstjänster
Routern kör nätverkstjänster som kan utnyttjas av andra. Detta kan vara på grund av dålig konfiguration eller att routern utsatts för en attack. Kontrollera routerns konfiguration.

Känsliga öppna nätverkstjänster
Routern kör känsliga nätverkstjänster som kan utnyttjas av andra. Detta kan vara på grund av dålig konfiguration eller att routern utsatts för en attack. Kontrollera routerns konfiguration.

Firmware utdaterad
Routerns firmware är inaktuell och kan innehålla sårbarheter. Uppdatera routerns firmware.

Skadlig routerinställning
DNS-servern som routern använder är skadlig och kan skicka dig till farliga webbplatser. Detta kan betyda att routern utsatts för en attack. Ändra routerns DNS-serverinställningar.

Nätverkstjänster
Routern kör vanliga nätverkstjänster. Dessa behövs av nätverket och är förmodligen säkra. Kontrollera routerns konfiguration.

Karantän

Karantänen huvudfunktion är att säkert lagra rapporterade objekt (till exempel skadlig kod, infekterade filer eller potentiellt oönskade program).

Karantän är tillgänglig från ESET Smart Security Premium programmets huvudfönster genom att klicka på **Verktyg** > **Karantän**.

Filer som lagras i karantänmappen kan visas i en tabell som visar:

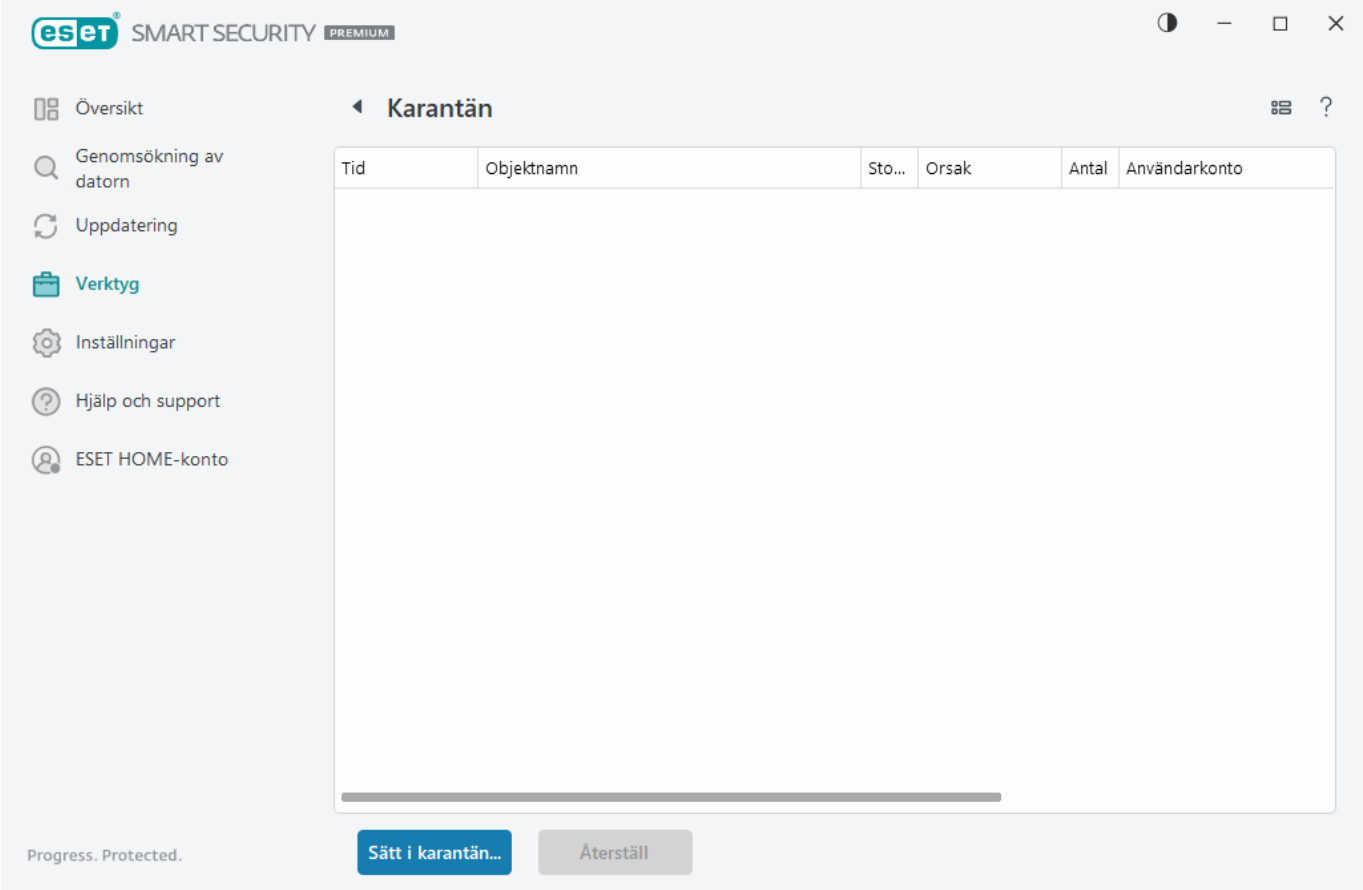
- datum och tidpunkt för karantänen,

• sökvägen till filens ursprungliga plats,

• dess storlek i byte,

• orsak (till exempel objekt som lagts till av användaren),

• och ett antal detekteringar (till exempel duplicerade detekteringar av samma fil eller om det är ett arkiv som innehåller flera infiltreringar).



Sätta filer i karantän

ESET Smart Security Premium sätter automatiskt borttagna filer i karantän (om du inte har inaktiverat det här alternativet i varningsfönstret).

Ytterligare filer bör sättas i karantän om de:

a.inte kan rensas,

b.om det inte är säkert eller rekommenderat att ta bort dem,

c.om de felaktigt detekteras av ESET Smart Security Premium,

d.eller om en fil beter sig misstänkt men inte detekteras av Skydd.

Om du vill sätta en fil i karantän finns det flera alternativ:

a.Använd funktionen för att dra och släppa för att sätta en fil i karantän manuellt genom att klicka på filen, flytta muspekaren till det markerade området med musknappen nedtryckt och sedan släppa den. Därefter flyttas programmet fram till förgrunden.

b.Högerklicka på filen > klicka på **Avancerade alternativ** > **Karantänfil**.

c.Klicka på **Flytta till karantän** från fönstret **Karantän**.

d.Snabbmenyn kan även användas för detta ändamål: högerklicka i fönstret **Karantän** och välj **Karantän**.

Återställer från karantän

Filer i karantän kan även återställas till sin ursprungliga plats:

- Använd funktionen **Återställning** för detta ändamål, som är tillgänglig från snabbmenyn genom att högerklicka på en viss fil i karantänen.
- Om en fil är markerad som ett potentiellt oönskat program är alternativet **Återställ och exkludera från genomsökning** aktiverat. Se även Exkluderingar.
- Snabbmenyn har även alternativet **Återställ till** som återställer en fil till en annan plats från vilken filen togs bort.
- Återställningsfunktionen är inte tillgänglig i vissa fall, till exempel för filer som finns på en skrivskyddad nätverksresurs.

Radera från karantänen

Högerklicka på önskat objekt och välj **Ta bort från karantän** eller markera objektet du vill ta bort och tryck på **Delete** på tangentbordet. Om du vill markera och ta bort alla objekt i karantän kan du trycka på **Ctrl + A** och sedan **Delete** på tangentbordet. Borttagna objekt tas bort permanent från enheten och karantänen.

Skicka in en fil från Karantän

Om du sätter en misstänkt fil som inte har upptäckts av programmet i karantän eller om en fil felaktigt bedöms vara infekterad (till exempel genom heuristisk analys av koden) och därför sätts i karantän, ber vi dig skicka skicka ett prov för analys till ESET:s viruslaboratorium. Skicka en fil genom att högerklicka på den och välja **Skicka in för analys** på snabbmenyn.

Detekteringsbeskrivning

Högerklicka på ett objekt och klicka på **Beskrivning av detektering** för att öppna ESET Threat Encyclopedia, som innehåller detaljerad information om farorna med och symptomen på den registrerade infiltrationen.

> **Anvisningar med bilder**
> Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:
> - Återställa en fil i karantän i ESET Smart Security Premium
> - Radera en fil i karantän i ESET Smart Security Premium
> - Min ESET-produkt informerade mig om en detektering – vad ska jag göra?

Karantänen misslyckades

Orsaker till att vissa filer inte kan sättas i karantän är följande:

- **Du har inte läsbehörighet** – det innebär att du inte kan visa innehållet i en fil.
- **Du har inte skrivbehörighet** – det innebär att du inte kan ändra innehållet i filen, dvs. antingen lägga till nytt innehåll eller ta bort det befintliga innehållet.
- **Filen du försöker sätta i karantän är för stor** – du måste minska filstorleken.

När felmeddelandet Karantänen misslyckades visas klickar du på **Mer information**. Fönstret med karantänfellistan öppnas och du ser namnet på filen och orsaken till att filen inte kan sättas i karantän.

Välj prov för analys

Om du hittar en misstänkt fil på datorn eller en misstänkt webbplats på internet kan du skicka den till ESET:s forskningslabb för analys (detta kanske inte är tillgängligt baserat på din konfiguration av ESET LiveGrid®).

> **Innan du skicka prover till ESET**
> Skicka inte in ett prov om det inte uppfyller minst ett av följande villkor:
> • Provet har inte identifierats av ESET-produkten
> • Provet är felaktigt identifierat som ett hot
> • Vi godkänner inte personliga filer (som du vill genomsöka efter skadlig kod hos ESET) som prover (ESET forskningslagg utför inte genomsökningar på begäran för användare)
> • Skriv en beskrivande ämnesrad och ta med så mycket information som möjligt om filen (t.ex. en skärmbild eller webbplatsen där du hämtade filen).

Det går att skicka ett prov (en fil eller en webbplats) till ESET för analys på något av dessa sätt:

1. Använd formuläret för insändning av prov i produkten. Det finns i **Verktyg** > **Skicka in prov för analys**. Den maximala storleken på ett inskickat prov är 256 MB.

2. Det går även att skicka filen med e-post. Om du föredrar det alternativet, arkivera filerna med WinRAR/WinZIP, skydda arkivet med lösenordet "infected" och skicka det till samples@eset.com.

3. Läs vår ESET kunskapsbasartikel om du vill rapportera skräppost, falsk positiv identifiering eller felaktigt kategoriserade webbplatser i modulen Föräldrakontroll.

Välj beskrivningen på rullgardinsmenyn **Orsak att skicka in provet** som bäst motsvarar meddelandets syfte i formuläret **Välj prov för analys**:

- Misstänkt fil
- Misstänkt webbplats (en webbplats som är infekterad av skadlig kod),
- Falsk positiv webbplats
- Falsk positiv fil (fil som detekterats som infekterad men inte är infekterad),
- Annat

Fil/webbplats – sökväg till filen eller webbplatsen som du tänker skicka in.

E-postadress E-postadressen skickas tillsammans med misstänkta filer till ESET och används för att kontakta dig om det krävs ytterligare information för analysen. Det är valfritt att ange en e-postadress. Välj **Skicka anonymt** för

att lämna den tom.

> **Du får kanske inget svar från ESET**
> Du får inget något svar från ESET såvida det inte behövs mer information från dig. Våra servrar tar varje dag emot tiotusentals filer vilket gör det omöjligt att svara på alla insändningar.
> Om filen visar sig vara ett skadligt program eller en skadlig webbplats läggs den till i en kommande ESET-uppdatering.

Välj prov för analys, misstänkt fil

Observerade tecken och symptom på infektion av skadlig kod – ge en beskrivning av hur den misstänkta filen beter sig på datorn.

Filens ursprung (URL-adress eller leverantör) – ange filens ursprung (källa) och hur du träffade på den här filen.

Anteckningar och ytterligare information – ange ytterligare information eller en beskrivning som hjälper till att bearbeta den misstänkta filen.

> Den första parametern – **Observerade tecken och symptom på infektion av skadlig kod** – krävs, men att ge ytterligare information hjälper våra laboratorier att identifiera och bearbeta prover.

Välj prov för analys. misstänkt webbplats

Välj ett av följande alternativ från rullgardinsmenyn **Vad är det för fel med webbplatsen**:

- **Infekterad** – en webbplats som innehåller virus eller annan skadlig kod som distribuerats på olika sätt.
- **Nätfiske** används för att få tillgång till känsliga data som bankkontonummer, PIN-koder och annat. Läs mer om den här attacktypen i ordlistan.
- **Bluff** – en bedräglig eller falsk webbsida, särskilt i syfte att göra snabba vinster.
- Välj **Annat** om webbplatsen du ska skicka inte stämmer in bland ovannämnda alternativ.

Anteckningar och ytterligare information – du kan skriva ytterligare information eller en beskrivning som hjälper oss att analysera den misstänkta webbplatsen.

Välj prov för analys, falsk positiv fil

Vi ber dig skicka in filer som identifierats som en infektion men inte är infekterade så att vi kan förbättra vårt skydd mot virus och spionprogram och hjälpa andra att skydda sig. Falska positiva (FP) kan inträffa när ett filmönster motsvarar samma mönster i en detekteringsmotor.

Programmets namn och version – programtiteln och dess version (t.ex. nummer, alias eller kodnamn).

Filens ursprung (URL-adress eller leverantör) – ange filens ursprung (källa) och hur du träffade på den här filen.

Programmets syfte – allmän beskrivning av programmet, programtyp (t.ex. webbläsare, mediaspelare osv.) och dess funktion.

Anteckningar och ytterligare information – ange ytterligare information eller en beskrivning som hjälper till att bearbeta den misstänkta filen.

> De tre första parametrarna krävs för att identifiera legitima program och skilja dem från skadlig kod. Genom att ge ytterligare information, hjälper du våra laboratorier i identifieringsprocessen och bearbetningen av prover.

Välj prov för analys, falsk positiv webbplats

Vi ber dig skicka in webbplatser som identifierats som infekterade, bedrägliga eller utsatta för nätfiske med inte är det. Falska positiva (FP) kan inträffa när ett filmönster motsvarar samma mönster i en detekteringsmotor. Var vänlig skicka sådana webbplatser så att vi kan förbättra vår motor mot virus och nätfiske och hjälpa andra att skydda sig.

Anteckningar och ytterligare information – ange ytterligare information eller en beskrivning som hjälper till att behandla den misstänkta webbplatsen.

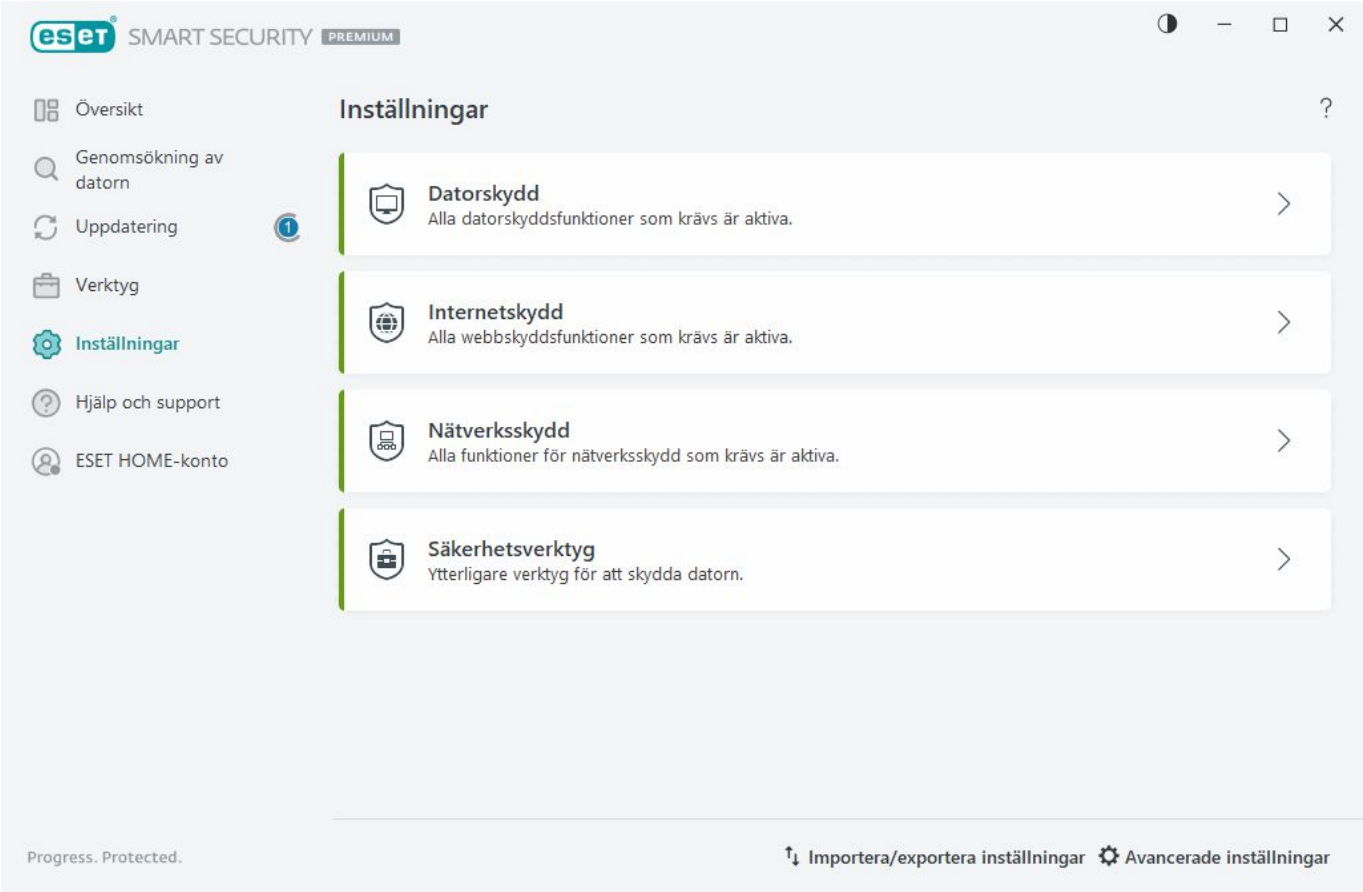
Välj prov för analys, övrigt

Använd detta formulär om filen inte går att kategorisera som en **Misstänkt fil** eller som en **Falsk positiv**.

Orsak att skicka in filen – ange en ingående beskrivning och orsaken till att skicka in filen.

Installation

Du hittar grupper av tillgängliga skyddsfunktioner i programmets huvudfönster > **Inställningar**.



Menyn **Inställningar** är indelad i följande avsnitt:

Datorskydd

Internetskydd

Nätverksskydd

Säkerhetsverktyg

Det finns ytterligare alternativ längst ned i inställningsfönstret. Använd länken Avancerade inställningar för att ställa in mer utförliga parametrar för varje modul. Använd Importera/exportera inställningar om du vill läsa in inställningsparametrar med en .xml-konfigurationsfil, eller om du vill spara de aktuella inställningsparametrarna till en konfigurationsfil.

Datorskydd

Klicka på **Datorskydd** i programmets huvudfönster > **Inställningar** för att se en översikt över alla skyddsmoduler:

- Skydd av filsystemet i realtid – alla filer genomsöks efter skadlig kod när de öppnas, skapas eller körs.
- ESET LiveGuard – lägger till ett molnbaserat skyddslager som är särskilt utformat för att minska hot som är nya.
- Proaktivt skydd – Blockerar körning av nya filer tills ESET LiveGuard-analysresultatet tas emot. Om du vill

avblockera filen som analyseras högerklickar du på filen och klickar på **Avblockera fil som analyseras av ESET LiveGuard.**

- Enhetskontroll – denna modul gör det möjligt att genomsöka, blockera eller justera utökade filter/behörigheter och välja hur användaren får åtkomst till och kan använda en viss enhet (CD/DVD/USB...).

- HIPS – HIPS-systemet övervakar händelser inne i operativsystemet och reagerar på dem enligt en uppsättning anpassade regler.

- Spelläge – aktiverar eller inaktiverar Spelläge. Du får ett varningsmeddelande (potentiell säkerhetsrisk) och huvudfönstret blir orange när spelläget aktiveras.

- Webbkameraskydd – styr de processer och program som har åtkomst till webbkameran.

Om du vill pausa eller inaktivera enskilda skyddsmoduler ska du klicka på växlingsknappen  .

⚠ Om du stänger av skyddsmoduler kan datorns skyddsnivå minskas.

Klicka på kugghjulsikone intill en skyddsmodul för att komma åt de avancerade inställningarna för den modulen.

För **Skydd av filsystemet i realtid** klickar du på kugghjulsikonen och väljer bland följande alternativ:

- **Konfigurera** – öppnar de avancerade inställningarna för Skydd av filsystemet i realtid.

- **Redigera exkluderingar** – öppnar inställningsfönstret Exkluderingar så att du kan utesluta filer och mappar från genomsökning.

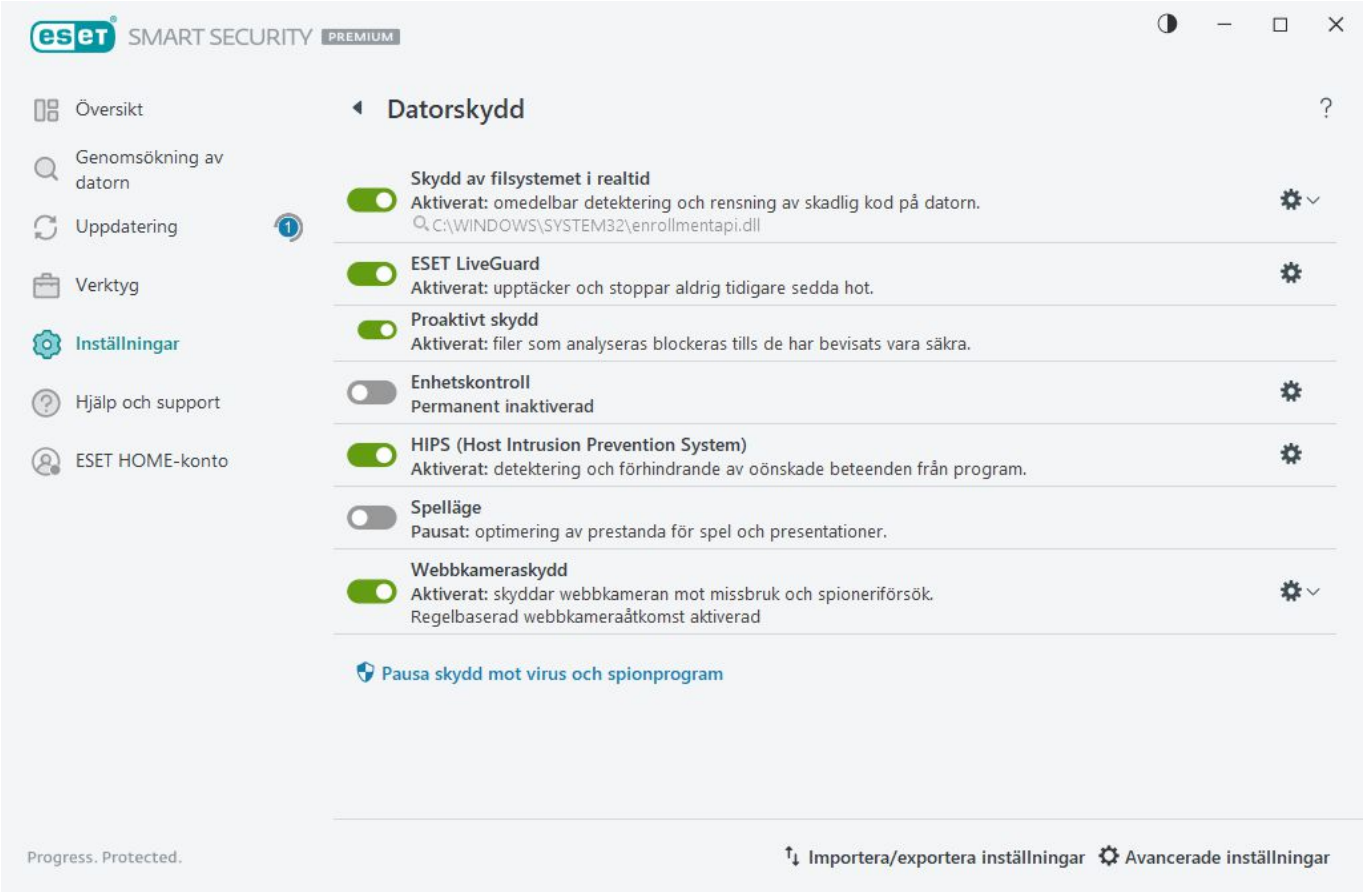
För **webbkameraskyddet** klickar du på kugghjulsikonen och väljer bland följande alternativ:

- **Konfigurera** – öppnar de avancerade inställningarna för webbkameraskyddet.

- **Blockera all åtkomst fram till omstart** – blockerar all åtkomst till webbkameran tills datorn startas om.

- **Blockera all åtkomst permanent** – blockerar all åtkomst till webbkameran tills den här inställningen inaktiveras.

- **Sluta blockera all åtkomst** – inaktiverar möjligheten att blockera webbkameraåtkomsten. Det här alternativet är endast tillgängligt om webbkameraåtkomsten är blockerad.



Pausa antivirus- och antispionskydd – inaktiverar alla antivirus- och antispionskyddsmoduler. När du inaktiverar skyddet öppnas ett fönster för att avgöra hur länge skyddet ska vara inaktiverat med hjälp av rullgardinsmenyn **Tidsintervall**. Använd endast detta om du är en erfaren användare eller instrueras av ESET:s tekniska support.

En infiltration identifieras

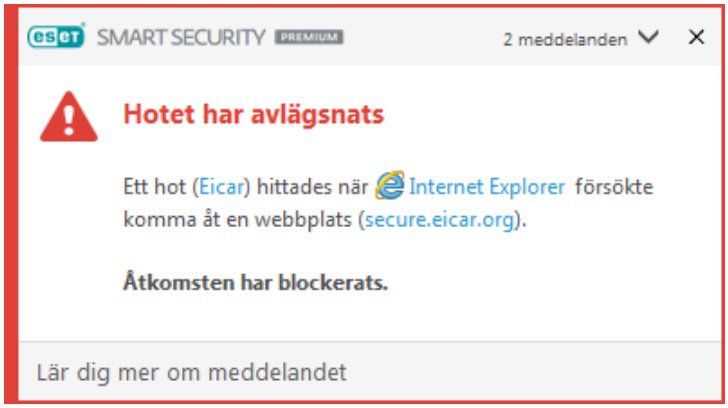
Datorn kan infiltreras från många olika håll, som t.ex. från webbsidor, delade mappar, via e-post eller från flyttbara lagringsenheter (USB-enheter, externa enheter, CD- och DVD-skivor, osv.).

Standardbeteende

Som ett allmänt exempel på hur infiltrationer hanteras av ESET Smart Security Premium går det att identifiera infiltrationer med:

- Skydd av filsystemet i realtid
- Webbåtkomstskydd
- Skydd av e-postklient
- Genomsökning av datorn på begäran

Var och en använder standardrensningsnivån och försöker att rensa filer och flytta den till Karantän eller avbryta anslutningen. Ett meddelandefönster visas i meddelandefältet längst ned till höger på skärmen. För utförlig information om detekterade/rensade objekt, se Loggfiler. För mer information om rensningsnivåer och beteende, se Rensningsnivå.



Genomsöka datorn efter infekterade filer

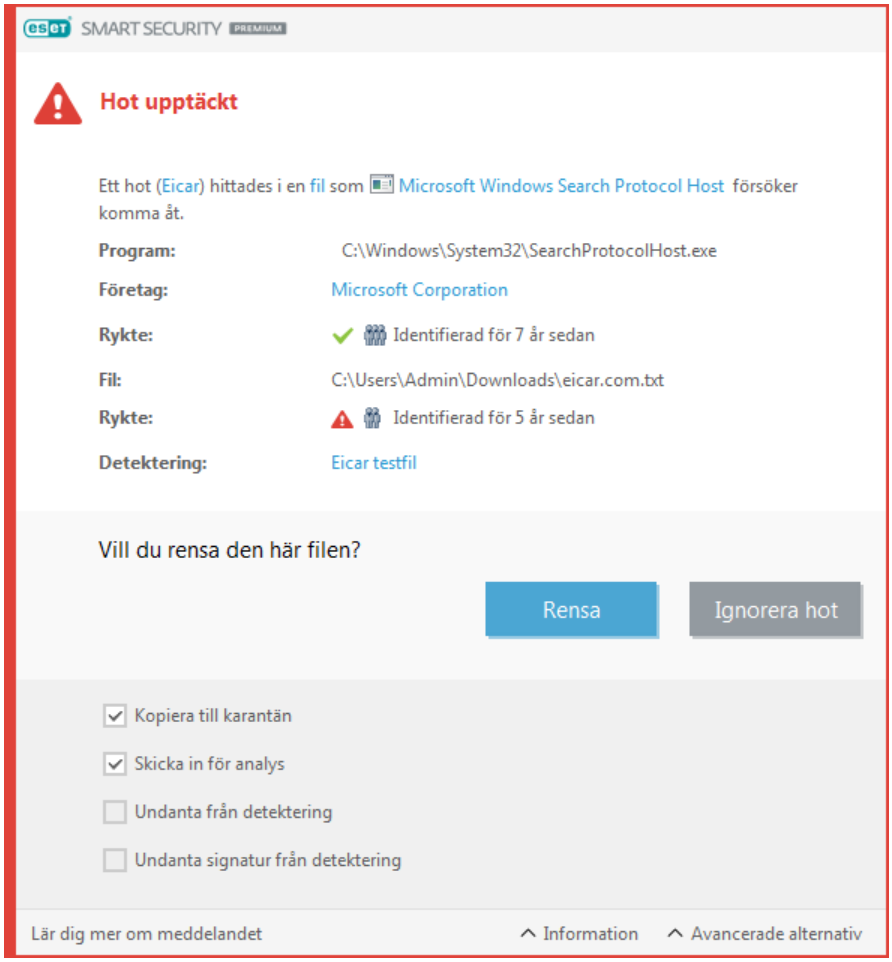
Om datorn visar tecken på att ha blivit infekterad av skadlig programvara, till exempel om den har blivit långsammare eller ofta låser sig, rekommenderar vi att du gör följande:

1. Öppna ESET Smart Security Premium och klicka på **Genomsökning av datorn**.
2. Klicka på **Genomsök datorn** (för mer information, se Genomsökning av datorn).
3. När genomsökningen har slutförts visas antalet genomsökta, infekterade och rensade filer i loggen.

Om du endast vill genomsöka en viss del av disken klickar du på **Anpassad genomsökning** och anger vad som ska genomsökas efter virus.

Rensa och ta bort

Om det inte finns någon fördefinierad åtgärd för skydd av filsystemet i realtid visas ett varningsfönster och du uppmanas att ange ett alternativ. Vanligen är alternativen **Rensa**, **Ta bort** och **Ingen åtgärd** tillgängliga. Vi rekommenderar inte att välja **Ingen åtgärd** eftersom detta lämnar infekterade filer orensade. Undantaget är när du är säker på att en fil är ofarlig och identifierades av misstag.



Verkställ rensning om en fil har angripits av ett virus som har lagt till skadlig kod i filen. Om detta är fallet ska du först försöka rensa den infekterade filen så att den återgår till ursprungsläget. Om filen endast består av skadlig kod tas den bort.

Om en infekterad fil är ”låst” eller används av en systemprocess tas den vanligtvis inte bort förrän den har släppts (normalt efter det att systemet har startats om).

Återställer från karantän

Karantän är tillgänglig från ESET Smart Security Premium programmets huvudfönster genom att klicka på **Verktyg** > **Karantän**.

Filer i karantän kan även återställas till sin ursprungliga plats:

- Använd funktionen **Återställning** för detta ändamål, som är tillgänglig från snabbmenyn genom att högerklicka på en viss fil i karantänen.
- Om en fil är markerad som ett potentiellt oönskat program är alternativet **Återställ och exkludera från genomsökning** aktiverat. Se även Exkluderingar.
- Snabbmenyn har även alternativet **Återställ till** som återställer en fil till en annan plats från vilken filen togs bort.
- Återställningsfunktionen är inte tillgänglig i vissa fall, till exempel för filer som finns på en skrivskyddad nätverksresurs.

Flera hot

Om en del infekterade filer inte rensades under Genomsökning av datorn (eller Rensningsnivå ställdes in på **Ingen rensning**) visas ett varningsfönster där du ombeds välja åtgärder för filerna. Välj åtgärder för filerna (åtgärderna anges individuellt för varje fil i listan) och klicka sedan på **Slutför**.

Ta bort filer i arkiv

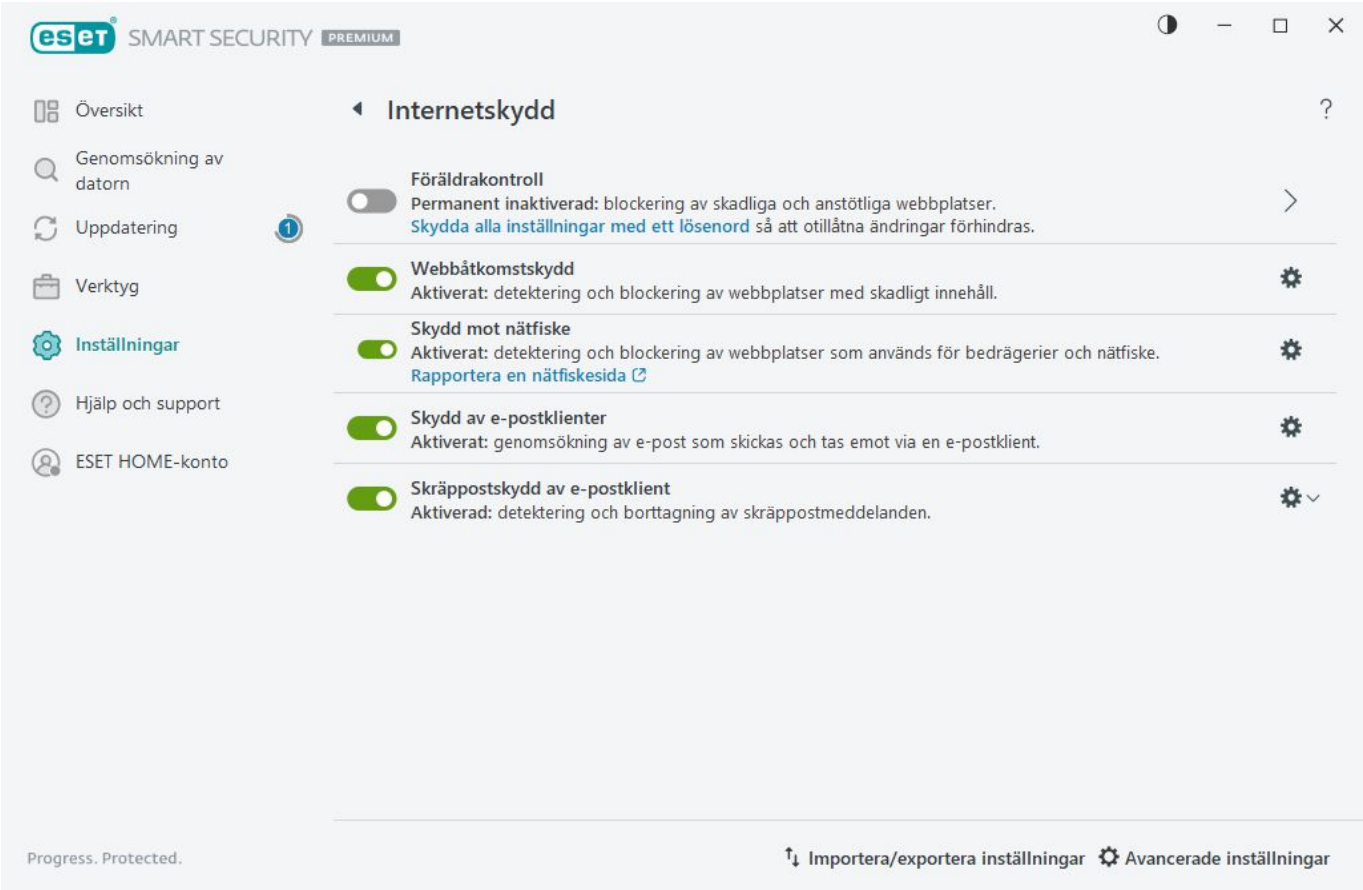
I standardläget tas hela arkivet endast bort om det bara innehåller infekterade filer och inga rena filer. I standardläget tas arkiv inte bort om de även innehåller ofarliga, rena filer. Var försiktig när du utför en genomsökning med Strikt rensning. Om Strikt rensning är aktiverat tas hela arkivet bort om det innehåller minst en infekterad fil, oavsett status för de andra filerna i arkivet.

Internetskydd

Möjligheten att ansluta till Internet har blivit en standardfunktion hos dagens datorer. Det är tyvärr även huvudvägen för att överföra skadlig kod. Öppna programmets huvudfönster > **Inställningar** > **Internetskydd** för att konfigurera funktioner i ESET Smart Security Premium som ökar ditt internetskydd.

Om du vill pausa eller inaktivera enskilda skyddsmoduler ska du klicka på växlingsknappen .

Om du stänger av skyddsmoduler kan datorns skyddsnivå minskas.



Klicka på kugghjulsikone intill en skyddsmodul för att komma åt de avancerade inställningarna för den modulen.

Modulen Föräldrakontroll skyddar föräldrakontroll dina barn genom att blockera olämpligt eller skadligt innehåll på internet.

Webbåtkomstskydd genomsöker HTTP/HTTPS-kommunikation efter skadlig kod och nätfiske. Webbåtkomstskydd bör endast inaktiveras för felsökning.

Med Skydd mot nätfiske kan du blockera webbsidor som är kända för att distribuera sådant innehåll. Vi rekommenderar starkt att du låter Skydd mot nätfiske vara markerat.

Rapportera en webbplats med nätfiske – rapportera en webbplats med närfiske eller skadlig kod till ESET för analys.

Innan du skickar en webbplats till ESET, kontrollera att den uppfyller ett eller flera av följande villkor:
- Webbplatsen är inte alls identifierad.
- Webbplatsen är felaktigt identifierad som ett hot. I så fall kan du Rapportera felaktigt blockerad sida.

Skydd av e-postklient kontrollerar e-postkommunikation som sker med POP3(S)- och IMAP(S)-protokollet. Med plugin-programmet för e-postklienter ger ESET Smart Security Premium användaren kontroll över alla typer av kommunikation från e-postklienten.

Skräppostskydd för e-postklient filtrerar oönskade e-postmeddelanden.

För **Skräppostskydd för e-postklient** ska du klicka på kugghjulsikonen och välja bland följande alternativ:

- **Konfigurera** – öppnar avancerade inställningar för Skräppostskydd för e-postklient.
- **Användarens adresslista** (om den är aktiverad) – öppnar en dialogruta där du kan lägga till, redigera eller ta bort adresser för att definiera antispamreglerna. Regler i den här listan tillämpas på den aktuella användaren.
- **Global adresslista** (om den är aktiverad) – öppnar en dialogruta där du kan lägga till, redigera eller ta bort adresser för att definiera antispamreglerna. Reglerna i den här listan tillämpas på alla användare.

Skydd mot nätfiske

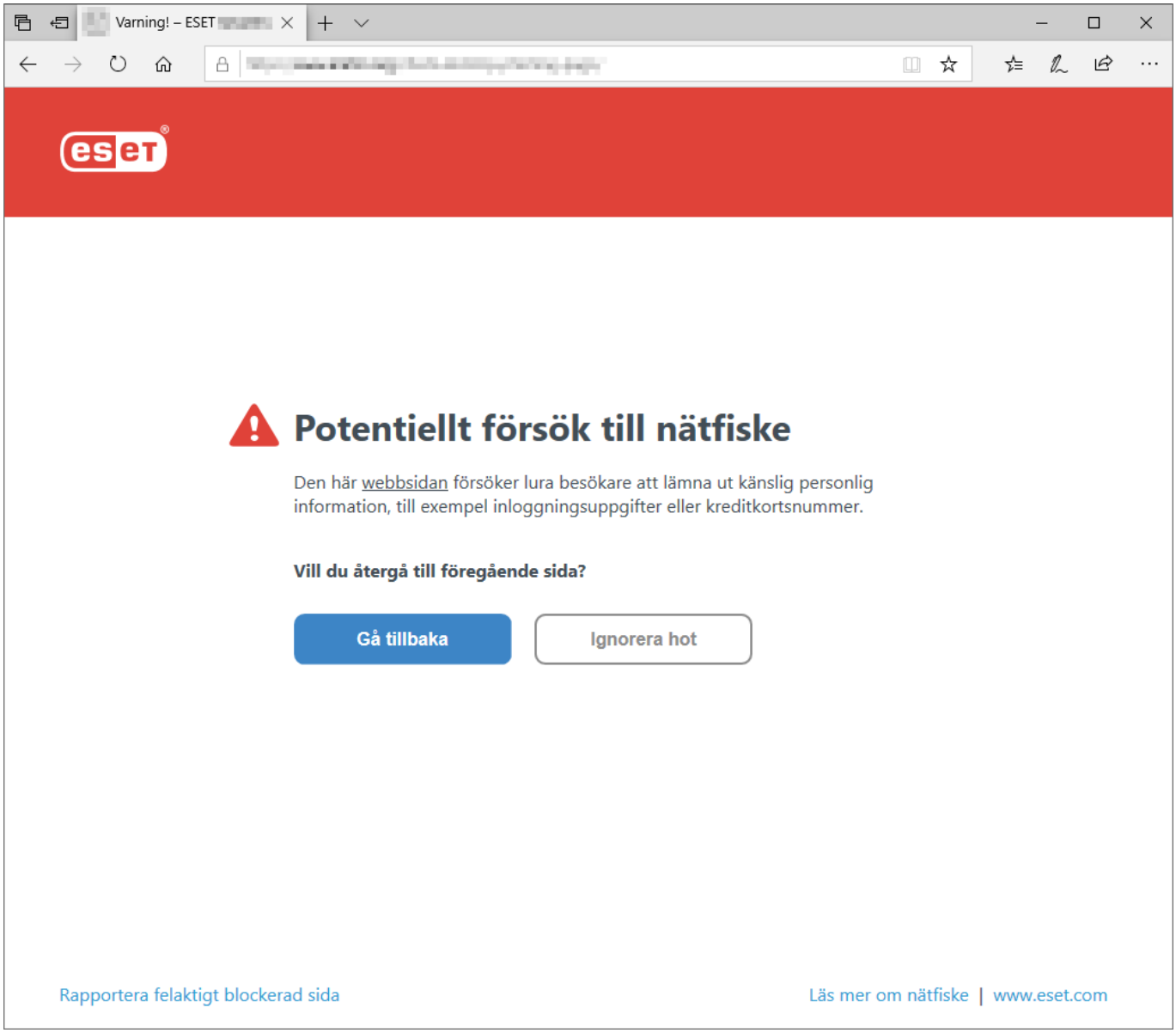
Nätfiske är en kriminell aktivitet som använder social manipulation (användare manipuleras för att komma åt konfidentiell information). Nätfiske används för att komma åt känsliga uppgifter som bankkontonummer, PIN-koder och så vidare. Läs mer i ordlistan. ESET Smart Security Premium inkluderar skydd mot nätfiske, som blockerar webbsidor som är kända för att distribuera sådant.

Skydd mot nätfiske är aktiverat som standard. Det går att konfigurera den här inställningen i Avancerade inställningar > **Skydd** > **Webbåtkomstskydd**.

Besök vår kunskapsbas för mer information om skydd mot nätfiske i ESET Smart Security Premium.

Öppna en webbplats med nätfiske

När du öppnar en känd nätfiskewebbplats visar webbläsaren följande dialogruta. Om du vill besöka webbplatsen ändå klickar du på **Ignorera hot** (rekommenderas inte).



Potentiella nätfiskewebbplatser som har vitlistats upphör som standard efter flera timmar. Tillåt en webbplats permanent genom att använda verktyget URL-adressbehandling. I Avancerade inställningar > **Skydd** > **Webbåtkomstskydd** > **URL-adressbehandling** > **Adresslista** > **Redigera** lägger till webbplatsen du vill redigera i listan.

Rapportera en nätfiskesida

Med länken **Rapportera en felaktigt blockerad sida** kan du rapportera en webbplats som felaktigt identifieras som ett hot.

Det går även att skicka webbplatsen med e-post. Skicka e-postmeddelandet till samples@eset.com. Kom ihåg att använda en beskrivande ämnesrad och ta med så mycket information som möjligt om filen (t.ex. webbplatsen du hänvisades dit från, hur du hörde talas om webbplatsen osv.).

Föräldrakontroll

Modulen Föräldrakontroll gör det möjligt att konfigurera inställningar för föräldrakontroll, vilken ger föräldrar automatiska verktyg för att skydda sina barn och ställa in begränsningar för enheter och tjänster. Målet är att

förhindra att barn och ungdomar får åtkomst till sidor med olämpligt eller skadligt innehåll.

Föräldrakontroll gör det möjligt att blockera webbsidor med potentiellt stötande innehåll. Det går även att blockera åtkomst till upp till 40 fördefinierade webbplatskategorier och över 140 underkategorier.

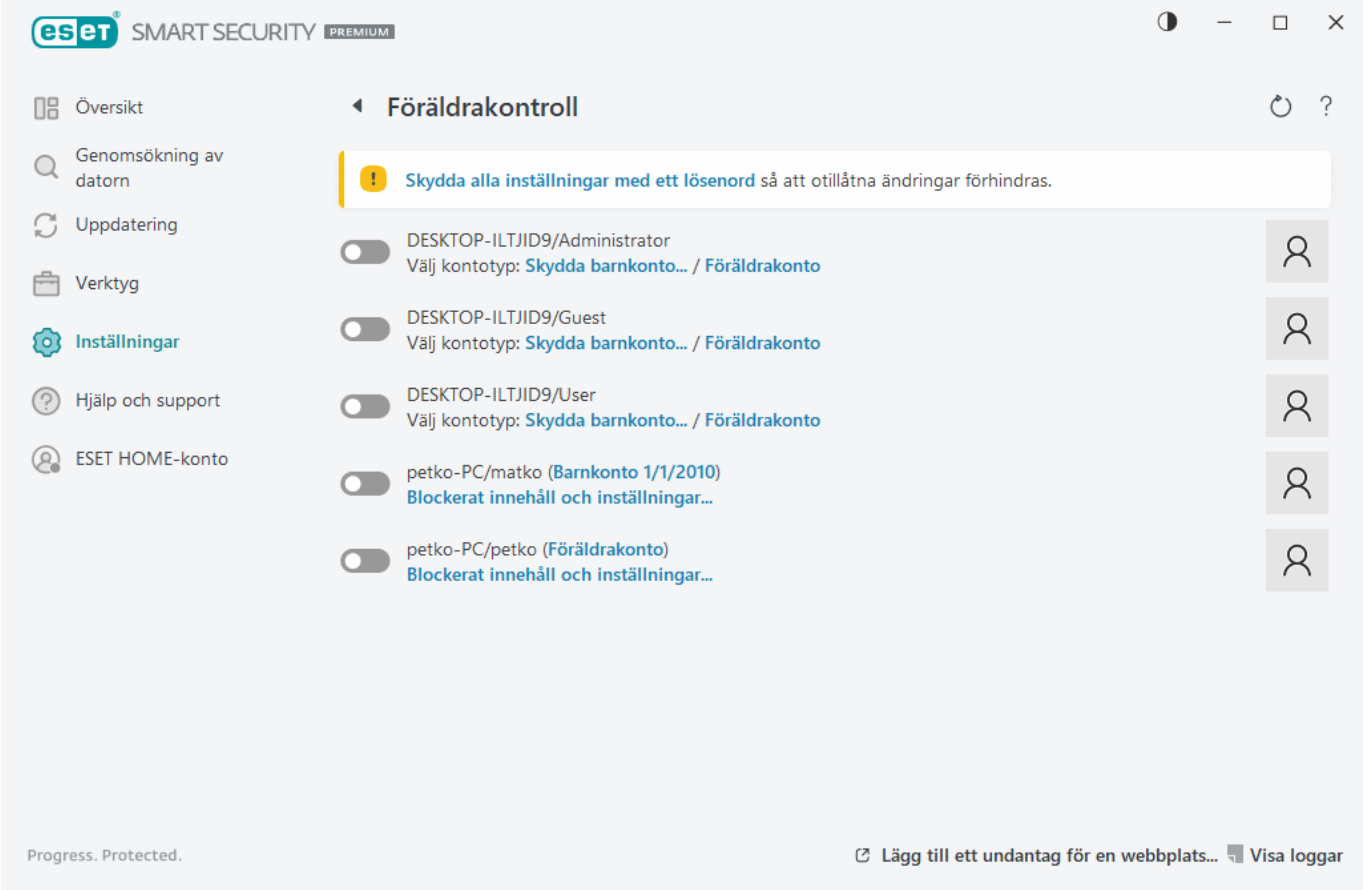
Aktivera Föräldrakontroll för ett visst användarkonto genom att följa stegen nedan:

1. Föräldrakontroll är inaktiverad som standard i ESET Smart Security Premium. Det finns två sätt att aktivera föräldrakontroll:

   • Klicka på växlingsikonen i **Inställningar** > **Internetskydd** > **Föräldrakontroll** från programmets huvudfönster och ändra statusen för Föräldrakontroll till aktiverad.

   • Öppna Avancerade inställningar > **Skydd** > **Webbåtkomstskydd** > **Föräldrakontroll** och aktivera sedan växlingsknappen bredvid **Aktivera föräldrakontroll**.

2. Klicka på **Inställningar** > **Internetskydd** > **Föräldrakontroll** i programmets huvudfönster. Även om **Aktiverad** visas intill **Föräldrakontroll**, måste du konfigurera föräldrakontrollen för önskat konto genom att klicka på pilsymbolen och i nästa fönster sedan välja **Skydda barnkonto** eller **Föräldrakonto**. I nästa fönster anger du födelsedatum för att avgöra nivån för åtkomst och rekommenderad ålder enligt webbsidorna. Föräldrakontroll aktiveras nu för det angivna användarkontot. Klicka på **Blockerat innehåll och inställningar...** under ett kontonamn för att anpassa kategorier du vill tillåta eller blockera på fliken Kategorier. Tillåt eller blockera anpassade webbsidor som inte passar in i en kategori genom att klicka på fliken Undantag.



Om du klickar på **Inställningar** > **Internetskydd** > **Föräldrakontroll** i huvudproduktfönstret för ESET Smart Security Premium ser du att huvudfönstret innehåller:

Windows-användarkonton

Om du har skapat en roll till ett befintligt konto visas det här. Klicka på växlingsknappen  så att en grön bock  visas bredvid Föräldrakontroll för kontot. Klicka på Blockerat innehåll och inställningar under ett aktivt konto för att visa en lista med tillåtna kategorier webbsidor för kontot och blockerade och tillåtna webbsidor.

Fönstrets nedre del innehåller

Lägg till ett undantag för en webbplats – den specifika webbplatsen kan tillåtas eller blockeras enligt dina preferenser för varje föräldrakonto separat.

Visa loggar – visar en detaljerad logg för aktiviteten i Föräldrakontroll (blockerade sidor, kontot sidan blockerades för, kategori osv.). Det går även att filtrera den här loggen med villkor du väljer genom att klicka på  **Filtrering**.

Föräldrakontroll

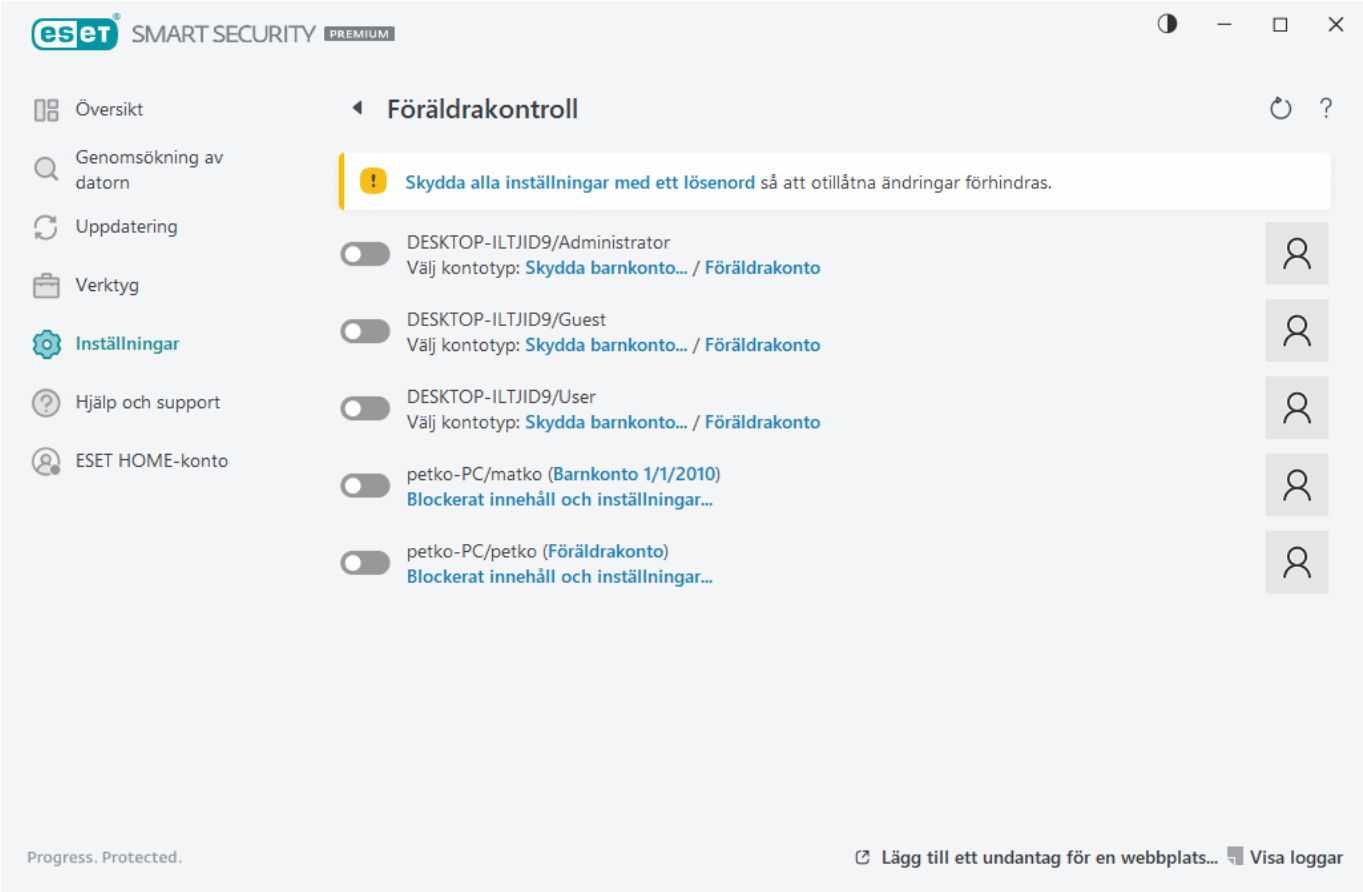
När Föräldrakontroll inaktiverats visas fönstret **Inaktivera föräldrakontroll**. Här går det att ställa in tidsintervallet under vilket skyddet är inaktiverat. Alternativet ändras sedan till **Pausat** eller **Permanent inaktiverat**.

Det är viktigt att skydda inställningarna i ESET Smart Security Premium med ett lösenord. Lösenordet går att ställa in i avsnittet Inställningar för åtkomst. Om inget lösenord ställts in visas följande varning: **Skydda alla inställningar med ett lösenord**, så att otillåtna ändringar förhindras. De inställda begränsningarna i Föräldrakontroll påverkar endast standardanvändarkonton. Eftersom en administratör kan åsidosätta begränsningarna har de ingen verkan.

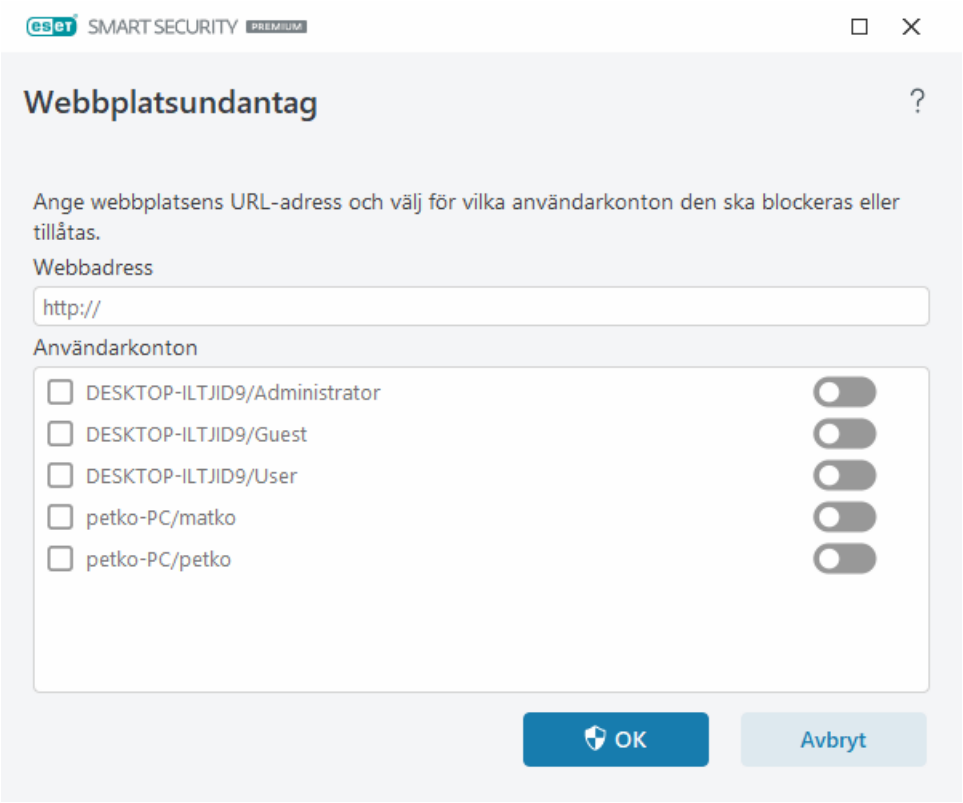
> Föräldrakontroll kräver att Nätverkstrafikskanner, HTTP(S)-trafikgenomsökning och Brandvägg är aktiverade för att fungera korrekt. Alla dessa funktioner är aktiverade som standard.

Webbplatsundantag

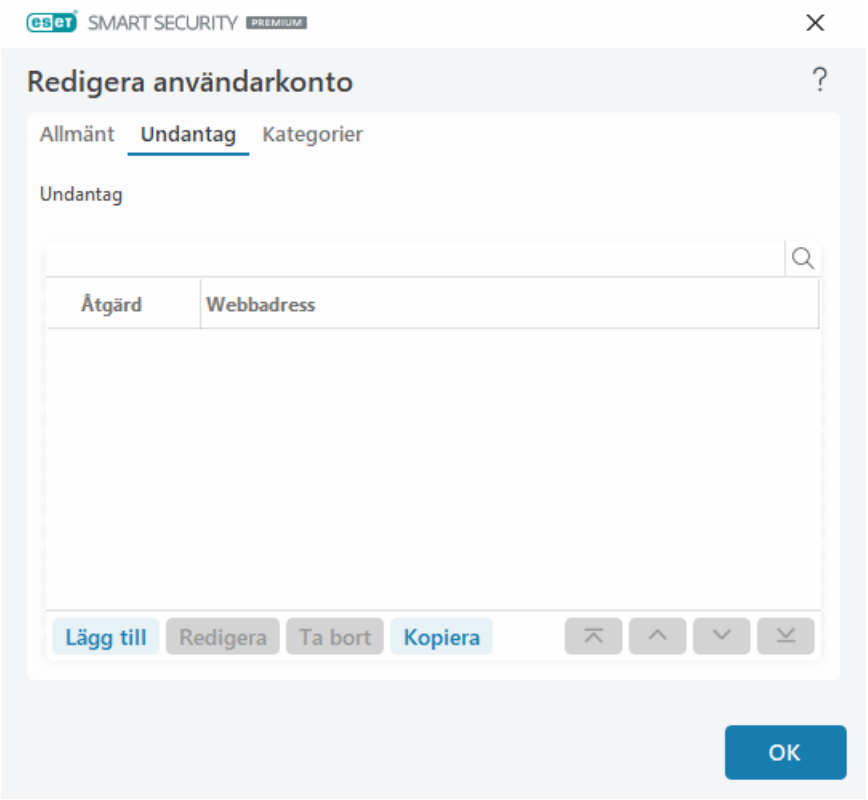
Om du vill lägga till ett undantag för en webbplats klickar du på **Inställningar** > **Internetskydd** > **Föräldrakontroll** och sedan på **Lägg till ett undantag för en webbplats**.



Ange en webbadress i fältet **Webbplatsens adress** och välj ✔ (tillåtet) eller ⊘ (blockerat) för varje specifikt användarkonto och klicka sedan på **OK** för att lägga till det i listan.



Om du vill ta bort en webbadress från listan klickar du på **Inställningar** > **Internetskydd** > **Föräldrakontroll**, klickar på **Blockerat innehåll och inställningar** under önskat användarkonto, klickar på fliken **Undantag**, markerar undantaget och klickar sedan på **Ta bort**.



I URL-adresslistan går det inte att använda symbolerna * (asterisk) och ? (frågetecken). Till exempel webbsideadresser med flera TLD måste anges manuellt (*examplepage.com*, *examplepage.sk* osv.). När du lägger till en domän i listan, blockeras eller tillåts allt innehåll på denna domän och alla underdomäner (t.ex. *sub.examplepage.com*) baserat på ditt val av URL-baserad åtgärd.

Blockera eller tillåta en viss webbsida kan vara noggrannare än att blockera eller tillåta en kategori webbsidor. Var försiktig när du ändrar dessa inställningar och när du lägger till en kategori/webbsida på listan.

Kopiera undantag från användar

Välj en användare i listrutan som du vill kopiera ett skapat undantag från.

Kopiera kategorier från konto

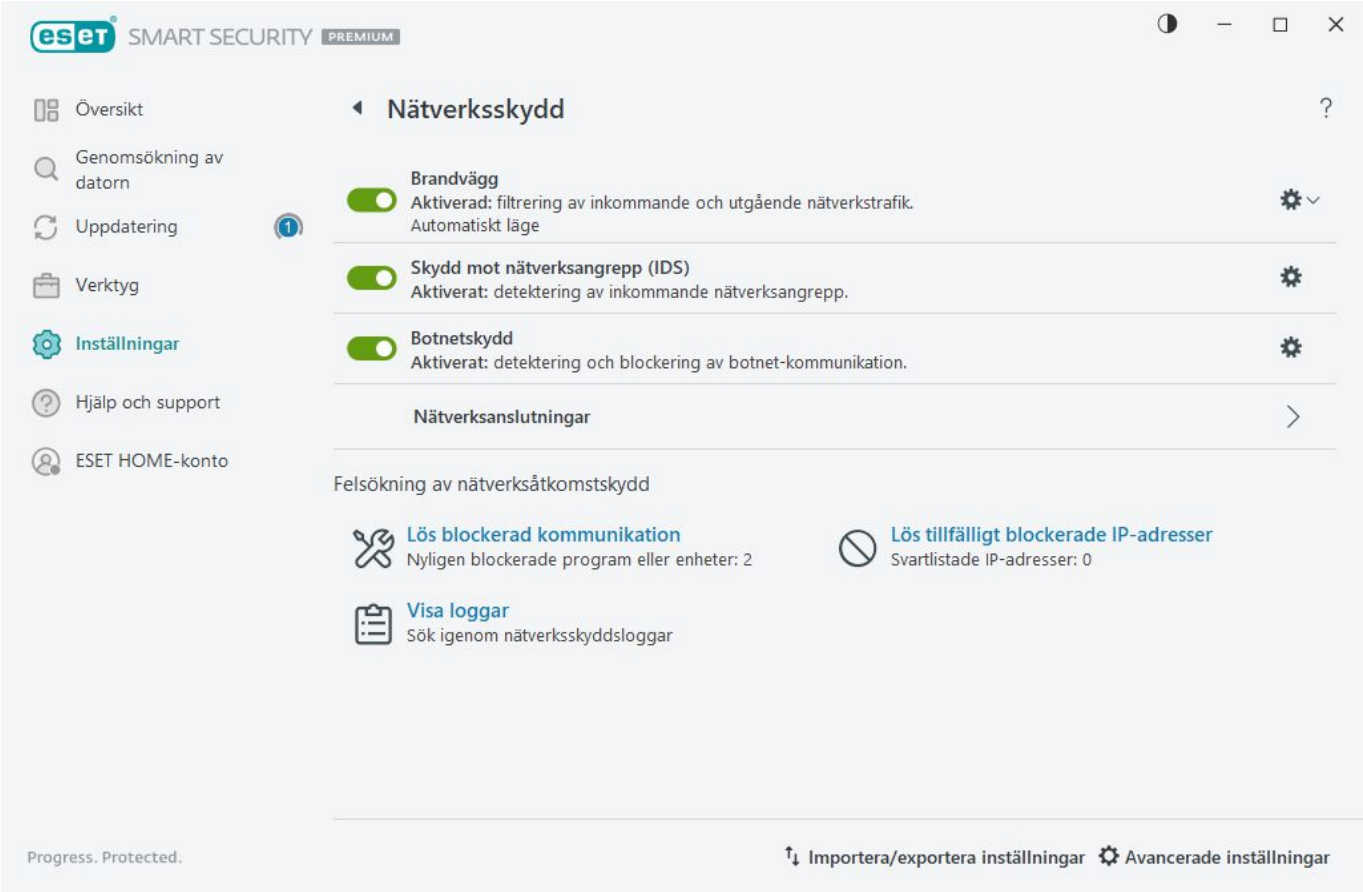
Gör det möjligt att kopiera en lista med blockerade eller tillåtna kategorier från ett befintligt ändrat konto.

Nätverksskydd

Öppna programmets huvudfönster > **Inställningar** > **Nätverksskydd** för att konfigurera grundläggande inställningar för Nätverksskydd eller felsöka nätverkskommunikation.

Om du vill pausa eller inaktivera enskilda skyddsmoduler ska du klicka på växlingsknappen .

Om du stänger av skyddsmoduler kan datorns skyddsnivå minskas.



Klicka på kugghjulsikone ⚙ intill en skyddsmodul för att komma åt de avancerade inställningarna för den modulen.

Brandvägg – filtrerar all nätverkskommunikation baserat på konfigurationen av ESET Smart Security Premium.

Konfigurera – öppnar Avancerade inställningar för brandvägg där du kan definiera hur brandväggen hanterar nätverkskommunikation.

Pausa brandvägg (tillåt all trafik) – alla filtreringsalternativ för brandväggen stängs av och alla inkommande och utgående anslutningar tillåts. Klicka på **Aktivera brandvägg** för att aktivera brandväggen igen när Filtrering av nätverkstrafik befinner sig i det här läget.

Blockera all trafik – all inkommande och utgående kommunikation blockeras av brandväggen. Använd detta alternativ endast om du misstänker att en kritisk säkerhetsrisk kräver att hela systemet kopplas bort från nätverket. När Filtrering av nätverkstrafik befinner sig i läget **Blockera all trafik** klickar du på **Sluta blockera all trafik** för att återställa brandväggen till normal drift.

Automatiskt läge – (när ett annat filtreringsläge är aktiverat) – klicka för att ändra filtreringsläget till automatiskt filtreringsläge (med användardefinierade regler).

Interaktivt läge – (när ett annat filtreringsläge är aktiverat) – klicka för att ändra filtreringsläget till interaktivt filtreringsläge.

Skydd mot nätverksangrepp (IDS) – analyserar innehållet i nätverkstrafik och skyddar mot nätverksangrepp. Trafik som anses skadlig blockeras. ESET Smart Security Premium informerar dig när du ansluter till ett oskyddat nätverk eller ett nätverk med svagt skydd.

Botnätsskydd – upptäcker snabbt och tillförlitligt skadlig programvara i systemet.

Nätverksanslutningar – visar nätverken som nätverkskorten är anslutna till med detaljerad information.

Felsök blockerad kommunikation – hjälper dig att lösa anslutningsproblem som orsakas av ESET Brandvägg. För mer utförlig information, se Felsökningsguide.

Lös tillfälligt blockerade IP-adresser – Visa en lista över IP-adresser som har identifierats som källor till attacker och lagts till i svartlistan för att blockera anslutning under en viss tidsperiod.

Visa loggar – öppnar loggfilen för Nätverksskydd.

Nätverksanslutningar

Visar vilka nätverk nätverksadaptrar är anslutna till. Om du vill se nätverksanslutningar ska du öppna programmets huvudfönster > **Inställningar** > **Nätverksskydd** > **Nätverksanslutningar**.

Dubbelklicka på en anslutning i listan för att visa information om anslutningen och om nätverkskortet.

Håll muspekaren över en specifik nätverksanslutning och klicka på menyikonen ⋮ i kolumnen **Betrodda** för att välja ett av följande alternativ:

- **Redigera** – öppnar fönstret Konfigurera nätverksskydd där du kan tilldela en nätverksskyddsprofil till ett visst nätverk
- **Glöm** – återställer nätverksanslutningen till standardkonfigurationen
- **Genomsök nätverk med Network Inspector** – öppnar Network Inspector för att köra en nätverksgenomsökning
- **Markera som ”Mitt nätverk”** – lägger till taggen ”Mitt nätverk”. Den här taggen visas bredvid nätverket i hela ESET Smart Security Premium för bättre identifiering och säkerhetsöversikt
- **Avmarkera som ”Mitt nätverk”** – tar bort taggen ”Mitt nätverk”. Endast tillgängligt om nätverket redan är taggat

Information om nätverksanslutning

Dubbelklicka på en anslutning i listan över nätverksanslutningar för att visa information om anslutningen tillsammans med information om nätverkskortet. Information om nätverksanslutning och nätverkskort kan hjälpa dig att identifiera nätverket som du försöker konfigurera i Nätverksåtkomstskydd.

Information om nätverksanslutning:

- Status för nätverksanslutningen
- Datum och tid för den första nätverksidentifieringen
- Förra gången nätverket var aktivt
- Total tid som har spenderats ansluten till det här nätverket
- Nätverksanslutningsprofil
- Nätverksanslutningsprofil definierad i Windows

- Konfiguration av nätverksskydd (om nätverket är betrott)

Information om nätverkskort:

- Typ av anslutning (trådbunden, virtuell etc.)
- Namn på nätverkskort
- Beskrivning av nätverkskort
- IP-adress med MAC-adress
- IPv4- och IPv6-adressen för nätverket med undernät
- DNS-suffix
- IP-adress för DNS-server
- IP-adress för DHCP-server
- IP-adress och MAC-adress för standardateway
- Kortets MAC-adress

Felsökning av nätverksåtkomst

Felsökningsguiden hjälper dig att lösa anslutningsproblem orsakade av brandväggen. **Felsökning av nätverksåtkomst** finns i programmets huvudfönster > **Inställningar** > **Nätverksskydd** > **Lös blockerad kommunikation**.

Välj om du vill visa kommunikation blockerad för **Lokala program** eller blockerad kommunikation från **Fjärrenheter**.

Välj en tidsperiod under vilken kommunikation blockerats i listrutan. En lista över nyligen blockerad kommunikation ger en översikt över typen av program eller enhet, rykte och totalt antal program och enheter som blockerats under tidsperioden. För mer information om blockerad kommunikation klickar du på **Information**. Nästa steg är att avblockera programmet eller enheten som har anslutningsproblem.

När du klickar på **Avblockera** tillåts den tidigare blockerade kommunikationen. Om du fortfarande har problem med ett program, eller om enheten inte fungerar som väntat, ska du klicka på **Skapa en regel till** så att all kommunikation som tidigare blockerades för enheten nu tillåts. Starta om datorn om problemet kvarstår.

Klicka på **Öppna brandväggsregler** om du vill visa regler som har skapats av guiden. Det går dessutom att visa reglerna skapade av guiden i Avancerade inställningar > **Skydd** > **Nätverksskydd** > **Brandvägg** > **Regler** > **Redigera**.

> Ett felmeddelande visas om det inte går att skapa regeln. Klicka på **Försök igen** och upprepa processen för att häva blockeringen av kommunikationen eller skapa en annan regel från listan över blockerad kommunikation.

Temporär svartlista över IP-adresser

Om du vill visa om IP-adresser som har identifierats som källor till attacker har lagts till i svartlistan för att blockera anslutning under en viss tidsperiod ska du öppna programmets huvudfönster > **Inställningar** > **Nätverksskydd** > **Lös tillfälligt blockerade IP-adresser**. Tillfälligt blockerade IP-adresser är blockerade i 1 timme.

Kolumner

IP-adress – visar en IP-adress som har blockerats.

Orsak till blockering – visar den attacktyp som adressen har skyddats från (till exempel TCP-portgenomsökningsattack).

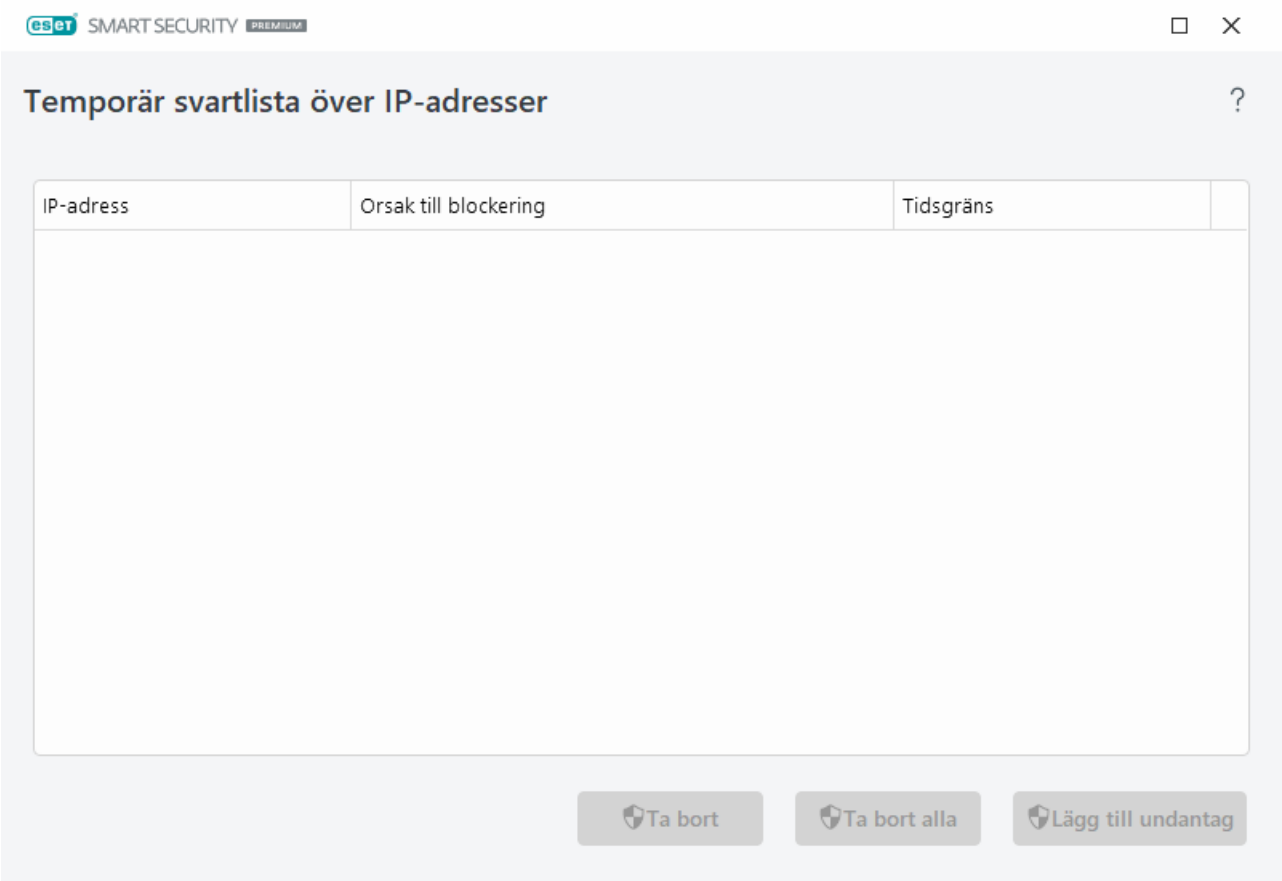
Timeout – visar tidpunkt och datum när adressen upphör att vara svartlistad.

Kontrollelement

Ta bort – klicka för att ta bort en adress från svartlistan innan tiden löper ut.

Ta bort alla – klicka för att ta bort alla adresser från svartlistan omedelbart.

Lägg till undantag – klicka för att lägga till ett brandväggsundantag i IDS-filtreringen.



Nätverksskyddsloggar

ESET Smart Security Premium Nätverksskydd sparar alla viktiga händelser i en loggfil. Om du vill visa loggfilen ska du öppna programmets huvudfönster > **Inställningar** > **Nätverksskydd** > **Visa loggar**.

Loggfilerna går att använda till att identifiera fel och avslöja intrång i systemet. Nätverksskyddsloggarna innehåller följande data:

- Datum och tid för händelsen
- Händelsens namn
- Källa
- Måladress på nätverket
- Kommunikationsprotokoll för nätverket
- Använd regel eller namnet på masken, om en sådan identifierats
- Programsökväg och namn
- Hash
- Användare
- Programmets signerare (utgivare)
- Paketnamn
- Tjänstens namn

En grundlig analys av dessa data kan hjälpa till att upptäcka försök att äventyra systemets säkerhet. Flera andra faktorer kan indikera potentiella säkerhetsrisker och hjälper dig att minska riskerna: regelbundna anslutningar från okända platser, upprepade försök att upprätta anslutningar, kommunikation från okända program eller användning av ovanliga portnummer.

> **Exploatering av säkerhetssårbarhet**
> Meddelandet om utnyttjande av säkerhetssårbarhet loggas även om den aktuella sårbarheten redan har patchats sedan försöket till utnyttjande detekterats och blockerats på nätverksnivå innan det faktiska utnyttjandet kunde ske.

Lösa problem med Brandvägg

Om det uppstår anslutningsproblem med ESET Smart Security Premium installerat finns det flera metoder för att fastställa om det är Brandvägg som orsakar problemet. Brandvägg kan dessutom hjälpa dig att skapa nya regler eller undantag för att lösa anslutningsproblem.

Se följande ämnen för hjälp med att lösa problem med Brandvägg:

- Felsökning av nätverksåtkomst

- Logga och skapa regler eller undantag från logg
- Skapa undantag från brandväggsmeddelanden
- Avancerad loggning för nätverksskydd
- Lösa problem med nätverkstrafikskannern

Logga och skapa regler eller undantag från logg

Som standard loggas inte alla blockerade anslutningar av ESET Brandvägg. Om du vill se vad som har blockerats av Nätverksskydd ska du öppna Avancerade inställningar > **Verktyg** > **Diagnostik** > **Avancerad loggning** och aktivera **Aktivera avancerad loggning för Nätverksskydd**. Om du ser något i loggen som du inte vill att brandväggen ska blockera kan du skapa en regel eller ett IDS-regel för detta genom att högerklicka på objektet och välja **Blockera inte liknande händelser i framtiden**. Observera att loggen över alla blockerade anslutningar kan innehålla tusentals objekt och att det kan vara svårt att hitta en specifik anslutning i den. När problemet lösts kan du stänga av loggningen.

För mer information om loggen, se Loggfiler.

> Använd loggning för att se i vilken ordning Nätverksskydd har blockerat specifika anslutningar. Genom att skapa regler från loggen kan du dessutom skapa regler som gör exakt det du vill.

Skapa regel från logg

I den nya versionen av ESET Smart Security Premium kan du skapa en regel från loggen. På huvudmenyn klickar du på **Verktyg** > **Loggfiler**. Välj **Nätverksskydd** i listrutan, högerklicka på önskad loggpost och välj **Blockera inte liknande händelser i framtiden** på kontextmenyn. Den nya regeln visas i ett meddelandefönster.

För att det ska gå att skapa nya regler från loggen måste ESET Smart Security Premium ha följande inställningar:

1. Ställ in det minimala omfånget för loggning till **Diagnostik** i Avancerade inställningar > **Verktyg** > **Loggfiler**.
2. Aktivera **Meddela om inkommande attacker mot säkerhetshål** i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Skydd mot nätverksangrepp (IDS)** > **Avancerade alternativ** > **Intrångsdetektering**.

Skapa undantag från brandväggsmeddelanden

När ESET-brandväggen identifierar skadlig nätverksaktivitet visas ett meddelandefönster där händelsen beskrivs. Meddelandet innehåller en länk så att du kan lära dig mer om händelsen och skapa en regel för den om du vill.

> Om ett nätverksprogram eller -enhet inte implementerar nätverksstandarder korrekt kan upprepade brandväggs-IDS-meddelanden utlösas. Du kan skapa ett undantag direkt från meddelandet om du inte vill att ESET-brandväggen ska identifiera programmet eller enheten.

Avancerad loggning för nätverksskydd

Med den här funktionen kan du förse ESET:s tekniska support med mer komplexa loggfiler. Funktionen ska endast användas på begäran av ESET:s tekniska support eftersom loggfilen som skapas kan bli mycket stor och göra datorn långsammare.

1. Öppna Avancerade inställningar > **Verktyg** > **Diagnostik** > **Avancerad loggning** och **Aktivera avancerad loggning för Nätverksskydd**.

2. Försök att återskapa det aktuella problemet.

3. Inaktivera avancerad loggning för nätverksskydd.

4. PCAP-loggfilen som skapas av nätverksskyddets avancerade loggning finns i samma katalog som diagnostiska minnesdumpar genereras i: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Lösa problem med nätverkstrafikskannern

Om det uppstår problem med webbläsaren eller e-postklienten är det första steget att fastställa om det beror på nätverkstrafikskannern. För att göra det här ska du prova att tillfälligt inaktivera Nätverkstrafiksskanner i Avancerade inställningar > **Detekteringsmotor** > **Nätverkstrafikskanner** (glöm inte att aktivera den igen när du är klar – annars förblir webbläsaren och e-postklienten oskyddade). Om problemet upphör när du stänger av det använder du dig av den här listan över vanliga problem och hur du löser dem:

Problem med uppdateringar eller säker kommunikation

Om programmet meddelar att det inte går att uppdatera eller att en kommunikationskanal inte är säker:

- Om SSL/TLS är aktiverat ska du prova att stänga av det tillfälligt. Om det hjälper kan du fortsätta använda SSL/TLS och få uppdateringen att fungera genom att undanta den problematiska kommunikationen: Inaktivera SSL/TLS. Kör uppdateringen igen. En dialogruta om krypterad nätverkstrafik ska visas. Kontrollera att programmet matchar det du felsöker och att certifikatet verkar komma från den server uppdateringen kommer från. Välj sedan att komma ihåg åtgärden för certifikatet och klicka på Ignorera. Om inga flera relevanta dialogrutor visas kan du ändra tillbaka till automatiskt filtreringsläge, och problemet bör vara löst.

- Om det aktuella programmet inte är en webbläsare eller e-postklient kan du undanta den helt Webbåtkomstskydd (det är dock riskabelt att göra det här för webbläsare eller e-postklienter). Ett program vars kommunikation filtrerats tidigare ska redan finnas i den tillhandahållna listan när du lägger till undantaget, så det ska inte vara nödvändigt att lägga till det manuellt.

Problem med att komma åt en enhet i nätverket

Om du inte kan använda funktioner i en enhet i nätverket (det kan vara att öppna en webbsida i webbkameran eller spela upp video i en mediespelare) kan du prova att lägga till dess IPv4- eller IPv6-adresser i listan över undantagna adresser.

Problem med en viss webbplats

Du kan undanta specifika webbplatser från Webbåtkomstskydd med hjälp av URL-adresshantering. Om du exempelvis inte kan öppna https://www.gmail.com/intl/en/mail/help/about.html provar du att lägga till *gmail.com* i listan över undantagna adresser.

Felet ”Vissa program kapabla att importera rotcertifikatet körs fortfarande”

När du aktiverar SSL/TLS ser ESET Smart Security Premium till att installerade program litar på hur SSL filtereras genom att importera ett certifikat till deras certifikatarkiv. Vissa program kan kräva en omstart för att kunna importera ett certifikat. Exempelvis Firefox och Opera. Säkerställ att inget av dem körs (det bästa sättet att göra det på är att öppna Aktivitetshanteraren och kontrollera att det inte firefox.exe eller opera.exe finns på fliken Processer) och försök sedan igen.

Fel gällande en ej betrodd utfärdare eller ogiltig signatur

Detta beror oftast på att importen som beskrivs ovan misslyckats. Säkerställ först att inget av de nämnda programmen körs. Inaktivera sedan SSL/TLS och aktivera det igen. Så att importen görs om.

> Läs artikeln i kunskapsbasen för att lära dig hur man hanterar Nätverkstrafiksskanner i ESET Windows-hemprodukten.

Nätverkshot blockerat

Den här situationen kan uppstå exempelvis när ett program på datorn försöker överföra skadlig trafik till en annan enhet i nätverket, utnyttja ett säkerhetshål eller om ett försök till portskanning upptäcks i systemet.

Du hittar typen av hot och den relaterade enhetens IP-adress i meddelandet. Klicka på **Ändra hantering av detta hot** för att visa följande alternativ:

Fortsätt blockera – blockerar detekterade hot. Om du vill sluta ta emot meddelanden om denna typ av hot från den specifika fjärradressen ska du välja alternativknappen bredvid **Meddela inte** innan du klickar på **Fortsätt blockera**. Detta skapar en IDS-regel (Intrusion Detection Service) med följande konfiguration: **Blockera** – standard, **Meddela** – nej, **Logga** – nej.

