McAfee®

VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

Användarhandbok

Innehåll

KAPITEL 1

Introduktion

McAfee VirusScan Plus erbjuder proaktiv datorsäkerhet som förhindrar skadliga attacker, så att du kan skydda värdefulla filer och tryggt surfa, söka och hämta filer online. Med hjälp av McAfee SiteAdvisors webbsäkerhetsklassificeringar kan du undvika osäkra webbplatser. Tjänsten skyddar även mot attacker på flera fronter genom att kombinera tekniker för antivirus, antispionprogram och brandvägg. McAfees säkerhetsabonnemang levererar kontinuerligt den senaste programvaran så att ditt skydd alltid är uppdaterat. Nu kan du enkelt lägga till och hantera säkerhet för flera datorer i hemmet. Förbättrade prestanda gör dessutom att du skyddas utan att bli störd.

I detta kapitel

KAPITEL 2

McAfee SecurityCenter

Med hjälp av McAfee SecurityCenter kan du övervaka datorns säkerhetsstatus så att du med en gång ser om datorns virusskydd, antispionprogramsskydd, e-postskydd eller brandväggsskydd behöver uppdateras och kan åtgärda potentiella säkerhetsrisker. Här finns de navigeringsverktyg och kontroller du behöver för att samordna och hantera alla delar av datorskyddet.

Innan du börjar konfigurera och hantera datorskyddet bör du undersöka gränssnittet i SecurityCenter och försäkra dig om att du förstår skillnaden mellan skyddsstatus, skyddskategorier och skyddstjänster. Sedan bör du uppdatera SecurityCenter så att du har det senaste skyddet från McAfee.

När den inledande konfigureringen är klar kan du börja använda SecurityCenter vid övervakningen av datorns skyddsstatus. Om SecurityCenter upptäcker något problem med skyddet får du en varning så att du antingen kan åtgärda eller ignorera problemet (beroende på hur allvarligt det är). Du kan även granska SecurityCenter-händelser, till exempel konfigurationsändringar av virussökning, i en händelselogg.

Obs! SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician.

I detta kapitel

Funktioner i SecurityCenter

SecurityCenter innehåller följande funktioner:

Enkel kontroll av skyddsstatus

Granska enkelt datorns skyddsstatus, leta efter uppdateringar och korrigera potentiella skyddsproblem.

Automatiska uppdateringar och uppgraderingar

Uppdateringar för registrerade program hämtas och installeras automatiskt. När det kommer en ny version av ett registrerat McAfee-program får du den utan kostnad så länge du prenumererar. På så vis har du alltid ett aktuellt skydd.

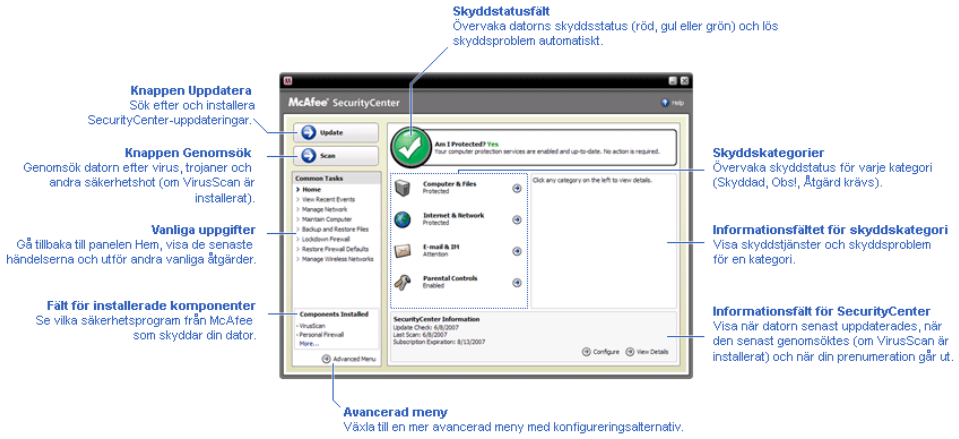
Realtidsvarningar

Säkerhetsvarningar informerar om aktuella virusutbrott och säkerhetshot och gör det möjligt att åtgärda, neutralisera eller ta reda på mer om hotet.

KAPITEL 3

Använda SecurityCenter

Innan du börjar använda SecurityCenter bör du undersöka de komponenter och konfigurationsområden som du kommer att använda för att hantera datorns skyddsstatus. Mer information om den terminologi som används i bilden finns i Introduktion till skyddsstatus (sida 8) och Introduktion till skyddskategorier (sida 9). Sedan kan du gå igenom uppgifterna om ditt McAfee-konto och kontrollera att du har en giltig prenumeration.



I detta kapitel

Introduktion till skyddsstatus

Datorns skyddsstatus visas i skyddsstatusfältet på Hem-panelen i SecurityCenter. Här anges om datorn har ett fullständigt skydd mot de senaste säkerhetshoten och är mottaglig för exempelvis externa säkerhetsattacker, andra säkerhetsprogram och program som ger tillgång till Internet.

Datorns skyddsstatus kan vara röd, gul eller grön.

Skyddsstatus	Beskrivning
Röd	Datorn är inte skyddad. Skyddsstatusfältet på Hem-panelen i SecurityCenter är rött, vilket anger att du inte har något skydd. SecurityCenter rapporterar minst ett allvarligt säkerhetsproblem. Om du vill ha ett fullständigt skydd måste du åtgärda alla allvarliga säkerhetsproblem i varje skyddskategori (problemkategorins status är **Åtgärd krävs!**, även det i rött). Mer information om hur du åtgärdar skyddsproblem finns i Åtgärda skyddsproblem (sida 18).
Gul	Datorn är delvis skyddad. Skyddsstatusfältet på Hem-panelen i SecurityCenter är gult, vilket anger att du inte har något skydd. SecurityCenter rapporterar minst ett mindre allvarligt säkerhetsproblem. Om du vill ha ett fullständigt skydd måste du åtgärda eller ignorera de mindre allvarliga säkerhetsproblemen för varje skyddskategori. Mer information om hur du åtgärdar eller ignorerar skyddsproblem finns i Åtgärda eller ignorera skyddsproblem (sida 17).
Grön	Datorn är fullständigt skyddad. Skyddsstatusfältet på Hem-panelen i SecurityCenter är grönt, vilket anger att datorn är skyddad. SecurityCenter rapporterar inga allvarliga eller mindre allvarliga säkerhetsproblem. I varje skyddskategori listas de tjänster som skyddar datorn.

Introduktion till skyddskategorier

SecurityCenters skyddstjänster delas in i fyra kategorier: Dator och filer, Internet och nätverk, E-post och snabbmeddelanden samt Vuxenkontroll. Med hjälp av de här kategorierna kan du söka bland och konfigurera de säkerhetstjänster som skyddar datorn.