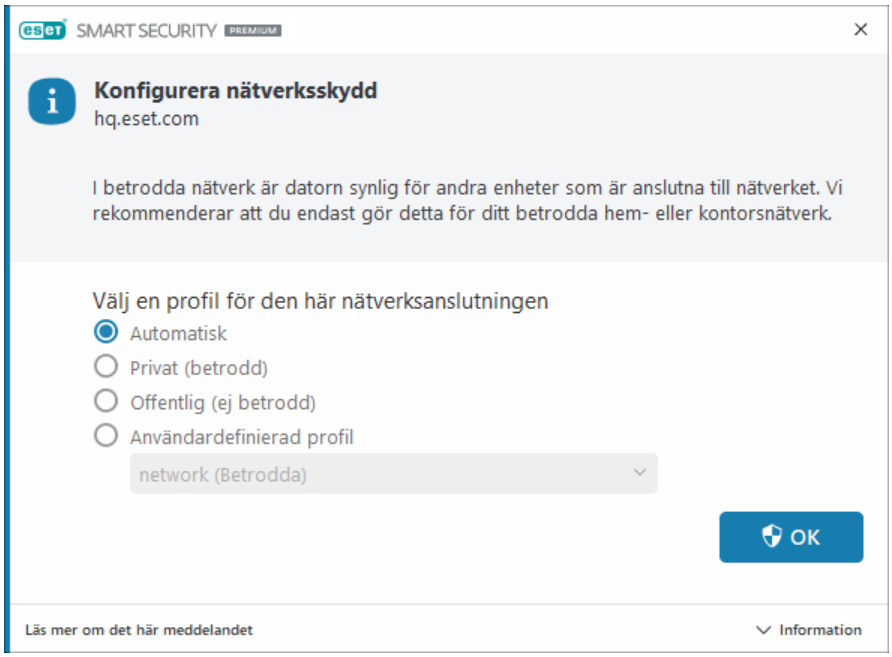
Tillåt – skapar en IDS-regel (Intrusion Detection Service) för att tillåta det detekterade hotet. Välj ett av följande alternativ innan du klickar på **Tillåt** för att ange regelinställningarna:

- **Meddela endast när hotet blockeras** – regelkonfiguration: **Blockera** – nej, **Meddela** – nej, **Logga** – nej.
- **Meddela när detta hot uppstår** – regelkonfiguration: **Blockera** – nej, **Meddela** – standard, **Logga** – standard.
- **Meddela inte** – regelkonfiguration: **Blockera** – nej, **Meddela** – nej, **Logga** – nej.

Vilken information som visas i meddelandefönstret kan variera beroende på typen av detekterat hot. Mer information om hot och andra relaterade begrepp finns i Typer av fjärrangrepp eller Typer av detekteringar.
Information om hur du löser **duplicerade IP-adresser i nätverket** finns i vår artikel i ESET:s kunskapsbas.

Ett nytt nätverk har identifierats

Som standard använder ESET Smart Security Premium Windows-inställningar när en ny nätverksanslutning identifieras. Om du vill visa en dialogruta när ett nytt nätverk identifieras ska du ändra Tilldelning av nätverksskyddsprofil till **Fråga**. Konfiguration av nätverksskydd visas varje gång datorn ansluter till ett nytt nätverk.



Du kan välja bland följande nätverksanslutningsprofiler:

Automatiskt – ESET Smart Security Premium väljer profilen automatiskt baserat på de aktivatorer som har konfigurerats för varje profil.

Privat – för betrodda nätverk (hem- eller kontorsnätverk). Datorn och delade filer som lagras på datorn är synliga för andra nätverksanvändare och systemresurserna är tillgängliga för andra användare i nätverket (åtkomst till delade filer och skrivare är aktiverad, inkommande RPC-kommunikation är aktiverad och fjärrdelning av skrivbord är aktiverad). Vi rekommenderar att du använder den här inställningen när du kommer åt ett säkert lokalt nätverk. Den här profilen tilldelas automatiskt till en nätverksanslutning om den är konfigurerad som ett Domän- eller Privat-närverk i Windows.

Offentligt – för ej betrodda nätverk (offentligt nätverk). Filer och mappar i systemet delas inte med eller är synliga för andra användare i nätverket och delning av systemresurser är inaktiverad. Vi rekommenderar att du använder den här inställningen vid åtkomst till trådlösa nätverk. Den här profilen tilldelas automatiskt till alla nätverksanslutningar som inte är konfigurerade som ett Domän- eller Privat-nätverk i Windows.

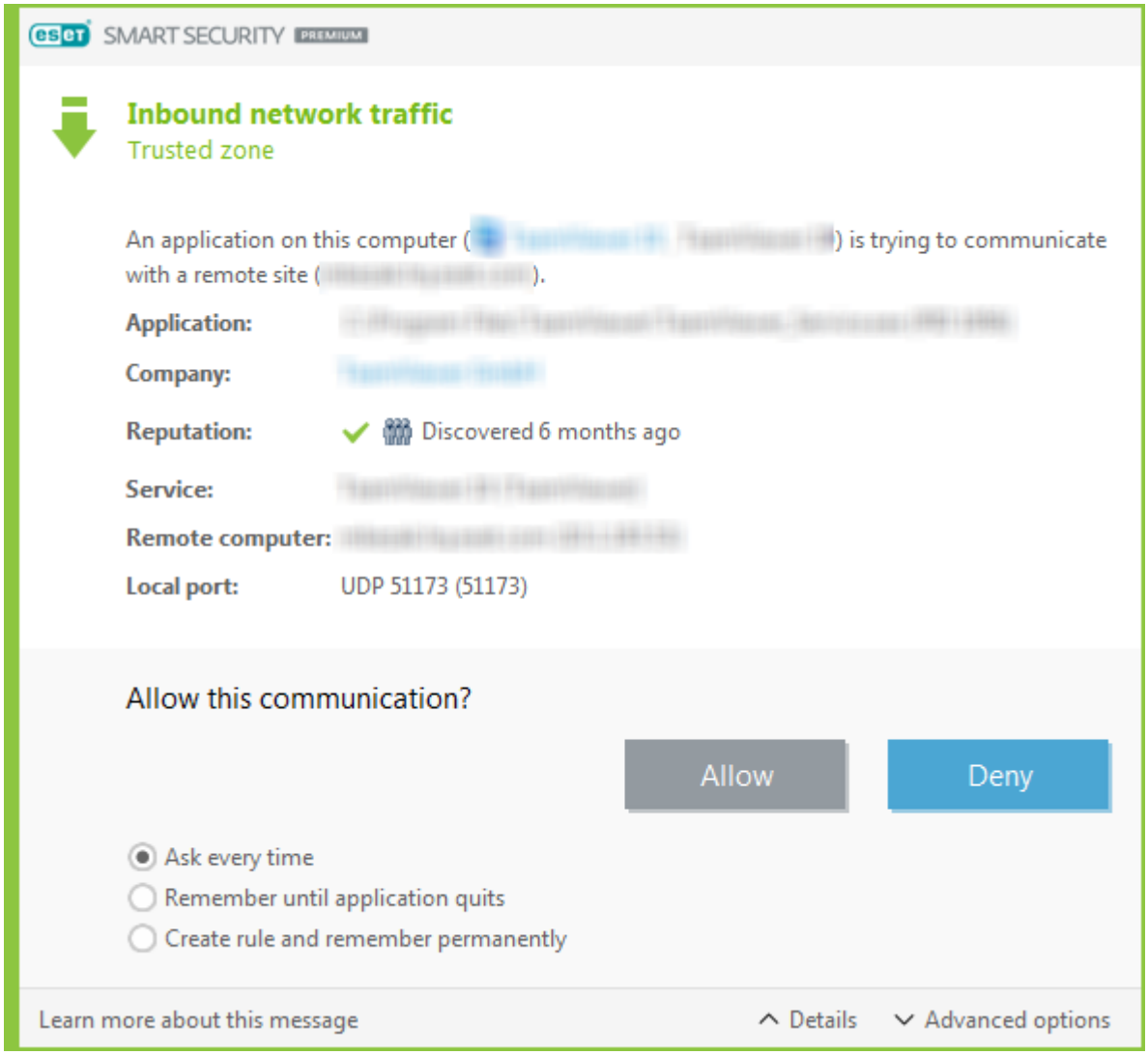
Användardefinierad profil – du kan välja en av profilerna du har skapat i listrutan. Det här alternativet är bara tillgängligt om du har skapat minst en anpassad profil.

En felaktig nätverkskonfiguration kan innebära en säkerhetsrisk för datorn.

Etablera en anslutning – identifiering

Brandväggen identifierar varje ny nätverksanslutning. Det aktuella brandväggsläget avgör vilka åtgärder som ska utföras för den nya regeln. Om **Automatiskt läge** eller **Policybaserat läge** aktiverats utför brandväggen fördefinierade åtgärder utan användarinteraktion.

I det **interaktiva läget** visas ett informationsfönster där identifiering av nya nätverksanslutningar rapporteras tillsammans med detaljerad information om anslutningen. Du kan välja att **tillåta** eller **neka** (blockera) anslutningen. Om samma anslutning tillåts upprepade gånger i den här dialogrutan, rekommenderar vi att du skapar en ny regel för anslutningen. Genom att välja **Skapa regel och kom ihåg permanent** och spara åtgärden som en ny regel för brandväggen. Om samma anslutning identifieras av brandväggen i framtiden, kommer den nya regeln att användas utan användaråtgärder.



När du skapar nya regler ska du endast tillåta anslutningar som du vet är säkra. Om alla anslutningar är tillåtna fungerar inte brandväggen som avsett. Följande viktiga parametrar finns tillgängliga för anslutningar:

Program – plats för körbar fil och process-ID. Tillåt inte anslutningar för okända program och processer.

Signerare – programmets utgivarnamn. Klicka på texten för att visa ett säkerhetscertifikat för företaget.

Rykte – risknivå för anslutningen. Anslutningar tilldelas en risknivå: Okej (grön), Okänd (orange) eller Riskfylld (röd), genom att använda en serie heuristiska regler som undersöker egenskaperna för varje anslutning, antalet

användare och identifieringstiden. Denna information samlas in med ESET LiveGrid®-teknik.

Tjänst – tjänstens namn, om programmet är en Windows-tjänst.

Fjärrdator – fjärrenhetens adress. Tillåt endast anslutningar till betrodda och kända adresser.

Fjärrport – kommunikationsport. Kommunikation på vanliga porter (t.ex. webbtrafik – port 80.443) kan tillåtas under normala omständigheter.

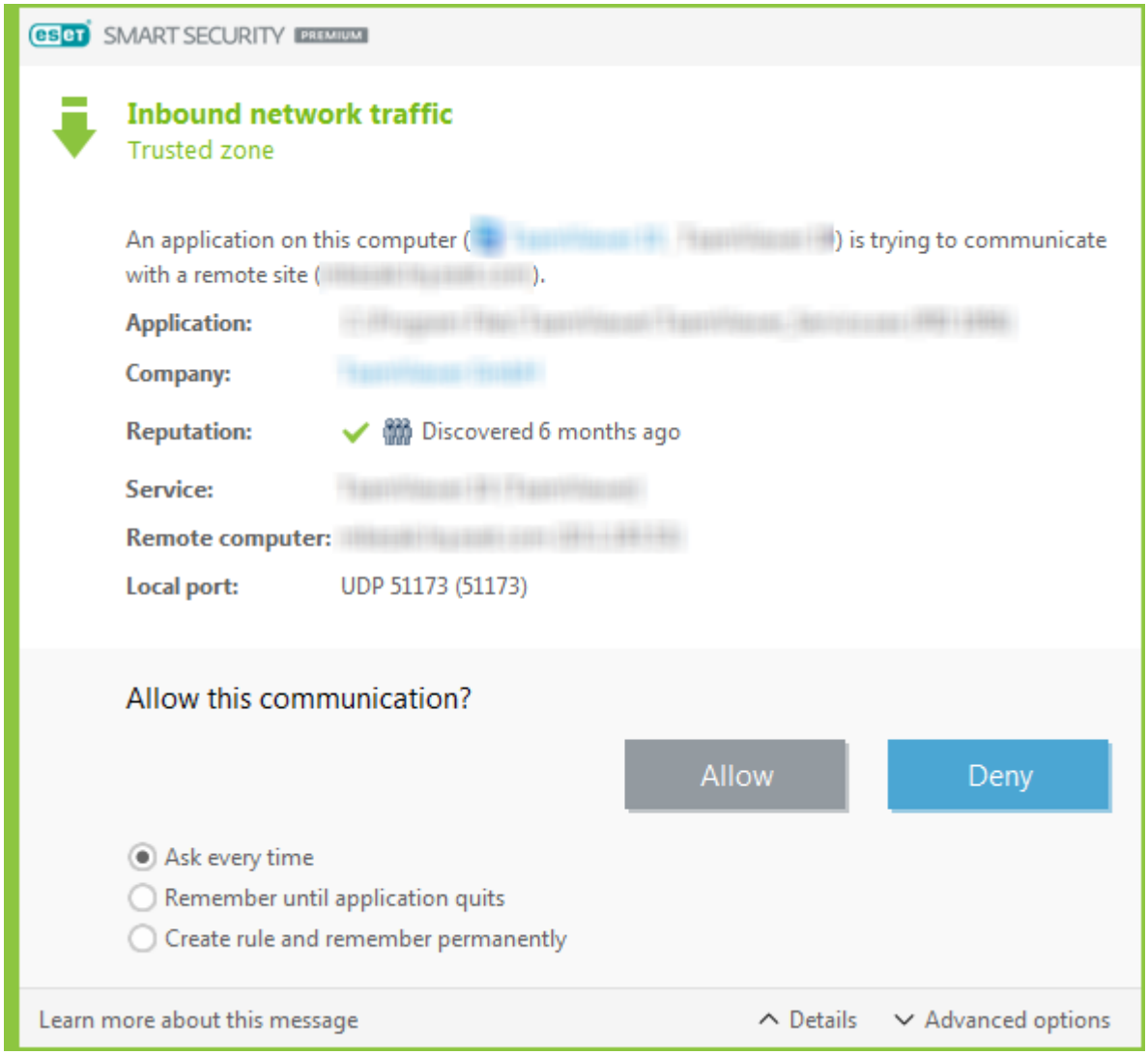
Datorinfiltreringar använder ofta Internet och dolda anslutningar för att infektera fjärrsystem. Är reglerna korrekt konfigurerade blir brandväggen ett användbart verktyg mot attacker med olika typer av skadlig kod.

Programändring

Brandväggen har identifierat en ändring i ett program som används till att etablera utgående anslutningar från datorn. Det är möjligt att programmet helt enkelt har uppdaterats till en ny version. Å andra sidan kan en ändring ha utförts av ett skadligt program. Om du inte är medveten om någon legitim ändring rekommenderas det att du nekar anslutningen och genomsöker datorn med den senaste virussignaturdatabasen.

Inkommande tillförlitlig kommunikation

Exempel på en inkommande anslutning inom den betrodda zonen:
En fjärrdator inom Tillförlitliga platser försöker upprätta kommunikation med ett lokalt program som körs på din dator.



Program – program som kontaktas av en fjärrenhet.

Programsökväg – programmets plats.

Microsoft Store-program – namnet på programmet i Microsoft Store.

Signerare – programmets utgivarnamn. Klicka på texten för att visa ett säkerhetscertifikat för företaget.

Rykte – programmets rykte som inhämtats med ESET LiveGrid®-teknik.

Tjänst – namnet på tjänsten som för tillfället körs på datorn.

Fjärrdator – fjärrdatorn försöker upprätta kommunikation med programmet i din dator.

Fjärrport – port som används för kommunikationen.

Fråga varje gång – om standardåtgärden för en regel ställs in till **Fråga** visas en dialogruta varje gång regeln utlöses.

Kom ihåg tills programmet stängs – ESET Smart Security Premium kommer ihåg den valda åtgärden till nästa omstart.

Skapa regel och kom ihåg permanent – om du väljer det här alternativet innan du tillåter eller nekar en

kommunikation kommer ESET Smart Security Premium att komma ihåg åtgärden och använda den om programmet kontaktas av fjärrdatorn igen.

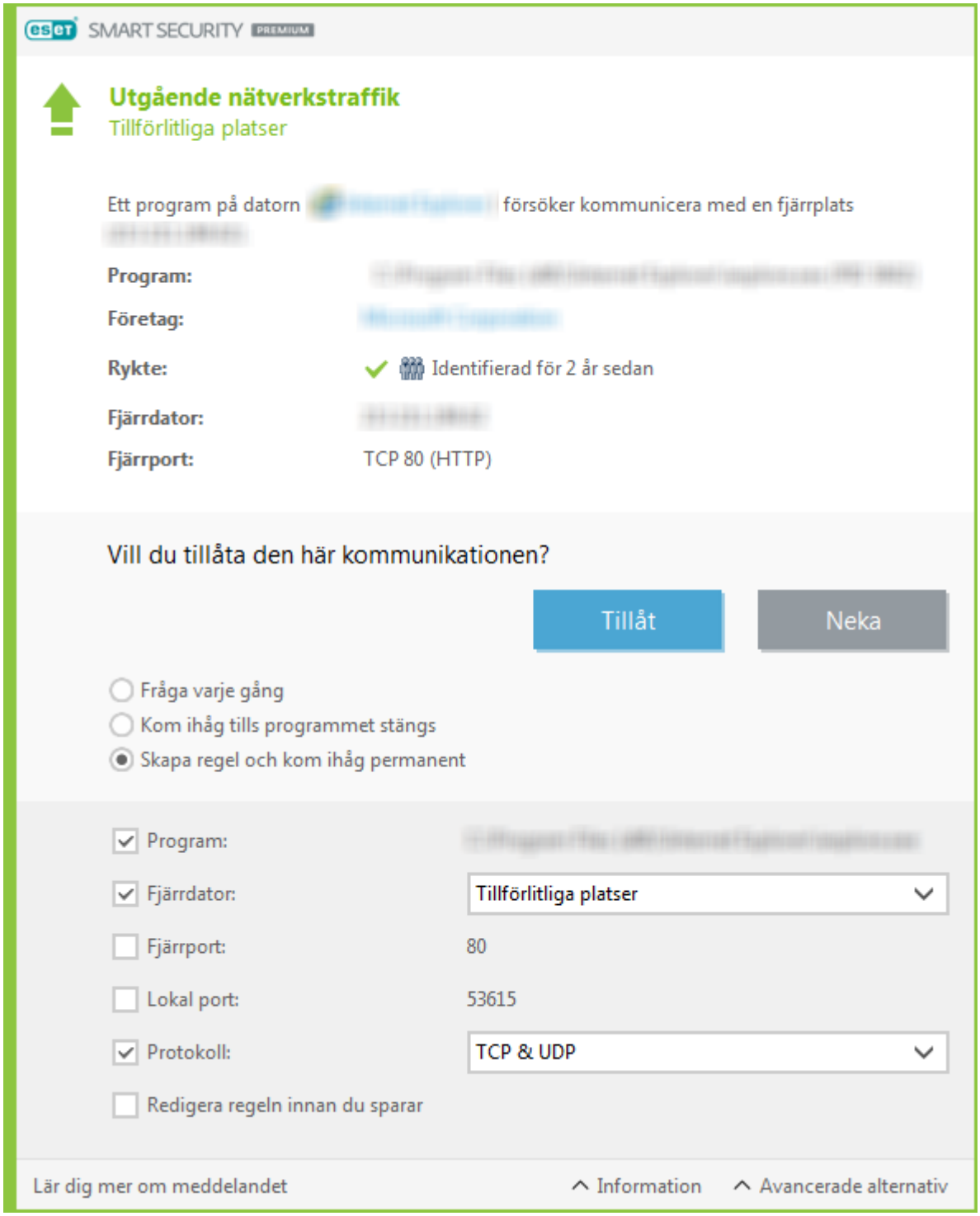
Tillåt – tillåter den inkommande kommunikationen.

Neka – avvisar den inkommande kommunikationen.

Redigera regel – gör att du kan anpassa regelegenskaper med Redigerare för brandväggsregler.

Utgående tillförlitlig kommunikation

Exempel på en utgående anslutning inom den betrodda zonen:
Ett lokalt program försöker upprätta en anslutning med en annan dator inom det lokala nätverket, eller inom nätverken i Tillförlitliga platser.



Program – program som kontaktas av en fjärrenhet.

Programsökväg – programmets plats.

Microsoft Store-program – namnet på programmet i Microsoft Store.

Signerare – programmets utgivarnamn. Klicka på texten för att visa ett säkerhetscertifikat för företaget.

Rykte – programmets rykte som inhämtats med ESET LiveGrid®-teknik.

Tjänst – namnet på tjänsten som för tillfället körs på datorn.

Fjärrdator – fjärrdatorn försöker upprätta kommunikation med programmet i din dator.

Fjärrport – port som används för kommunikationen.

Fråga varje gång – om standardåtgärden för en regel ställs in till **Fråga** visas en dialogruta varje gång regeln utlöses.

Kom ihåg tills programmet stängs – ESET Smart Security Premium kommer ihåg den valda åtgärden till nästa omstart.

Skapa regel och kom ihåg permanent – om du väljer det här alternativet innan du tillåter eller nekar en kommunikation kommer ESET Smart Security Premium att komma ihåg åtgärden och använda den om programmet kontaktas av fjärrdatorn igen.

Tillåt – tillåter den inkommande kommunikationen.

Neka – avvisar den inkommande kommunikationen.

Redigera regel – gör att du kan anpassa regelegenskaper med Redigerare för brandväggsregler.

Inkommande kommunikation

Exempel på en inkommande Internetanslutning:
En fjärrdator försöker kommunicera med ett program som körs på datorn.

Program – program som kontaktas av en fjärrenhet.

Programsökväg – programmets plats.

Microsoft Store-program – namnet på programmet i Microsoft Store.

Signerare – programmets utgivarnamn. Klicka på texten för att visa ett säkerhetscertifikat för företaget.

Rykte – programmets rykte som inhämtats med ESET LiveGrid®-teknik.

Tjänst – namnet på tjänsten som för tillfället körs på datorn.

Fjärrdator – fjärrdatorn försöker upprätta kommunikation med programmet i din dator.

Fjärrport – port som används för kommunikationen.

Fråga varje gång – om standardåtgärden för en regel ställs in till **Fråga** visas en dialogruta varje gång regeln utlöses.

Kom ihåg tills programmet stängs – ESET Smart Security Premium kommer ihåg den valda åtgärden till nästa omstart.

Skapa regel och kom ihåg permanent – om du väljer det här alternativet innan du tillåter eller nekar en kommunikation kommer ESET Smart Security Premium att komma ihåg åtgärden och använda den om programmet kontaktas av fjärrdatorn igen.

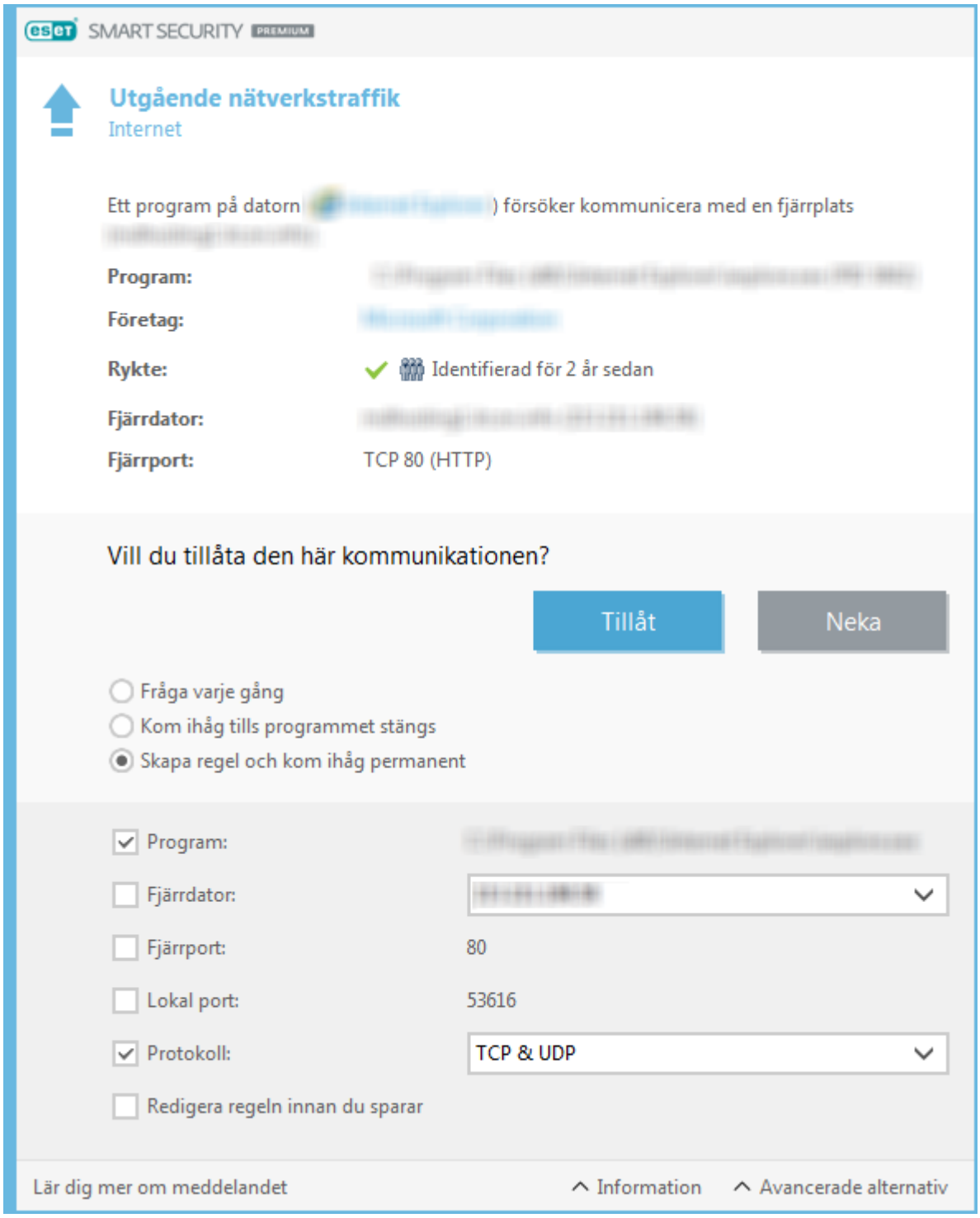
Tillåt – tillåter den inkommande kommunikationen.

Neka – avvisar den inkommande kommunikationen.

Redigera regel – gör att du kan anpassa regelegenskaper med Redigerare för brandväggsregler.

Utgående kommunikation

Exempel på en utgående Internetanslutning:
Ett lokalt program försöker upprätta en Internetanslutning.



Program – program som kontaktas av en fjärrenhet.

Programsökväg – programmets plats.

Microsoft Store-program – namnet på programmet i Microsoft Store.

Signerare – programmets utgivarnamn. Klicka på texten för att visa ett säkerhetscertifikat för företaget.

Rykte – programmets rykte som inhämtats med ESET LiveGrid®-teknik.

Tjänst – namnet på tjänsten som för tillfället körs på datorn.

Fjärrdator – fjärrdatorn försöker upprätta kommunikation med programmet i din dator.

Fjärrport – port som används för kommunikationen.

Fråga varje gång – om standardåtgärden för en regel ställs in till **Fråga** visas en dialogruta varje gång regeln utlöses.

Kom ihåg tills programmet stängs – ESET Smart Security Premium kommer ihåg den valda åtgärden till nästa omstart.

Skapa regel och kom ihåg permanent – om du väljer det här alternativet innan du tillåter eller nekar en kommunikation kommer ESET Smart Security Premium att komma ihåg åtgärden och använda den om programmet kontaktas av fjärrdatorn igen.

Tillåt – tillåter den inkommande kommunikationen.

Neka – avvisar den inkommande kommunikationen.

Redigera regel – gör att du kan anpassa regelegenskaper med Redigerare för brandväggsregler.

Inställning av anslutningsvy

Högerklicka på en anslutning för att se ytterligare alternativ som innefattar:

Matcha värdnamn – om möjligt visas alla nätverksadresser i DNS-format, inte i IP-adressformat med siffror.

Visa endast TCP-anslutningar – listan visar endast anslutningar som tillhör protokollsviten TCP.

Visa anslutningar som lyssnar – markera det här alternativet för att enbart visa anslutningar där ingen kommunikation har upprättats men där systemet har öppnat en port och inväntar anslutning.

Visa anslutningar inom datorn – markera det här alternativet om du endast vill visa anslutningar där fjärrsidan är ett lokalt system, så kallade localhost-anslutningar.

Uppdateringshastighet – välj frekvensen för uppdatering av de aktiva anslutningarna.

Uppdatera nu – uppdaterar fönstret **Nätverksanslutningar**.

Säkerhetsverktyg

Öppna programmets huvudfönster > **Inställningar** > **Säkerhetsverktyg** för att justera följande moduler:

Säkra banktjänster och surfning – Ger dig ett extra lager av webbläsarskydd som är gjort för att skydda dina finansiella data vid onlinetransaktioner. Aktivera **Skydda alla webbläsare** i avancerade inställningar för Säkra banktjänster och surfning för att starta alla webbläsare som stöds i ett säkert läge.

Webbläsarsekretess och säkerhet – Håller din onlineaktivitet privat och säker utan att lämna ett digitalt fotavtryck.

Anti-Theft – aktivera Stöldskydd för att skydda din dator i händelse av förlust eller stöld.

Secure Data – med Secure Data aktiverat kan du kryptera din data för att förhindra missbruk av privat, konfidentiell information.

Password Manager – Password Manager skyddar och lagrar dina lösenord och personuppgifter.

Säkra banktjänster och surfning

Säkra banktjänster och surfning är ett ytterligare skyddslager utformat för att skydda dina finansiella data under onlinetransaktioner.

Som standard startar alla webbläsare som stöds i ett säkert läge. Detta gör att du kan surfa på internet, komma åt internetbank och göra köp och transaktioner online i en säkrad webbläsare automatiskt.

ESET LiveGrid®-ryktessystemet måste vara aktiverat (aktiverat som standard) för att säkerställa att Säkra banktjänster och surfning fungerar korrekt.

Information om hur du konfigurerar hur säkrad webbläsare ska agera finns i Avancerade inställningar för Säkra banktjänster och surfning. Om du inaktiverar **Skydda alla webbläsare** kan du komma åt den säkrade webbläsaren i programmets huvudfönster > **Översikt** > **Säkra banktjänster och surfning** eller genom att klicka på skrivbordsikonen för **Säkra banktjänster och surfning**. Den webbläsare som är installerad som standard i Windows startas i säkert läge.

För att kunna surfa säkert måste kommunikationen vara HTTPS-krypterad. Följande webbläsare har stöd för Säkra banktjänster och surfning:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Endast Firefox och Microsoft Edge stöds på enheter med ARM-processorer.

Mer information om Säkra banktjänster och surfning finns i följande artiklar i ESET:s kunskapsbas (som finns på engelska och flera andra språk):

- Hur använder jag ESET Säkra banktjänster och surfning?
- Pausa eller inaktivera Säkra banktjänster och surfning i Windows-hemprodukter från ESET
- ESET Säkra banktjänster och surfning – vanliga fel
- ESET-ordlista | Säkra banktjänster och surfning

Meddelande i webbläsaren

Säkrad webbläsare informerar om dess aktuella status genom meddelanden i webbläsaren och färgen på webbläsarramen.

Meddelanden i webbläsaren visas på fliken till höger.

Om du vill expandera meddelandet i webbläsaren klickar du på ESET-ikonen . Om du vill minimera meddelandet klickar du på meddelandetexten. Om du vill stänga meddelandet och den gröna webbläsarramen ska du klicka du på stängningsikonen .

Endast det informativa meddelandet och den gröna webbläsarramen kan avvisas.

Meddelanden i webbläsaren

Meddelandetyp	Status
Informativt meddelande och grön webbläsarram	Maximalt skydd garanteras och meddelandet i webbläsaren minimeras som standard. Expandera meddelandet i webbläsaren och klicka på **Inställningar** för att öppna inställningarna för säkerhetsverktyg.
Varning och orange webbläsarram	Säkrad webbläsare kräver din uppmärksamhet för ett icke-kritiskt problem. Mer information om problemet eller en lösning finns i anvisningarna i meddelandet i webbläsaren.
Säkerhetsvarning och röd webbläsarram	Webbläsaren skyddas inte av ESET Säkra banktjänster och surfning. Starta om webbläsaren för att säkerställa att skyddet är aktivt. Om du vill lösa en konflikt med filer som läses in i webbläsaren öppnar du Loggfiler > **Säkra banktjänster och surfning** och ser till att de loggade filerna inte läses in nästa gång du startar webbläsaren. Om problemet kvarstår kontaktar du ESET:s tekniska support genom att följa anvisningarna i vår artikel i kunskapsbasen.

Webbläsarsekretess och säkerhet

Du kan aktivera funktionen Webbläsarsekretess och säkerhet via ett anpassat tillägg som är tillgängligt i webbläsare som stöds (endast Google Chrome, Mozilla Firefox och Microsoft Edge).

Så här installerar och aktiverar du tillägget:

1. Se till att du använder den senaste ESET Smart Security Premium-versionen och startar om datorn efter uppdateringen.
2. Öppna din webbläsare.
3. Tillägget installeras i din webbläsare.
4. Aktivera tillägget så visas webbläsaren med tilläggets informationssida.

Huvudmenyn för webbläsartillägget Webbläsarsekretess och säkerhet är uppdelad i följande avsnitt:

Översikt

Säker sökning

Klicka på växlingsikonen  bredvid **Genomsök sökresultat** för att aktivera funktionen och se vilka resultat som är säkra att klicka på. Säker sökning utvärderar listade länkadresser och betyder inte nödvändigtvis att webbplatsen inte innehåller skadlig kod. Vår detekteringsmotor upptäcker sedan eventuell skadlig kod på webbplatsen.

Webbläsarrensning

Ta bort din webbläsningsdata eller ställ in regelbunden rensning. Du kan lägga till webbplatser som du vill godkänna cookies ifrån och förbli inloggad på även efter webbläsarrensning genom att **lägga till dem i en lista**.

- **Engångsrensning** – Välj tidsintervall på den nedrullningsbara menyn och den datatyp som du vill ta bort. Du kan välja mellan alternativen alla data, privata och anpassade val.

- **Regelbunden rensning** – Klicka på växlingsikonen  bredvid **Regelbunden rensning** för att aktivera funktionen. Välj tidsintervall i den nedrullningsbara menyn och den datatyp som du vill ta bort regelbundet. Du kan välja mellan alternativen alla data, privata och anpassade val.

Alternativet **Anpassade data** omfattar följande kategorier:

- Webbläsarhistorik
- Ladda ner historik
- Cookies och webbplatsdata
- Cachelagrade bilder och filer
- Lösenord och inloggningsdata
- Autofylldata för formulär

Metadatarensning

Funktionen Metadatarensning styr sekretessdata som kan exponeras genom EXIF-metadata som delas i mediefiler, dokument och andra filformat som stöds. Klicka på växlingsikonen  bredvid **Rensa metadata varje gång du laddar upp en bild** för att göra det möjligt att ta bort metadata.

Du måste starta om webbläsaren för att säkerställa att **Metadatarensning** fungerar korrekt.

Klicka på växlingsikonen  bredvid **Få meddelanden i webbläsaren** för att aktivera visning av meddelanden efter metadatarensning.

Granskning av webbplatsinställningar

Få åtkomst till och hantera webbplatsbehörigheter för att kontrollera vilken information webbplatser får använda.

- **Meddelanden** – se över vilka webbplatser du vill **Tillåta/Blockera** meddelanden från eller om du vill att webbläsartillägget ska **Fråga dig varje gång**.

Avancerade inställningar

Webbläsarrensning

Avancerade cookieinställningar

Lista över webbplatser som du vill godkänna cookies ifrån och förbli inloggad på även efter webbläsarrensning. Ange webbadressen i textfältet och klicka på **Lägg till**. Du kan när som helst ta bort den från listan genom att klicka på minusikonen bredvid den specifika webbplatsen.

Längst ner på sidan finns en lista över föreslagna domäner som för närvarande är öppna i webbläsaren. Om du inte kan se den specifika webbplatsen klickar du på **uppdatera listan** och lägger till webbplatsen i listan över godkända cookies genom att klicka på plusikonen .

Granskning av webbplatsinställningar

Få åtkomst till och hantera webbplatsbehörigheter för att kontrollera vilken information webbplatser får använda.

- **Meddelanden** – se över vilka webbplatser du vill **Tillåta/Blockera** meddelanden från eller om du vill att webbläsartillägget ska **Fråga dig varje gång**.

Utseende

Anpassa gränssnittets färgschema så att det passar dina preferenser. Välj önskat färgschema genom att markera kryssrutan **Ljus** eller **Mörk**.

Stöldskydd

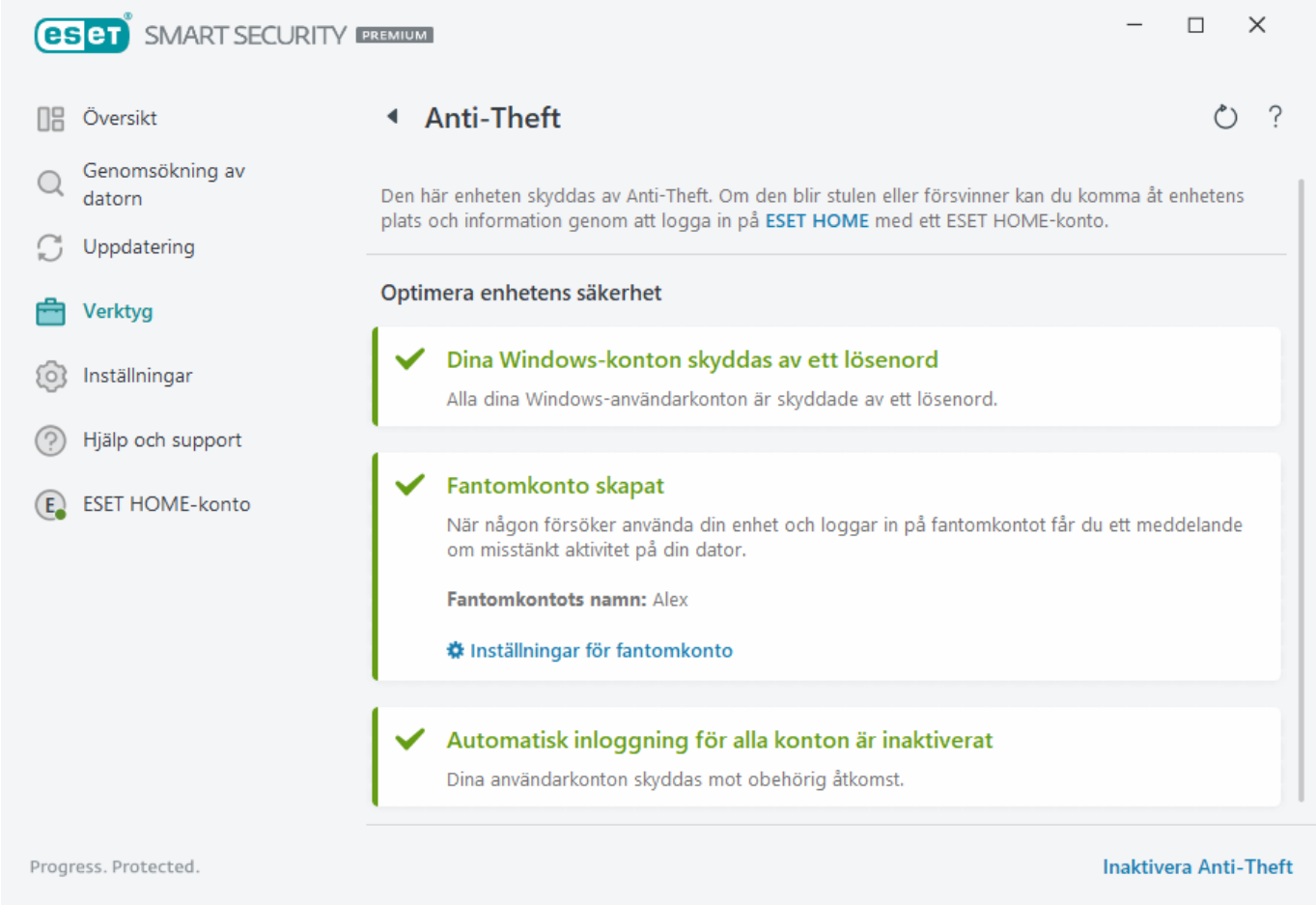
Under våra dagliga resor mellan hem och arbete eller andra offentliga platser riskerar vi ständigt att tappa bort eller bli bestulna på våra personliga enheter. Stöldskydd är en funktion som utökar användarens säkerhet i händelse av förlorad eller stulen enhet. Med Stöldskydd kan du spåra den saknade enheten och övervaka dess användning genom att söka upp IP-adressen i ESET HOME för att få tillbaka enheten och skydda din personliga data.

Genom att använda moderna tekniker som geografisk IP-adressuppsökning, lagring av webbkamerabild, skydd av användarkonto och enhetsövervakning kan Stöldskydd hjälpa dig och polisen att lokalisera datorn eller enheten om den försvinner eller stjäls. I ESET HOME kan du se vilken aktivitet som äger rum på din dator eller enhet.

Mer information om Stöldskydd i ESET HOME hittar du i ESET HOME-onlinehjälpen.

Stöldskydd kanske inte fungerar korrekt på datorer i domäner på grund av begränsningar i hanteringen av användarkonton.

När du har aktiverat Stöldskydd kan du optimera enhetens säkerhet i huvudprogramfönstret > **Inställningar** > **säkerhetsverktyg** > **Stöldskydd**.



Alternativ för optimering

Inget fantomkonto skapat

Att skapa ett fantomkonto ökar chansen att hitta en förlorad eller stulen enhet. Om du markerar din enhet som saknad blockerar Stöldskydd åtkomsten till dina aktiva användarkonton för att skydda din känsliga data. Alla som försöker använda enheten får endast använda fantomkontot. Ett fantomkonto är en form av gästkonto med begränsad behörighet. Det kommer att användas som standardsystemkonto tills enheten är markerad som återfunnen, vilket hindrar någon från att logga in på andra användarkonton eller komma åt användarens data.

Varje gång någon loggar in på fantomkontot när datorn är i normalt tillstånd får du ett meddelande med information om misstänkt aktivitet på datorn. När du har fått e-postmeddelandet kan du bestämma om du vill markera datorn som saknad.

Om du vill skapa ett fantomkonto klickar du på **Skapa ett fantomkonto**, skriver **fantomkontonamnet** i textfältet och klickar på **Skapa**.

När du har skapat ett fantomkonto klickar du på **Inställningar för fantomkonto** om du vill byta namn på eller ta bort kontot.

Lösenordsskydd för Windows-konton

Ditt användarkonto är inte lösenordsskyddat. Du kommer att få denna optimeringsvarning om minst ett användarkonto inte är skyddat med ett lösenord. Att skapa ett lösenord för alla användare (utom **fantomkontot**) på datorn löser problemet.

Om du vill skapa ett lösenord för användarkontot klickar du på **Hantera Windows-konton** och ändrar lösenordet eller följer anvisningarna nedan:

1. Tryck på CTRL+Alt+Delete på tangentbordet.
2. Klicka på **Ändra ett lösenord**.
3. Lämna fältet **Gammalt lösenord** tomt.
4. Skriv lösenordet i fälten **Nytt lösenord** och **Bekräfta lösenord** och tryck på **Retur**.

Automatisk inloggning för Windows-konton

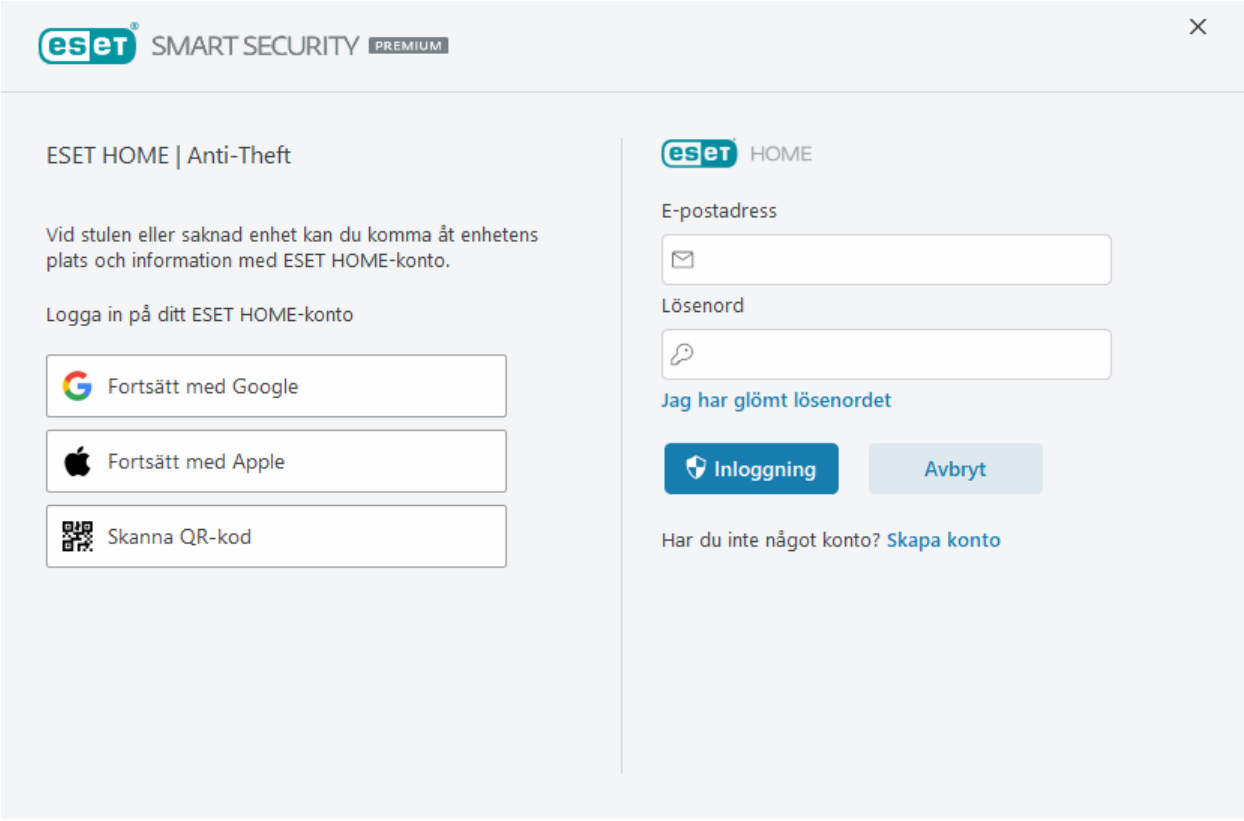
Ditt användarkonto har automatisk inloggning aktiverad. Det är därför inte skyddat mot obehörig åtkomst. Du får den här optimeringsvarningen om minst ett användarkonto har automatisk inloggning aktiverad. Klicka på **Inaktivera automatisk inloggning** för att lösa optimeringsproblemet.

Automatisk inloggning för fantomkontot

Automatisk inloggning är aktiverad för **fantomkontot** på din enhet. När enheten är i normalt tillstånd rekommenderar vi inte att du använder automatisk inloggning eftersom det kan orsaka problem med åtkomst till ditt riktiga användarkonto eller skicka falska larm om datorns tillstånd som saknad. Klicka på **Inaktivera automatisk inloggning** för att lösa optimeringsproblemet.

Logga in på ditt ESET HOME konto.

För att aktivera/inaktivera Stöldskydd och för att komma åt enhetens plats och information i ESET HOME loggar du in på ditt ESET HOME-konto.



Det finns flera metoder för att logga in på ditt ESET HOME-konto:

- **Använd din ESET HOME-e-postadress och ditt lösenord** – Skriv den **e-postadress** och det **lösenord** som du använde för att skapa ditt ESET HOME-konto och klicka på **Logga in**.

- **Använd ditt Google-konto/AppleID** – Klicka på **Fortsätt med Google** eller **Fortsätt med Apple** och logga in till lämpligt konto. Efter en lyckad inloggning omdirigeras du till ESET HOME-bekräftelsewebbsidan. Om du vill fortsätta växlar du tillbaka till ESET-produktfönstret. Mer information om Google-kontot/AppleID-inloggningen finns i instruktioner i ESET HOME-onlinehjälpen.

- **Skanna QR-kod** – Klicka på **Skanna QR-kod** för att visa QR-koden. Öppna din ESET HOME-mobilapp och skanna QR-koden eller peka enhetskameran mot QR-koden. Mer information finns i instruktionerna i ESET HOME-onlinehjälpen.

Inloggningen misslyckades – vanliga fel.

Om du inte har ett ESET HOME-konto klickar du på **Skapa konto** för att registrera dig eller läser anvisningarna i ESET HOME-onlinehjälpen.
Om du har glömt ditt lösenord klickar du på **Jag har glömt lösenordet** och följer stegen på skärmen eller läser anvisningarna i ESET HOME-onlinehjälpen.

Stöldskydd stöder inteMicrosoft Windows Home Server.

Ange ett enhetsnamn

Fältet **Enhetsnamn** representerar namnet på din dator (enhet) som visas som en identifierare i alla ESET HOME-tjänster. Datornamnet på din dator används som standard. Skriv enhetsnamnet eller använd standardnamnet och klicka på **Fortsätt**.

Stöldskydd aktiverat/inaktiverat

Det här fönstret innehåller ett bekräftelsemeddelande när du aktiverar/inaktiverar Stöldskydd:

- Aktiverat – enheten skyddas nu av Stöldskydd och du kan fjärrhantera dess säkerhet på ESET HOME-portalen med ditt konto.

- Inaktiverat – Stöldskydd är inaktiverat på enheten och all data relaterad till <%ESET_ANTTHEFT%> för enheten tas bort från ESET HOME-portalen.

Det gick inte att lägga till ny enhet

Du fick ett meddelande vid aktivering av Stöldskydd.

De vanligaste scenarierna är:

- Fel vid inloggning till ESET HOME

- Ingen Internetanslutning (eller så fungerar inte Internet för tillfället)

Om du inte kan lösa problemet kontaktar du ESET:s tekniska support.

Secure Data

Secure Data är en funktion i ESET Smart Security Premium som gör att du kan kryptera data på datorn och flyttbara enheter för att skydda din privata data och förhindra missbruk. Se FAQ för ESET Secure Data för mer information.

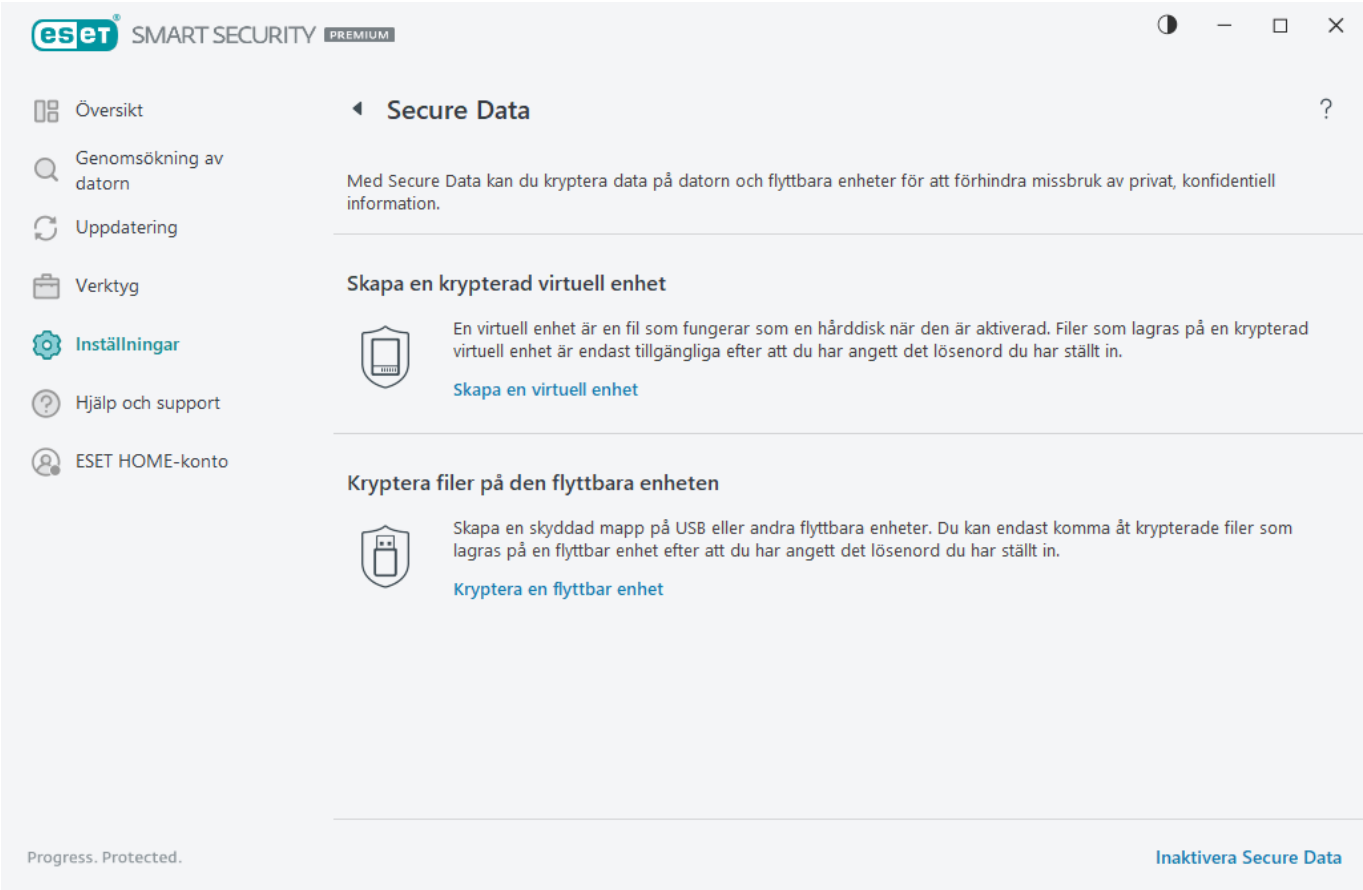
För att aktivera Secure Data väljer du något av följande alternativ:

- Klicka på **INSTÄLLNINGAR** bredvid **Secure Data** i programmets huvudfönster > **Översikt**.
- Aktivera växlingsknappen **Secure Data** i programmets huvudfönster > **Inställningar** > **Säkerhetsverktyg**.

> Det går inte att installera ESET Endpoint Encryption på samma dator som Secure Data redan är installerat på.

När Secure Data är aktiverat, i huvudprogramfönstret, klickar du på **Inställningar** > **Säkerhetsverktyg** > **Secure Data** och väljer ett av följande krypteringsalternativ:

- Skapa en krypterad virtuell enhet
- Kryptera filer på den flyttbara enheten



Skapa en krypterad virtuell enhet

Du kan använda Secure Data för att skapa krypterade virtuella enheter. Det finns ingen gräns för hur många enheter du kan skapa, så länge det finns hårddiskutrymme. Följ stegen nedan om du vill skapa en krypterad virtuell enhet:

1. I huvudprogramfönstret klickar du på **Inställningar** > **Säkerhetsverktyg** > **Secure Data** > **Skapa en virtuell enhet**.

2. Klicka på **Bläddra** för att välja den plats som den virtuella enheten ska sparas på.

3. Ange ett namn för den virtuella enheten och klicka på **Spara**.

4. Använd rullgardinsmenyn **Maximal kapacitet** för att ställa in storleken på den virtuella enheten och klicka på **Fortsätt**.

5. Ställ in ett lösenord för den virtuella enheten. Om du inte vill att den virtuella enheten ska dekrypteras automatiskt när du loggar in på ditt Windows-konto avmarkerar du **Dekryptera automatiskt på det här Windows-kontot**. Klicka på **Fortsätt**.

6. Klicka på **Klar**. Den krypterade virtuella enheten skapas och är klar att använda. Den visas som en lokal enhet om du öppnar **Den här datorn**.

För att komma åt den krypterade enheten efter att datorn har startats om letar du upp den krypterade enhetsfilen (av filtypen `.eed`) du skapade och dubbelklickar på den. Om du uppmanas till det anger du lösenordet du ställde in när den krypterade enheten skapades. Enheten monteras och visas som en lokal disk under Den här datorn. När den krypterade enheten monteras som en lokal disk blir den lokala enheten och dess dekrypterade innehåll tillgängligt för andra användare på datorn om du inte loggar ut eller startar om datorn.

> **Kan jag ta bort en virtuell enhet?**
> Ja. Om du vill ta bort en krypterad virtuell enhet följer du anvisningarna i vår artikel med svar på vanliga frågor om ESET Secure Data.

Kryptera filer på den flyttbara enheten

Secure Data kan användas för att skapa en krypterad mapp på flyttbara enheter. Följ stegen nedan för att kryptera filer på din flyttbara enhet:

1. Sätt in den flyttbara enheten (USB-flashminnet, USB-hårddisken) i datorn.

2. I huvudprogramfönstret klickar du på **Inställningar** > **Säkerhetsverktyg** > **Secure Data** > **Kryptera en flyttbar enhet**.

3. Välj den anslutna flyttbara enheten som ska krypteras och klicka på **Fortsätt**.
Klicka på **Uppdatera** om du vill uppdatera listan med flyttbara enheter. Krypterade enheter eller enheter som inte stöds listas inte.
Om du vill kryptera den säkrade mappen på den valda flyttbara enheten på alla Windows-enheter utan att ESET Smart Security Premium behöver vara installerat väljer du **Kryptera mappen på alla Windows-enheter**.

4. Ställ in ett lösenord för den krypterade katalogen. Om du inte vill att den virtuella enheten ska dekrypteras

automatiskt när du loggar in på ditt Windows-konto avmarkerar du **Dekryptera automatiskt på det här Windows-kontot**. Klicka på **Fortsätt**.

5. Den flyttbara enheten skyddas och den krypterade katalogen på den är klar att användas.

Om du ansluter den flyttbara enheten till en dator där Secure Data inte är installerat, så kommer den krypterade mappen nu inte att vara synlig. Om den flyttbara enheten ansluts till en dator där Secure Data är installerat ombeds du att ange lösenordet för att dekryptera den flyttbara enheten. Om du inte skriver lösenordet kommer den krypterade mappen att vara synlig men inte tillgänglig.

Password Manager

Password Manager ingår i ESET Smart Security Premium-paketet.

Detta är en lösenordshanterare som skyddar och lagrar dina lösenord och personuppgifter. Det har dessutom en funktion för ifyllning av formulär som sparar tid genom att automatiskt och korrekt fylla i webbformulär.

Ytterligare information finns i onlinehjälpen för Password Manager.

- Password Manager installation
- Börja använda Password Manager.
- Hantera Password Manager-lager i ESET HOME

Importera och exportera inställningar

Det går att importera eller exportera dina anpassade ESET Smart Security Premium .xml -konfigurationsfiler från menyn **Inställningar**.

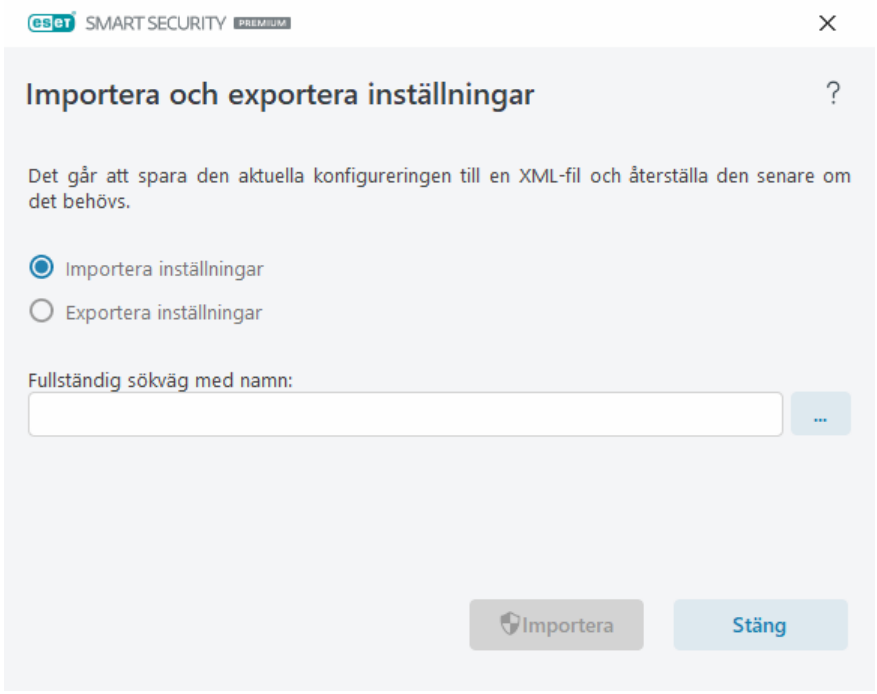
> **Anvisningar med bilder**
> Se Importera eller exportera ESET-konfigurationsinställningar med hjälp av en .xml-fil för illustrerade instruktioner som finns på engelska och flera andra språk.

Import och export av konfigurationsfiler är praktisk om du vill säkerhetskopiera den aktuella konfigurationen av ESET Smart Security Premium för användning senare. Alternativet exportinställningar är också praktiskt när du vill använda din föredragna konfiguration på flera system. De kan enkelt importera en .xml-fil för att överföra dessa inställningar.

Om du vill importera en konfiguration går du till programmets huvudfönster och klickar på **Inställningar** > **Importera/exportera inställningar** och väljer **Importera inställningar**. Skriv konfigurationsfilens namn eller klicka på knappen **...** för att söka efter konfigurationsfilen du vill importera.

Om du vill exportera en konfiguration går du till programmets huvudfönster och klickar på **Inställningar** > **Importera/exportera inställningar**. Väljer **Exportera inställningar** och skriver hela filsökvägen med namnet. Klicka på **...** för att navigera till en plats på datorn som konfigurationsfilen ska sparas på.

> Det kan uppstå ett fel vid export av inställningarna om du inte har tillräcklig behörighet att skriva den exporterade filen till en viss katalog.



Hjälp och support

Klicka på **Hjälp och support** i programmets huvudfönster för att visa supportinformation och felsökningsverktyg som kan hjälpa dig att lösa problem som du stöter på.

Abonnemang

- Felsökning av abonnemang – Klicka på den här länken om du vill hitta lösningar på problem med aktivering eller ändring av abonnemang.
- Ändra abonnemang – Klicka för att öppna aktiveringsfönstret och aktivera produkten. Om enheten är ansluten till ESET HOME väljer du ett abonnemang från ESET HOME-kontot eller lägger till ett nytt.

Installerad produkt

- Vad är nytt – Klicka på den här för att öppna informationsfönstret om nya och förbättrade funktioner.
- Om ESET Smart Security Premium – visar information om ESET Smart Security Premium.
- Felsökning av produkter – klicka på den här länken för att hitta lösningar på de vanligaste problemen.
- **Ändra produkt** – Klicka för att se om ESET Smart Security Premium kan ändras till en annan produktserie med det aktuella abonnemanget.

Hjälpsida – klicka för att öppna hjälpsidorna för ESET Smart Security Premium.

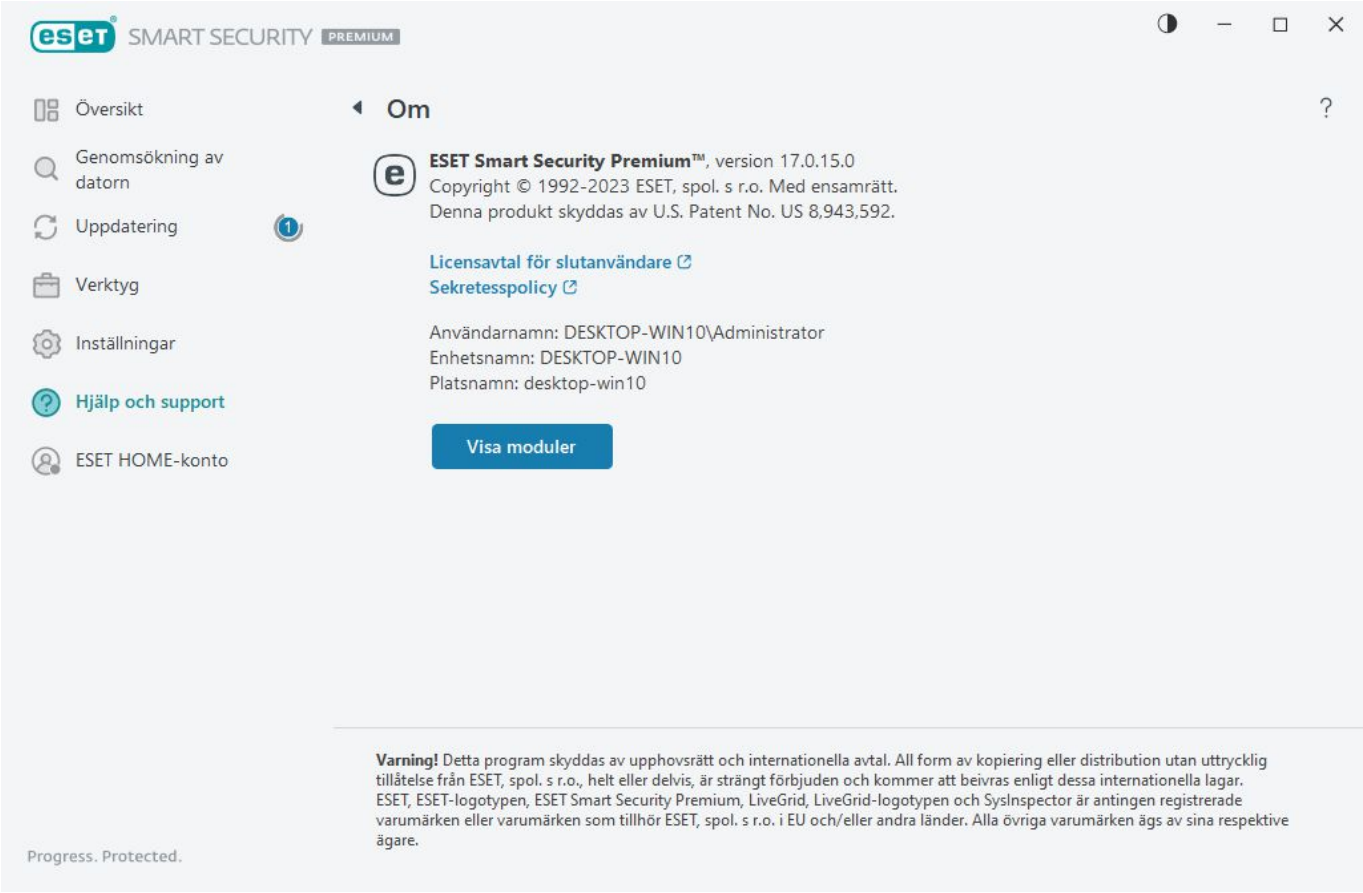
Teknisk support

Kunskapsbas – ESET:s kunskapsbas innehåller svar på de vanligaste frågorna samt rekommenderade lösningar på olika problem. ESET:s tekniska specialister uppdaterar kunskapsbasen regelbundet vilket gör den till

ett kraftfullt verktyg som kan hjälpa dig att lösa olika problem.

Om ESET Smart Security Premium

Det här fönstret innehåller information om den installerade versionen av ESET Smart Security Premium och datorn.



Klicka på **Visa moduler** om du vill visa information om listan över inlästa programmoduler.

- Det går att kopiera information om modulerna till Urklipp genom att klicka på **Kopiera**. Detta kan vara användbart under felsökning eller vid kontakt med teknisk support.

- Klicka på **Detekteringsmotor** i fönstret Moduler för att öppna ESET-virusradarn, som innehåller information om varje version av ESET-detekteringsmotorn.

ESET-nyheter

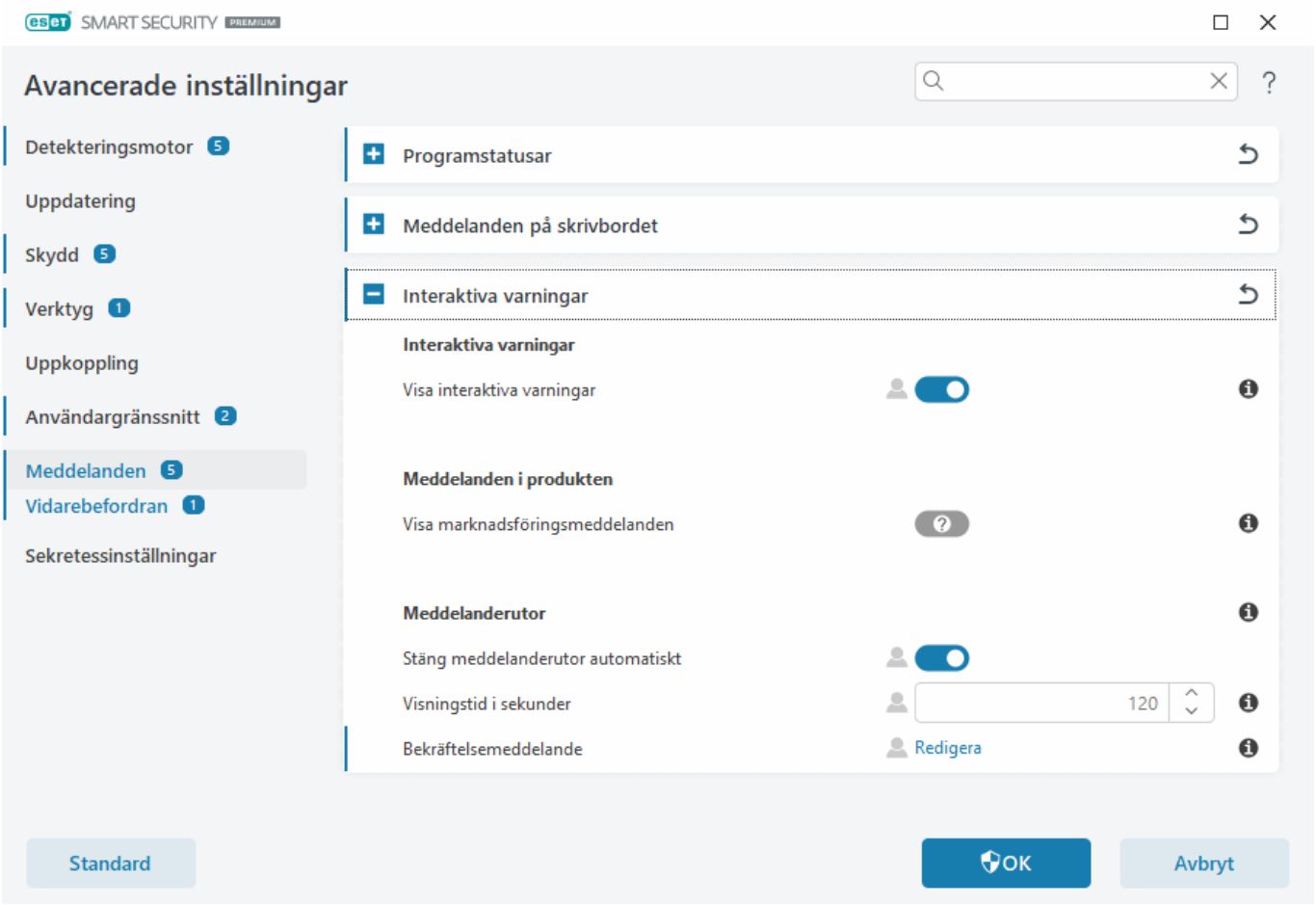
I det här fönstret informerar ESET Smart Security Premium regelbundet om ESET-nyheter.

Meddelanden i produkten är utformade för att informera användare om ESET-nyheter och annan kommunikation. För att skicka marknadsföringsmeddelanden krävs användarens samtycke. Marknadsföringsmeddelanden skickas därför inte till användare som standard (visas med ett frågetecken). Genom att aktivera det här alternativet samtycker du till att få marknadsföringsmeddelanden från ESET. Om du inte vill ha marknadsföringsmaterial från ESET inaktiverar du alternativet **Visa marknadsföringsmeddelanden**.

Följ anvisningarna nedan om du vill aktivera eller inaktivera marknadsföringsmeddelanden via

meddelandefönstret.

1. Öppnar Avancerade inställningar.
2. Klicka på **Meddelanden** > **Interaktiva varningar**.
3. Ändra **Visa marknadsföringsmeddelanden**-alternativet.



Skicka data om systemkonfiguration

För att kunna ge assistans så snabbt och effektivt som möjligt behöver ESET information om ESET Smart Security Premium -konfigurationen, utförlig information om systemet och processer som körs (ESET SysInspector-loggfil) samt registerdata. ESET använder dessa data uteslutande i syfte att ge kunden teknisk assistans.

När du har skickat in webbformuläretskickas data om systemets konfiguration till ESET. Välj **Skicka alltid den här informationen** om du vill komma ihåg den här åtgärden för processen. För att skicka in webbformuläret utan att skicka några data ska du klicka på **Skicka inte data** och fortsätta.

Du kan konfigurera inlämning av systemkonfigurationsdata i Avancerade inställningar > **Verktyg** > **Diagnostik** > Teknisk support.

> Om du har bestämt dig för att skicka in systemkonfigurationsdata är det nödvändigt att fylla i och skicka in webbformuläret. Annars skapas inte ditt ärende och dina systemkonfigurationsdata går förlorade. Om det inte går att skicka systemkonfigurationsdata ska du fylla i webbformuläret och vänta på instruktioner från teknisk support.

Teknisk support

I programmets huvudfönster klickar du på **Hjälp och Support** > **Teknisk support**.

Kontakta teknisk support

Begär support – hittar du ingen lösning på problemet går det även att snabbt kontakta ESET:s tekniska support med formuläret på ESET:s webbplats. Baserat på dina inställningar visas fönstret Skicka data om systemets konfiguration innan webbformuläret fylls i.

Få information för teknisk support

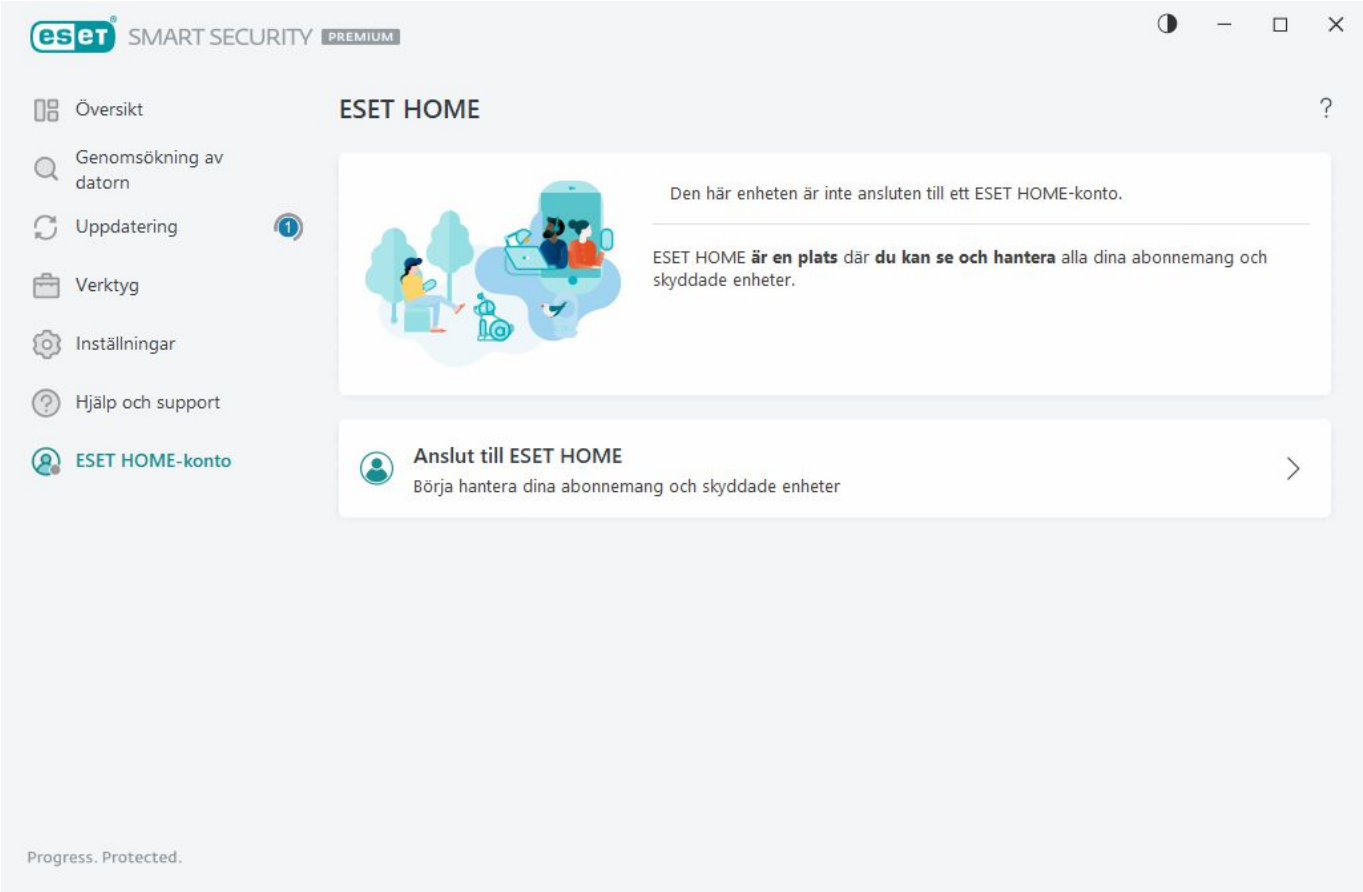
Uppgifter för teknisk support – du kan bli ombedd att kopiera och skicka information till ESET:s tekniska support (till exempel abonnemanginformation, produktnamn, produktversion, operativsystem och datorinformation).

ESET Log Collector – länkar till artikeln i ESET kunskapsbas där du kan hämta ESET Log Collector, ett program som automatiskt samlar in information och loggar från en dator för att lösa problem snabbare. Mer information finns i ESET Log Collector användarguide online.

Aktivera Avancerad loggning om du vill skapa avancerade loggar för alla tillgängliga funktioner så att utvecklare lättare kan diagnostisera och åtgärda problem. Det minsta loggningsomfånget är inställt på nivån **Diagnostik**. Den avancerade loggningen inaktiveras automatiskt efter två timmar om du inte stoppar den tidigare genom att klicka på **Stoppa avancerad loggning**. När alla loggar har skapats visas aviseringsfönstret med direktåtkomst till mappen Diagnostik med de skapade loggarna.

ESET HOME-konto

Du kan granska ESET HOME-kontoanslutningsstatusen i huvudprogramfönstret > **ESET HOME-kontot**.



Den här enheten är inte ansluten till ett ESET HOME-konto

Klicka på Anslut till ESET HOME för att ansluta enheten till ESET HOME och hantera dina abonnemang och skyddade enheter. Du kan förnya, uppgradera eller utöka abonnemang och visa viktig information. I hanteringsportalen eller mobilappen för ESET HOME kan du lägga till olika abonnemang, ladda ned produkter till dina enheter, kontrollera produktens säkerhetsstatus eller dela abonnemang via e-post. Mer information finns i ESET HOME-onlinehjälpen.

Den här enheten är ansluten till ett ESET HOME-konto

Du kan fjärrhantera enhetens säkerhet med hjälp av ESET HOME-portalen eller -mobilappen. Klicka på **App Store** eller **Google Play** för att visa en QR-kod som du kan skanna med din mobiltelefon för att ladda ner ESET HOME-mobilappen från App Store eller Google Play.

ESET HOME-konto – ditt ESET HOME-kontonamn.

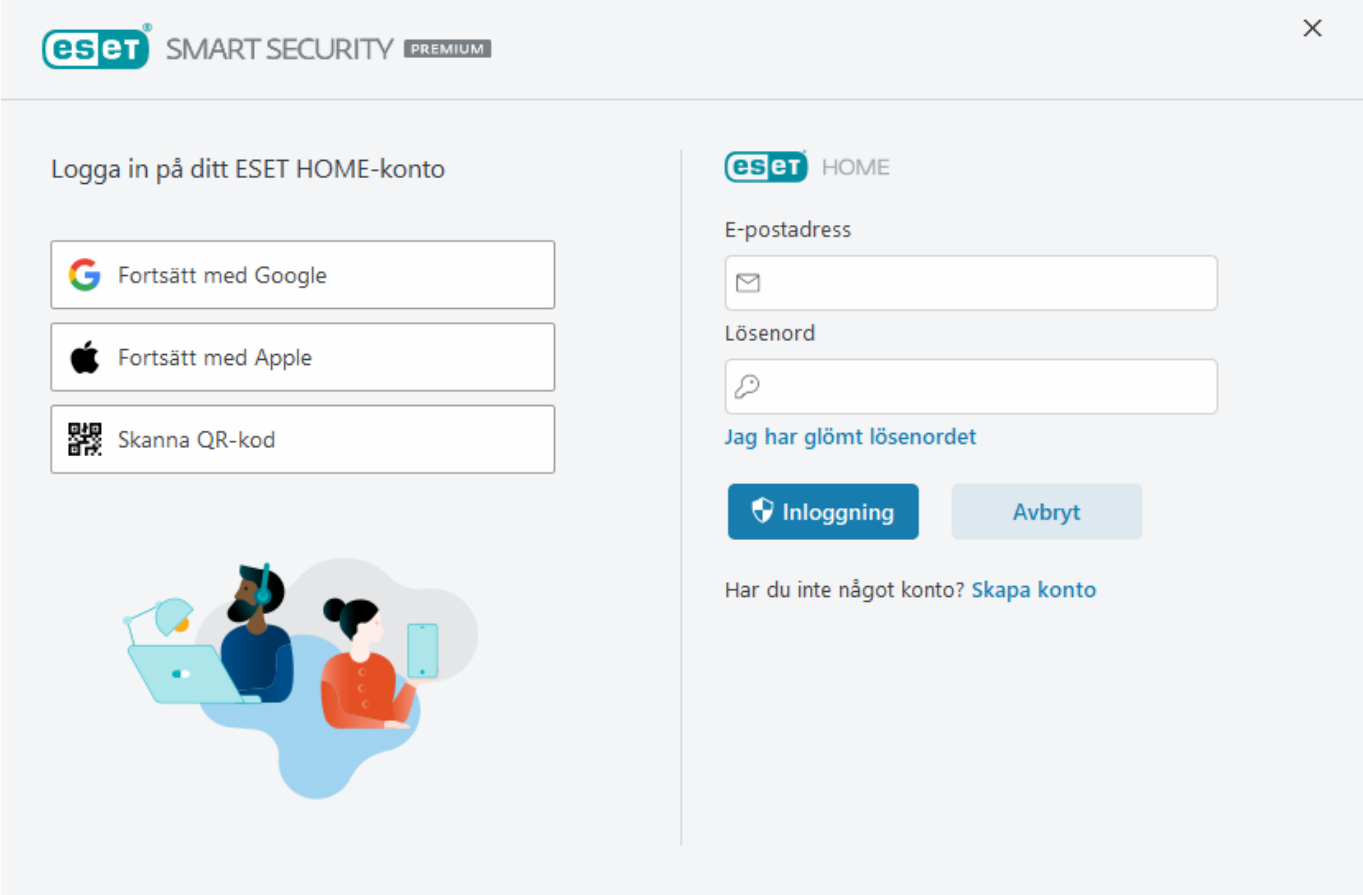
Enhetsnamn – namnet på den här enheten som visas i ESET HOME-kontot.

Öppna ESET HOME – öppnar ESET HOME-hanteringsportalen.

Om du vill koppla bort enheten från ESET HOME-kontot klickar du på **Koppla bort från ESET HOME** > **Koppla från**. Abonnemanget som används för aktivering förblir aktiv och din enhet kommer att skyddas.

Anslut till ESET HOME

Anslut din enhet till ESET HOME för att visa och hantera alla dina aktiverade ESET-abonnemang och enheter. Du kan förnya, uppgradera eller utöka abonnemanget och visa viktig information. I ESET HOME-hanteringsportalen eller -mobilappen kan du lägga till olika abonnemang, ladda ned produkter till dina enheter, kontrollera produktens säkerhetsstatus eller dela abonnemang via e-post. Mer information finns i ESET HOME-onlinehjälpen.



Så här ansluter du enheten till ESET HOMEtill:

Om du ansluter till ESET HOME under installationen eller när du väljer **Använd ESET HOME-konto** som aktiveringsmetod, så följer du anvisningarna i ämne Använd ESET HOME-konto.
Om du redan har ESET Smart Security Premium installerat och aktiverat med ett abonnemang som lagts till i ditt ESET HOME-konto kan du ansluta enheten till ESET HOME i ESET HOME-portalen. Följ anvisningarna i ESET HOME-onlinehjälpguiden och tillåt anslutningen i ESET Smart Security Premium.

1. I programmets huvudfönster klickar du på **ESET HOME-konto** > **Anslut till ESET HOME** eller klickar på **Anslut till ESET HOME** i **Anslut den här enheten till ett ESET HOME-konto**-meddelandet.

2. Logga in på ditt ESET HOME konto.

Om du inte har ett ESET HOME-konto klickar du på **Skapa konto** för att registrera dig eller läser anvisningarna i ESET HOME-onlinehjälpen.
Om du har glömt ditt lösenord klickar du på **Jag har glömt lösenordet** och följer stegen på skärmen eller läser anvisningarna i ESET HOME-onlinehjälpen.

3. Ange ett **enhetsnamn** och klicka på **Fortsätt**.

4. Efter anslutningen visas ett informationsfönster. Klicka på **Klar**.

Logga in till ESET HOME

Det finns flera metoder för att logga in på ditt ESET HOME-konto:

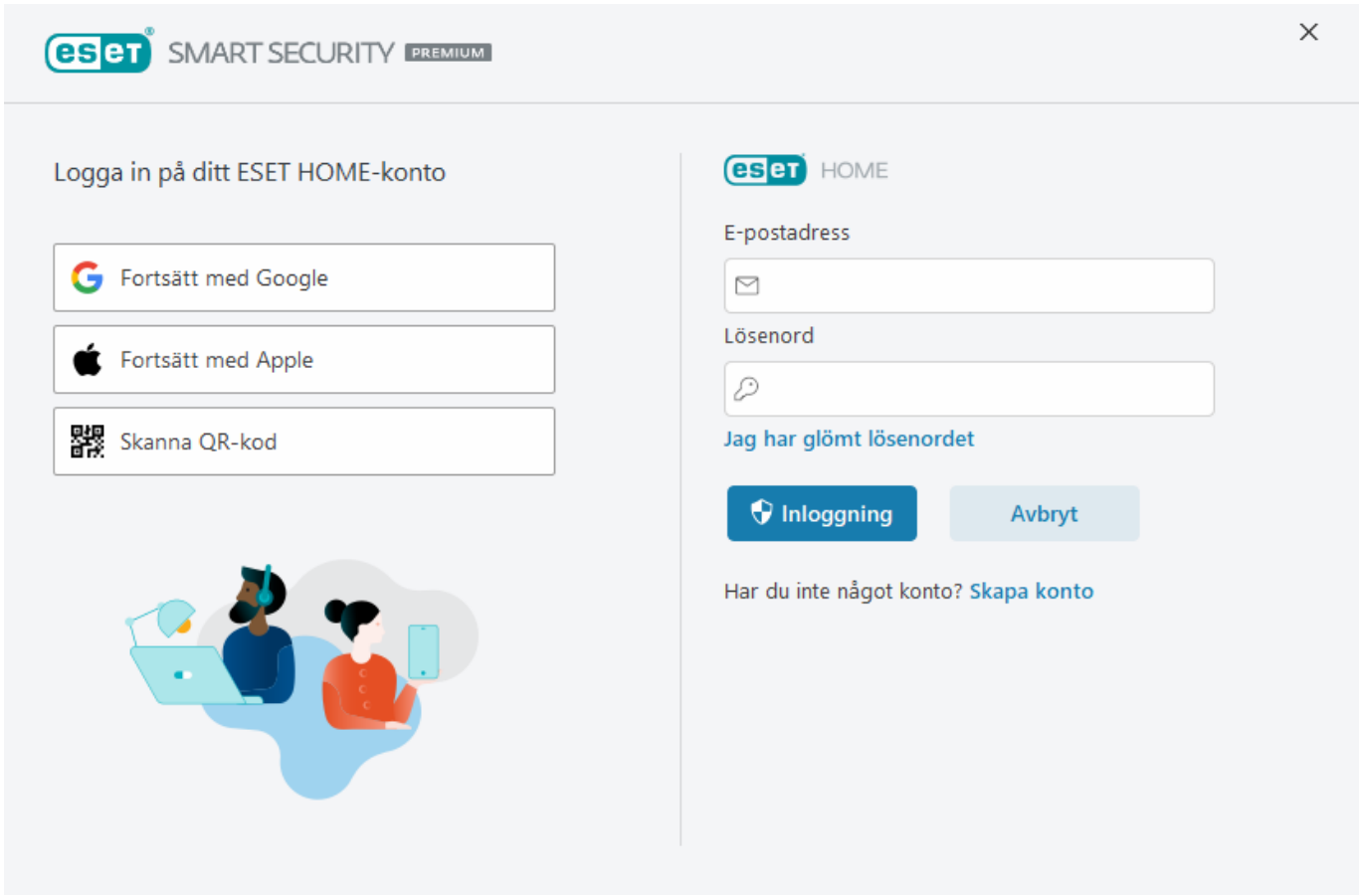
- **Använd din ESET HOME-e-postadress och ditt lösenord** – Skriv den **e-postadress** och det **lösenord** som du använde för att skapa ditt ESET HOME-konto och klicka på **Logga in**.

- **Använd ditt Google-konto/AppleID** – Klicka på **Fortsätt med Google** eller **Fortsätt med Apple** och logga in till lämpligt konto. Efter en lyckad inloggning omdirigeras du till ESET HOME-bekräftelsewebbsidan. Om du vill fortsätta växlar du tillbaka till ESET-produktfönstret. Mer information om Google-kontot/AppleID-inloggningen finns i instruktioner i ESET HOME-onlinehjälpen.

- **Skanna QR-kod** – Klicka på **Skanna QR-kod** för att visa QR-koden. Öppna din ESET HOME-mobilapp och skanna QR-koden eller peka enhetskameran mot QR-koden. Mer information finns i instruktionerna i ESET HOME-onlinehjälpen.

Om du inte har ett ESET HOME-konto klickar du på **Skapa konto** för att registrera dig eller läser anvisningarna i ESET HOME-onlinehjälpen.
Om du har glömt ditt lösenord klickar du på **Jag har glömt lösenordet** och följer stegen på skärmen eller läser anvisningarna i ESET HOME-onlinehjälpen.

Inloggningen misslyckades – vanliga fel.



Inloggningen misslyckades – vanliga fel

Vi kunde inte hitta ett konto som matchar den angivna e-postadressen

E-postadressen du angav matchar inget ESET HOME-konto. Klicka på **Tillbaka** och skriv rätt e-postadress och lösenord.

Om du vill logga in måste du skapa ett ESET HOME-konto. Om du inte har något ESET HOME-konto klickar du på **Bakåt** > **Skapa konto** eller läser i Skapa ett nytt ESET HOME-konto.

Användarnamn och lösenord matchar inte

Det angivna lösenordet matchar inte den angivna e-postadressen. Klicka på **Tillbaka**, skriv in rätt lösenord och kontrollera att den angivna e-postadressen är korrekt. Om du fortfarande inte kan logga in klickar du på **Bakåt** > **Jag har glömt lösenordet** för att återställa ditt lösenord och följer stegen på skärmen, eller läser i Jag har glömt mitt ESET HOME-lösenord.

Det valda inloggningsalternativet matchar inte ditt konto

Ditt konto är länkat till ditt konto på sociala medier. Om du vill logga in till ESET HOME klicka r du på **Fortsätt med Google** eller **Fortsätt med Apple** och loggar in på lämpligt konto. Efter en lyckad inloggning omdirigeras du till ESET HOME-bekräftelsewebbsidan. Du kan koppla bort ditt sociala mediekonto från ditt ESET HOME-konto på ESET HOME-portalen.

Felaktigt lösenord

Det här felet kan uppstå om ditt ESET Smart Security Premium redan är anslutet till ESET HOME och du gör ändringar som kräver att du loggar in (till exempel att inaktivera Anti-Theft) och lösenordet du angav inte matchar ditt konto. Klicka på **Tillbaka** och skriv rätt lösenord. Om du fortfarande inte kan logga in klickar du på **Bakåt** > **Jag har glömt lösenordet** för att återställa ditt lösenord och följer stegen på skärmen, eller läser i Jag har glömt mitt ESET HOME-lösenord.

Lägg till enhet i ESET HOME

Om du redan har ESET Smart Security Premium installerat och aktiverat med ett abonnemang som lagts till i ditt ESET HOME-konto kan du ansluta enheten till ESET HOME i ESET HOME-portalen:

1. Skicka en anslutningsbegäran till enheten.

2. ESET Smart Security Premium visar dialogfönstret **Anslut den här enheten till ett ESET HOME-konto** med ett ESET HOME-kontonamn. Klicka på **Tillåt** för att ansluta enheten till det nämnda ESET HOME-kontot.

i Om det inte finns någon interaktion avbryts anslutningsbegäran automatiskt efter cirka 30 minuter.

Avancerade inställningar

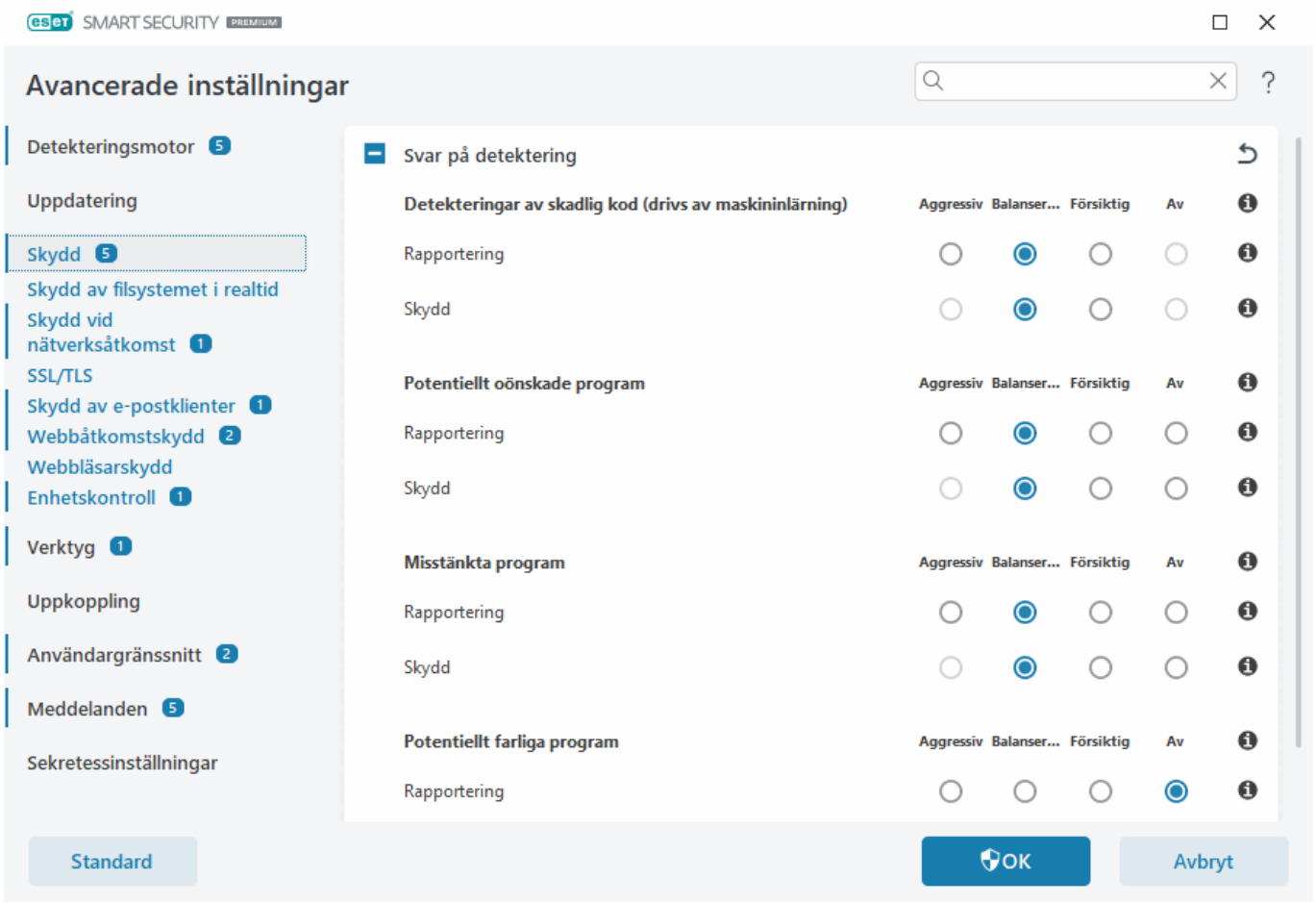
Med Avancerade inställningar kan du konfigurera detaljerade inställningar för ESET Smart Security Premium så att de passar dina behov.

Du öppnar Avancerade inställningar genom att öppna programmets huvudfönster och trycka på **F5-tangenten** på tangentbordet eller klicka på **Inställningar** > **Avancerade inställningar**.

> Beroende på dina Åtkomstinställningar kan du uppmanas att ange ett lösenord för att öppna Avancerade inställningar.

I Avancerade inställningar kan du konfigurera följande inställningar:

- Detekteringsmotor
- Uppdatera
- Skydd
- Verktyg
- Uppkoppling
- Användargränssnitt
- Meddelanden
- Sekretessinställningar



Detekteringsmotor

Med Avancerade inställningar > **Detekteringsmotor** kan du konfigurera följande alternativ:

- Undantag
- Avancerade alternativ
- Nätverkstrafiksskanner

Undantag

Exkluderingar gör det möjligt att exkludera objekt från detekteringsmotorn. För att säkerställa att alla objekt genomsöks rekommenderar vi att du bara skapar exkluderingar när det är absolut nödvändigt. Situationer där du kan behöva exkludera ett objekt kan exempelvis vara genomsökning av stora databasposter som skulle göra datorn långsam under en genomsökning eller programvara som står i konflikt med genomsökningen.

Prestandaexkluderingar – exkludera filer och mappar från genomsökning. Prestandaundantag är användbara för att exkludera genomsökning på filnivå av spelprogram eller när detta orsakar onormalt systembeteende eller ökad prestanda.

Detekteringsexkluderingar gör det möjligt att exkludera objekt från detektering med hjälp av dess detekteringsnamn, sökväg eller hash. Detekteringsexkluderingar exkluderar inte filer och mappar från genomsökning som prestandaexkluderingar gör. Detekteringsexkluderingar exkluderar endast objekt när de

detekteras av detekteringsmotorn och en lämplig regel finns i exkluderingslistan.

Ej att förväxla med andra typer av exkluderingar:

- Processexkluderingar – alla filåtgärder som tillhör exkluderade programprocesser exkluderas från genomsökning (kan krävas för snabbare säkerhetskopiering och tjänsters tillgänglighet),
- Exkluderade filändelser,
- HIPS-exkluderingar,
- Exkluderingsfilter för molnbaserat skydd.

Prestandaundantag

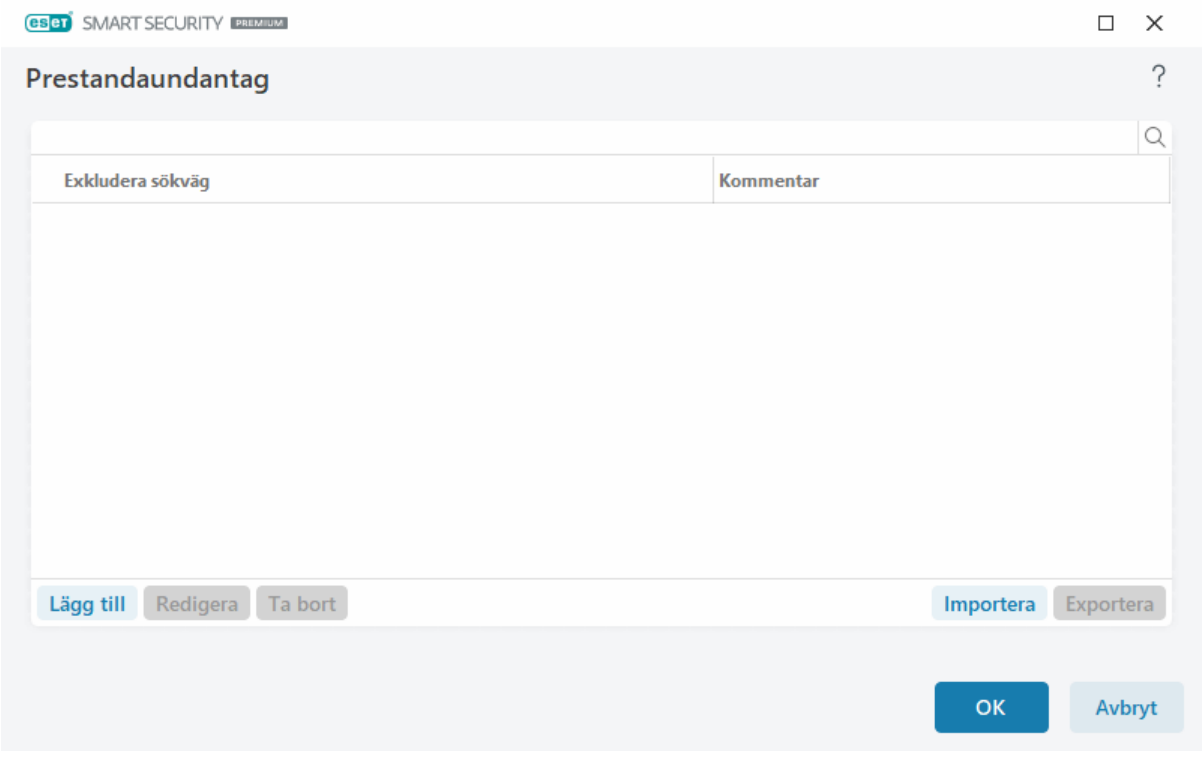
Med prestandaexkluderingar kan du exkludera filer och mappar från genomsökning.

För att säkerställa att alla objekt genomsöks efter hot rekommenderar vi att du bara skapar exkluderingar när det är absolut nödvändigt. Däremot finns det situationer när du kan behöva exkludera ett objekt, exempelvis för stora databasposter som skulle göra datorn långsam under en genomsökning eller programvara som står i konflikt med genomsökningen.

Du kan lägga till filer och mappar som ska undantas från genomsökning i exkluderingslistan via Avancerade inställningar > **Detekteringsmotor** > **Exkluderingar** > **Prestandaexkluderingar** > **Redigera**.

> Blanda inte samman detta med detekteringsexkluderingar, exkluderade filändelser, HIPS-exkluderingar och processexkluderingar.

Om du vill exkludera ett objekt (sökväg: fil eller mapp) från genomsökning klickar du på **Lägg till** och anger önskad sökväg eller väljer den i trädstrukturen.



Ett hot inom en fil detekteras inte av modul **Skydd av filsystemet i realtid** eller **genomsökning av datorn** modul om en fil uppfyller kriterierna för uteslutande från genomsökning.

Kontrollelement

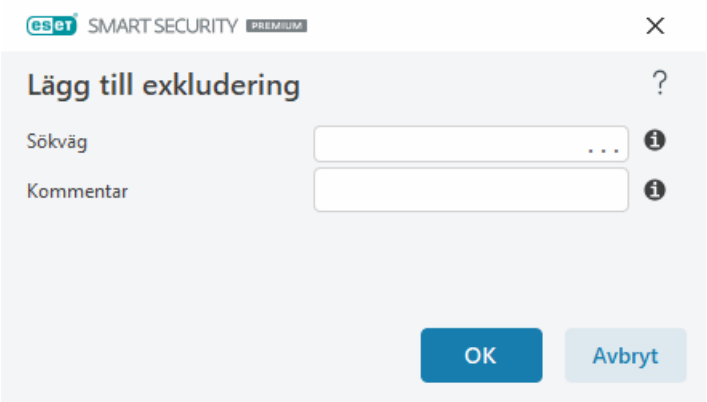
- **Lägg till** – undantar objekt från genomsökning.
- **Redigera** – redigerar valda poster.
- **Ta bort** – tar bort markerade poster (CTRL + klicka för att välja flera poster).

Lägg till eller redigera prestandaexkluderingar

I den här dialogrutan kan du exkludera en viss sökväg (fil eller katalog) för datorn.

Välj sökväg eller ange den manuellt

För att välja önskad sökväg klickar du på **...** i fältet **Sökväg**.
När du skriver manuellt, se fler exempel på exkluderingsformat nedan.



Använd jokertecken för att exkludera en grupp filer. Ett frågetecken (*?*) motsvarar ett tecken, medan en asterisk (***) motsvarar en sträng på noll eller fler tecken.

Exkluderingsformat

• Vill du exkludera alla filer och undermappar i en mapp anger du sökvägen till mappen och använder masken ***
• Vill du endast exkludera doc-filer använder du masken **.doc*
• Om namnet på en körbar fil har ett visst antal tecken (med varierande tecken) och du endast är säker på det första (till exempel ”D”) använder du följande format:
D????.exe (frågetecken ersätter de saknade/okända tecknen)
Exempel:
• *C:\Tools** – sökvägen måste avslutas med snedstreck och (\) asterisk (*) för att indikera att det är en mapp och att allt mappinnehåll (filer och undermappar) som kommer att exkluderas.
• *C:\Tools*.** – samma beteende som *C:\Tools**
• *C:\Tools* – *Tools*-mappen exkluderas inte. Ur skannerns perspektiv kan *Tools* även vara ett filnamn.
• *C:\Tools*.dat* – exkluderar .dat-filer i *Tools*-mappen.
• *C:\Tools\sg.dat* – exkluderar just den här filen med exakt den här sökvägen.

Systemvariabler i exkluderingar

Du kan använda systemvariabler som %PROGRAMFILES% för att definiera exkluderingar vid genomsökningar.

- Om du vill exkludera mappen Programfiler med den här systemvariabeln använder du sökvägen *%PROGRAMFILES%** (glöm inte det omvända snedstrecket och asterisken i slutet av sökvägen) när du lägger till exkluderingar.
- Om du vill exkludera alla filer och mappar i en *%PROGRAMFILES%*-underkatalog anger du sökvägen *%PROGRAMFILES%\exkluderad katalog**

Utöka listan med systemvariabler som stöds

Följande variabler kan användas i formatet för sökvägsexkludering:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Användarspecifika systemvariabler (som *%TEMP%* eller *%USERPROFILE%*) eller miljövariabler (som *%PATH%*) stöds inte.

Jokertecken i mitten av en sökväg stöds inte

Att använda jokertecken i mitten av en sökväg (till exempel *C:\Tools*\Data\file.dat*) kan fungera men stöds inte officiellt för prestandaexkluderingar.

Det finns inga begränsningar för att använda jokertecken i mitten av en sökväg när detekteringsexkluderingar används.

Ordning för exkluderingar

- Det finns inga alternativ för att justera prioritetsnivån för undantag med knapparna för topp/botten (jämfört med Brandväggsregler där regler tillämpas uppifrån och ned).
- När den första tillämpliga regeln matchas av skannern, så utvärderas inte den andra tillämpliga regeln.
- Ju färre regler, desto bättre genomsökningsresultat.
- Undvik att skapa konkurrerande regler.

Format för sökvägsexkludering

Använd jokertecken för att exkludera en grupp filer. Ett frågetecken (*?*) motsvarar ett tecken, medan en asterisk (***) motsvarar en sträng på noll eller fler tecken.

Exkluderingsformat

• Vill du exkludera alla filer och undermappar i en mapp anger du sökvägen till mappen och använder masken *

• Vill du endast exkludera doc-filer använder du masken **.doc*

• Om namnet på en körbar fil har ett visst antal tecken (med varierande tecken) och du endast är säker på det första (till exempel ”D”) använder du följande format:
D????.exe (frågetecken ersätter de saknade/okända tecknen)

Exempel:

• *C:\Tools** – sökvägen måste avslutas med snedstreck och (\) asterisk (*) för att indikera att det är en mapp och att allt mappinnehåll (filer och undermappar) som kommer att exkluderas.

• *C:\Tools*.** – samma beteende som *C:\Tools**

• *C:\Tools* – *Tools*-mappen exkluderas inte. Ur skannerns perspektiv kan *Tools* även vara ett filnamn.

• *C:\Tools*.dat* – exkluderar .dat-filer i *Tools*-mappen.

• *C:\Tools\sg.dat* – exkluderar just den här filen med exakt den här sökvägen.

Systemvariabler i exkluderingar

Du kan använda systemvariabler som %PROGRAMFILES% för att definiera exkluderingar vid genomsökningar.

• Om du vill exkludera mappen Programfiler med den här systemvariabeln använder du sökvägen *%PROGRAMFILES%** (glöm inte det omvända snedstrecket och asterisken i slutet av sökvägen) när du lägger till exkluderingar.

• Om du vill exkludera alla filer och mappar i en *%PROGRAMFILES%*-underkatalog anger du sökvägen *%PROGRAMFILES%\exkluderad katalog**

Utöka listan med systemvariabler som stöds

Följande variabler kan användas i formatet för sökvägsexkludering:

• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Användarspecifika systemvariabler (som *%TEMP%* eller *%USERPROFILE%*) eller miljövariabler (som *%PATH%*) stöds inte.

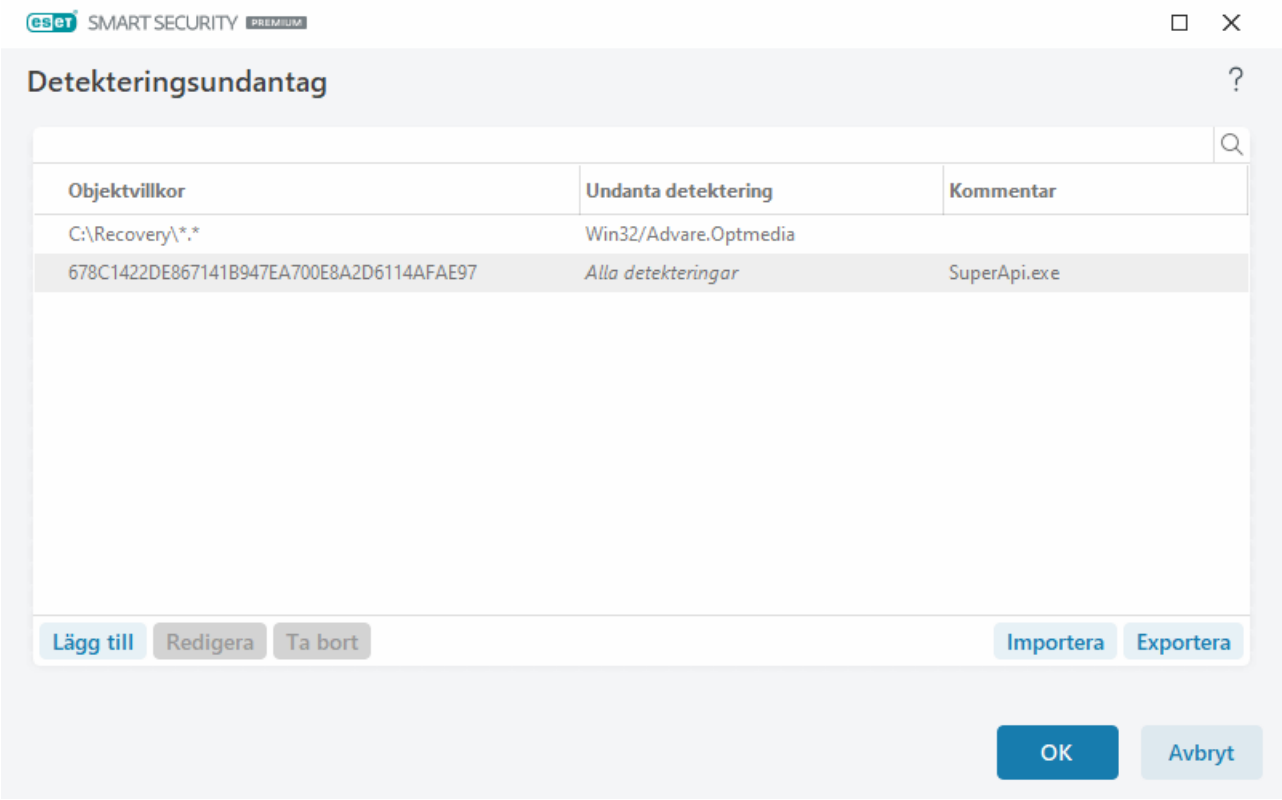
Detekteringsundantag

Detekteringsexkluderingar gör det möjligt att exkludera objekt från detektering genom att filtrera detekteringsnamnet, objektsökvägen eller dess hash.

Så fungerar detekteringsexkluderingar

Detekteringsexkluderingar exkluderar inte filer och mappar från genomsökning som prestandaexkluderingar gör. Detekteringsexkluderingar exkluderar endast objekt när de detekteras av detekteringsmotorn och en lämplig regel finns i exkluderingslistan.

Till exempel när (se den första raden i bilden nedan) ett objekt detekteras som Win32/Adware.Optmedia och den detekterade filen är *C:\Recovery\file.exe*. På den andra raden kommer varje fil, som har lämpligt SHA-1-hash, alltid att exkluderas trots detekteringsnamnet.



För att säkerställa att alla hot detekteras rekommenderar vi att detekteringsexkluderingar endast skapas när det är absolut nödvändigt.

Du kan lägga till filer och mappar i exkluderingslistan via Avancerade inställningar > **Detekteringsmotor** > **Exkluderingar** > **Detekteringsundantag** > **Redigera**.

> Blanda inte samman detta med prestandaexkluderingar, exkluderade filändelser, HIPS-exkluderingar och processexkluderingar.

Om du vill exkludera ett objekt (efter dess detekteringsnamn eller hash) från detekteringsmotorn klickar du på **Lägg till**.

För Potentiellt oönskade program och Potentiellt osäkra program kan uteslutning efter detekteringsnamn också skapas:

- I aviseringsfönstret som rapporterar om detekteringen (klicka på **Visa avancerade alternativ** och välj sedan **Uteslut från detektering**).
- På snabbmenyn Loggfiler med hjälp av guiden för att skapa detekteringsexkluderingar.
- Genom att klicka på **Verktyg** > **Karantän** och sedan högerklicka på filen i karantän och välja **Återställ och exkludera från genomsökning** på kontextmenyn.

Objektvillkor för detekteringsexkluderingar

- **Sökväg** – begränsa en detekteringsexkludering för en viss sökväg (om någon).
- **Detekteringsnamn** – om det finns ett namn på en detektering intill en undantagen fil betyder detta att filen endast är undantagen för den angivna detekteringen (dvs. inte fullständigt undantagen). Om filen vid ett senare tillfälle infekteras av annan skadlig kod detekteras denna skadliga kod.

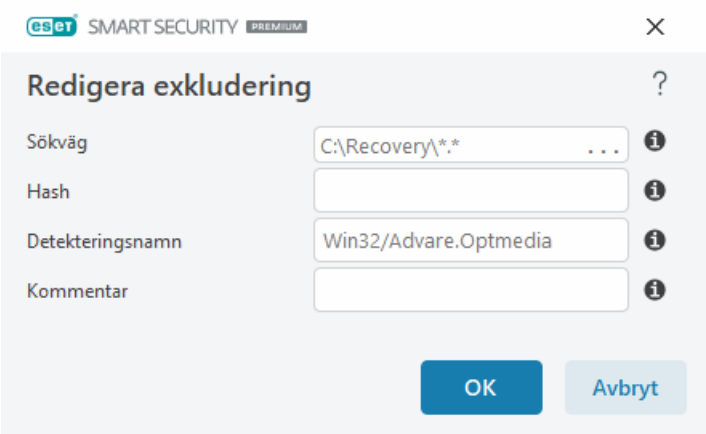
- **Hash** – exkluderar en fil baserat på ett visst hash SHA-1 oavsett filens typ, plats, namn eller ändelse.

Lägga till eller redigera detekteringsexkluderingar

Undanta detektering

Ett giltigt detekteringsnamn från ESET behöver anges. Se loggfilerna för ett giltigt detekteringsnamn och välj sedan **Detekteringar** i listrutan Loggfiler. Detta är användbart när ett falskt positivt prov detekteras i ESET Smart Security Premium. Exkluderingar av riktiga infiltrationer är mycket farliga, så överväg att endast exkludera berörda filer/kataloger genom att klicka på **...** i fältet **Sökväg** och/eller endast under en begränsad tid. Exkluderingar gäller även för potentiellt oönskade program, potentiellt farliga program och misstänkta program.

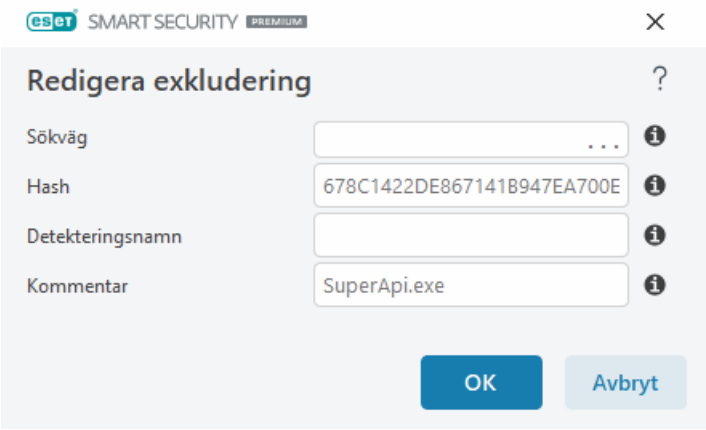
Se även Format för sökvägsexkludering.



Se exemplet på detekteringsexkluderingar nedan.

Exkludera hash

Exkluderar en fil baserat på ett visst hash SHA-1 oavsett filens typ, plats, namn eller ändelse.



Exkluderingar efter detekteringsnamn

Om du vill exkludera en viss detektering anger du det giltiga detekteringsnamnet: Win32/Adware.Optmedia

Du kan även använda följande format när du exkluderar en detektering från ESET Smart Security Premium-varningsfönstret:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Kontrollelement

- **Lägg till** – undantar objekt från genomsökning.
- **Redigera** – redigerar valda poster.
- **Ta bort** – tar bort markerade poster (CTRL + klicka för att välja flera poster).

Guide för att skapa detekteringsexkluderingar

En detekteringsexkludering kan även skapas från kontextmenyn Loggfiler (ej tillgänglig för detektering av skadlig kod):

1. I programmets huvudfönster klickar du på **Verktyg** > **Loggfiler**.
2. Högerklicka på en detektering i **detekteringsloggen**.
3. Klicka på **Skapa exkludering**.

Om du vill exkludera en eller flera detekteringar baserat på **exkluderingsvillkor** klickar du på **Ändra villkor**:

- **Exakta filer** – exkludera varje fil efter dess SHA-1-hash.
- **Detektering** – exkludera varje fil efter dess detekteringsnamn.
- **Sökväg + detektering** – exkludera varje fil efter detekteringsnamn + sökväg, inklusive filnamn (till exempel *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Det rekommenderade alternativet är förvalt baserat på detekteringstypen.

Om du vill kan du lägga till en **kommentar** innan du klickar på **Skapa exkludering**.

Avancerade alternativ för detekteringsmotorn

Aktivera avancerad genomsökning via AMSI, vilket är verktyget Microsoft Antimalware Scan Interface, som möjliggör genomsökning av PowerShell-skript, skript som körs av Windows Script Host och data som genomsöks med AMSI SDK).

Nätverkstrafiksskanner

Nätverkstrafiksskannern ger skydd mot skadlig kod för programprotokoll och integrerar flera avancerade skanningstekniker för skadlig kod. Nätverkstrafiksskannern genomsöker HTTP(S)-, POP3(S)- och IMAP(S)-protokoll automatiskt, oavsett webbläsare eller e-postklient. NDu kan aktivera eller inaktivera Nätverkstrafikskanner i Avancerade inställningar > **Detekteringsmotor** > **Nätverkstrafikskanner**.

Aktivera Nätverkstrafiksskanner – om du inaktiverar det här alternativet genomsöks inte protokollen HTTP(S), POP3(S) och IMAP(S). Observera att följande funktioner i ESET Smart Security Premium kräver att Nätverkstrafiksskanner är aktiverad:

- Webbåtkomstskydd
- Föräldrakontroll
- Webbläsarsekretess och säkerhet
- Säkra banktjänster och surfning
- SSL/TLS
- Skydd mot nätfiske
- Skydd av e-postklient

Molnbaserat skydd

ESET LiveGrid® (bygger på ESET ThreatSense.Netavancerat varningssystem) använder data som ESET:s användare har skickat jorden runt och skickat dem till ESET:s forskningslabb. Genom att erbjuda prov på misstänkt material och metadata gör ESET LiveGrid® det möjligt för oss att reagera omedelbart på våra kunders behov och hålla ESET uppmärksamma på de senaste hoten.

ESET LiveGuard är en funktion som lägger till ett skyddslager som är särskilt utformat för att minska hot som är nya. När detta är aktiverat skickas misstänkta prover som ännu inte har bekräftats som skadliga och som potentiellt kan innehålla skadlig kod automatiskt till ESET-molnet.

Följande alternativ finns tillgängliga:

Aktivera ESET LiveGrid®-ryktessystemet, ESET LiveGrid®-feedbacksystemet och ESET LiveGuard

Ryktessystemet ESET LiveGrid® tillhandahåller molnbaserad vitlistning och svartlistning. ESET LiveGrid®-feedbacksystemet samlar in information om datorn relaterad till nyligen upptäckta hot. Funktionen ESET LiveGuard upptäcker nya, aldrig tidigare sedda hot genom att analysera deras beteende i en sandlåda.

Du kan kontrollera ryktet för filer och Processer som körs direkt från programmets gränssnitt eller kontextmeny med ytterligare information från ESET LiveGrid®. Med proaktivt skydd från ESET LiveGuard blockeras nya filer från att köras tills analysresultatet tas emot.

Aktivera ESET LiveGrid®-ryktessystemet

Ryktessystemet ESET LiveGrid® tillhandahåller molnbaserad vitlistning och svartlistning.

Du kan kontrollera ryktet för filer och Processer som körs direkt från programmets gränssnitt eller kontextmeny med ytterligare information från ESET LiveGrid®.

Aktivera ESET LiveGrid®-feedbacksystemet

Förutom ryktessystemet ESET LiveGrid® samlar feedbacksystemet ESET LiveGrid® in information om din dator relaterad till nyligen upptäckta hot. Denna information kan omfatta följande:

- Prov eller kopia av filen där hotet uppstod
- Sökväg till filen
- Filnamn
- Datum och tid
- Processen genom vilken hotet uppstod på datorn
- Information om datorns operativsystem

Som standard är ESET Smart Security Premium konfigurerat så att misstänkta filer skickas för detaljerad analys till ESET:s viruslaboratorium. Filer med vissa tillägg som *.doc* eller *.xls* är alltid undantagna. Det går att lägga till ytterligare filtillägg om du eller din organisation vill att andra filer inte heller skickas.

Läs mer om att skicka relevanta data i sekretesspolicyn.

Du kan välja att inte aktivera ESET LiveGrid®

Du missar inga programfunktioner, men i vissa fall kan ESET Smart Security Premium reagera snabbare på nya hot när ESET LiveGrid® är aktiverat. Om du har använt ESET LiveGrid® tidigare och inaktiverat det, så finns det kanske datapaket att skicka. Sådana paket skickas till ESET även efter inaktivering. När all aktuell information skickats skapas inte fler paket.

Läs mer om ESET LiveGrid® i Ordlistan.
Se våra illustrerade instruktioner som finns på engelska och flera andra språk för att aktivera eller inaktivera ESET LiveGrid® på ESET Smart Security Premium.

Konfiguration av molnbaserat skydd i Avancerade inställningar

För att komma åt inställningarna för ESET LiveGrid® och ESET LiveGuard ska du öppna Avancerade inställningar > **Detekteringsmotor** > **Molnbaserat skydd**.

- **Aktivera ESET LiveGrid®-ryktessystemet (rekommenderas)** – ESET LiveGrid®-ryktessystemet förbättrar effektiviteten för ESET-lösningar mot skadlig programvara genom att genomsökta filer jämförs mot en databas med vit- och svartlistade objekt i molnet.

• **Aktivera ESET LiveGrid®-feedbacksystem** – skickar relevanta data (som beskrivs i avsnittet **Skicka in prover** nedan) tillsammans med kraschrapporter och statistik till ESET:s forskningslabb för vidare analys.

• **Aktivera ESET LiveGuard** – ESET LiveGuard-funktionen identifierar nya, aldrig tidigare sedda hot genom att analysera deras beteende i en sandlåda. ESET LiveGuard kan endast aktiveras om ESET LiveGrid® är aktiverat.

• **Skicka kraschrapporter och diagnostikdata** – skicka ESET LiveGrid®-relaterade diagnostikdata som kraschrapporter och modulers minnesdumpar. Vi rekommenderar att det här alternativet hålls aktiverat för att hjälpa ESET att förbättra sina produkter och säkerställa bättre skydd för slutanvändare.

• **Skicka anonym statistik** – tillåt att ESET samlar in information om nyligen upptäckta hot, såsom hotets namn, datum och tid då det upptäcktes, detekteringsmetod och associerade metadata, produktversion och -konfiguration, inklusive information om ditt system.

• **E-postadress (valfritt)** – din e-postadress skickas med de misstänkta filerna och används för att kontakta dig om ytterligare information är nödvändig för analysen. Du får endast ett svar från ESET om ytterligare information är nödvändig.

Skicka prover

Skicka in prover manuellt – gör det möjligt att skicka prov manuellt till ESET från snabbmenyn, Karantän eller Verktyg.

Skicka in detekterade prover automatiskt

Välj vilken typ av prover som ska skickas till ESET för analys och för att förbättra framtida detektering (maximal provstorlek är som standard 64 MB). Följande alternativ finns tillgängliga:

• **Alla detekterade prover** – alla objekt som detekteras av detekteringsmotorn (inklusive potentiellt oönskade program när detta har aktiverats i skannerinställningarna).

• **Alla prover utom dokument** – alla detekterade objekt utom **dokument** (se nedan).

• **Skicka inte** – detekterade objekt skickas inte till ESET.

Skicka in misstänkta prover automatiskt

Dessa prover skickas även till ESET om detekteringsmotorn inte detekterar dem. Det kan till exempel vara prover som nästan missade detekteringen eller om någon av ESET Smart Security Premium-skyddsmodulerna anser proverna vara misstänkta eller ha ett oklart beteende (maximal provstorlek är som standard 64 MB).

• **Körbara filer** – inkluderar körbara filer såsom .exe, .dll, .sys.

• **Arkiv** – inkluderar arkivfiltyper såsom .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Skript** – inkluderar skriptfiltyper såsom .bat, .cmd, .hta, .js, .vbs, .ps1.

• **Övriga** – inkluderar filtyper såsom .jar, .reg, .msi, .sfw, .lnk.

• **Möjliga skräppostmeddelanden** – med det här alternativet går det att skicka hela eller delvisa möjliga skräppostmeddelanden med bilagor till ESET för vidare analys. Om alternativet aktiveras förbättras den globala detekteringen av skräppost, inklusive bättre framtida skräppostdetektering för dig.

• **Ta bort körbara filer, arkiv, skript, andra prover och möjliga skräppostmeddelanden från ESET:s servrar** – Definierar när prover som har skickats för analys ska tas bort av ESET LiveGuard.

• **Dokument** – inkluderar Microsoft Office- eller PDF-dokument med eller utan aktivt innehåll.

• **Ta bort dokument från ESET:s servrar** – Definierar när dokument som har skickats för analys ska tas bort av ESET LiveGuard.

Expandera för en lista över alla inkluderade dokumentfiltyper

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Undantag

Med exkluderingsfiltret går det att exkludera filer/mappar från att skickas in (det kan till exempel vara lämpligt att exkludera filer som kan innehålla konfidentiell information, som till exempel dokument eller kalkylblad). De filer som finns listade skickas inte till ESET:s labb för analys, även om de innehåller misstänkt kod. De vanligaste filtyperna är undantagna som standard (.doc osv.). Det går att lägga till filtyper till listan.

Om du vill exkludera filer som hämtats från `download.domain.com` navigerar du till Avancerade inställningar > **Detekteringsmotor** > **Molnbaserat skydd** > **Skicka prover** och klickar på **Redigera** bredvid **Exkluderingar**. Lägg till exkluderingen `.download.domain.com`.

Maximal provstorlek (MB) – anger den maximala storleken på automatiskt inskickade prover (1–64 MB).

ESET LiveGuard

Exkluderingsfilter för molnbaserat skydd

Med exkluderingsfiltret går det att exkludera vissa filer eller mappar från att skickas in som prover. De filer som finns listade skickas inte till ESET:s labb för analys, även om de innehåller misstänkt kod. Vanliga filtyper (till exempel .doc osv.) exkluderas som standard.

Funktionen är praktisk för att undanta filer som kan innehålla konfidentiell information, som dokument eller kalkylblad.

Om du vill utesluta filer nedladdade från download.domain.com klickar du på download.domain.com klickar du på Avancerade inställningar > **Detekteringsmotor** > **Molnbaserat skydd** > **Skicka prover** > **Exkluderingar** och lägger till exkluderingen *download.domain.com*.

ESET LiveGuard

ESET LiveGuard är en funktion som lägger till ett molnbaserat skyddslager som är särskilt utformat för att minska hot som är nya.

När detta är aktiverat skickas misstänkta prover som ännu inte har bekräftats som skadliga och som potentiellt kan innehålla skadlig kod automatiskt till ESET-molnet. Inlämnade prover körs i en sandlåda och utvärderas av

våra avancerade detekteringsmotorer för skadlig kod. Skadliga prover eller misstänkta skräppostmeddelanden skickas till ESET LiveGrid®. E-postbilagor hanteras separat och kan komma att skickas till ESET LiveGuard. Du kan definiera omfattningen av skickade filer och fillagringsperioden i ESET-molnet. Dokument och PDF-filer med aktivt innehåll (makron, javascript) skickas inte som standard.

ESET LiveGuard kan aktiveras eller inaktiveras i:

- Programmets huvudfönster > **Inställningar** > **Datorskydd**
- Avancerade inställningar > **Detekteringsmotor** > **Molnbaserat skydd**

För att komma åt de avancerade inställningarna för ESET LiveGuard öppnar du Avancerade inställningar > **Detekteringsmotor** > **Molnbaserat skydd** > **ESET LiveGuard**.

Åtgärd efter identifiering – Ställer in åtgärden som ska vidtas om det analyserade provet utvärderas som ett hot.

Proaktivt skydd – tillåter eller blockerar körningen av filer som analyseras av ESET LiveGuard. Om en fil är misstänkt blockerar det proaktiva skyddet körning av den tills analysen är klar. Förebyggande skydd identifierar filer från följande källor:

- Filer som laddats ner med en webbläsare som stöds
- Hämtade från en e-postklient
- Filer som extraheras från ett okrypterat eller krypterat arkiv med hjälp av ett av de arkivverktyg som stöds
- Körda och öppnade filer som finns på en flyttbar enhet

Se de program som stöds i tabellen nedan:

Webbläsare	E-postklienter	Arkivprogram	Flyttbara enheter
Internet Explorer	Microsoft Outlook	WinRAR	USB-minne
Microsoft Edge	Mozilla Thunderbird	WinZIP	USB-hårddisk
Chrome	Microsoft Mail	Microsoft Explorers inbyggda uppackare	CD/DVD
Firefox		7zip	Diskett
Opera			Inbyggd kortläsare
Brave Webbläsare			

Obs
Filer som kopieras med Utforskaren från en exkluderad plats till en skyddad plats blockeras av det proaktiva skyddet eftersom ESET Smart Security Premium känner igen `explorer.exe` som ett arkivverktyg.

Om proaktivt skydd är inställt på **Blockera körning tills analysresultatet tas emot** och du vill avblockera filen som analyseras, så högerklickar du på filen och klickar på **Avblockera fil analyserad av ESET LiveGuard.**

Maximal väntetid för analysresultatet (min) – Anger den tid efter vilken de analyserade filerna ska avblockeras oavsett om analysen är klar.

ESET LiveGuard informerar dig om analysstatusen med hjälp av meddelanden. Se tillgängliga meddelanden nedan:

Meddelandetitel	Beskrivning
Fil blockerad på grund av analys	Filen blockeras av ESET LiveGuard. ESET LiveGuard analyserar filen för att säkerställa att den är säker att använda. Du kan vänta eller välja något av följande alternativ: • **Avblockera filen** – Avblockerar filen, men analysen fortsätter. Du får en avisering om resultatet. Detta rekommenderas inte om du inte är säker på filens integritet. • **Ändra inställningar** – Öppnar fönstret Inställning av datorskydd där du kan inaktivera ESET LiveGuard och dess proaktiva skydd.
Fil avblockerad	Filen är inte längre blockerad. Analysen fortsätter och du får ett meddelande om resultatet. Du kan öppna filen.
Fil analyseras fortfarande	ESET LiveGuard behöver mer tid för att slutföra analysen. Du kan öppna filen om det behövs.
Hotet har avlägsnats	ESET LiveGuard har slutfört analysen och filen innehöll ett hot. Filen har rensats.
Fil säker att använda	ESET LiveGuard har slutfört analysen och filen är säker att använda.

Om ESET LiveGuard inte fungerar korrekt får du ett meddelande i huvudprogramfönstret > **Översikt**. Lös problemet genom att följa anvisningarna i meddelandet. Kontakta teknisk support om du inte kan lösa problemet.

Genomsökningar efter skadlig kod

Avsnittet **Genomsökningar efter skadlig kod** är tillgängligt från Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod**. Det gör att du kan konfigurera genomsökningsparametrar för genomsökningsprofiler.

Genomsökning på begäran

Vald profil – en viss uppsättning parametrar som används vid genomsökning på begäran. Om du vill skapa en ny klickar du på **Redigera** intill **Lista över profiler**. Se Genomsökningsprofiler för mer information.

Du kan konfigurera följande alternativ när du har valt genomsökningsprofilen:

Genomsökningsobjekt – om du bara vill genomsöka ett visst objekt eller en grupp med objekt kan du klicka på **Redigera** bredvid **Genomsökningsobjekt** och välja ett alternativ i mappstrukturen. Se Genomsökningsobjekt för mer information.

Skydd på begäran och maskininlärningsskydd – du kan konfigurera rapporterings- och skyddsnivåer för varje genomsökningsprofil. Som standard använder genomsökningsprofiler samma inställningar som definierats i Skydd av filsystemet i realtid. Inaktivera växlingsknappen bredvid **Använd inställning för realtidsskydd** för att konfigurera anpassade rapporterings- och skyddsnivåer. Du hittar en detaljerad förklaring av rapporterings- och skyddsnivåer i Skydd.

ThreatSense – avancerade inställningsalternativ, till exempel filnamnstillägg som du vill kontrollera och detekteringsmetoder som används. Du hittar mer information i ThreatSense.

Genomsökningsprofiler

Det finns fyra fördefinierade genomsökningsprofiler i ESET Smart Security Premium:

- **Smart genomsökning** – Detta är standardprofilen för avancerad genomsökning. Profilen Smart genomsökning använder Smart optimering, som exkluderar som var rena i en tidigare genomsökning och som inte har ändrats sedan dess. Det här möjliggör kortare genomsökningstider med minsta påverkan på systemets säkerhet.

- **Genomsökning av kontextmeny** – Du kan starta en sökning på begäran av valfri fil från kontextmenyn. Med hjälp av genomsökningsprofilen för kontextmenyn kan du definiera en genomsökningskonfiguration som ska användas när du utlöser genomsökningen på detta sätt.

- **Djup genomsökning** – Profilen Djup genomsökning använder inte Smart optimering som standard, därför exkluderas inga filer från genomsökning med den här profilen.

- **Genomsökning av datorn** – Detta är standardprofilen som används för standardgenomsökningen av datorn.

Det går att spara genomsökningsinställningarna för framtida genomsökning. Vi rekommenderar att skapar en profiler (med olika genomsökningsobjekt, genomsökningsmetoder och andra parametrar) för varje regelbunden genomsökning.

Skapa en ny profil genom att öppna Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Genomsökning på begäran** > **Lista över profiler** > **Redigera**. Fönstret **Profilhanteraren** innehåller rullgardinsmenyn **Vald profil** med befintliga genomsökningsprofiler och alternativet att skapa en ny. Du hittar hjälp om hur du skapar en genomsökningsprofil som motsvarar dina behov i avsnittet ThreatSense som innehåller en beskrivning av varje parameter i genomsökningsinställningen.

> Anta att du vill skapa en egen genomsökningsprofil och konfigurationen **Genomsök datorn** är delvis lämplig, men du vill inte genomsöka internt packade filer eller potentiellt farliga program och dessutom vill du använda **Åtgärda alltid detektering**. Ange namnet på den nya profilen i fönstret **Profilhanteraren** och klicka på **Lägg till**. Välj den nya profilen i listrutan **Vald profil** och justera de återstående parametrarna så att de uppfyller dina krav och klicka på **OK** för att spara den nya profilen.

Genomsökningsobjekt

På rullgardinsmenyn **Genomsökningsobjekt** kan du välja fördefinierade genomsökningsobjekt.

- **Med profilinställningar** – väljer mål angivna i den valda genomsökningsprofilen.
- **Flyttbara media** – väljer disketter, USB-enheter, CD/DVD.

- **Lokala enheter** – kontrollerar alla hårddiskar i systemet.

- **Nätverksenheter** – genomsöker alla mappade nätverksenheter.

- **Anpassat val** – avbryter alla tidigare val.

Mapp(träd)strukturen innehåller även specifika genomsökningsmål.

- **Arbetsminne** – söker igenom alla processer och data som för närvarande används av arbetsminnet.

- **Startsektorer/UEFI** – genomsöker startsektorerna och UEFI efter skadlig kod. Läs mer om UEFI-skannern i ordlistan.

- **WMI-databas** – söker igenom hela Windows Management Instrumentation (WMI)-databasen, alla namnrymder, alla klassinstanser och alla egenskaper. Söker efter referenser till infekterade filer eller skadlig kod inbäddad som data.

- **Systemregistret** – söker igenom hela systemregistret, alla nycklar och undernycklar. Söker efter referenser till infekterade filer eller skadlig kod inbäddad som data. När detekteringarna rensas finns referensen kvar i registret så att ingen viktig data går förlorad.

Om du snabbt vill navigera till ett genomsökningsmål (fil eller mapp) skriver du dess sökväg i textfältet under trädstrukturen. Sökvägen är skiftlägeskänslig. Om du vill inkludera målet i genomsökningen markerar du dess kryssruta i trädstrukturen.

Genomsökning vid inaktivitet

Du kan aktivera genomsökning vid inaktivitet i Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Genomsökning vid inaktivitet**.

Genomsökning vid inaktivitet

Aktivera växlingsknappen bredvid **Aktivera genomsökning vid inaktivitet** för att aktivera den här funktionen. När datorn är i inaktivt läge utförs en genomsökning av datorn på alla lokala enheter.

Som standard körs inte genomsökningen när en (bärbar) dator går på batteri. Du kan åsidosätta den här inställningen genom att aktivera växlingsknappen bredvid **Kör även om datorn är batteridriven** i Avancerade inställningar.

Aktivera växlignsknappen bredvid **Aktivera loggning** i Avancerade inställningar för att registrera resultatet av en genomsökning av datorn i avsnittet Loggfiler (klicka på **Verktyg** > **Loggfiler** i programmets huvudfönster och välj **Genomsökning av datorn** i listrutan **Logg**).

Detektering av inaktivt tillstånd

I Utlösare för detektering av inaktivt tillstånd finns en fullständig lista över de villkor som måste uppfyllas för att genomsökning vid inaktivt tillstånd ska utlösas.

ThreatSense – avancerade inställningsalternativ, till exempel filnamnstillägg som du vill kontrollera och detekteringsmetoder som används. Du hittar mer information i ThreatSense.

Detektering av inaktivt tillstånd

Det går att konfigurera inställningarna för detektering av inaktivt tillstånd i Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Genomsökning vid inaktivitet** > **Detektering av inaktivt tillstånd**. Dessa inställningar anger en utlösning av Genomsökning vid inaktivitet:

- **Skärmen eller skärmsläckaren stängdes av**
- **Datorlås**
- **Användarutloggning**

Använd växlingsknappen för respektive status för att aktivera och inaktivera utlösarna för detektering vid inaktivitet.

Startskanner

Automatisk kontroll av filer som startas utförs som standard när systemet startar eller vid uppdatering av detekteringsmotorn. Denna genomsökning beror på Schemaläggarens konfiguration och aktiviteter.

Genomsökningsalternativ vid start är en del av den schemalagda aktiviteten **Kontroll av filer som startas automatiskt**. För att ändra dess inställningar ska du gå till **Verktyg** > **Schemaläggare**, klicka på **Kontroll av filer som startas automatiskt** och sedan på **Redigera**. I det sista steget öppnas fönstret Kontroll av filer som startas automatiskt. Ytterligare information om att skapa och hantera schemalagda aktiviteter finns i Skapa nya aktiviteter.

ThreatSense – avancerade inställningsalternativ, till exempel filnamnstillägg som du vill kontrollera och detekteringsmetoder som används. Du hittar mer information i ThreatSense.

Kontroll av filer som startas automatiskt

När du skapar den schemalagda aktiviteten Kontroll av filer som startas automatiskt, finns flera alternativ att justera följande parametrar:

Rullgardinsmenyn **Genomsökningsobjekt** anger genomsökningsdjupet för filer som körs vid systemstart baserat på en hemlig sofistikerad algoritm. Filer ordnas i fallande ordning enligt följande villkor:

- **Alla registrerade filer** (flest genomsökta filer)
- **Filer som används sällan**
- **Filer som används relativt ofta**
- **Filer som används ofta**
- **Endast de mest använda filerna** (minst antal genomsökta filer)

Även två specifika grupper inkluderas:

- **Filer som körs innan användaren loggar in** – innehåller filer från platser som tillåter åtkomst utan att användaren är inloggad (inkluderar nästan alla startplatser som tjänster, webbläsartillägg, winlogon-meddelande, Windows schemaläggarposter, kända dll-filer osv.)
- **Filer som körs när användaren har loggat in** - innehåller filer från platser som endast tillåter åtkomst när användaren är inloggad (inkluderar filer som endast körs för en viss användare, typiskt filer i *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Listor över filer som ska genomsökas är fasta för varje grupp ovan. Om du väljer ett lägre genomsökningsdjup för filer som körs vid systemstart, så genomsöks inte de genomsökta filerna när de öppnas eller körs.

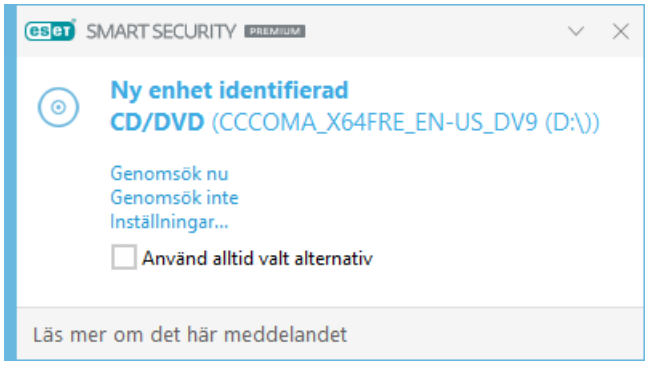
Genomsökningsprioritet – prioritetsnivå som avgör när en genomsökning startar:

- **Vid inaktivitet** – aktiviteten utförs endast när systemet är inaktivt,
- **Lägst** – när systemets belastning är den lägsta möjliga,
- **Lägre** – vid en låg systembelastning,
- **Normal** – vid genomsnittlig systembelastning.

Flyttbara medier

ESET Smart Security Premium ger automatisk genomsökning av flyttbara medier (CD/DVD/USB/...) när dessa sätts in i en dator. Detta kan vara användbart om administratören vill förhindra användning av flyttbara medier med oönskat innehåll.

Följande dialogruta visas när flyttbara medier sätts in och **Visa genomsökningsalternativ** har ställts in i Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Flyttbara medier**:



Alternativ för den här dialogrutan:

- **Genomsök nu** – med det här alternativet utlöses en genomsökning av flyttbara medier.
- **Skanna inte** – flyttbara medier skannas inte.
- **Inställningar** – öppnar Avancerade inställningar.
- **Använd alltid valt alternativ** – när det här alternativet väljs utförs samma åtgärd när ett flyttbart medium sätts in en igen.

ESET Smart Security Premium Har dessutom funktionen Enhetskontroll som gör det möjligt att definiera regler för användning av externa enheter på en viss dator. Ytterligare information om Enhetskontroll finns i avsnittet Enhetskontroll.

För att komma åt inställningarna för genomsökning av flyttbara medier öppnar du Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Flyttbara medier**.

Åtgärd att vidta efter isättning av flyttbara medier – välj standardåtgärd att vidta när en flyttbar medieenhet sätts in i datorn (CD/DVD/USB). Välj önskad åtgärd när ett flyttbart medium sätts in i datorn:

- **Genomsök inte** – ingen åtgärd vidtas och fönstret **Ny enhet identifierad** öppnas inte.
- **Automatisk genomsökning av enhet** – en genomsökning av den isatta flyttbara medieenheten utförs.
- **Visa genomsökningsalternativ** – öppnar avsnittet Inställning av **flyttbara medier**.

Dokumentskydd

Dokumentskyddsfunktionen genomsöker Microsoft Office-dokument innan de öppnas, samt filer som hämtats automatiskt av Internet Explorer, som t.ex. Microsoft ActiveX-kontroller. Dokumentskydd tillhandahåller ett skyddslager utöver skydd av filsystemet i realtid och går att inaktivera för att förbättra prestanda på system som inte hanterar stora mängder Microsoft Office-dokument.

Om du vill aktivera Dokumentskydd ska du öppna Avancerade inställningar > **Detekteringsmotor** > **Genomsökningar efter skadlig kod** > **Dokumentskydd** och klickar på växlingsknappen bredvid **Aktivera Dokumentskydd**.

ThreatSense – avancerade inställningsalternativ, till exempel filnamnstillägg som du vill kontrollera och detekteringsmetoder som används. Du hittar mer information i ThreatSense.

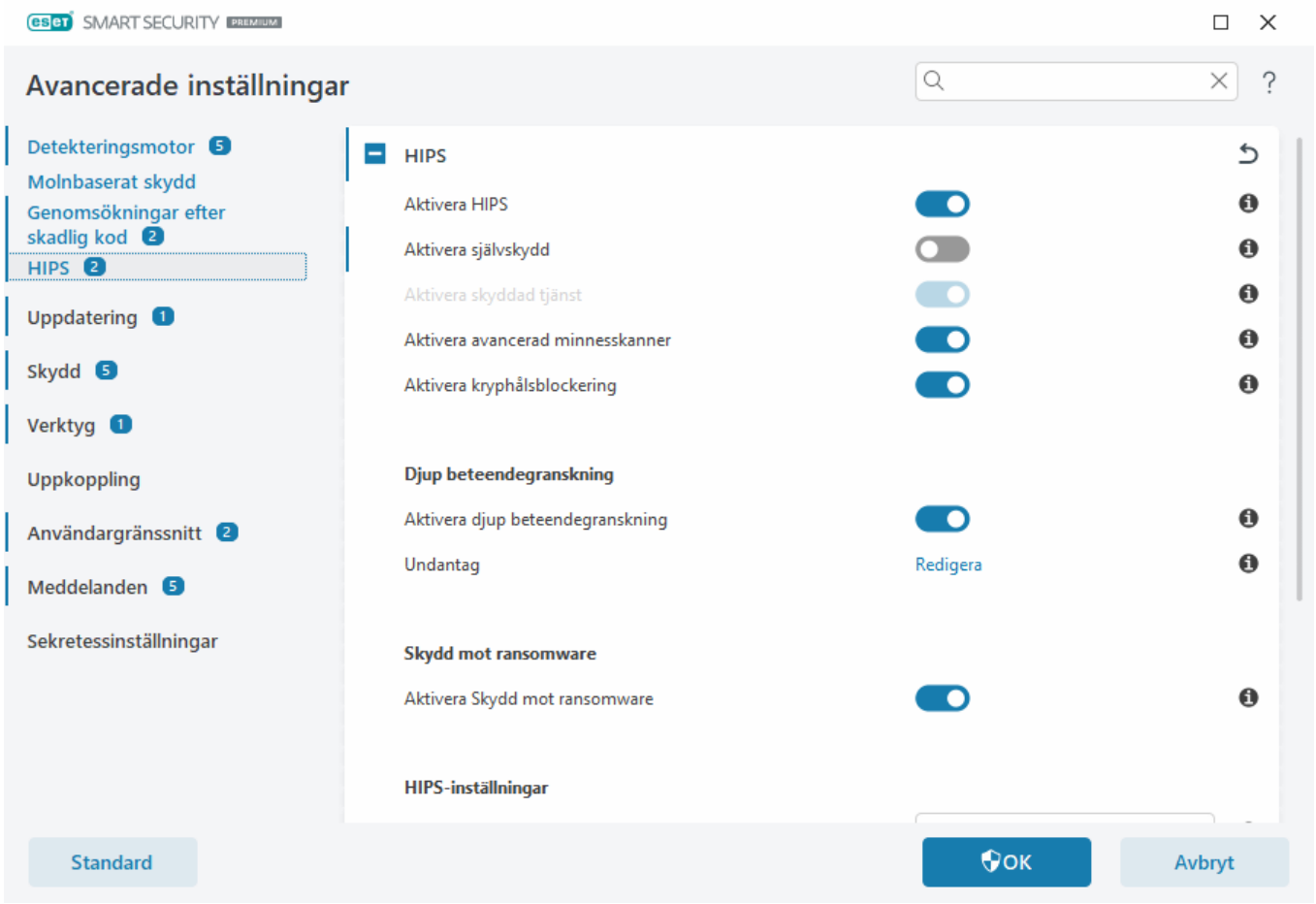
Funktionen aktiveras av program som använder Microsoft Antivirus API (t.ex. Microsoft Office 2000 och senare eller Microsoft Internet Explorer 5.0 och senare).

HIPS – Host Intrusion Prevention System

Endast en erfaren användare bör ändra inställningarna för HIPS. Felaktig konfiguration av HIPS-inställningar kan leda till systeminstabilitet.

Host Intrusion Prevention System (HIPS) skyddar systemet mot skadlig kod och oönskad aktivitet oönskad aktivitet som försöker att påverka datorn negativt. HIPS använder avancerad beteendeanalys tillsammans med detekteringsfunktioner i nätverksfilter för att övervaka aktiva processer, filer och registernycklar. HIPS är åtskilt från skydd av filsystemet i realtid och är inte en brandvägg.

Du kan konfigurera HIPS-inställningar i Avancerade inställningar > **Detekteringsmotor** > **HIPS** > **HIPS**. HIPS läge (aktiverat/inaktiverat) visas i huvudprogramfönstret för ESET Smart Security Premium > **Inställningar** > **Datorskydd**.



HIPS

Aktivera HIPS – HIPS är aktiverat som standard i ESET Smart Security Premium. Om HIPS stängs av inaktiveras övriga HIPS-funktioner som till exempel kryphålsblockering.

Aktivera självskydd – ESET Smart Security Premium använder den inbyggda **självskyddstekniken** i HIPS för att förhindra att skadlig programvara skadar eller inaktiverar skyddet mot virus och spionprogram. Självskyddet ser till att viktiga system och ESET:s processer, registernycklar och filer inte manipuleras.

Aktivera skyddad tjänst – aktiverar skyddet för ESET-tjänsten (ekrn.exe). När det har aktiverats startas tjänsten som en skyddad Windows-process för att kunna försvara sig mot attacker av skadlig kod.

Aktivera avancerad minnesskanner – fungerar i kombination med Kryphålsblockering för att stärka skyddet mot skadlig programvara som har utformats för att kringgå detekteringen genom skadlig programvara vid användning av förvridning eller kryptering. Avancerad minnesskanner är aktiverad som standard. Läs mer om den här skyddstypen i ordlistan.

Aktivera kryphålsblockering – utformat för att förstärka ofta exploaterade programtyper, såsom webbläsare, PDF-läsare, e-postklienter och MS Office-komponenter. Kryphålsskyddet är aktiverat som standard. Läs mer om den här skyddstypen i ordlistan.

Djup beteendegranskning

Aktivera djup beteendegranskning – ytterligare ett skyddslager som fungerar som en del av HIPS-funktionen. Det här HIPS-tillägget analyserar beteendet hos alla program som körs på datorn och varnar om processens beteende är skadligt.

HIPS-exkluderingar från djup beteendegranskning gör det möjligt att exkludera processer från analys. För att säkerställa att alla processer genomsöks efter hot rekommenderar vi att endast skapa exkluderingar när det är absolut nödvändigt.

Sköld mot ransomware

Aktivera sköld mot ransomware – ännu ett skyddslager som ingår i HIPS-funktionen. För att skölden mot ransomware ska fungera måste ESET LiveGrid®-ryktessystemet vara aktiverat. Läs mer om den här skyddstypen.

Aktivera Intel® Threat Detection Technology – hjälper till att identifiera ransomware-attacker genom att använda unik Intel-processortelemetri för att öka detekteringseffektiviteten, minska antalet falska positiva varningar och utöka synligheten för att fånga upp avancerade tekniker för undvikande. Se de processorer som stöds.

HIPS-inställningar

Filtreringsläget används med ett av följande lägen:

Filtreringsläge	Beskrivning
Automatiskt läge	Åtgärder aktiverade, utom sådana som blockeras av fördefinierade regler som skyddar systemet.
Smart läge	Användaren meddelas endast om misstänkta händelser.
Interaktivt läge	Användaren ombeds bekräfta åtgärder.
Principbaserat läge	blockerar alla åtgärder som inte definieras av en specifik regel som tillåter dem.
Inlärningsläge	Åtgärder är aktiverade och en regel skapas efter varje åtgärd. Regler skapade i detta läge går att visa i redigeraren **HIPS-regler**, men deras prioritet är lägre än för regler som skapas manuellt eller i automatiskt läge. När du väljer **Inlärningsläge** i rullgardinsmenyn **Filtreringsläge** blir inställningen **Inlärningsläget kommer att avslutas vid** tillgänglig. Välj hur länge du vill att inlärningsläget ska pågå. Den längsta tidsperioden är 14 dagar. När den angivna tiden gått ut ombeds du att redigera de regler som skapats av HIPS medan det befann sig i inlärningsläget. Du kan även välja ett annat filtreringsläge eller senareläge beslutet och fortsätta använda inlärningsläget.

Läge inställt efter inlärningslägets utgång – välj vilket filtreringsläge som ska tillämpas efter inlärningslägets utgång. Efter utgången behöver alternativet **Fråga användare** administratörsbehörighet för att utföra en ändring av HIPS-filtreringsläget.

HIPS-systemet övervakar händelser inne i operativsystemet och reagerar enligt reglerna som liknar dem för brandväggen. Klicka på **Redigera** bredvid **Regler** för att öppna redigeraren för **HIPS-regler**. I HIPS-regelhanteringsfönstret kan du välja, lägga till, redigera eller ta bort regler. Mer information om att skapa regler och HIPS-åtgärder finns i kapitlet Redigera en HIPS-regel.

HIPS-exkluderingar

Med exkluderingar kan du exkludera processer från djup HIPS-beteendegranskning.

Om du vill redigera HIPS-undantag ska du öppna Avancerade inställningar > **Detekteringsmotor** > **HIPS** > **HIPS** > **Undantag** > **Redigera**.

Blanda inte samman detta med exkluderade filändelser, detekteringsexkluderingar, prestandaexkluderingar eller processexkluderingar.

Om du vill undanta ett objekt klickar du på **Lägg till** och anger sökvägen till objektet eller väljer det i trädstrukturen. Du kan även redigera eller ta bort valda poster.

Avancerade inställningar för HIPS

Följande alternativ är användbara för felsökning och analys av ett programs beteende:

Drivrutiner får alltid läsas in – valda drivrutiner får alltid läsas in oavsett konfigurerat filtreringsläge om inte detta uttryckligen blockeras av en användarregel.

Logga alla blockerade åtgärder – alla blockerade åtgärder skrivs till HIPS-loggen. Använd endast den här funktionen när du felsöker eller när så begärs av ESET:s tekniska support, eftersom det kan generera en mycket stor loggfil och göra datorn långsammare.

Meddela när ändringar äger rum i startprogram – visar ett meddelande på skrivbordet varje gång ett program läggs till eller tas bort från systemstart.

Drivrutiner får alltid läsas in

Drivrutiner i den här listan får alltid läsas in oavsett HIPS-filtreringsläge om inte detta uttryckligen blockeras av en användarregel.

Lägg till – lägger till en ny drivrutin.

Redigera – redigerar en vald drivrutin.

Ta bort – tar bort en drivrutin från listan.

Återställ – läser in en uppsättning systemdrivrutiner igen.

Klicka på **Återställ** om du inte vill att manuellt tillagda drivrutiner ska inkluderas. Detta kan vara användbart om du lagt till flera drivrutiner och inte kan ta bort dem från listan manuellt.

Efter installationen är listan över drivrutiner tom. ESET Smart Security Premium fyller i listan automatiskt med tiden.

HIPS interaktivt fönster

Dialogrutan för HIPS-meddelanden gör det möjligt att skapa en regel baserad på nya åtgärder som HIPS identifierar och sedan definiera villkoren under vilka åtgärden tillåts eller avvisas.

Regler som skapas i meddelandefönstret anses vara likvärdiga med regler som skapas manuellt. En regel som skapas i ett meddelandefönster kan vara mindre specifik är regeln som utlöste dialogfönstret. Detta betyder att när en regel har skapats i dialogrutan, så kan samma åtgärd utlösa samma fönster. Läs mer i Prioritet för HIPS-regler.

Om en standardåtgärd för en regel ställs in till **Fråga varje gång** visas en dialogruta varje gång regeln utlöses. Du kan välja att **Neka** eller **Tillåta** åtgärden. Om du inte väljer en åtgärd inom angiven tid, väljs en ny åtgärd baserat på reglerna.

Kom ihåg tills programmet stängs orsakar att åtgärden (**Tillåt/Neka**) används tills regler eller filtreringslägen ändras, HIPS-modulen uppdateras eller systemet startas om. Efter någon av dessa tre åtgärder tas temporära regler bort.

Med alternativet **Skapa regel och kom ihåg permanent** skapas en ny HIPS-regel som kan ändras senare i avsnittet HIPS regelbehandling (administratörsbehörighet krävs).

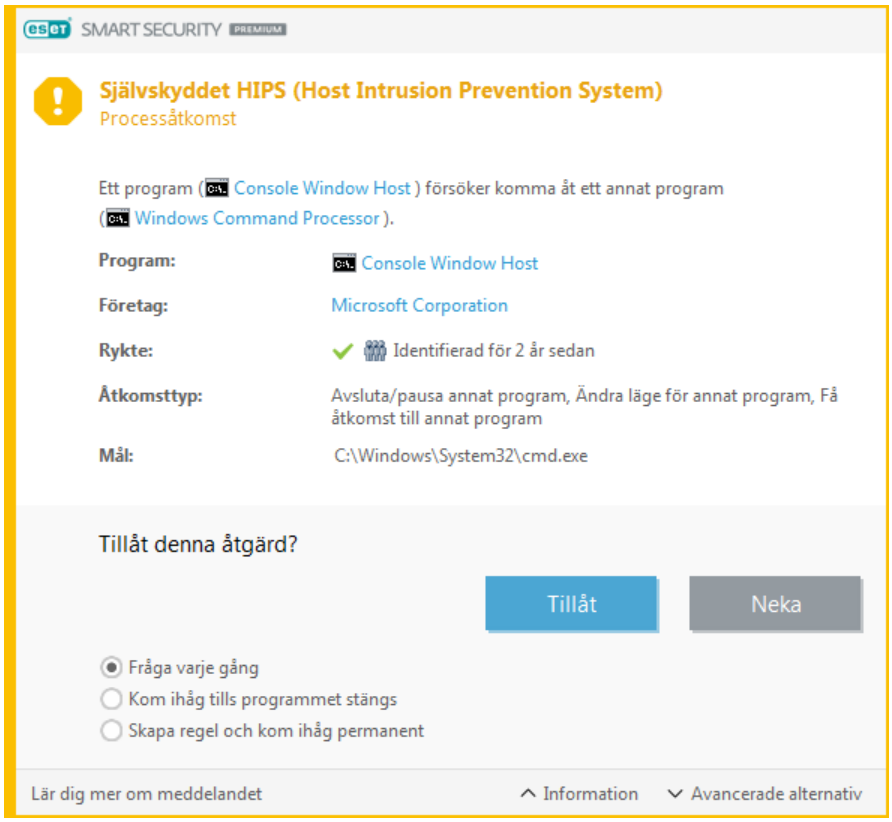
Klicka på **Information** nedtill för att se vilket program som utlöser åtgärden, vad filen har för rykte eller vilken slags åtgärd du ombeds att tillåta eller neka.

Inställningar för mer detaljerade regelparametrar kan kommas åt genom att klicka på **Avancerade alternativ**. Alternativen nedan är tillgängliga om du väljer **Skapa regel och kom ihåg permanent**:

- **Skapa en regel endast för detta program** – om du avmarkerar den här kryssrutan skapas regeln för alla källprogram.
- **Endast för åtgärd** – välj regelns fil-/program-/registeråtgärd(er). Se beskrivningar för alla HIPS-åtgärder.
- **Endast för mål** – välj regelns fil-/program-/registeråtgärd(er).

Ständiga HIPS-meddelanden?

Om du vill hindra meddelandena från att visas ska du ändra filtreringsläget till **Automatiskt** i Avancerade inställningar > **Detekteringsmotor** > **HIPS** > **HIPS**.



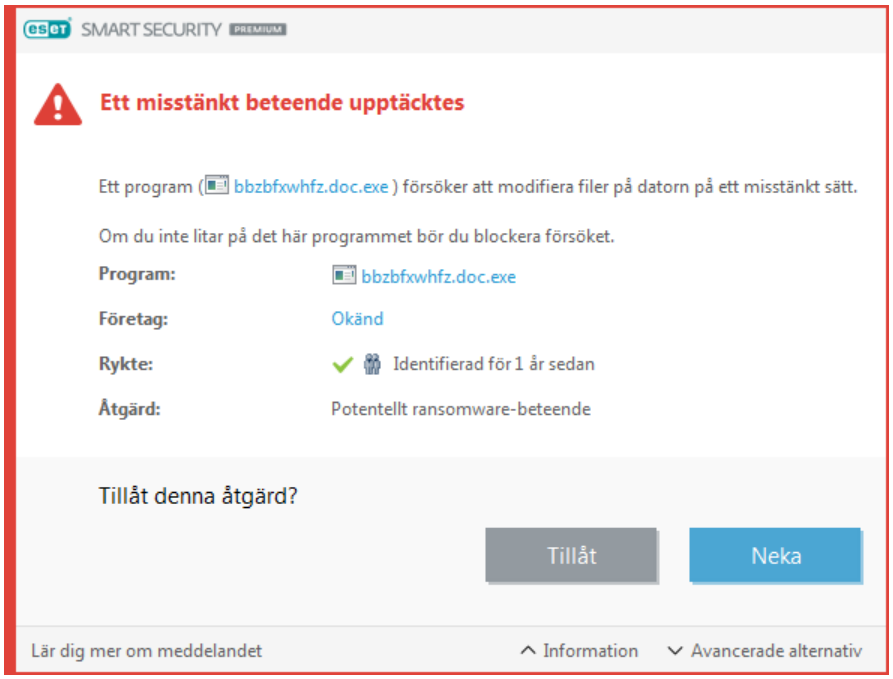
Inlärningsläge avslutat

Inlärningsläget skapar och sparar regler automatiskt. Du kan kontrollera alla skapade regler i inställningarna för HIPS-regler. Det passar bäst att använda det här läget för den inledande konfigurationen av HIPS, men det bör bara vara aktiverat under en kort tid. Ingen användarinteraktion krävs eftersom ESET Smart Security Premium sparar regler enligt fördefinierade parametrar. Undvik säkerhetsrisker genom att växla till **interaktivt** eller **principbaserat läge** när alla regler för nödvändiga processer som körs i operativsystemet har skapats.

Du kan senarelägga det här beslutet om du inte vill ändra inställningarna.

Ett potentellt ransomware-beteende upptäcktes

Det här interaktiva fönstret visas när ett potentellt ransomware-beteende upptäcks. Du kan välja att **Neka** eller **Tillåta** åtgärden.



Klicka på **Information** om du vill visa specifika detekteringsparametrar. I dialogrutan kan du **skicka in för analys** eller **undanta från detektering**.

ESET LiveGrid®E måste vara aktiverat så att skyddet mot ransomware fungerar korrekt.

HIPS regelbehandling

En lista med användardefinierade och automatiskt tillagda regler från HIPS-systemet. Ytterligare information om att skapa regler och HIPS-åtgärder finns i kapitlet HIPS-regelinställningar. Se även den allmänna principen för HIPS.

Kolumner

Regel – användardefinierat eller automatiskt valt regelnamn.

Aktiverad – inaktivera växlingsknappen om du vill behålla regeln i listan men inte använda den.

Åtgärd – regeln anger en åtgärd – **Tillåt**, **Blockera** eller **Fråga** – som utförs när villkoren uppfylls.

Källor – regeln används endast om händelsen utlöses av ett eller flera program.

Målobjekt – regeln används endast om åtgärden är relaterad till en viss fil, program eller registerpost.

Loggar allvarlighet – aktivera det här alternativet för att skriva information om regeln till HIPS-loggen.

Meddela – ett litet meddelandefönster öppnas i det nedre högra hörnet om en händelse utlöses.

Kontrollelement

Lägg till – skapar en ny regel.

Redigera – redigerar valda poster.

Ta bort – tar bort markerade poster.

Prioritet för HIPS-regler

Det finns inga alternativ för att justera prioritetsnivån för HIPS-regler med knapparna för topp/botten (jämfört med Brandväggsregler där regler tillämpas uppifrån och ned).

- Alla regler du skapar har samma prioritet
- Ju mer specifik regeln är, desto högre prioritet (till exempel har en regel för ett visst program högre prioritet än en regel för alla program)
- Internt innehåller HIPS regler med högre prioritet som inte är åtkomliga för dig (du kan till exempel inte åsidosätta regler definierade för självskydd)
- En regel du skapar som kan frysa operativsystemet tillämpas inte (får lägst prioritet)

Redigera en HIPS-regel

Se HIPS-regelhantering först.

Regelnamn – användardefinierat eller automatiskt valt regelnamn.

Åtgärd – anger en åtgärd – **Tillåt**, **Blockera** eller **Fråga** – som utförs när villkoren uppfylls.

Åtgärder som påverkar – du måste välja typ av åtgärd för vilken regeln ska gälla. Regeln används endast för denna typ av åtgärd och för valt mål.

Aktiverad – inaktivera växlingsknappen om du vill behålla regeln i listan men inte tillämpa den.

Loggar allvarlighet – aktivera det här alternativet för att skriva information om regeln till HIPS-loggen.

Meddela användare – ett litet meddelandefönster öppnas i det nedre högra hörnet om en händelse utlöses.

Regeln består av delar som beskriver villkoren som utlöser denna regel:

Källprogram – regeln används endast om händelsen utlöses av detta/dessa program. Välj **Specifika program** i listrutan och klicka på **Lägg till** om du vill lägga till nya filer, eller så kan du välja **Alla program** i listrutan om du vill lägga till alla program.

Målfiler – regeln används endast om åtgärden är relaterad till detta mål. Välj **Specifika filer** i listrutan och klicka på **Lägg till** om du vill lägga till nya filer eller mappar, eller så kan du välja **Alla filer** i listrutan om du vill lägga till alla filer.

Program – regeln används endast om åtgärden är relaterad till detta mål. Välj **Specifika program** i listrutan och klicka på **Lägg till** om du vill lägga till nya filer eller mappar, eller så kan du välja **Alla program** i listrutan om du vill lägga till alla program.

Registerposter – regeln används endast om åtgärden är relaterad till detta mål. Välj **Specifika poster** i listrutan och klicka på **Lägg till** för att skriva den manuellt, eller så kan du klicka på **Öppna registerredigerare** för att välja en nyckel i registret. Du kan även välja **Alla poster** i listrutan om du vill lägga till alla program.

> En det åtgärder i vissa regler fördefinierade av HIPS går inte att blockera och är tillåtna som standard. Inte alla systemåtgärder övervakas heller av HIPS. HIPS övervakar åtgärder som anses vara osäkra.

Beskrivning av viktiga åtgärder:

Filåtgärder

- **Ta bort fil** – programmet begär tillstånd att ta bort målfilen.
- **Skriv till fil** – programmet begär tillstånd att skriva till målfilen.
- **Direkt åtkomst till disk** – programmet försöker läsa från eller skriva till disk på ett sätt som inte är standard och kringgår vanliga procedurer i Windows. Detta kan leda till att filer ändras utan att motsvarande regler tillämpas. Denna åtgärd kan orsakas av skadlig kod som försöker undvika detektering, ett säkerhetskopieringsprogram som försöker göra en exakt kopia av disken eller en partitionshanterare som försöker omorganisera diskvolymer.
- **Installera global hook** – hänvisar till anrop av funktionen SetWindowsHookEx i MSDN-biblioteket.
- **Läs in drivrutin** – installation och inläsning av drivrutiner i systemet.

Programåtgärder

- **Felsök ett annat program** – koppla ett felsökningsprogram till processen. När programmet felsöks går det att visa och ändra detaljer i dess beteende och det går att få åtkomst till dess data.
- **Intervenera händelser från annat program** – källprogrammet försöker att fånga händelser riktade till ett visst program (till exempel ett keylogger-program som försöker fånga webbläsarhändelser).
- **Avsluta/pausa annat program** – pausar eller återupptar eller avslutar en process (åtkomst direkt från

Process Explorer eller fönstret Processer).

• **Starta nytt program** – starta nya program eller processer.

• **Ändra läge för annat program** – källprogrammet försöker skriva till målprogrammets minne eller körningskod för dess räkning. Denna funktion är användbar för att skydda ett viktigt program genom att konfigurera det som ett målprogram i en regel som blockerar användning av denna åtgärd.

Registeråtgärder

• **Ändra startinställningar** – ändringar i inställningar som definierar vilka program som körs när Windows startar. Dessa går till exempel att hitta genom att söka efter nyckeln Run i Windows register.

• **Ta bort från registret** – tar bort en registernyckel eller dess värde.

• **Byt namn på registernyckel** – byter namn på registernyckelarna.

• **Ändra register** – skapar nya värden till registernycklar, ändrar befintliga värden, flyttar data i databasträdet eller ställer in användar- eller gruppbehörighet för registernycklar.

Det går att använda jokertecken med vissa begränsning när ett mål anges. Det går att använda * (asterisk) i registersökvägar i stället för en viss nyckel. Till exempel *HKEY_USERS*\software* kan betyda *HKEY_USER\.default\software*, men inte *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
*HKEY_LOCAL_MACHINE\system\ControlSet** är inte en giltig registernyckelsökväg. En registernyckelsökväg innehåller * betyder "denna sökväg eller någon annan sökväg på alla nivåer efter den symbolen". Detta är endast sättet att använda jokertecken för filmål. Först utvärderas en viss del av sökvägen, sedan sökvägen som följer jokertecknet (*).

Om du skapar en mycket generisk regel visas varningen om den här typen av regel.

I följande exempel visar vi hur oönskat beteende i ett visst program kan begränsas:

1. Namnge regeln och välj **Blockera** (eller **Fråga** om du föredrar att välja senare) från rullgardinsmenyn **Åtgärd**.