Genom att klicka på en kategori kan du konfigurera skyddstjänsterna och visa eventuella säkerhetsproblem som upptäckts för tjänsterna. Om datorns skyddsstatus är röd eller gul visas meddelandet *Åtgärd krävs!* eller *Obs!* för minst en kategori, vilket anger att SecurityCenter har upptäckt ett problem i kategorin. Mer information om skyddsstatus finns i Introduktion till skyddsstatus (sida 8).

Skyddskategori	Beskrivning
Dator och filer	Med kategorin Dator och filer kan du konfigurera följande skyddstjänster: ▪ Virusskydd ▪ PUP-skydd ▪ Systemövervakning ▪ Windows-skydd
Internet och nätverk	Med kategorin Internet och nätverk kan du konfigurera följande skyddstjänster: ▪ Brandväggsskydd ▪ Identitetsskydd
E-post och snabbmeddelanden	Med kategorin E-post och snabbmeddelanden kan du konfigurera följande skyddstjänster: ▪ E-postskydd ▪ Skräppostskydd
Vuxenkontroll	Med kategorin Vuxenkontroll kan du konfigurera följande skyddstjänster: ▪ Innehållsblockering

Introduktion till skyddstjänster

Skyddstjänsterna är de nyckelkomponenter i SecurityCenter som du konfigurerar för att skydda datorn. Skyddstjänsterna står i direkt relation till McAfee-program. När du installerar VirusScan får du till exempel tillgång till följande skyddstjänster: Virusskydd, PUP-skydd, systemövervakning och Windows-skydd. Mer information om just dessa skyddstjänster finns i hjälpen till VirusScan.

Som standard aktiveras alla de skyddstjänster som förknippas med ett program när du installerar programmet. Du kan däremot när som helst välja att inaktivera en skyddstjänst. Om du installerar Privacy Service aktiveras till exempel både innehållsblockering och identitetsskydd. Om du inte har för avsikt att använda skyddstjänsten innehållsblockering kan du inaktivera den helt. Du kan även inaktivera en skyddstjänst tillfälligt medan du utför inställningar eller underhåll.

Hantera ditt McAfee-konto

Du kan enkelt hantera ditt McAfee-konto från SecurityCenter genom att öppna och granska kontoinformation och kontrollera prenumerationsstatus.

Obs! Om du har installerat dina McAfee-program från en cd-skiva måste du registrera dem på McAfees webbplats innan du kan öppna eller uppdatera ditt McAfee-konto. Det är endast genom att registrera dem som du kan få regelbundna, automatiska programuppdateringar.

Hantera ditt McAfee-konto

Du kan enkelt nå dina McAfee-kontouppgifter (Mitt konto) från SecurityCenter.

1. Klicka på **Mitt konto** under **Vanliga uppgifter**.
2. Logga in på ditt McAfee-konto.

Verifiera din prenumeration

Du verifierar din prenumeration för att kontrollera att den inte har gått ut.

- Högerklicka på SecurityCenter-ikonen i meddelandefältet längst till höger i aktivitetsfältet och klicka sedan på **Verifiera prenumeration**.

KAPITEL 4

Uppdatera SecurityCenter

Tack vare att SecurityCenter söker efter och installerar onlineuppdateringar var fjärde timme kan du vara säker på att dina registrerade McAfee-program är uppdaterade. Onlineuppdateringarna kan omfatta de senaste virusdefinitionerna samt uppgraderingar av skydd mot hackare, skräppostskydd, antispionprogram eller sekretesskydd, beroende på vilka program du har installerat och registrerat. Om du vill kan du när som helst leta efter uppdateringar även inom den här perioden. Medan SecurityCenter söker efter uppdateringar kan du fortsätta arbeta med annat.

Du kan ändra SecurityCenter-metoderna för sökning och installation av uppdateringar, men det är inget vi rekommenderar. Du kan exempelvis konfigurera SecurityCenter så att uppdateringar hämtas men inte installeras eller så att du får ett meddelande innan hämtning eller installation påbörjas. Du kan även inaktivera den automatiska uppdateringen.

Obs! Om du har installerat dina McAfee-program från en cd-skiva kan du inte ta emot regelbundna, automatiska uppdateringar av programmen förrän du registrerat dem på McAfees webbplats.

I detta kapitel

Söka efter uppdateringar

Som standard söker SecurityCenter automatiskt efter uppdateringar var fjärde timme när datorn är ansluten till Internet. Om du vill kan du söka efter uppdateringar inom den här fyratimmarsperioden. Om du inaktiverar funktionen för automatiska uppdateringar måste du själv regelbundet söka efter uppdateringar.

- Klicka på **Uppdatera** på Hem-panelen i SecurityCenter.

Tips: Du kan söka efter uppdateringar utan att starta SecurityCenter genom att högerklicka på SecurityCenter-ikonen i meddelandefältet längst till höger i aktivitetsfältet och sedan klicka på **Uppdateringar**.

Konfigurera automatiska uppdateringar

Som standard söker SecurityCenter automatiskt efter och installerar uppdateringar var fjärde timme när datorn är ansluten till Internet. Om du vill ändra standardinställningen kan du konfigurera SecurityCenter så att uppdateringar hämtas automatiskt och du får ett meddelande som talar om när de kan installeras eller så att du får ett meddelande innan uppdateringarna hämtas.

Obs! När uppdateringar kan hämtas eller installeras informeras du via ett meddelande i SecurityCenter. Från själva varningsmeddelandet kan du välja att hämta eller installera uppdateringarna eller att skjuta upp uppdateringen. När du uppdaterar program från ett sådant varningsmeddelande kan det hända att du måste verifiera din prenumeration innan du kan gå vidare. Mer information finns i avsnittet Arbeta med varningar (sida 23).

1 Öppna panelen Konfigurera SecurityCenter.

   Hur?

   1. Klicka på **Hem** under **Vanliga uppgifter**.
   2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.

2 Klicka på **På** under **Automatiska uppdateringar är inaktiverade** på panelen Konfigurera SecurityCenter och klicka sedan på **Avancerat**.

3 Klicka på någon av följande knappar:

   - **Installera uppdateringarna automatiskt och meddela mig när mina tjänster uppdateras (rekommenderas)**
   - **Hämta uppdateringarna automatiskt och meddela mig när de är klara att installeras**
   - **Meddela mig innan några uppdateringar hämtas**

4 Klicka på **OK**.

Inaktivera automatiska uppdateringar

Om du inaktiverar funktionen för automatiska uppdateringar ansvarar du själv för att regelbundet söka efter uppdateringar. Om du inte gör det kommer datorn inte att vara utrustad med det senaste skyddet. Mer information om hur du söker efter uppdateringar manuellt finns i Söka efter uppdateringar (sida 13).

1 Öppna panelen Konfigurera SecurityCenter.

   Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.

2 Klicka på **Av** under **Automatiska uppdateringar är aktiverade** på panelen Konfigurera SecurityCenter.

Tips: Du aktiverar automatiska uppdateringar genom att klicka på **På** eller genom att avmarkera **Inaktivera automatiska uppdateringar och låt mig kontrollera manuellt om det finns några uppdateringar** på panelen Uppdateringsalternativ.

KAPITEL 5

Åtgärda eller ignorera skyddsproblem

SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Allvarliga skyddsproblem måste åtgärdas omedelbart eftersom de påverkar din skyddsstatus, som ändras till röd. Mindre allvarliga problem behöver inte åtgärdas med en gång och det är inte säkert att de påverkar din skyddsstatus (beroende på vilken typ av problem det rör sig om). Om du vill uppnå grön skyddsstatus måste du åtgärda alla allvarliga problem och antingen åtgärda eller ignorera mindre allvarliga problem. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician. Mer information om McAfee Virtual Technician finns i hjälpen till McAfee Virtual Technician.

I detta kapitel

Åtgärda skyddsproblem

De flesta säkerhetsproblem åtgärdas automatiskt, men ibland måste du agera själv. Om exempelvis brandväggsskyddet inaktiveras kan SecurityCenter aktivera det automatiskt, men om brandväggsskyddet däremot inte installerats måste du installera det själv. I följande tabell beskrivs en del andra åtgärder som du kan vidta för att åtgärda skyddsproblem manuellt:

Problem	Åtgärd
En fullständig genomsökning av datorn har inte genomförts de senaste 30 dagarna.	Genomsök datorn manuellt. Mer information finns i hjälpen till VirusScan.
Dina avkänningssignaturfiler (DAT) är för gamla.	Uppdatera skyddet manuellt. Mer information finns i hjälpen till VirusScan.
Ett program har inte installerats.	Installera programmet från McAfees webbplats eller från en cd-skiva.
Ett program saknar komponenter.	Installera om programmet från McAfees webbplats eller från en cd-skiva.
Ett program har inte registrerats och kan därför inte skyddas helt.	Registrera programmet på McAfees webbplats.
Ett program har löpt ut.	Kontrollera kontostatus på McAfees webbplats.

Obs! Ett enskilt skyddsproblem påverkar ofta mer än en skyddskategori. När du åtgärdar det i en skyddskategori åtgärdas det i alla kategorier.

Åtgärda skyddsproblem automatiskt

SecurityCenter åtgärdar de flesta skyddsproblem automatiskt. De konfigurationsändringar som SecurityCenter utför vid automatiska åtgärder registreras inte i händelseloggen. Mer information om händelser finns i Visa händelser (sida 29).

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Åtgärda** i skyddsstatusfältet på Hem-panelen i SecurityCenter.

Åtgärda skyddsproblem manuellt

Om något problem kvarstår efter att du försökt åtgärda dem automatiskt kan du åtgärda det manuellt.

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på den skyddskategori på Hem-panelen i SecurityCenter där det rapporterade problemet finns.
3. Klicka på den länk som du hittar efter beskrivningen av problemet.

Ignorera skyddsproblem

Om SecurityCenter hittar ett mindre allvarligt problem kan du välja att åtgärda eller ignorera det. Vissa mindre allvarliga problem (som att Anti-Spam eller Privacy Service inte har installerats) ignoreras automatiskt. Problem som ignoreras visas inte i informationsfältet för skyddskategorin på Hem-panelen i SecurityCenter om inte datorns skyddsstatus är grön. Om du först ignorerar ett problem men senare vill att det ska visas i informationsfältet för skyddskategorin även om datorns skyddsstatus inte är grön kan du välja att visa det.

Ignorera ett skyddsproblem

Om SecurityCenter hittar ett mindre allvarligt problem som du inte vill åtgärda kan du välja att ignorera det. När du ignorerar ett problem tas det bort från informationsfältet för skyddskategorin i SecurityCenter.

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på den skyddskategori på Hem-panelen i SecurityCenter där det rapporterade problemet finns.
3. Klicka på länken **Ignorera** intill skyddsproblemet.

Visa eller dölja ignorerade problem

Du kan välja att visa eller dölja ett skyddsproblem beroende på hur allvarligt det är.

1. Öppna panelen Varningsalternativ.

   Hur?

   1. Klicka på **Hem** under **Vanliga uppgifter**.
   2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.
   3. Klicka på **Avancerat** under **Varningar**.
2. Klicka på **Ignorerade problem** på panelen Konfigurera SecurityCenter.
3. På panelen Ignorerade problem gör du följande:
   - Om du vill ignorera ett problem markerar du kryssrutan för problemet.
   - Om du vill rapportera ett problem i informationsfältet för skyddskategorin avmarkerar du kryssrutan för problemet.

4 Klicka på **OK**.

Tips: Du kan även ignorera ett problem genom att klicka på länken **Ignorera** intill det rapporterade problemet i informationsfältet för skyddskategorin.

KAPITEL 6

Arbeta med varningar

Varningar är små popup-fönster som visas längst ned i skärmens högra hörn när vissa SecurityCenter-händelser inträffar. En varning innehåller information om en händelse samt rekommendationer och alternativ som anger hur du kan åtgärda de problem som händelsen eventuellt medför. I vissa varningar finns dessutom länkar till mer information om händelsen. Med hjälp av de här länkarna kan du öppna McAfees globala webbplats eller skicka information till McAfee för felsökning.

Det finns tre typer av varningar: röd, gul och grön.

Varningstyp	Beskrivning
Röd	En röd varning är en viktig avisering som kräver en åtgärd från dig. Röda varningar inträffar när SecurityCenter inte kan avgöra hur ett skyddsproblem ska åtgärdas automatiskt.
Gul	En gul varning är en mindre viktig avisering som vanligen kräver en åtgärd från dig.
Grön	En grön varning är en mindre viktig avisering som inte kräver någon åtgärd från dig. Gröna varningar innehåller grundläggande information om en händelse.

Eftersom varningarna är så avgörande vid övervakning och hantering av skyddsstatus kan du inte inaktivera dem. Du kan däremot bestämma huruvida vissa typer av informationsvarningar ska visas samt konfigurera andra varningsalternativ (som att det ska höras en signal vid en varning eller att McAfees startbild ska visas vid start).