2. Aktivera växlingsknappen bredvid **Meddela användare** för att visa ett meddelande när en regel tillämpas.

3. Välj minst en åtgärd för regeln i avsnittet **Åtgärder som påverkar** som regeln ska tillämpas på.

4. Klicka på **Nästa**.

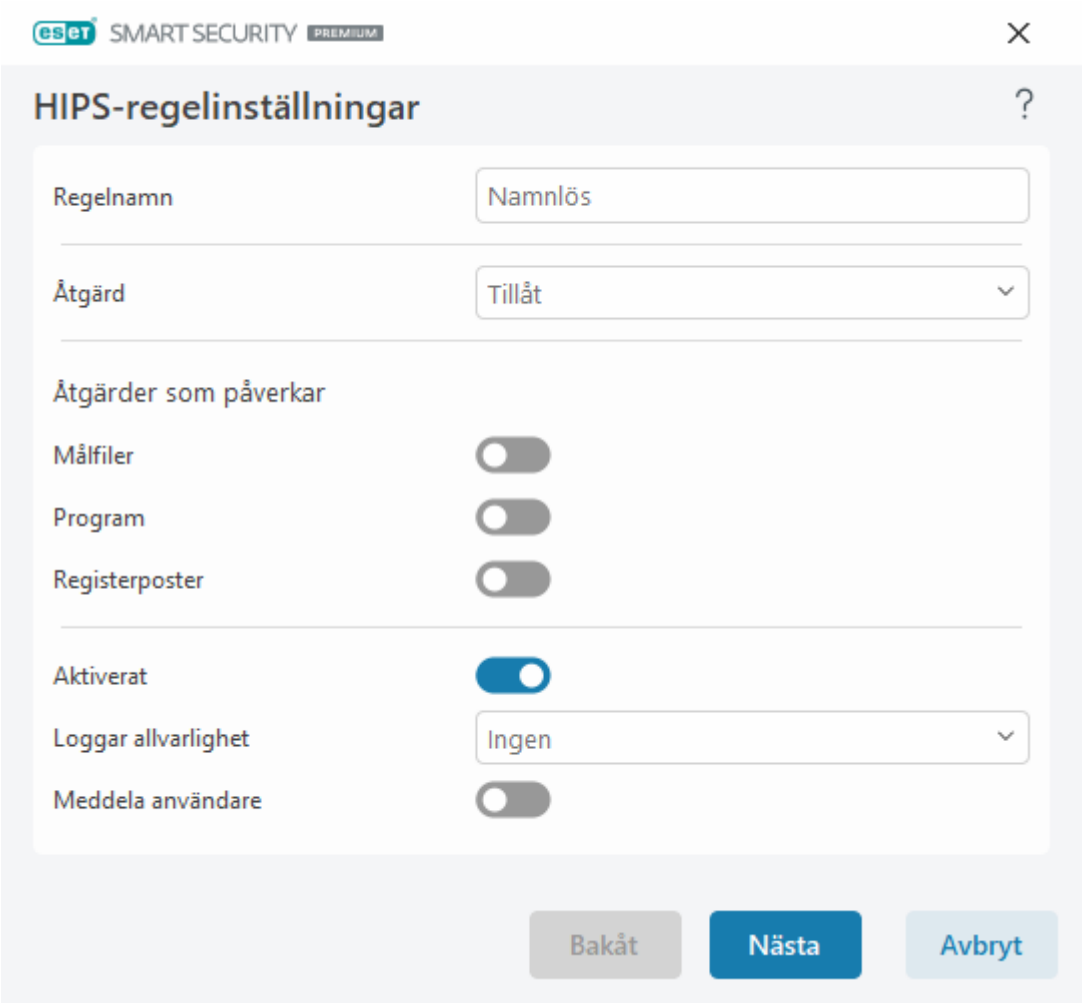
5. I fönstret **Källprogram** väljer du **Specifika program** i listrutan om du vill tillämpa den nya regeln på alla program som försöker utföra någon av de valda programåtgärderna på de program du angett.

6. Klicka på **Lägg till** och sedan **...** för att välja en sökväg till ett visst program och tryck sedan på **OK**. Lägg till fler program om du vill.
Till exempel: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Välj åtgärden **Skriv till fil**.

8. Välj **Alla filer** i listrutan. Då blockeras alla försök att skriva till några filer av det eller de valda programmen från föregående steg.

9. Klicka på **Slutför** för att spara den nya regeln.



Lägg till program-/registersökväg för HIPS

Välj en filsökväg till ett program genom att klicka på alternativet **...**. Väljs en mapp, inkluderas alla program på denna plats.

Alternativet **Öppna registerredigerare** startar Windows registerredigerare (regedit). Lägger du till en registersökväg, ange korrekt plats i fältet **Värde**.

Exempel på fil- eller registersökvägar:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Uppdatera

Alternativ för uppdateringsinställningar finns i Avancerade inställningar > **Uppdatera**. Detta avsnittet anger information om uppdateringskällan, t.ex. uppdateringsservrar och deras autentiseringsuppgifter.

Uppdatera

Den uppdateringsprofil som för närvarande används visas i listrutan **Välj standardprofil för uppdateringar**.

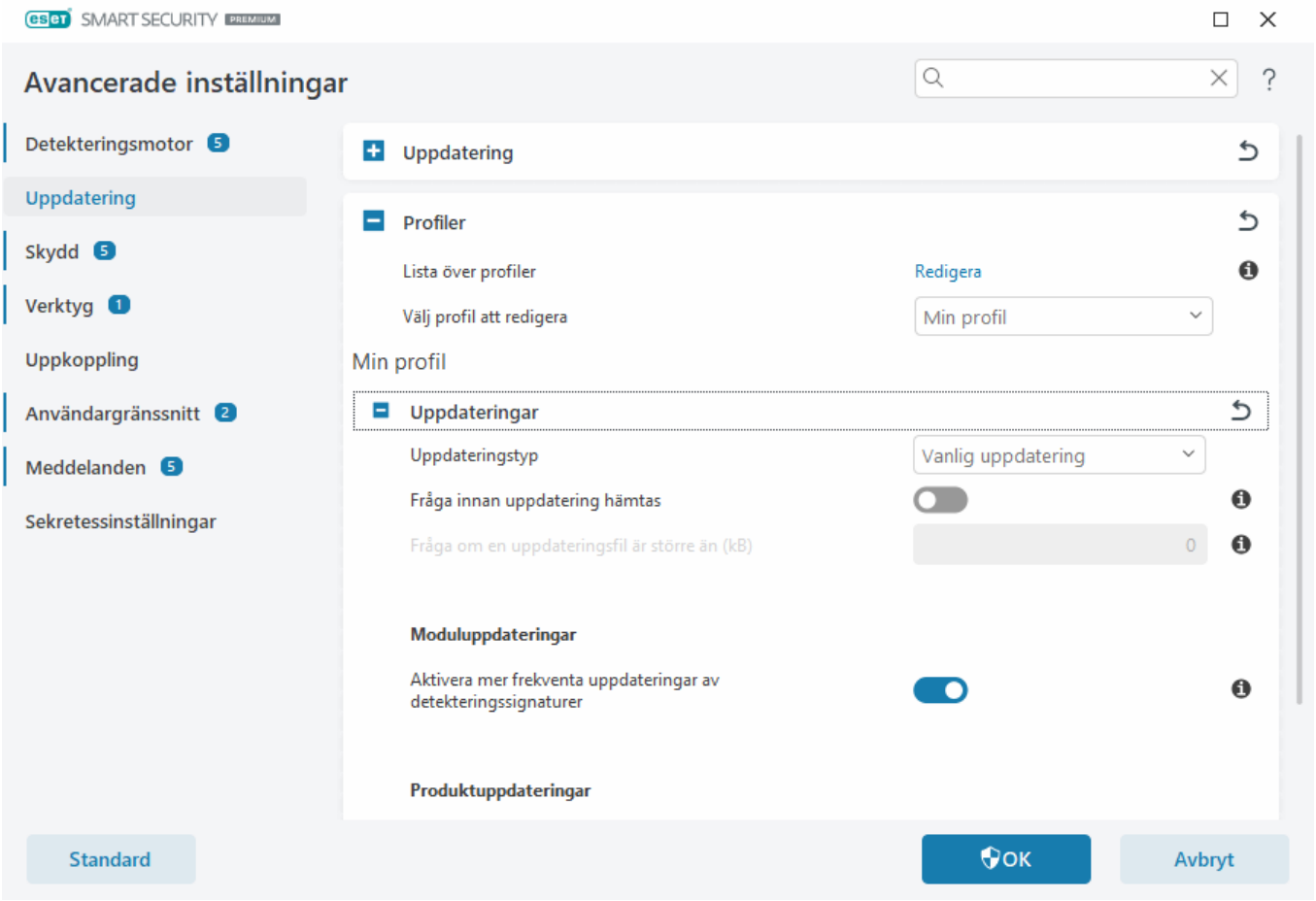
Se avsnittet Uppdateringsprofiler om du vill skapa en ny profil.

Automatiskt profilbyte – gör att du kan tilldela en uppdateringsprofil till en specifik nätverksanslutningsprofil.

Om det uppstår problem vid hämtning av uppdateringar av detekteringsmotorn eller moduler ska du klicka på **Rensa** bredvid **Rensa uppdateringscache** för att ta bort temporära uppdateringsfiler/cache.

Modulåterställning

Misstänker du att en ny uppdatering av detekteringsmotorn och/eller programmodulerna är instabila eller skadade, går det att återställa till den föregående versionen och inaktivera uppdateringar under en viss tidsperiod.



Det är mycket viktigt att du fyller i alla uppdateringsparametrar korrekt för att uppdateringarna ska hämtas korrekt. Om du använder en brandvägg, kontrollera att ESET-programmet kan kommunicera med Internet (t.ex. HTTP-kommunikation).

Profiler

Uppdateringsprofiler skapas för olika uppdateringskonfigurationer och -aktiviteter. Att skapa uppdateringsprofiler är särskilt användbart för mobila användare som behöver skapa en alternativ profil för anslutningsegenskaper till internet som regelbundet ändras.

Rullgardinsmenyn **Välj profil att redigera** visar den aktuella profilen och är inställd på **Min profil** som standard. Skapa en ny profil genom att klicka på **Redigera** intill **Lista över profiler**, ange ett eget **Profilnamn** och klicka sedan på **Lägg till**.

Uppdateringar

Som standard är **Uppdateringstypen** inställd på **Vanlig uppdatering** för att säkerställa att uppdateringsfiler hämtas automatiskt från ESET-servern med minst nätverkstrafik. Testlägesuppdateringar (alternativet **Testläge**) är uppdateringar som har genomgått grundlig intern testning och snart är allmänt tillgängliga. Du kan dra fördel av att ha tillgång till de senaste identifieringsmetoderna och korrigeringarna genom att aktivera testläge. Testläget är inte alltid stabilt och FÅR INTE användas på produktionsservrar och arbetsstationer där maximal åtkomst och stabilitet krävs.

Fråga innan uppdatering hämtas – en avisering visas där du kan välja att bekräfta eller neka hämtningar av uppdateringsfiler.

Fråga om en uppdateringsfil är större än (kB) – en bekräftelseruta visas om uppdateringsfilen är större än det angivna värdet. Om uppdateringsfilens storlek är inställd på 0 kB visas alltid en bekräftelseruta.

Uppdatera moduler

Aktivera mer frekventa uppdateringar av detekteringssignaturer – detekteringssignaturer uppdateras oftare. Om alternativet inaktiveras kan detekteringshastigheten försämras.

Produktuppdateringar

Uppdateringar av programfunktioner – installera automatiskt nya versioner av ESET Smart Security Premium.

Anslutningsalternativ

Om du vill använda en proxyserver för hämtning av uppdateringar tittar du i avsnittet Anslutningsalternativ.

Ångra uppdatering

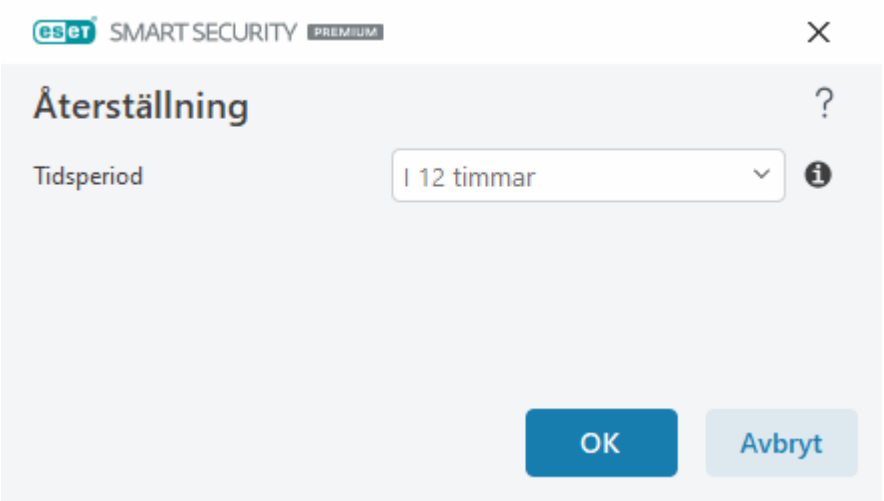
Misstänker du att en ny uppdatering av detekteringsmotorn eller programmodulerna är instabila eller skadade, går det att återställa till den föregående versionen och tillfälligt inaktivera uppdateringar. Det går även att aktivera tidigare inaktiverade uppdateringar och du sköt upp dem på obestämd tid.

ESET Smart Security Premium registrerar avbildninger av detekteringsmotorn och programmodulerna för användning med återställningsfunktionen. Om du vill skapa virusdatabasavbildninger behåller du **Skapa avbildninger av moduler** aktiverat. När **Skapa avbildninger av moduler** är aktiverat skapas den första avbildningen under den första uppdateringen. Nästa skapas efter 48 timmar. Fältet **Antal lokalt lagrade avbildninger** definierar antalet lagrade avbildninger av detektionsmotorn.

> i När den maximala mängden avbildninger nås (till exempel tre) ersätts den äldsta avbildningen med en ny avbildning var 48:e timme. ESET Smart Security Premium återställer uppdateringar av detekteringsmotor- och programmodulversioner till den äldsta avbildningen.

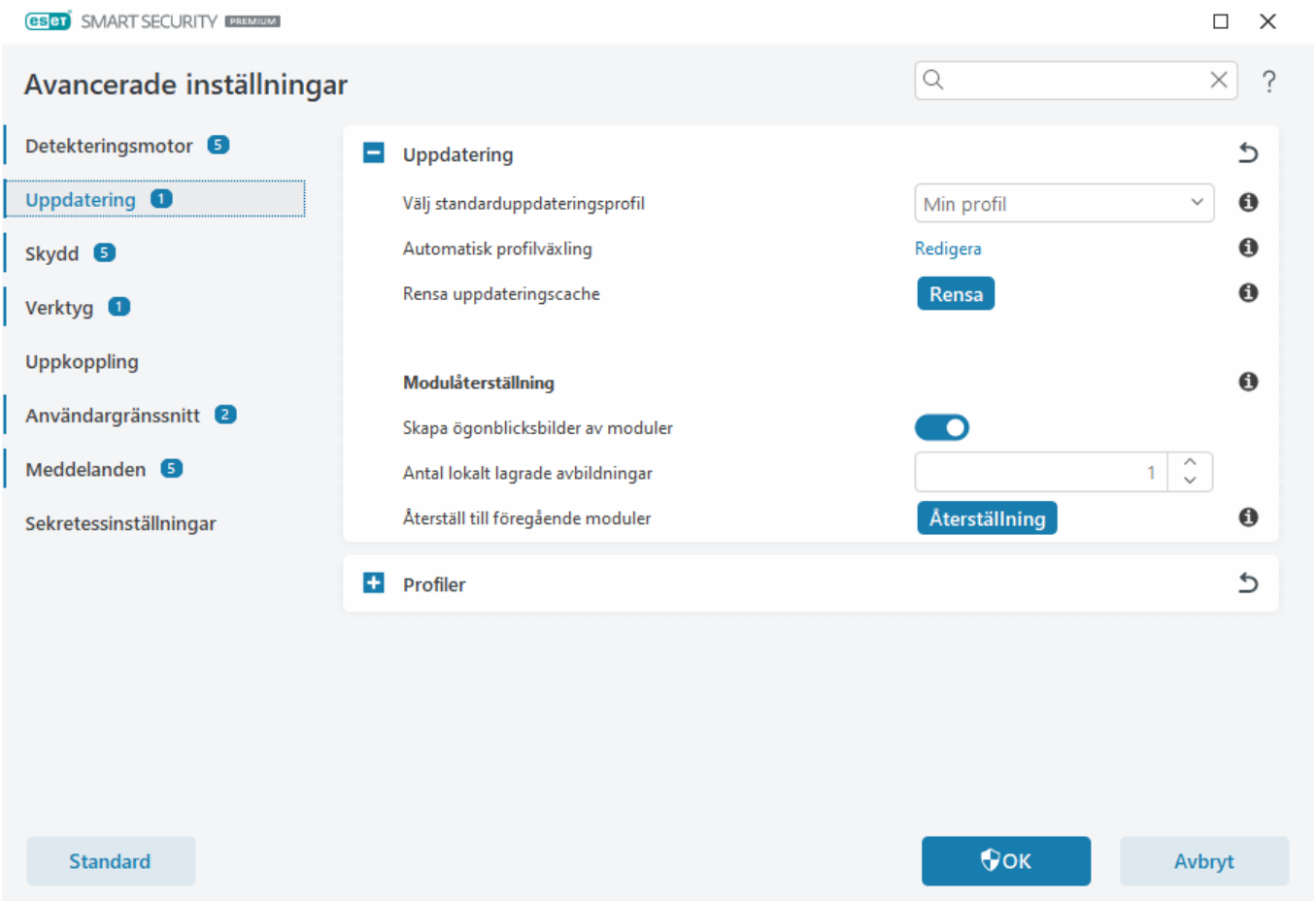
Om du klickar på **Återställ** i Avancerade inställningar > **Uppdatera** > **Uppdatera**) måste du välja ett tidsintervall i

listrutan **Tidsperiod** som representerar en tidsperiod under vilken uppdateringarna av detekteringsmotorn och programmodulerna pausas.



Markera **Tills återkallad** för att skjuta upp regelbundna uppdateringar på obestämd tid till du återställer uppdateringsfunktionen manuellt. ESET rekommenderar inte detta alternativ eftersom det är en potentiell säkerhetsrisk.

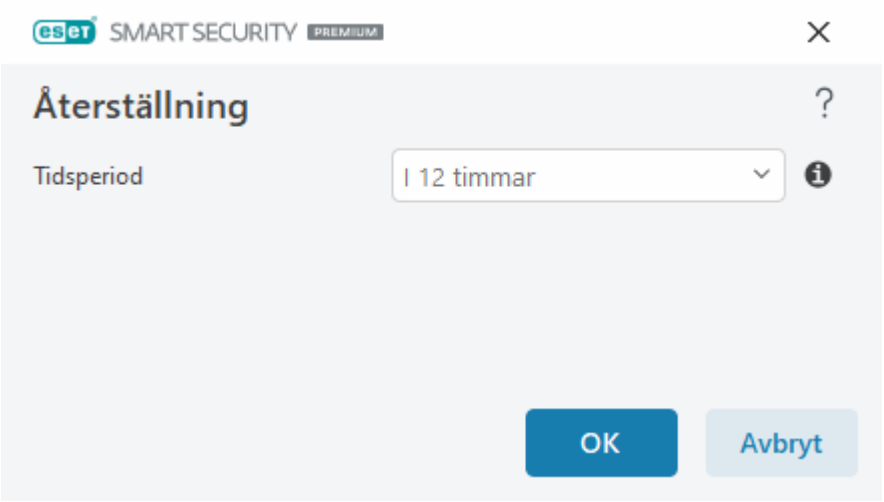
Om en återställning utförs ändras knappen **Återställ** till **Tillåt uppdateringar**. Uppdateringar tillåts inte under tidsintervallet som väljs på rullgardinsmenyn **Pausa uppdateringar**. Detekteringsmotorns version nedgraderas till den äldsta tillgängliga versionen och lagras som en avbildning i den lokala datorns filsystem.



Anta att 22700 är detekteringsmotorns senaste version, och 22698 och 22696 är lagrade som avbildningar av detekteringsmotorn. Observera att 22697 inte är tillgänglig. I det här exemplet var datorn avstängd under 22697-uppdateringen och en nyare uppdatering gjordes tillgänglig innan 22697 hämtades. Om fältet **Antal lokalt lagrade avbildningar** är två och du klickar på **Återställ**, så återställs detekteringsmotorn (inklusive programmoduler) till versionsnummer 22696. Detta kan ta en stund. Kontrollera om detekteringsmotorns version har nedgraderats på skärmen Uppdatering.

Tidsintervall för återställning

Om du klickar på **Återställ** i Avancerade inställningar > **Uppdatera** > **Uppdatera**) måste du välja ett tidsintervall i listrutan **Tidsperiod** som representerar en tidsperiod under vilken uppdateringarna av detekteringsmotorn och programmodulerna pausas.



Markera **Tills återkallad** för att skjuta upp regelbundna uppdateringar på obestämd tid till du återställer uppdateringsfunktionen manuellt. ESET rekommenderar inte detta alternativ eftersom det är en potentiell säkerhetsrisk.

Produktuppdateringar

I avsnittet **Produktuppdateringar** kan du installera nya funktionsuppdateringar automatiskt när de är tillgängliga.

Uppdateringar av programfunktioner ger nya funktioner eller ändrar de som redan finns från tidigare versioner. Den kan utföras automatiskt utan att du behöver göra något, eller så kan du välja att få ett meddelande. När en uppdatering av en programfunktion har installerats kan en omstart av datorn krävas.

Uppdateringar av programfunktioner – när det här alternativet är aktiverat utförs uppdateringar av programfunktioner automatiskt.

Anslutningsalternativ

Om du vill komma åt proxyserverns inställningsalternativ för en specifik uppdateringsprofil ska du öppna Avancerade inställningar > **Uppdatera** > **Profiler** > **Uppdateringar** > **Anslutningsalternativ**. Klicka på listrutan **Proxyläge** och välj ett följande tre alternativ:

- Använd inte proxyserver
- Anslutning via en proxyserver
- Använd globala inställningar för proxyserver

Välj **Använd globala proxyserverinställningar** om du vill använda proxyserverns konfigurationsalternativ som redan angivits i Avancerade inställningar > **Anslutning** > **Proxyserver**.

Välj **Använd inte proxyserver** för att ange att ingen proxyserver ska användas för att uppdatera ESET Smart Security Premium.

Alternativet **Anslutning via en proxyserver** ska väljas om:

- En annan proxyserver än den som angetts i Avancerade inställningar > **Uppkoppling** används för att uppdatera ESET Smart Security Premium. I den här konfigurationen ska information för den nya proxyn anges under **proxyserverns** adress, **port** för kommunikation (3128 som standard) samt **användarnamn** och **lösenord** för proxyservern om så krävs.
- Proxyserverns inställningar inte ställts in globalt, utan ESET Smart Security Premium ansluter till en proxyserver för uppdateringar.
- Datorn är ansluten till Internet via en proxyserver. Inställningarna tas från Internet Explorer under programinstallationen, men om de ändras senare (till exempel om du ändrar din leverantör), kontrollera att proxyinställningarna är korrekta i det här fönstret. Annars kan inte programmet ansluta till uppdateringsservern.

Standardalternativet för proxyservern är **Använd globala inställningar för proxyserver**.

Använd direktanslutning om proxy inte är tillgänglig – proxyn åsidosätts under uppdatering om den inte kan nås.

Fälten **Användarnamn** och **Lösenord** i det här avsnittet är specifika för proxyservern. Fyll endast i de här fälten om användarnamn och lösenord krävs för åtkomst till proxyservern. Dessa fält fylls endast i om du vet att du behöver ett lösenord för åtkomst till internet genom en proxyserver.

Skydd

Skydd skyddar mot skadliga systemangrepp genom att fil-, e-post- och internetkommunikation kontrolleras. Om till exempel ett objekt som är klassificerat som skadlig kod detekteras, så vidtas en åtgärd. Skydd kan eliminera det genom att blockera det och sedan rensa, ta bort eller sätta det i karantän.

Om du vill konfigurera skydden i detalj ska du öppna Avancerade inställningar > **Skydd**.

Endast en erfaren användare bör ändra Skydd. Om felaktiga inställningar görs kan skyddet försämras.

I det här avsnittet:

- Svar på detektering
- Rapporteringsinställningar

- Skyddsinställningar

Svar på detektering

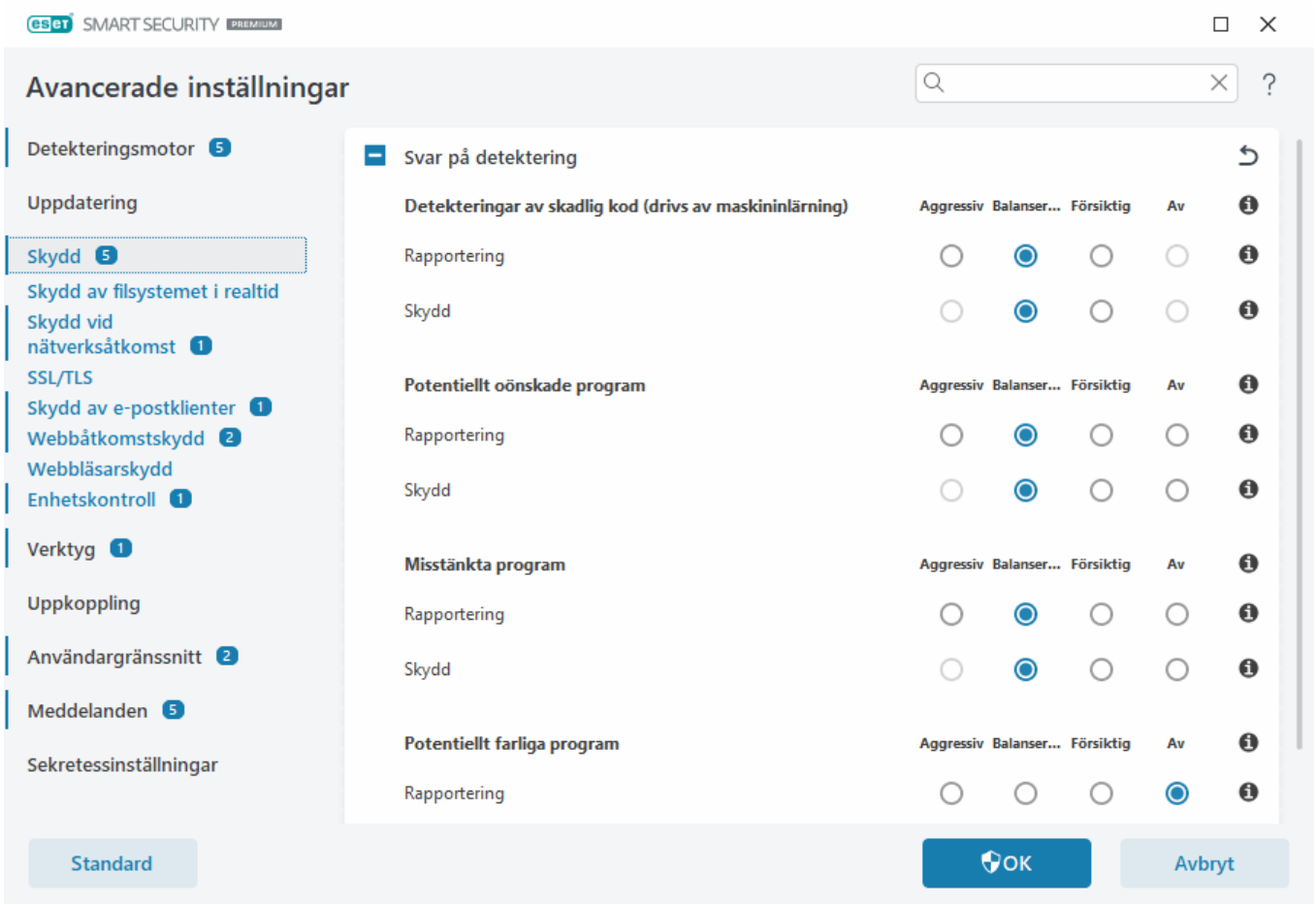
Med Detekteringssvar kan du konfigurera rapporterings- och skyddsnivåer för följande kategorier:

- **Detekteringar av skadlig kod (drivs av maskininlärning)** – Ett datorvirus är ett stycke skadlig kod som läggs till befintliga filer på din dator. Begreppet ”virus” används dock ofta slarvigt. ”Malware” (skadlig kod) är en mer exakt term. Identifiering av skadlig kod utförs av detekteringsmotormodulen i kombination med maskininlärningskomponenten. Läs mer om dessa programtyper i ordlistan.

- **Potentiellt oönskade program** – grayware eller potentiellt oönskade program (PUA; potentially unwanted application) är en bred kategori programvara vars syfte inte är direkt skadligt, till skillnad från andra typer av skadlig kod, som virus eller trojaner. De kan dock installera ytterligare oönskad programvara, ändra digitala enheters beteenden eller utföra aktiviteter som inte är godkända eller inte förväntas av användaren. Läs mer om dessa programtyper i ordlistan.

- **Misstänkta program** – inkluderar program som komprimerats med packers eller skydd. Dessa typer av skydd utnyttjas ofta av skadlig kod för att undvika upptäckt.

- **Potentiellt farliga program** – avser kommersiell programvara som kan missbrukas i skadliga syften. Exempel på sådana potentiellt farliga program (PUA) är verktyg för fjärråtkomst, program som spårar lösenord och keylogger-program (program som registrerar varje tangent användaren trycker ned). Läs mer om dessa programtyper i ordlistan.



> **Förbättrat skydd**
> Avancerad maskininlärning ingår nu som en del av skydden som ett avancerat skyddslager som förbättrar detekteringen baserat på maskininlärning. Läs mer om den här typen av skydd i ordlistan.

Rapporteringsinställningar

När en detektering görs (till exempel att ett hot hittas och klassificeras som skadlig kod) registreras informationen i detekteringsloggen och det visas meddelanden på skrivbordet om detta har konfigurerats i ESET Smart Security Premium.

Rapporteringströskelvärdet konfigureras för varje kategori (benämnd ”KATEGORI”):

1. Detekteringar av skadlig kod
2. Potentiellt oönskade program
3. Potentiellt farliga
4. Misstänkta program

Rapportering görs med detekteringsmotorn, inklusive maskininlärningskomponenten. Det går att ställa in ett högre rapporteringströskelvärde än det aktuella tröskelvärdet för skydd. Dessa rapporteringsinställningar påverkar inte blockering, rensning eller borttagning av objekt.

Läs följande innan du ändrar ett tröskelvärde (eller nivå) för KATEGORI-rapportering:

Tröskelvärde	Förklaring
Aggressiv	KATEGORI-rapportering är inställd på maximal känslighet. Fler detekteringar rapporteras. Inställningen **Aggressiv** kan felaktigt identifiera objekt som KATEGORI.
Balanserad	KATEGORI-rapportering är inställd på balanserad. Den här inställningen är optimerad för att balansera prestanda och tillförlitligheten hos detekteringsfrekvenser och antalet felaktigt rapporterade objekt.
Försiktig	KATEGORI-rapportering är inställd för att minimera antalet felaktigt identifierade objekt samtidigt som en tillräcklig skyddsnivå bibehålls. Objekt rapporteras endast när sannolikheten är uppenbar och matchar KATEGORI-beteendet.
Av	KATEGORI-rapportering är inte aktiv och detekteringar av den här typen varken hittas, rapporteras eller rensas. Med den här inställningen inaktiveras därför skydd mot den här detekteringstypen. Av är inte tillgängligt för rapportering av skadlig kod and är standardvärdet för potentiellt farliga program.

Tillgänglighet för ESET Smart Security Premium-skyddsmoduler

Tillgängligheten (aktiverad eller inaktiverad) för en skyddsmodul för ett valt KATEGORI-tröskelvärde är följande:

	Aggressiv	Balanserad	Försiktig	Av*
Modul för avancerad maskininlärning	✓ (aggressivt läge)	✓ (konservativt läge)	X	X
Modul för detekteringsmotor	✓	✓	✓	X
Andra skyddsmoduler	✓	✓	✓	X

* Inte rekommenderat.

Fastställa produktversion, programmodulers versioner och versionsdatum

1. Klicka på **Hjälp och support** > **Om ESET Smart Security Premium**.
2. ESET-produktens versionsnummer står på den första textraden på skärmen **Om**.
3. Klicka på **Installerade komponenter** för information om specifika moduler.

Att tänka på

Tänk på följande när ett lämpligt tröskelvärde väljs för din miljö:

- Tröskelvärdet **Balanserad** rekommenderas för de flesta konfigurationer.
- Ju högre tröskelvärde för rapportering, desto högre detekteringsgrad, men även högre risk för felaktigt identifierade objekt.
- I realiteten finns det ingen garanti för en 100 %-ig detekteringsgrad och det går aldrig helt att utesluta felaktig kategorisering av rena objekt som skadlig kod.
- Håll ESET Smart Security Premium och dess moduler uppdaterade för att maximera balansen mellan prestanda och tillförlitliga detekteringsgrader och antalet felaktigt rapporterade objekt.

Skyddsinställningar

Om ett objekt klassificerat som KATEGORI rapporteras, så blockeras objektet av programmet som sedan rensar, tar bort eller sätter det i karantän.

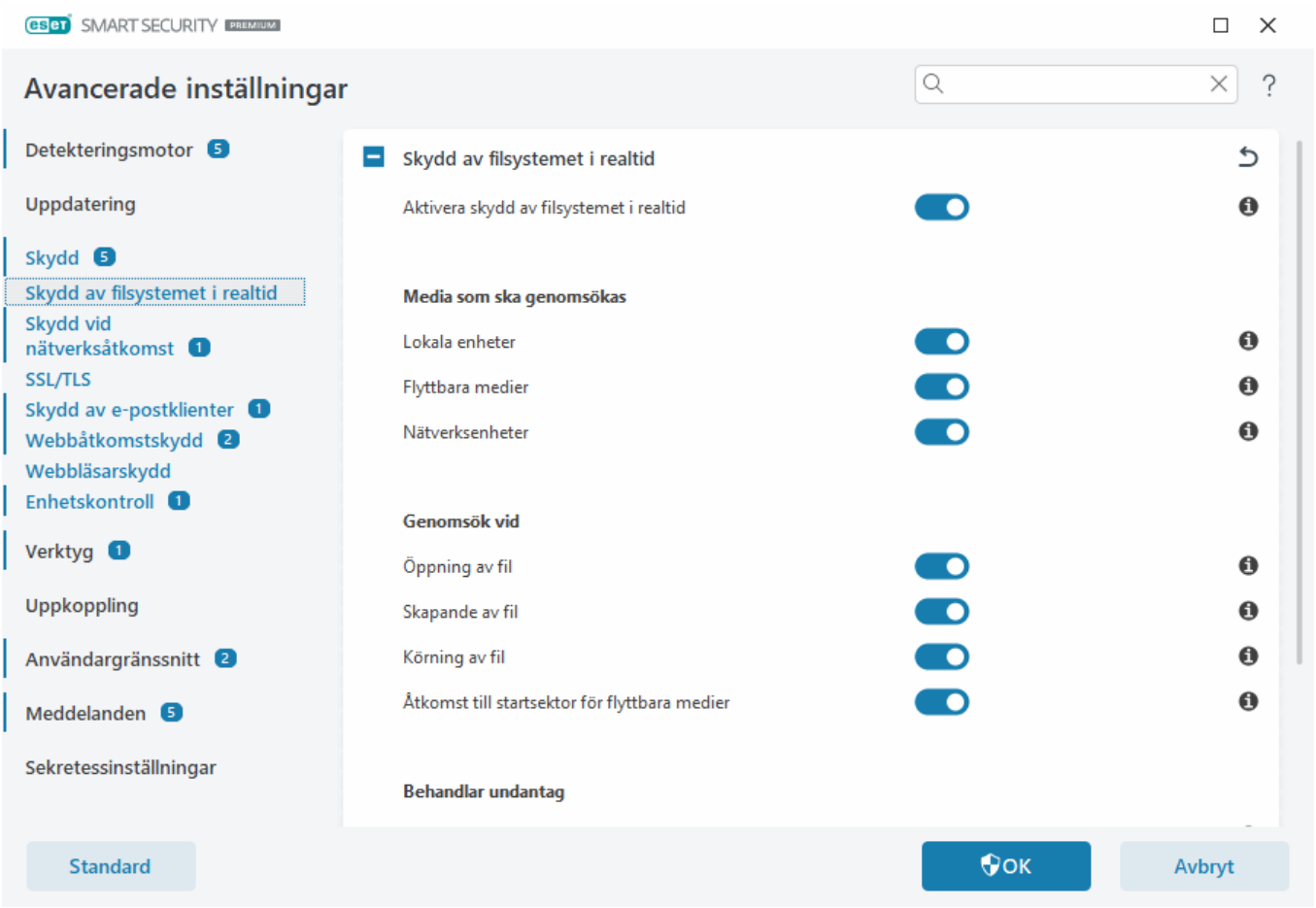
Läs följande innan du ändrar ett tröskelvärde (eller nivå) för KATEGORI-skydd:

Tröskelvärde	Förklaring
Aggressiv	Rapporterade detekteringar på aggressiv (eller lägre) nivå blockeras och en automatisk åtgärd (det vill säga rensning) startas. Den här inställningen rekommenderas när alla endpoints har genomsökts med aggressiva inställningar och felaktigt rapporterade objekt har lagts till som detekteringsundantag.
Balanserad	Rapporterade detekteringar på balanserad (eller lägre) nivå blockeras och en automatisk åtgärd (det vill säga rensning) startas.
Försiktig	Rapporterade detekteringar på försiktig nivå blockeras och en automatisk åtgärd (det vill säga rensning) startas.

Tröskelvärde	Förklaring
Av	Detta är användbart för att identifiera och utesluta felaktigt rapporterade objekt. Av är inte tillgängligt för skydd mot skadlig kod and är standardvärdet för potentiellt farliga program.

Skydd av filsystemet i realtid

Skyddet av filsystemet i realtid kontrollerar alla filer i systemet beträffande skadlig kod när de öppnas, skapas eller körs.



Skydd av filsystemet i realtid startas som standard när systemet startas och ger oavbruten genomsökning. Vi rekommenderar inte att **Aktivera skydd av filsystemet i realtid** inaktiveras i Avancerade inställningar > **Skydd** > **Skydd av filsystemet i realtid** > **Skydd av filsystemet i realtid** .

Media som ska genomsökas

Som standard kontrolleras alla mediatyper efter potentiella hot:

- **Lokala enheter** – genomsöker alla system- och fasta hårddiskar (exempel: *C:*\, *D:*\).
- **Flyttbara medier** – genomsöker CD/DVD, USB-minnen, minneskort och så vidare.
- **Nätverksenheter** – genomsöker alla mappade nätverksenheter (exempel: *H:*\ som *store04*) eller nätverksenheter med direktåtkomst (exempel: *store08*).

Vi rekommenderar att du använder standardinställningarna och endast ändrar dem i speciella fall, till exempel om kontroll av vissa media gör att dataöverföring går betydligt långsammare.

Genomsök vid

Som standard genomsöks alla filer när de öppnas, skapas eller körs. Vi rekommenderar att behålla standardinställningarna eftersom de ger datorn ett maximalt realtidsskydd:

- **Öppning av fil** – genomsöker när en fil öppnas.
- **Skapande av fil** – genomsöker när en fil skapas eller ändras.
- **Körning av fil** – genomsöker när en fil körs.
- **Åtkomst till startsektor för flyttbara medier** – när flyttbara medier som innehåller en startsektor sätts in i enheten genomsöks startsektorn omedelbart. Alternativet aktiverar inte genomsökning av filer på flyttbara medier. Genomsökning av filer på flyttbara medier finns i **Media som ska genomsökas** > **Flyttbara medier**. För att **Åtkomst till startsektor på flyttbara medier** ska fungera korrekt ska **Startsektorer/UEFI** aktiveras i ThreatSense.

Behandlar undantag

Se Behandlar undantag.

ThreatSense

Skydd av filsystemet i realtid kontrollerar alla typer av media och utlöses av olika systemhändelser som t.ex. åtkomst till en fil. Med **ThreatSense**-teknikens detekteringsmetoder (beskrivs i avsnittet ThreatSense) kan Skydd av filsystemet i realtid konfigureras så att det hanterar nya filer på annat sätt än befintliga filer. Det går till exempel att konfigurera skydd av filsystemet i realtid så att det övervakar nyskapade filer mer noga.

För att använda så lite systemresurser som möjligt under realtidsskyddet kommer filer som redan genomsökts inte att genomsökas igen (om de inte har modifierats). Filerna genomsöks igen omedelbart efter varje uppdatering av detekteringsmotorn. Detta beteende kontrolleras med **Smart optimering**. Om **Smart optimering** är inaktiverat genomsöks filerna varje gång de används. Om du vill ändra den här inställningen ska du öppna Avancerade inställningar > **Skydd** > **Skydd av filsystemet i realtid**. Klicka på **ThreatSense** > **Andra** och markera eller avmarkera **Aktivera Smart optimering**.

Med Skydd av filsystemet i realtid kan du också konfigurera Ytterligare parametrar för ThreatSense.

Behandlar undantag

Med funktionen för processundantag kan du undanta programprocesser från skyddet av filsystemet i realtid. För att förbättra säkerhetskopieringens hastighet, processintegritet och tjänstens tillgänglighet används viss teknik som är känd för att stå i konflikt med skyddet mot skadlig kod på filnivå under säkerhetskopiering. Det enda effektiva sättet att undvika båda situationerna är att inaktivera programmet som skyddar mot skadlig kod. Genom att undanta vissa processer (till exempel dem i säkerhetskopieringslösningen) ignoreras alla filåtgärder som tillhör sådana undantagna processer och anses vara säkra, så att säkerhetskopieringsprocessen störs så lite som möjligt. Vi rekommenderar att du skapar undantag med försiktighet – ett säkerhetskopieringsverktyg som har undantagits kan komma åt infekterade filer utan att någon varning ges och därför tillåts utökade behörigheter endast i

modulen för realtidsskydd.

Blanda inte samman detta med exkluderade filändelser, HIPS-exkluderingar, detekteringsexkluderingar eller prestandaexkluderingar.

Processexkluderingar bidrar till att minimera risken för potentiella konflikter och förbättra prestanda för exkluderade program, vilket i sin tur har en positiv effekt på operativsystemets prestanda och stabilitet överlag. En exkludering av en process/ett program är en exkludering av dess körbara fil (*.exe*).

Du kan lägga till körbara filer i listan över undantagna processer i Avancerade inställningar > Skydd av **Skydd** > **Skydd av filsystemet i realtid** > **Skydd av filsystemet i realtid** > **Processexkluderingar**.

Den här funktionen är utformad för att undanta säkerhetskopieringsverktyg. Att undanta säkerhetskopieringsverktygets process från genomsökning inte bara säkerställer systemstabiliteten, utan påverkar inte heller säkerhetskopieringens prestanda eftersom säkerhetskopieringen inte saktas ned när den körs.

Klicka på **Redigera** för att öppna hanteringsfönstret **Processundantag**, där du kan lägga till exkluderingar och bläddra efter körbara filer (till exempel *Backup-tool.exe*) som ska undantas från genomsökning. Så snart *.exe*-filen har lagts till i undantaget övervakas inte den här processens aktivitet av ESET Smart Security Premium och ingen genomsökning görs av några filåtgärder som utförs av den här processen.

Om du inte använder bläddringsfunktionen när du väljer den körbara filen behöver du ange hela sökvägen till den manuellt. Annars fungerar inte undantaget korrekt och HIPS kan rapportera fel.

Du kan även **redigera** befintliga processer eller **ta bort** dem från undantagen.

Webbåtkomstskyddet beaktar inte det här undantaget, så hämtade filer genomsöks även om du undantar den körbara filen för din webbläsare. På så vis kan infiltrationer fortfarande upptäckas. Det här scenariot är endast ett exempel och vi rekommenderar inte att du skapar undantag för webbläsare.

Lägg till eller redigera processexkluderingar

I det här dialogfönstret kan du **lägga till** processer som ska exkluderas från detekteringsmotorn. Processexkluderingar bidrar till att minimera risken för potentiella konflikter och förbättra prestanda för exkluderade program, vilket i sin tur har en positiv effekt på operativsystemets prestanda och stabilitet överlag. En exkludering av en process/ett program är en exkludering av dess körbara fil (*.exe*).

Välj filsökvägen för ett undantaget program genom att klicka på ... (till exempel *C:\Program Files\Firefox\Firefox.exe*). Ange INTE programmets namn. Så snart *.exe*-filen har lagts till i undantaget övervakas inte den här processens aktivitet av ESET Smart Security Premium och ingen genomsökning görs av några filåtgärder som utförs av den här processen.

Om du inte använder bläddringsfunktionen när du väljer den körbara filen behöver du ange hela sökvägen till den manuellt. Annars fungerar inte undantaget korrekt och HIPS kan rapportera fel.

Du kan även **redigera** befintliga processer eller **ta bort** dem från undantagen.

Ändring av konfiguration för realtidsskydd

Realtidsskyddet är den viktigaste komponenten för att upprätthålla ett säkert system. Var alltid försiktig när dessa parametrar ändras. Vi rekommenderar att endast ändra dessa inställningar under vissa förutsättningar.

Efter installation av ESET Smart Security Premium optimeras alla inställningar så att användarna får ett maximalt systemskydd. Om du vill återställa standardinställningarna ska du klicka på bredvid Avancerade inställningar > **Skydd** > **Detekteringssvar**.

Kontroll av realtidsskyddet

Kontrollera att realtidsskyddet fungerar och identifierar virus med hjälp av en testfil från *www.eicar.com*. Den här testfilen är en ofarlig fil som identifieras av alla antivirusprogram. Filen skapades av EICAR (European Institute for Computer Antivirus Research) för test av funktionaliteten i antivirusprogram.

Det går att hämta filen på http://www.eicar.org/download/eicar.com
När den här webbadressen har angetts i webbläsaren ska ett meddelande visas om att hotet har tagits bort.

Vad gör jag om realtidsskyddet inte fungerar?

I detta kapitel beskrivs problem som kan uppstå när realtidsskyddet används och hur de felsöks.

Realtidsskyddet har inaktiverats

Om en användare av misstag inaktiverar realtidsskyddet bör du återaktivera funktionen. Om du vill återaktivera realtidsskyddet går du till **Inställningar** i programmets huvudfönster och klickar på **Datorskydd** > **Skydd av filsystemet i realtid**.

Om realtidsskyddet inte startas samtidigt som datorn startas beror det troligen på att **Aktivera skydd av filsystemet i realtid** har inaktiverats. Kontrollera att det här alternativet är aktiverat genom att öppna Avancerade inställningar > **Skydd** > **Skydd av filsystemet i realtid**.

Infiltreringar identifieras och rensas inte av realtidsskyddet

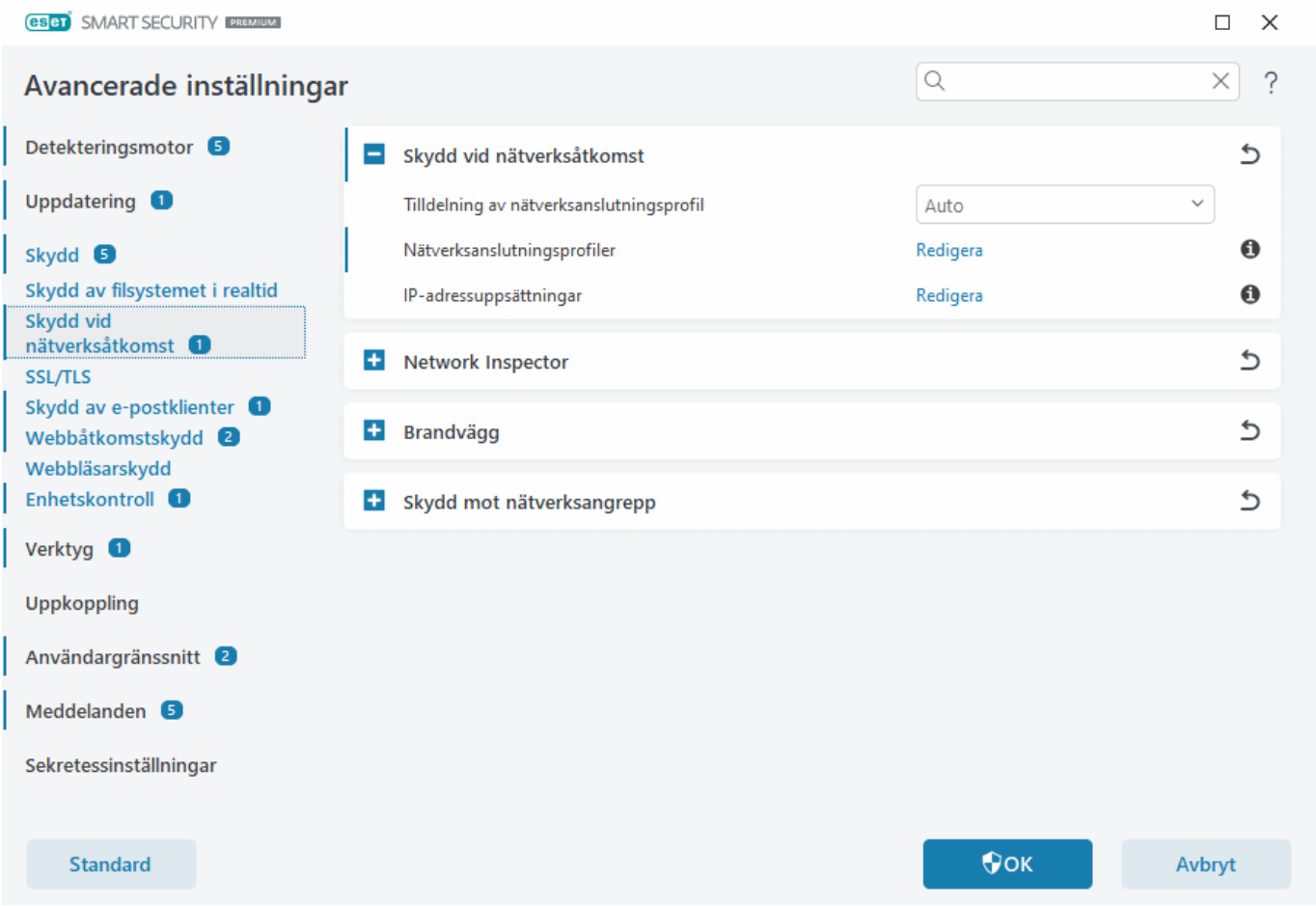
Kontrollera att inga andra antivirusprogram är installerade på datorn. Om två antivirusprogram är installerade samtidigt kan de stå i konflikt med varandra. Det rekommenderas att du avinstallerar alla andra antivirusprogram på datorn innan du installerar ESET.

Realtidsskyddet startar inte

Om realtidsskyddet inte startas när datorn startas (och **Aktivera skydd av filsystemet i realtid** har aktiverats) kan det bero på konflikter med andra program. För att lösa problemet skapar du en ESET SysInspector-logg och skickar den till ESET:s tekniska support för analys.

Skydd vid nätverksåtkomst

Med Nätverksåtkomstskydd kan du konfigurera alla dina nätverksanslutningar i detalj. Du kan tillåta/neka åtkomst till din dator i specifika nätverk, tillåta/neka åtkomst till nätverksenheter från din dator med mera baserat på konfigurationen. Som standard har ESET Smart Security Premium förkonfigurerade brandväggsregler och nätverksåtkomstskydd för maximal säkerhet. Vissa miljöer kan dock behöva anpassad konfiguration. Standardinställningarna bör endast ändras av en erfaren användare.



Du kan konfigurera följande inställningar i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** (klicka på länkarna nedan för en detaljerad beskrivning av varje alternativ i Nätverksåtkomstskydd):

Skydd vid nätverksåtkomst

Nätverksanslutningsprofiler – du kan använda profiler för att styra brandväggens beteende för specifika nätverksanslutningar.

IP-uppsättningar – du kan definiera uppsättningar av IP-adresser som skapar en logisk grupp med IP-adresser. Du kan använda dem för brandväggsregler.

Network Inspector

Brandvägg

Skydd mot nätverksattacker

Nätverksanslutningsprofiler

Profiler kan användas för att styra hur ESET Smart Security Premium Nätverksskydd fungerar för specifika nätverksanslutningar. När du skapar eller redigerar en brandväggsregel, IDS-regel eller regel för skydd mot brute force-attackl kan du tilldela den till en specifik profil eller tillämpa den på alla profiler. När en profil är aktiv i ett nätverksanslutning tillämpas endast de globala reglerna (regler utan angiven profil) och de regler som har tilldelats den valda profilen. Det går att skapa flera profiler med olika regler tilldelade till nätverksanslutningar för att enkelt ändra brandväggens beteende.

Du kan konfigurera profiler och tilldelningar för nätverksanslutningar i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Nätverksåtkomstskydd**.

Tilldelning av nätverksanslutningsprofil – gör att du kan välja om nyligen identifierade nätverksanslutningar automatiskt (välj **Auto** i listrutan) tilldelas en fördefinierad eller anpassad profil baserat på aktivatorer som har konfigurerats i nätverksanslutningsprofiler eller om du vill bli ombedd (välj **Fråga** i listrutan) att konfigurera nätverksskydd och tilldela en profil manuellt varje gång en ny nätverksanslutning identifieras.

Du kan också manuellt tilldela en specifik nätverksanslutningsprofil i programmets huvudfönster > **Inställningar** > **Nätverksskydd** > **Nätverksanslutningar**. Håll muspekaren över en specifik nätverksanslutning och klicka på menyikonen ⋮ > **Redigera** för att öppna fönstret Konfigurera nätverksskydd och välja en profil.

Nätverksanslutningsprofiler – klicka på **Redigera** för att lägga till eller redigera nätverksanslutningsprofiler.

Följande profiler är fördefinierade och kan inte redigeras eller tas bort:

Privat – för betrodda nätverk (hem- eller kontorsnätverk). Datorn och delade filer som lagras på datorn är synliga för andra nätverksanvändare och systemresurserna är tillgängliga för andra användare i nätverket (åtkomst till delade filer och skrivare är aktiverad, inkommande RPC-kommunikation är aktiverad och fjärrdelning av skrivbord är aktiverad). Vi rekommenderar att du använder den här inställningen när du kommer åt ett säkert lokalt nätverk. Den här profilen tilldelas automatiskt till en nätverksanslutning om den är konfigurerad som ett Domän- eller Privat-närverk i Windows.

Offentligt – för ej betrodda nätverk (offentligt nätverk). Filer och mappar i systemet delas inte med eller är synliga för andra användare i nätverket och delning av systemresurser är inaktiverad. Vi rekommenderar att du använder den här inställningen vid åtkomst till trådlösa nätverk. Den här profilen tilldelas automatiskt till alla nätverksanslutningar som inte är konfigurerade som ett Domän- eller Privat-nätverk i Windows.

När nätverksanslutningen växlar till en annan profil visas ett meddelande längst ned i högra hörnet av skärmen.

Lägga till eller redigera nätverksanslutningsprofiler

Du kan lägga till eller redigera Nätverksanslutningsprofiler i Avancerade inställningar > **Skydd** **Nätverksåtkomstskydd** > **Nätverksåtkomstskydd** > **Nätverksanslutningsprofiler** > **Redigera**. Om du vill redigera en profil måste den väljas i fönstret **Nätverksanslutningsprofiler**.

Följande profiler är fördefinierade och kan inte redigeras eller tas bort:

Privat – för betrodda nätverk (hem- eller kontorsnätverk). Datorn och delade filer som lagras på datorn är synliga för andra nätverksanvändare och systemresurserna är tillgängliga för andra användare i nätverket (åtkomst till delade filer och skrivare är aktiverad, inkommande RPC-kommunikation är aktiverad och fjärrdelning av skrivbord

är aktiverad). Vi rekommenderar att du använder den här inställningen när du kommer åt ett säkert lokalt nätverk. Den här profilen tilldelas automatiskt till en nätverksanslutning om den är konfigurerad som ett Domän- eller Privat-närverk i Windows.

Offentligt – för ej betrodda nätverk (offentligt nätverk). Filer och mappar i systemet delas inte med eller är synliga för andra användare i nätverket och delning av systemresurser är inaktiverad. Vi rekommenderar att du använder den här inställningen vid åtkomst till trådlösa nätverk. Den här profilen tilldelas automatiskt till alla nätverksanslutningar som inte är konfigurerade som ett Domän- eller Privat-nätverk i Windows.

Topp/Upp/Ned/Botten  – gör att du kan justera prioritetsnivån för nätverksanslutningsprofiler (Nätverksanslutningsprofiler utvärderas och tillämpas efter prioritet. Den första matchande profilen används alltid.)

Lägga till eller redigera en profil

Med en anpassad nätverksanslutningsprofil kan du tillämpa brandväggsregler och definiera ytterligare inställningar för specifika nätverksanslutningar. Du anger till vilka nätverksanslutningar den anpassade profilen ska tilldelas i avsnittet Aktivatorer.

Så här öppnar du profilredigeraren i fönstret **Nätverksanslutningsprofiler**:

- Klicka på **Lägg till**.
- Välj en av de befintliga profilerna och klicka på **Redigera**.
- Välj en av de befintliga profilerna och klicka på **Kopiera**.

Namn – anpassat namn på profilen.

Beskrivning – beskrivning av profilen för att identifiera den.

Ytterligare betrodda adresser – adresser som definieras här läggs till i den betrodda platsen för nätverksanslutningen som profilen tillämpas på (oavsett nätverkets skyddstyp).

Betrodd anslutning – datorn och delade filer som lagras på datorn är synliga för andra nätverksanvändare och systemresurserna är tillgängliga för andra användare i nätverket (åtkomst till delade filer och skrivare är aktiverad, inkommande RPC-kommunikation är aktiverad och fjärrdelning av skrivbord är aktiverad). Vi rekommenderar att du använder den här inställningen när du skapar en profil för en säker lokal nätverksanslutning. Alla direkt anslutna nätverksundernät anses också vara betrodda. Om till exempel ett nätverkskort är anslutet till nätverket med IP-adressen 192.168.1.5 och undernätsmasken 255.255.255.0 läggs undernätet 192.168.1.0/24 till i kortets betrodda plats. Om kortet har fler adresser/undernät är alla betrodda.

Varna om svag Wi-Fi-kryptering – ESET Smart Security Premium visar ett meddelande på skrivbordet när du ansluter till ett oskyddat trådlöst nätverk eller ett nätverk med svagt skydd.

Aktivatorer – anpassade villkor som måste uppfyllas för att tilldela den här nätverksanslutningsprofilen till en nätverksanslutning. Du hittar en detaljerad förklaring i Aktivatorer.

Aktiverare

Aktivatorer är anpassade villkor som måste uppfyllas för att tilldela en nätverksanslutningsprofil till en nätverksanslutning. Om det anslutna nätverket har samma attribut som definierats i aktivatorer för en ansluten nätverksprofil tillämpas profilen på nätverket. En nätverksanslutningsprofil kan ha en eller flera aktivatorer. Om det finns flera aktivatorer gäller ELLER-logiken (minst ett villkor måste uppfyllas). Du kan definiera aktivatorer i redigeraren för nätverksanslutningsprofil. Anpassade nätverksanslutningsprofiler bör skapas av en erfaren användare.

Följande aktivatorer är tillgängliga (om du vill veta mer om ditt aktuella nätverk ska du läsa Nätverksanslutningar):

Nätverkskort

Korttyp – använd profil om nätverksanslutningen är upprättas på den valda korttypen.
Kortnamn – använd profil om nätverkskortets namn matchar.
Kort-IP – använd profil om nätverkskortets IP-adress matchar.

DNS

DNS-suffix – använd profil om domännamnet matchar.
DNS-IP – använd profilen om DNS-serverns IP-adress matchar.

WINS

Använd profilen om den mappade IP-adressen för Windows Internet Name Service (WINS) matchar.

DHCP

DHCP-IP – matcha DHCP-serverns IP-adress.

Standardgateway

IP – använd profil om standardgatewayens IP-adress matchar.
MAC-adress – använd profil om standardgatewayens MAC-adress matchar.

Wi-Fi

SSID – använd profil om SSID (Wi-Fi-namnet) matchar.
Profilnamn – använd profil om Wi-Fi-profilnamnet matchar.
Säkerhetstyp – använd profil om säkerhetstypen matchar den som valts i listrutan. Skapa ytterligare en aktivator om du vill matcha mer än en.
Krypteringstyp – använd profil om krypteringstypen matchar den som valts i listrutan. Skapa ytterligare en aktivator om du vill matcha mer än en.
Nätverkssäkerhet – använd profil om nätverket är **öppet/skyddat**.

Windows-profil

Använd profil om nätverket är konfigurerat i Windows som **Domän/Privat/Offentligt.**

Autentisering

Nätverksautentiseringen söker efter en specifik server i nätverket och använder asymmetrisk kryptering (RSA) för att autentisera servern. Nätverksnamnet som autentiseras måste matcha namnet som angetts i inställningarna för autentiseringsservern. Namnet är skiftlägeskänsligt. Servernamnet kan skrivas som en IP-adress, DNS eller ett NetBios-namn.
Hämta ESET-autentiseringsservern.
Den offentliga nyckeln kan importeras genom att använda någon av följande filtyper:
- PEM-krypterad offentlig nyckel (.pem). Du kan generera den här nyckeln med ESET-autentiseringsservern
- Krypterad offentlig nyckel
- Certifikat för offentlig nyckel (.crt)

Klicka på **Test** för att testa inställningarna. Om autentiseringen lyckas visas Serverautentiseringen lyckades.
Om autentiseringen inte är rätt konfigurerad visas ett av följande felmeddelanden:
Det gick inte att autentisera servern. Ogiltig eller felaktig signatur.
Serversignaturen matchar inte den angivna offentliga nyckeln.
Det gick inte att autentisera servern. Nätverksnamnet matchar inte.
Namnet på det konfigurerade nätverket stämmer inte överens med autentiseringsserverns nätverksnamn. Kontrollera båda namnen och säkerställ att de är identiska.
Det gick inte att autentisera servern. Ogiltigt eller inget svar från servern.
Inget svar tas emot om servern inte körs eller inte är åtkomlig. Ett ogiltigt svar kan tas emot om en annan HTTP-server körs på den angivna adressen.
Ogiltig offentlig nyckel har angivits.
Kontrollera att den angivna filen för offentlig nyckel inte är skadad.

IP-adressuppsättningar

En IP-uppsättning är en samling IP-adresser som skapar en logisk grupp med IP-adresser. Det är användbart när du återanvänder samma uppsättning adresser i flera brandväggsregler eller reglar för skydd mot brute force-attack. ESET Smart Security Premium innehåller också fördefinierade IP-uppsättningar för vilka interna regler tillämpas. Ett exempel på en sådan grupp är gruppen **Tillförlitliga platser**. Betrodda platser representerar en grupp med nätverksadresser där datorn och de delade filer som lagras på datorn är synliga för andra nätverksanvändare och systemresurserna är tillgängliga för andra användare i nätverket.

Så här lägger du till en IP-uppsättning:

1. Öppna Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **IP-uppsättningar** > **Redigera**.

2. Klicka på **Lägg till**, skriv ett **Namn** och en **Beskrivning** för zonen och skriv en fjärr-IP-adress i **Fjärrdatoradress (IPv4/IPv6, intervall, mask)**.

3. Klicka på **OK**.

Du hittar mer information i Redigera IP-uppsättningar.

Redigera IP-uppsättningar

Du hittar mer information om IP-uppsättningar i IP-uppsättningar.

Kolumner

Namn – namnet på en grupp fjärrdatorer.

Beskrivning – en allmän beskrivning av gruppen.

IP-adresser – fjärr-IP-adresser som tillhör en IP-uppsättning.

Kontrollelement

När du **lägger till** eller **redigerar** en IP-uppsättning är följande fält tillgängliga:

Namn – namnet på en grupp fjärrdatorer.

Beskrivning – en allmän beskrivning av gruppen.

Fjärrdatoradress (IPv4, IPv6, intervall, mask) – gör det möjligt att lägga till en fjärradress, ett adressintervall eller ett undernät.

Ta bort – tar bort en zon från listan.

Det går inte att ta bort fördefinierade IP-uppsättningar.

Exempel på IP-adresser

Lägg till IPv4-adress:
Enskild adress – lägger till en IP-adress för en enskild dator (till exempel *192.168.0.10*).
Adressintervall – ange den första och den sista IP-adressen för att ange IP-intervallet för flera datorer (till exempel *192.168.0.1–192.168.0.99*).
Undernät – undernät (en grupp datorer) definierade av en IP-adress och en mask. 255.255.255.0 är till exempel nätverksmasken för undernätet 192.168.1.0. Om du vill undanta hela undernätet ska du skriva *192.168.1.0/24*.
Lägg till IPv6-adress:
Enskild adress – lägger till en IP-adress för en enskild dator (till exempel *2001:718:1c01:16:214:22ff:fec9:ca5*).
Undernät – undernät (en grupp datorer) som definieras av en IP-adress och en mask (till exempel: *2002:c0a8:6301:1::1/64*).

Network Inspector

Network Inspector kan hjälpa till att identifiera sårbarheter i ditt betrodda nätverk (hem- eller kontorsnätverk) (till exempel öppna portar eller ett svagt routerlösenord). Det innehåller även en lista över anslutna enheter, kategoriserade efter enhetstyp (till exempel skrivare, router, mobil enhet osv.) för att visa vad som är anslutet till ditt nätverk (till exempel spelkonsol, IoT eller andra smarta hemenheter). Du kan konfigurera Network Inspector i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Network Inspector**.

Aktivera Network Inspector – Network Inspectorhjälper till att identifiera sårbarheter i hemnätverk, som till exempel öppna portar eller ett svagt routerlösenord. Dessutom finns en lista över anslutna enheter, kategoriserade efter enhetstyp.

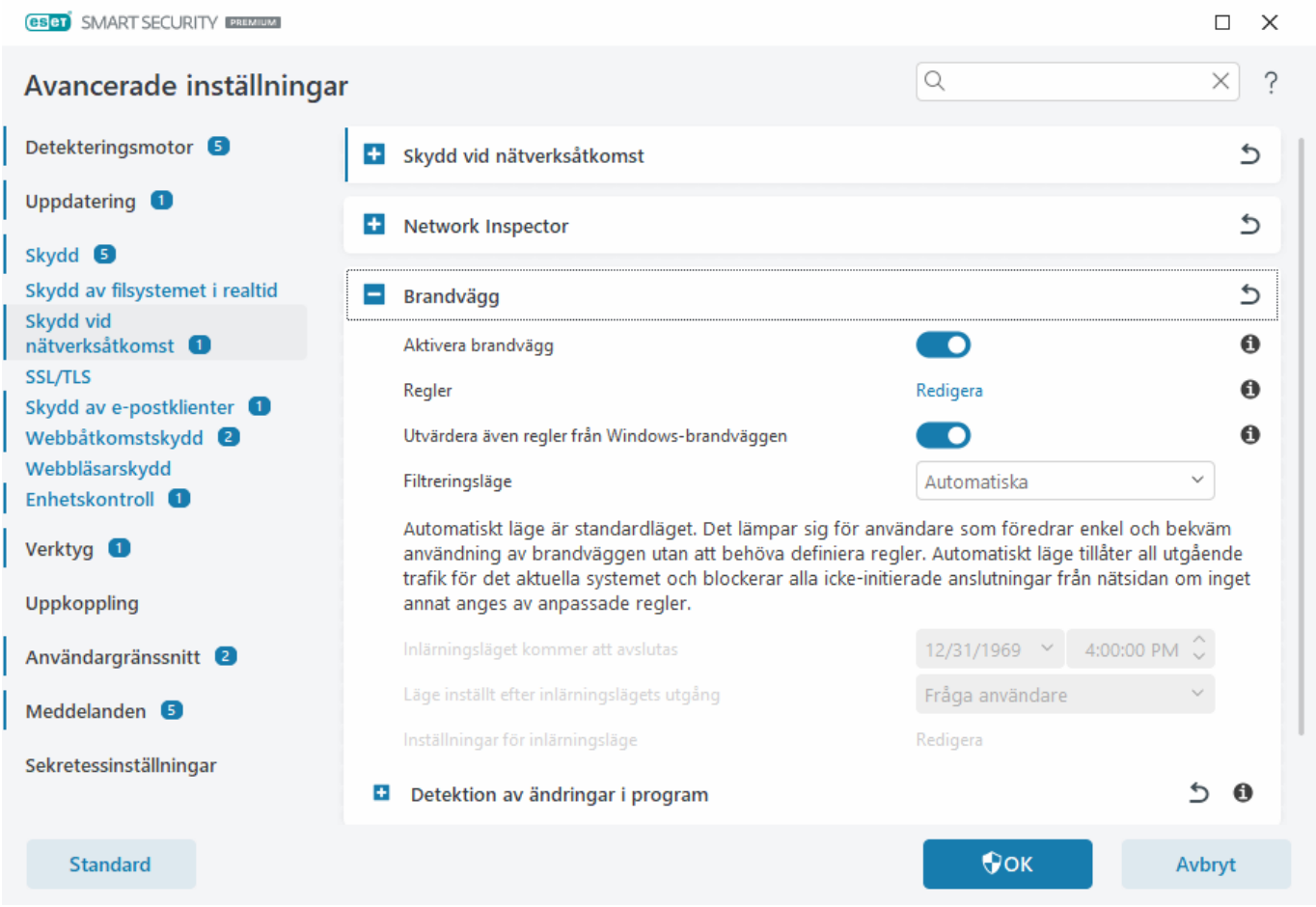
Meddela om nyupptäckta nätverksenheter – meddelar när en ny enhet upptäcks i nätverket.

Brandvägg

Brandväggen styr all inkommande och utgående nätverkstrafik på datorn baserat på interna regler och regler som har definierats av dig. Det här åstadkoms genom att olika nätverksanslutningar tillåts eller nekas beroende på filtreringsregler. Brandväggen skyddar mot attacker från fjärrenheter och kan blockera vissa potentiellt farliga

tjänster.

Om du vill konfigurera brandväggen ska du öppna Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Brandvägg**.



Brandvägg

Aktivera brandvägg

den här funktionen bör lämnas aktiverad för att säkerställa systemets säkerhet. När Brandvägg är aktiverad genomsöks nätverkstrafiken i båda riktningarna.

Regler

Med regelinställningar kan du visa och redigera alla brandväggsregler som tillämpas på trafiken som genererats av enskilda program inom tillförlitliga anslutningar och internet.

> Du kan skapa en IDS-regel vid en botnätsattack på datorn. En regel kan ändras i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Skydd mot nätverksangrepp (IDS)** > **IDS-regler** genom att klicka på **Redigera**.

Utvärdera även regler från Windows-brandväggen

I automatiskt filtreringsläge tillåts även inkommande trafik som tillåts av regler från Windows-brandväggen om den inte uttryckligen blockeras av ESET-regler.

Filtreringsläge

Brandväggens beteende ändras beroende på filtreringsläget. Filtreringsläget påverkar också hur mycket användaren behöver göra.

Följande filtreringslägen finns för ESET Smart Security Premium brandvägg:

Filtreringsläge	Beskrivning
Automatiskt läge	Standardläget. Detta läge lämpar sig för användare som föredrar en enkel och bekväm användning av brandväggen utan att behöva definiera regler. Egna, användardefinierade regler kan också skapas, men krävs inte i **automatiskt läge**. Det automatiska läget tillåter all utgående trafik för det givna systemet och blockerar den mesta inkommande trafiken utom viss trafik från Tillförlitliga platser (enligt inställningarna i IDS och avancerade alternativ/Tillåtna tjänster) samt svar på nyligen skickad utgående kommunikation.
Interaktivt läge	Interaktivt läge – gör det möjligt att anpassa en konfiguration för brandväggen. När kommunikation identifieras och det inte finns en regler som gäller denna kommunikation, öppnas en dialogruta som rapporterar en okänd anslutning. Du kan sedan välja att tillåta eller neka kommunikation och beslutet att tillåta eller neka kan sparas som en ny regel för brandväggen. Om du väljer att skapa en ny regel, kommer alla framtida anslutningar av den här typen att tillåtas eller blockeras enligt regeln.
Principbaserat läge	Blockerar alla anslutningar som inte definierats i en regel som tillåter dem. I det här läget kan avancerade användare definiera regler som endast tillåter önskade och säkra anslutningar. Alla övriga ospecificerade anslutningar blockeras av brandväggen.
Inlärningsläge	Skapar och sparar regler automatiskt; det här läget är mest lämpligt att använda för den initiala konfigurationen av brandväggen, men bör inte användas längre tidsperioder. Ingen användarinteraktion krävs eftersom ESET Smart Security Premium sparar regler enligt fördefinierade parametrar. För att undvika säkerhetsrisker bör inlärningsläget endast användas tills alla nödvändiga kommunikationsregler skapats.

Inlärningsläget avslutas vid – ange datum och tid när inlärningsläget avslutas automatiskt. Du kan också stänga av inlärningsläget manuellt när du vill.

Läge inställt efter inlärningslägets utgång – ange vilket filtreringsläge -brandväggen ska återgå till när tiden för inlärningsläge har gått ut. Läs mer om filtreringslägen i tabellen ovan. Efter utgången behöver alternativet **Fråga användare** administratörsbehörighet för att utföra en ändring av brandväggens filtreringsläge.

Inställningar för inlärningsläge – klicka på **Redigera** för att konfigurera parametrar för att spara regler som skapats i Inlärningsläge.

Detektion av ändringar i program

Funktionen detektering av ändringar i program visar meddelanden om ändrade program, som har en brandväggsregel, försöker att upprätta anslutningar.

Inställningar för inlärningsläge

I inlärningsläget skapas och sparas automatiskt en regel för varje kommunikation som upprättats i systemet. Ingen användarinteraktion krävs eftersom ESET Smart Security Premium sparar regler enligt fördefinierade parametrar.

Läget kan utsätta systemet för risker och rekommenderas endast för initial konfiguration av brandväggen.

Välj **Inlärning** från listrutan i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Brandvägg** >

Brandvägg, > **Filtreringsläge** för att aktivera Alternativ för inlärningsläge. Klicka på **Redigera** bredvid **Inställningar för inlärningsläge** för att konfigurera följande alternativ:

> I Inlärningsläge utför brandväggen ingen filtrering av kommunikationen. All utgående och inkommande kommunikation tillåts. I det här läget är datorn inte helt skyddad av brandväggen.

Inkommande trafik från tillförlitliga platser – ett exempel på en inkommande anslutning inom Tillförlitliga platser är en fjärrenhet som inom den tillförlitliga platsen försöker upprätta kommunikation med ett lokalt program som körs på din dator.

Utgående trafik till tillförlitliga platser – ett lokalt program försöker upprätta en anslutning med en annan enhet inom det lokala nätverket, eller inom nätverken i Tillförlitliga platser.

Inkommande Internettrafik – en fjärrenhet försöker kommunicera med ett program som körs på datorn.

Utgående Internettrafik – ett lokalt program försöker upprätta en anslutning med en annan enhet.

I varje avsnitt kan du ange parametrar som ska läggas till i nyligen skapade regler:

Lägg till lokal port – innefattar lokalt portnummer för nätverkskommunikationen. För utgående kommunikation genereras i regel slumpmässiga nummer. Därför rekommenderar vi att det här alternativet endast aktiveras för inkommande kommunikation.

Lägg till program – innefattar namnet på det lokala programmet. Alternativet är lämpligt för framtida regler på programnivå (regler som definierar kommunikationen för ett helt program). Du kan till exempel aktivera kommunikation för en viss webbläsare eller e-postklient.

Lägg till fjärrport – innefattar fjärrportnummer för nätverkskommunikationen. Du kan till exempel tillåta eller neka en specifik tjänst som associerats med ett standardportnummer (HTTP – 80, POP3 – 110, osv.).

Lägg till fjärr-IP-adress / Tillförlitliga platser – en fjärr-IP-adress eller zon kan användas som en parameter för nya regler som definierar alla nätverksanslutningar mellan det lokala systemet och fjärradressen/zonen. Det här alternativet är lämpligt om du vill definiera åtgärder för en viss enhet eller en grupp av nätverksanslutna enheter.

Maximalt antal olika regler för ett program – om ett program kommunicerar genom olika portar, till olika IP-adresser, etc., kommer brandväggen i inlärningsläget att skapa ett lämpligt antal regler för det aktuella programmet. Med det här alternativet kan du begränsa antalet regler som kan skapas för ett visst program.

Brandväggsregler

Brandväggsregler består av en uppsättning villkor som används för kontroll av nätverksanslutningar, samt de åtgärder som är tilldelade dessa villkor. Genom att använda reglerna för brandväggen kan du definiera åtgärden som vidtas när olika typer av nätverksanslutningar är upprättade.

Regler utvärderas uppifrån och ned och du kan se deras prioritet i den första kolumnen. Åtgärden för den första matchande regeln används för varje nätverksanslutning som utvärderas.

Anslutningar går att dela upp i inkommande och utgående anslutningar. Inkommande anslutningar initieras av en fjärrenhet som försöker upprätta en anslutning till det lokala systemet. Utgående anslutningar fungerar på motsatt sätt – det lokala systemet kontaktar en fjärrenhet.

Om en okänd kommunikation upptäcks, måste du noga överväga att tillåta eller avvisa den. Oönskade, oskyddade eller okända anslutningar utgör en säkerhetsrisk för systemet. Om en sådan anslutning upprättas rekommenderar vi arr du noggrant granskar fjärrenhet och det program som försöker ansluta till din dator. Många infiltreringar försöker ofta att söka upp och skicka privat information eller läsa in andra skadliga program till värddatorerna. Med hjälp av brandväggen går det att identifiera och avsluta sådana anslutningar.

Du kan visa och redigera brandväggsregler i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Brandvägg** > **Regler** > **Redigera**.

Om du har många brandväggsregler kan du använda ett filter för att bara visa specifika regler. Om du vill filtrera brandväggsregler ska du klicka på **Fler filter** ovanför listan Brandväggsregler. Du kan filtrera reglerna baserat på följande kriterier:

- Ursprung
- Riktning
- Åtgärd
- Tillgänglighet

Som standard är de fördefinierade brandväggsreglerna dolda. Om du vill visa alla fördefinierade regler ska du inaktivera växlingsknappen bredvid **Dölj inbyggda (fördefinierade) regler**. Du kan inaktivera dessa regler, men det går inte att ta bort en fördefinierad regel.

Klicka på sökikonen längst upp till höger om du vill söka efter regler.

Kolumner

Prioritet – regler utvärderas uppifrån och ned och du kan se deras prioritet i den första kolumnen.

Aktiverad – visar om regler är aktiverade eller inaktiverade. Motsvarande kryssruta måste markeras för att en regel ska aktiveras.

Program – det program för vilket regeln gäller.

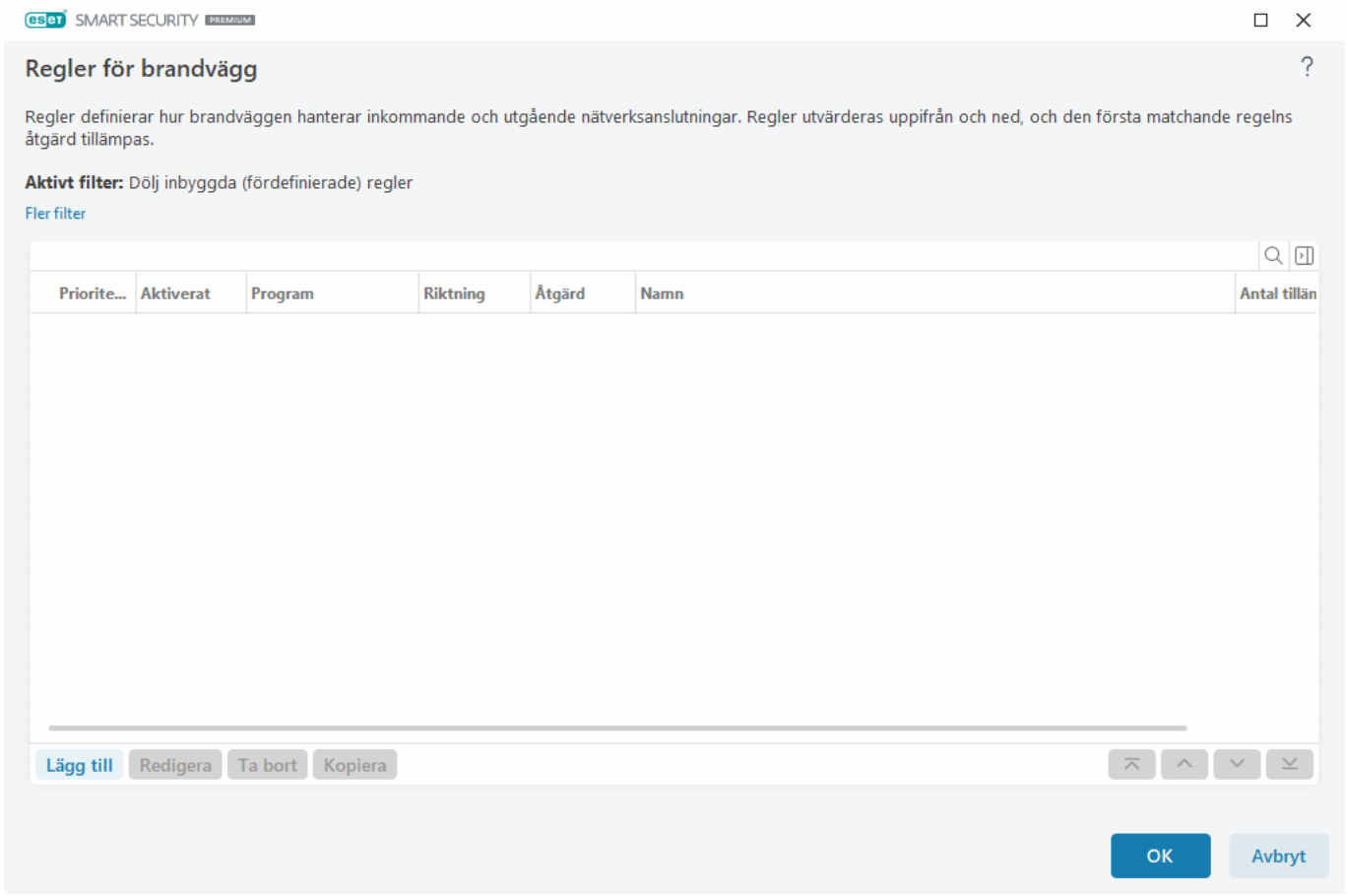
Riktning – kommunikationsriktning (inkommande/utgående/båda).

Åtgärd – visar kommunikationsstatusen (blockera/tillåt/fråga).

Namn – regelns namn. ESET-ikonen representerar en fördefinierad regel.

Antal tillämpningar – totalt antal gånger som regeln har tillämpats.

Klicka på expanderingsikonen för att visa regelinformationen.



Kontrollelement

Lägg till – skapar en ny regel.

Redigera – redigera en befintlig regel.

Ta bort – ta bort en befintlig regel.

Kopiera – skapa en kopia av en vald regel.

 **Överst/Upp/Ned/Underst** – gör så att du kan justera prioritetsnivån för regler (regler körs uppifrån och ned).

Lägga till eller redigera brandväggsregler

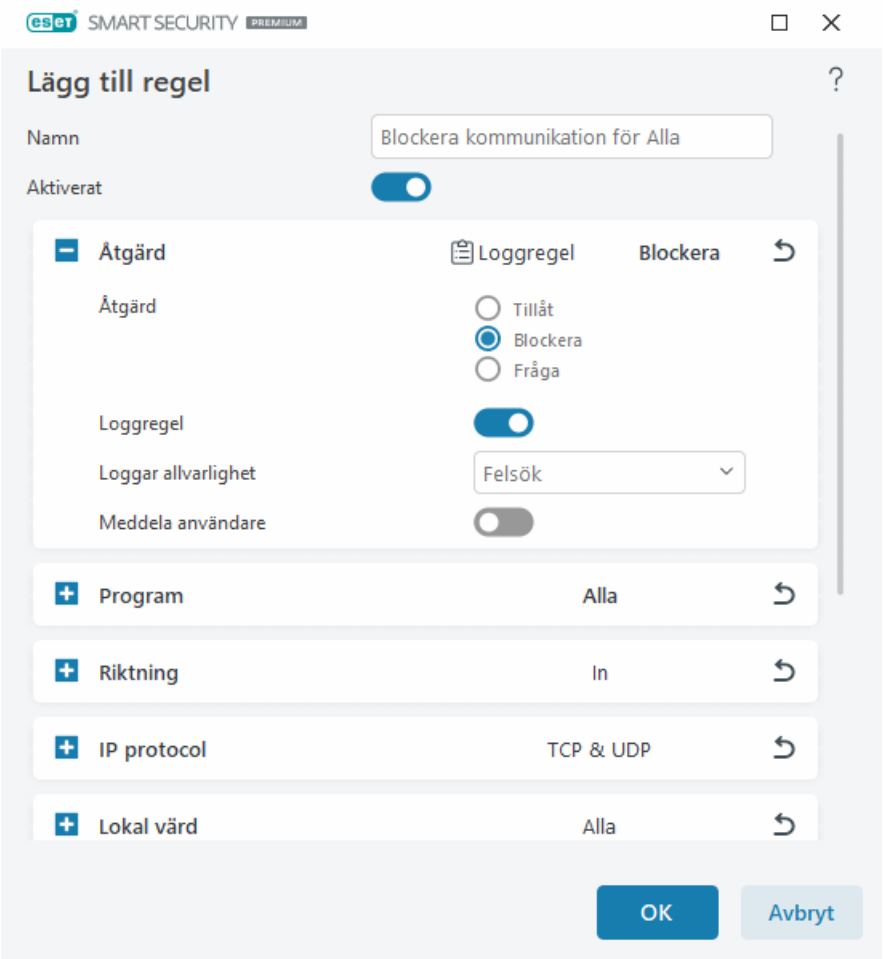
Brandväggsregler representerar villkor som används för kontroll av nätverksanslutningar, samt de åtgärder som är tilldelade dessa villkor. Redigering eller tillägg av brandväggsregler kan krävas när nätverksinställningarna ändras (till exempel om nätverksadressen eller portnumret för fjärrsidan har ändrats) för att säkerställa att ett program som påverkas av en regel fungerar korrekt. En erfaren användare bör skapa anpassade brandväggsregler.