I detta kapitel

Dölja och visa informationsvarningar

Informationsvarningar anger att det inträffat något som inte hotar datorsäkerheten. Om du till exempel har installerat brandväggsskyddet visas en informationsvarning som standard varje gång något program i din dator beviljas åtkomst till Internet. Om du vill att en viss typ av informationsvarning inte ska visas kan du välja att dölja den. Om du inte vill att några informationsvarningar alls ska visas kan du välja att dölja alla. Du kan även dölja alla informationsvarningar när du spelar spel på datorn i helskärmsläge. När du spelat klart och lämnar helskärmsläget visas informationsvarningarna i SecurityCenter igen.

Om du döljer en informationsvarning av misstag kan du när som helst visa den igen. Som standard visas alla informationsvarningar i SecurityCenter.

Visa eller dölja informationsvarningar

Du kan konfigurera SecurityCenter så att vissa informationsvarningar visas och andra döljs eller så att alla informationsvarningar är dolda.

1 Öppna panelen Varningsalternativ.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.
3. Klicka på **Avancerat** under **Varningar**.

2 Klicka på **Informationsvarningar** på panelen Konfigurera SecurityCenter.

3 På panelen Informationsvarningar gör du följande:

- Om du vill att en informationsvarning ska visas avmarkerar du kryssrutan för den.
- Om du vill att en informationsvarning ska vara dold markerar du kryssrutan för den.
- Om du vill dölja alla informationsvarningar markerar du kryssrutan **Visa inga informationsvarningar**.

4 Klicka på **OK**.

Tips: Du kan även dölja en informationsvarning genom att markera kryssrutan **Visa inte den här varningen igen** i själva varningen. Om du väljer att göra det kan du visa informationsvarningen igen genom att avmarkera kryssrutan på panelen Informationsvarningar.

Visa eller dölja informationsvarningar när du spelar

När du spelar spel på datorn i helskärmsläge kan du välja att dölja alla informationsvarningar. När du spelat klart och lämnar helskärmsläget visas informationsvarningarna i SecurityCenter igen.

1 Öppna panelen Varningsalternativ.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.
3. Klicka på **Avancerat** under **Varningar**.

2 Markera eller avmarkera kryssrutan **Visa informationsvarningar när spelläge upptäcks** på panelen Varningsalternativ.

3 Klicka på **OK**.

Konfigurera varningsalternativ

Vilken typ av varningar som visas och hur ofta ställs in av SecurityCenter, men du kan ändra vissa grundläggande varningsalternativ. Du kan exempelvis välja att en signal ska höras vid en varning eller att startbilden inte ska visas när Windows startar. Du kan även dölja varningar som informerar om virusutbrott och andra säkerhetshot på Internet.

Signal vid varningar

Om du vill höra en ljudsignal när du tar emot en varning kan du konfigurera SecurityCenter så att ett ljud spelas upp vid varje varning.

1 Öppna panelen Varningsalternativ.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.
3. Klicka på **Avancerat** under **Varningar**.

2 Markera kryssrutan **Spela upp ett ljud vid varningar** under **Ljud** på panelen Varningsalternativ.

Visa inte startbilden vid start

Som standard visas McAfees startbild när du startar Windows, som ett tecken på att datorn skyddas med SecurityCenter. Om du däremot inte vill att den ska visas kan du dölja den.

1 Öppna panelen Varningsalternativ.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.
3. Klicka på **Avancerat** under **Varningar**.

2 Avmarkera kryssrutan **Visa McAfees startbild när Windows startas** under **Startbild** på panelen Varningsalternativ.

Tips: Du kan när som helst visa startbilden igen genom att markera kryssrutan **Visa McAfees startbild när Windows startas**.

Dölja varningar om virusutbrott

Du kan även dölja varningar som informerar om virusutbrott och andra säkerhetshot på Internet.

1 Öppna panelen Varningsalternativ.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Konfigurera** under **SecurityCenter – information** på den högra panelen.
3. Klicka på **Avancerat** under **Varningar**.

2 Markera kryssrutan **Varna mig vid virusutbrott och säkerhetshot** på panelen Varningsalternativ.

Tips: Du kan när som helst visa varningar om virusutbrott genom att markera kryssrutan **Varna mig vid virusutbrott och säkerhetshot**.

KAPITEL 7

Visa händelser

En händelse är en åtgärd eller konfigurationsändring som inträffar inom en skyddskategori eller dess relaterade skyddstjänster. Olika typer av händelser registreras för olika skyddstjänster. I SecurityCenter registreras en händelse om en skyddstjänst aktiveras eller inaktiveras, i antivirusskyddet registreras en händelse varje gång ett virus upptäcks eller åtgärdas och i brandväggsskyddet registreras en händelse varje gång ett försök att ansluta till Internet stoppas. Mer information om skyddskategorier finns i Introduktion till skyddskategorier (sida 9).

Du kan visa händelser vid felsökning av konfigurationsproblem samt när du granskar åtgärder som utförts av andra användare. Det är vanligt att föräldrar använder sig av händelseloggen för att skaffa sig insyn i barnens Internetanvändande. Om du vill granska aktuella händelser visar du de senaste 30 händelserna. Om du vill ha en utförlig lista över alla händelser som inträffat visar du alla händelser. När du visar alla händelser startas händelseloggen i SecurityCenter. Där sorteras händelser efter den skyddskategori de tillhör.

I detta kapitel

Visa de senaste händelserna

Om du vill granska aktuella händelser visar du de senaste 30 händelserna.

- Klicka på **Visa senaste händelser** under **Vanliga uppgifter**.

Visa alla händelser

Om du vill ha en utförlig lista över alla händelser som inträffat visar du alla händelser.

1. Klicka på **Visa senaste händelser** under **Vanliga uppgifter**.
2. I rutan De senaste händelserna klickar du på **Visa logg**.
3. Till vänster i händelseloggen klickar du på den typ av händelse som du vill visa.

KAPITEL 8

McAfee VirusScan

VirusScans avancerade tjänster för sökning och skydd försvarar dig och datorn mot de senaste säkerhetshoten, som virus, trojaner, spårningscookies, spionprogram, reklamprogram och andra oönskade program. Skyddet täcker mer än bara filer och mappar i datorn och upptäcker hot från olika ingångspunkter, som e-post, snabbmeddelanden och Internet.

Med VirusScan får du snabbt och konstant skydd för din dator (kräver ingen administration). Medan du arbetar, spelar spel, surfar på Internet eller läser e-post körs funktionen i bakgrunden, där den övervakar, söker efter och upptäcker potentiella säkerhetsrisker i realtid. Omfattande sökningar sker utifrån ett visst schema och datorn söks regelbundet igenom utifrån en uppsättning avancerade inställningar. Du kan ändra inställningarna i VirusScan om du vill anpassa skyddet, men även om du väljer att inte göra det är datorn alltid skyddad.

Vid normal datoranvändning kan virus, maskar och andra potentiella hot göra intrång i datorn. Om det skulle hända något skickas ett meddelande från VirusScan, men vanligen åtgärdas problemet automatiskt och infekterade objekt tas bort eller placeras i karantän innan det uppstår någon skada. I sällsynta fall måste du vidta ytterligare åtgärder. Då får du själv avgöra hur du vill gå vidare (göra en ny sökning nästa gång du startar om datorn, spara eller ta bort upptäckta objekt).

Obs! SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician.

I detta kapitel

Funktioner i VirusScan

VirusScan innehåller följande funktioner.

Omfattande virusskydd

VirusScans avancerade tjänster för sökning och skydd försvarar dig och datorn mot de senaste säkerhetshoten, som virus, trojaner, spårningscookies, spionprogram, reklamprogram och andra oönskade program. Skyddet täcker mer än bara filer och mappar i datorn och upptäcker hot från olika ingångspunkter, som e-post, snabbmeddelanden och Internet. Kräver ingen administration.

Resurskänsliga genomsökningsalternativ

Om du tycker att genomsökningen är långsam kan du inaktivera alternativet för att använda mindre av datorns resurser, men tänk på att virusskyddet kommer att prioriteras högre än andra åtgärder. Du kan ändra inställningarna i VirusScan om du vill anpassa alternativen för manuell genomsökning och genomsökning i realtid, men även om du väljer att inte göra det är datorn alltid skyddad.

Automatisk reparation

Om VirusScan upptäcker ett säkerhetshot vid en manuell genomsökning eller genomsökning i realtid försöker tjänsten åtgärda hotet automatiskt utifrån typen av hot. Det innebär att de flesta hot upptäcks och åtgärdas utan att du behöver ingripa. I sällsynta fall kan inte hotet åtgärdas automatiskt. Då får du själv avgöra hur du vill gå vidare (göra en ny sökning nästa gång du startar om datorn, spara eller ta bort upptäckta objekt).

Stoppa åtgärder när helskärmsläget används

När du till exempel tittar på film, spelar spel på datorn eller ägnar dig åt något annat som tar upp hela skärmen gör VirusScan en paus i ett antal åtgärder, däribland automatisk uppdatering och manuell genomsökning.

Aktivera realtidsvirusskyddet

VirusScan omfattar två typer av virusskydd: realtidsskydd och manuellt skydd. Realtidsvirusskyddet övervakar virusaktiviteten i datorn hela tiden och genomsöker filer varje gång de används. Med det manuella virusskyddet kan du genomsöka filer när du vill. Om du vill vara säker på att datorn alltid är skyddad mot de senaste säkerhetshoten bör du lämna realtidsvirusskyddet på och skapa ett schema för regelbundna och mer omfattande manuella genomsökningar. Som standard genomförs en schemalagd sökning per vecka i VirusScan. Mer information om realtidsgenomsökning och manuell genomsökning finns i Genomsökning av datorn (sida 57).

Det kan i sällsynta fall hända att du måste stänga av realtidsgenomsökningen tillfälligt, till exempel för att ändra vissa genomsökningsalternativ eller felsöka ett problem. När du gör det är inte datorn skyddad och skyddsstatus i SecurityCenter är röd. Mer information om skyddsstatus finns i Introduktion till skyddsstatus i hjälpen till SecurityCenter.

Aktivera realtidsvirusskyddet

Som standard är realtidsvirusskyddet aktiverat och skyddar datorn mot virus, trojaner och andra säkerhetshot. Om du av någon anledning stänger av det måste du aktivera det igen för att bibehålla skyddet.

1 Öppna panelen Dator- och filkonfiguration

   Hur?

   1. Klicka på **Avancerad meny** på den vänstra panelen.
   2. Klicka på **Konfigurera**.
   3. På panelen Konfigurera klickar du på **Dator och filer**.

2 Under **Virusskydd** klickar du på **På**.

Stänga av realtidsvirusskyddet

Du kan stänga av realtidsvirusskyddet tillfälligt och ange när det ska sätta igång igen. Du kan låta skyddet aktiveras igen efter 15, 30, 45 eller 60 minuter, vid omstart eller aldrig.

1 Öppna panelen Dator- och filkonfiguration

   Hur?

1. Klicka på **Avancerad meny** på den vänstra panelen.
2. Klicka på **Konfigurera**.
3. På panelen Konfigurera klickar du på **Dator och filer**.

2 Under **Virusskydd** klickar du på **Av**.

3 I dialogrutan anger du när realtidsgenomsökningen ska återupptas.

4 Klicka på **OK**.

KAPITEL 9

Aktivera extra skydd

Förutom realtidsvirusskydd omfattar VirusScan avancerat skydd mot skript, spionprogram och eventuellt skadliga bilagor till e-post och snabbmeddelanden. Skriptgenomsökning och skydd mot spionprogram, e-post och snabbmeddelanden är som standard aktiverade och skyddar datorn.

Skriptgenomsökning

Vid skriptgenomsökning spåras potentiellt skadliga skript så att de inte körs på datorn. Datorn övervakas och misstänkt skriptaktivitet noteras, till exempel om skript skapar, kopierar eller tar bort filer eller öppnar Windows-registret, och du får en varning innan det uppstår någon skada.

Skydd mot spionprogram

Skydd mot spionprogram används för att upptäcka spionprogram, reklamprogram och andra eventuellt oönskade program. Spionprogram är program som installeras på datorn utan att du vet om det för att sedan övervaka din datoranvändning och samla in personuppgifter. Ett spionprogram kan till och med påverka din kontroll över datorn genom att installera nya program eller styra om webbläsaren.

E-postskydd

E-postskydd används för att upptäcka misstänkt aktivitet i e-postmeddelanden och bilagor som du skickar och tar emot.

Snabbmeddelandeskydd

Snabbmeddelandeskydd används för att upptäcka potentiella säkerhetshot i bilagor till snabbmeddelanden som du tar emot. Det förhindrar även att snabbmeddelandeprogram delar ut personuppgifter.

I detta kapitel

Aktivera skriptgenomsökningsskyddet

Skriptgenomsökningsskyddet spårar potentiellt skadliga skript och förhindrar att de körs på datorn. Skriptgenomsökningsskyddet skickar varningar när ett skript försöker skapa, kopiera eller ta bort filer på datorn eller göra ändringar i Windows-registret.

1 Öppna panelen Dator- och filkonfiguration

   Hur?

   1. Klicka på **Avancerad meny** på den vänstra panelen.
   2. Klicka på **Konfigurera**.
   3. På panelen Konfigurera klickar du på **Dator och filer**.