Anvisningar med bilder

Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:

- Öppna eller stänga (tillåta eller neka) en viss port med en brandvägg
- Skapa en brandväggsregel från loggfilerna i ESET Smart Security Premium

Om du vill lägga till eller redigera en brandväggsregel ska du öppna Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Brandvägg** > **Regler** > **Redigera**. Klicka på **Lägg till** eller **Redigera** i fönstret Brandväggsregler.



Namn – ange ett namn för regeln.

Aktiverad – klicka på växlingsknappen för att aktivera regeln.

Lägg till åtgärder och villkor för brandväggsregeln:

Åtgärd

Åtgärd – välj om du vill **Tillåta**/**Blockera** kommunikationen som matchar villkoren som definieras i den här regeln eller om du vall att ESET Smart Security Premium ska **Fråga** varje gång kommunikationen upprättas.
Logga regel – om regeln tillämpas registreras den i Loggfiler.
Loggningens allvarlighetsgrad – välj allvarlighetsgraden för loggposten för den här regeln.
Meddela användare visar ett meddelande när regeln tillämpas.

Program

Ange ett program där den här regeln ska tillämpas.
Programsökväg – klicka på **...** och gå till ett program eller ange programmets fullständiga sökväg (till exempel C:\Program Files\Firefox\Firefox.exe). Ange INTE enbart programmets namn.
Programsignatur – du kan tillämpa regeln på program baserat på deras signaturer (utgivarens namn). Välj i listrutan om du vill tillämpa regeln på program med **Valfri giltig signatur** eller på program **Signerade av en specifik signerare**. Om du väljer program **Signerade av en viss signerare** måste du definiera signeraren i fältet **Namn på signerare**.
Microsoft Store-program – välj ett program som har installerats från Microsoft Store i listrutan.
Tjänst – du kan välja en systemtjänst i stället för ett program. Öppna listrutan för att välja en tjänst.
Använd på underordnade processer – vissa program kan köra fler processer medan du bara ser ett programfönster. Klicka på växlingsknappen för att aktivera regeln för varje process i det angivna programmet.

Riktning

Välj **kommunikationsriktningen** för den här regeln:
- **Båda** – inkommande och utgående kommunikation
- **In** – endast inkommande kommunikation
- **Ut** – endast utgående kommunikation

IP-protokoll

Välj ett **protokoll** i listrutan om du vill att regeln endast ska gälla för ett visst protokoll.

Lokal värd

Lokala adresser, adressintervall eller undernät där den här regeln tillämpas. Om ingen adress anges gäller regeln för all kommunikation med lokala värdar. Du kan lägga till IP-adresser, adressintervall eller undernät direkt i textfältet **IP** eller välja bland befintliga IP-uppsättningar genom att klicka på **Redigera** bredvid **IP-uppsättningar**.

Lokal port

Nummer på lokala **portar**. Om inga nummer anges gäller regeln för alla portar. Du kan lägga till en enskild kommunikationsport eller ett intervall med kommunikationsportar.

Fjärrvärd

Fjärradress, adressintervall eller undernät där den här regeln tillämpas. Om ingen adress anges gäller regeln för all kommunikation med fjärrvärdar. Du kan lägga till IP-adresser, adressintervall eller undernät direkt i textfältet **IP** eller välja bland befintliga IP-uppsättningar genom att klicka på **Redigera** bredvid **IP-uppsättningar**.

Fjärrport

Nummer på **fjärrportar**. Om inga nummer anges gäller regeln för alla portar. Du kan lägga till en enskild kommunikationsport eller ett intervall med kommunikationsportar.

Profil

En brandväggsregel kan tillämpas på specifika nätverksanslutningsprofiler.
Alla – regeln tillämpas på alla nätverksanslutningar trots den använda profilen.
Vald – regeln tillämpas på en specifik nätverksanslutning baserat på den valda profilen. Markera kryssrutan bredvid profilerna du vill välja.

Vi skapar en ny regel som ger Firefox-webbläsaren åtkomst till Internet/lokala nätverksplatser.
1.Välj **Åtgärd** > **Tillåt** i avsnittet **Åtgärd**.
2.Ange webbläsarens **programsökväg** i avsnittet **Program** (till exempel C:\Program Files\Firefox\Firefox.exe). Ange INTE enbart programmets namn.
3.Välj **Riktning** > **Ut** i avsnittet **Riktning**.
4.Välj **TCP & UDP** i listrutan **Protokoll** i avsnittet **IP-protokoll**.
5.Lägg till **portnummer** i avsnittet **Fjärrport**: *80, 443* för att tillåta standardsurfning.

Detektion av ändringar i program

Funktionen för detektion av ändringar i program visar meddelanden om ändrade program, för vilka det finns en brandväggsregel, försöker upprätta en anslutning. Ändrade program är en mekanism för att tillfälligt eller permanent ersätta ett ursprungligt program mot ett annat program med en annan körbar fil (skyddar mot missbruk av brandväggsregler).

Observera att funktionen inte är avsedd att identifiera ändringar av program i allmänhet. Syftet är att undvika att befintliga brandväggsregler missbrukas, och endast program för vilka specifika brandväggsregler finns övervakas.

Om du vill redigera **Detektering av ändringar i program** ska du öppna Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Brandvägg** > **Detektion av ändringar i program**.

Aktivera detektering av ändringar i program – om det här alternativet väljs övervakas ändringar i programmen (uppdateringar, infektioner, andra ändringar). När ett ändrat program försöker upprätta en anslutning får du ett meddelande av brandväggen.

Tillåt ändringar av signerade (betrodda) program – meddela inte om programmet har samma giltiga digitala signatur före och efter ändringen.

Lista över program som är undantagna från detektering – i det här fönstret kan du lägga till eller ta bort enskilda program för vilka ändringar är tillåtna utan meddelande.

Lista över program som är undantagna från detektering

Brandväggen i ESET Smart Security Premium detekterar ändringar av program för vilka regler finns (se Detektion av ändringar i program).

I vissa fall kanske du inte vill använda den här funktionen för vissa program om du vill att de inte ska kontrolleras av brandväggen.

Lägg till – Öppnar ett fönster där du kan välja ett program att lägga till i listan över program som undantas från detektering av ändringar. Du kan välja från en lista över program som körs med öppen nätverkskommunikation, som det finns en brandväggsregel för, eller lägga till ett visst program.

Redigera – Öppnar ett fönster där du kan ändra platsen för ett program som finns i listan över program som är uteslutna från ändringsdetektering. Du kan välja från en lista över program som körs med öppen nätverkskommunikation, som det finns en brandväggsregel för, eller ändra platsen manuellt.

Ta bort – tar bort poster från listan över program som undantas från detektering av ändringar.

Skydd mot nätverksangrepp (IDS)

Skyddet mot nätverksattacker (IDS) förbättrar detekteringen av exploateringar för kända sårbarheter. Läs mer om skydd mot nätverksattacker i Ordlistan. Om du vill konfigurera Skydd mot nätverksangrepp (IDS) ska du öppna Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Skydd mot nätverksangrepp (IDS)**.

Skydd mot nätverksangrepp (IDS) – analyserar innehållet i nätverkstrafik och skyddar mot nätverksangrepp. Eventuell trafik som anses skadlig blockeras.

Aktivera Botnet-skydd – detekterar och blockerar kommunikation med skadliga kommando- och kontrollservrar baserat på olika mönster när datorn är infekterad och en bot försöker kommunicera. Läs mer om Botnet-skydd i ordlistan.

IDS-regler – Detta alternativ gör det möjligt att konfigurera avancerade filtreringsalternativ för identifiering av olika typer av attacker och trojaner som kan skada din dator.

> **Anvisningar med bilder**
> Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:
> - Exkludera en IP-adress från IDS i ESET Smart Security Premium

Alla viktiga händelser som upptäcks av nätverksskyddet sparas i en loggfil. Se nätverksskyddsloggen för mer information.

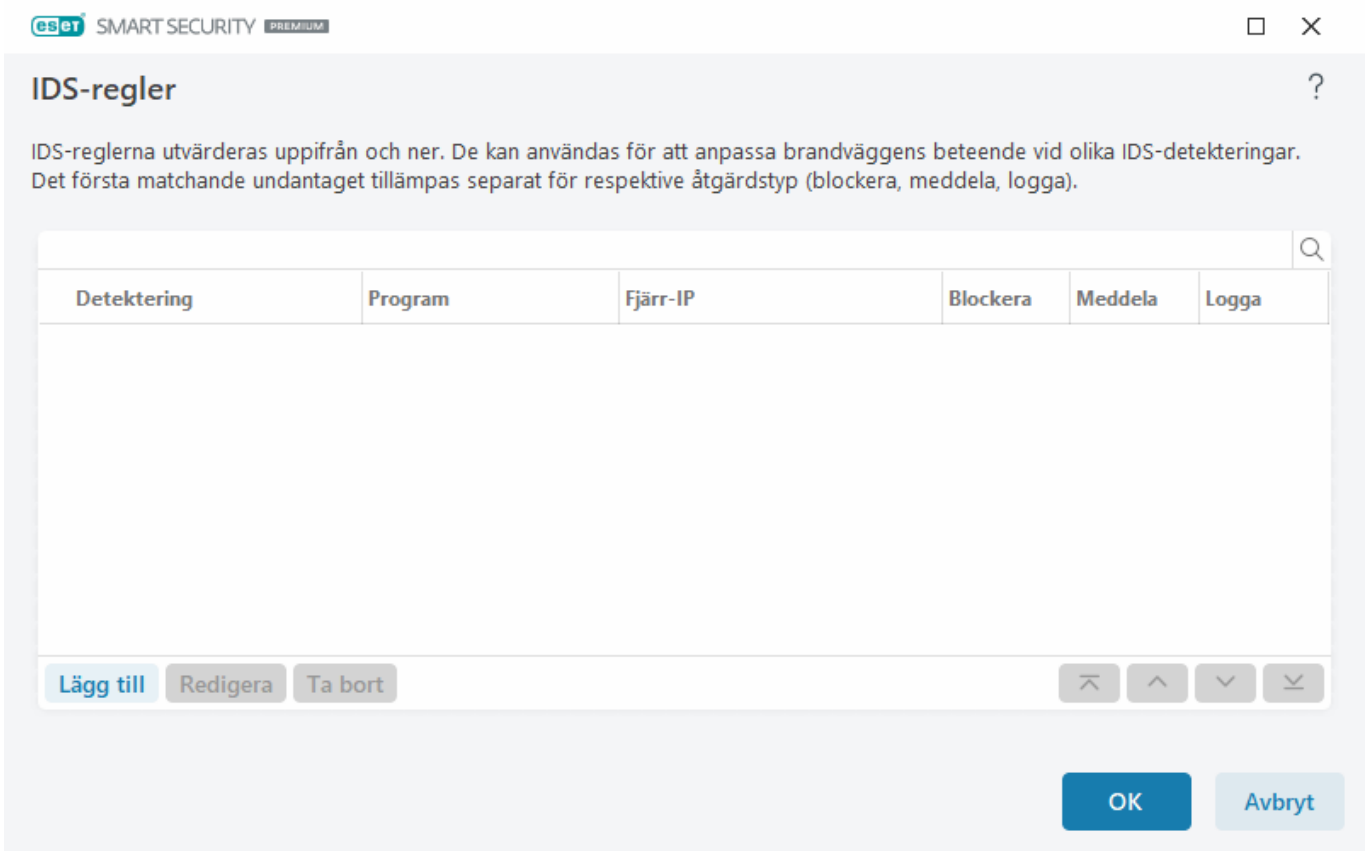
IDS regler

I vissa situationer kan IDS (Intrusion Detection Service) detektera kommunikation mellan routrar eller andra interna nätverksenheter som en potentiell attack. Du kan till exempel lägga till den kända säkra adressen till de adresser som är undantagna från IDS-zonen för att kringgå IDS.

> **Anvisningar med bilder**
> Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:
> - Exkludera en IP-adress från IDS i ESET Smart Security Premium

Hantera IDS-regler

- **Lägg till** – klicka för att skapa en ny IDS-regel.
- **Redigera** – klicka för att redigera en befintlig IDS-regel.
- **Ta bort** – välj och klicka om du vill ta bort en befintlig regel från listan över IDS-regler.
-  **Överst/Upp/Ned/Underst** – gör så att du kan justera prioritetsnivån för regler (undantag utvärderas uppifrån och ned).



Regelredigerare

Detektering – Detekteringstyp.

Hotnamn – du kan ange ett hotnamn för vissa av de tillgängliga detekteringarna.

Program – välj filsökvägen för ett undantaget program genom att klicka på ... (till exempel *C:\Program Files\Firefox\Firefox.exe*). Ange INTE programmets namn.

Fjärr-IP-adress – en lista över IPv4- eller IPv6-fjärradresser/-områden/-undernät. Flera adresser måste avgränsas med ett kommatecken.

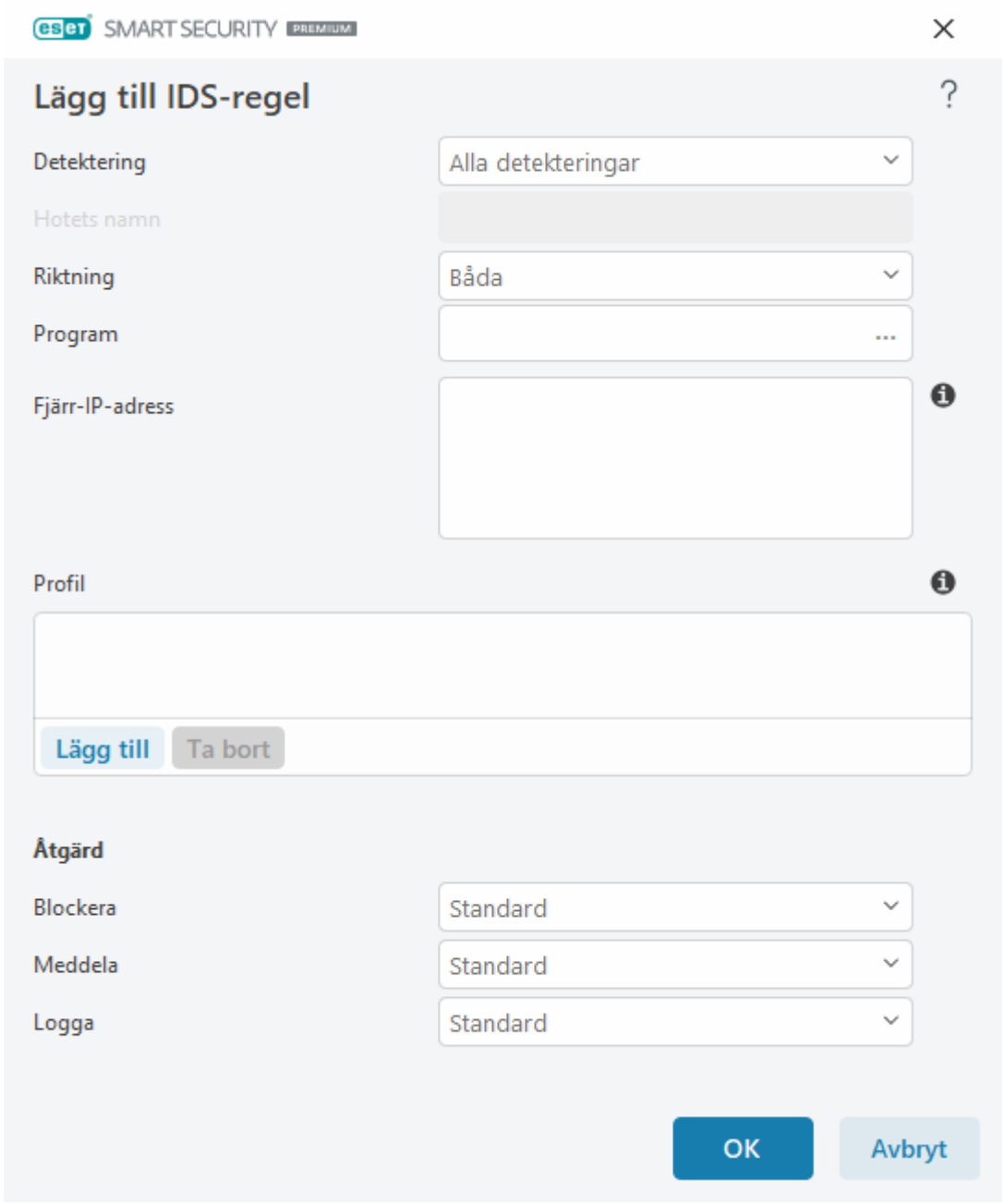
Profil – du kan välja en nätverksanslutningsprofil som den här regeln gäller för.

Åtgärd

Blockera – varje systemprocess har ett eget standardbeteende och tilldelad åtgärd (blockera eller tillåt). Om du vill åsidosätta standardbeteendet för ESET Smart Security Premium kan du välja mellan att blockera eller tillåta i listrutan.

Meddela – välj Ja om du vill visa meddelanden på skrivbordet på datorn. Välj Nej om du inte vill visa meddelanden på skrivbordet. De tillgängliga värdena är Standard/Ja/Nej.

Logga – välj **Ja** om du vill logga händelser i -loggfiler. Välj **Nej** Om du inte vill logga händelser. De tillgängliga värdena är **Standard/Ja/Nej**.



Om du vill visa ett meddelande och samla in en logg varje gång händelsen inträffar:
1.Klicka på **Lägg till** för att lägga till en ny IDS-regel.
2.Välj specifik detektering på rullgardinsmenyn **Detektering**.
3.Välj en programsökväg genom att klicka på **...** som du vill tillämpa meddelandet på.
4.Lämna **Standard** i listrutan **Blockera**. Då används standardåtgärden som tillämpas av ESET Smart Security Premium.
5.Ställ in både listrutan **Meddela** och listrutan **Logga** till **Ja**.
6.Klicka på **OK** för att spara meddelandet.

Om du inte vill visa ett återkommande meddelande om något du inte anser vara ett hot av en viss typ av **detektering**:

1.Klicka på **Lägg till** för att lägga till en ny IDS-regel.

2.Välj särskild detektering i rullgardinsmenyn **Detektering**, till exempel **SMB-session utan säkerhetstillägg** eller **TCP-portskanningsattack**.

3.Välj **In** i listrutan för riktning om det är från inkommande kommunikation.

4.Ställ in listrutan **Meddela** till **Nej**.

5.Ställ in listrutan **Logga** till **Ja**.

6.Lämna **Program** tomt.

7.Om kommunikationen inte kommer från en viss IP-adress lämnar du **Fjärr-IP-adresser** tomt.

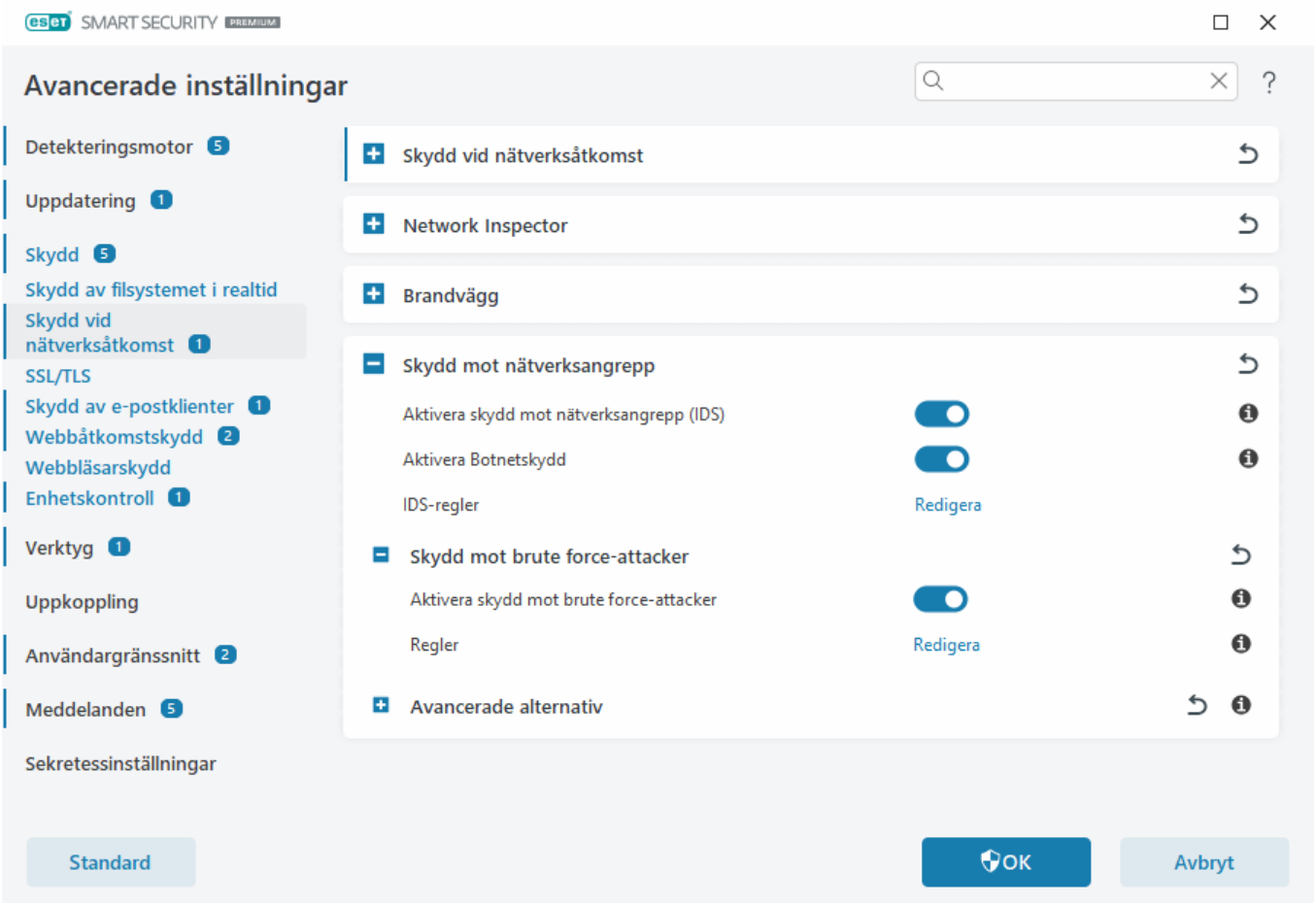
8.Klicka på **OK** för att spara meddelandet.

Skydd mot brute force-attacker

Skyddet mot brute force-attacker blockerar attacker som försöker lista ut lösenord för RDP- och SMB-tjänster. En brute force-attack är en metod för att avslöja ett utvalt lösenord genom att systematiskt prova alla möjliga kombinationer av bokstäver, siffror och symboler. Om du vill konfigurera Skydd mot brute-force-attacks ska du öppna Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Skydd mot nätverksangrepp (IDS)** > **Skydd mot brute force-attack**.

Aktivera skydd mot brute force-attacker – ESET Smart Security Premium inspekterar nätverkstrafikens innehåll och blockerar attacker som försöker lista ut lösenord.

Regler – används för att skapa, redigera och visa regler för inkommande och utgående nätverksanslutningar. Läs mer i kapitlet Regler.



Regler

Med regler för skydd mot brute force-attacker kan du skapa, redigera och visa regler för inkommande och utgående nätverksanslutningar. De fördefinierade reglerna kan inte redigeras eller tas bort.

Hantera regler för skydd mot brute force-attacker

Lägg till – skapar en ny regel.

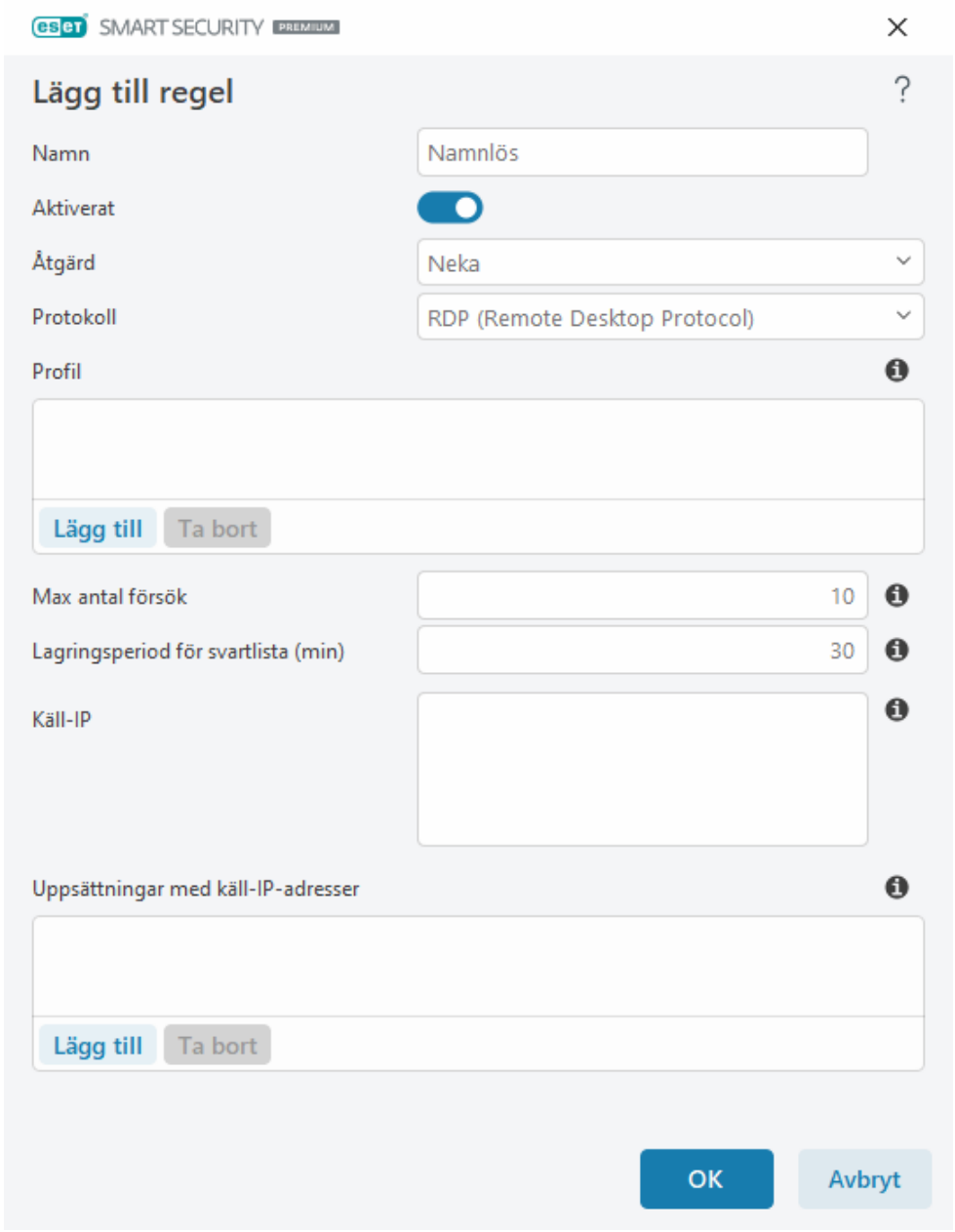
Redigera – redigera en befintlig regel.

Ta bort – ta bort en befintlig regel från listan med regler.

 **Överst/Upp/Ned/Underst** – justera prioritetsnivån för regler.

> För att säkerställa högsta möjliga skydd tillämpas blockeringsregeln med det lägsta värdet för **högsta antal försök**, även om regeln är placerad lägre i regellistan när flera blockeringsregler matchar detekteringsvillkoren.

Regelredigerare



Namn – regelns namn.

Aktiverad – inaktivera växlingsknappen om du vill behålla regeln i listan men inte tillämpa den.

Åtgärd – välj om du vill **neka** eller **tillåta** anslutningen om regelinställningarna är uppfyllda.

Protokoll – kommunikationsprotokollet som den här regeln kommer att inspektera.

Profil – anpassade regler kan ställas in och tillämpas för vissa profiler.

Max antal försök – Det maximala antalet tillåtna upprepade försök till attack tills IP-adressen blockeras och läggs till i svartlistan.

Lagringsperiod för svartlista (min) – anger tiden för när adressen tas bort från svartlistan.

Käll-IP – en lista över IP-adresser/intervall/undernät. Flera adresser måste avgränsas med ett kommatecken.

Käll-IP-uppsättningar – en uppsättning IP-adresser som du redan har definierat i IP-uppsättningar.

Avancerade alternativ

Du kan aktivera eller inaktivera detektering av flera typer av attacker och kryphål som kan skada datorn i Avancerade inställningar > **Skydd** > **Nätverksåtkomstskydd** > **Skydd mot nätverksangrepp (IDS)** > **Avancerade alternativ**.

I en del fall får du inget hotmeddelande om blockerad kommunikation. Se avsnittet Logga och skapa regler eller undantag från logg för anvisningar om hur du visar all blockerad kommunikation i brandväggsloggen.

Vilka alternativ som finns i fönstret kan variera beroende på ESET-produktens och brandväggmodulens typ och version samt operativsystemets version.

Intrångsdetektering

Intrångsdetektering söker efter skadlig aktivitet i enhetsnätverkskommunikationen.

- **Protokollet SMB** – identifierar och blockerar olika säkerhetsproblem i SMB-protokollet.
- **RPC-protokoll** – identifierar och blockerar olika CVE:er i RPC-system som utvecklats för DCE (Distributed Computing Environment).
- **Protokollet RDP** – identifierar och blockerar olika CVE i RDP-protokollet (se ovan).
- **Identifiering av ARP**-förgiftningsattacker – identifiering av ARP-förgiftningsattacker som orsakas av man-in-the-middle-attacker eller detektering av en nätverksanalysator. ARP (Address Resolution Protocol) används av nätverksprogrammet eller enheten för att fastställa Ethernet-adressen.
- Identifiering av **TCP/UDP-portskanningsattacker** – detekterar program för portskanningsattacker – program som avsöker värdar för att se om det finns öppna portar genom att skicka en klientförfrågan till flera olika portadresser i syfte att hitta aktiva portar och utnyttja tjänstens sårbarhet. Läs mer om den här attacktypen i ordlistan.
- **Blockera osäkra adresser efter detektering av attacker** – IP-adresser som har identifierats som attackkällor läggs till i svartlistan för att hindra att de ansluts under en viss tid. Du kan definiera **Kvarhållningsperiod på svartlista** vilket anger tiden för hur länge adressen ska blockeras efter attackdetektering.
- **Meddela om detektering av attack** – aktiverar Windows-meddelandefältet i nedre högra hörnet av skärmen.
- **Visa meddelanden även för inkommande attacker mot säkerhetshål** – varnar om attacker mot säkerhetshål upptäcks eller om ett försök gjorts av ett hot att ta sig in i systemet på det här sättet.

Paketkontroll

En typ av paketanalys som filtrerar data som överförs över nätverket.

- **Tillåt inkommande anslutning till admin shares i SMB-protokoll** - administrativa resurser (admin shares) är standardnätverksresurser som delar hårddiskpartitioner (*C$, D$*, ...) i systemet tillsammans med systemmappen (*ADMIN$*). Genom att inaktivera anslutningen till admin shares bör du minimera många säkerhetsrisker. Conficker-masken till exempel utför ordlisteattacker för att ansluta till admin shares.

- **Neka gamla (som inte stöds) SMB-dialekter** – neka SMB-sessioner som använder en gammal SMB-dialekt som inte stöds av IDS. Moderna Windows-operativsystem stöder gamla SMB-dialekter på grund av att de är bakåtkompatibla med gamla operativsystem, som Windows 95. Angriparen kan använda en gammal dialekt i en SMB-session för att undvika trafikkontroll. Neka gamla SMB-dialekter om datorn inte behöver dela filer (eller använda SMB-kommunikation i allmänhet) med en dator som har en gammal Windows-version.

- **Neka SMB-sessioner utan utökad säkerhet** – utökad säkerhet kan användas för en SMB-session för att erbjuda en säkrare autentiseringsmekanism än LAN Manager (LM) anrop/svar-autentisering. LM-systemet anses vara svagt och rekommenderas inte.

- **Neka att körbar fil öppnas på en server utanför Tillförlitliga platser med SMB-protokoll** – släpper anslutningen när du försöker att öppna en körbar fil (.exe, .dll) från en delad mapp på en server som inte tillhör Tillförlitliga platser i brandväggen. Observera att kopiering av körbara filer från betrodda källor kan vara legitimt. Observera att det kan vara legitimt att kopiera körbara filer från betrodda källor. Denna identifiering minskar dock riskerna från oönskat öppnande av en fil på en skadlig server (orsakat till exempel genom en klickning på en länk till en delad skadlig körbar fil).

- **Neka NTLM-autentisering med SMB-protokoll för att ansluta en server i/utanför Tillförlitliga platser** – protokoll som använder NTLM-autentisering (båda versionerna) kan utsättas för en attack som vidarebefordrar autentiseringsuppgifter (kallas också SMB-reläattacker om det gäller SMB-protokoll). Genom att neka NTLM-autentisering med en server utanför Tillförlitliga platser bör riskerna minimeras för vidarebefordran av autentiseringsuppgifter av en skadlig server utanför Tillförlitliga platser. På samma sätt går det att neka NTLM-autentisering med servrar i Tillförlitliga platser.

- **Tillåt kommunikation med tjänsten Hanterare för kontosäkerhet** – för mer information om den här tjänsten, se [MS-SAMR].

- **Tillåt kommunikation med tjänsten Lokal säkerhetskontroll** – för mer information om den här tjänsten, se [MS-LSAD] och [MS-LSAT].

- **Tillåt kommunikation med tjänsten Remote Registry** – för mer information om den här tjänsten, se [MS-RRP].

- **Tillåt kommunikation med tjänsten Service Control Manager** – för mer information om den här tjänsten, se [MS-SCMR].

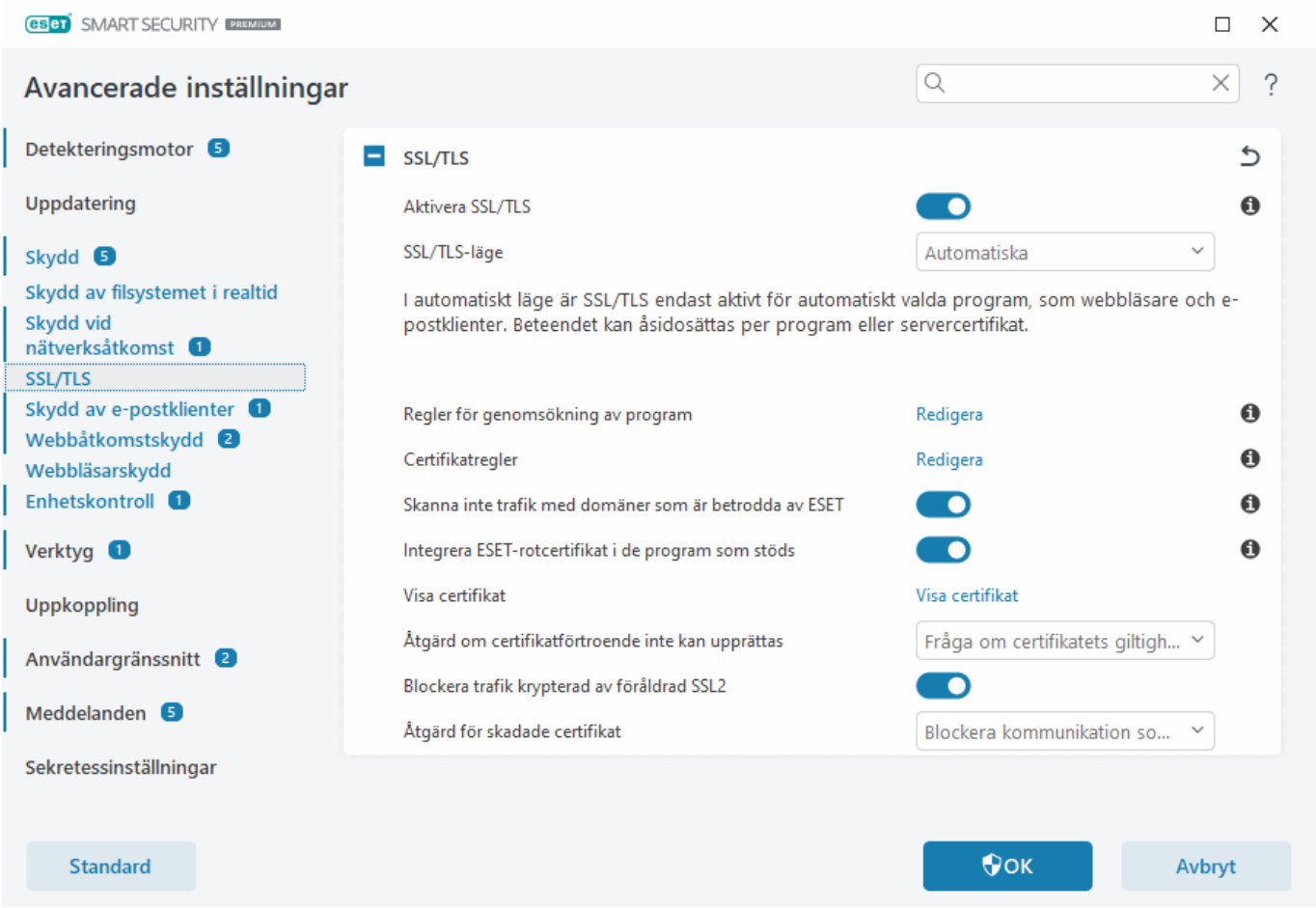
- **Tillåt kommunikation med tjänsten Server Service** – för mer information om den här tjänsten, se [MS-SRVS].

- **Tillåt kommunikation med övriga tjänster** – övriga MSRPC-tjänster. MSRPC är Microsofts implementering av DCE RPC-mekanismen. MSRPC kan dessutom använda namngivna pipes till SMB-protokollet (fildelning i nätverk) för transport (ncacn_np-transport). MSRPC-tjänster erbjuder gränssnitt för fjärråtkomst och -hantering av Windows-system. Flera sårbarheter har identifierats och utnyttjats på marknaden i Windows MSRPC-systemet (Conficker-mask, Sasser-mask osv.). Inaktivera kommunikation med MSRPC-tjänster som du inte behöver för att minimera många säkerhetsrisker (till exempel fjärrkörning av kod eller attacker som orsakar fel på tjänster).

SSL/TLS

ESET Smart Security Premium kan söka efter kommunikationshot som använder SSL-protokollet. Det går att använda olika filtreringslägen för att undersöka SSL-skyddad kommunikation med betrodda certifikat, okända certifikat eller certifikat som är undantagna från kontroll av SSL-skyddad kommunikation. Om du vill redigera

SSL/TLS-inställningar ska du öppna Avancerade inställningar > **Skydd** > **SSL/TLS**.



Aktivera SSL/TLS – om alternativet är inaktiverat genomsöker ESET Smart Security Premium inte kommunikationen via SSL/TLS.

SSL/TLS-läge finns i följande alternativ:

Filtreringsläge	Beskrivning
Automatisk	I standardläget genomsöks endast lämpliga program som webbläsare och e-postklienter. Du kan åsidosätta det genom att välja programmen där kommunikationen genomsöks.
Interaktivt	Om du anger en ny SSL-skyddad plats (med ett okänt certifikat) visas en dialogruta med åtgärdsalternativ. Detta läge gör det möjligt att skapa en lista med SSL-certifikat/program som ska undantas från genomsökning.
Principbaserat	Välj detta alternativ för att genomsöka all SSL-skyddad kommunikation utom kommunikation skyddad av certifikat undantagna från kontroll. Om ny kommunikation upprättas som använder ett okänt, signerat certifikat, meddelas du inte om detta och kommunikationen filtreras automatiskt. När du öppnar en server med ett obetrott certifikat som markerats som betrott (det finns i listan betrodda certifikat), tillåts kommunikation med servern och innehållet i kommunikationskanalen filtreras.

Regler för programgenomsökning – gör att du kan anpassa hur ESET Smart Security Premium ska bete sig för specifika program.

Certifikatregler – gör att du kan anpassa hur ESET Smart Security Premium ska bete sig för specifika SSL-certifikat.

Genomsök inte trafik med domäner som är betrodda av ESET – när det här alternativet är aktiverat undantas

kommunikation med betrodda domäner från genomsökning. En ESET-hanterad, inbyggd vitlista avgör en domäns tillförlitlighet.

Integrera ESET-rotcertifikat i de program som stöds – för att SSL-kommunikation ska fungera korrekt i webbläsare och e-postklienter är det viktigt att rotcertifikatet för ESET läggs till i listan över kända rotcertifikat (utgivare). När detta aktiveras lägger ESET Smart Security Premium automatiskt till ESET SSL Filter CA-certifikatet till kända webbläsare (t.ex. Opera). För webbläsare som lagrar uppgifter om systemcertifiering läggs certifikatet automatiskt. Till exempel, så konfigureras Firefox automatiskt att lita på rotutgivare i lagringen av systemcertifiering.

Om du vill lägga till certifikatet i webbläsare som inte stöds klickar du på **Visa certifikat** > **Information** > **Kopiera till fil** och importerar det manuellt till webbläsaren.

Åtgärd om certifikatförtroende inte kan upprättas – i vissa fall kan ett webbplatscertifikat inte verifieras med hjälp av TRCA-arkivet (Trusted Root Certification Authorities) (till exempel utgånget certifikat, ej betrott certifikat, certifikat som inte är giltigt för den specifika domänen eller signatur som kan tolkas men inte signerar certifikatet korrekt). Legitima webbplatser använder alltid betrodda certifikat. Om de inte tillhandahåller ett kan det innebära att en angripare dekrypterar din kommunikation eller att webbplatsen har tekniska problem.

Om **Fråga om certifikatets giltighet** har valts (standard) ombeds du att välja en åtgärd att vidta när krypterad kommunikation upprättas. En dialogruta för val av åtgärd visas där det går att markera certifikatet som betrott eller undantaget. Om certifikatet inte finns på TRCA-listan är fönstret rött. Om certifikatet finns på TRCA-listan är fönstret grönt.

Det går att ställa in alternativet **Blockera kommunikation som använder certifikatet** för att alltid avsluta en krypterad anslutning en webbplats som använder ett ej betrott certifikat.

Blockera trafik krypterad med föråldrad SSL2 – kommunikation som använder den tidigare versionen av SSL-protokollet blockeras automatiskt.

Åtgärd för skadade certifikat – ett skadat certifikat innebär att certifikatet använder ett format som inte känns igen av ESET Smart Security Premium eller har tagits emot skadat (till exempel har skrivits över av slumpmässiga data). I det här fallet rekommenderar vi att du lämnar **Blockera kommunikation som använder certifikatet** valt. Om **Fråga om certifikatets giltighet** har valts uppmanas användaren att välja en åtgärd som ska vidtas när den krypterade kommunikationen upprättas.

> **Illustrerade exempel**
>
> Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:
> - Certifikatmeddelanden i ESET:s Windows-hemprodukter
> - ”Krypterad nätverkstrafik: ej betrott certifikat” visas när webbplatser besöks

Regler för genomsökning av program

Reglerna för genomsökning av program kan användas för att anpassa hur ESET Smart Security Premium ska bete sig för specifika program samt för att komma ihåg åtgärder som har valts när **SSL/TLS-läge** är i **Interaktivt läge**. Listan kan visas och redigeras i Avancerade inställningar > **Skydd** > **SSL/TLS** > **Regler för genomsökning av program** > **Redigera**.

Fönstret **Regler för genomsökning av program** består av:

Kolumner

Program – välj en körbar fil i katalogträdet, klicka på alternativet **...** eller ange sökvägen för hand.

Genomsökningsåtgärd – välj **Genomsök** eller **Ignorera** för att genomsöka eller ignorera kommunikation. Välj **Auto** för att genomsöka i automatiskt läge och fråga i interaktivt läge. Välj **Fråga** för att alltid fråga användaren om vad som ska göras.

Kontrollelement

Lägg till – lägg till filtrerat program.

Redigera – välj det program du vill konfigurera och klicka på **Redigera**.

Ta bort – välj det program du vill ta bort och klicka på **Ta bort**.

Importera/exportera – importera program från en fil eller spara den aktuella listan med program i en fil.

OK/Avbryt – klicka på **OK** om du vill spara ändringarna eller på **Avbryt** om du vill avsluta utan att spara.

Certifikatregler

Certifikatregler kan användas för att anpassa hur ESET Smart Security Premium ska bete sig för specifika SSL-certifikat och för att komma ihåg åtgärder som valts när **SSL/TLS-läget** är i **Interaktivt läge**. Listan kan visas och redigeras i Avancerade inställningar > **Skydd** > **SSL/TLS** > **Certifikatregler** > **Redigera**.

Fönstret **Certifikatregler** består av:

Kolumner

Namn – certifikatets namn.

Certifikatutgivare – namnet på den som skapat certifikatet.

Certifikatämne – ämnesfältet identifierar den enhet som är associerad med den offentliga nyckel som lagras i fältet för ämnets offentliga nyckel.

Åtkomst – välj **Tillåt** eller **Blockera** som **Åtkomståtgärd** för att tillåta/blockera kommunikation som säkrats av certifikatet oavsett dess tillförlitlighet. Välj **Auto** för att tillåta betrodda certifikat och fråga om obetrodda. Välj **Fråga** för att alltid fråga användaren om vad som ska göras.

Genomsök – välj **Genomsök** eller **Ignorera** som **Genomsökningsåtgärd** för att genomsöka eller ignorera kommunikation som säkrats av certifikatet. Välj **Auto** för att genomsöka i automatiskt läge och fråga i interaktivt läge. Välj **Fråga** för att alltid fråga användaren om vad som ska göras.

Kontrollelement

Lägg till – lägg till ett nytt certifikat och justera dess inställningar oavsett alternativ för åtkomst och genomsökning.

Redigera – välj det certifikat du vill konfigurera och klicka på **Redigera**.

Ta bort – välj det certifikat du vill ta bort och klicka på **Ta bort**.

OK/Avbryt – klicka på **OK** om du vill spara ändringarna eller på **Avbryt** om du vill avsluta utan att spara.

Krypterad nätverkstrafik

Om systemet är konfigurerat att använda genomsökning av SSL/TLS visas en dialogruta där du kan välja en åtgärd i två situationer:

För det första, om en webbplats använder ett certifikat som inte kan verifieras eller är ogiltigt, och om ESET Smart Security Premium är konfigurerat att fråga användaren i sådana fall (som standard ja för certifikat som inte kan verifieras, nej för ogiltiga certifikat), så visas en dialogruta där du får välja att **Tillåta** eller **Blockera** anslutningen. Om certifikatet inte är placerat i Trusted Root Certification Authorities store (TRCA) anses det vara ej betrott.

För det andra, om **SSL/TLS-läget** är inställt till **Interaktivt läge** visas en dialogruta för varje webbplats där du får välja om du vill **Genomsöka** eller **Ignorera** trafiken. Vissa program kontrollerar att deras SSL-trafik inte ändras eller inspekteras av någon, och i sådana fall måste ESET Smart Security Premium **Ignorera** den trafiken för att programmet ska fortsätta fungera.

> **Illustrerade exempel**
>
> Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:
> - Certifikatmeddelanden i ESET:s Windows-hemprodukter
> - ”Krypterad nätverkstrafik: ej betrott certifikat” visas när webbplatser besöks

I båda fallen kan användaren välja att den valda åtgärden ska kommas ihåg. Sparade åtgärder lagras i Certifikatregler.

Skydd av e-postklient

Om du vill konfigurera Skydd för e-postklienter ska du öppna Avancerade inställningar > **Skydd** > **Skydd av e-postklienter** och välja bland följande konfigurationsalternativ:

- Skydd av e-postöverföring
- Inkorgsskydd
- Hantering av adresslistor
- ThreatSense

Skydd av e-postöverföring

IMAP(S) och POP3(S) är de vanligaste protokollen som används för att ta emot e-postkommunikation i en e-postklient. Internet Message Access Protocol är ett annat Internetprotokoll för hämtning av e-post. IMAP har en del fördelar framför POP3, t.ex. kan flera klienter samtidigt ansluta till samma brevlåda och upprätthålla information om meddelandetillstånd, om meddelandet har lästs, besvarats eller tagits bort. Skyddsmodulen för

denna kontroll startas automatiskt vid systemstart och är sedan aktivt i minnet.

ESET Smart Security Premium ger skydd för dessa protokoll oavsett vilken e-postklient som används och utan att e-postklienten behöver omkonfigureras. Som standard genomsöks alla kommunikation via POP3- och IMAP-protokoll, oavsett standard-POP3/IMAP-portnumren.
MAPI-protokollet genomsöks inte. Kommunikationen med Microsoft Exchange-servern kan dock genomsökas av integrationsmodulen i e-postklienter som till exempel Microsoft Outlook.

ESET Smart Security Premium har även stöd för genomsökning av IMAPS-protokoll (585, 993) och POP3S-protokoll (995), som använder en krypterad kanal för att överföra information mellan server och klient. ESET Smart Security Premium kontrollerar kommunikationen med SSL-kryptering (Secure Socket Layer) och TLS-kryptering (Transport Layer Security).
Krypterad kommunikation genomsöks som standard. Om du vill visa skannerinställningarna ska du öppna Avancerade inställningar > **Skydd** > SSL/TLS.

Om du vill konfigurera Skydd av e-posttransport ska du öppna Avancerade inställningar > **Skydd** > **Skydd av e-postklienter** > **Skydd av e-posttransport**.

Aktivera Skydd av e-posttransport – när det här alternativet är aktiverat genomsöks e-posttransportkommunikation av ESET Smart Security Premium.

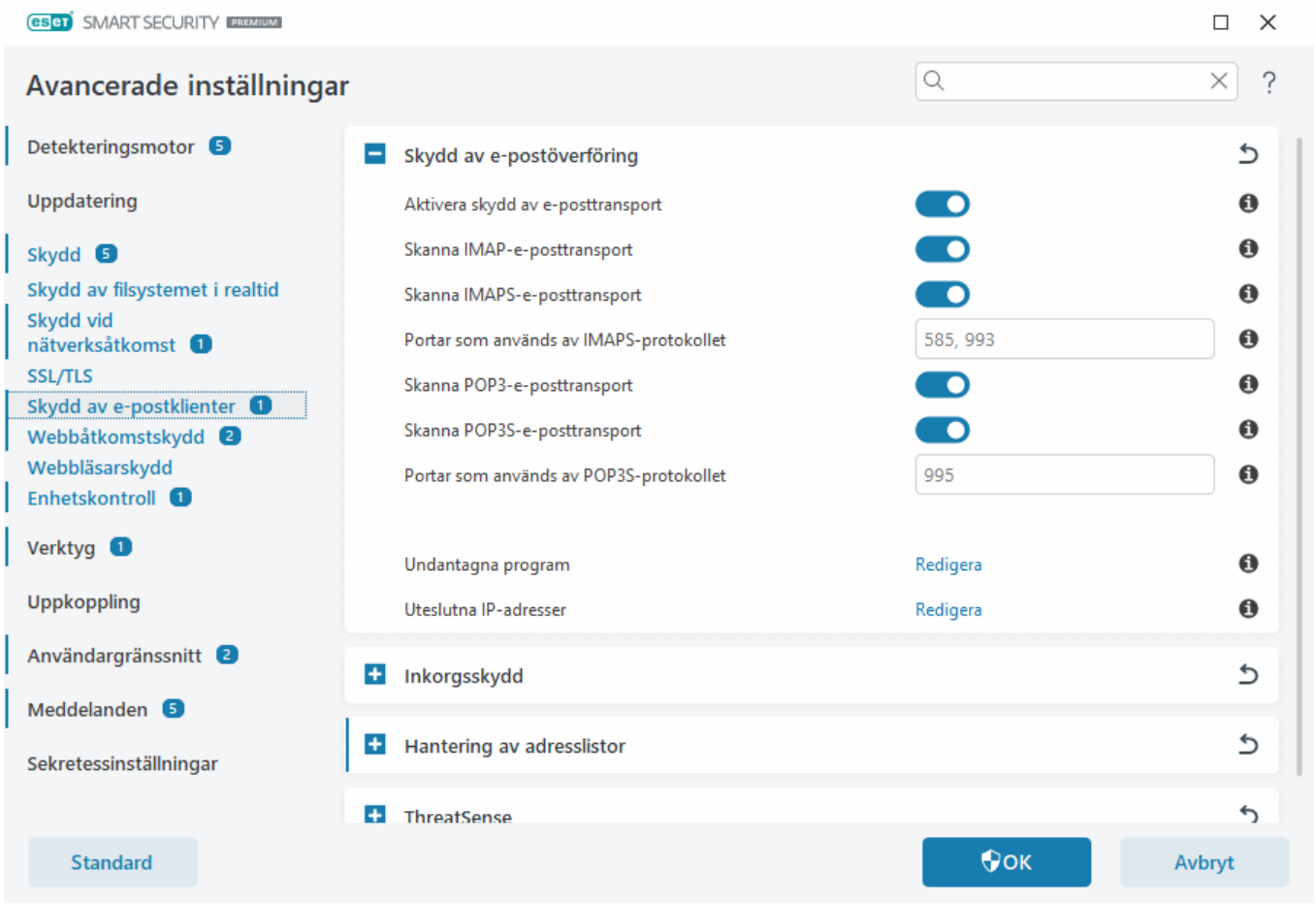
Du kan välja vilka e-posttransportprotokoll som ska genomsökas genom att klicka på växlingsknappen bredvid följande alternativ (som standard är genomsökning av alla protokoll aktiverad):

- **Skanna IMAP-e-posttransport**
- **Skanna IMAPS-e-posttransport**
- **Skanna POP3S-e-posttransport**
- **Skanna POP3S-e-posttransport**

Som standard genomsöker ESET Smart Security Premium IMAPS- och POP3S-kommunikation på standardportarna. Om du vill lägga till anpassade portar för IMAPS- och POP3S-protokoll ska du lägga till dem i textfältet bredvid **Portar som används av IMAPS-protokollet** eller **Portar som används av POP3S-protokollet**. Flera portnummer måste avgränsas med kommatecken.

Undantagna program – gör att du kan undanta specifika program från att genomsökas av Skydd av e-posttransport. Användbart när Webbåtkomstskydd orsakar kompatibilitetsproblem.

Undantagna IP-adresser – gör att du kan undanta specifika fjärradresser från att genomsökas av Skydd av e-posttransport. Användbart när Webbåtkomstskydd orsakar kompatibilitetsproblem.



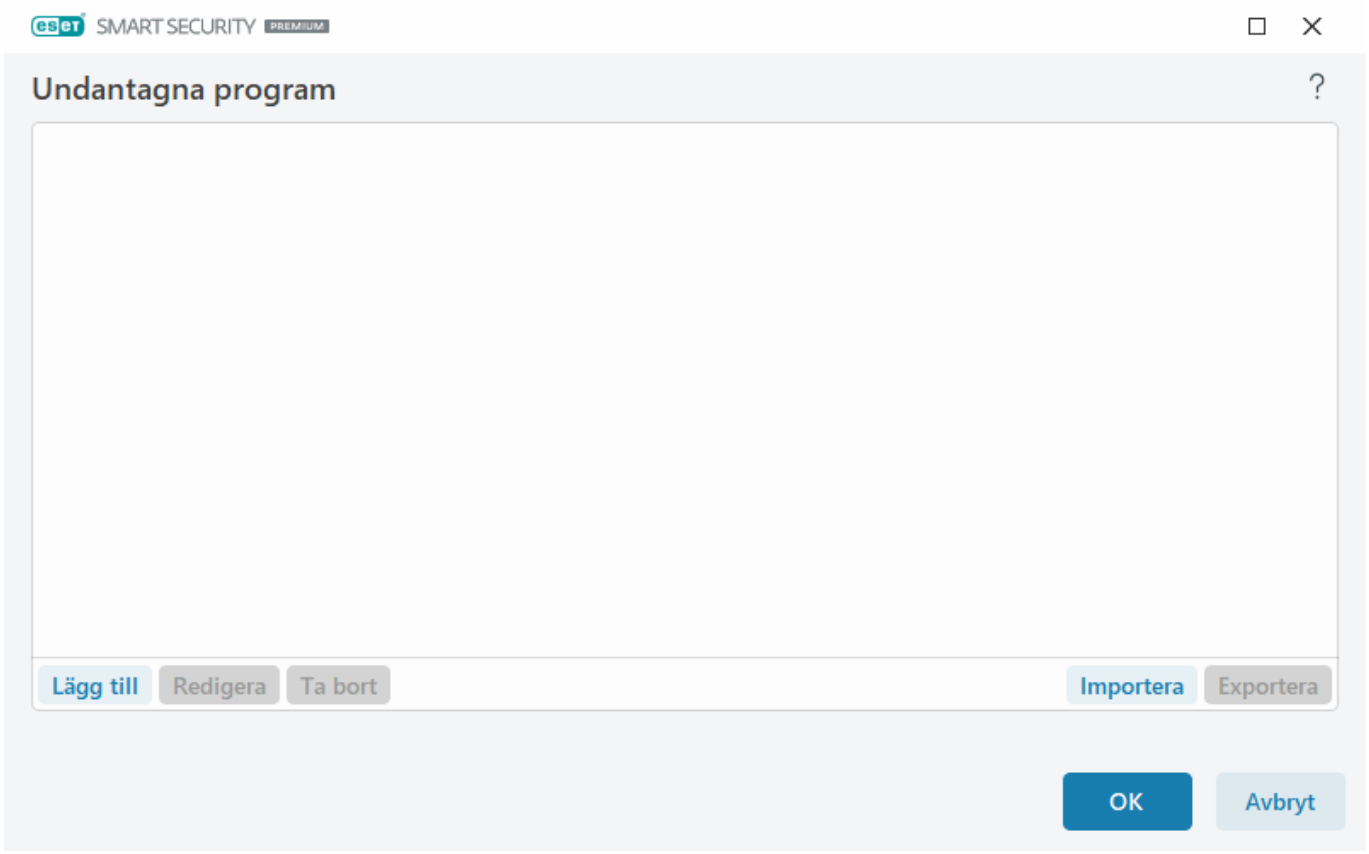
Undantagna program

Om du vill utesluta genomsökning av kommunikation för specifika program ska du lägga till dem i listan. De valda programmens HTTP(S)/POP3(S)/IMAP(S)-kommunikation kontrolleras inte. Vi rekommenderar att endast använda detta för program som inte fungerar normalt när deras kommunikation kontrolleras.

Aktiva program och tjänster är automatiskt tillgängliga här när du klickar på **Lägg till**. Klicka på **...** och gå till ett program för att lägga till undantaget manuellt.

Redigera – redigera valda poster i listan.

Ta bort – tar bort valda poster från listan.



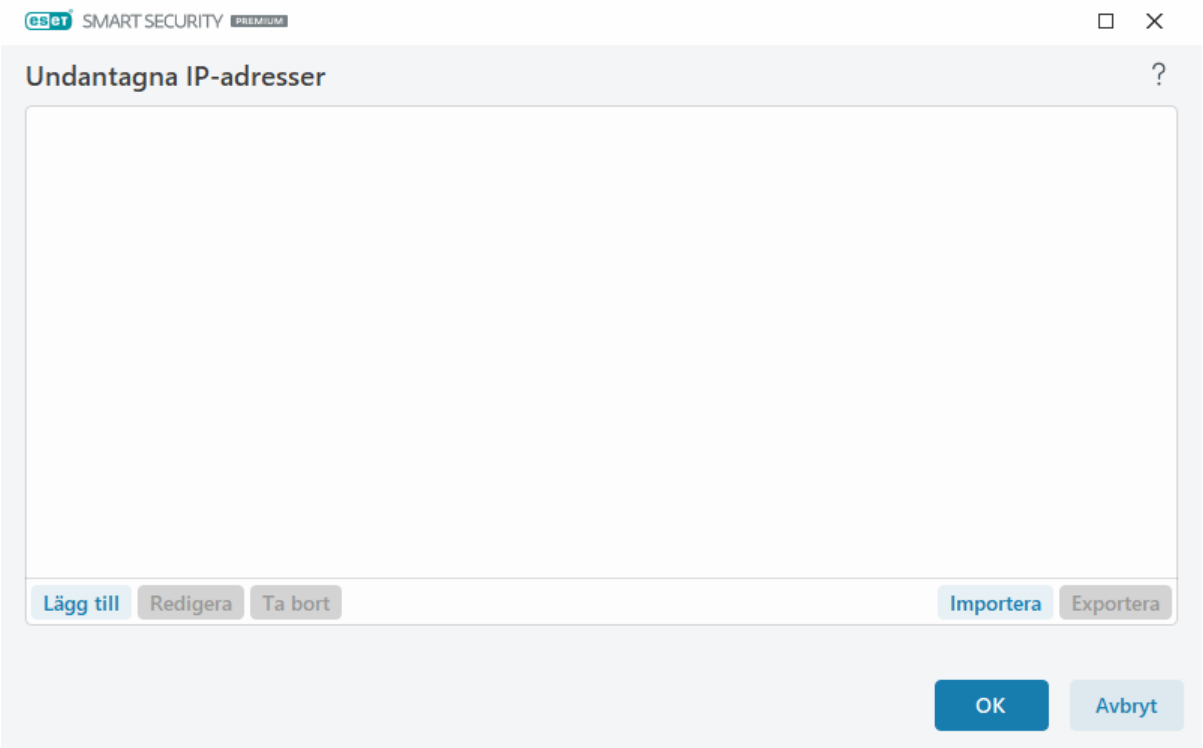
Uteslutna IP-adresser

Posterna på listan undantas från genomsökning. HTTP(S)/POP3(S)/IMAP(S)-kommunikation från/till de valda adresserna kontrolleras inte. Vi rekommenderar att du endast använder detta alternativ för adresser som är kända som trovärdiga.

Klicka på **Lägg till** om du vill undanta en IP-adress/ett adressintervall/ett undernät till en fjärrpunkt.

Klicka på **Redigera** för att ändra vald IP-adress.

Klicka på **Ta bort** om du vill ta bort valda poster från listan.



Exempel på IP-adresser

Lägg till IPv4-adress:
Enskild adress – lägger till en IP-adress för en enskild dator (till exempel *192.168.0.10*).
Adressintervall – ange den första och den sista IP-adressen för att ange IP-intervallet för flera datorer (till exempel *192.168.0.1–192.168.0.99*).
Undernät – undernät (en grupp datorer) definierade av en IP-adress och en mask. 255.255.255.0 är till exempel nätverksmasken för undernätet 192.168.1.0. Om du vill undanta hela undernätet ska du skriva *192.168.1.0/24*.
Lägg till IPv6-adress:
Enskild adress – lägger till en IP-adress för en enskild dator (till exempel *2001:718:1c01:16:214:22ff:fec9:ca5*).
Undernät – undernät (en grupp datorer) som definieras av en IP-adress och en mask (till exempel: *2002:c0a8:6301:1::1/64*).

Inkorgsskydd

Integrering av ESET Smart Security Premium med din inkorg ökar nivån av aktivt skydd mot skadlig kod i e-postmeddelanden.

Om du vill konfigurera Inkorgsskydd ska du öppna Avancerade inställningar > **Skydd** > **Skydd av e-postklienter** > **Inkorgsskydd**.

Aktivera e-postskydd genom klient-plugin-program – när det här alternativet är inaktiverat är skyddet för klient-plugin-program avstängt.

Välj e-postmeddelanden som ska genomsökas:

- **Mottagen e-post**
- **Skickad e-post**

- **Läst e-post**
- **Ändrad e-post**

Vi rekommenderar att du låter **Aktivera e-postskydd genom klient-plugin-program** vara aktiverat. EnÄven om integrering inte är aktiveras eller inte fungerar skyddas e-postkommunikationen av modulen Skydd av e-postklienter genom Skydd av e-posttransport (IMAP/IMAPS och POP3/POP3S).

Skanna efter skräppost

Oönskad e-post, även kallat spam, är ett av de största problemen inom elektronisk kommunikation. Spam utgör upp till 30 procent av all e-postkommunikation. Skräppostskydd för e-postklient skyddar mot det här problemet. Skräppostskydd för e-postklient kombinerar flera e-postsäkerhetsprinciper vilket ger en överlägsen filtrering och håller inkorgen ren. För spamdetektering är en viktig princip att känna igen oönskade e-postmeddelanden baserat på fördefinierade betrodda adresser (tillåtna) och spamadresser (blockerade).

Den huvudsakliga metoden som används för detektering av spam är genomsökning av egenskaper i e-postmeddelanden. Mottagna meddelanden genomsöks med avseende på grundläggande spamskyddskriterier (meddelandedefinitioner, statistisk heuristik, identifieringsalgoritmer och andra unika metoder) och det resulterande indexvärdet anger om ett meddelande är spam.

Aktivera Skräppostskydd för e-postklient – när det här alternativet är aktiverat genomsöks mottagna meddelanden efter skräppost.

Använd avancerad skräppostskanner – ytterligare skräppostdata laddas ned regelbundet vilket ökar skräppostskyddet och ger bättre resultat.

Spampoängloggning – ESET Smart Security Premium Antispam-motorn tilldelar en spampoäng till varje genomsökt meddelande. Meddelandet registreras i Spamskyddsloggen (programmets huvudfönster > **Verktyg** > **Loggfiler** > **Skräppostskydd för e-postklient**).

- **Ingen** – poängen från antispamgenomsökningen loggas inte.
- **Omklassificerat och märkt som spam** – markera detta om du vill registrera spampoäng för meddelanden markerade som SPAM.
- **Alla** – alla meddelanden registreras i loggen med en spampoäng.

När du klickar på ett meddelande i mappen för spam kan du välja **Klassificera om markerade meddelanden som inte spam** om du vill flytta meddelandet till inkorgen. När du klickar på ett meddelande du anser vara spam i inkorgen kan du välja **Klassificera om meddelanden som spam** om du vill flytta meddelandet till mappen för spam. Du kan välja flera meddelanden och agera på dem alla samtidigt.

Optimering av hantering av bifogade filer – om optimering är inaktiverat genomsöks alla bifogade filer omedelbart. Du kan uppleva en att e-postklientens prestanda blir långsammare.

Integrationer – gör att du kan integrera Inkorgsskydd i din e-postklient. Du hittar mer information i Integrationer.

Svar – gör att du kan anpassa hanteringen av skräppostmeddelanden. Du hittar mer information i Svar.

Integrationer

Integrering av ESET Smart Security Premium med din e-postklient ökar nivån av aktivt skydd mot skadlig kod i e-postmeddelanden. Om din e-postklient stöds kan du aktivera integrering i ESET Smart Security Premium. När e-postklienten har integrerats infogas ESET Smart Security Premium-verktygfältet direkt i den och ger mer effektivt e-postskydd. Om du vill redigera Integreringsinställningar ska du öppna Avancerade inställningar > **Skydd** > **Skydd av e-postklienter** > **Inkorgsskydd** > **Integrering**.

Integrera med Microsoft Outlook – Microsoft Outlook är för närvarande den enda e-postklienten som stöds. Skydd av e-post fungerar som ett plugin-program. Den största fördelen med plugin-program är att det inte spelar någon roll vilket protokoll som används. När e-postklienten tar emot ett krypterat meddelande dekrypteras det och skickas till virusgenomsökaren. Se den här artikeln i ESET:s kunskapsbas för en fullständig lista över Microsoft Outlook-versioner som stöds.

Avancerad bearbetning av e-postklienter – bearbetar extra Outlook Messaging API (MAPI)-händelser: Objekt ändrat (`fnevObjectModified`) och Objekt skapat (`fnevObjectCreated`). Om du märker att systemet går långsammare när du använder e-postklienten kan du aktivera det här alternativet.

Verktygsfält i Microsoft Outlook

Skyddet för Microsoft Outlook fungerar som en plugin-modul. När ESET Smart Security Premium har installerats läggs det här verktygsfältet som innehåller antivirusskyddet och Skräppostskydd för e-postklient till i Microsoft Outlook:

Spam – markerar valda meddelanden som spam. När ett meddelande har markerats skickas ett ”fingeravtryck” av det till en central server som lagrar spamsignaturer. Om servern får liknande ”fingeravtryck” från flera användare klassificeras meddelandet som spam i framtiden.

Inte spam – markerar valda meddelanden som inte spam.

Skräppostadress (blockerad, en lista över spamadresser) – lägger till en ny avsändaradress i adresslistan som blockerad. Alla meddelanden som tas emot och som finns på listan klassificeras automatiskt som spam.

> ⚠ Se upp med så kallad spoofing – avsändaradresser på e-postmeddelanden förfalskas för att lura e-postmottagare att läsa och svara på meddelandet.

Betrodd adress (tillåten, en lista över tillåtna adresser) – lägger till en ny avsändaradress i adresslistan som tillåten. Alla meddelanden som tas emot från tillåtna adresser klassificeras aldrig automatiskt som spam.

ESET Smart Security Premium – Dubbelklicka på ikonen för att öppna huvudfönstret i ESET Smart Security Premium.

Kontrollera e-post – startar kontroll av e-post manuellt. Du kan ange vilka meddelanden som ska kontrolleras och du kan aktivera genomsökning av mottagna meddelanden på nytt. Du hittar mer information i Inkorgsskydd.

Inställning av skanner – visar inställningsalternativ för Inkorgsskydd.

Inställning av skräppostskydd – visar inställningsalternativ för Inkorgsskydd.

Adressböcker – öppnar fönstret Hantering av adresslistor där du har tillgång till listor över adresser som är undantagna, betrodda och spam.

Bekräftelsedialogruta

Meddelandet bekräftar att du verkligen vill utföra den valda åtgärden och eliminerar möjliga misstag.

Å andra sidan går det också att stänga av bekräftelser från dialogrutan.

Genomsök meddelanden på nytt

Med det integrerade verktygsfältet för ESET Smart Security Premium i e-postklienter går det att ange flera alternativ för att kontrollera e-post. Alternativet **Genomsök meddelanden på nytt** erbjuder två genomsökningslägen:

Alla meddelanden i den aktuella mappen – genomsöker meddelanden i den visade mappen.

Endast markerade meddelanden – genomsöker endast meddelanden markerade av användaren.

Kryssrutan **Genomsök redan genomsökta meddelanden på nytt** ger användaren möjlighet att köra en ny genomsökning på redan genomsökta meddelanden.

Svar

Baserat på resultaten från meddelandegenomsökning kan ESET Smart Security Premium flytta genomsökta meddelanden eller lägga till anpassad text i ämnet. Du kan konfigurera de här inställningarna i Avancerade inställningar > **Skydd** > **Skydd av e-postklienter** > **Inkorgsskydd** > **Svar**.

Med Skräppostskydd för e-postklient i ESET Smart Security Premium kan du konfigurera följande parametrar för meddelanden:

Lägg till text till ämne i e-postmeddelande – gör det möjligt att lägga till en anpassad textsträng till ämnesraden i meddelanden som har klassificerats som spam. **Standardtexten** är ”[SPAM]”.

Flyttat till skräppostmapp – när det här alternativet valts flyttas spammeddelanden till standardmappen för spam och dessutom flyttas meddelanden som omklassificerats till inte spam till inkorgen. När du högerklickar på ett e-postmeddelande och väljer ESET Smart Security Premium i kontextmenyn kan du välja bland tillämpliga alternativ.

Flytta till anpassad mapp – när det här alternativet är aktiverat flyttas skräppostmeddelanden till en mapp som anges nedan.

Mapp – ange den anpassade mapp dit du vill flytta infekterad e-post när de upptäckts.

Om det finns ett meddelande som innehåller detektering försöker ESET Smart Security Premium rensa meddelandet som standard. Om meddelandet inte kan rensas kan du välja en **åtgärd att vidta om rensning inte är möjlig**:

- **Ingen åtgärd** – om aktiverat identifieras infekterade bilagor, men ingen åtgärd vidtas för e-postmeddelanden.

- **Ta bort e-post** – användaren får ett meddelande om infiltration(er) och e-postmeddelandet tas bort.
- **Flytta e-postmeddelande till mappen Borttaget** – infekterade e-postmeddelanden flyttas automatiskt till mappen Borttaget.
- **Flytta e-postmeddelande till mappen** (standardåtgärd) – infekterade e-postmeddelanden flyttas automatiskt till den angivna mappen.

Mapp – ange den anpassade mapp dit du vill flytta infekterad e-post när de upptäckts.

Markera spammeddelanden som lästa – aktivera detta om du vill markera spammeddelanden som lästa automatiskt. Det gör det lättare att fokusera på "rena" meddelanden.

Markera omklassificerade meddelanden som olästa – meddelanden som först klassificerades som spam men som senare markerats som ”rena” visas som olästa.

Efter att ett e-postmeddelande har kontrollerats bifogas ett meddelande med genomsökningsresultatet till e-postmeddelandet. Välj **Lägg till meddelanden till mottagen och läst e-post** eller **Lägg till meddelanden till skickad e-post**. Tänk på att meddelandena i sällsynta fall kan undantas i problematiska HTML-meddelanden eller om meddelanden förfalskas av skadlig kod. Meddelanden kan läggas till i mottagen och läst e-post, i skickad e-post eller i båda. Följande alternativ finns tillgängliga:

- **Aldrig** – inga meddelanden läggs till.
- **När en detektering inträffar** – endast meddelanden som innehåller skadlig programvara märks som kontrollerad (standard).
- **Till all e-post vid genomsökning** – programmet lägger till meddelanden till all genomsökt e-post.

Uppdatera ämnet för mottaget och läst e-postmeddelande/Uppdatera ämnet för skickat e-postmeddelande – aktivera det här alternativet om du vill lägga till anpassad text som anges nedan i meddelandet.

Text som ska läggas till i ämnet i det infekterade e-postmeddelandet – redigera mallen om du vill ändra ämnesradens format i ett infekterat e-postmeddelande. Denna funktion ersätter ämnesraden "Hej" till följande format: ”[detekteringens %DETEKTERINGSNAMN%] Hello". Variabeln %DETECTIONNAME% representerar detekteringen.

Hantering av adresslistor

Med funktionen Skräppostskydd för e-postklient i ESET Smart Security Premium går det att konfigurera olika parametrar för adressböcker. Om du vill konfigurera adresslistor ska du öppna Avancerade inställningar > **Skydd** > **Skydd av e-postklienter** > **Hantering av adresslistor**.

Aktivera användarens adresslista – aktivera det här alternativet för att aktivera användarens adresslista.

Användarens adresslista – en lista över e-postadresser där du kan lägga till, redigera eller ta bort adresser för att definiera antispamreglerna. Regler i den här listan tillämpas på den aktuella användaren.

Aktivera globala adresslistor – aktivera det här alternativet för att aktivera den globala adresslistan som delas av alla användare på enheten.

Global adresslista – en lista över e-postadresser där du kan lägga till, redigera eller ta bort adresser för att definiera antispamreglerna. Reglerna i den här listan tillämpas på alla användare.

Tillåt och lägg automatiskt till på användarens adresslista

Behandla adresser i adressboken som betrodda – Adresser på kontaktlistan behandlas som betrodda utan att läggas till på användarens adresslista.

Lägg till mottagaradresser från utgående meddelanden – lägg till mottagaradresser från skickade meddelanden till användarens adresslista som tillåtna.

Lägg till adresser från meddelanden som har klassificerats om som INTE spam – lägg till avsändaradresser från meddelanden som omklassificerats som INTE spam till användarens adresslista som tillåtna.

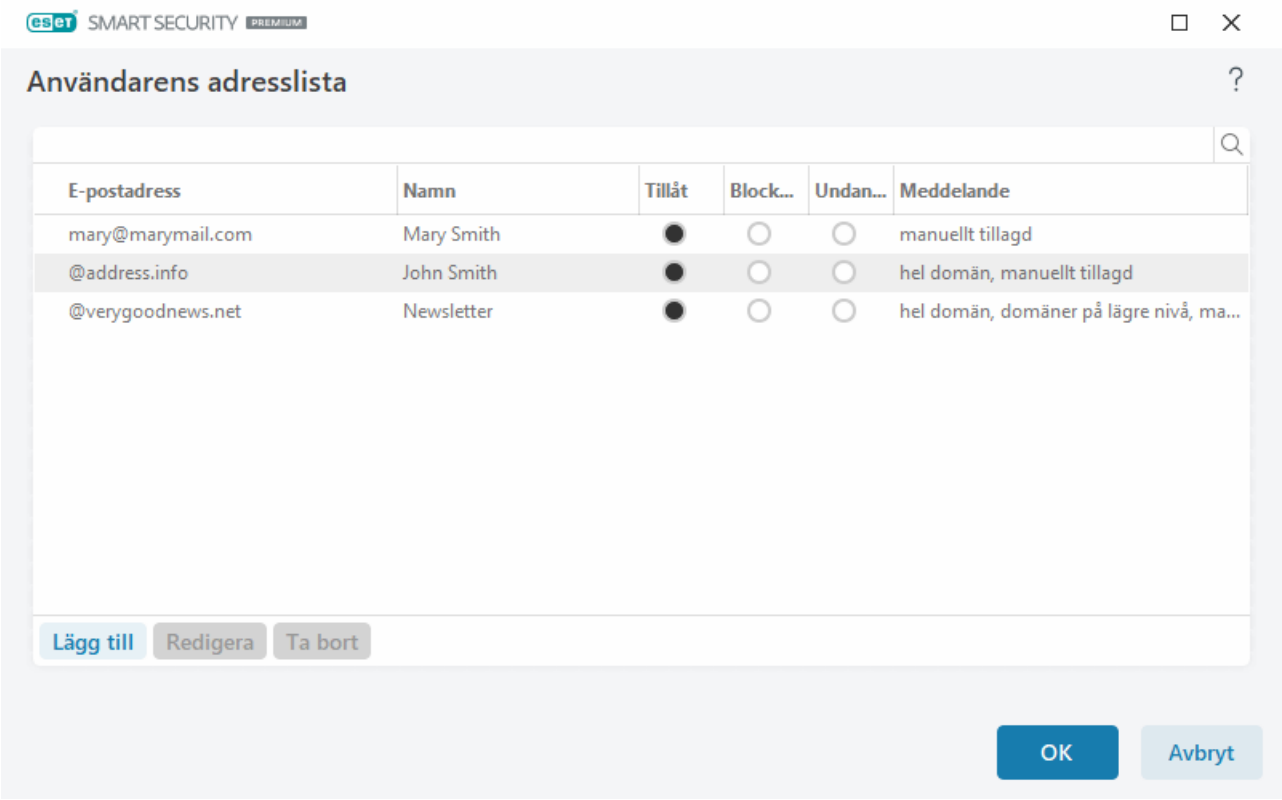
Lägg automatiskt till på användarens adresslista som ett undantag

Lägg till adresser från egna konton – lägg till adresser från befintliga e-postklientkonton till användarens adresslista som ett undantag.

Adresslistor

För att skyddas mot oönskade e-postmeddelanden kan du klassificera e-postadresser i adresslistor i ESET Smart Security Premium.

Om du vill redigera adresslistor ska du öppna Avancerade inställningar > **Skydd** > **Skydd av e-postklienter** > **Hantering av adresslistor** och klicka på **Redigera** bredvid **Användares adresslista** eller **Global adresslista**.



Kolumner

E-postadress – den adress som regeln ska gälla för. Jokertecken stöds inte.

Namn – anpassat regelnamn.

Tillåt/Blockera/Undantag – alternativknappar som används för att avgöra vilken åtgärd som ska vidtas för e-postadressen (klicka på alternativknappen i önskad kolumn för att snabbt ändra åtgärden):

- **Tillåt** – adresser som anses vara säkra och från vilka du vill ta emot meddelanden.
- **Blockera** – adresser som anses vara osäkra/spam och som du inte vill ta emot meddelanden från.
- **Undantag** – adresser som alltid kontrolleras för spam och som kan förfalskas och användas för att skicka spam.

Anmärkning – information om hur regeln skapades och om den gäller för hela domänen/domäner på lägre nivå.

Hantera adresserna

- **Lägg till** – klicka för att lägga till en regel för en ny adress.
- **Redigera** – välj och klicka för att redigera en befintlig regel.
- **Ta bort** – välj och klicka om du vill ta bort en regel från adresslistan.

Lägg till/redigera adress

I det här fönstret kan du lägga till eller redigera en adress i Hantering av adresslista och konfigurera den åtgärd som ska vidtas:

E-postadress – den adress som regeln ska gälla för.

Namn – anpassat regelnamn.

Åtgärd – den åtgärd som ska vidtas om kontaktens e-postadress matchar den adress som anges i fältet **E-postadress**:

- **Tillåt** – adresser som anses vara säkra och från vilka du vill ta emot meddelanden.
- **Blockera** – adresser som anses vara osäkra/spam och som du inte vill ta emot meddelanden från.
- **Undantag** – adresser som alltid kontrolleras för spam och som kan förfalskas och användas för att skicka spam.

Hel domän – välj detta alternativ för regel som tillämpas på hela kontaktens domän (inte bara adressen som anges i fältet **E-postadress**, utan alla e-postadresser i domänen *address.info*).

Domäner på lägre nivå – välj detta alternativ för regel som tillämpas på kontaktens domäner på lägre nivå (*address.info* representerar domänen, medan *my.address.info* representerar en underdomän).

Resultat av adressbehandling

När du lägger till nya adresser eller ändrar den åtgärd som ska vidtas för e-postadressen ESET Smart Security Premium visas meddelanden. Innehållet i informationsmeddelandet beror på vilken åtgärd du försöker utföra.

Markera kryssrutan **Fråga inte igen** för att utföra åtgärden automatiskt utan att meddelandet visas nästa gång.

ThreatSense

ThreatSense består av många avancerade hotidentifieringsmetoder. ThreatSense är en proaktiv metod vilket innebär att den kan skydda datorn mot tidig spridning av ett nytt hot. Genom att kombinera kodanalys, kodemulering, generiska signaturer, virussignaturer och använda dem tillsammans ökas systemsäkerheten avsevärt. Genomsökningsmotorn kan kontrollera flera dataströmmar samtidigt vilket maximerar effektiviteten och upptäcktsfrekvensen. ThreatSense-tekniken eliminerar även framgångsrikt rootkits.

med alternativen för inställning av ThreatSense går det att ange ett antal olika genomsökningsparametrar:

- Filtyper och tillägg som genomsöks
- En kombination av olika identifieringsmetoder
- Rensningsnivåer, osv.

Öppna inställningsfönstret genom att klicka på **ThreatSense** i Avancerade inställningar för moduler som använder ThreatSense-teknik (se nedan). Olika säkerhetsscenarier kan kräva olika konfigurationer. Det går därmed att individuellt konfigurera följande skyddsmoduler i ThreatSense:

- Skydd av filsystemet i realtid
- Genomsökning vid inaktivitet
- Startskanner
- Dokumentskydd
- Skydd av e-postklienter
- Webbåtkomstskydd
- Genomsökning av datorn

ThreatSense-parametrarna är starkt optimerade för varje modul och ändringar av dem kan märkbart påverka systemets funktion. Att till exempel ändra parametrarna så att internt packade filer alltid söks igenom eller att aktivera avancerad heuristik i modulen för skydd av filsystemet i realtid kan resultera i att systemet blir långsammare (normalt används dessa metoder endast för genomsökning av nyskapade filer). Vi rekommenderar att lämna ThreatSense-standardparametrarna oförändrade för alla moduler utom för genomsökningsmodulen.

Objekt som ska genomsökas

I det här avsnittet går det att definiera vilka komponenter och filer på datorn som genomsöks efter infiltrationer.

Arbetsminne – söker efter hot som angriper systemets arbetsminne.

Startsektorer/UEFI – genomsöker startsektorerna efterskadlig kod i MBR (master boot record). Läs mer om UEFI i ordlistan.

E-postfiler – programmet stöder följande filnamnstillägg: DBX (Outlook Express) och EML.

Arkiv – programmet stöder följande filnamnstillägg: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE och många andra.

Självuppackande arkiv – självuppackande arkiv (SFX) är arkiv som kan extrahera sig själva.

Internt packade filer – när internt packade filer (till skillnad från standardarkivtyper) körs dekomprimeras de i minnet. Förutom statiska arkiverare av standardtyp (UPX, yoda, ASPack, FSG osv.) känner skannern igen många fler typer av arkiverare genom kodemulering.

Genomsökningsalternativ

Välj vilka metoder som ska användas för att söka efter infiltrationer i systemet. Följande alternativ finns tillgängliga:

Heuristik – heuristik är en algoritm som analyserar (skadliga) aktiviteter i program. Huvudfördelen med tekniken är möjligheten att identifiera skadlig programvara som inte fanns eller som inte var känd av den tidigare detekteringsmotorn. Nackdelen är (en mycket liten) risk för falska larm.

Avancerad heuristik/DNA-signaturer – avancerad heuristik är en unik heuristikalgoritm som utvecklats av ESET och som optimerats för att upptäcka datormaskar och trojanska hästar som skrivits på programmeringsspråk på hög nivå. Genom att använda avancerad heuristik blir ESET-produkterna bättre på att detektera hot. Signaturer används för att pålitligt detektera och identifiera virus. Med det automatiska uppdateringssystemet är nya signaturer tillgängliga inom några timmar efter att ett hot identifierades. Nackdelen med signaturer är att de bara detekterar virus de känner till (eller lätt ändrade versioner av dessa virus).

Rensning

Inställningarna för rensning anger hur ESET Smart Security Premium fungerar under rensning av infekterade objekt. Det finns fyra rensningsnivåer:

ThreatSense har följande åtgärdsnivåer (det vill säga rensningsnivåer).