2 Under **Skydd med skriptgenomsökning** klickar du på **På**.

Obs! Du kan visserligen när som helst stänga av skriptgenomsökningsskyddet, men om du gör det kan datorn utsättas för skadliga skript.

Aktivera spionprogramsskyddet

Aktivera spionprogramsskyddet om du vill hitta och ta bort spionprogram, reklamprogram och andra eventuellt oönskade program som samlar in och överför information utan att du vet om eller godkänner det.

1 Öppna panelen Dator- och filkonfiguration

   Hur?

   1. Klicka på **Avancerad meny** på den vänstra panelen.
   2. Klicka på **Konfigurera**.
   3. På panelen Konfigurera klickar du på **Dator och filer**.

2 Under **Skydd med skriptgenomsökning** klickar du på **På**.

Obs! Du kan visserligen när som helst stänga av spionprogramsskyddet, men om du gör det är datorn mottaglig för oönskade program.

Aktivera e-postskyddet

Du aktiverar e-postskyddet för att upptäcka maskar och andra potentiella hot i utgående (SMTP) och inkommande (POP3) e-postmeddelanden och bilagor.

1 Öppna panelen Konfigurering av e-post och snabbmeddelanden

   Hur?

1. Klicka på **Avancerad meny** på den vänstra panelen.
2. Klicka på **Konfigurera**.
3. På panelen Konfigurera klickar du på **E-post och snabbmeddelanden**.

2 Under **E-postskydd** klickar du på **På**.

Obs! Du kan visserligen när som helst stänga av e-postskyddet, men om du gör det är datorn mottaglig för e-posthot.

Aktivera snabbmeddelandeskyddet

Aktivera snabbmeddelandeskyddet för att upptäcka säkerhetshot som kan finnas i inkommande snabbmeddelandebilagor.

1 Öppna panelen Konfigurering av e-post och snabbmeddelanden

Hur?

1. Klicka på **Avancerad meny** på den vänstra panelen.
2. Klicka på **Konfigurera**.
3. På panelen Konfigurera klickar du på **E-post och snabbmeddelanden**.

2 Under **Snabbmeddelandeskydd** klickar du på **På**.

Obs! Du kan visserligen när som helst stänga av snabbmeddelandeskyddet, men om du gör det är datorn mottaglig för skadliga snabbmeddelandebilagor.

KAPITEL 10

Konfigurera virusskydd

VirusScan omfattar två typer av virusskydd: realtidsskydd och manuellt skydd. Realtidsvirusskyddet söker igenom filer varje gång du eller datorn använder dem. Med det manuella virusskyddet kan du genomsöka filer när du vill. Du kan ställa in olika alternativ för de två typerna av skydd. Eftersom realtidsskyddet övervakar datorn kontinuerligt kan du till exempel välja en uppsättning grundläggande genomsökningsalternativ för realtidsskyddet och skapa en mer omfattande uppsättning alternativ för det manuella skydd som utförs på din begäran.

I detta kapitel

Ställa in alternativ för realtidsgenomsökning

När du aktiverar realtidsvirusskyddet används en standarduppsättning med alternativ i VirusScan för genomsökning av filer, men du kan ändra inställningarna och anpassa sökningen efter dina behov.

Om du vill ändra alternativen för realtidsgenomsökning måste du bestämma vad VirusScan ska kontrollera vid en genomsökning samt var och i vilka filtyper genomsökningen ska ske. Du kan exempelvis bestämma om VirusScan ska leta efter okända virus eller cookies, som används av webbplatser för att spåra din användning, samt om du vill genomsöka nätverksenheter som är kopplade till din dator eller endast lokala enheter. Du kan dessutom bestämma vilka typer av filer som ska genomsökas – alla filer eller endast programfiler och dokument, där de flesta virus finns.

När du ändrar alternativen för realtidsgenomsökning måste du även avgöra om det är viktigt att datorn har ett skydd mot buffertspill. En buffert är en del av minnet som används för tillfällig lagring av datorinformation. Buffertspill kan uppstå när mängden information som misstänkta program eller processer försöker spara i en buffert överstiger buffertens kapacitet. Om det skulle inträffa blir datorn extra känslig för säkerhetsattacker.

Ställa in alternativ för realtidsgenomsökning

Du kan ställa in alternativ för realtidsgenomsökning och ange vad VirusScan ska kontrollera vid en realtidsgenomsökning samt var och i vilka filtyper sökningen ska ske. Det finns alternativ för sökning efter okända virus och spårningscookies samt för skydd mot buffertspill. Du kan även ange att du vid realtidsgenomsökningen vill kontrollera nätverksenheter som är kopplade till din dator.

1 Öppna panelen Realtidsgenomsökning.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Dator och filer** på Hem-panelen i SecurityCenter.
3. Klicka på **Konfigurera** i fältet Dator och filer.
4. Kontrollera att virusskyddet är aktiverat på panelen Dator- och filkonfiguration och klicka sedan på **Avancerat**.

2 Ställ in alternativen för realtidsgenomsökning och klicka på **OK**.

Om du vill..	Gör du så här...
Upptäcka okända virus och nya versioner av kända virus	Markera kryssrutan **Sök efter okända virus med hjälp av heuristik**.
Upptäcka cookies	Markera kryssrutan **Sök och ta bort spårningscookies**.
Upptäcka virus och andra potentiella hot på enheter anslutna till nätverket	Markera kryssrutan **Genomsök nätverksenheter**.
Skydda datorn mot buffertspill	Markera kryssrutan **Aktivera skydd mot buffertspill**.
Ange vilka filtyper som ska genomsökas	Klicka antingen på **Alla filer (rekommenderas)** eller **Endast programfiler och dokument**.

Ställa in alternativ för manuell genomsökning

Med det manuella virusskyddet kan du genomsöka filer när du vill. Vid en manuell sökning söker VirusScan igenom datorn och letar efter virus och andra potentiellt skadliga objekt med hjälp av en mer omfattande uppsättning alternativ för genomsökning. Om du vill ändra alternativen för manuell genomsökning måste du bestämma vad VirusScan ska kontrollera under sökningen. Du kan exempelvis bestämma om VirusScan ska leta efter okända virus, potentiellt oönskade program, som spionprogram eller reklamprogram, dolda program, som rootkit som kan ge obehörig åtkomst till din dator, eller cookies som webbplatser använder sig av för att spåra din användning. Du måste även bestämma vilka typer av filer som ska kontrolleras. Du kan exempelvis bestämma om VirusScan ska kontrollera alla filer eller endast programfiler och dokument, där de flesta virus finns. Du kan även bestämma om arkivfiler, som zip-filer, ska omfattas av sökningen.

Som standard genomsöker VirusScan alla enheter och mappar på datorn varje gång du kör en manuell genomsökning, men du kan anpassa sökningen utifrån just dina behov. Du kan till exempel välja att endast genomsöka viktiga systemfiler, objekt på skrivbordet eller objekt i mappen Programfiler. Om du inte själv vill ansvara för att starta den manuella genomsökningen kan du skapa ett schema för regelbunden sökning. Vid schemalagd genomsökning kontrolleras alltid hela datorn utifrån standardgenomsökningsalternativen. Som standard genomförs en schemalagd sökning per vecka i VirusScan.

Om du tycker att genomsökningen är långsam kan du inaktivera alternativet för att använda mindre av datorns resurser, men tänk på att virusskyddet kommer att prioriteras högre än andra åtgärder.

Obs! När du till exempel tittar på film, spelar spel på datorn eller ägnar dig åt något annat som tar upp hela skärmen gör VirusScan en paus i ett antal åtgärder, däribland automatisk uppdatering och manuell genomsökning.

Ställa in alternativ för manuell genomsökning

Du kan ställa in alternativ för manuell genomsökning och ange vad VirusScan ska kontrollera vid en manuell genomsökning samt var och i vilka filtyper sökningen ska ske. Du kan bland annat välja att söka efter okända virus, filarkiv, spionprogram och potentiellt oönskade program, spårningscookies, rootkit och dolda program.

1 Öppna panelen Manuell genomsökning.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Dator och filer** på Hem-panelen i SecurityCenter.
3. Klicka på **Konfigurera** i fältet Dator och filer.
4. Kontrollera att virusskyddet är aktiverat på panelen Dator- och filkonfiguration och klicka sedan på **Avancerat**.
5. Klicka på **Manuell genomsökning** i rutan Virusskydd.

2 Ställ in alternativen för manuell genomsökning och klicka på **OK**.

Om du vill..	Gör du så här...
Upptäcka okända virus och nya versioner av kända virus	Markera kryssrutan **Sök efter okända virus med hjälp av heuristik**.
Upptäcka och ta bort virus i zip-filer och andra arkivfiler	Markera kryssrutan **Genomsök .zip-filer och andra arkivfiler**.
Upptäcka spionprogram, reklamprogram och andra eventuellt oönskade program	Markera kryssrutan **Sök efter spionprogram och eventuellt oönskade program**.
Upptäcka cookies	Markera kryssrutan **Sök och ta bort spårningscookies**.
Upptäcka rootkit och dolda program som kan förändra och utnyttja befintliga Windows-systemfiler	Markera kryssrutan **Sök efter rootkit och andra dolda program**.
Använda mindre processorkraft vid genomsökning och prioritera andra åtgärder högre (som att surfa på nätet och öppna dokument)	Markera kryssrutan **Använd mindre av datorns resurser vid genomsökning**.
Ange vilka filtyper som ska genomsökas	Klicka antingen på **Alla filer (rekommenderas)** eller **Endast programfiler och dokument**.

Ställa in område för manuell genomsökning

Ställ in det område där VirusScan ska leta efter virus och andra skadliga objekt vid en manuell genomsökning. Du kan välja att genomsöka alla filer, mappar och enheter på datorn eller begränsa genomsökningen till specifika mappar eller enheter.

1 Öppna panelen Manuell genomsökning.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Dator och filer** på Hem-panelen i SecurityCenter.
3. Klicka på **Konfigurera** i fältet Dator och filer.
4. Kontrollera att virusskyddet är aktiverat på panelen Dator- och filkonfiguration och klicka sedan på **Avancerat**.
5. Klicka på **Manuell genomsökning** i rutan Virusskydd.

2 Klicka på **Standardplats för genomsökning**.

3 Ställ in område för manuell genomsökning och klicka på **OK**.

Om du vill..	Gör du så här...
Söka igenom alla filer och mappar på datorn	Markera kryssrutan **(Den här) datorn**.
Söka igenom specifika filer, mappar och enheter på datorn	Avmarkera kryssrutan **(Den här) datorn** och välj minst en mapp eller enhet.
Genomsöka viktiga systemfiler	Avmarkera kryssrutan **(Den här) datorn** och markera kryssrutan **Viktiga systemfiler**.

Schemalägga genomsökning

Du kan schemalägga genomsökningar och söka igenom datorn ordentligt efter virus och andra hot när du vill. Vid schemalagd genomsökning kontrolleras alltid hela datorn utifrån standardgenomsökningsalternativen. Som standard genomförs en schemalagd sökning per vecka i VirusScan. Om du tycker att genomsökningen är långsam kan du inaktivera alternativet för att använda mindre av datorns resurser, men tänk på att virusskyddet kommer att prioriteras högre än andra åtgärder.

1 Öppna panelen Schemalagd genomsökning.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Dator och filer** på Hem-panelen i SecurityCenter.
3. Klicka på **Konfigurera** i fältet Dator och filer.
4. Kontrollera att virusskyddet är aktiverat på panelen Dator- och filkonfiguration och klicka sedan på **Avancerat**.
5. Klicka på **Schemalagd genomsökning** i rutan Virusskydd.

2 Välj **Aktivera schemalagd genomsökning**.

3 Om du vill begränsa den processorkraft som vanligtvis går åt vid genomsökning markerar du **Använd mindre av datorns resurser vid genomsökning**.

4 Välj en eller flera dagar för sökningen.

5 Ange starttid.

6 Klicka på **OK**.

Tips: Du kan återställa standardschemat genom att klicka på **Återställ**.

Använda SystemGuards-alternativ

SystemGuards övervakar, loggar, rapporterar och hanterar potentiellt obehöriga ändringar i Windows-registret och viktigt systemfiler på datorn. Obehöriga register- och filändringar kan skada datorn, hota säkerheten och skada viktiga systemfiler.

Register- och filändringar är vanligt förekommande och inträffar ofta. Eftersom många av dem är oskadliga är SystemGuard som standard konfigurerat för att erbjuda tillförlitligt, smart och realistiskt skydd mot obehöriga ändringar som utgör ett påtagligt hot. När SystemGuards upptäcker ovanliga ändringar som utgör ett potentiellt påtagligt hot rapporteras och loggas därför aktiviteten. Ändringar som är mer vanligt förekommande, men som ändå utgör ett visst hot, loggas bara. Övervakning och spårning av standardändringar och ändringar med låg riskfaktor är som standard inaktiverat. SystemGuards-tekniken kan konfigureras så att skyddet omfattar de miljöer du vill skydda.

Det finns tre versioner av SystemGuards: Program SystemGuards, Windows SystemGuards och Browser SystemGuards.