Åtgärd i ESET Smart Security Premium

Rensningsnivå	Beskrivning
Åtgärda alltid detektering	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa sällsynta fall (till exempel systemfiler) lämnas det rapporterade objektet på sin ursprungliga plats om detekteringen inte kan åtgärdas.
Åtgärda detektering om det är säkert, behåll annars	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa fall (till exempel systemfiler eller arkiv med både rena och infekterade filer) lämnas det rapporterade objektet på sin ursprungliga plats om en detektering inte kan åtgärdas.

Rensningsnivå	Beskrivning
Åtgärda detektering om det är säkert, fråga annars	Försök att åtgärda detekteringen när du rensar objekt. I vissa fall, om ingen åtgärd kan utföras, får slutanvändaren en interaktiv avisering och måste välja en åtgärd (till exempel ta bort eller ignorera). Den här inställningen rekommenderas i de flesta fall.
Fråga alltid slutanvändaren	Ett interaktivt fönster visas för slutanvändaren när objekt rensas och en åtgärd måste väljas (till exempel ta bort eller ignorera). Denna nivå är avsedd för mer avancerade användare som vet vilka som ska åtgärder vidtas i händelse av detektering.

Undantag

Ett filnamnstillägg är den del av filnamnet som avgränsas med en punkt. Ett filändelse definierar filens typ och innehåll. I det här avsnittet för ThreatSense-inställningarna kan du definiera vilka typer av filer som ska genomsökas.

Övrigt

När du konfigurerar parameterinställningarna för ThreatSense-motorn för en Genomsökning av datorn på begäran är följande alternativ i avsnittet **Andra** också tillgängliga:

Genomsök alternativa dataströmmar (ADS) – de alternativa dataströmmarna som används av filsystemet NTFS består av fil- och mappassociationer som inte är synliga för vanliga genomsökningsmetoder. Många infiltrationsförsök maskerar sig som alternativa dataströmmar för att undvika upptäckt.

Kör genomsökningar i bakgrunden med låg prioritet – varje genomsökningssekvens kräver en viss mängd systemresurser. Om du arbetar med program som kräver mycket systemresurser kan du aktivera genomsökning i bakgrunden med låg prioritet och spara resurser till dina program.

Logga alla objekt – i genomsökningsloggen visas alla genomsökta filer i självuppackande arkiv, även sådana som inte är infekterade (detta kan generera mycket genomsökningsloggdata och öka genomsökningsloggfilens storlek).

Aktivera Smart optimering – med aktiverad smart optimering används de optimala inställningarna för effektivast genomsökning och bibehåller samtidigt den högsta genomsökningshastigheten. De olika skyddsmodulerna genomsöker intelligent och använder olika genomsökningsmetoder och tillämpar dem på vissa filtyper. Om smart optimering är inaktiverad tillämpas endast de användardefinierade inställningarna i ThreatSense-kärnan när en genomsökning utförs.

Bevara tidsstämpeln för senaste åtkomst – markera det här alternativet om du vill behålla den ursprungliga åtkomsttiden för genomsökta filer i stället för att uppdatera dem (t.ex. för användning med system för säkerhetskopiering av data).

Begränsningar

Under Begränsningar kan du ange en maximal storlek på objekt och nivåer på de nästlade arkiv som ska genomsökas:

Objektinställningar

Maximal objektstorlek – anger maximal storlek på objekt som ska genomsökas. Den angivna antivirusmodulen kommer endast att genomsöka objekt som är mindre än den angivna storleken. Alternativet ska endast ändras av avancerade användare som kan ha särskilda anledningar till att undanta större objekt från genomsökning. Standardvärde: obegränsat.

Maximal tid för genomsökning av objekt (sek.) – definierar det maximala tidsvärdet för genomsökning av filer i ett behållarobjekt (till exempel ett RAR/ZIP-arkiv eller ett e-postmeddelande med flera bilagor). Den här inställningen gäller inte för fristående filer. Om ett användardefinierat värde har angetts och den tiden har förflutit stoppas en genomsökning så snart som möjligt, oavsett om genomsökningen av varje fil i ett behållarobjekt har slutförts.
När det gäller ett arkiv med stora filer stoppas genomsökningen tidigast då en fil från arkivet extraheras (till exempel när en användardefinierad variabel är 3 sekunder, men extraheringen av en fil tar 5 sekunder). Resten av filerna i arkivet kommer inte att genomsökas när den tiden har förflutit.
Om du vill begränsa genomsökningstiden, inklusive större arkiv, använder du **Maximal objektstorlek** och **Maximal filstorlek i arkivet** (rekommenderas inte på grund av möjliga säkerhetsrisker).
Standardvärde: obegränsat.

Inställningar för genomsökning av arkiv

Antal nästlade arkiv – anger maximalt djup vid arkivgenomsökningen. Standardvärde: 10.

Maximal filstorlek i arkivet – ange maximal filstorlek för filer i arkiven (efter att de extraherats) som genomsöks. Maxvärdet är **3 GB**.

> Vi rekommenderar inte att ändra standardvärdena, eftersom det i regel inte finns någon anledning att ändra dem.

Webbåtkomstskydd

Med Webbåtkomstskydd kan du konfigurera avancerade inställningar för modulen Internetskydd. Följande alternativ är tillgängliga i Avancerade inställningar > **Skydd** > **Webbåtkomstskydd** > **Webbåtkomstskydd**:

Aktivera webbåtkomstskydd – när detta inaktiverats kan inte webbåtkomstskydd och skydd mot nätfiske köras.

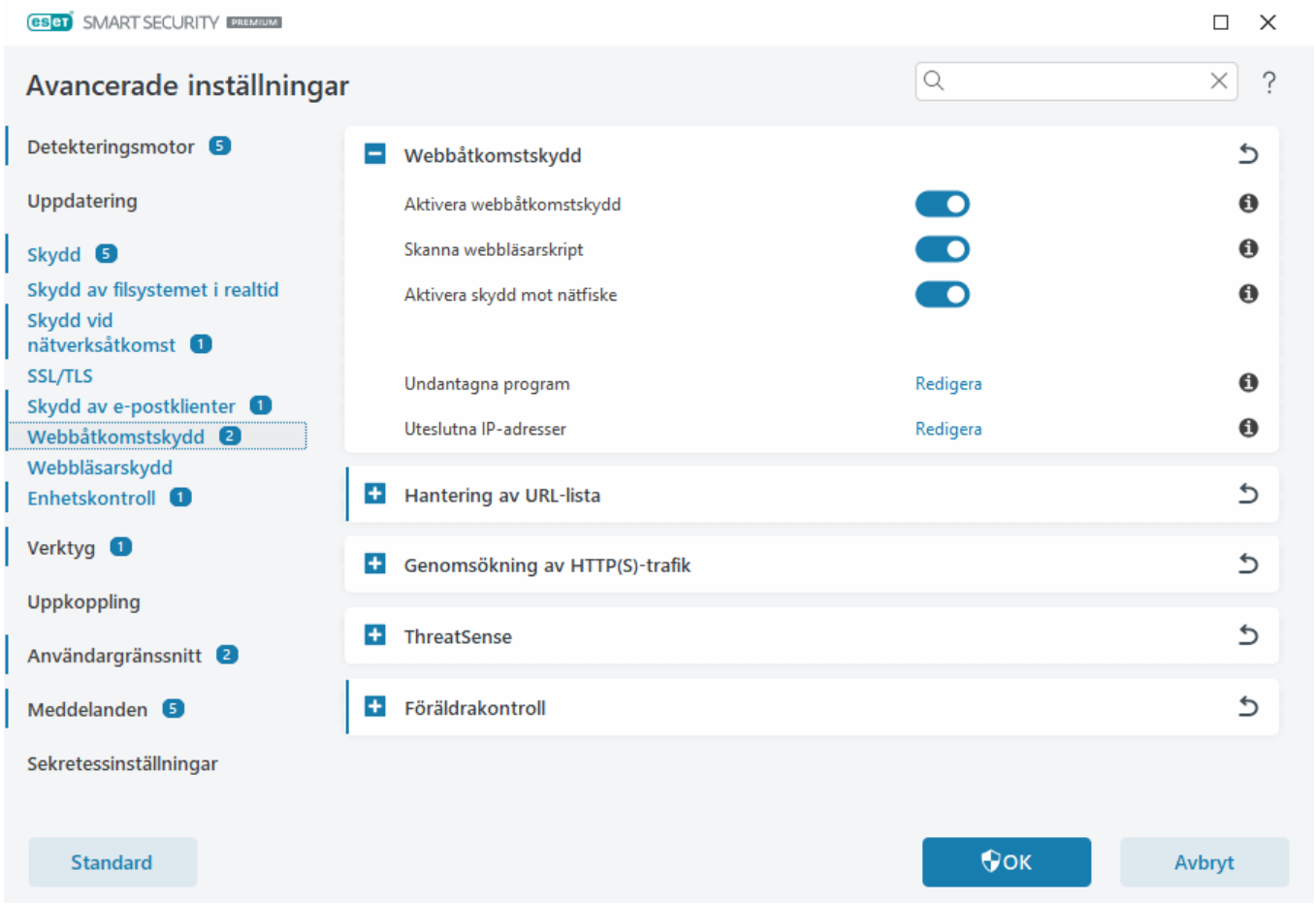
> Vi rekommenderar starkt att du låter Webbåtkomstskydd vara aktiverat och inte utesluter några program eller IP-adresser som standard.

Genomsök webbläsarskript – när det här alternativet är aktiverat kontrollerar detekteringsmotorn alla JavaScript-program som körs av webbläsare.

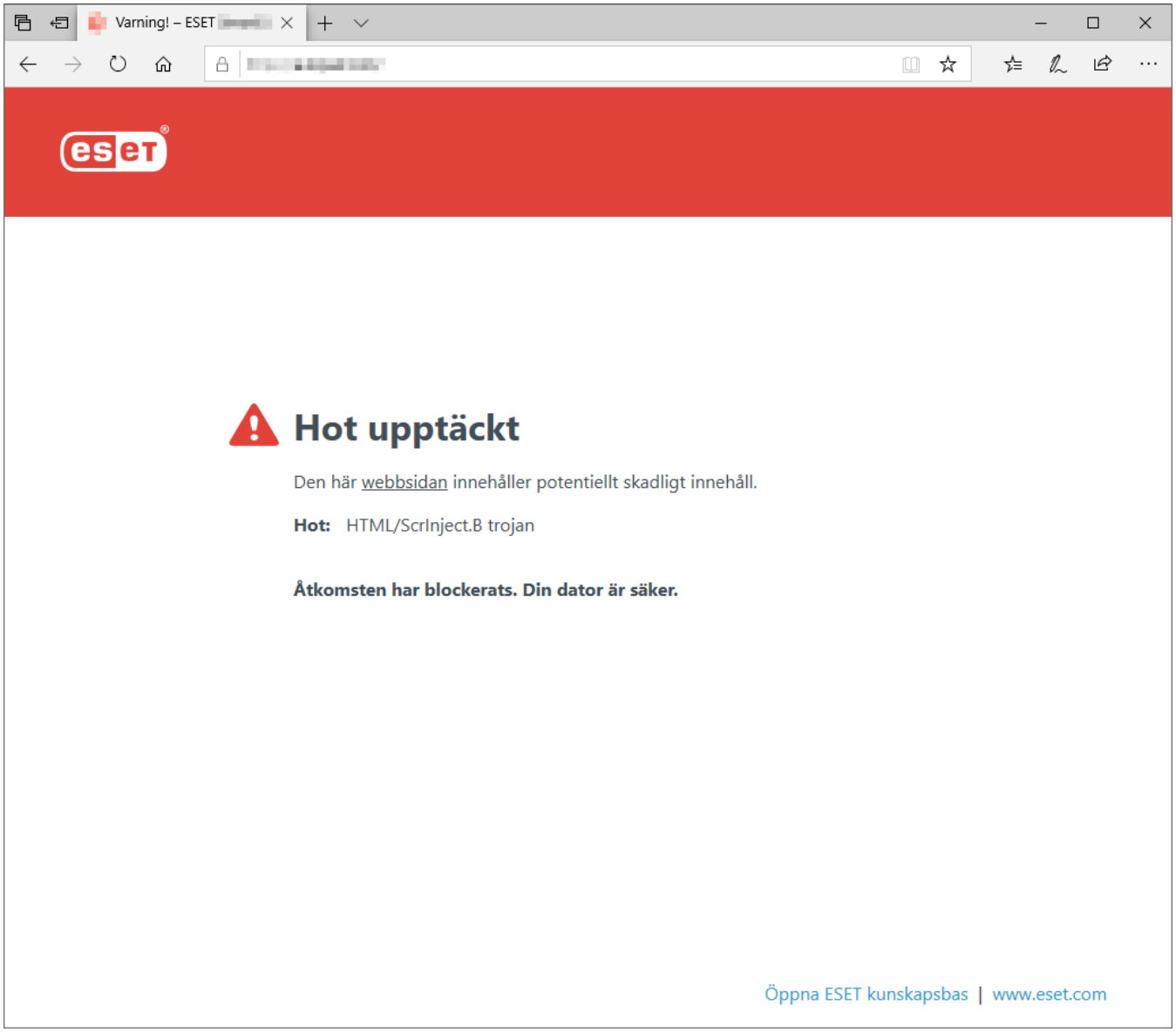
Aktivera Skydd mot nätfiske – när det här alternativet är aktiverat blockeras webbsidor med nätfiske. Se Skydd mot nätfiske för mer information.

Undantagna program – gör att du kan undanta specifika program från genomsökning av Webbåtkomstskydd. Användbart när Webbåtkomstskydd orsakar kompatibilitetsproblem.

Undantagna IP-adresser – gör att du kan undanta specifika fjärradresser från genomsökning av Webbåtkomstskydd. Användbart när Webbåtkomstskydd orsakar kompatibilitetsproblem.



Webbåtkomstskyddet visar följande meddelande i webbläsaren när webbplatsen blockeras:



Anvisningar med bilder

Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:

- Exkludera en säker webbplats från att blockeras av webbåtkomstskyddet
- Blockera en webbplats med hjälp av ESET Smart Security Premium

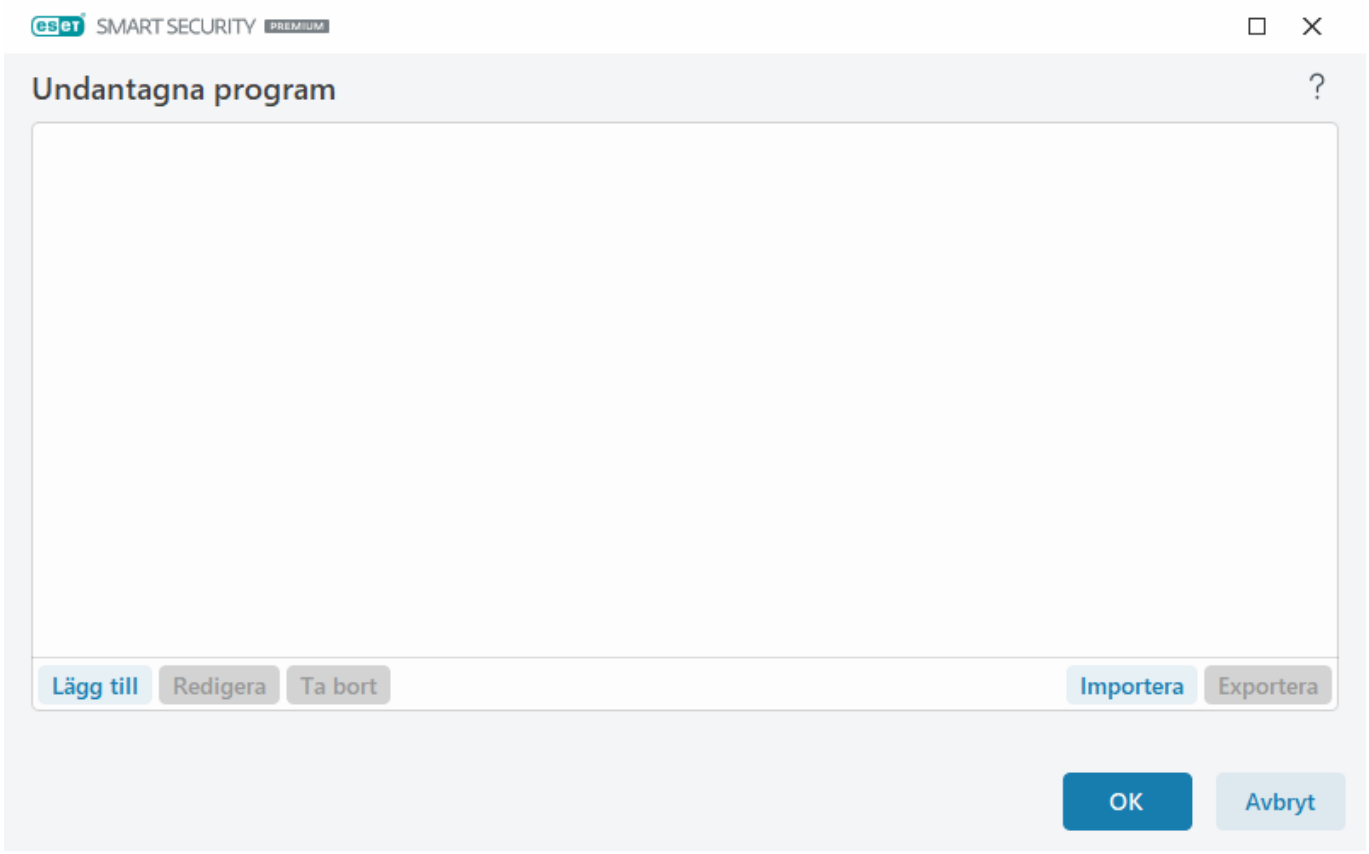
Undantagna program

Om du vill utesluta genomsökning av kommunikation för specifika program ska du lägga till dem i listan. De valda programmens HTTP(S)/POP3(S)/IMAP(S)-kommunikation kontrolleras inte. Vi rekommenderar att endast använda detta för program som inte fungerar normalt när deras kommunikation kontrolleras.

Aktiva program och tjänster är automatiskt tillgängliga här när du klickar på **Lägg till**. Klicka på **...** och gå till ett program för att lägga till undantaget manuellt.

Redigera – redigera valda poster i listan.

Ta bort – tar bort valda poster från listan.



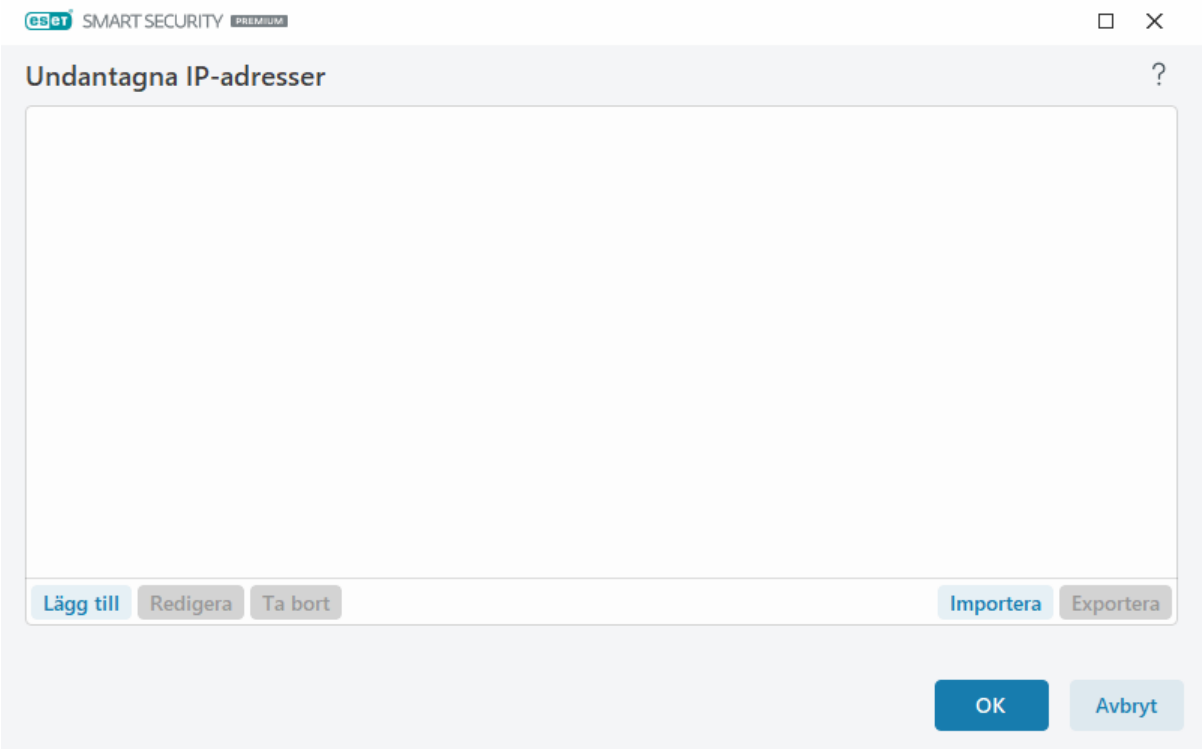
Uteslutna IP-adresser

Posterna på listan undantas från genomsökning. HTTP(S)/POP3(S)/IMAP(S)-kommunikation från/till de valda adresserna kontrolleras inte. Vi rekommenderar att du endast använder detta alternativ för adresser som är kända som trovärdiga.

Klicka på **Lägg till** om du vill undanta en IP-adress/ett adressintervall/ett undernät till en fjärrpunkt.

Klicka på **Redigera** för att ändra vald IP-adress.

Klicka på **Ta bort** om du vill ta bort valda poster från listan.



Exempel på IP-adresser

Lägg till IPv4-adress:
Enskild adress – lägger till en IP-adress för en enskild dator (till exempel *192.168.0.10*).
Adressintervall – ange den första och den sista IP-adressen för att ange IP-intervallet för flera datorer (till exempel *192.168.0.1–192.168.0.99*).
Undernät – undernät (en grupp datorer) definierade av en IP-adress och en mask. 255.255.255.0 är till exempel nätverksmasken för undernätet 192.168.1.0. Om du vill undanta hela undernätet ska du skriva *192.168.1.0/24*.
Lägg till IPv6-adress:
Enskild adress – lägger till en IP-adress för en enskild dator (till exempel *2001:718:1c01:16:214:22ff:fec9:ca5*).
Undernät – undernät (en grupp datorer) som definieras av en IP-adress och en mask (till exempel: *2002:c0a8:6301:1::1/64*).

Hantering av URL-lista

Med **Hantering av URL-lista** i Avancerade inställningar > **Skydd** > **Webbåtkomstskydd** kan du ange HTTP-adresser som ska blockeras, tillåtas eller undantas från innehållsgenomsökning.

SSL/TLS måste vara aktiverat om du vill filtrera HTTPS-adresser förutom HTTP. Annars läggs endast domänerna för besökta HTTPS-platser till – inte hela URL-adressen.

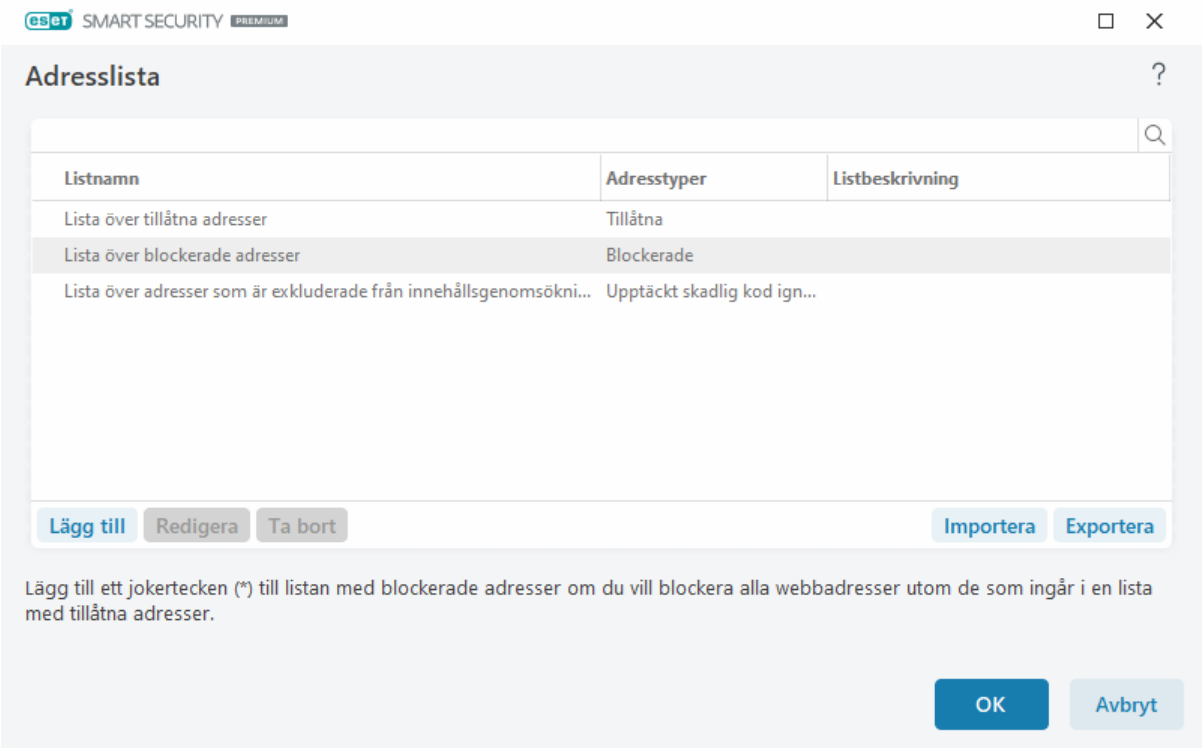
Webbplatser i **Lista över blockerade adresser** är inte åtkomliga såvida de inte också finns i **Lista över tillåtna adresser**. Webbplatser i **Lista över adresser exkluderade från genomsökning av innehåll** genomsöks inte efter skadlig kod när de besöks.

Om du vill blockera alla HTTP-adresser utom adresserna i aktiv **Lista över tillåtna adresser** lägger du till * till aktiv **Lista över blockerade adresser**.

Specialtecknen * (asterisk) och ? (frågetecken) kan användas i listor. Asterisken motsvarar alla teckensträngar och frågetecknet motsvarar alla symboler. Var särskilt försiktig när du anger exkluderade adresser eftersom listan

endast ska innehålla betrodda och säkra adresser. På samma sätt är det nödvändigt att kontrollera att symbolerna * och ? används på ett korrekt sätt i den listan. Se Lägg till HTTP-adress/domänmask för information om hur en domän inklusive alla underdomäner kan matchas säkert. Aktivera en lista genom att välja **Visa aktiva**. Vill du ha ett meddelande när du anger en adress från den aktuella listan väljer du **Meddela vid tillämpning**.

> **Adresser som är betrodda av ESET**
> Om **Genomsök inte trafik med domäner som är betrodda av ESET** är aktiverat i SSL/TLS påverkas inte domäner på ESET:s vitlista av konfigurationen av Hantering av URL-listor.



Kontrollelement

Lägg till – skapar en ny lista utöver de fördefinierade. Det kan vara användbart om du vill dela olika adressgrupper logiskt. Till exempel kan en lista över blockerade adresser innehålla adresser från en extern offentlig svartlista, och en annan kan innehålla din egen svartlista, vilket gör det enklare att uppdatera den externa listan medan din egen hålls intakt.

Redigera – ändrar befintliga listor. Används för att lägga till eller ta bort adresser.

Ta bort – tar bort befintliga listor. Endast tillgängligt för listor skapade med **Lägg till**, inte för standardlistorna.

Adresslista

Här kan du ange listor över HTTP(S)-adresser som kommer att blockeras, tillåtas eller undantas från kontroll.

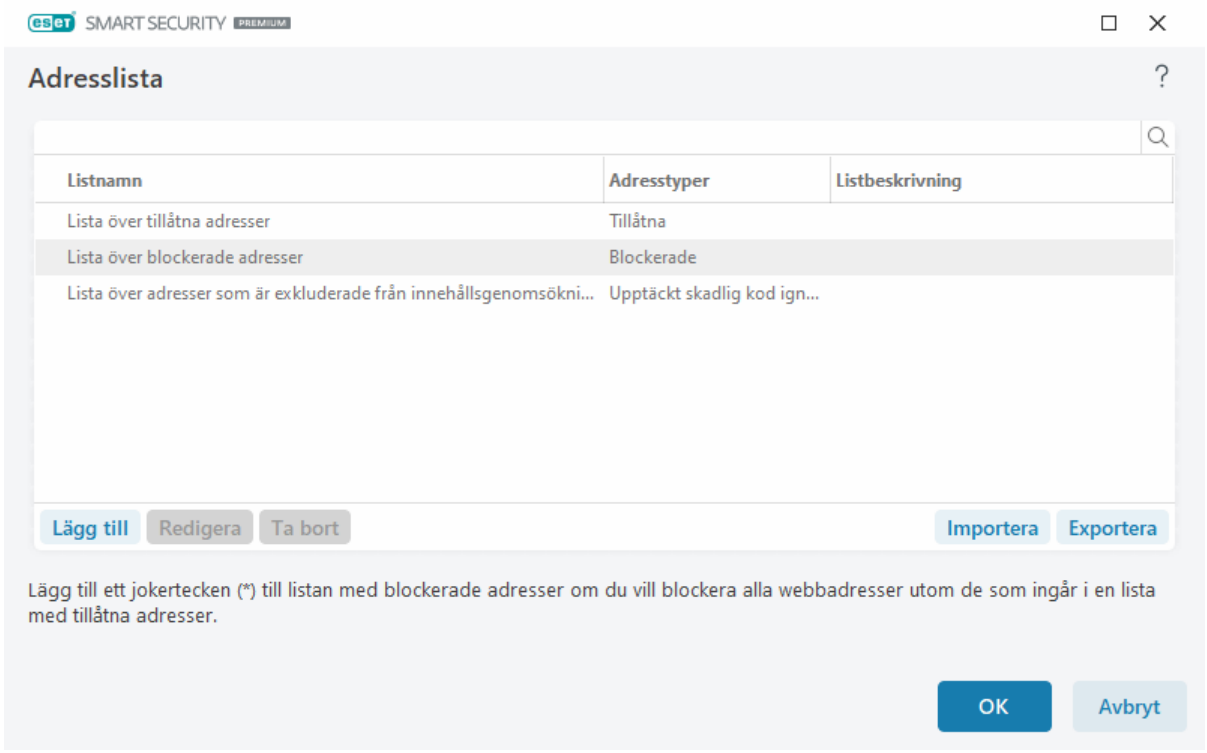
Följande tre listor är tillgängliga som standard:

- **Lista över adresser som är undantagna från innehållsgenomsökning** – ingen sökning efter skadlig kod görs för adresser på denna lista.
- **Lista över tillåtna adresser** – om Tillåt endast åtkomst till HTTP-adresser i listan över tillåtna adresser och

listan med blockerade adresser innehåller * (matcha allt) kommer användaren endast att ha åtkomst till adresser i den här listan. Adresserna i den här listan är tillåtna även när de finns med i listan över blockerade adresser.

- **Lista över blockerade adresser** - användaren får inte åtkomst till adresser angivna i denna lista om de inte även finns med i listan över blockerade adresser.

Klicka på **Lägg till** om du vill skapa en ny lista. Ta bort valda listor genom att klicka på **Ta bort**.



Anvisningar med bilder

Följande artiklar i ESET:s kunskapsbas kanske endast finns på engelska:

- Exkludera en säker webbplats från att blockeras av webbåtkomstskyddet
- Blockera en webbplats med Windows-hemprodukter från ESET

Du hittar mer information i Hantering av URL-lista.

Skapa en ny adresslista

I det här dialogfönstret kan du konfigurera en ny lista över URL-adresser/masker som ska blockeras, tillåtas eller uteslutas från kontroll.

Det går att konfigurera följande alternativ:

Typ av adresslista – det finns tre typer av listor:

- **Upptäckt skadlig kod ignoreras** – ingen sökning efter skadlig kod på adresser på denna lista.
- **Blockerade** – åtkomst till adresser som anges i den här listan blockeras.
- **Tillåtna** – åtkomst till adresser som anges i den här listan tillåts. Adresser i den här listan är tillåtna även om de matchar listan över blockerade adresser.

Listnamn – ange listans namn. Det här fältet är inte tillgängligt när du redigerar en av de fördefinierade listorna.

Listbeskrivning – ge en kort beskrivning av listan (tillval). Inte tillgängligt när du redigerar en av de fördefinierade listorna.

Om du vill aktivera en lista väljer du **Visa aktiva** intill den. Om du vill få ett meddelande när en specifik lista används vid åtkomst till webbplatser väljer du **Meddela vid tillämpning**. Exempelvis får du ett meddelande när en webbplats blockeras eller tillåts på grund av att den finns i en lista över blockerade eller tillåtna adresser. Meddelandet innehåller namnet på den lista den aktuella webbplatsen finns i.

Allvarlighetsgrad för loggning – information om den specifika listan som används vid åtkomst till webbplatser kan skrivas till loggfilerna.

Kontrollelement

Lägg till – lägg till en ny URL-adress i listan (ange flera värden med en avgränsare).

Redigera – ändra befintliga adresser i listan. Endast tillgängligt för adresser som har skapats med **Lägg till**.

Ta bort – ta bort befintliga adresser i listan. Endast tillgängligt för adresser som har skapats med **Lägg till**.

Importera – importera en fil med URL-adresser (avgränsa värden med en radbrytning, exempelvis *.txt med UTF-8-kodning).

Lägga till en webbadressmask

Se anvisningarna i denna dialogruta innan du anger önskad adress/domänmask.

MedESET Smart Security Premium kan användarna blockera angivna webbplatser och hindra att webbläsaren visar innehållet i dessa. Det går även att ange adresser som ska undantas från kontrollen. Om fjärrserverns fullständiga namn är okänt, eller om användaren vill ange en hel grupp med fjärrservrar, går det att ange en sådan grupp med hjälp av masker. Maskerna innehåller symbolerna ? och *.

- Symbolen ? motsvarar ett tecken.
- Symbolen * motsvarar en textsträng.

Exempelvis anger *.c?m alla adresser där den sista delen börjar med bokstaven c, avslutas med bokstaven m och innehåller ett okänt tecken mellan dessa bokstäver (.com, .cam osv.)

En sekvens som inleds med *. behandlas speciellt om det används i början av domännamnet. För det första matchar jokertecknet (*) inte snedstreck (/) i det här fallet. Detta för att undvika att masken kringgås, exempelvis matchar **.domain.com* inte *http://anydomain.com/anypath#.domain.com* (ett sådant suffix kan läggas till i alla URL-adresser utan att hämtningen påverkas). Och för det andra matchar *. även en tom sträng i det här specialfallet. Detta för att möjliggöra matchning av hela domänen inklusive eventuella underdomäner med en enda mask. Exempelvis matchar masken **.domain.com* även *http://domain.com*. Att använda **domain.com* vore fel, eftersom det även skulle matcha *http://anotherdomain.com*.

Genomsökning av HTTP(S)-trafik

Som standard är ESET Smart Security Premium konfigurerad för att genomsöka HTTP- och HTTPS-trafik som används av webbläsare och andra program. Du bör endast inaktivera genomsökning av trafik om du har problem med programvara från tredje part och vill veta om problemet orsakas av ESET Smart Security Premium.

Aktivera genomsökning av HTTP-trafik – HTTP-trafiken i alla portar för alla program.

Aktivera genomsökning av HTTPS-trafik – HTTPS-trafik använder en krypterad kanal för att överföra information mellan server och klient. ESET Smart Security Premium kontrollerar kommunikation med SSL-protokollet (Secure Socket Layer) och TLS-protokollet (Transport Layer Security). Programmet genomsöker endast trafik på portar som har definierats i **Portar som används av HTTPS-protokollet** oavsett versionen av operativsystemet (du kan lägga till portar förutom de fördefinierade portarna 433 och 0–65535).

ThreatSense

ThreatSense består av många avancerade hotidentifieringsmetoder. ThreatSense är en proaktiv metod vilket innebär att den kan skydda datorn mot tidig spridning av ett nytt hot. Genom att kombinera kodanalys, kodemulering, generiska signaturer, virussignaturer och använda dem tillsammans ökas systemsäkerheten avsevärt. Genomsökningsmotorn kan kontrollera flera dataströmmar samtidigt vilket maximerar effektiviteten och upptäcktsfrekvensen. ThreatSense-tekniken eliminerar även framgångsrikt rootkits.

med alternativen för inställning av ThreatSense går det att ange ett antal olika genomsökningsparametrar:

- Filtyper och tillägg som genomsöks
- En kombination av olika identifieringsmetoder
- Rensningsnivåer, osv.

Öppna inställningsfönstret genom att klicka på **ThreatSense** i Avancerade inställningar för moduler som använder ThreatSense-teknik (se nedan). Olika säkerhetsscenarier kan kräva olika konfigurationer. Det går därmed att individuellt konfigurera följande skyddsmoduler i ThreatSense:

- Skydd av filsystemet i realtid
- Genomsökning vid inaktivitet
- Startskanner
- Dokumentskydd
- Skydd av e-postklienter
- Webbåtkomstskydd
- Genomsökning av datorn

ThreatSense-parametrarna är starkt optimerade för varje modul och ändringar av dem kan märkbart påverka systemets funktion. Att till exempel ändra parametrarna så att internt packade filer alltid söks igenom eller att aktivera avancerad heuristik i modulen för skydd av filsystemet i realtid kan resultera i att systemet blir

långsammare (normalt används dessa metoder endast för genomsökning av nyskapade filer). Vi rekommenderar att lämna ThreatSense-standardparametrarna oförändrade för alla moduler utom för genomsökningsmodulen.

Objekt som ska genomsökas

I det här avsnittet går det att definiera vilka komponenter och filer på datorn som genomsöks efter infiltrationer.

Arbetsminne – söker efter hot som angriper systemets arbetsminne.

Startsektorer/UEFI – genomsöker startsektorerna efterskadlig kod i MBR (master boot record). Läs mer om UEFI i ordlistan.

E-postfiler – programmet stöder följande filnamnstillägg: DBX (Outlook Express) och EML.

Arkiv – programmet stöder följande filnamnstillägg: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE och många andra.

Självuppackande arkiv – självuppackande arkiv (SFX) är arkiv som kan extrahera sig själva.

Internt packade filer – när internt packade filer (till skillnad från standardarkivtyper) körs dekomprimeras de i minnet. Förutom statiska arkiverare av standardtyp (UPX, yoda, ASPack, FSG osv.) känner skannern igen många fler typer av arkiverare genom kodemulering.

Genomsökningsalternativ

Välj vilka metoder som ska användas för att söka efter infiltrationer i systemet. Följande alternativ finns tillgängliga:

Heuristik – heuristik är en algoritm som analyserar (skadliga) aktiviteter i program. Huvudfördelen med tekniken är möjligheten att identifiera skadlig programvara som inte fanns eller som inte var känd av den tidigare detekteringsmotorn. Nackdelen är (en mycket liten) risk för falska larm.

Avancerad heuristik/DNA-signaturer – avancerad heuristik är en unik heuristikalgoritm som utvecklats av ESET och som optimerats för att upptäcka datormaskar och trojanska hästar som skrivits på programmeringsspråk på hög nivå. Genom att använda avancerad heuristik blir ESET-produkterna bättre på att detektera hot. Signaturer används för att pålitligt detektera och identifiera virus. Med det automatiska uppdateringssystemet är nya signaturer tillgängliga inom några timmar efter att ett hot identifierades. Nackdelen med signaturer är att de bara detekterar virus de känner till (eller lätt ändrade versioner av dessa virus).

Rensning

Inställningarna för rensning anger hur ESET Smart Security Premium fungerar under rensning av infekterade objekt. Det finns fyra rensningsnivåer:

ThreatSense har följande åtgärdsnivåer (det vill säga rensningsnivåer).

Åtgärd i ESET Smart Security Premium

Rensningsnivå	Beskrivning
Åtgärda alltid detektering	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa sällsynta fall (till exempel systemfiler) lämnas det rapporterade objektet på sin ursprungliga plats om detekteringen inte kan åtgärdas.
Åtgärda detektering om det är säkert, behåll annars	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa fall (till exempel systemfiler eller arkiv med både rena och infekterade filer) lämnas det rapporterade objektet på sin ursprungliga plats om en detektering inte kan åtgärdas.
Åtgärda detektering om det är säkert, fråga annars	Försök att åtgärda detekteringen när du rensar objekt. I vissa fall, om ingen åtgärd kan utföras, får slutanvändaren en interaktiv avisering och måste välja en åtgärd (till exempel ta bort eller ignorera). Den här inställningen rekommenderas i de flesta fall.
Fråga alltid slutanvändaren	Ett interaktivt fönster visas för slutanvändaren när objekt rensas och en åtgärd måste väljas (till exempel ta bort eller ignorera). Denna nivå är avsedd för mer avancerade användare som vet vilka som ska åtgärder vidtas i händelse av detektering.

Undantag

Ett filnamnstillägg är den del av filnamnet som avgränsas med en punkt. Ett filändelse definierar filens typ och innehåll. I det här avsnittet för ThreatSense-inställningarna kan du definiera vilka typer av filer som ska genomsökas.

Övrigt

När du konfigurerar parameterinställningarna för ThreatSense-motorn för en Genomsökning av datorn på begäran är följande alternativ i avsnittet **Andra** också tillgängliga:

Genomsök alternativa dataströmmar (ADS) – de alternativa dataströmmarna som används av filsystemet NTFS består av fil- och mappassociationer som inte är synliga för vanliga genomsökningsmetoder. Många infiltrationsförsök maskerar sig som alternativa dataströmmar för att undvika upptäckt.

Kör genomsökningar i bakgrunden med låg prioritet – varje genomsökningssekvens kräver en viss mängd systemresurser. Om du arbetar med program som kräver mycket systemresurser kan du aktivera genomsökning i bakgrunden med låg prioritet och spara resurser till dina program.

Logga alla objekt – i genomsökningsloggen visas alla genomsökta filer i självuppackande arkiv, även sådana som inte är infekterade (detta kan generera mycket genomsökningsloggdata och öka genomsökningsloggfilens storlek).

Aktivera Smart optimering – med aktiverad smart optimering används de optimala inställningarna för effektivast genomsökning och bibehåller samtidigt den högsta genomsökningshastigheten. De olika skyddsmodulerna genomsöker intelligent och använder olika genomsökningsmetoder och tillämpar dem på vissa filtyper. Om smart optimering är inaktiverad tillämpas endast de användardefinierade inställningarna i ThreatSense-kärnan när en genomsökning utförs.

Bevara tidsstämpeln för senaste åtkomst – markera det här alternativet om du vill behålla den ursprungliga åtkomsttiden för genomsökta filer i stället för att uppdatera dem (t.ex. för användning med system för säkerhetskopiering av data).

Begränsningar

Under Begränsningar kan du ange en maximal storlek på objekt och nivåer på de nästlade arkiv som ska genomsökas:

Objektinställningar

Maximal objektstorlek – anger maximal storlek på objekt som ska genomsökas. Den angivna antivirusmodulen kommer endast att genomsöka objekt som är mindre än den angivna storleken. Alternativet ska endast ändras av avancerade användare som kan ha särskilda anledningar till att undanta större objekt från genomsökning. Standardvärde: obegränsat.

Maximal tid för genomsökning av objekt (sek.) – definierar det maximala tidsvärdet för genomsökning av filer i ett behållarobjekt (till exempel ett RAR/ZIP-arkiv eller ett e-postmeddelande med flera bilagor). Den här inställningen gäller inte för fristående filer. Om ett användardefinierat värde har angetts och den tiden har förflutit stoppas en genomsökning så snart som möjligt, oavsett om genomsökningen av varje fil i ett behållarobjekt har slutförts.
När det gäller ett arkiv med stora filer stoppas genomsökningen tidigast då en fil från arkivet extraheras (till exempel när en användardefinierad variabel är 3 sekunder, men extraheringen av en fil tar 5 sekunder). Resten av filerna i arkivet kommer inte att genomsökas när den tiden har förflutit.
Om du vill begränsa genomsökningstiden, inklusive större arkiv, använder du **Maximal objektstorlek** och **Maximal filstorlek i arkivet** (rekommenderas inte på grund av möjliga säkerhetsrisker).
Standardvärde: obegränsat.

Inställningar för genomsökning av arkiv

Antal nästlade arkiv – anger maximalt djup vid arkivgenomsökningen. Standardvärde: 10.

Maximal filstorlek i arkivet – ange maximal filstorlek för filer i arkiven (efter att de extraherats) som genomsöks. Maxvärdet är **3 GB**.

> Vi rekommenderar inte att ändra standardvärdena, eftersom det i regel inte finns någon anledning att ändra dem.

Föräldrakontroll

Alternativet **Aktivera föräldrakontroll** integrerar föräldrakontrollen i ESET Smart Security Premium. Klicka på **Redigera** bredvid Användarkonton för att associera Windows-användarkonton som används av Föräldrakontroll med specifika användare för att begränsa deras åtkomst till olämpligt eller skadligt innehåll på internet.

Användarkonton

I Avancerade inställningar > **Skydd** > **Webbåtkomstskydd** > **Föräldrakontroll** > **Användarkonton** > **Redigera** kan du associera Windows-användarkonton som används av Föräldrakontroll med specifika användare för att begränsa deras åtkomst till olämpligt eller skadligt innehåll på internet.

Kolumner

Windows-konto – användarens namn.

Aktiverad – när detta aktiveras, så aktiveras föräldrakontroller för ett specifikt användarkonto.

Domän – namnet på den domän användaren tillhör.

Födelsedag – åldern på den användare kontot tillhör.

Kontrollelement

Lägg till – dialogrutan Arbeta med användarkonton visas.

Redigera – med det här alternativet kan du redigera de valda kontona.

Ta bort – ta bort det markerade kontot.

Uppdatera – om du har lagt till ett användarkonto kan ESET Smart Security Premium uppdatera listan med användarkonton utan att det här fönstret behöver öppnas igen.

Inställningar för användarkonto

Fönstret har tre flikar:

Allmänt

Klicka på växlingsknappen bredvid **Aktiverad** om du vill aktivera Föräldrakontroll för Windows-kontot som har valts nedan.

Välj först ett systemkonto från datorn. De inställda begränsningarna i Föräldrakontroll påverkar endast standard-Windows-konton. Administratörskonton kan åsidosätta begränsningar.

Om kontot används av en förälder väljer du **Föräldrakonto**.

Ange **Barnets födelsedatum** för kontot för att avgöra nivån för åtkomst och ställa in åtkomstregler för lämpliga webbsidor för den åldern.

Allvarlighetsgrad för loggning

ESET Smart Security Premium sparar alla viktiga händelser i en loggfil som går att visa direkt från huvudmenyn Klicka på **Verktyg** > **Loggfiler** och välj sedan **Föräldrakontroll** på rullgardinsmenyn **Logg**.

- **Diagnostik** – loggar information som behövs för att fininställa programmet.
- **Information** – loggar alla informationsmeddelanden, inklusive tillåtna och blockerade undantag, samt alla poster ovan.
- **Varning** – registrerar kritiska fel och varningsmeddelanden.
- **Inga** – inga loggar registreras.

Undantag

Genom att skapa ett undantag går det att tillåta eller neka en användare åtkomst till webbplatser som inte finns i undantagslistan. Detta är användbart om du vill kontrollera åtkomsten till specifika webbplatser istället för att använda kategorier. Undantag skapade för ett konto kan kopieras och användas för andra konton. Detta kan vara användbart när du vill skapa identiska regler för barn i ungefär samma ålder.

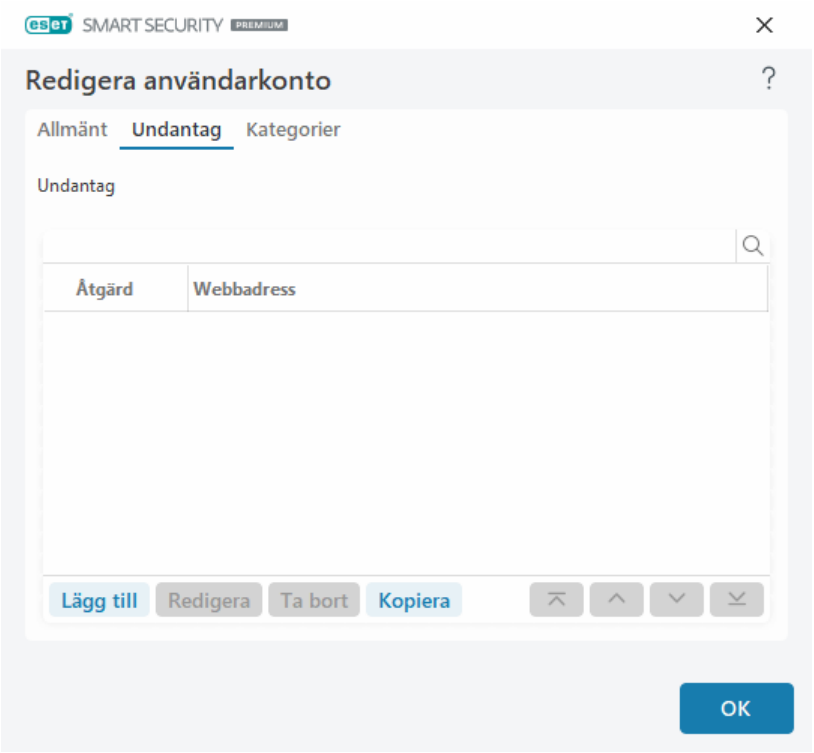
Klicka på **Lägg till** om du vill skapa ett nytt undantag. Ange **Åtgärd** (till exempel **Blockera**) i listrutan, skriv den **URL**undantaget gäller för och klicka sedan på **OK**. Undantaget läggs till i listan med befintliga undantag och dess status visas.

Lägg till – skapar ett nytt undantag.

Redigera – redigera det valda undantagets **URL** eller **Åtgärd**.

Ta bort – tar bort valt undantag.

Kopiera – välj en användare i listrutan som du vill kopiera ett skapat undantag från.



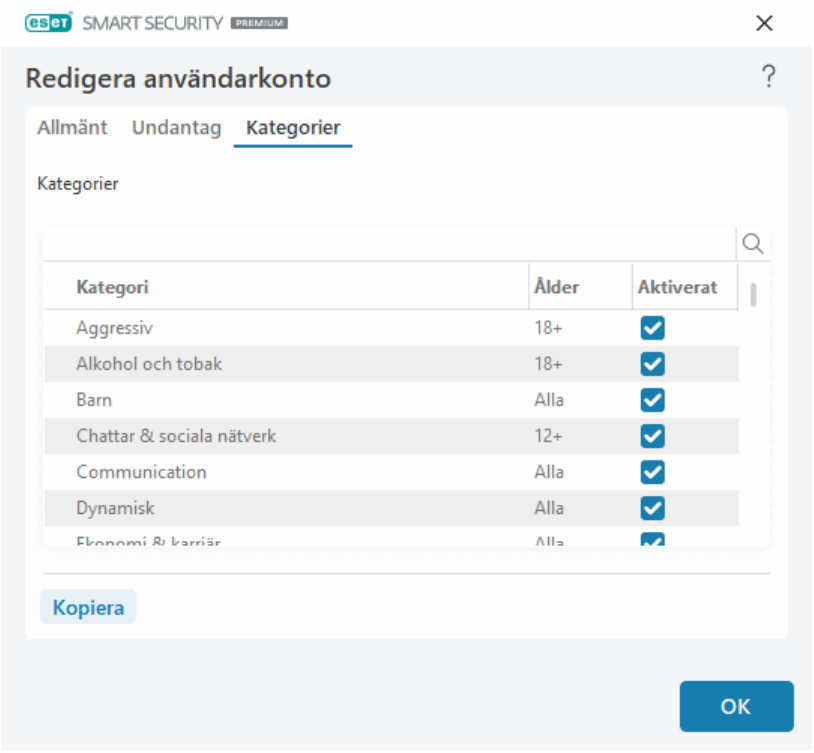
Undantag som definieras åsidosätter det valda kontots (eller de valda kontonas) definierade kategorier. Om kontot till exempel har kategorin **Nyheter** blockerad, men om du definierade en tillåten nyhetssida som ett undantag kan kontot öppna den tillåtna webbsidan. Du kan visa eventuella ändringar gjorda här i avsnittet Undantag.

Kategorier

På fliken **Kategorier** går det att definiera de allmänna kategorierna för webbplatser du vill blockera eller tillåta för varje konto. Markera kryssrutan intill en kategori om den ska tillåtas. Om du lämnar kryssrutan omarkerad tillåts inte kategorin för det kontot.

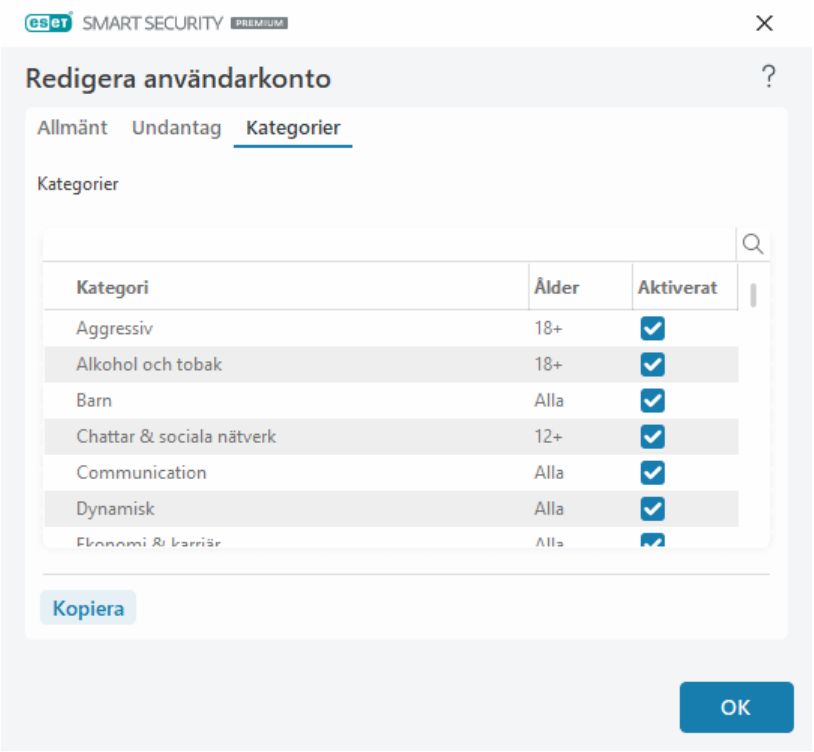
Kopiera – gör det möjligt att kopiera en lista med blockerade eller tillåtna kategorier från ett befintligt ändrat

konto.



Kategorier

Kontrollera kryssrutan i kolumnen **Aktiverad** bredvid en kategori för att tillåta det. Om du låter kryssrutan vara tom kommer kategorin inte att tillåtas för det kontot.



Här är några exempel på grupper som användarna kanske inte är bekanta med:

- **Övrigt** – vanligen privata (lokala) IP-adresser såsom intranät, 127.0.0.0/8, 192.168.0.0/16, osv. Visas

felkoden 403 eller 404 matchar webbplatsen även denna kategori.

- **Inte matchad** – denna kategori inkluderar webbsidor som inte matchar på grund av ett fel vid anslutning till föräldrakontrollens databasmotor.
- **Utan kategori** – okända webbsidor som ännu inte finns i föräldrakontrollens databas.
- **Dynamiska** – webbsidor som omdirigerar till andra sidor på andra webbplatser.

Webbläsarskydd

Med Webbläsarskydd får du ett extra lager av säkerhets- och sekretesskydd som skyddar webbläsarminnet från att inspekteras av andra processer, ökar skyddet mot tangentloggare och förhindrar inklistring av data relaterade till onlinebetalningar som modifierats av skadlig kod från urklipp till den säkrade webbläsaren. Om du vill konfigurera Webbläsarskydd ska du öppna Avancerade inställningar > **Skydd** > **Webbläsarskydd** och välja bland följande konfigurationsalternativ:

- Säkra banktjänster och surfning
- Lista över tillåtna webbläsarskydd
- Webbläsarens ram

Säkra banktjänster och surfning

Du kan konfigurera Säkra banktjänster och surfning i Avancerade inställningar > **Skydd** > **Webbläsarskydd** > **Säkra banktjänster och surfning**.

Säkra banktjänster och surfning

Aktivera Säkra banktjänster och surfning – När Säkra banktjänster och surfning är aktiverat startar alla webbläsare som stöds i ett säkert läge som standard.

Webbläsarskydd

Aktivera **Skydda alla webbläsare för** att starta alla webbläsare som stöds i ett säkert läge.

Installationsläge för tillägg – Från rullgardinsmenyn kan du välja vilka tillägg som ska få installeras på en webbläsare som säkrats av ESET:

- **Viktiga tillägg –** Endast de viktigaste tilläggen som utvecklats av en viss webbläsartillverkare.
- **Alla tillägg** – Alla tillägg som stöds av en viss webbläsare.

> Om du ändrar installationsläget för tillägget påverkas inte tidigare installerade webbläsartillägg:

Säkrad webbläsare

Utökat minnesskydd – om det här alternativet aktiveras skyddas den säkrade webbläsarens minne från att inspekteras av andra processer.

Tangentbordsskydd – om det här alternativet är aktiverat döljs information som matas du går in med tangentbordet i en säkrad webbläsare från andra program. Detta stärker skyddet mot keylogger-program.

Urklippsskydd – om det här alternativet är aktiverat förhindrar ESET Smart Security Premium att data för onlinebetalningar som modifierats av skadlig kod klistras in från Urklipp i den säkrade webbläsaren. Detta säkerställer skydd mot ändringar som skadlig programvara kan komma att göra.

Webbläsarens ram – Anpassa visningsinställningarna för webbläsarens ram i skyddade webbläsare.

Lista över tillåtna webbläsarskydd – Hantera filer som har lagts till i listan över tillåtna webbläsarskydd.

Webbläsarsekretess och säkerhet

Aktivera Webbläsarsekretess och säkerhet – om den här funktionen inaktiveras tas tillägget Webbläsarsekretess och säkerhet bort från alla webbläsare som stöds på alla Windows-konton.

Visa meddelanden för Webbläsarsekretess och säkerhet – om det här alternativet är aktiverat visar ESET Smart Security Premium meddelanden för Webbläsarsekretess och säkerhet.

Skanner för webbläsarskript

Aktivera avancerad genomsökning av webbläsarskript – om det här alternativet är aktiverat kontrollerar antivirusskannern alla JavaScript-program som körs av webbläsare.

00

Enhetskontroll

ESET Smart Security Premium ger automatisk enhetskontroll (CD/DVD/USB etc.). Denna modul gör det möjligt att blockera eller justera utökade filter/behörigheter och välja hur användaren får åtkomst till och arbetar med en viss enhet. Detta kan vara användbart om administratören vill förhindra användning av enheter med oönskat innehåll.

Externa enheter som stöds:

- Disklagring (hårddisk, USB flyttbar disk)
- CD/DVD
- USB Skrivare
- FireWire-lagring
- Bluetooth Enhet

- Smartkortläsare
- Bildenhet
- Modem
- LPT/COM port
- Bärbar enhet (batteridrivna enheter som mediaspelare, smartphones, plug-and-play-enheter och så vidare)
- Alla enhetstyper

Inställningarna för enhetskontroll går att ändra i Avancerade inställningar > **Skydd** > **Enhetskontroll**.

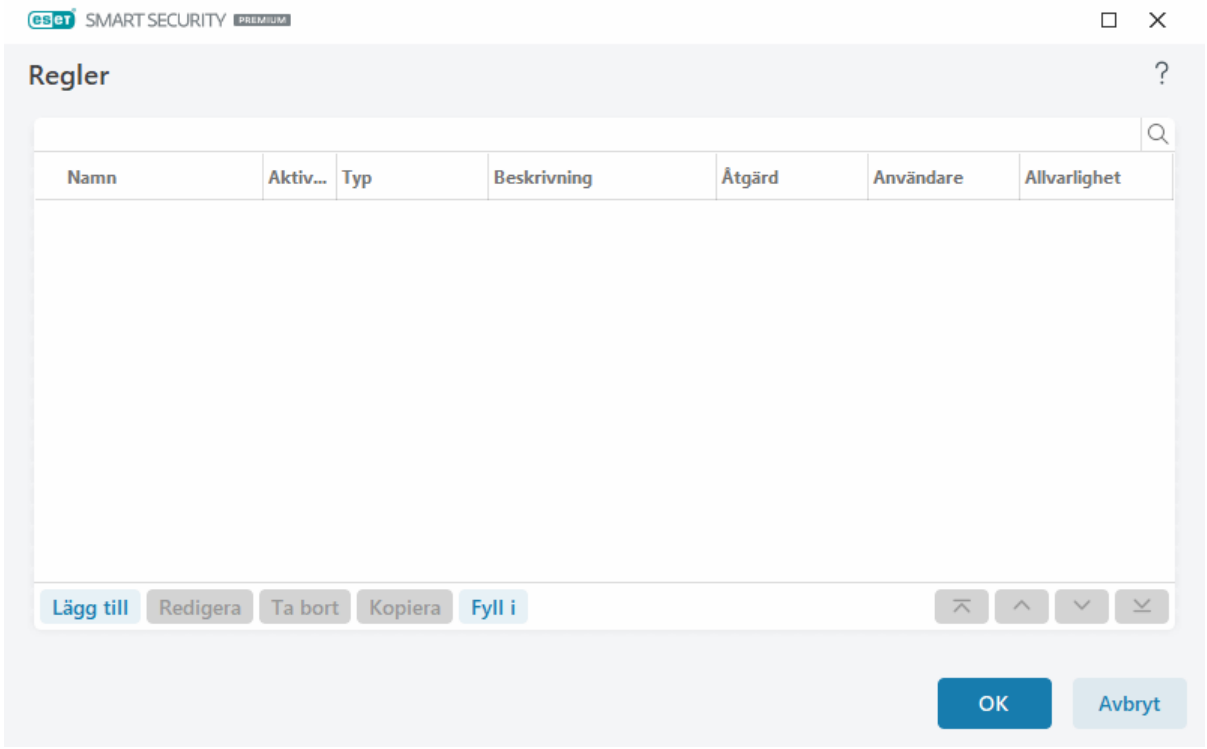
Klicka på växlingsknappen **Aktivera enhetskontroll** för att aktivera funktionen Enhetskontroll i ESET Smart Security Premium. Du måste starta om datorn för att ändringen ska börja gälla. När enhetskontrollen har aktiverats kan du definiera **reglerna** i fönstret Regelredigerare.

> Du kan skapa olika grupper med enheter för vilka olika regler tillämpas. Du kan även skapa en enda grupp med enheter för vilka regeln med åtgärden **Tillåt** eller **Skriv block** tillämpas. På så vis säkerställs att okända enheter blockeras av enhetsstyrningen när de ansluts till datorn.

Om en enhet som blockeras av en befintlig regel ansluts öppnas ett meddelandefönster och åtkomst till enheten tillåts inte.

Regelredigerare för enhetskontroll

Fönstret **Regelredigerare för enhetskontroll** visar befintliga regler för externa enheter och gör det möjligt att exakt styra externa enheter som användare ansluter till datorn.



Det går att tillåta eller blockera vissa enheter per användare eller användargrupp och basera dem på ytterligare enhetsparametrar som går att ange i regelkonfigurationen. Listan med regler innehåller flera beskrivningar av en regel, såsom namn, typ, åtgärd att utföra efter att en extern enhet anslutits till datorn och logga allvarlighet. Se även Lägga till regler för enhetskontroll.

Klicka på **Lägg till** eller **Redigera** för att hantera en regel. Klicka på **Kopiera** för att skapa en ny regel med förinställda alternativ som används av en annan vald regel. XML-strängar som visas vid klick på en regel går att kopiera till Urklipp för att hjälpa systemadministratörer att exportera/importera dessa data och använda dem i .

Klicka på **CTRL** och klicka för att välja flera regler och tillämpa åtgärder, såsom att ta bort eller flytta dem upp eller ned på listan, på alla valda regler. Kryssrutan **Aktiverad** inaktiverar eller aktiverar en regel, vilka kan vara användbart om du vill behålla regeln.

Klicka på alternativet **Fyll i** för att automatiskt populera parametrar för flyttbara mediaenheter anslutna till din dator.

Regler listas i prioritetsordning, med högsta prioritet högst upp. Regler kan flyttas genom att du klickar på  **Överst/Upp/Ned/Underst** och kan flyttas enskilt eller i grupper.

Loggposter kan visas i huvudprogramfönstret > **Verktyg** > Loggfiler.

I enhetsstyrningsloggen registreras alla händelser där enhetsstyrning utlösts.

Identifierade enheter

Om du klickar på knappen **Fyll i** visas en översikt över alla för närvarande anslutna enheter, med information om enhetstyp, enhetsleverantör, modell och serienummer (om sådant finns). Om du vill se alla dolda enheter väljer du **Visa dolda enheter**.

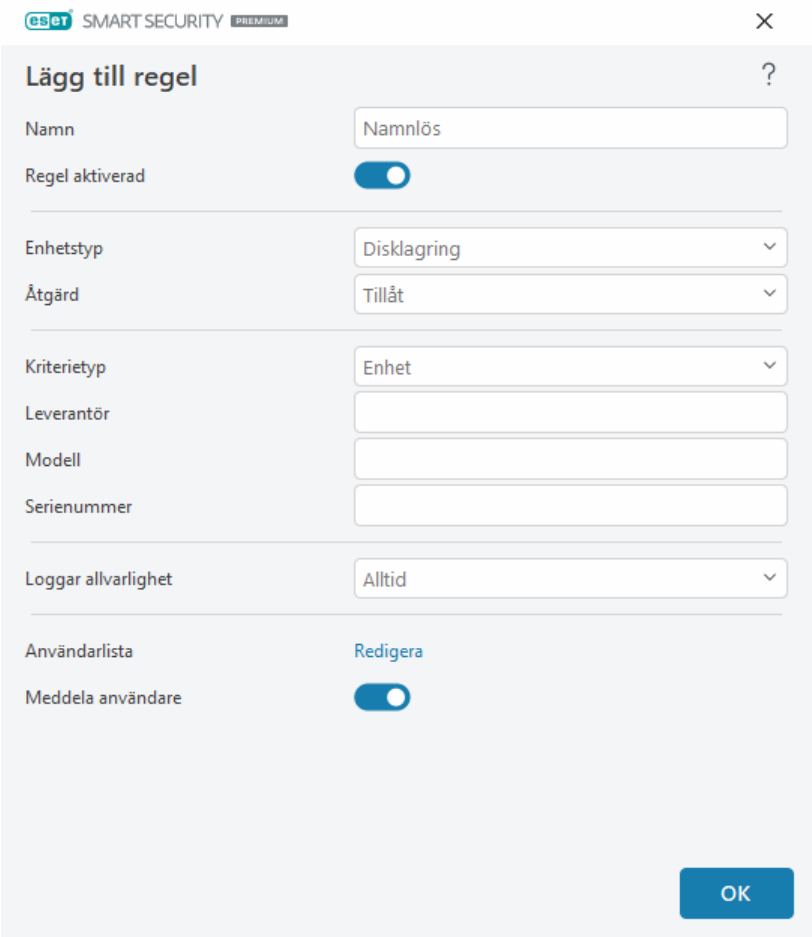
Välj en enhet i listan över identifierade enheter och klicka på **OK** för att lägga till en enhetskontrollregel med fördefinierad information (alla inställningar kan justeras).

Enheter i lågeffektläge (viloläge) är markerade med en varningsikon . Så här aktiverar du **OK**-knappen och lägger till en regel för enheten:

- Anslut enheten igen
- Använd enheten (starta till exempel appen Kamera i Windows för att väcka en webbkamera)

Lägga till regler för enhetskontroll

En regel för enhetskontroll definierar en åtgärd som ska vidtas när en enhet som motsvarar villkoren ansluts till datorn.



Ange en beskrivning av regeln i fältet **Namn** för bättre identifiering. Klicka på växlingsknappen bredvid **Regel aktiverad** för att inaktivera eller aktivera den här regeln. Det här är praktiskt om du inte vill ta bort regeln permanent.

Enhetstyp

Välj extern enhetstyp på rullgardinsmenyn (Disklagring/Bärbar enhet/Bluetooth/FireWire/...). Informationen om enhetstyp hämtas från operativsystemet och visas i Enhetshanteraren om en enhet är ansluten till datorn. Lagringsenheter inkluderar externa diskar eller vanliga minneskortläsare anslutna med USB eller FireWire. Smartkortläsare inkluderar alla läsare för smarta kort med en inbyggd krets, såsom SIM-kort eller autentiseringskort. Exempel på bildenheter är skannrar eller kameror. Eftersom dessa enheter endast tillhandahåller information om sina åtgärder och inte om användare kan de endast blockeras globalt.

Åtgärd

Åtkomst till icke-lagringsenheter går antingen att tillåta eller blockera. I motsats till det tillåter regler för lagringsenheter val av en av följande inställningar:

- **Tillåt** – fullständig åtkomst till enheten tillåten.
- **Blockera** – åtkomst till enheten blockeras.
- **Skriv block** – endast läsning från enheten är tillåten.
- **Varna** – varje gång en enhet ansluts meddelas användaren om den är tillåten/blockerad och en post skrivs i loggen. Enheter koms inte ihåg och ett meddelande visas om samma enhet ansluts igen.

Observera att inte alla åtgärder (rättigheter) är tillgängliga för alla enhetstyper. Om det är en enhet av lagringstyp är alla fyra åtgärder tillgängliga. För icke-lagringsenheter finns det endast tre åtgärder tillgängliga (t.ex. är **Skriv**

block inte tillgänglig för Bluetooth, vilket innebär att det endast går att tillåta, blockera eller varna för Bluetooth-enheter).

Kriterietyp

– välj **Enhetsgrupp** eller **Enhet**.

Ytterligare parametrar som visas nedan kan användas för att finjustera regler för olika enheter. Alla parametrar är skiftlägeskänsliga och stöder jokertecken (*, ?):

- **Leverantör** – filtrera enligt leverantörsnamn eller ID.
- **Modell** – enhetens namn.
- **Serienummer** – externa enheter har vanligen sina egna serienummer. För CD/DVD har skivan ett serienummer, inte CD-enheten.

> Om dessa parametrar inte definierats ignorerar regeln dessa fält vid matchning. Filtrering av parametrar i alla textfält är skiftlägeskänsligt och stöder jokertecken (ett frågetecken (?) motsvarar ett tecken, medan en asterisk (*) motsvarar en sträng på noll eller fler tecken).

> Om du vill visa information om en enhet skapar du en regel för enhetstypen, ansluter enheten till datorn och kontrollerar enhetsinformationen i enhetsstyrningsloggen.

Allvarlighetsgrad för loggning

ESET Smart Security Premium sparar alla viktiga händelser i en loggfil som går att visa direkt från huvudmenyn Klicka på**Verktyg** > **Loggfiler** och välj sedan **Enhetskontroll** på rullgardinsmenyn **Logg**.

- **Alltid** – alla händelser loggas.
- **Diagnostik** – loggar information som behövs för att fininställa programmet.
- **Informativ** – loggar alla informationsmeddelanden, inklusive framgångsrika uppdateringar och alla poster ovan.
- **Varning** – registrerar kritiska fel och varningsmeddelanden.
- **Inga** – inga loggar registreras.

Användarlista

Det går att begränsa regler till vissa användare eller användargrupper genom att lägga till dem i användarlistan genom att klicka på **Redigera** bredvid **Användarlista**.

- **Lägg till** – öppnar dialogfönstret **Objekttyper: Användare eller grupper** som gör det möjligt att välja önskade användare.
- **Ta bort** – tar bort markerad användare från filtret.

Begränsningar för användarlista

Det går inte att definiera användarlistan för regler med specifika enhetstyper:

- USB-skrivare
- Bluetooth-enhet
- Smartkortläsare
- Bildenhet
- Modem
- LPT/COM-port

Meddela användare – om en enhet som blockeras av en befintlig regel ansluts öppnas ett meddelandefönster.

Enhetsgrupper

Enheter som ansluts till datorn kan utgöra en säkerhetsrisk.

Fönstret Enhetsgrupper är indelat i två delar. Den högra delen av fönstret innehåller en lista över enheter som tillhör respektive grupp och den vänstra delen innehåller skapade grupper. Välj en grupp för att visa enheter i den högra rutan.

När du öppnar fönstret Gruppredigerare och väljer en grupp kan du lägga till eller ta bort enheter i listan. Det går även att lägga till enheter i gruppen genom att importera dem från en fil. Alternativt kan du klicka på knappen **Fyll i**, så att alla enheter anslutna till datorn listas i fönstret **Identifierade enheter**. Välj enheter i den ifyllda listan för att lägga till dem i gruppen genom att klicka på **OK**.

Kontrollelement

Lägg till – du kan lägga till en grupp genom att skriva dess namn eller en enhet i en befintlig grupp, beroende på i vilken del av fönstret du klickade på knappen.

Redigera – gör det möjligt att ändra namnet på den valda gruppen eller enhetens parametrar (leverantör, modell, serienummer).

Ta bort – tar bort den valda gruppen eller enheten beroende på i vilken del av fönstret du klickade på knappen.

Importera – importerar en lista över enheter från en textfil. För att importera enheter från en textfil krävs korrekt formatering:

- Varje enhet börjar på en ny rad.
- **Leverantör**, **Modell** och **Serienummer** måste finnas för varje enhet och separeras med ett kommatecken.

Här är ett exempel på textfilsinnehållet:

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

Exportera – exporterar en lista över enheter till en fil.

Om du klickar på knappen **Fyll i** visas en översikt över alla för närvarande anslutna enheter, med information om enhetstyp, enhetsleverantör, modell och serienummer (om sådant finns).

Lägg till enhet

Klicka på **Lägg till** i det högra fönstret för att lägga till en enhet i en befintlig grupp. Ytterligare parametrar som visas nedan kan användas för att finjustera regler för olika enheter. Alla parametrar är skiftlägeskänsliga och stöder jokertecken (*, ?):

- **Leverantör** – filtrera efter leverantörens namn eller ID.
- **Modell** – enhetens namn.
- **Serienummer** – externa enheter har vanligen sina egna serienummer. För CD/DVD har skivan ett serienummer, inte CD-enheten.
- **Beskrivning** – din beskrivning av enheten för bättre organisation.

> Om dessa parametrar inte definierats ignorerar regeln dessa fält vid matchning. Filtrering av parametrar i alla textfält är skiftlägeskänsligt och stöder jokertecken (ett frågetecken [?] motsvarar ett tecken, medan en asterisk [*] motsvarar en sträng på noll eller fler tecken).

Klicka på **OK** för att spara ändringarna. Klicka på **Avbryt** om du vill stänga fönstret **Enhetsgrupper** utan att spara ändringarna.

> När du har skapat en enhetsgrupp måste du lägga till en ny enhetskontrollregel för den skapade enhetsgruppen och välja vilken åtgärd som ska vidtas.

Observera att inte alla åtgärder (rättigheter) är tillgängliga för alla enhetstyper. Alla fyra åtgärder tillgängliga om det är en enhet av lagringstyp. För icke-lagringsenheter är endast tre åtgärder tillgängliga (t.ex. är **Skriv block** inte tillgänglig för Bluetooth, vilket innebär att det endast går att tillåta, blockera eller varna för Bluetooth-enheter).

Webbkameraskydd

Webbkameraskydd informerar dig om processer och program som har åtkomst till datorns webbkamera. Du får ett meddelande om ett program försöker få åtkomst till kameran och du kan välja att **tillåta** eller **blockera** åtkomsten. Varningsfönstrets färg beror på programmets rykte.

Inställningsalternativ för webbkameraskydd kan ändras i Avancerade inställningar > **Skydd** > **Enhetskontroll** > **Webbkameraskydd**.

Om du vill aktivera funktionen Webbkameraskydd i ESET Smart Security Premium ska du aktivera växlingsknappen bredvid **Aktivera Webbkameraskydd**.

När webbkameraskyddet är aktiverat blir **regler** aktiva, så att du kan öppna fönstret Regelredigerare.

Om du vill inaktivera varningar för program med en regel som har ändrats men fortfarande har en giltig digital signatur (till exempel en programuppdatering) ska du aktivera växlingsknappen bredvid **Inaktivera varningar om webbkameraåtkomst för ändrade program**.

Regelredigerare för webbkameraskydd

Det här fönstret visar befintliga regler och möjliggör styrning av program och processer som har åtkomst till datorns webbkamera utifrån den åtgärd du har vidtagit.

Följande åtgärder finns tillgängliga:

- **Tillåt åtkomst**
- **Spärra åtkomst**
- **Fråga** (frågar användaren varje gång ett program försöker komma åt webbkameran)

Avmarkera kryssrutan i kolumnen **Meddela** om du vill sluta få meddelanden när ett program tillgår webbkameran.

> **Anvisningar med bilder**
> Så här skapar och redigerar du webbkameraregler i ESET Smart Security Premium.

ThreatSense

ThreatSense består av många avancerade hotidentifieringsmetoder. ThreatSense är en proaktiv metod vilket innebär att den kan skydda datorn mot tidig spridning av ett nytt hot. Genom att kombinera kodanalys, kodemulering, generiska signaturer, virussignaturer och använda dem tillsammans ökas systemsäkerheten avsevärt. Genomsökningsmotorn kan kontrollera flera dataströmmar samtidigt vilket maximerar effektiviteten och upptäcktsfrekvensen. ThreatSense-tekniken eliminerar även framgångsrikt rootkits.

med alternativen för inställning av ThreatSense går det att ange ett antal olika genomsökningsparametrar:

- Filtyper och tillägg som genomsöks
- En kombination av olika identifieringsmetoder
- Rensningsnivåer, osv.

Öppna inställningsfönstret genom att klicka på **ThreatSense** i Avancerade inställningar för moduler som använder ThreatSense-teknik (se nedan). Olika säkerhetsscenarier kan kräva olika konfigurationer. Det går därmed att individuellt konfigurera följande skyddsmoduler i ThreatSense:

- Skydd av filsystemet i realtid
- Genomsökning vid inaktivitet
- Startskanner
- Dokumentskydd
- Skydd av e-postklienter
- Webbåtkomstskydd
- Genomsökning av datorn

ThreatSense-parametrarna är starkt optimerade för varje modul och ändringar av dem kan märkbart påverka systemets funktion. Att till exempel ändra parametrarna så att internt packade filer alltid söks igenom eller att aktivera avancerad heuristik i modulen för skydd av filsystemet i realtid kan resultera i att systemet blir långsammare (normalt används dessa metoder endast för genomsökning av nyskapade filer). Vi rekommenderar att lämna ThreatSense-standardparametrarna oförändrade för alla moduler utom för genomsökningsmodulen.

Objekt som ska genomsökas

I det här avsnittet går det att definiera vilka komponenter och filer på datorn som genomsöks efter infiltrationer.

Arbetsminne – söker efter hot som angriper systemets arbetsminne.

Startsektorer/UEFI – genomsöker startsektorerna efterskadlig kod i MBR (master boot record). Läs mer om UEFI i ordlistan.

E-postfiler – programmet stöder följande filnamnstillägg: DBX (Outlook Express) och EML.

Arkiv – programmet stöder följande filnamnstillägg: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE och många andra.

Självuppackande arkiv – självuppackande arkiv (SFX) är arkiv som kan extrahera sig själva.

Internt packade filer – när internt packade filer (till skillnad från standardarkivtyper) körs dekomprimeras de i minnet. Förutom statiska arkiverare av standardtyp (UPX, yoda, ASPack, FSG osv.) känner skannern igen många fler typer av arkiverare genom kodemulering.

Genomsökningsalternativ

Välj vilka metoder som ska användas för att söka efter infiltrationer i systemet. Följande alternativ finns tillgängliga:

Heuristik – heuristik är en algoritm som analyserar (skadliga) aktiviteter i program. Huvudfördelen med tekniken är möjligheten att identifiera skadlig programvara som inte fanns eller som inte var känd av den tidigare detekteringsmotorn. Nackdelen är (en mycket liten) risk för falska larm.

Avancerad heuristik/DNA-signaturer – avancerad heuristik är en unik heuristikalgoritm som utvecklats av ESET och som optimerats för att upptäcka datormaskar och trojanska hästar som skrivits på programmeringsspråk på hög nivå. Genom att använda avancerad heuristik blir ESET-produkterna bättre på att detektera hot. Signaturer används för att pålitligt detektera och identifiera virus. Med det automatiska uppdateringssystemet är nya signaturer tillgängliga inom några timmar efter att ett hot identifierades. Nackdelen med signaturer är att de bara detekterar virus de känner till (eller lätt ändrade versioner av dessa virus).

Rensning

Inställningarna för rensning anger hur ESET Smart Security Premium fungerar under rensning av infekterade objekt. Det finns fyra rensningsnivåer:

ThreatSense har följande åtgärdsnivåer (det vill säga rensningsnivåer).

Åtgärd i ESET Smart Security Premium

Rensningsnivå	Beskrivning
Åtgärda alltid detektering	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa sällsynta fall (till exempel systemfiler) lämnas det rapporterade objektet på sin ursprungliga plats om detekteringen inte kan åtgärdas.
Åtgärda detektering om det är säkert, behåll annars	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa fall (till exempel systemfiler eller arkiv med både rena och infekterade filer) lämnas det rapporterade objektet på sin ursprungliga plats om en detektering inte kan åtgärdas.
Åtgärda detektering om det är säkert, fråga annars	Försök att åtgärda detekteringen när du rensar objekt. I vissa fall, om ingen åtgärd kan utföras, får slutanvändaren en interaktiv avisering och måste välja en åtgärd (till exempel ta bort eller ignorera). Den här inställningen rekommenderas i de flesta fall.
Fråga alltid slutanvändaren	Ett interaktivt fönster visas för slutanvändaren när objekt rensas och en åtgärd måste väljas (till exempel ta bort eller ignorera). Denna nivå är avsedd för mer avancerade användare som vet vilka som ska åtgärder vidtas i händelse av detektering.

Undantag

Ett filnamnstillägg är den del av filnamnet som avgränsas med en punkt. Ett filändelse definierar filens typ och innehåll. I det här avsnittet för ThreatSense-inställningarna kan du definiera vilka typer av filer som ska genomsökas.

Övrigt

När du konfigurerar parameterinställningarna för ThreatSense-motorn för en Genomsökning av datorn på begäran är följande alternativ i avsnittet **Andra** också tillgängliga:

Genomsök alternativa dataströmmar (ADS) – de alternativa dataströmmarna som används av filsystemet NTFS består av fil- och mappassociationer som inte är synliga för vanliga genomsökningsmetoder. Många infiltrationsförsök maskerar sig som alternativa dataströmmar för att undvika upptäckt.

Kör genomsökningar i bakgrunden med låg prioritet – varje genomsökningssekvens kräver en viss mängd systemresurser. Om du arbetar med program som kräver mycket systemresurser kan du aktivera genomsökning i bakgrunden med låg prioritet och spara resurser till dina program.

Logga alla objekt – i genomsökningsloggen visas alla genomsökta filer i självuppackande arkiv, även sådana som inte är infekterade (detta kan generera mycket genomsökningsloggdata och öka genomsökningsloggfilens storlek).

Aktivera Smart optimering – med aktiverad smart optimering används de optimala inställningarna för effektivast genomsökning och bibehåller samtidigt den högsta genomsökningshastigheten. De olika skyddsmodulerna genomsöker intelligent och använder olika genomsökningsmetoder och tillämpar dem på vissa filtyper. Om smart optimering är inaktiverad tillämpas endast de användardefinierade inställningarna i ThreatSense-kärnan när en genomsökning utförs.

Bevara tidsstämpeln för senaste åtkomst – markera det här alternativet om du vill behålla den ursprungliga

åtkomsttiden för genomsökta filer i stället för att uppdatera dem (t.ex. för användning med system för säkerhetskopiering av data).

Begränsningar

Under Begränsningar kan du ange en maximal storlek på objekt och nivåer på de nästlade arkiv som ska genomsökas:

Objektinställningar

Maximal objektstorlek – anger maximal storlek på objekt som ska genomsökas. Den angivna antivirusmodulen kommer endast att genomsöka objekt som är mindre än den angivna storleken. Alternativet ska endast ändras av avancerade användare som kan ha särskilda anledningar till att undanta större objekt från genomsökning. Standardvärde: obegränsat.

Maximal tid för genomsökning av objekt (sek.) – definierar det maximala tidsvärdet för genomsökning av filer i ett behållarobjekt (till exempel ett RAR/ZIP-arkiv eller ett e-postmeddelande med flera bilagor). Den här inställningen gäller inte för fristående filer. Om ett användardefinierat värde har angetts och den tiden har förflutit stoppas en genomsökning så snart som möjligt, oavsett om genomsökningen av varje fil i ett behållarobjekt har slutförts.
När det gäller ett arkiv med stora filer stoppas genomsökningen tidigast då en fil från arkivet extraheras (till exempel när en användardefinierad variabel är 3 sekunder, men extraheringen av en fil tar 5 sekunder). Resten av filerna i arkivet kommer inte att genomsökas när den tiden har förflutit.
Om du vill begränsa genomsökningstiden, inklusive större arkiv, använder du **Maximal objektstorlek** och **Maximal filstorlek i arkivet** (rekommenderas inte på grund av möjliga säkerhetsrisker).
Standardvärde: obegränsat.

Inställningar för genomsökning av arkiv

Antal nästlade arkiv – anger maximalt djup vid arkivgenomsökningen. Standardvärde: 10.

Maximal filstorlek i arkivet – ange maximal filstorlek för filer i arkiven (efter att de extraherats) som genomsöks. Maxvärdet är **3 GB**.

> Vi rekommenderar inte att ändra standardvärdena, eftersom det i regel inte finns någon anledning att ändra dem.

Rensningsnivåer

Om du vill ändra inställningarna för rensningsnivå för en önskad skyddsmodul ska du expandera **ThreatSense** (till exempel **Skydd av filsystemet i realtid**) och sedan välja en **rensningsnivå** i listrutan.

ThreatSense har följande åtgärdsnivåer (det vill säga rensningsnivåer).

Åtgärd i ESET Smart Security Premium

Rensningsnivå	Beskrivning
Åtgärda alltid detektering	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa sällsynta fall (till exempel systemfiler) lämnas det rapporterade objektet på sin ursprungliga plats om detekteringen inte kan åtgärdas.
Åtgärda detektering om det är säkert, behåll annars	Försök att åtgärda detekteringen när du rensar objekt utan några åtgärder från slutanvändaren. I vissa fall (till exempel systemfiler eller arkiv med både rena och infekterade filer) lämnas det rapporterade objektet på sin ursprungliga plats om en detektering inte kan åtgärdas.
Åtgärda detektering om det är säkert, fråga annars	Försök att åtgärda detekteringen när du rensar objekt. I vissa fall, om ingen åtgärd kan utföras, får slutanvändaren en interaktiv avisering och måste välja en åtgärd (till exempel ta bort eller ignorera). Den här inställningen rekommenderas i de flesta fall.
Fråga alltid slutanvändaren	Ett interaktivt fönster visas för slutanvändaren när objekt rensas och en åtgärd måste väljas (till exempel ta bort eller ignorera). Denna nivå är avsedd för mer avancerade användare som vet vilka som ska åtgärder vidtas i händelse av detektering.

Filändelser som är undantagna från genomsökning

Undantagna filändelser är en del av ThreatSense. Om du vill konfigurera uteslutna filändelser ska du klicka på **ThreatSense** i Avancerade inställningar för moduler som använder ThreatSense-teknik.

En filändelse är den del av filnamnet som kommer efter punkten. Ett filändelse definierar filens typ och innehåll. I det här avsnittet för ThreatSense-inställningar kan du definiera vilka typer av filer som ska genomsökas.

Blanda inte samman processexkluderingar, HIPS-exkluderingar och fil-/mappexkluderingar.

Som standard genomsöks alla filer. Det går att lägga till vilket tillägg som helst i listan över filer som undantas för genomsökning.

Det är ibland nödvändigt att undanta vissa filtyper från genomsökning om detta förhindrar att programmet som använder vissa filnamnstillägg fungerar normalt. Det kan till exempel vara lämpligt att undanta filer med tilläggen `.edb`, `.eml` och `.tmp` när MS Exchange server används.

Om du vill lägga till ett nytt undantag i listan klickar du på **Lägg till**. Skriv undantaget i det tomma fältet (till exempel tmp) och klicka på **OK**. När du väljer **Ange flera värden** kan du lägga till flera filändelser avgränsade med rader, kommatecken eller semikolon (till exempel välja **semikolon** som skiljetecken i listrutan och skriva `edb;eml;tmp`).
Det går att använda specialsymbolen ? (frågetecken). Frågetecknet motsvarar alla tecken (till exempel `?db`).

För att se det exakta tillägget (om något) för en fil i ett Windows-operativsystem måste du markera kryssrutan **Filnamnstillägg** i **Utforskaren** > **Visa** (flik).

Ytterligare ThreatSense-parametrar

Om du vill redigera de här inställningarna ska du öppna Avancerade inställningar > **Skydd** > **Skydd av filsystemet i realtid** > **Ytterligare parametrar för ThreatSense**.

Ytterligare ThreatSense-parametrar för filer som nyligen skapats eller ändrats

Möjligheten att filer som nyligen skapats eller ändrats infekteras är jämförelsevis högre än för befintliga filer. Detta är orsaken till att programmet kontrollerar dessa filer med ytterligare genomsökningsparametrar. ESET Smart Security Premium använder avancerad heuristik som kan upptäcka nya hot innan detekteringsmotorns uppdatering ges ut i kombination med signaturbaserade genomsökningsmetoder.

Utöver nya skapade filer, utförs även genomsökning i **självuppackande arkiv** (.sfx) och **internt packade filer** (internt komprimerade exekverbara filer). I standardläget genomsöks arkiv upp till 10:e nästlingsnivån och kontrolleras oavsett faktisk storlek. Ändra inställningarna för arkivgenomsökning genom att avmarkera **Standardinställningar för genomsökning av arkiv**.

Ytterligare ThreatSense-parametrar för filer som har körts

Avancerad heuristik vid körning av fil – som standard används Avancerad heuristik när filer körs. När det används bör Smart optimering och ESET LiveGrid® vara aktiverade så att systemets prestanda inte påverkas lika mycket.

Avancerad heuristik när filer körs från flyttbara medier – med avancerad heuristik emuleras kod i en virtuell miljö och dess beteende utvärderas innan koden tillåts att köras från flyttbara medier.

Verktyg

Du kan konfigurera avancerade inställningar för funktioner som ger ytterligare säkerhet och förenklar administrationen av ESET Smart Security Premium i Avancerade inställningar > **Verktyg**.

- Microsoft Windows®-uppdatering
- ESET CMD
- Loggfiler
- Spelläge
- Diagnostik

Microsoft Windows®-uppdatering

Windows-uppdateringar är en viktig komponent som skyddar användarna från skadlig programvara. Därför är det viktigt att installera alla uppdateringar för Microsoft Windows så snart de blir tillgängliga. ESET Smart Security Premium meddelar dig om saknade uppdateringar enligt nivån du har angett i Avancerade inställningar > **Verktyg**. Följande nivåer finns tillgängliga:

- **Inga uppdateringar** – inga systemuppdateringar erbjuds för hämtning.
- **Valfria uppdateringar** – uppdateringar markerade med låg och högre prioritet erbjuds för hämtning.
- **Rekommenderade uppdateringar** – uppdateringar markerade med vanlig och högre prioritet erbjuds för hämtning.

- **Viktiga uppdateringar** – uppdateringar markerade med viktig och högre prioritet erbjuds för hämtning.
- **Kritiska uppdateringar** – endast kritiska uppdateringar erbjuds för hämtning.

Dialogruta – systemuppdateringar

Om det finns uppdateringar för ditt operativsystem visar ESET Smart Security Premium ett meddelande i huvudprogramfönstret > **Översikt**. Klicka på **Mer information** om du vill öppna fönstret Systemuppdateringar.

I fönstret Systemuppdateringar visas en lista över tillgängliga uppdateringar som är redo att hämtas och installeras. Uppdateringen visas bredvid uppdateringens namn.

Dubbelklicka på en uppdateringsrad om du vill visa ett fönstret Uppdateringsinformation med mer information.

Klicka på **Kör systemuppdatering** för att ladda ned och installera alla listade uppdateringar för operativsystemet.

Uppdateringsinformation

I fönstret Systemuppdateringar visas en lista över tillgängliga uppdateringar som är redo att hämtas och installeras. Uppdateringens prioritetsnivå visas bredvid uppdateringens namn.

Klicka på **Kör systemuppdatering** för att påbörja hämtning och installation av uppdateringar för operativsystemet.

Högerklicka på en uppdateringsrad och klicka på **Visa information** för att visa ett nytt fönster med ytterligare information.

ESET CMD

Med den här funktionen går det att använda avancerade ecmd-kommandon. Då kan du exportera och importera inställningar via kommandoraden (ecmd.exe). Tidigare har det endast varit möjligt att exportera inställningar via GUI. ESET Smart Security Premium-konfigurationer kan exporteras till en *.xml*-fil.

När ESET CMD har aktiverats finns det två auktoriseringsmetoder att välja mellan:

- **Ingen** – ingen auktorisering. Den här metoden bör inte användas eftersom den tillåter import av alla osignerade konfigurationer, vilket medför potentiella risker.
- **Lösenord för avancerade inställningar** – Ett lösenord krävs för att importera en konfiguration från en .xml-fil. Filen måste vara signerad (se signering av .xml-konfigurationsfiler längre ned). Lösenordet som angetts i Inställningar för åtkomst måste anges innan en ny konfiguration kan importeras. Om åtkomstinställningarna inte har aktiverats, lösenorden inte överensstämmer eller .xml-konfigurationsfilen inte är signerad, så importeras inte konfigurationen.

När ESET CMD har aktiverats kan du använda kommandoraden för att importera eller exportera ESET Smart Security Premium-konfigurationer. Du kan göra detta manuellt eller automatisera det med ett skript.

För att kunna använda avancerade ecmd-kommandon måste du ha administratörsbehörighet eller öppna Windows kommandoprompt (cmd) med **Kör som administratör**. Annars visas meddelandet **Error executing command**. När en konfiguration exporteras måste dessutom målmappen finnas. Exportkommandot fungerar även när ESET CMD-inställningen är avstängd.

Kommando för export av inställningar:
`ecmd /getcfg c:\config\settings.xml`

Kommando för import av inställningar:
`ecmd /setcfg c:\config\settings.xml`

Avancerade ecmd-kommandon kan endast köras lokalt.

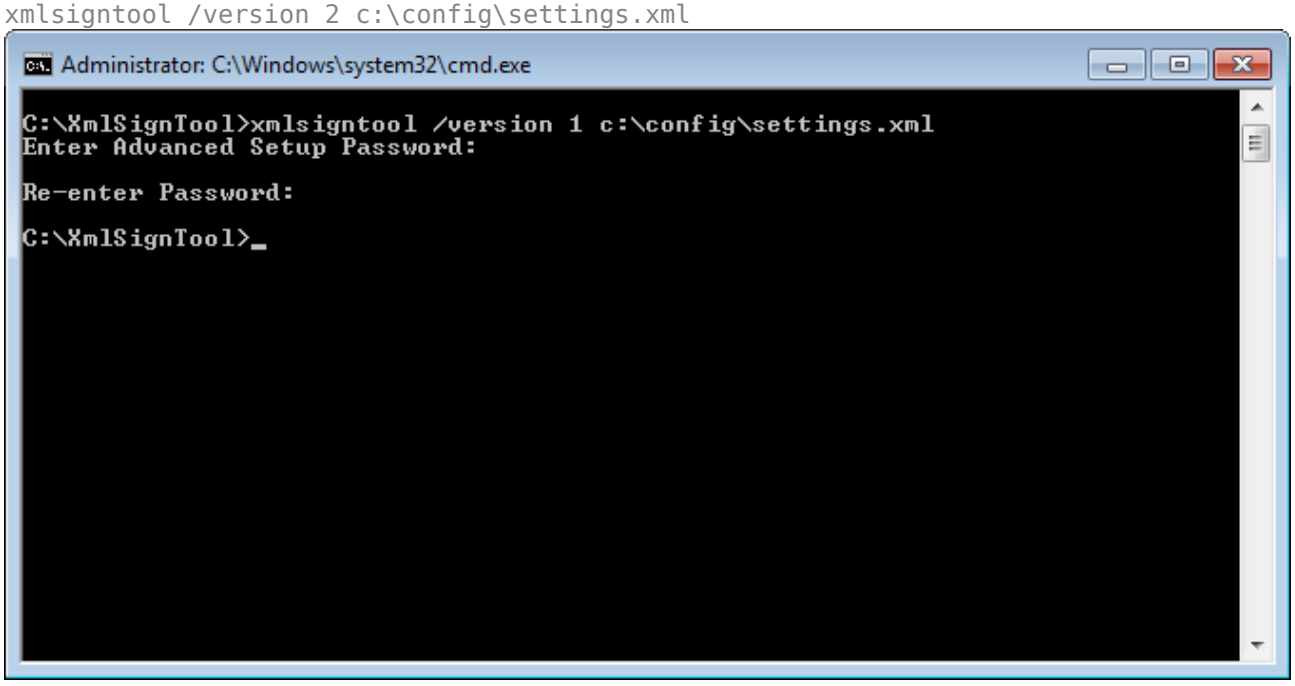
Signera en *.xml*-konfigurationsfil:

1. Hämta den körbara filen XmlSignTool.
2. Öppna en Windows-kommandoprompt (cmd) med **Kör som administratör**.
3. Navigera till platsen där du vill spara `xmlsigntool.exe`
4. Kör ett kommando för att signera *.xml*-konfigurationsfilen, användning: `xmlsigntool /version 1|2 <xml_file_path>`

Värdet för parametern `/version` beror på vilken version av ESET Smart Security Premium du har. Använd `/version 1` för tidigare versioner av ESET Smart Security Premium än 11.1. Använd `/version 2` för den aktuella versionen av ESET Smart Security Premium.

5. Ange och upprepa lösenordet för avancerade inställningar när du ombeds att göra det av XmlSignTool. Nu är *.xml*-konfigurationsfilen signerad och kan användas för att importera en annan instans av ESET Smart Security Premium med ESET CMD där lösenord används som auktoriseringsmetod.

Kommando för att signera en exporterad konfigurationsfil:
`xmlsigntool /version 2 c:\config\settings.xml`



Om lösenordet för åtkomst till inställningar ändras och du vill importera en konfigurationsfil som redan har signerats med ett äldre lösenord, så måste *.xml*-konfigurationsfilen signeras igen med det aktuella lösenordet. Då kan du använda en äldre konfigurationsfil utan att behöva exportera den till en annan dator med ESET Smart Security Premium före importen.

ESET CMD bör inte aktiveras utan auktorisering, eftersom import av osignerade konfigurationer då tillåts. Ställ in lösenordet i Avancerade inställningar > **Användargränssnitt** > **Inställningar för åtkomst** för att förhindra att användare gör obehöriga ändringar.

Loggfiler

Du hittar loggningskonfigurationen för ESET Smart Security Premium i Avancerade inställningar > **Verktyg** > **Loggfiler**. Avsnittet Loggar används för att definiera hur loggarna ska hanteras. Programmet tar automatiskt bort gamla loggar för att spara hårddiskutrymme. Det går att välja följande alternativ för loggfiler:

Minimalt omfång för loggning – anger den lägsta omfångsnivån för händelser som ska loggas:

- **Diagnostik** – loggar information som behövs för att fininställa programmet och alla poster ovan.
- **Informativ** – loggar alla informationsmeddelanden, inklusive framgångsrika uppdateringar och alla poster ovan.
- **Varningar** – registrerar kritiska fel och varningsmeddelanden.
- **Fel** – fel som ”Fel när filen hämtades” och kritiska fel registreras.
- **Kritiska** – loggar endast kritiska fel (fel vid start av antivirusskyddet, brandvägg, osv...).

Alla blockerade anslutningar kommer att registreras när du väljer omfångsnivån Diagnostik.

Loggposter äldre än angivet antal dagar i **Ta automatiskt bort poster äldre än (dagar)** tas bort automatiskt.

Optimera loggfiler automatiskt – markera för att automatiskt defragmentera loggfilerna om procenttalet är högre än angivet i **Om antalet oanvända poster överskrider (%)**.

Klicka på **Optimera** för att starta defragmentering av loggfiler. Alla tomma loggposter tas bort under denna process, vilket förbättrar prestanda och hastighet när loggarna bearbetas. Denna förbättring märks särskilt om loggarna innehåller ett stort antal poster.

Välj **Aktivera textprotokoll** för att aktivera lagring av loggar i ett annat filformat separat från Loggfiler:

- **Målkatalog** – målkatalogen där loggfiler lagras (gäller endast text/CSV). Varje loggavsnitt har en egen fil med ett fördefinierat filnamn (exempelvis virlog.txt för avsnittet **Detekteringar** i Loggfiler, om du använder vanligt textfilsformat för att lagra loggar).
- **Typ** – om du väljer **Text**-filformatet lagras loggarna i en textfil; data avgränsas med tabbar. Detsamma gäller för det kommaavgränsade **CSV**-filformatet. Om du väljer **Händelse** lagras loggarna i händelseloggen i Windows (som kan visas med hjälp av Loggboken på Kontrollpanelen) i motsats till filen.
- **Ta bort loggar** – tar bor alla lagrade loggar som för närvarande valts i listrutan **Typ**. Ett meddelande om att loggarna tagits bort visas.

För att problem ska kunna lösas snabbare ombeds du ibland av ESET att tillhandahålla loggar från din dator. Med ESET Log Collector är det enkelt att samla in den information som behövs. För mer information om ESET Log Collector, se artikeln i ESET-kunskapsbasen.

Spelläge

Spelläge är en funktion för användare som kräver oavbruten användning av sina program och inte vill bli störda av meddelande/aviseringsfönster och vill minska belastningen på sin CPU. Spelläge går även att använda under presentationer som inte går att avbryta med antivirusaktiviteter. Genom att aktivera funktionen, inaktiveras alla popup-fönster och schemaläggarens aktivitet stoppas helt. Systemskyddet körs fortfarande i bakgrunden men kräver inte användaråtgärder.

Det går att aktivera och inaktivera spelläge i programmets huvudfönster under **Inställningar** > **Datorskydd** genom att klicka på  eller  bredvid **Spelläge**. Aktivering av spelläget är en potentiell säkerhetsrisk och skyddsstatusikonen i aktivitetsfältet blir orange och visar en varning. Du ser även denna varning i programmets huvudfönster där **Spelläget är aktivt** visas i orange.

Aktivera **Aktivera spelläge automatiskt när program körs i helskärmsläge** under Avancerade inställningar > **Verktyg** > **Spelläge** om du vill att spelläget ska startas varje gång ett program startas i helskärm och avslutas när programmet stängs.

Aktivera **Inaktivera spelläge automatiskt efter** för att ange efter hur lång tid spelläget ska inaktiveras automatiskt.

Om brandväggen är i interaktivt läge och spelläget aktiveras kan du få problem att ansluta till Internet. Detta kan vara ett problem om du startar ett spel som ansluter till Internet. Normalt ombeds du att bekräfta en sådan åtgärd (on inga kommunikationsregler eller undantag har definierats), men användarinteraktion är inaktiverat i spelläget. Om du vill tillåta kommunikation anger du en kommunikationsregel för de program som problemet kan uppstå för, eller använder ett annat Filtreringsläge i brandväggen. Kom ihåg att om spelläge är aktiverat och du går till en webbsida eller ett program som kan vara en säkerhetsrisk kanske den blockeras, men du ser ingen förklaring eller varning eftersom användarinteraktion är inaktiverad.

Diagnostik

Diagnostik tillhandahåller krashdumpar från ESET-processer (till exempel ekrn). Om ett program krashar kommer en dump att genereras. Det kan hjälpa utvecklare att felsöka och åtgärda olika ESET Smart Security Premium problem.

Klicka på listrutan intill **Dumptyp** och välj ett av de tre tillgängliga alternativen:

- Välj **Inaktivera** om du vill inaktivera funktionen.

- **Mini** (standard) – sparar en liten uppsättning användbar information som kan hjälpa till att identifiera varför programmet kraschade oväntat. Denna typ av dumpfil är användbar vid begränsat utrymme. På grund av den begränsade mängden information går det dock kanske inte vid en analys av den här filen att upptäcka fel som inte direkt orsakades av tråden som kördes vid tiden för problemet.

• **Fullständig** – sparar hela innehållet i systemminnet när programmet stannar oväntat. En fullständig minnesdump kan innehålla data från processer som kördes när minnesdumpen samlades in.

Målkatalog – katalogen där dumpen skapas vid kraschen.

Öppna diagnostikmappen – klicka på **Öppna** för att öppna katalogen i ett nytt fönster i *Utforskaren*.

Skapa diagnostikdump – klicka på **Skapa** om du vill skapa diagnostiska dumpfiler i **målkatalogen**.

Avancerad loggning

Aktivera avancerad inloggning i marknadsföringsmeddelanden – spela in alla händelser relaterade till marknadsföringsmeddelanden i produkten.

Aktivera avancerad loggning för spamskyddsmotor – registrera alla händelser som inträffar under genomsökning efter spam. Detta kan hjälpa utvecklare att diagnostisera och åtgärda problem relaterade till ESET Antispam-motorn.

Aktivera avancerad loggning för stöldskyddsmotor – registrera alla händelser som inträffar i stöldskyddet så att problem kan diagnostiseras och åtgärdas.

Aktivera avancerad loggning för Webbläsarskydd − registrera alla händelser som inträffar i Säkra banktjänster och surfning.

Aktivera avancerad loggning för genomsökning av datorn – registrerar händelser som uppstår under genomsökning av filer eller mappar av genomsökningen av datorn.

Aktivera avancerad loggning för enhetskontroll – registrera alla händelser som inträffar i Enhetskontroll. Det hjälper utvecklare att diagnostisera och åtgärda problem relaterade till Enhetskontroll.

Aktivera avancerad loggning för Direct Cloud – registrera alla händelser som inträffar i ESET LiveGrid®. Detta kan hjälpa utvecklare att diagnostisera och åtgärda problem relaterade till ESET LiveGrid®.

Aktivera avancerad loggning för Dokumentskydd – registrera alla händelser som sker i Dokumentskydd för att möjliggöra diagnostisering och lösa problem.

Aktivera avancerad loggning för skydd av e-postklienter – registrera alla händelser som inträffar i skydd av e-postklienter och plugin-program för e-postklienter för att möjliggöra diagnostisering och lösning av problem.

Aktivera avancerad loggning för ESET LiveGuard – registrera alla händelser som sker i ESET LiveGuard för att möjliggöra diagnostisering och lösa problem.

Aktivera avancerad kernelloggning – registrera alla händelser som inträffar i ESET-kerneln (ekrn).

Aktivera avancerad loggning för licensiering – registrera all produktkommunikation med ESET-aktiverings- eller ESET License Manager-servrar.

Aktivera minnesspårning – registrera alla händelser som hjälper utvecklare att diagnostisera minnesläckor.

Aktivera avancerad loggning för nätverksskydd – registrera all nätverksdata som passerar genom brandväggen i PCAP-format för att hjälpa utvecklare att diagnostisera och åtgärda problem relaterade till brandväggen.

Aktivera avancerad loggning av nätverkstrafikskanner – registrera alla data som passerar genom

nätverkstrafiksskannern i formatet PCAP för att hjälpa utvecklarna att diagnostisera och åtgärda problem relaterade till nätverkstrafikskannern.

Aktivera avancerad loggning av operativsystem – registrera ytterligare information om operativsystemet, till exempel processer som körs, processoraktivitet, diskåtgärder och så vidare, samlas in. Denna kan hjälpa utvecklare att diagnostisera och åtgärda problem relaterade till ESET-produkter som körs i operativsystemet.

Aktivera avancerad loggning för föräldrakontroll – registrera alla händelser som inträffar i Föräldrakontroll. Detta kan hjälpa utvecklare att diagnostisera och åtgärda problem relaterade till Föräldrakontroll.

Aktivera avancerad loggning av push-meddelanden – registrera alla händelser som inträffar under push-meddelanden.

Aktivera avancerad loggning för Skydd av filsystemet i realtid – registrera alla händelser som inträffar under genomsökning av filer eller mappar av Skydd av filsystemet i realtid.

Aktivera avancerad loggning av uppdateringsmotor – registrera alla händelser som inträffar under uppdateringen. Detta kan hjälpa utvecklare att diagnostisera och åtgärda problem relaterade till uppdateringsmotorn.

Loggfiler finns i *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Teknisk support

När du kontaktar ESET:s tekniska support från ESET Smart Security Premium kan du skicka systemkonfigurationsdata. Välj **Skicka alltid** i listrutan **Skicka systemkonfigurationsdata** för att skicka data automatiskt eller välj **Fråga före skickande** för att tillfrågas innan du skickar data.

Uppkoppling

I specifika nätverk kan kommunikationen mellan datorn och internet gå via en proxyserver. Om du använder en proxyserver måste du definiera följande inställningar. Annars går det inte att uppdatera ESET Smart Security Premium och dess moduler automatiskt. I ESET Smart Security Premium är proxyserverinställningar tillgängliga i två olika avsnitt av Avancerade inställningar.

Globala proxyserverinställningar går att konfigurera i Avancerade inställningar > **Anslutning** > **Proxyserver**. Anges proxyservern på denna nivå definieras de globala proxyserverinställningarna för hela ESET Smart Security Premium. Dessa parametrar används av alla moduler som kräver anslutning till Internet.

Om du vill ange globala proxyserverinställningar ska du aktivera **Använd proxyserver** och fylla i **proxyserveradressen** tillsammans med proxyserverns **portnummer**.

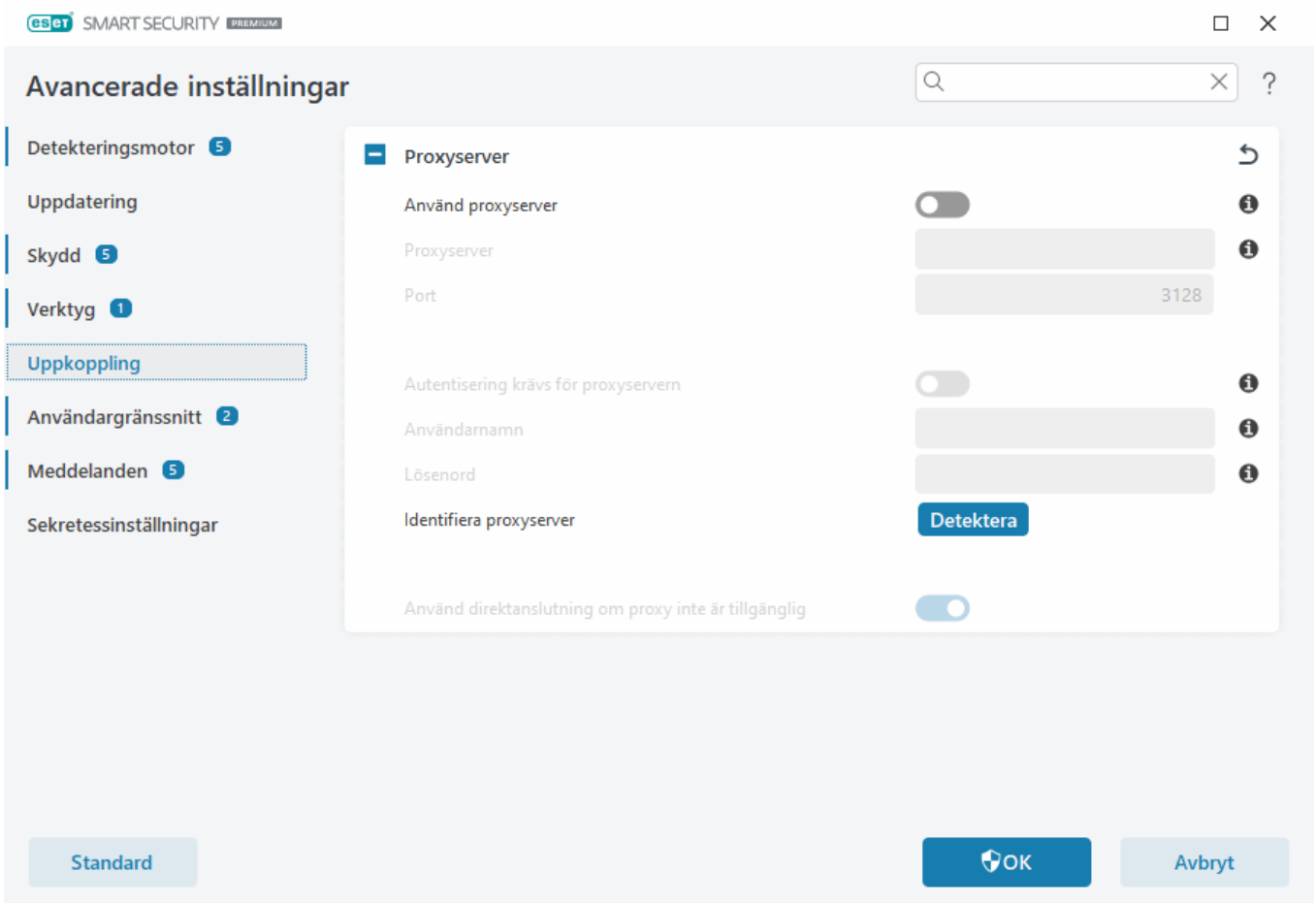
Om kommunikationen med proxyservern kräver autentisering, välj **Proxyservern kräver autentisering** och ange ett giltigt **Användarnamn** och **Lösenord** i respektive fält. Klicka på **Identifiera proxyserver** om du vill identifiera och fylla i proxyserverinställningarna automatiskt. ESET Smart Security Premium kopierar parametrarna som anges i internetalternativen för Internet Explorer eller Google Chrome.

> Användarnamnet och lösenordet måste fyllas i manuellt i **Proxyserver**-inställningarna.

Använd direktanslutning om proxy inte är tillgänglig – om ESET Smart Security Premium är konfigurerad att

ansluta via proxy och proxyn inte kan nås, så åsidosätter ESET Smart Security Premium proxyn och kommunicerar direkt med ESET:s servrar.

Det går även att ställa in proxyserverinställningarna i Avancerade uppdateringsinställningar Avancerade inställningar > **Uppdatera** > **Profiler** > **Uppdateringar** > **Anslutningsalternativ** genom att välja **Anslutning via en proxyserver** i listrutan **Proxyläge**. Den här konfigurationen gäller endast för uppdateringar och rekommenderas för bärbara datorer som tar emot moduluppdateringar från fjärranslutna platser. Du hittar mer information i Avancerade uppdateringsinställningar.



Användargränssnitt

Om du vill konfigurera programmets grafiska användargränssnitt (GUI) ska du öppna Avancerade inställningar > **Användargränssnitt**.

Du kan justera programmets utseende och effekterna som används på skärmen Element i användargränssnitt i Avancerade inställningar.

För att tillhandahålla maximal säkerhet för säkerhetsprogrammet går det att förhindra avinstallation eller obehöriga ändringar genom att lösenordskydda inställningarna med verktyget Inställningar för åtkomst.

> Se avsnittet Meddelanden om du vill konfigurera beteendet för systemmeddelanden, detekteringsvarningar och programstatusar.

Element i användargränssnitt

Du kan justera ESET Smart Security Premium-arbetsmiljön (GUI) så att den passar dina behov i Avancerade inställningar > **Användargränssnitt** > **Element i användargränssnittet**.

Färgläge – välj färgschemat för det grafiska användargränssnittet för ESET Smart Security Premium på rullgardinsmenyn:

- **Samma som systemfärgen** – ställer in färgschemat för ESET Smart Security Premium baserat på operativsystemets inställningar.
- **Mörkt** – ESET Smart Security Premium kommer att ha ett mörkt färgschema (mörkt läge).
- **Ljust** – ESET Smart Security Premium kommer att ha ett vanligt, ljust färgschema.

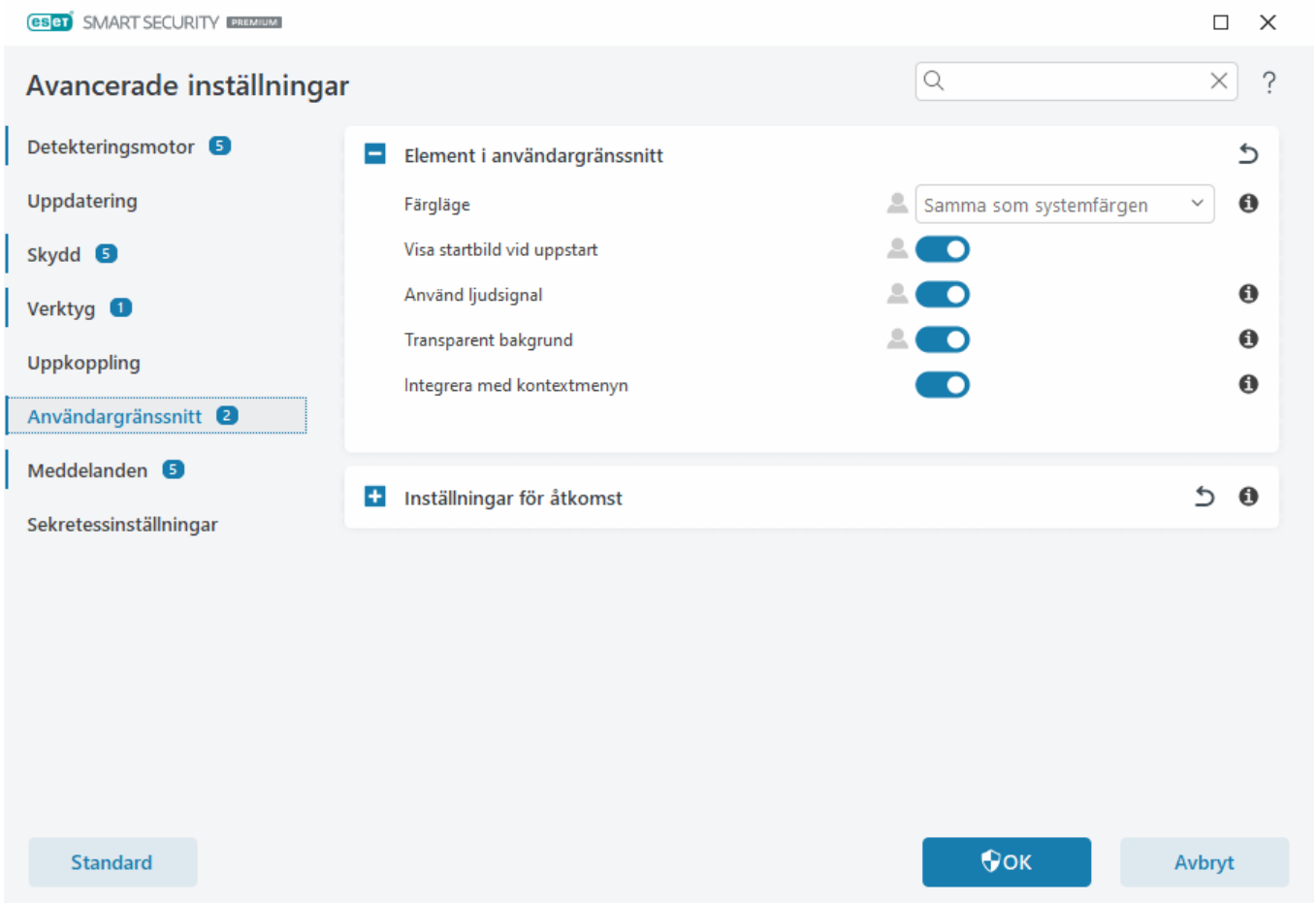
> Du kan också välja färgschemat för användargränssnittet för ESET Smart Security Premium i det övre högra hörnet av huvudprogramfönstret.

Visa startbild vid uppstart – visar ESET Smart Security Premium-startbilden under start.

Använd ljudsignal – spelar ett ljud när en viktig händelse inträffar, till exempel när ett hot har upptäckts eller när genomsökningen har slutförts.

Transparent bakgrund – aktiverar en transparent bakgrundseffekt för huvudprogramfönstret. Transparent bakgrund är endast tillgängligt för de senaste Windows-versionerna (RS4 och senare).

Integrera i kontextmenyn – integrera kontrollelementen i ESET Smart Security Premium i kontextmenyn.



Inställningar för åtkomst

ESET Smart Security Premium-inställningarna är en viktig del i din säkerhetspolicy. Obehöriga ändringar kan potentiellt äventyra systemets stabilitet och skydd. Om du vill undvika obehöriga ändringar installationsparametrarna och avinstallation för ESET Smart Security Premium lösenordsskyddas. Åtkomstinställningar kan konfigureras i Avancerade inställningar > **Användargränssnitt** > **Åtkomstinställningar**.

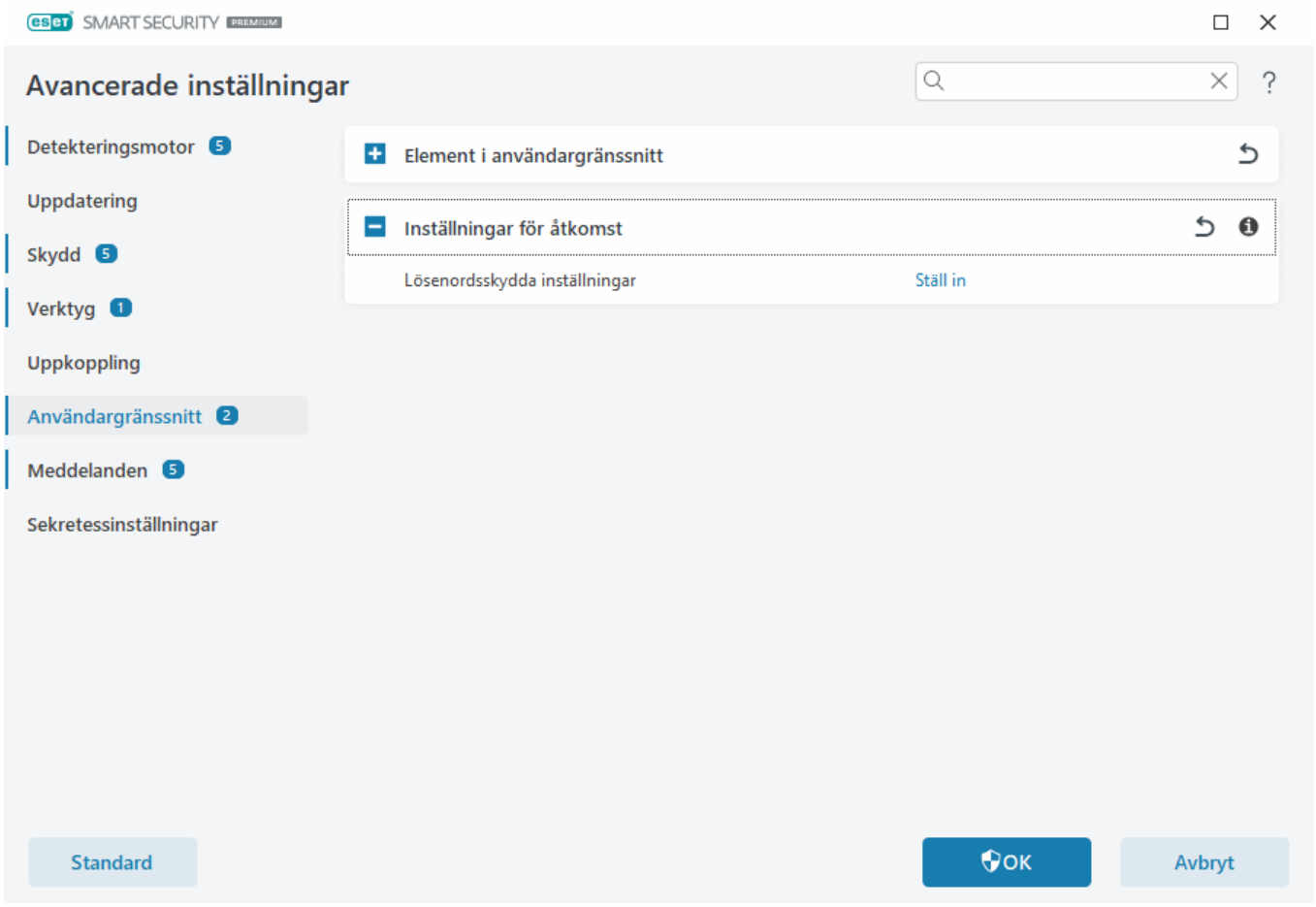
Om du vill ange ett lösenord för att skydda installationsparametrar och avinstallation för ESET Smart Security Premium klickar du på **Ställ in** bredvid **Inställningar för lösenordsskydd**.

När du vill komma åt de skyddade avancerade inställningarna visas fönstret för att ange lösenordet. Om du har glömt eller blivit av med lösenordet klickar du på alternativet **Återställ lösenord** nedan och anger den e-postadress som användes när abonnemanget registrerades. ESET skickar ett e-postmeddelande med verifieringskoden och anvisningar om hur du återställer lösenordet.

- Låsa upp avancerade inställningar

Om du vill ändra ditt lösenord klickar du på **Ändra lösenord** bredvid **Inställningar för lösenordsskydd**.

Om du vill ta bort lösenordet klickar du på **Ta bort** bredvid **Inställningar för lösenordsskydd**.



Lösenord för Avancerade inställningar

Om du vill skydda de avancerade inställningarna för ESET Smart Security Premium och undvika obehöriga ändringar, så skriver du ditt nya lösenord i fälten **Nytt lösenord** och **Bekräfta lösenord**. Klicka på **OK**.

När du vill ändra ett befintligt lösenord:

1. Skriv det gamla lösenordet i fältet **Gammalt lösenord**.
2. Ange det nya lösenordet i fälten **Nytt lösenord** och **Bekräfta lösenord**.
3. Klicka på **OK**.

Det här lösenordet krävs för åtkomst till avancerade inställningar.

Om du glömmer ditt lösenord läser du Låsa upp ditt inställningslösenord i ESET:s hemprodukter.

Information om hur du återställer en borttappad ESET-aktiveringsnyckel, abonnemangets utgångsdatum eller annan abonnemangsinformation för ESET Smart Security Premium finns i Jag har tappat bort min aktiveringsnyckel.

Stöd för skärmläsare

ESET Smart Security Premium kan användas tillsammans med skärmläsare för att låta ESET-användare med nedsatt syn navigera i produkten eller för att konfigurera inställningarna. Följande skärmläsare stöds (JAWS,

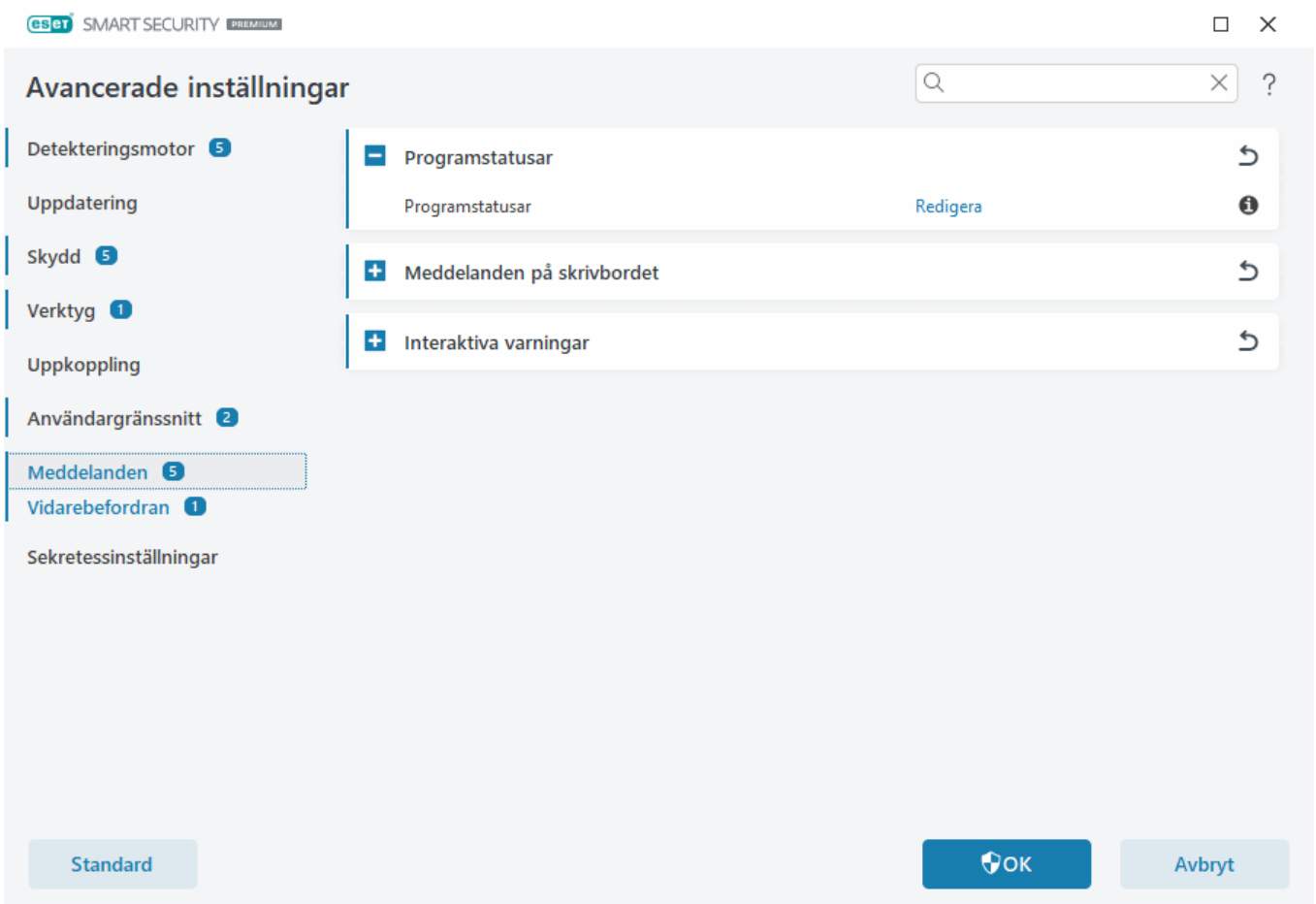
NVDA, Narrator).

För att kontrollera att skärmläsarprogramvaran ESET Smart Security Premium kan komma åt GUI på rätt sätt följer du instruktionerna i vårt artikel i kunskapsbas.

Meddelanden

Om du vill hantera meddelanden för ESET Smart Security Premium ska du öppna Avancerade inställningar > **Meddelanden**. Du kan konfigurera följande typer av meddelanden:

- Programstatusar – meddelanden som visas i hemavsnittet i huvudprogramfönstret > **Översikt**.
- Skrivbordsmeddelanden – små meddelandefönster bredvid systemaktivitetsfältet.
- Interaktiva aviseringar – varningsfönster och meddelanderutor som kräver användarinteraktion.
- Vidarebefordran (Meddela via e-post) – E-postmeddelanden skickas till den angivna e-postadressen.



Programstatusar

Programstatusar – klicka på **Redigera** för att välja vilka programstatusar som ska visas i hemavsnittet i programmets huvudfönster > **Översikt**.

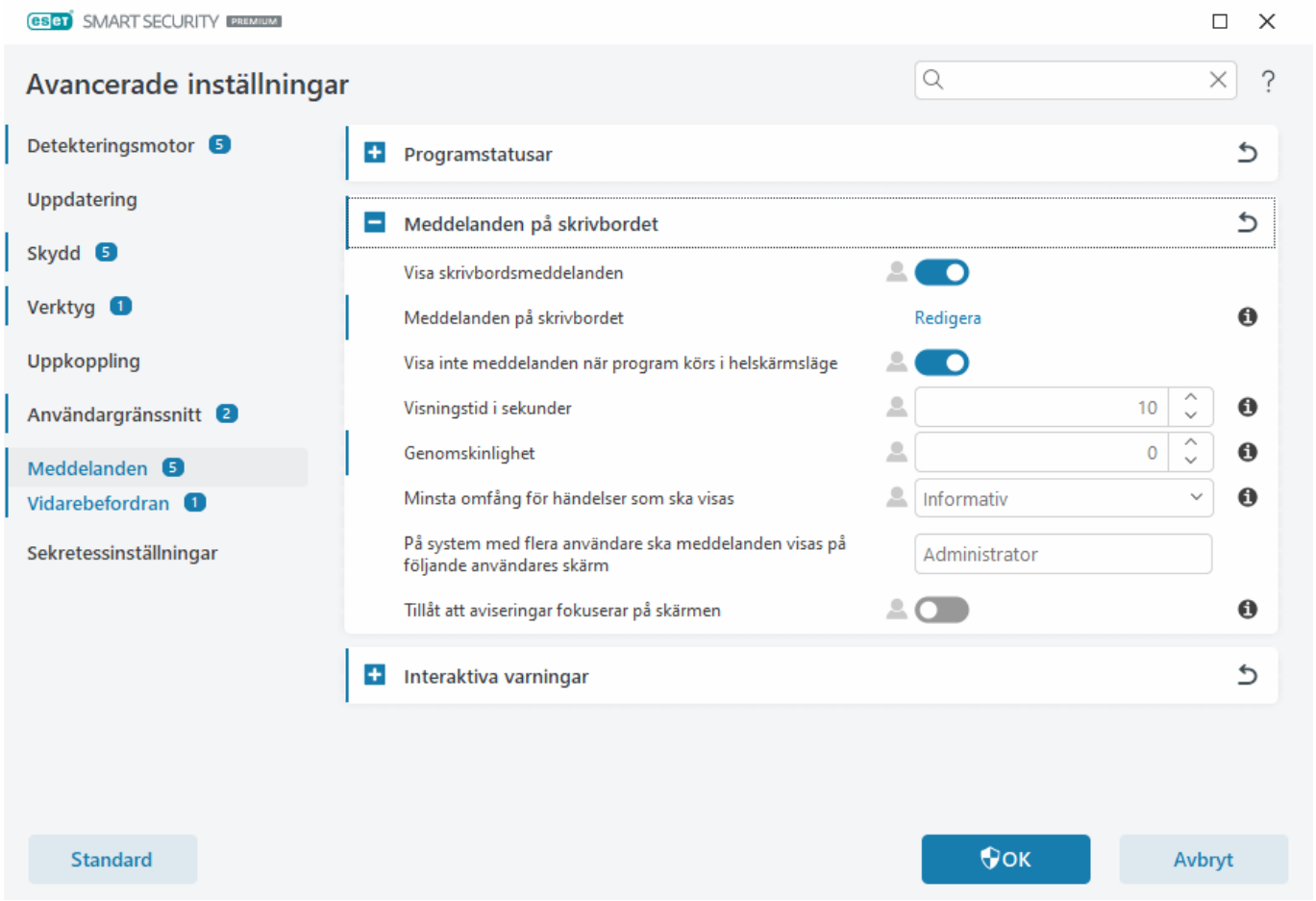
Dialogfönster – programstatusar

I det här dialogfönstret kan du välja vilka programstatusar som ska visas. Till exempel när du pausar skydd mot virus och spionprogram eller aktiverar spelläget.

Programstatus visas även om produkten inte är aktiverad eller om abonnemanget har upphört.

Meddelanden på skrivbordet

Meddelanden på skrivbordet aviseras med ett litet meddelandefönster bredvid aktivitetsfältet. Som standard visas de i 10 sekunder och försvinner sedan långsamt. Meddelandena inkluderar slutförda produktuppdateringar, anslutning av nya enheter, slutförda genomsökningar efter virus eller nya hot som har hittats.



Visa meddelanden på skrivbordet – vi rekommenderar att det här alternativet hålls aktiverat så att produkten kan informera om när en ny händelse inträffar.

Skrivbordsmeddelanden – klicka på **Redigera** om du vill aktivera eller inaktivera vissa skrivbordsmeddelanden.

Visa inte meddelanden när program körs i helskärmsläge – ignorera alla icke-interaktiva meddelanden när du kör program i helskärmsläge.

Visningstid i sekunder – Ange hur länge meddelanden ska synas. Värdet måste vara mellan 3-30 sekunder.

Genomskinlighet – Ange meddelandets transparens i procent. Det intervall som stöds är 0 (ingen transparens) till 80 (mycket hög transparens).

Minsta omfång för händelser som ska visas – Ange den lägsta allvarlighetsgraden för meddelanden som visas. Välj något av följande alternativ på rullgardinsmenyn:

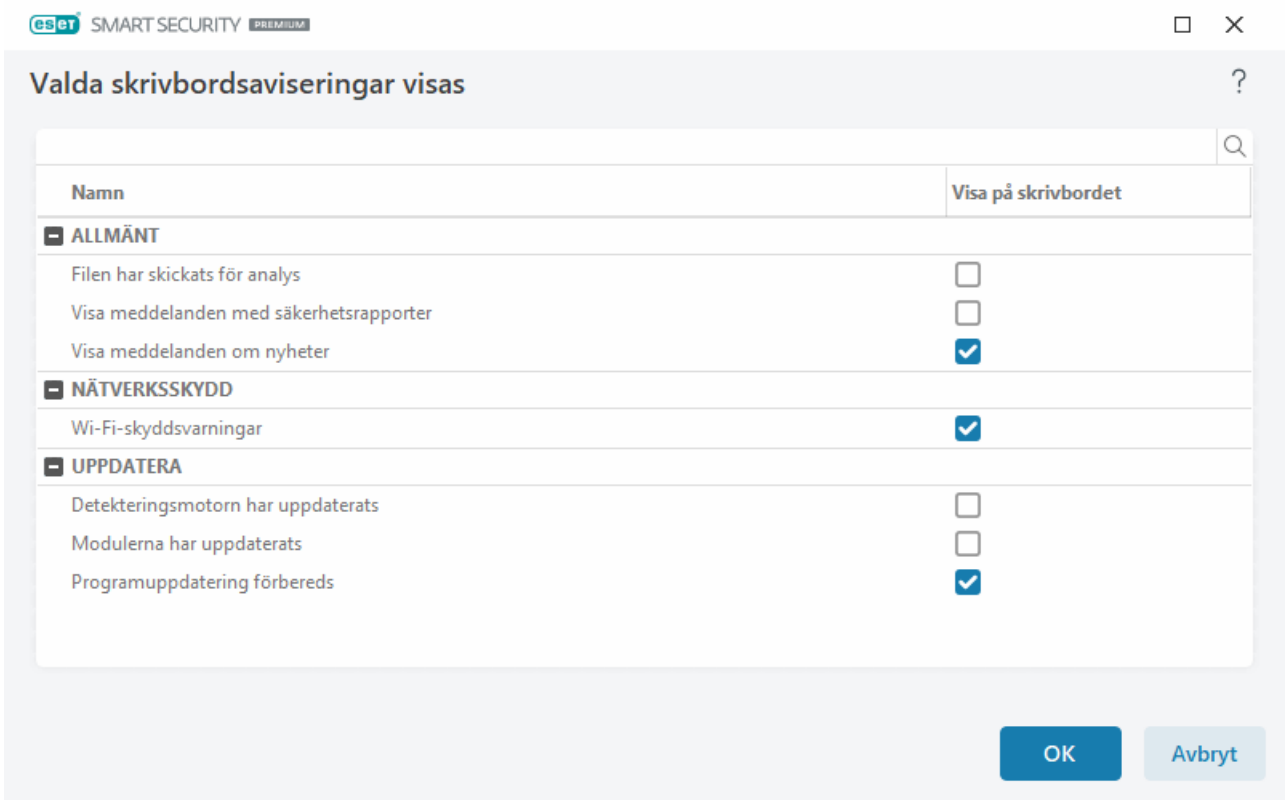
- **Diagnostik** – visar information som behövs för att fininställa programmet och alla poster ovan.
- **Information** – visar alla informationsmeddelanden, exempelvis ovanliga nätverkshändelser, inklusive framgångsrika uppdateringar och alla poster ovan.
- **Varningar** – visar varningsmeddelanden, fel och kritiska fel (till exempel misslyckad uppdatering).
- **Fel** – Visar fel (till exempel att dokumentskyddet inte har startats) och kritiska fel.
- **Kritiska** – Visar endast kritiska fel (fel vid start av antivirusskyddet eller infekterat system och så vidare).

På system med flera användare ska meddelanden visas på följande användares skärm – gör så att det valda kontot kan ta emot skrivbordsmeddelanden. Om du till exempel inte använder administratörskontot skriver du det fullständiga kontonamnet, så visas skrivbordsmeddelanden för det specifika kontot. Endast ett användarkonto kan ta emot skrivbordsmeddelanden.

Tillåt att aviseringar fokuserar på skärmen – Gör att aviseringar kan fokusera på skärmen och är tillgängliga på **ALT + tabb**-menyn.

Lista med meddelanden på skrivbordet

Om du vill justera synligheten för skrivbordsmeddelanden (som visas längst ned till höger på skärmen) öppnar du Avancerade inställningar > **Meddelanden** > **Skrivbordsmeddelanden**. Klicka på **Redigera** bredvid **Skrivbordsmeddelanden** och markera lämplig **Visa**-kryssruta.



Allmänt

Visa meddelanden med säkerhetsrapporter – få ett meddelande när en ny säkerhetsrapport genereras.

Visa meddelanden om nyheter – meddelanden om helt nya förbättrade funktioner i den senaste produktversionen.

Filen skickades för analys – få ett meddelande varje gång ESET Smart Security Premium skickar en fil för analys.

Network Inspector

Meddela mig om nyligen upptäckta nätverksenheter – få ett meddelande när en ny enhet ansluts till nätverket.

Nätverksskydd

Nätverksprofilen har ändrats – få ett meddelande när nätverksprofilen ändras.

Varningar om skydd av Wi-Fi – få ett meddelande när du försöker ansluta till ett Wi-Fi-nätverk med ett svagt eller inget lösenord.

Uppdatera

Programuppdatering förbereds – få ett meddelande när en uppdatering till en ny version av ESET Smart Security Premium förbereds.

Detekteringsmotorn har uppdaterats – få ett meddelande när detekteringsmotorns moduler har uppdaterats.

Modulerna har uppdaterats – få ett meddelande när programkomponenterna har uppdaterats.

Om du vill göra allmänna inställningar för meddelanden på skrivbordet, till exempel hur länge ett meddelande ska visas eller minsta omfång för händelser som ska visas, går du till Meddelanden på skrivbordet i Avancerade inställningar > **Meddelanden**.

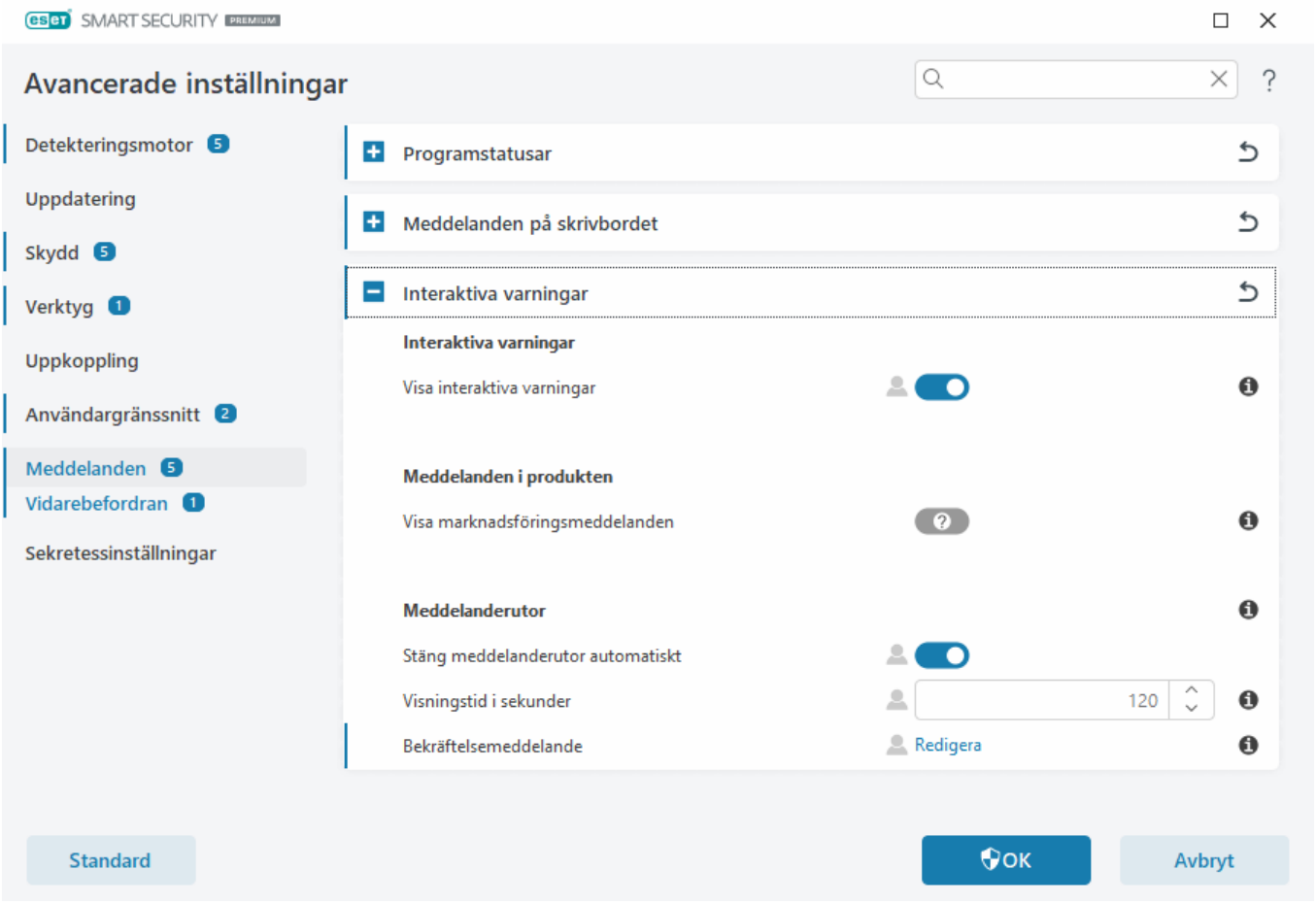
Interaktiva varningar

Letar du efter information om vanliga varningar och meddelanden?

- Hot upptäckt
- Adressen har blockerats
- Produkten inte aktiverad
- Byt till en produkt med fler funktioner
- Byt till en produkt med färre funktioner
- Uppdatering tillgänglig
- Uppdateringsinformationen är inte konsekvent
- Felsöka meddelandet Moduluppdateringen misslyckades
- Lösa uppdateringsfel för moduler
- Nätverkshot blockerat
- Webbplatscertifikatet har återkallats

Avsnittet **Interaktiva aviseringar** i Avancerade inställningar > **Meddelanden** gör att du kan konfigurera hur

meddelanderutor och interaktiva aviseringar för detekteringar där ett beslut måste fattas av en användare (till exempel en potentiell nätfiskewebbplats) hanteras av ESET Smart Security Premium.



Interaktiva varningar

Om du inaktiverar **Visa interaktiva varningar** döljs alla varningsfönster och dialogrutor i webbläsaren, vilket endast är lämpligt för ett mycket begränsat antal situationer. Vi rekommenderar att du håller detta alternativ aktiverat.

Meddelanden i produkten

Meddelanden i produkten är utformade för att informera användare om ESET-nyheter och annan kommunikation. För att skicka marknadsföringsmeddelanden krävs användarens samtycke. Marknadsföringsmeddelanden skickas därför inte till användare som standard (visas med ett frågetecken). Genom att aktivera det här alternativet samtycker du till att få marknadsföringsmeddelanden från ESET. Om du inte vill ha marknadsföringsmaterial från ESET inaktiverar du alternativet **Visa marknadsföringsmeddelanden**.

Meddelanderutor

Vill du att meddelanderutorna stängs automatiskt efter en viss tid markerar du **Stäng meddelanderutor automatiskt**. Stänger användaren inte själv varnings- och meddelandefönster, så stängs de automatiskt efter den angivna tiden.

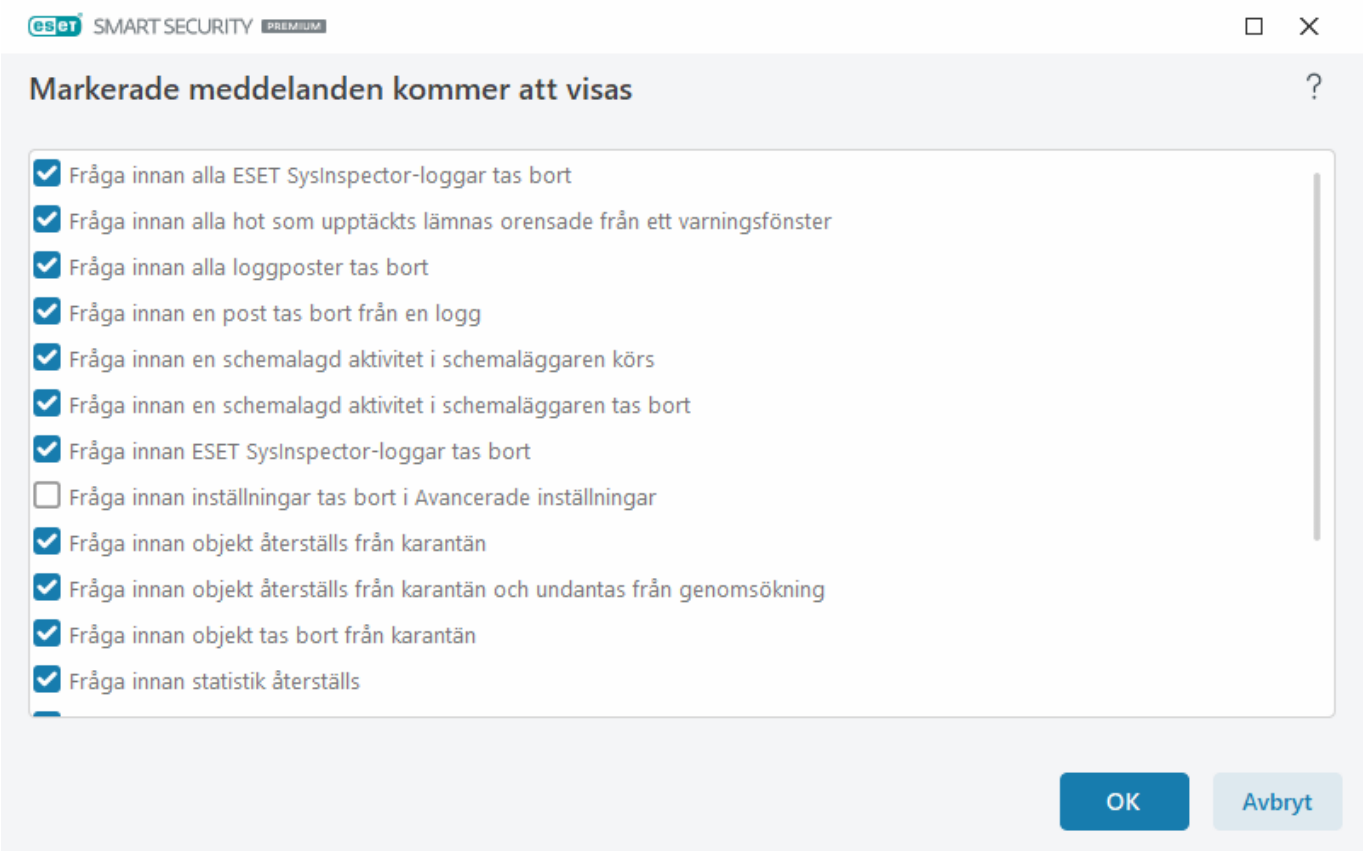
Visningstid i sekunder – anger hur länge meddelanden ska synas. Värdet måste vara mellan 10-999 sekunder.

Bekräftelsemeddelanden – klicka på **Redigera** för att visa en lista med bekräftelsemeddelanden som du kan välja

att visa eller inte visa.

Bekräftelsemeddelande

Justera bekräftelsemeddelanden genom att navigera till Avancerade inställningar > **Meddelanden** > **Interaktiva aviseringar** och klicka på **Redigera** bredvid **Bekräftelsemeddelanden**.



I den här dialogrutan visas bekräftelsemeddelanden som ESET Smart Security Premium visar innan en åtgärd utförs. Markera eller avmarkera kryssrutan intill varje bekräftelsemeddelande för att aktivera eller inaktivera det.

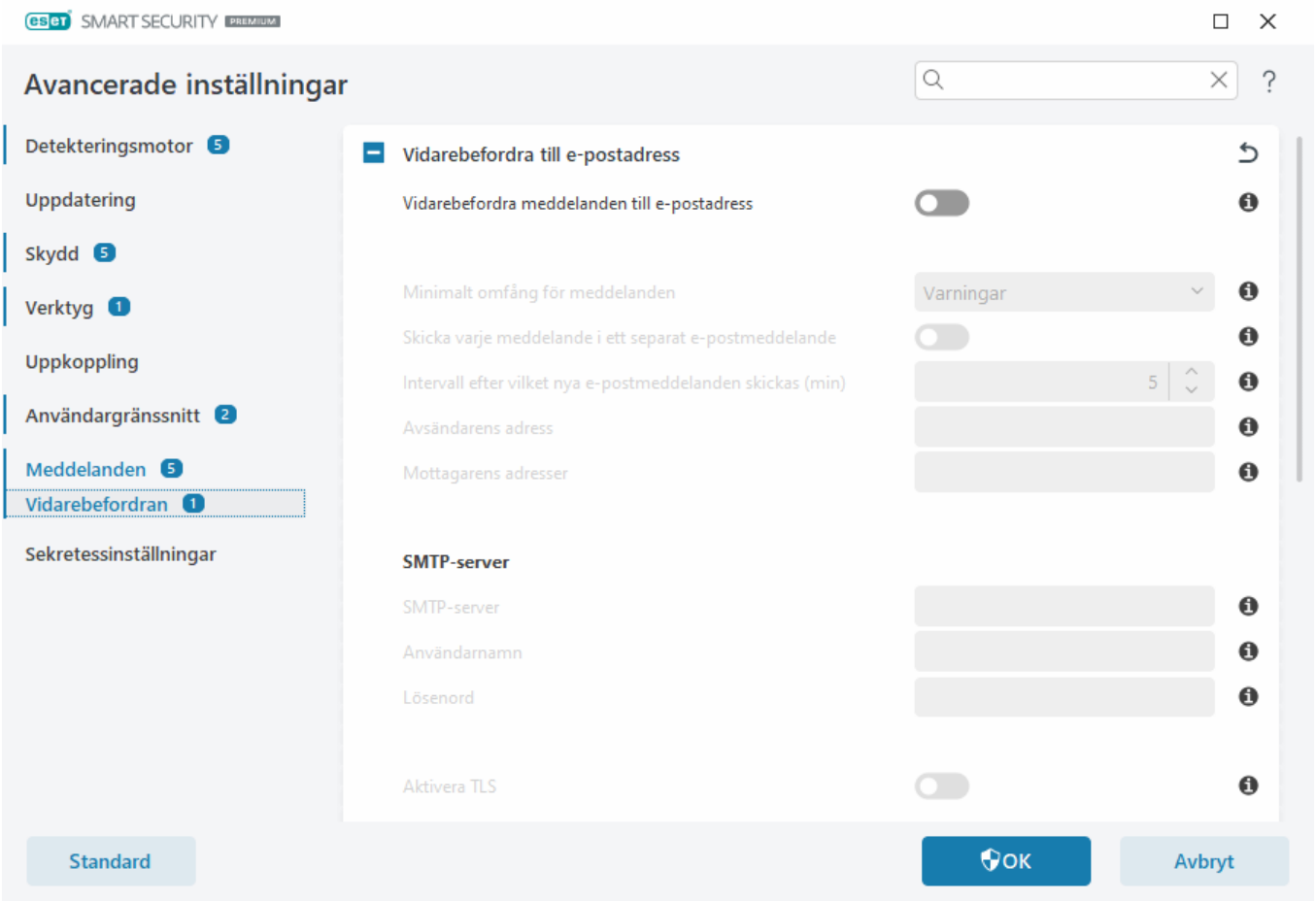
Läs mer om specifika funktioner relaterade till bekräftelsemeddelanden:

- Fråga innan ESET SysInspector-loggar tas bort
- Fråga innan alla ESET SysInspector-loggar tas bort
- Fråga innan objekt tas bort från karantän
- Fråga innan inställningar tas bort i Avancerade inställningar
- Fråga innan alla hot som upptäckts lämnas orensade från ett varningsfönster
- Fråga innan en post tas bort från en logg
- Fråga innan en schemalagd aktivitet i schemaläggaren tas bort
- Fråga innan alla loggposter tas bort
- Fråga innan statistik återställs

- Fråga innan objekt återställs från karantän
- Fråga innan objekt återställs från karantän och undantas från genomsökning
- Fråga innan en schemalagd aktivitet i schemaläggaren körs
- Visa meddelanden om bearbetningsresultat för spamskydd
- Visa meddelanden om bearbetningsresultat för spamskydd för e-postklienter
- Visa dialogrutor om produktbekräftelse för Outlook Express- och Windows Mail-e-postklienter
- Visa dialogrutor om produktbekräftelse för Windows Live Mail
- Visa dialogrutor om produktbekräftelse för Outlook-e-postklienten

Vidarebefordran

ESET Smart Security Premium kan skicka meddelanden via e-post automatiskt om en händelse med vald omfångsnivå inträffar. Öppna Avancerade inställningar > **Meddelanden** > **Vidarebefordra** och aktivera **Vidarebefordra meddelanden till e-postadress** för att aktivera e-postmeddelanden.



I listrutan **Minimalt omfång för meddelanden** kan du välja från vilken allvarlighetsnivå meddelanden ska skickas.

- **Diagnostik** – loggar information som behövs för att fininställa programmet och alla poster ovan.

- **Information** – loggar alla informationsmeddelanden, exempelvis ovanliga nätverkshändelser, inklusive framgångsrika uppdateringar och alla poster ovan.
- **Varningar** – registrerar kritiska fel och varningsmeddelanden (till exempel misslyckad uppdatering).
- **Fel** – fel (dokumentskyddet startades inte) och kritiska fel registreras.
- **Kritisk** – loggar endast kritiska fel (till exempel fel vid start av antivirusskyddet eller om hot hittades).

Skicka varje meddelande i ett separat e-postmeddelande – när det här alternativet aktiveras får mottagaren ett nytt e-postmeddelande för varje enskilt meddelande. Det kan resultera i att många e-postmeddelanden tas emot på kort tid.

Intervall efter vilket nya e-postmeddelanden skickas (min) – intervall i minuter efter vilket nya meddelanden skickas till e-postadressen. Om värdet ställs in till 0 skickas meddelandena omedelbart.

Avsändarens adress – här anger du avsändaradressen som visas i huvudet på meddelanden som går via e-post.

Mottagaradresser – här anger du mottagaradresserna som ska visas i huvudet på meddelanden via e-post. Flera värden stöds. Använd semikolon som avgränsare.

SMTP-server

SMTP-server – SMTPS-servern används för att skicka meddelanden (till exempel smtp.provider.com:587, fördefinierad port är 25).

> SMTP-servrar med TLS-kryptering stöds av ESET Smart Security Premium.

Användarnamn och **lösenord** – om autentisering krävs för SMTP-servern ska dessa fält fyllas i med ett giltigt användarnamn och lösenord som ger åtkomst till SMTP-servern.

Aktivera TLS – Secure Alert och meddelanden med TLS-kryptering.

Testa SMTP-anslutning – en test-e-postmeddelande skickas till mottagarens e-postadress. SMTP-server, användarnamn, lösenord, avsändarens adress och mottagarens adress behöver anges.

Meddelandeformat

Kommunikation mellan programmet och en fjärranvändare eller systemadministratör sker via e-post eller LAN-meddelanden (med Windows meddelandetjänst). **Standardformatet för varningsmeddelanden och meddelanden** passar de flesta situationer. Under vissa omständigheter kan du behöva ändra meddelandeformatet för händelsemeddelanden.

Format för händelsemeddelanden – format för händelsemeddelanden som visas på fjärrdatorer.

Format för meddelanden med varning om hot – varningar och meddelanden om hot har ett fördefinierat standardformat. Vi rekommenderar att du behåller det fördefinierade formatet. Under vissa omständigheter (om du exempelvis har ett automatiskt e-postbehandlingssystem) kan du dock behöva ändra meddelandeformatet.

Teckenuppsättning – konverterar ett e-postmeddelande till ANSI-teckenuppsättning baserat på Windows nationella inställningar (till exempel windows-1250, Unicode (UTF-8), ACSII 7-bit eller japanska (ISO-2022-JP)).

Därför ändras "á" till "a" och en okänd symbol till "?".

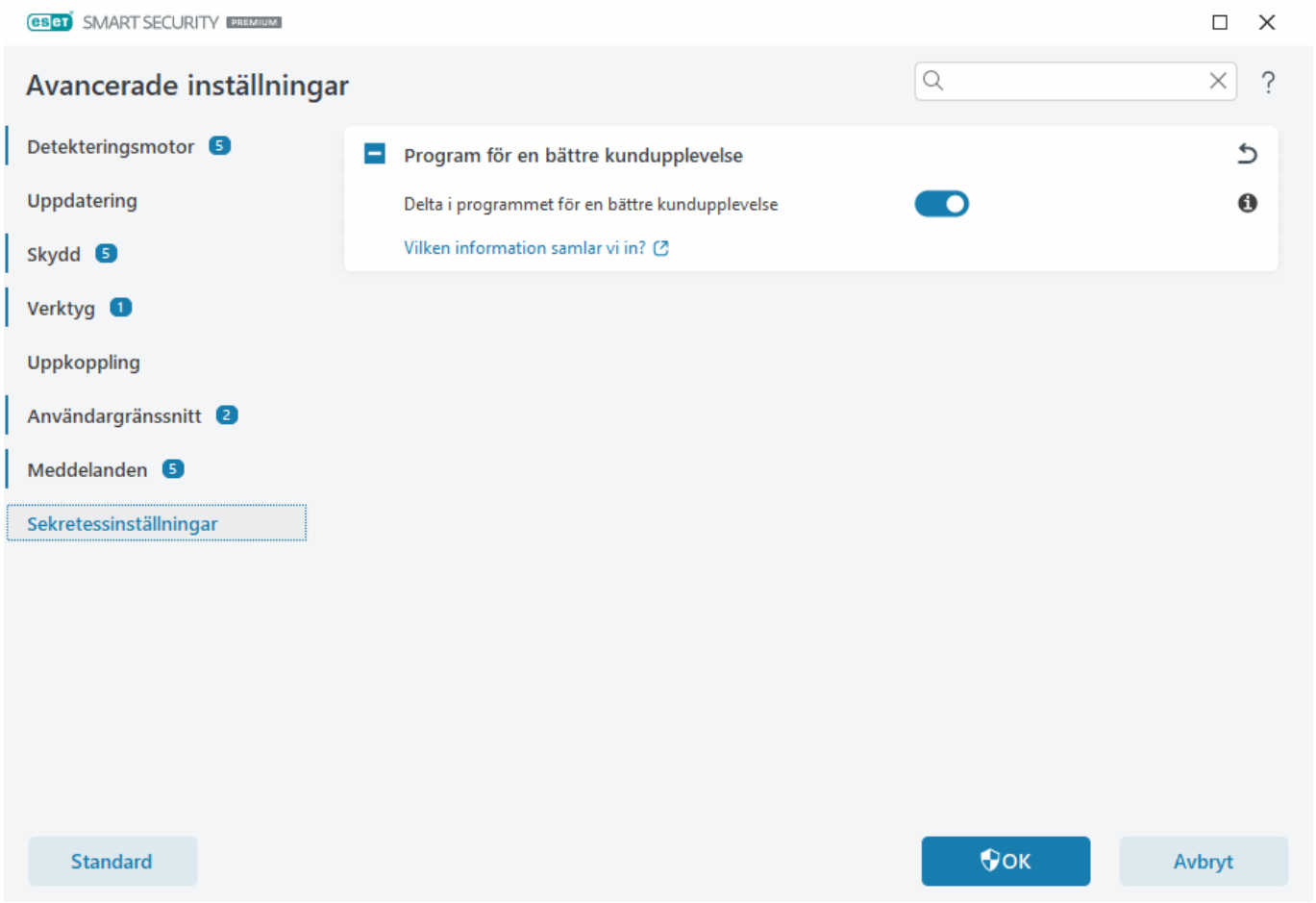
Använd QP-kodning – e-postmeddelandets källa kodas till formatet Quoted printable (QP) som använder ASCII-tecken och överför särskilda tecken med e-post i 8-bitarsformat (ááíóú) korrekt.

- **%TimeStamp%** – datum och tid för händelsen
- **%Scanner%** – berörd modul
- **%ComputerName%** – namnet på den dator där varningen utlöstes
- **%ProgramName%** – programmet som genererade varningen
- **%InfectedObject%** – namn på den infekterade filen, meddelande osv.
- **%VirusName%** – identifiering av infektionen
- **%Action%** – åtgärd vidtagen mot infiltreringen
- **%ErrorDescription%** – beskrivning av en icke-virushändelse

Nyckelorden **%InfectedObject%** och **%VirusName%** används bara i hotvarningsmeddelnaden och **%ErrorDescription%** används i händelsemeddelanden.

Sekretessinställningar

Öppna Avancerade inställningar > **Sekretessinställningar**.



Program för en bättre kundupplevelse

Aktivera växlingsknappen bredvid **Delta i programmet för en bättre kundupplevelse** för att gå med i programmet för en bättre kundupplevelse. Genom att gå med förser du ESET med anonym information om användningen av ESET-produkter. De insamlade uppgifterna hjälper oss att förbättra din upplevelse och kommer aldrig att delas med tredje part. Vilken information samlar vi in?

Återställa till standardinställningar

Klicka på **Standard** i Avancerade inställningar för att återställa alla programinställningar för alla moduler. Modulerna återställs till den status de skulle ha haft efter en ny installation.

Se även Importera och exportera inställningar.

Återställa alla inställningar i det aktuella avsnittet

Klicka på den böjda pilen om du vill återställa alla inställningar i det aktuella avsnittet till de standardinställningar som har angetts av ESET.

Observera att eventuella ändringar du har gjort går förlorade när du klickar på **Återställ till standard**.

Återställ innehållet i tabellerna – när det här alternativet aktiveras går de aktiviteter eller profiler som lagts till manuellt eller automatiskt förlorade.

Se även Importera och exportera inställningar.

Fel när konfigurationen skulle sparas

Det här felmeddelandet anger att inställningarna inte sparades korrekt på grund av ett fel.

Detta innebär vanligen att användaren som försökte ändra programparametrarna:

- har otillräcklig åtkomstbehörighet eller saknar de nödvändiga operativsystemsbehörigheter som krävs för att ändra konfigurationsfiler och systemregister.
  > För att kunna utföra önskade ändringar måste systemadministratören logga in.

- nyligen har aktiverat Inlärningsläge i HIPS eller brandväggen och försökt göra ändringar i Avancerade inställningar.
  > För att spara konfigurationen och undvika konfigurationskonflikten stänger du Avancerade inställningar utan att spara och försöker att göra önskade ändringar igen.

Det näst vanligaste fallet är att programmet inte längre fungerar normalt, är skadat och därför måste startas om.

Kommandoradsskanner

Det går att starta antivirusmodulen i ESET Smart Security Premium via kommandoraden, antingen manuellt (med kommandot ecls) eller med en kommandofil (.bat).

Användning av ESET-kommandoradsskanner:

```
ecls [OPTIONS..] FILES..
```

Det går att använda följande parametrar och växlar när genomsökning körs från kommandoraden:

Alternativ

/base-dir=MAPP	läs in moduler från MAPP
/quar-dir=MAPP	karantän-MAPP
/exclude=MASK	undanta filer från genomsökning som matchar MASK
/subdir	genomsök undermappar (standard)
/no-subdir	genomsök inte undermappar
/max-subdir-level=NIVÅ	maximal undernivå för mappar inom mappar som ska genomsökas
/symlink	följ symboliska länkar (standard)
/no-symlink	hoppa över symboliska länkar
/ads	genomsök ADS (standard)
/no-ads	genomsök inte ADS
/log-file=FIL	logga utdata till FIL
/log-rewrite	skriv över utdatafilen (standard – lägg till)
/log-console	logga utdata till konsol (standard)
/no-log-console	logga inte utdata till konsol

/log-all	logga även rena filer
/no-log-all	logga inte rena filer (standard)
/aind	visa aktivitetsindikator
/auto	skanna och rensa alla lokala diskar automatiskt

Skanneralternativ

/files	genomsök filer (standard)
/no-files	genomsök inte filer
/memory	skanna minne
/boots	genomsök startsektorer
/no-boots	genomsök inte startsektorer (standard)
/arch	genomsök arkiv (standard)
/no-arch	genomsök inte arkiv
/max-obj-size=STORLEK	genomsök endast filer som är mindre än STORLEK megabyte (standard 0 = obegränsad)
/max-arch-level=NIVÅ	maximal undernivå för arkiv inom arkiv (kapslade arkiv) som ska genomsökas
/scan-timeout=GRÄNS	genomsök arkiv i max GRÄNS sekunder
/max-arch-size=STORLEK	genomsök endast filerna i ett arkiv om de är mindre än STORLEK (standard 0 = obegränsad)
/max-sfx-size=STORLEK	genomsök endast filerna i ett självuppackande arkiv om de är mindre än STORLEK megabyte (standard 0 = obegränsad)
/mail	genomsök e-postfiler (standard)
/no-mail	genomsök inte e-postfiler
/mailbox	genomsök brevlådor (standard)
/no-mailbox	genomsök inte brevlådor
/sfx	genomsök självuppackande arkiv (standard)
/no-sfx	genomsök inte självuppackande arkiv
/rtp	genomsök internt packade filer (standard)
/no-rtp	genomsök inte internt packade filer
/unsafe	sök efter potentiellt farliga program
/no-unsafe	sök inte efter potentiellt farliga program (standard)
/unwanted	sök efter potentiellt oönskade program
/no-unwanted	sök inte efter potentiellt oönskade program (standard)
/suspicious	genomsök efter misstänkta program (standard)
/no-suspicious	genomsök inte efter misstänkta program
/pattern	använd signaturer (standard)
/no-pattern	använd inte signaturer
/heur	aktivera heuristik (standard)
/no-heur	inaktivera heuristik
/adv-heur	aktivera Avancerad heuristik (standard)

/no-adv-heur	inaktivera Avancerad heuristik
/ext-exclude=TILLÄGG	undanta FILTILLÄGG avgränsade med kolon från genomsökning
/clean-mode=LÄGE	använd LÄGE för rensning av infekterade objekt Följande alternativ finns tillgängliga: • `none` (standard) – Ingen automatisk rensning sker. • `standard` – ecls.exe försöker rensa eller ta bort infekterade filer automatiskt. • `strikt` – ecls.exe försöker rensa eller ta bort infekterade filer automatiskt utan att du behöver göra något (du meddelas inte innan filer tas bort). • `utförlig` – ecls.exe försöker ta bort filer utan att rensa dem oavsett vad det är för fil. • `ta bort` – ecls.exe försöker ta bort filer utan att rensa dem, men undviker att ta bort känsliga filer som Windows-systemfiler.
/quarantine	kopiera infekterade filer (om rensade) till karantän (kompletterar åtgärden som utförs vid rensning)
/no-quarantine	kopiera inte infekterade filer till karantän

Allmänna alternativ

/help	visa hjälp och avsluta
/version	visa versionsinformation och avsluta
/preserve-time	bevara tidsstämpeln för senaste åtkomst

Slutkoder

0	inga hot upptäcktes
1	hot upptäcktes och rensades
10	det gick inte att genomsöka en del filer (kan vara hot)
50	hot upptäckt
100	fel

Slutkoder som överskrider 100 betyder att filen inte har genomsökts och därför kan vara infekterad.

FAQ

Nedan hittar du en del ofta förekommande frågor och problem som uppkommer. Klicka på en ämnesrubrik om du vill få information om hur du kan lösa ett problem:

- Hur man uppdaterar ESET Smart Security Premium
- ESET Smart Security Premium har upptäckt ett hot
- Ta bort ett virus från datorn
- Tillåta kommunikation för ett visst program
- Aktivera Föräldrakontroll för ett konto

- Skapa en ny aktivitet i Schemaläggare
- Schemalägga en genomsökningsaktivitet (veckovis)
- Låsa upp avancerade inställningar
- Så här löser du produktinaktivering från ESET HOME

Om problemet inte finns med i listan ovan kan du leta i ESET Smart Security Premium-onlinehjälpen.

Om du inte hittar lösningen på problemet/frågan i ESET Smart Security Premium-onlinehjälpen kan du besöka ESET:s kunskapsbas som uppdateras regelbundet. Nedan finns länkar till de mest populära artiklarna i vår kunskapsbas:

- Hur förnyar jag mitt abonnemang?
- Jag fick ett meddelande om ett aktiveringsfel när jag installerade min ESET-produkt. Vad betyder det?
- Aktivera min Windows-hemprodukt från ESET med hjälp av aktiveringsnyckeln
- Avinstallera eller återinstallera min ESET-hemprodukt
- Jag får ett meddelande om att min ESET-installation avslutats för tidigt
- Vad måste jag göra när jag har förnyat abonnemanget? (Hemanvändare)
- Vad händer om jag ändrar e-postadress?
- Överföra min ESET-produkt till en ny dator eller enhet
- Starta Windows i Felsäkert läge eller Felsäkert läge med nätverk
- Exkludera en säker webbplats från att blockeras
- Tillåt åtkomst för skärmläsares programvara till ESET-gränssnittet

Vid behov är du välkommen att kontakta vår tekniska support med frågor eller problem.

Hur man uppdaterar ESET Smart Security Premium

Det går att uppdatera ESET Smart Security Premium manuellt eller automatiskt. Starta uppdateringen genom att klicka på **Uppdatera** i programmets huvudfönster och klicka sedan på **Leta efter uppdateringar**.

Standardinstallationens inställningar skapar en automatisk uppdateringsaktivitet som utförs en gång i timmen. Gå till **Verktyg** > Schemaläggaren om du vill ändra intervallet.

Ta bort ett virus från datorn

Om datorn visar symptom på att ha blivit infekterad av skadlig programvara, t.ex. om den har blivit långsammare eller ofta låser sig, rekommenderar vi att du gör följande:

1. Klicka på **Genomsökning av datorn** i programmets huvudfönster.

2. Klicka på **Genomsök datorn** för att genomsöka systemet.

3. När genomsökningen har slutförts visas antalet genomsökta, infekterade och rensade filer i loggen.

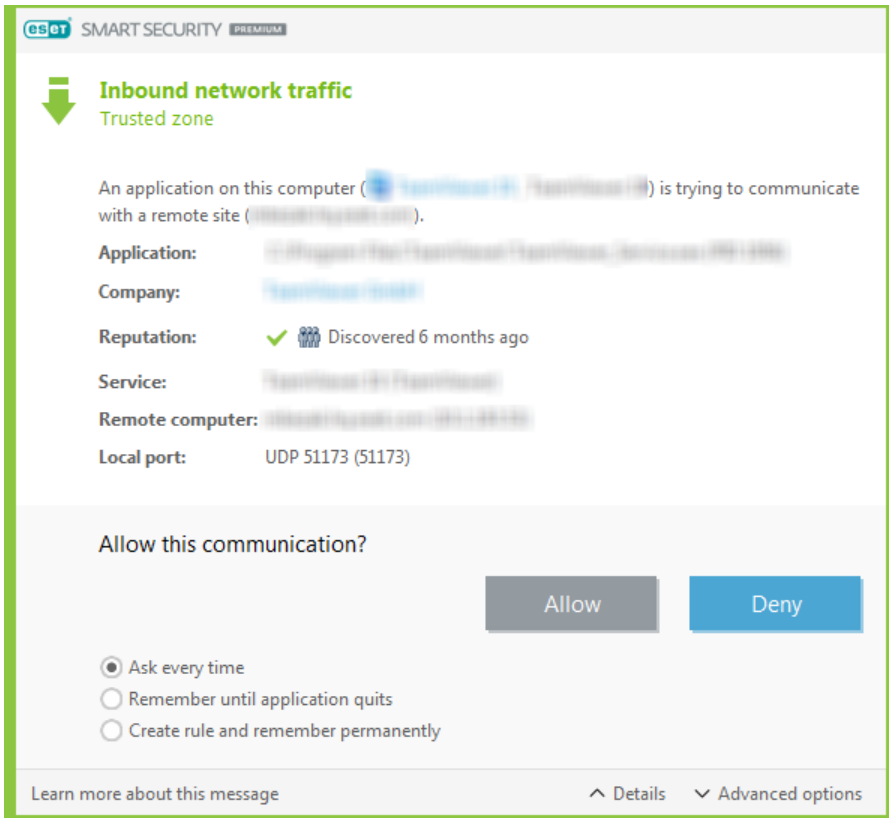
4. Om du endast vill genomsöka en viss del av disken klickar du på **Anpassad genomsökning** och väljer mål som ska genomsökas efter virus.

Mer information hittar du i:

- artikeln i ESET:s kunskapsbas
- Karantän

Tillåta kommunikation för ett visst program

Om en ny anslutning identifieras i interaktivt läge och det inte finns någon regel för den, ombeds du att **tillåta** eller **avvisa** anslutningen. Markera kryssrutan **Skapa regel och kom ihåg permanent** om du vill utföra samma åtgärd varje gång ESET Smart Security Premium försöker upprätta anslutningen.



Du kan skapa nya brandväggsregler för program innan de upptäcks av ESET Smart Security Premium i fönstret för brandväggsinställningar. Öppna huvudprogramfönstret > **Inställningar** > **Nätverksskydd** > klicka på ⚙ bredvid **Brandvägg** > **Konfigurera** > **Avancerat** > **Regler** > **Redigera**.

Klicka på knappen **Lägg till** och ange namn, riktning och kommunikationsprotokoll för regeln på fliken **Allmänt**. Det går att ställa in vilken åtgärd som ska utföras när regeln används.

Ange sökvägen till programmets körbara fil och den lokala kommunikationsporten på fliken **Lokal**. Klicka på fliken

Fjärrpunkt för att ange fjärradress och -port (om tillämpligt). Den nya regeln används när programmet försöker kommunicera igen.

Aktivera Föräldrakontroll för ett konto

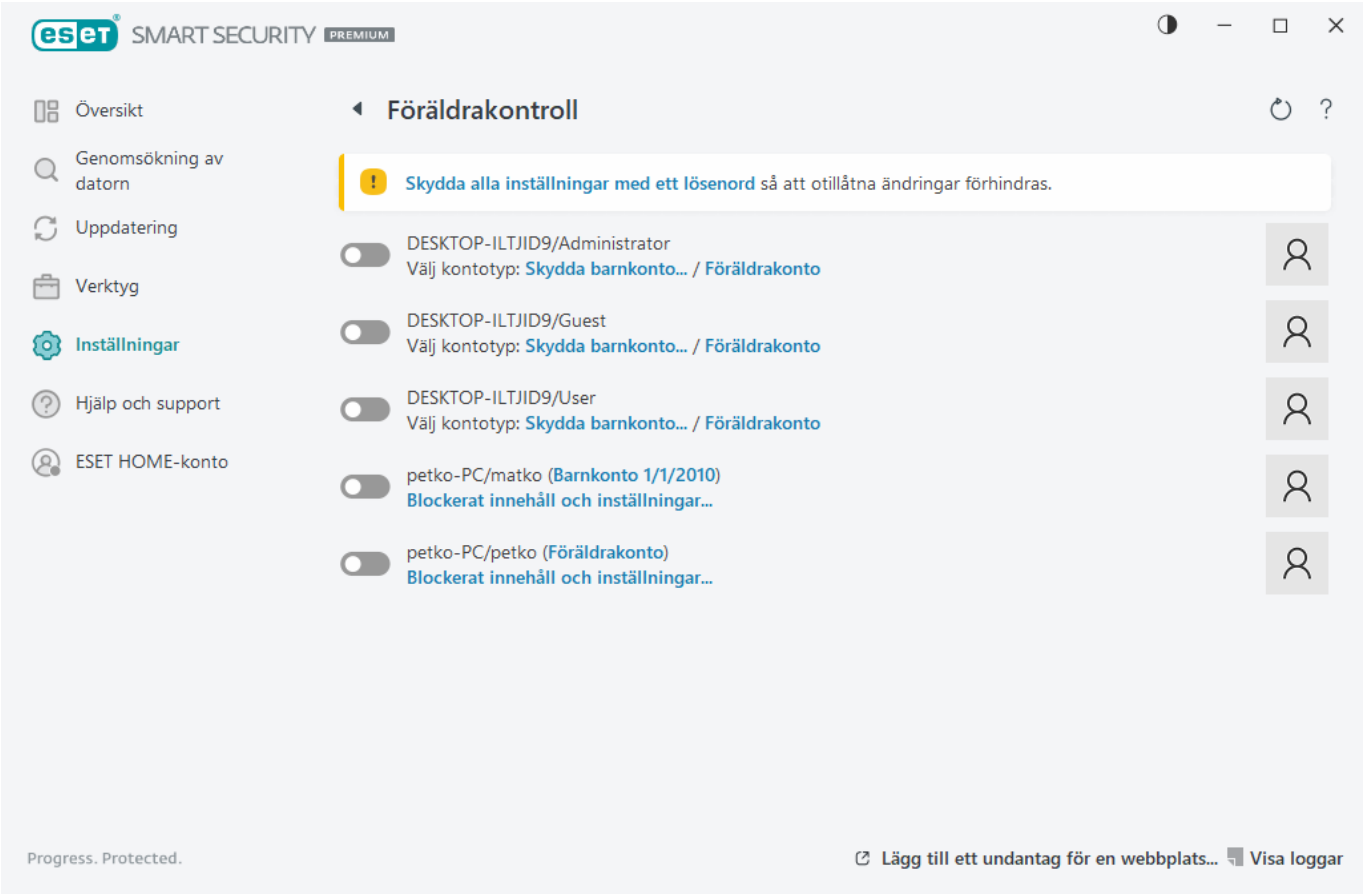
Aktivera Föräldrakontroll för ett visst användarkonto genom att följa stegen nedan:

1. Föräldrakontroll är inaktiverad som standard i ESET Smart Security Premium. Det finns två sätt att aktivera föräldrakontroll:

   • Klicka på växlingsikonen i **Inställningar** > **Internetskydd** > **Föräldrakontroll** från programmets huvudfönster och ändra statusen för Föräldrakontroll till aktiverad.

   • Öppna Avancerade inställningar > **Skydd** > **Webbåtkomstskydd** > **Föräldrakontroll** och aktivera sedan växlingsknappen bredvid **Aktivera föräldrakontroll**.

2. Klicka på **Inställningar** > **Internetskydd** > **Föräldrakontroll** i programmets huvudfönster. Även om **Aktiverad** visas intill **Föräldrakontroll**, måste du konfigurera föräldrakontrollen för önskat konto genom att klicka på pilsymbolen och i nästa fönster sedan välja **Skydda barnkonto** eller **Föräldrakonto**. I nästa fönster anger du födelsedatum för att avgöra nivån för åtkomst och rekommenderad ålder enligt webbsidorna. Föräldrakontroll aktiveras nu för det angivna användarkontot. Klicka på **Blockerat innehåll och inställningar...** under ett kontonamn för att anpassa kategorier du vill tillåta eller blockera på fliken Kategorier. Tillåt eller blockera anpassade webbsidor som inte passar in i en kategori genom att klicka på fliken Undantag.



Skapa en ny aktivitet i Schemaläggare

Skapa en ny aktivitet i **Verktyg** > **Schemaläggaren** genom att klicka på **Lägg till aktivitet** eller högerklicka på kontextmenyn och välj **Lägg till**. Det finns fem typer av schemalagda aktiviteter:

- **Kör externt program** – schemalägger körning av ett extern program.
- **Underhåll av loggning** – loggfiler innehåller även rester från borttagna poster. Denna aktivitet optimerar regelbundet posterna i loggfiler för effektiv funktion.
- **Kontroll av filer som startas automatiskt** – kontrollerar filer som tillåts köra vid systemstart eller inloggning.
- **Skapa en avbildning av datorns status** – skapar en avbildning av datorn i ESET SysInspector – samlar detaljerad information om systemkomponenter (t.ex. drivrutiner och program) och utvärderar risknivån för varje komponent.
- **Genomsökning av datorn på begäran** – utför genomsökning av filer och mappar på datorn.
- **Uppdatering** – schemalägger en uppdateringsaktivitet genom att uppdatera modulerna.

Eftersom **Uppdatering** är en av de schemalagda aktiviteter som används oftast förklarar vi hur du skapar en ny uppdateringsaktivitet.

Välj **Uppdatera** från rullgardinsmenyn **Schemalagd aktivitet**. Ange aktivitetens namn i fältet **Aktivitetsnamn** och klicka på **Nästa**. Välj hur ofta aktiviteten ska utföras. Följande alternativ finns tillgängliga: **En gång**, **Flera gånger**, **Dagligen**, **Varje vecka** och **Händelseutlöst**. Välj **Hoppa över aktivitet när datorn körs på batteri** för att minimera systemresurserna när datorns körs på batteri. Aktiviteten körs vid det datum och den tidpunkt som angetts i fältet **Utförande av aktivitet**. Definiera sedan åtgärden som vidtas om aktiviteten inte kan genomföras eller slutföras den schemalagda tiden. Följande alternativ finns tillgängliga:

- **Vid nästa schemalagda tid**
- **Så snart som möjligt**
- **Omedelbart om tiden sedan senaste körning överskrider angivet värde** (intervallet kan anges i rullningsrutan **Tid sedan senaste körning (timmar)**)

I nästa steg visas ett översiktsfönster med information om den aktuella schemalagda aktiviteten. Klicka på **Slutför** när du är klar med ändringarna.

En dialogruta öppnas där användaren kan välja vilka profiler som ska användas för den schemalagda aktiviteten. Här kan du välja primär och alternativ profil. Den alternativa profilen används om aktiviteten inte kan slutföras med den primära profilen. Den nya schemalagda aktiviteten läggs till i listan över aktuella schemalagda aktiviteter när du klickar på **Slutför**.

Schemalägga en veckovis genomsökning av datorn

Schemalägg en regelbunden aktivitet genom att öppna programmets huvudfönster och klicka på **Verktyg** > **Schemaläggare**. Nedan finns en kort guide om att schemalägga en aktivitet som startar en genomsökning av

lokala diskar varje vecka. Se vår artikel i kunskapsbasen för mer detaljerade instruktioner.

Schemalägga en aktivitet:

1. Klicka på **Lägg till** i huvudskärmen i Schemaläggare.

2. Ange ett namn på uppgiften och välj **Genomsökning av datorn på begäran** på den nedrullningsbara menyn **Typ av aktivitet**.

3. Välj **Veckovis** som aktivitetsfrekvens.

4. Ange dag och tidpunkt som aktiviteten ska utföras.

5. Välj **Kör aktiviteten så snart som möjligt** för att utföra aktiviteten senare om den av någon anledning inte startades (exempelvis om datorn var avstängd).

6. Granska sammanfattningen av den schemalagda aktiviteten och klicka på **Slutför**.

7. Välj **Lokala enheter** på rullgardinsmenyn **Målobjekt**.

8. Klicka på **Slutför** om du vill använda aktiviteten.

Låsa upp de lösenordsskyddade avancerade inställningarna

När du vill komma åt de skyddade avancerade inställningarna visas fönstret för att ange lösenordet. Om du har glömt eller blivit av med lösenordet klickar du på **Återställ lösenord** och anger den e-postadress som användes när abonnemanget registrerades. ESET skickar ett e-postmeddelande med verifieringskoden. Ange verifieringskoden och skriv sedan och bekräfta det nya lösenordet. Verifieringskoden är giltig i sju dagar.

Återställ lösenord via ditt ESET HOME-konto – Använd det här alternativet om abonnemanget som används för aktivering är kopplat till ditt ESET HOME-konto. Skriv den e-postadress du använder för att logga in på ditt ESET HOME-konto.

Om du inte kommer ihåg din e-postadress eller har problem med att återställa lösenordet klickar du på **Kontakta teknisk support**. Du omdirigeras till ESET:s webbplats för att kontakta vår tekniska supportavdelning.

Generera kod för teknisk support – Det här alternativet genererar koden som du uppger till teknisk support. Kopiera koden från teknisk support och klicka på **Jag har en verifieringskod**. Ange verifieringskoden och ange och bekräfta sedan det nya lösenordet. Verifieringskoden är giltig i sju dagar.

Mer information finns i Lås upp lösenordet för dina inställningar i ESET Windows-hemprodukter.

Så här löser du produktinaktivering från ESET HOME

Produkten inte aktiverad

Det här felmeddelandet visas när abonnemangsägaren inaktiverar ditt ESET Smart Security Premium från ESET HOME-portalen eller om abonnemanget som delas med ditt ESET HOME-konto inte längre delas. Så här löser du

problemet:

- Klicka på **Aktivera** och använd någon av aktiveringsmetoderna för att aktivera ESET Smart Security Premium.

- Kontakta abonnemangsägaren med information om att ditt ESET Smart Security Premium har inaktiverats av abonnemangsägaren eller att abonnemanget inte längre delas med dig. Ägaren kan lösa problemet i ESET HOME.

Produkten har avaktiverats, enheten har frånkopplats

Det här felmeddelandet visas när du har tagit bort en enhet från ESET HOME-konto. Så här löser du problemet:

- Klicka på **Aktivera** och använd någon av aktiveringsmetoderna för att aktivera ESET Smart Security Premium.

- Kontakta abonnemangsägaren och tala om att ESET Smart Security Premium som du använder har inaktiverats och att enheten har kopplats bort från ESET HOME.

- Om du är abonnemangsägare och inte känner till dessa ändringar ska du granska ESET HOME-aktivitetsfeeden. Om du hittar någon misstänkt aktivitet ändrar du ditt ESET HOME-kontolösenord och kontaktar ESET:s tekniska support.

Produkten har avaktiverats, enheten har frånkopplats

Det här felmeddelandet visas när du har tagit bort en enhet från ESET HOME-konto. Så här löser du problemet:

- Klicka på **Aktivera** och använd någon av aktiveringsmetoderna för att aktivera ESET Smart Security Premium.

- Kontakta abonnemangsägaren och tala om att ESET Smart Security Premium som du använder har inaktiverats och att enheten har kopplats bort från ESET HOME.

- Om du är abonnemangsägare och inte känner till dessa ändringar ska du granska ESET HOME-aktivitetsfeeden. Om du hittar någon misstänkt aktivitet ändrar du ditt ESET HOME-kontolösenord och kontaktar ESET:s tekniska support.

Produkten inte aktiverad

Det här felmeddelandet visas när abonnemangsägaren inaktiverar ditt ESET Smart Security Premium från ESET HOME-portalen eller om abonnemanget som delas med ditt ESET HOME-konto inte längre delas. Så här löser du problemet:

- Klicka på **Aktivera** och använd någon av aktiveringsmetoderna för att aktivera ESET Smart Security Premium.

- Kontakta abonnemangsägaren med information om att ditt ESET Smart Security Premium har inaktiverats av abonnemangsägaren eller att abonnemanget inte längre delas med dig. Ägaren kan lösa problemet i ESET HOME.

0

Program för en bättre kundupplevelse

Om du går med i programmet för en bättre kundupplevelse förser du ESET med anonym information gällande användningen av våra produkter. Mer information om databehandling hittar du i vår sekretesspolicy.

Ditt samtycke

Det är frivilligt att delta i programmet är frivilligt och bygger på ditt samtycke. När du har gått med deltar du passivt, vilket innebär att du inte behöver göra något mer. Du kan ta tillbaka samtycket när som helst genom att ändra produktinställningarna. Om du gör det förhindras vidare bearbetning av dina anonyma data.

Du kan när som helst återkalla ditt samtycke genom att ändra produktinställningarna:

- Ändra inställningarna för programmet för en bättre kundupplevelse i ESET:s Windows-hemprodukter

Vilka typer av information samlar vi in?

Data om interaktion med produkten

Den här informationen säger oss mer om hur våra produkter används. Tack vare den vet vi till exempel vilka funktioner som används ofta, vilka inställningar användare ändrar och hur mycket tid de ägnar åt att använda produkten.

Data om enheter

Vi samlar in den här informationen för att förstå var och på vilka enheter våra produkter används. Typiska exempel är enhetsmodell, land, version och operativsystemets namn.

Data om feldiagnostik

Information om fel- och kraschsituationer samlas också in. Det kan till exempel vara vilket fel som har inträffat och vilka åtgärder som ledde fram till det.

Varför samlar vi in den här informationen?

Den här anonyma informationen gör det möjligt att förbättra våra produkter för dig, användaren. Den hjälper oss att göra dem så relevanta, lättanvända och felfria som möjligt.

Vem har kontroll över den här informationen?

ESET, spol. s r.o. är ensam registeransvarig för data som samlas in i programmet. Informationen delas inte med tredje part.

Licensavtal för slutanvändare

Gäller från den 19 oktober 2021.

VIKTIGT! Innan du hämtar, installerar, kopierar eller använder produkten bör du läsa igenom villkoren nedan. **GENOM ATT HÄMTA, INSTALLERA, KOPIERA ELLER ANVÄNDA PROGRAMMET, GODKÄNNER DU DESSA VILLKOR SAMT BEKRÄFTAR SEKRETESSPOLICY.**

Slutanvändaravtalet

Enligt detta Licensavtal för slutanvändare (”Avtalet”) som gäller mellan ESET, spol. s r. o., med adress Einsteinova 24, 85101 Bratislava, Slovak Republic, och som registrerats i handelsregistret hos regiondomstolen Bratislava I. avdelning Sro, diarienummer 3586/B, BIN: 31333532 (”ESET” eller ”Leverantören”) och dig, en fysisk person eller juridisk person (”du” eller ”Slutanvändaren”), har du rätt att använda programvaran enligt paragraf 1 i detta Avtal. Den programvara som definierats i paragraf 1 i Avtalet kan lagras på en datalagringsenhet, skickas via e-post, hämtas från Internet, hämtas från Leverantörens servrar eller erhållas på annat sätt enligt de villkor som anges nedan.

DETTA ÄR ETT AVTAL GÄLLANDE SLUTANVÄNDARENS RÄTTIGHETER OCH INTE ETT KÖPEKONTRAKT. Leverantören förblir ägare av programvaran och det eventuella fysiska medium, på vilket Programvaran säljs samt alla de kopior av programvaran som Slutanvändaren har rätt att göra enligt detta Avtal.

Genom att klicka på alternativet ”Jag godkänner” eller ”Jag godkänner…” under installation, hämtning, kopiering eller användning av programvaran, godkänner du villkoren i detta Avtal och samtycker till Sekretesspolicyn. Om du inte godkänner alla villkor i detta Avtal och/eller Sekretesspolicyn, klicka omgående på alternativet ”Stäng”, avbryt installationen eller hämtningen, eller förstör eller returnera Programvaran, installationsmediet, medföljande dokumentation och försäljningskvitto till Leverantören eller återförsäljaren där du införskaffade Programvaran.

DU ÄR MEDVETEN OM ATT DU GENOM DIN ANVÄNDNING AV PROGRAMVARAN MEDGER ATT DU HAR LÄST DETTA AVTAL, ATT DU FÖRSTÅTT DET OCH GODKÄNNER OCH ÄR BUNDEN TILL DESS VILLKOR.

1. **Programvara**. Så som det används i det här Avtalet avser begreppet ”Programvara”: (i) datorprogrammet och alla dess komponenter; (ii) allt innehåll på skivor, cd-skivor, dvd-skivor, e-postmeddelanden med eventuella bilagor eller annat medium som omfattas av detta Avtal, inklusive Programvaran i form av objektkod på datalagringsenheter, via e-post eller hämtad på internet; (iii) eventuellt relaterat förklarande skriftligt material och eventuell annan dokumentation för Programvaran, framförallt eventuell beskrivning av Programvaran, dess specifikationer, eventuell beskrivning av Programvarans egenskaper eller drift, eventuell beskrivning av driftmiljön i vilken Programvaran används, anvisningar för användning eller installation av Programvaran eller eventuell beskrivning av hur Programvaran ska användas ("Dokumentationen"); (iv) kopior av Programvaran, eventuella felkorrigeringar, tillägg eller utökningar av Programvaran, modifierade versioner av Programvaran samt alla eventuella uppgraderingar av Programvarans olika komponenter, som Leverantören licensierar till dig enligt paragraf 3 i detta Avtal. Programvaran tillhandahålls exklusivt i form av exekverbar objektkod.

2. **Installation, Dator och en Licensnyckel**. Programvara som levereras på en datalagringsenhet, skickas via e-post, hämtas från Internet, hämtas från Leverantörens servrar eller erhålls på annat sätt från andra källor kräver installation. Programvaran måste installeras på en korrekt konfigurerad Dator som minst uppfyller de systemkrav som beskrivs i Dokumentationen. Installationsmetoden beskrivs i Dokumentationen. Ingen program- eller maskinvara som kan påverka Programvaran negativt får installeras på den Dator där Programvaran installerats. Med Dator avses maskinvara, inklusive med inte begränsat till persondatorer, bärbara datorer, stationära datorer, handdatorer, smarttelefoner, handburna elektroniska enheter eller andra elektroniska enheter för vilka

Programvaran är utformad, på vilka den kommer att installeras eller användas. Med Licensnyckel avses den unika sekvens med symboler, bokstäver, siffror eller specialtecken som Slutanvändaren har tillhandahållit för att möjliggöra laglig användning av Programvaran, dess specifika version eller utökning av Licensens giltighet i enlighet med detta Avtal.

3. **Licensavtalet**. Under förutsättning att du godkänner villkoren i detta Avtal, betalar licensavgiften inom angiven tid och följer alla villkor häri, ger Leverantören dig följande rättigheter ("Licensen"):

a) **Installation och användning**. Du har den icke-exklusiva, ej överförbara rätten att installera Programvaran på hårddisken i en dator eller liknande medium för permanent datalagring, att installera och lagra Programvaran i minnet i ett datorsystem och att implementera, lagra och visa Programvaran.

b) **Bestämmelse av antalet licenser**. Rätten att använda Programvaran är bunden till antalet Slutanvändare. En Slutanvändare definieras enligt följande: (i) att Programvaran installeras på ett datorsystem eller (ii) om licensavtalet gäller antalet e-postkonton, är en Slutanvändare en datoranvändare som erhåller e-post via en e-postagent (”MUA”). Om en MUA tar emot e-post och sedan automatiskt distribuerar den till flera användare så motsvarar antalet Slutanvändare det antal användare e-posten distribueras till Om en e-postserver fungerar som ”mail-gate” är antalet Slutanvändare det antal e-postserveranvändare som denna mail-gate betjänar. Om ett ospecificerat antal e-postadresser (genom t.ex. aliasadresser) är ämnade för en och samma användare och e-postmeddelanden inte automatiskt distribueras till ett stort antal användare, gäller Licensavtalet endast en dator. Du får inte använda samma Licens samtidigt på fler än en dator. Slutanvändaren får endast ange Licensnyckeln till Programvaran i den utsträckning som Slutanvändaren har rätt att använda Programvaran enligt den begränsning som uppstår av antalet Licenser som tillhandahållits av Leverantören. Licensnyckeln är konfidentiell; du får inte dela Licensen med tredje part eller låta tredje part använda Licensnyckeln om inte detta medges i detta Avtal eller av Leverantören. Meddela omgående Leverantören om Licensnyckeln hamnar i orätta händer.

c) **Home/Business Edition.** En Home Edition-version av Programvaran får uteslutande användas i privata och/eller icke-kommersiella miljöer, och där endast för hem- och familjeanvändning. En Business Edition-version av Programvaran måste införskaffas för användning i en kommersiell miljö samt för att använda Programvaran på e-postservrar, e-postrelän, e-postgateway eller Internet-gateway.

d) **Licensvillkor.** Din rätt att använda Programvaran är tidsbegränsad.

e) **OEM-programvara.** Programvara klassificerad som ”OEM” är begränsad till den dator på vilken den medföljde. Den får inte överföras till en annan dator.

f) **Programvara som NFR, PROV.** Programvara betecknad som ”Inte till försäljning”, NFR eller PROV får inte erhållas mot betalning och får endast användas för demonstration eller utvärdering av Programvarans funktioner.

g) **Licensens hävande.** Licensen upphävs automatiskt vid slutet av perioden för vilken den är giltig. Om du inte uppfyller något av villkoren i detta Avtal, har leverantören rätt att häva Avtalet, utan förfång eller laglig gottgörelse för Leverantören i detta fall. Om Licensen skulle hävas måste du genast ta bort, förstöra eller på egen bekostnad returnera Programvaran och alla säkerhetskopior till ESET eller till återförsäljaren där Programvaran erhölls. Vid hävande av licensen har Leverantören även rätt att avbryta Slutanvändarens rätt att använda de funktioner i Programvaran som kräver anslutning till leverantörens servrar eller tredjepartsservrar.

4. **Funktioner med datainsamlings- och Internetanslutningskrav.** För att Programvaran ska fungera korrekt krävs en Internetanslutning och regelbunden anslutning till Leverantörens servrar eller tredjepartsservrar samt tillämplig datainsamling i enlighet med Sekretesspolicyn. Anslutning till Internet och tillämplig datainsamling krävs för följande funktioner i Programvaran:

a) **Uppdateringar av Programvaran**. Leverantören har rätt från tid till annan att utfärda uppdateringar eller uppgraderingar av Programvaran (”Uppdateringar”), men är inte skyldig att tillhandahålla Uppdateringar. Denna

funktion är aktiverad i Programvarans standardinställningar och Uppdateringar installeras därför automatiskt om inte Slutanvändaren har inaktiverat automatisk installation av Uppdateringar. För att kunna tillhandahålla Uppdateringar kan verifiering av Licensers autenticitet krävas, inklusive information om Datorn eller plattformen på vilken Programvaran är installerad i enlighet med Sekretesspolicyn.

Tillhandahållandet av Uppdateringar kan omfattas av livscykelpolicyn, som är tillgänglig på https://go.eset.com/eol_home. Inga Uppdateringar kommer att tillhandahållas efter att Programvaran eller någon av dess funktioner har nått datumet för slutet av sin livslängd enligt definition i livscykelpolicyn.

b) **Vidarebefordran av infiltreringar och information till Leverantören**. Programvaran innehåller funktioner som samlar in prover på virus och andra skadliga program och misstänkta, problematiska, potentiellt oönskade eller potentiellt osäkra objekt som filer, webbadresser, IP-paket och Ethernet-ramar (”Infiltreringar”) och därefter skickar dem till Leverantören, inklusive men inte begränsat till information om installationsprocessen, Datorn och/eller plattformen på vilken Programvaran installerats och information om Programvarans åtgärder och funktionalitet (”Information”). Informationen och Infiltreringarna kan innehålla data (inklusive slumpmässigt eller oavsiktligt erhållna personliga data) om Slutanvändaren eller andra användare av den dator där Programvaran finns installerad, och filer påverkade av Infiltreringar med associerade metadata.

Information och Infiltreringar kan samlas in av följande funktioner i Programvaran:

i. LiveGrid Reputation System-funktionen inkluderar insamling och skickande av envägs-hash-värden relaterade till Infiltreringar till Leverantören. Funktionen är aktiv i Programvarans standardinställningar.

ii. LiveGrid Feedback System-funktionen inkluderar insamling och skickande av Infiltreringar med associerade metadata och Information till Leverantören. Funktionen aktiveras av Slutanvändaren under installationen av Programvaran.

Leverantören ska endast använda Information och Infiltreringar som tagits emot för analys av och forskning på Infiltreringar, förbättring av Programvaran och verifiering av Licensers autenticitet, och ska vidta lämpliga åtgärder för att säkerställa att Infiltreringar och Information som tagits emot hålls säker. Genom att aktivera den här funktionen i Programvaran godkänner du att Infiltreringar och Information samlas in och behandlas av Leverantören i enlighet med Sekretesspolicyn och tillämpliga lagar. Du kan när som helst inaktivera dessa funktioner.

För att kunna uppfylla detta Avtal är det nödvändigt att samla in, behandla och lagra data så att Leverantören kan identifiera dig i enlighet med Sekretesspolicyn. Du godkänner härmed att Leverantören har rätt att med egna metoder kontrollera att du använder Programvaran i enlighet med villkoren i det här Avtalet. Du godkänner härmed att under Programvarans kommunikation med Leverantörens eller dess partners datasystem som ingår i Leverantörens distributions- och supportnätverk, kan data överföras vars avsikt är att säkerställa Programvarans funktion och auktorisera dess användning samt att skydda Leverantörens rättigheter.

Efter Avtalets ingående har Leverantören och dess affärspartner som ingår i Leverantörens distributions- och supportnätverk rätt att överföra, behandla och lagra viktiga data som identifierar dig i syfte att kunna fakturera dig, uppfylla Avtalet och skicka meddelanden på Datorn.

Information om sekretess, personuppgiftsskydd och dina rättigheter som registrerad finns i Sekretesspolicyn som är tillgänglig på Leverantörens webbplats och är åtkomlig direkt från installationsprocessen. Du kan även besöka den via Programvarans hjälpavsnitt.

5. **Slutanvändarens rättigheter**. Rättigheterna som Slutanvändare måste utövas av dig personligen eller av dina anställda. Du har endast rätt att använda Programvaran till att skydda dina verksamheter och de Datorer eller datorsystem för vilka du har erhållit en Licens.

6. **Begränsning av rättigheter.** Du får inte kopiera, distribuera, extrahera komponenter eller egna produkter av Programvaran. Vid användning av Programvaran gäller följande begränsningar:

a) Du får göra en kopia av Programvaran på ett permanent lagringsmedium som en säkerhetskopia, förutsatt att denna säkerhetskopia inte installeras eller används på en dator. Alla andra kopior av denna Programvara anses vara ett brott mot detta Avtal.

b) Du får inte använda, ändra, översätta, reproducera Programvaran eller överföra rättigheterna att använda Programvaran eller kopior av Programvaran på något annat sätt än som anges i detta Avtal.

c) Du får inte sälja, underlicensiera, leasa eller hyra eller låna ut Programvaran eller använda Programvaran i syfte att tillhandahålla kommersiella tjänster.

d) Du får inte bakåtkompilera eller disassemblera Programvaran eller på annat sätt identifiera Programvarans källkod, om inte denna begränsning är uttryckligen förbjuden i lag.

e) Du förbinder dig att endast använda Programvaran på ett sätt som är i överensstämmelse med gällande lag i den jurisdiktion som din användning av Programvaran lyder under, inklusive, men inte begränsat till, gällande upphovsrättslagstiftning.

f) Du godkänner att du endast använder Programvaran och dess funktioner på ett sätt som inte begränsar andra Slutanvändares möjligheter till åtkomst till dessa tjänster. Leverantören förbehåller sig rätten att begränsa tjänsternas omfattning för vissa Slutanvändare för att möjliggöra högsta möjliga antal Slutanvändares åtkomst till tjänsten. Begränsning av tjänsternas omfattning innebär också fullständigt avbrytande av möjligheten att använda någon av Programvarans funktioner och borttagning av Data på Leverantörens servrar eller på tredjepartsservrar angående en viss funktion i Programvaran.

g) Du godkänner att inte utföra några aktiviteter som involverar användning av Licensnyckeln som strider mot detta Avtal eller leder till att Licensnyckeln tillhandahålls till någon person som inte är berättigad att använda Programvaran, till exempel överföring av en använd eller oanvänd Licensnyckel i någon form, såväl som obehörig reproduktion eller distribution av duplicerade eller genererade Licensnycklar eller att använda Programvaran till följd av användning av en Licensnyckel som har erhållits från en annan källa än Leverantören.

7. **Copyright**. Programvaran tillsammans med alla rättigheter utan begränsningar inklusive ägarrättigheter och immateriella rättigheter tillhör ESET och/eller dess licensgivare. De skyddas av överenskommelser och internationella avtal och alla andra tillämpbara nationella lagar i det land där Programvaran används. Programvarans struktur, organisation och kod utgör värdefulla affärshemligheter och hemlig information som tillhör ESET och/eller dess licensgivare. Du får inte kopiera Programvaran utom det undantag som anges i paragraf 6 (a). Kopior som du är tillåten att göra enligt detta Avtal måste innehålla samma upphovsrättsliga och andra egendomsrättsliga meddelanden som finns på Programvaran. Om du bakåtkompilerar eller disassemblerar Programvaran eller på annat sätt försöker att identifiera Programvarans källkod i strid med detta Avtal, godkänner du att den information som därvid erhållits automatiskt och oåterkalleligen ska överföras till Leverantören och helt ägas av Leverantören från tidpunkten för dess uppkomst, oaktat Leverantörens rättigheter i samband med hävande av detta Avtal.

8. **Förbehållna rättigheter**. Leverantören förbehåller sig härmed alla rättigheter till Programvaran förutom de rättigheter som uttryckligen ges till dig som Slutanvändare av Programvaran i detta Avtal.

9. **Flera språkversioner, programvara på flera media, flera kopior**. I händelse av att Programvaran stöder flera plattformar eller språk eller om du mottar flera kopior av Programvaran, får du endast använda Programvaran på det antal datorer och med de versioner för vilka du har erhållit Licenser. Du får inte sälja, hyra ut, underlicensiera, låna ut eller överföra versioner eller kopior av Programvaran som du inte använder.

10. **Avtalets giltighet och hävande.** Detta Avtal gäller från det datum du godkänner villkoren i detta Avtal. Du kan avsluta det här Avtalet genom att permanent avinstallera, förstöra eller på egen bekostnad returnera Programvaran tillsammans med alla säkerhetskopior och relaterat material som erhållits från Leverantören eller dess partner. Din rätt att använda Programvaran och någon av dessa funktioner kan omfattas av livscykelpolicyn. Efter att Programvaran eller någon av dess funktioner har nått datumet för slutet av sin livslängd enligt definition i livscykelpolicyn, så upphör din rätt att använda Programvaran. Oberoende av på vilket sätt Avtalet hävs ska villkoren i paragraferna 7, 8, 11, 13, 19 och 21 fortsätta att gälla utan tidsbegränsning.

11. **SLUTANVÄNDARENS UTFÄSTELSER**. SOM SLUTANVÄNDARE ÄR DU MEDVETEN OM ATT PROGRAMVARAN LEVERERAS ”I BEFINTLIGT SKICK”, UTAN NÅGON UTTRYCKLIG ELLER UNDERFÖRSTÅDD GARANTI AV NÅGOT SLAG OCH VAD SOM FÖLJER AV TVINGANDE LAGSTIFTNING. VARE SIG LEVERANTÖREN, DESS LICENSGIVARE ELLER DOTTERBOLAG ELLER UPPHOVSRÄTTSINNEHAVARNA GER NÅGRA UTTRYCKLIGA ELLER UNDERFÖRSTÅDDA GARANTIER, INKLUSIVE, MEN INTE BEGRÄNSAT TILL FÖRSÄLJNINGSGARANTIER ELLER GARANTIER OM LÄMPLIGHET FÖR VISSA SYFTEN ELLER ATT PROGRAMVARAN INTE BRYTER MOT PATENT, UPPHOVSRÄTT, VARUMÄRKEN ELLER ANDRA RÄTTIGHETER. LEVERANTÖREN ELLER ANNAN PART GARANTERAR INTE ATT FUNKTIONERNA I PROGRAMVARAN UPPFYLLER DINA KRAV ELLER ATT PROGRAMVARAN FUNGERAR OAVBRUTET OCH FELFRITT. DU TAR DET FULLA ANSVARET OCH RISKEN FÖR ATT VALET AV PROGRAMVARA MOTSVARAR AVSEDDA BEHOV OCH FÖR INSTALLATION, ANVÄNDNING OCH RESULTAT SOM ÅSTADKOMS MED DETTA.

12. **Inga övriga skyldigheter**. Detta Avtal skapar inga skyldigheter för Leverantören och dess licensgivare förutom de som uttryckligen anges häri.

13. **ANSVARSBEGRÄNSNING**. MED UNDANTAG AV VAD SOM FÖLJER AV TVINGANDE LAG, ANSVARAR LEVERANTÖREN, DESS ANSTÄLLDA ELLER LICENSGIVARNA INTE UNDER NÅGRA OMSTÄNDIGHETER FÖR EVENTUELLA UTEBLIVNA VINSTER, INTÄKTER ELLER FÖRSÄLJNINGSVOLYMER, FÖRLUST AV INFORMATION ELLER FÖR KOSTNADER SOM UPPSTÅR FÖR ANSKAFFNING AV ERSÄTTNINGSVAROR ELLER -TJÄNSTER, FÖR SKADA PÅ EGENDOM, PERSONSKADA, DRIFTAVBROTT, FÖRLUST AV AFFÄRSINFORMATION ELLER FÖR ÖVRIGA SÄRSKILDA, DIREKTA, INDIREKTA, OAVSIKTLIGA, EKONOMISKA, STRAFFBARA, SPECIFIKA SKADOR ELLER FÖLJDSKADOR OAVSETT HUR DE UPPKOMMIT, TILL EXEMPEL FRÅN ETT KONTRAKT, ÅTALBAR HANDLING, VÅRDSLÖSHET ELLER ANDRA OMSTÄNDIGHETER SOM IMPLICERAR ANSVAR, SOM UPPSTÅTT TILL FÖLJD AV INSTALLATION, ANVÄNDNING AV ELLER OFÖRMÅGA ATT ANVÄNDA PROGRAMVARAN, ÄVEN OM LEVERANTÖREN ELLER NÅGON AV DESS LICENSGIVARE ELLER DOTTERBOLAG HAR UPPMÄRKSAMMATS PÅ RISKEN FÖR SÅDANA SKADOR. EFTERSOM VISSA LÄNDER OCH JURISDIKTIONER INTE TILLÅTER ANSVARSFRISKRIVNING SAMTIDIGT SOM BEGRÄNSAT ANSVAR ÄR TILLÅTET, BEGRÄNSAS I SÅDANA FALL ANSVARET FÖR LEVERANTÖREN, DESS ANSTÄLLDA ELLER DESS LICENSGIVARE TILL DET PRIS DU HAR BETALAT FÖR PROGRAMVARANS LICENS.

14. Inget i detta Avtal ska påverka de lagstadgade rättigheterna för någon part som agerar som kund om det står i motsats till dessa.

15. **Teknisk support**. ESET eller tredjepart på uppdrag av ESET tillhandahåller teknisk support efter eget gottfinnande, utan garantier eller utfästelser. Inga teknisk support kommer att tillhandahållas efter att Programvaran eller någon av dess funktioner har nått datumet för slutet av sin livslängd enligt definition i livscykelpolicyn. Slutanvändare ska säkerhetskopiera alla befintliga data och program före tillhandahållande av teknisk support. ESET och/eller tredjepart på uppdrag av ESET ansvarar inte för skada på eller förlust av data, egendom, programvara eller maskinvara eller förlust av vinst på grund av teknisk support. ESET och/eller tredjepart på uppdrag av ESET förbehåller sig rätten att avgöra om lösningen av problemet ligger utanför teknisk support. ESET förbehåller sig rätten att vägra, avbryta eller avsluta tillhandahållande av teknisk support enligt eget gottfinnande. Licensinformation, Information och andra data i enlighet med Sekretesspolicyn kan krävas för att tillhandahålla teknisk support.

16. **Överföring av licensen**. Programvaran får överföras från en dator till en annan, om detta inte strider mot villkoren i detta Avtal. Om det inte strider mot villkoren i detta Avtal har Slutanvändaren rätt att endast

permanent överföra Licensen och alla rättigheter i detta Avtal till en annan Slutanvändare med Leverantörens tillstånd, förutsatt att (i) den ursprungliga Slutanvändaren inte behåller kopior av Programvaran, (ii) överföringen av rättigheterna ska vara direkt, dvs. från den ursprungliga Slutanvändaren till den nya Slutanvändaren, (iii) den nya Slutanvändaren godkänner alla rättigheter och skyldigheter som åligger den ursprungliga Slutanvändaren enligt villkoren i detta Avtal, (iv) den ursprungliga Slutanvändaren förser den nya Slutanvändaren med dokumentation som gör det möjligt att verifiera Programvarans äkthet enligt paragraf 17.

17. **Verifikation av Programvarans äkthet.** Slutanvändaren kan påvisa rätt att använda Programvaran på något av följande sätt: (i) med ett licenscertifikat utfärdat av Leverantören eller av tredje part utsedd av Leverantören; (ii) med ett skriftligt licensavtal, om ett sådant avtal ingåtts; (iii) genom att skicka ett e-postmeddelande till Leverantören med licensieringsuppgifter (användarnamn och lösenord). Licensinformation och identifieringsdata för Slutanvändare i enlighet med Sekretesspolicyn kan krävas för att verifiera Programvarans autenticitet.

18. **Licensiering för offentliga myndigheter och USA:s regering**. Programvaran tillhandahålls till offentliga myndigheter, inklusive USA:s regering med de licensrättigheter och begränsningar som beskrivs i detta avtal.

19. **Efterlevnad av handelskontroll**.

a) Du får inte, direkt eller indirekt, exportera, återexportera, överföra eller på annat sätt tillgängliggöra Programvaran till någon person, eller använda den på något sätt, eller vara involverad i någon handling, som kan medföra att ESET eller dess holdingbolag, dess dotterbolag och dotterbolagen till något av dess holdingbolag, såväl som enheter som kontrolleras av dess holdingbolag (”Närstående bolag”) bryter mot, eller drabbas av negativa följder, i enlighet med handelskontrollagar som inkluderar

i. alla lagar som kontrollerar, begränsar eller ålägger licensieringskrav på export, återexport eller överföring av varor, programvara, teknik eller tjänster, stiftade eller antagna av någon regering, stat eller tillsynsmyndighet i USA, Singapore, Storbritannien, EU eller någon av dess medlemsstater, eller något land där avtalsförpliktelserna ska uppfyllas, eller där ESET eller något av dess närstående bolag har sitt säte eller bedriver verksamhet och

ii. alla ekonomiska, finansiella, handels- eller andra lagar, eller annan sanktion, restriktion, embargo, import- eller exportförbud, förbud mot överföring av medel eller tillgångar eller mot utförande av tjänster, eller motsvarande åtgärd ålagd av någon regering, stat eller tillsynsmyndighet i USA, Singapore, Storbritannien, EU eller någon av dess medlemsstater, eller något land där avtalsförpliktelserna ska uppfyllas, eller där ESET eller något av dess närstående bolag har sitt säte eller bedriver verksamhet (”Sanktionslagar”).

(rättsakter som avses i punkterna i och ii ovan tillsammans som ”Handelskontrollagar”).

b) ESET ska ha rätt att inställa fullgörandet av sina förpliktelser i enlighet med, eller avsluta, dessa Villkor med omedelbar verkan i händelse av att:

i. ESET i sitt motiverade yttrande fastställer att Användaren har brutit mot eller troligen kommer att bryta mot bestämmelsen i Artikel 19 a) i Avtalet, eller

ii. Slutanvändaren och/eller Programvaran omfattas av Handelskontrollagar och att ESET, till följd av detta, fastställer i sitt motiverade yttrande att fortsatt fullgörande av sina förpliktelser i enlighet med Avtalet kan medföra att ESET eller dess Närstående bolag bryter mot, eller drabbas av negativa följder i enlighet med, handelskontrollagar.

c) Inget i Avtalet är avsett, och inget ska tolkas som så, att förmå eller fordra någon part att agera eller avstå från att agera (eller att avtala om att agera eller avstå från att agera) på något sätt som är oförenligt med, straffbart eller förbjudet i enlighet med några tillämpliga Handelskontrollagar.

20. **Meddelanden**. Alla meddelanden, den returnerade Programvaran och Dokumentationen ska skickas till: ESET,

spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, utan förfång för ESET:s rätt att informera dig om eventuella ändringar av Avtalet, Sekretesspolicyer, EOL-policyn och Dokumentation i enlighet med art. 22 i Avtalet. ESET kan skicka e-post, meddelanden i appen via Programvara eller publicera informationen på vår webbplats. Du samtycker till att få juridiska meddelanden från ESET i elektronisk form, inklusive eventuella meddelanden om förändringar i villkor, specialvillkor eller sekretesspolicyer, avtalsförslag eller -godkännanden eller förhandlingar, meddelanden eller annan juridisk kommunikation. Sådan elektronisk kommunikation ska anses ha mottagits skriftligt, såvida inte en annan kommunikationsmetod specifikt krävs enligt gällande lag.

21. **Gällande lag**. Det här Avtalet styrs av och tolkas i enlighet med lagstiftning i Republiken Slovakien. Slutanvändaren och Leverantören är härmed överens om att villkor som står i konflikt med gällande lagstiftning eller med FN:s internationella köplag (Convention on Contracts for the International Sale of Goods) inte gäller. Du godkänner uttryckligen att eventuella tvister eller anspråk som uppstår i samband med detta Avtal med avseende på Leverantören eller tvister eller anspråk gällande användningen av programvaran löses av regiondomstolen i Bratislava och du godkänner uttryckligen denna domstols jurisdiktion.

22. **Allmänna bestämmelser**. Om något av villkoren i detta Avtal är ogiltigt eller icke-verkställbart, påverkar detta inte de övriga villkorens giltighet i Avtalet, som förblir giltiga och verkställbara enligt villkoren häri. Detta Avtal har genomförts på engelska. Om någon översättning av avtalet görs av bekvämlighetsskäl eller något annat syfte eller i något annat fall av avvikelse mellan språkversioner av detta Avtal, så har den engelska versionen företräde.

ESET förbehåller sig rätten att göra ändringar i Programvaran samt att revidera villkor i Avtalet, dess Bilagor, Tillägg, Sekretesspolicy, Livscykelpolicy och Dokumentation eller någon del av detta när som helst genom att uppdatera aktuella dokument (i) så att de speglar förändringar i Programvaran eller ESET:s verksamhet, (ii) av juridiska, regleringsmässiga eller säkerhetsmässiga skäl eller (iii) för att förhindra missbruk eller skada. Du meddelas om eventuell revidering av Avtalet via e-post, meddelanden i appen eller annat elektroniskt sätt. Om du inte samtycker till de föreslagna ändringarna av Avtalet kan du säga upp det i enlighet med artikel 10 inom 30 dagar efter att du fått ett meddelande om ändringen. Om du inte säger upp Avtalet inom denna tidsfrist kommer de föreslagna ändringarna att anses godkända och träda i kraft gentemot dig från och med det datum du fick ett meddelande om ändringen.

Detta är det fullständiga Avtalet mellan dig och Leverantören gällande Programvaran och ersätter alla tidigare uppgifter, diskussioner, åtaganden, meddelanden eller annonsering gällande Programvaran.

TILLÄGG TILL AVTALET

Bedömning av nätverksanslutna enheters säkerhet. Ytterligare bestämmelser gäller för bedömning av nätverksanslutna enheters säkerhet enligt följande:

Programvaran innehåller en funktion som kontrollerar säkerheten för Slutanvändarens lokala nätverk och säkerheten för enheter i det lokala nätverket, vilket kräver lokalt nätverksnamn och information om enheter i det lokala nätverket, till exempel enheternas närvaro, typ, namn, IP-adress och MAC-adress i det lokala nätverket i samband med licensinformation. Informationen inkluderar även typ av trådlös säkerhet och typ av trådlös kryptering för routerenheter. Funktionen kan även ge information om tillgängligheten på säkerhetsprogramlösningar för att skydda enheter i det lokala nätverket.

Skydd mot missbruk av data. Ytterligare bestämmelser gäller för skydd mot missbruk av data enligt följande:

Programvaran innehåller en funktion som förhindrar förlust eller missbruk av viktiga data i direkt anslutning till stöld av Datorn. Denna funktion är avstängd i Programvarans standardinställningar. ESET HOME-kontot behöver skapas för att den ska aktiveras, varigenom funktionen aktiverar datainsamling om datorn blir stulen. Om du väljer att aktivera den här funktionen i Programvaran godkänner du att data om den stulna Datorn samlas in och skickas till Leverantören, vilket kan inkludera data om Datorns nätverksplats, data om innehållet som visas på Datorns skärm, data om Datorns konfiguration eller data inspelade av en kamera ansluten till Datorn (hädanefter

”Data”). Slutanvändaren har rätt att använda Data anskaffade på detta sätt och tillhandahållna via ESET HOME-kontot endast i syfte att rätta till den ofördelaktiga situationen orsakad av stöld av en Dator. Du ger även Leverantören tillstånd att enligt Sekretesspolicyn och tillämpliga lagar behandla dessa Data inom Funktionens ramar. Leverantören ska tillåta Slutanvändaren att komma åt Data under den period som krävs för att uppnå det ändamål för vilken data anskaffades, vilket inte får överstiga den lagringsperiod som anges i Sekretesspolicyn. Skydd mot missbruk av data får uteslutande användas med Datorer och konton till vilka Slutanvändaren har legitim tillgång. Illegal användning rapporteras till behörig myndighet. Leverantören ska följa gällande lagar och hjälpa myndigheterna i händelse av missbruk. You agree and acknowledge that You are responsible for safeguarding the password to access ESET HOME Account and you agree that You shall not disclose your password to any third party. Slutanvändaren ansvarar för all aktivitet med funktionen Skydd mot missbruk av data och ESET HOME-kontot, behörig eller inte. Om ESET HOME-kontot avslöjas, meddela omedelbart Leverantören. Ytterligare bestämmelser för skydd mot missbruk av data gäller endast för Slutanvändare av ESET Internet Security och ESET Smart Security Premium.

ESET Secure Data. Ytterligare bestämmelser gäller för ESET Secure Data enligt följande:

1. Definitioner. I dessa ytterligare bestämmelser för ESET Secure Data har följande ord motsvarande betydelser:

a) ”Information” all information eller data som krypteras eller dekrypteras med hjälp av programvaran;

b) ”Produkter” ESET Secure Data-programvaran och dokumentationen;

c) ”ESET Secure Data” programvaran/programvarorna som används för kryptering och dekryptering av elektroniska data;

Alla hänvisningar i plural inkluderar även singular och alla hänvisningar i maskulinum inkluderar även femininum och neutrum och vice versa. Ord utan specifik definition ska användas i enlighet med definitioner som stipuleras i Avtalet.

2. Ytterligare slutanvändardeklaration. Du bekräftar och godkänner att:

a) Det är ditt ansvar att skydda, bevara och säkerhetskopiera Information;

b) Du bör säkerhetskopiera all information och data fullständigt (inklusive och utan begränsning all viktig information och data) på datorn innan installationen av ESET Secure Data;

c) Du måste hålla ett säkert register över alla lösenord eller annan information som används för att ställa in och använda ESET Secure Data, och du måste även göra säkerhetskopior av alla krypteringsnycklar, licenskoder, nyckelfiler och andra data som genereras för att separera lagringsmedier;

d) Du är ansvarig för användningen av Produkterna. Leverantören är inte ansvarig för eventuella förluster, anspråk eller skador som uppkommer till följd av otillåten eller felaktig kryptering eller dekryptering av information eller data oavsett var och hur denna information eller data lagras;

e) Även om Leverantören har vidtagit alla rimliga åtgärder för att säkerställa integriteten och säkerheten hos ESET Secure Data, så får Produkterna (eller någon av dem) inte användas inom något område som är beroende av en felsäker säkerhetsnivå eller som är potentiellt farligt, inklusive men inte begränsat till kärnkraftsanläggningar, flygplansnavigering, kontroll- eller kommunikationssystem, vapen- och försvarssystem samt livsuppehållande eller livsövervakande system;

f) Det är ditt ansvar att se till att säkerhetsnivån och krypteringsnivån som tillhandahålls av produkterna är tillräcklig för dina behov;

g) Du är ansvarig för din användning av Produkterna (eller någon av dem), inklusive men inte begränsat till att se

till att denna sker i överensstämmelse med alla tillämpliga lagar och förordningar i Slovakien eller annat land, annan region eller stat där Produkterna används. Innan all användning måste du måste se till att användningen inte är i strid med någon regerings (i Slovakien eller på annat sätt) embargo;

h) ESET Secure Data får kontakta Leverantörens servrar från tid till annan för att kontrollera licensinformation, tillgängliga korrigeringsfiler, servicepaket och andra uppdateringar som kan förbättra, bibehålla, ändra eller förbättra driften av ESET Secure Data och kan skicka generell systeminformation i samband med driften i enlighet med Sekretesspolicyn.

i) Leverantören är inte ansvarig för eventuella förluster, skador, kostnader eller krav som härrör från förlust, stöld, missbruk, korruption, skada eller förstörelse av lösenord, installationsinformation, krypteringsnycklar, licensaktiveringskoder och andra uppgifter som genereras eller lagras under användning av programvaran.

Ytterligare bestämmelser för ESET Secure Data gäller endast för Slutanvändare av ESET Smart Security Premium.

Password Manager Programvara. Ytterligare bestämmelser gäller för programvaran Password Manager enligt följande:

1. Ytterligare slutanvändardeklaration. Du bekräftar och godkänner att du inte får:

a) använda programvaran Password Manager för att driva någon verksamhetskritisk tillämpning där människors liv eller egendom kan stå på spel. Du förstår att programvaran Password Manager inte är utformad för sådana ändamål och att eventuellt fel på programvaran i sådana fall kan leda till dödsfall, personskada eller allvarlig skada på egendom eller miljöskador som Leverantören inte är ansvarig för.

PROGRAMVARAN PASSWORD MANAGER ÄR INTE UTFORMAD, AVSEDD ELLER LICENSIERAD FÖR ANVÄNDNING I FARLIGA MILJÖER SOM KRÄVER FELSÄKRA KONTROLLEN, INKLUSIVE OCH UTAN BEGRÄNSNING, KONSTRUKTION, TILLVERKNING, UNDERHÅLL OCH DRIFT AV KÄRNKRAFTVERK, FLYGPLANSNAVIGERING ELLER KOMMUNIKATIONSSYSTEM, FLYGLEDNING OCH LIVSUPPEHÅLLANDE SYSTEM ELLER VAPENSYSTEM. LEVERANTÖR AVSÄGER SIG SPECIELLT ALLA DIREKTA ELLER INDIREKTA GARANTIER FÖR LÄMPLIGHETEN FÖR SÅDANA ÄNDAMÅL.

b) använda programvaran Password Manager på ett sätt som bryter mot detta Avtal eller lagarna i Slovakien eller din jurisdiktion. Du får speciellt inte använda Password Manager för att genomföra eller främja olagliga aktiviteter, inklusive överföring av data med skadligt innehåll eller innehåll som kan användas för eventuella olagliga aktiviteter eller som på något sätt bryter mot lagen eller någon tredje parts rättigheter (inklusive immateriell äganderätt), inklusive men inte begränsat till alla försök att få tillgång till konton i Lagringen (i dessa ytterligare bestämmelser för programvaran Password Manager avser ”Lagring” datalagringsutrymme som förvaltas av Leverantören eller en tredje part annan än Leverantören och användaren för ändamålet att möjliggöra synkronisering och säkerhetskopiering av användardata) eller några konton och data från annan Password Manager-programvara eller andra Lagringsanvändare. Om du bryter mot någon av dessa bestämmelser har Leverantören rätt att omedelbart säga upp detta Avtal och vidarebefordra kostnaden för alla nödvändiga åtgärder till dig, samt vidta alla nödvändiga åtgärder för att hindra dig från vidare användning av programvaran Password Manager utan möjlighet till återbetalning.

2. ANSVARSBEGRÄNSNING. PROGRAMVARAN PASSWORD MANAGER LEVERERAS ”I BEFINTLIGT SKICK”. INGEN GARANTI AV NÅGOT SLAG, VARKEN UTTRYCKLIG ELLER UNDERFÖRSTÅDD, LÄMNAS. DU ANVÄNDER PROGRAMVARAN PÅ EGEN RISK. LEVERANTÖREN ÄR INTE ANSVARIG FÖR DATAFÖRLUST, SKADOR, BEGRÄNSNING AV TJÄNSTETILLGÄNGLIGHET INKLUSIVE ALL DATA SOM SKICKATS AV PROGRAMVARAN PASSWORD MANAGER TILL EXTERN LAGRING FÖR DATASYNKRONISERING OCH SÄKERHETSKOPIERING. DEKRYPTERING AV DATA MED HJÄLP AV PROGRAMVARAN PASSWORD MANAGER MEDFÖR INTE NÅGON SKYLDIGHET FÖR LEVERANTÖREN GÄLLANDE SÄKERHETEN FÖR DATAN. DU SAMTYCKER UTTRYCKLIGEN TILL ATT DEN DATA SOM ÄR INFÖRSKAFFAD, ANVÄND, KRYPTERAD, LAGRAD, SYNKRONISERAD ELLER SKICKAD MED HJÄLP

AV PROGRAMVARAN PASSWORD MANAGER ÄVEN KAN LAGRAS PÅ TREDJEPARTSTJÄNSTER (GÄLLER ENDAST FÖR ANVÄNDNINGEN AV PROGRAMVARAN PASSWORD MANAGER DÄR SYNKRONISERING OCH SÄKERHETSKOPIERING HAR AKTIVERATS). OM LEVERANTÖREN PÅ EGEN HAND VÄLJER ATT ANVÄNDA SÅDAN TREDJE PARTS LAGRING, WEBBPLATS, WEBBPORTAL, SERVER ELLER TJÄNST, SÅ ÄR LEVERANTÖREN INTE ANSVARIG FÖR KVALITET, SÄKERHET ELLER TILLGÄNGLIGHET AV SÅDANA TREDJEPARTSTJÄNSTER OCH LEVERANTÖREN ÄR PÅ INGET SÄTT SKYLDIG GENTEMOT DIG FÖR NÅGOT BROTT MOT AVTALSMÄSSIGA ELLER RÄTTSLIGA SKYLDIGHETER SOM DEN TREDJE PARTEN UTFÖR. INTE HELLER FÖR SKADOR, UTEBLIVEN VINST, FINANSIELLA ELLER IKKE-FINANSIELLA SKADOR ELLER NÅGON ANNAN TYP AV FÖRLUST VID ANVÄNDNINGEN AV DENNA PROGRAMVARA. LEVERANTÖREN ÄR INTE ANSVARIG FÖR INNEHÅLLET I ALLA DATA SOM SAMLATS IN, ANVÄNTS, KRYPTERATS, LAGRATS, SYNKRONISERATS ELLER SKICKATS MED PROGRAMVARAN PASSWORD MANAGER ELLER SOM ÄR I LAGRING. DU BEKRÄFTAR ATT LEVERANTÖREN INTE HAR TILLGÅNG TILL INNEHÅLLET I DEN LAGRADE DATAN OCH ATT LEVERANTÖREN INTE KAN ÖVERVAKA DEN ELLER TA BORT RÄTTSLIGT SKADLIGT INNEHÅLL.

Leverantören äger alla rättigheter till förbättringar, uppgraderingar och reparationer i samband med programvaran Password MANAGER (”Förbättringar”), även i händelse av att sådana förbättringar har skapats baserat på återkoppling, idéer eller förslag som lämnats in av dig i någon form. Du kommer inte ha rätt till någon ersättning, inklusive royalties, i samband med sådana förbättringar.

LEVERANTÖRENS ENHETER OCH LICENSGIVARE ÄR INTE ANSVARIGA FÖR FORDRINGAR OCH SKULDER AV NÅGOT SLAG TILL FÖLJD AV ELLER PÅ NÅGOT SÄTT I SAMBAND MED DIN ELLER TREDJE PARTS ANVÄNDNING AV PROGRAMVARAN PASSWORD MANAGER, FÖR ANVÄNDNINGEN ELLER ICKE-ANVÄNDNINGEN AV NÅGOT MÄKLARFIRMA ELLER ÅTERFÖRSÄLJARE ELLER FÖR FÖRSÄLJNINGEN ELLER KÖPET AV NÅGON SÄKERHET, OAVSETT OM SÅDANA ANSPRÅK OCH SKYLDIGHETER BASERAR SIG PÅ NÅGON RÄTTSLIG ELLER SKÄLIG GRUND.

LEVERANTÖRENS ENHETER OCH LICENSGIVARE ÄR INTE SKYLDIGA GENTEMOT DIG FÖR NÅGON DIREKT, INDIREKT, TILLFÄLLIG SKADA ELLER FÖLJDSKADOR FÖLJD AV ELLER I SAMBAND MED NÅGON TREDJEPARTSPROGRAMVARA, NÅGON DATA SOM NÅTTS VIA PROGRAMVARAN PASSWORD MANAGER, DIN ANVÄNDNING AV ELLER OFÖRMÅGA ATT ANVÄNDA PROGRAMVARAN PASSWORD MANAGER, OAVSETT OM SÅDANT SKADEANSPRÅK STÄLLS BASERAT PÅ NÅGON LAG ELLER SKÄLIGEN. SKADOR SOM UNDANTAS FRÅN DENNA KLAUSUL INNEFATTAR, UTAN BEGRÄNSNING, DE FÖR FÖRLUST AV VINST, SKADA PÅ PERSON ELLER EGENDOM, VERKSAMHETSAVBROTT, FÖRLUST AV AFFÄRS- ELLER PERSONLIG INFORMATION. VISSA LÄNDER TILLÅTER INTE BEGRÄNSNING AV SKADOR SÅ DENNA BEGRÄNSNING KANSKE INTE GÄLLER DIG. I SÅ FALL KOMMER LEVERANTÖRENS ANSVARSOMFATTNING ATT UTGÖRAS AV DEN MINSTA TILLÅTNA ANSVARSOMFATTNINGEN ENLIGT TILLÄMPLIG LAG.

INFORMATION SOM GES GENOM PROGRAMVARAN PASSWORD MANAGER, INKLUSIVE AKTIEKURSER, ANALYSER, MARKNADSINFORMATION, NYHETER OCH FINANSIELLA DATA KAN VARA FÖRDRÖJD, FELAKTIG ELLER INNEHÅLLA FEL ELLER BRISTER OCH LEVERANTÖRENS ENHETER OCH LICENSGIVARE HAR INGET ANSVAR I FÖRHÅLLANDE TILL DETTA. LEVERANTÖREN KAN VÄLJA ATT ÄNDRA ELLER AVBRYTA NÅGON KOMPONENT ELLER FUNKTION AV PROGRAMVARAN PASSWORD MANAGER ELLER ANVÄNDNINGEN AV ALLA ELLER NÅGRA FUNKTIONER ELLER TEKNIKER I PROGRAMVARAN PASSWORD MANAGER NÄR SOM HELST UTAN TIDIGARE MEDDELANDE TILL DIG.

OM BESTÄMMELSERNA I DENNA ARTIKEL ÄR OGILTIGA AV NÅGON ANLEDNING ELLER OM LEVERANTÖREN ANSES ANSVARIG FÖR FÖRLUSTER, SKADOR M.M. UNDER TILLÄMPLIG LAG, SÅ GODKÄNNER PARTNERNA ATT LEVERANTÖRENS ANSVAR GENTEMOT DIG KOMMER ATT BEGRÄNSAS TILL DEN TOTALA MÄNGDEN LICENSAVGIFTER SOM BETALATS AV DIG.

DU GÅR MED PÅ ATT ERSÄTTA, FÖRSVARA OCH HÅLLA LEVERANTÖREN OCH DESS ANSTÄLLDA, DOTTERBOLAG, OMPROFILERINGSPARTNERS OCH ANDRA PARTNERS FRÅN OCH MOT ALLA TREDJEPARTS (INKLUSIVE ÄGARE AV ENHETEN ELLER PARTER VARS RÄTTIGHETER PÅVERKATS AV DATA SOM ANVÄNTS I PROGRAMVARAN PASSWORD MANAGER ELLER I LAGRINGEN) KOSTNADER, FORDRINGAR, SKULDER, SKADOR, FÖRLUSTER OCH UTGIFTER SOM SÅDANA PARTER KAN HA ÅDRAGIT SIG GENOM DIN ANVÄNDNING AV PROGRAMVARAN PASSWORD MANAGER.

3. Data i programvaran Password Manager. Om inte annat uttryckligen valts av dig, så lagras alla data som anges av dig och som har sparats i programvaran Password Managers databas i krypterat format på datorn eller annan lagringsenhet som definieras av dig. Du förstår att när det gäller borttagande av, eller skada på någon Password Manager-databas eller andra filer, så kommer alla uppgifter som finns däri att oåterkalleligen förloras och du förstår och accepterar risken för sådan förlust. Det faktum att dina personuppgifter lagras i krypterat format på datorn betyder inte att informationen inte kan stjälas eller missbrukas av någon som upptäcker huvudlösenordet eller får tillgång till den kunddefinierade aktiveringsenheten för att öppna databasen. Du är ansvarig för att upprätthålla säkerheten för alla åtkomstmetoder.

4. Överföring av personuppgifter till Leverantören eller Lagring. Om du väljer det och enbart i syfte att säkerställa snabb datasynkronisering och säkerhetskopiering, så sänder eller skickar programvaran Password Manager personuppgifter från programvaran Password Managers databas – nämligen lösenord, inloggningsinformation och identiteter – via Internet till Lagring. Data överförs uteslutande i krypterad form. Användningen av programvaran Password Manager för att fylla i formulär med lösenord, inloggningar eller andra data kan kräva att information skickas via Internet till webbplatsen som identifieras av dig. Denna överföring av data initieras inte av programvaran Password Manager och därför kan Leverantören inte hållas ansvarig för säkerheten för sådana interaktioner med någon webbplats som stöds av olika leverantörer. Alla transaktioner via Internet i samband eller inte i samband med programvaran Password Manager sker på eget ansvar samt egen risk och du kommer att vara ensamt ansvarig för eventuella skador på ditt datorsystem eller förlust av data till följd av nedladdning och/eller användning av sådant material eller sådan tjänst. För att minimera risken att förlora värdefull data, rekommenderar Leverantören att kunderna utför regelbunden säkerhetskopiering av databasen och andra känsliga filer till externa enheter. Leverantören kan inte ge dig någon hjälp i att återskapa förlorade eller skadade data. Om Leverantören erbjuder säkerhetskopieringstjänster för användardatabasfiler i händelse av skada eller radering av filer på användarnas datorer, är en sådan säkerhetskopieringstjänst utan någon garanti och innebär inte något som helst ansvar för Leverantören gentemot dig.

Genom att använda programvaran Password Manager godkänner du att programvaran kan kontakta Leverantörens servrar från tid till annan för att kontrollera licensinformation, tillgängliga korrigeringsfiler, servicepaket och andra uppdateringar som kan förbättra, bibehålla, ändra eller förbättra driften av programvaran Password Manager. Programvaran kan skicka generell systeminformation i samband med driften av programvaran Password Manager i enlighet med Sekretesspolicyn.

5. Avinstalleringsinformation och instruktioner. All information som du vill behålla från databasen måste exporteras före avinstallationen av programvaran Password Manager.

Ytterligare bestämmelser för programvaran Password Manager gäller endast för Slutanvändare av ESET Smart Security Premium.

ESET LiveGuard. Ytterligare bestämmelser gäller för ESET LiveGuard enligt följande:

Programvaran innehåller en funktion för ytterligare analys av filer som Slutanvändaren har skickats in. Leverantören får endast använda filer inskickade av Slutanvändaren och analysresultat i enlighet med Sekretesspolicyn och gällande lagstiftning.

Ytterligare bestämmelser för ESET LiveGuard gäller endast för Slutanvändare av ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Sekretesspolicy

Skyddet av personuppgifter är synnerligen viktigt för ESET, spol. s r. o., med adress Einsteinova 24, 851 01 Bratislava, Slovak Republic, som registrerats i handelsregistret hos regiondomstolen Bratislava I, avdelning Sro,

diarienummer 3586/B, organisationsnummer: 31333532 som registeransvarig (”ESET” eller ”Vi”). Vi vill uppfylla transparenskravet så som det är juridiskt standardiserat enligt EU:s allmänna dataskyddsförordning (”GDPR”). Vi publicerar därför den här sekretesspolicyn i enda syfte att informera våra kunder (”Slutanvändaren” eller ”Du”) som registrerade om följande ämnen gällande skydd av personuppgifter:

- Rättslig grund för behandling av personuppgifter,
- Datadelning och konfidentialitet,
- Datasäkerhet,
- Dina rättigheter som registrerad,
- Behandling av dina personuppgifter
- Kontaktinformation.

Rättslig grund för behandling av personuppgifter

Det finns endast ett fåtal rättsliga grunder för databehandling som vi använder enligt tillämpligt juridiskt ramverk gällande skyddet av personuppgifter. Behandlingen av personuppgifter på ESET är främst nödvändig för utförandet av Slutanvändaravtalet (”Licensavtalet för slutanvändare”) med Slutanvändaren (art. 6 (1) (b) GDPR), som är tillämpligt för tillhandahållande av ESET:s produkter eller tjänster, om inte annat uttryckligen anges, till exempel:

- Berättigat intresse (art. 6 (1) (f) GDPR) – möjliggör behandling av data om hur våra kunder använder våra tjänster och hur nöjda de är, i syfte att ge våra användare bästa möjliga skydd, support och upplevelse som vi kan erbjuda. Även marknadsföring erkänns av den tillämpliga lagstiftningen som ett berättigat intresse, vilket vi förlitar oss på vid marknadsföringskommunikation med våra kunder.

- Samtycke (art. 6 (1) (a) GDPR) – vilket vi kan begära från dig i specifika situationer när vi anser att denna rättsliga grund är den mest lämpliga eller om det krävs enligt lag.

- Efterlevnad av lagens krav (art. 6 (1) (c) GDPR) – till exempel föreskrifter för elektronisk kommunikation och lagring av faktureringsdokument.

Datadelning och konfidentialitet

Vi delar inte din data med tredje part. ESET är dock ett företag med global verksamhet via dotterbolag eller partner som ingår i vårt försäljnings-, service- och supportnätverk. Information gällande licensiering, fakturering och teknisk support som behandlas av ESET kan överföras till och från dotterbolag eller partner för uppfyllande av licensavtalet för slutanvändare, till exempel tillhandahållande av tjänster eller support.

ESET behandlar helst sin data inom europeiska unionen (EU). Beroende på din plats (användning av våra produkter och/eller tjänster utanför EU) och/eller den tjänst du väljer kan det dock vara nödvändigt att överföra din data till ett land utanför EU. Vi använder till exempel tredjepartstjänster i samband med molnbaserad databehandling. I dessa fall väljer vi noggrant ut våra tjänsteleverantörer och säkerställer en lämplig nivå av dataskydd genom avtalsenliga såväl som tekniska och organisatoriska åtgärder. Vi avtalar i regel om EU:s standardavtalsklausuler, om nödvändigt med kompletterande avtalsbestämmelser.

För vissa länder utanför EU, såsom Förenade kungariket och Schweiz, har EU redan fastställt en jämförbar nivå av uppgiftsskydd. På grund av den jämförbara dataskyddsnivån kräver överföringen av data till dessa länder inget

särskilt tillstånd eller avtal.

Datasäkerhet

ESET vidtar lämpliga tekniska och organisatoriska åtgärder för att hålla en hög säkerhetsnivå som är lämplig i förhållande till potentiella risker. Vi gör vårt bästa för att säkerställa löpande sekretess, integritet, tillgänglighet och motståndskraft hos behandlingssystem och -tjänster. I händelse av ett dataintrång som innebär en risk för dina rättigheter och friheter är Vi dock redo att meddela såväl relevant tillsynsmyndighet som berörda Slutanvändare som registrerade personer.

Registrerade personers rättigheter

Varje slutanvändares rättigheter är viktiga och Vi vill informera dig om att alla Slutanvändare (från något EU-land eller något land utanför EU) har följande rättigheter garanterade hos ESET. För att utöva dina rättigheter som registrerad kan du kontakta oss via vårt supportformulär eller via e-post på dpo@eset.sk. För identifieringsändamål ber vi dig om följande information: Namn, e-postadress och – om sådan är tillgänglig – licensnyckel eller kundnummer och företagstillhörighet. Skicka oss inte några andra personuppgifter, till exempel födelsedatum. Vi vill påpeka att för att kunna behandla din begäran, såväl som för identifieringsändamål, kommer vi att behandla dina personuppgifter.

Rätt att återkalla samtycket. Rätt att återkalla samtycket är tillämpligt vid behandling som endast baseras på samtycke. Om Vi behandlar dina personuppgifter på grundval av ditt samtycke har du rätt att återkalla samtycket när som helst utan att ange några skäl. Återkallandet av ditt samtycke gäller endast för framtiden och påverkar inte lagligheten för de uppgifter som behandlats före återkallandet.

Rätt att göra invändningar. Rätt att invända mot behandlingen är tillämpligt vid behandling som baseras på ESET:s eller tredje parts berättigade intresse. Om Vi behandlar dina personuppgifter för att skydda ett berättigat intresse har Du som registrerad rätt att när som helst invända mot det berättigade intresse vi har angett och behandlingen av dina personuppgifter. Invändningen gäller endast för framtiden och påverkar inte lagligheten för de uppgifter som behandlats före invändningen. Om vi behandlar dina personuppgifter i direktmarknadsföringssyfte är det inte nödvändigt att ange skäl till din invändning. Detta gäller även profilering, i den mån denna är kopplat till sådan direktmarknadsföring. I alla andra fall ber vi dig att kort informera oss om dina invändningar mot ESET:s berättigade intresse att behandla dina personuppgifter.

Observera att vi i vissa fall, trots att du har återkallat ditt samtycke, har rätt att fortsätta behandla dina personuppgifter på annan rättslig grund, till exempel för att utföra ett avtal.

Rätt till åtkomst. Som registrerad har du rätt att när som helst och utan kostnad få information om din data som lagras av ESET.

Rätt till rättelse. Om vi oavsiktligt behandlar felaktiga personuppgifter om dig har du rätt att få detta korrigerat.

Rätt till radering och rätt till begränsning av behandlingen. Som registrerad har du rätt att begära radering eller begränsningar för hur dina personuppgifter behandlas. Om vi exempelvis behandlar dina personuppgifter med ditt samtycke, och du återkallar detta och det inte finns någon annan rättslig grund, exempelvis ett avtal, så raderar Vi omedelbart dina personuppgifter. Dina personuppgifter raderas även så snart de inte längre behövs för de angivna ändamålen i slutet av vår lagringsperiod.

Om vi använder dina personuppgifter enbart i direktmarknadsföringssyfte och du har återkallat ditt samtycke eller invänt mot ESET:s underliggande berättigade intresse, så begränsar vi behandlingen av dina personuppgifter till att vi inkluderar dina kontaktuppgifter i vår interna svartlista för att undvika oönskad kontakt. Annars kommer dina personuppgifter att raderas.

Observera att vi kan vara skyldiga att lagra dina uppgifter tills lagringsskyldigheten och de lagringsperioder som bestämts av lagstiftare eller tillsynsmyndigheter löper ut. Lagringsskyldigheter och lagringsperioder kan även bestämmas av den slovakiska lagstiftningen. Därefter raderas motsvarande data rutinmässigt.

Rätt till uppgiftsportabilitet. Vi förser gärna dig som registrerad med de personuppgifter som ESET behandlar i xls-format.

Rätt att göra en anmälan. Som registrerad person har Du rätt att göra en anmälan hos en tillsynsmyndighet när som helst. ESET lyder under slovakisk lagstiftning och som medlem av Europeiska unionen är Vi bundna av dataskyddslagstiftningen. Den relevanta datatillsynsmyndigheten är Slovakiens byrå för skydd för personuppgifter, som är belägen på Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Behandling av dina personuppgifter

Tjänster från ESET implementerade i vår produkt tillhandahålls enligt villkoren i EULA, men vissa av dem kan kräva särskild uppmärksamhet. Vi vill ge Dig mer information om datainsamling i samband med tillhandahållandet av våra tjänster. Vi tillhandahåller olika tjänster som beskrivs i Licensavtalet för slutanvändare och produktens dokumentation. För att allt ska fungera samlar Vi in följande information:

Licensierings- och faktureringsuppgifter. Namn, e-postadress, licensnyckel och (i förekommande fall) adress, företagstillhörighet och betalningsuppgifter samlas in och behandlas av ESET för att möjliggöra aktivering av licenser, leverans av licensnycklar, påminnelser om utgångsdatum, supportbegäranden, verifiering av licensers äkthet, tillhandahållande av vår tjänst samt andra meddelanden inklusive marknadsföringsmeddelanden i enlighet med tillämplig lagstiftning eller Ditt samtycke. ESET är juridiskt skyldigt att behålla faktureringsinformationen i tio år, men licensinformationen anonymiseras inom 12 månader efter licensens utgång.

Uppdateringar och annan statistik. Den behandlade informationen omfattar information gällande installationsprocess och din dator, inklusive på vilken plattform vår produkt installeras och information om våra produkters åtgärder och funktionalitet. Till exempel operativsystem, maskinvaruinformation, installations-ID, licens-ID, IP-adress, MAC-adress och konfigurationsinställningar för produkten behandlas i syfte att tillhandahålla uppdaterings- och uppgraderingstjänster och för underhåll, säkerhet och förbättring av vår infrastruktur på serversidan (backend).

Denna information hålls åtskild från den identifieringsinformation som krävs för licensierings- och faktureringsändamål eftersom den inte kräver identifiering av Slutanvändare. Lagringsperioden är upp till 4 år.

ESET LiveGrid®-ryktessystemet. Enkelriktade hashvärden relaterade till infiltreringar behandlas för ESET LiveGrid®-ryktessystemet, vilket förbättrar effektiviteten hos våra lösningar mot skadlig kod genom att genomsökta filer jämförs mot en databas med vitlistade och svartlistade objekt i molnet. Slutanvändaren identifieras inte under den här processen.

ESET LiveGrid®-feedbacksystemet. Misstänkta exempel och metadata insamlade från användare som en del av ESET LiveGrid®-feedbacksystemet, vilket gör det möjligt för ESET att omedelbart reagera på våra slutanvändares behov och vara redo att agera mot de senaste hoten. Vi är beroende av att Du skickar oss

- Infiltreringar som till exempel potentiella exempel på virus och andra skadliga program samt misstänkta, problematiska, potentiellt oönskade och potentiellt osäkra objekt som till exempel körbara filer, e-postmeddelanden Du har anmält som skräppost eller som har flaggats av vår produkt;

- Information om användningen av internet som till exempel IP-adress och geografisk information, IP-paket, webbadresser och Ethernet-ramar;

- Kraschdumpfiler och innehåll.

Vi strävar efter att inte samla in data från dig utanför den här omfattningen, men ibland är detta oundvikligt. Oavsiktligt insamlad data kan vara inkluderad i själva den skadliga programvaran (insamlad utan din vetskap eller ditt medgivande) eller ingå i filnamn eller webbadresser, och Vi avser inte att göra denna till en del av våra system eller behandla den i det syfte som beskrivs i den här Sekretesspolicyn.

All information som erhålls och behandlas via ESET LiveGrid®-feedbacksystemet är avsedd att användas utan identifiering av Slutanvändare.

Bedömning av nätverksanslutna enheters säkerhet. För att tillhandahålla funktionen för säkerhetsbedömning behandlar Vi det lokala nätverksnamnet och information om enheter i det lokala nätverket, till exempel enheternas närvaro, typ, namn, IP-adress och MAC-adress i det lokala nätverket i samband med licensinformation. Informationen inkluderar även typ av trådlös säkerhet och typ av trådlös kryptering för routerenheter. Licensinformation som identifierar Slutanvändaren anonymiseras inom 12 månader efter licensens utgång.

Teknisk support. Kontakt- och licensieringsinformation och data i dina supportfrågor kan krävas för att kunna ge dig support. Baserat på vilken kanal Du kontaktar oss genom kan Vi samla in din e-postadress, telefonnummer, licensinformation, produktuppgifter och beskrivning av ditt supportärende. Du kan bli ombedd att förse oss med annan information för att underlätta supporten. Den data som behandlas för teknisk support lagras i 4 år.

Skydd mot missbruk av data. Om ESET HOME-kontot på https://home.eset.com skapas och funktionen aktiveras av Slutanvändaren i samband med stöld av en dator, så samlas följande information in och behandlas: platsdata, skärmdumpar, data om konfigurationen av datorn samt data som registrerats av datorns kamera. Insamlad data lagras på våra servrar eller på våra tjänsteleverantörers servrar i 3 månader.

Password Manager. Om du väljer att aktivera funktionen för Password Manager, så lagras data relaterad till dina inloggningsuppgifter i krypterad form och endast på din dator eller annan utsedd enhet. Om du aktiverar synkroniseringstjänsten lagras krypterad data på våra servrar eller på våra tjänsteleverantörers servrar för att säkerställa tjänsten. Varken ESET eller tjänsteleverantören har tillgång till krypterad data. Endast du har nyckeln för att dekryptera data. Data tas bort när funktionen inaktiveras.

ESET LiveGuard. Om du väljer att aktivera ESET LiveGuard-funktionen måste inskickande av prover som till exempel filer fördefinieras och väljas av Slutanvändaren. De prover du väljer för fjärranalysen överförs till ESET-tjänsten och analysresultatet skickas tillbaka till datorn. Alla misstänkta prover behandlas så som information som samlas in av ESET LiveGrid®-feedbacksystemet.

Program för en bättre kundupplevelse. Om du väljer att aktivera Program för en bättre kundupplevelse kommer den anonyma telemetriinformationen relaterad till användningen av våra produkter att samlas in och användas, baserat på ditt samtycke.

Observera att om den person som använder våra produkter och tjänster inte är Slutanvändaren som har köpt produkten eller tjänsten och ingått Licensavtalet för slutanvändare med oss (till exempel en anställd hos Slutanvändaren, en familjemedlem eller en person som på annat sätt har tillåtelse av Slutanvändaren att använda produkten eller tjänsten i enlighet med Licensavtalet för slutanvändare), så sker behandlingen av uppgifterna inom ESET:s berättigade intresse så som avses i art. 6 (1) f) GDPR, för att göra det möjligt för Slutanvändaren att använda de produkter och tjänster som tillhandahålls av Oss i enlighet med Licensavtalet för slutanvändare.

Kontaktinformation

Om Du vill utöva någon av dina rättigheter som registrerad person eller om Du har en fråga kan du kontakta oss

på:

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