Program SystemGuards

Program SystemGuards upptäcker potentiellt obehöriga ändringar i datorns registerfiler och andra viktiga filer i Windows. Bland viktiga registerobjekt och filer ingår ActiveX-installationer, startobjekt, skalkörningskrokar för Windows och Shell Service Object Delay Load. Genom att övervaka dessa med hjälp av Program SystemGuards-tekniken kan du stoppa misstänkta ActiveX-program (som hämtas från Internet) samt spionprogram och eventuellt oönskade program som kan starta automatiskt när du startar Windows.

Windows SystemGuards

Även Windows SystemGuards upptäcker potentiellt obehöriga ändringar i datorns registerfiler och andra viktiga filer i Windows. Bland viktiga registerobjekt och filer ingår hanterare för snabbmenyer, appInit DLL-filer samt Windows Hosts-filen. Genom att övervaka dessa med hjälp av Windows SystemGuards-tekniken kan du förhindra att datorn skickar och tar emot obehörig information eller personuppgifter via Internet. Det hindrar dessutom misstänkta program som kan medföra oönskade ändringar i utseende och beteende hos de program som du och din familj använder mycket.

Browser SystemGuards

Precis som Program och Windows SystemGuards upptäcker Browser SystemGuards potentiellt obehöriga ändringar i datorns registerfiler och andra viktiga filer i Windows. Utöver det övervakar Browser SystemGuards ändringar i viktiga registerobjekt och filer, som tilläggsmoduler för Internet Explorer, URL-adresser i Internet Explorer och Internet Explorers säkerhetszoner. Genom att övervaka dessa med hjälp av Browser SystemGuards-tekniken kan du förhindra obehörig webbläsaraktivitet, som styrning till misstänkta webbplatser, ändringar av webbläsarinställningar och alternativ utan att du vet om det samt oönskat förtroende för misstänkta webbplatser.

Aktivera SystemGuards-skydd

När du aktiverar SystemGuards-skyddet upptäcker det och skickar varningar om potentiellt obehöriga ändringar av Windows-register och filer på datorn. Obehöriga register- och filändringar kan skada datorn, hota säkerheten och skada viktiga systemfiler.

1 Öppna panelen Dator- och filkonfiguration

Hur?

1. Klicka på **Avancerad meny** på den vänstra panelen.
2. Klicka på **Konfigurera**.
3. På panelen Konfigurera klickar du på **Dator och filer**.

2 Under **SystemGuard-skydd** klickar du på **På**.

Obs! Du inaktiverar SystemGuard-skyddet genom att klicka på **Av**.

Konfigurera SystemGuards-alternativ

På panelen SystemGuards kan du ställa in alternativ för skydd, loggning och varningar om obehöriga ändringar av register och filer i Windows-filer, program och Internet Explorer. Obehöriga register- och filändringar kan skada datorn, hota säkerheten och skada viktiga systemfiler.

1 Öppna panelen SystemGuards.

   Hur?

   1. Klicka på **Hem** under **Vanliga uppgifter**.
   2. Klicka på **Dator och filer** på Hem-panelen i SecurityCenter.
   3. Klicka på **Konfigurera** i fältet Dator och filer.
   4. Kontrollera att SystemGuard-skyddet är aktiverat på panelen Dator- och filkonfiguration och klicka sedan på **Avancerat**.

2 Välj en SystemGuard-typ på listan.

   - **Program SystemGuards**
   - **Windows SystemGuards**
   - **Browser SystemGuards**

3 Under **Jag vill** väljer du något av följande alternativ:

   - Upptäcka, logga och rapportera obehöriga register- och filändringar som associeras med Program, Windows och Browsers SystemGuards – klicka på **Visa varningar**.
   - Upptäcka och logga obehöriga register- och filändringar som associeras med Program, Windows och Browsers SystemGuards – klicka på **Logga bara ändringar**.
   - Inaktivera avkänning av obehöriga register- och filändringar som associeras med Program, Windows och Browsers SystemGuards – klicka på **Inaktivera SystemGuard**.

Obs! Mer information om SystemGuards-typer hittar du i Om SystemGuards-typer (sida 49).

Om SystemGuards-typer

SystemGuards upptäcker eventuella otillåtna ändringar av datorns registerfiler och andra viktiga filer som är nödvändiga för Windows. Det finns tre versioner av SystemGuards: Program SystemGuards, Windows SystemGuards och Browser SystemGuards.

Program SystemGuards

Med hjälp av tekniken i Programmet SystemGuards stoppas misstänkta ActiveX-program (hämtade från Internet) förutom spionprogram och eventuellt oönskade program som startar automatiskt när Windows startas.

SystemGuard	Upptäcker ...
ActiveX-installationer	Obehöriga register- och filändringar i ActiveX-installationer som kan skada datorn, hota säkerheten och skada viktiga systemfiler.
Startobjekt	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan installera filändringar i startobjekt, vilket medför att misstänkta program kan köras när du startar datorn.
Hook-program i Windows-skalet	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan installera Windows-hook-program för att förhindra att säkerhetsprogram körs.
Shell Service Object Delay Load	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan utföra registerändringar i Shell Service Object Delay Load, vilket medför att skadliga filer kan köras när du startar datorn.

Windows SystemGuards

Med hjälp av tekniken i Windows SystemGuards hindras datorn från att skicka och ta emot obehörig eller personlig information på Internet. Det hindrar dessutom misstänkta program som kan medföra oönskade ändringar i utseende och beteende hos de program som du och din familj använder mycket.

SystemGuard	Upptäcker ...
Hanterare för snabbmenyer	Obehöriga registerändringar i Windows-hanterare för snabbmenyer, som kan påverka utseende och beteende hos Windows-menyer. Med hjälp av snabbmenyer kan du utföra åtgärder på datorn, som att högerklicka på filer.
AppInit DLL-filer	Obehöriga registerändringar i Windows appInit DLL-filer som gör att potentiellt skadliga filer kan köras när du startar datorn.

Windows Hosts-fil	Spionprogram, reklamprogram och eventuellt oönskade program som kan utföra obehöriga ändringar i Windows Hosts-filen, vilket innebär att webbläsaren kan styras om till misstänkta webbplatser och att programuppdateringar stoppas.
Winlogon-skal	Spionprogram, reklamprogram och eventuellt oönskade program som kan utföra registerändringar i Winlogon-skalet, vilket innebär att andra program kan ersätta Windows Explorer.
Användarinitiering vid Windowsinloggning	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan göra registerändringar i användarinitiering vid Windowsinloggning, vilket medför att misstänkta program kan köras när du loggar in i Windows.
Windows-protokoll	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan göra registerändringar i Windows-protokoll, vilket påverkar hur datorn skickar och tar emot information på Internet.
Winsock Layered Service Providers	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan installera registerändringar i Winsock LSP:er (Layered Service Provider) för att komma åt och ändra information som du skickar och tar emot via Internet.
Kommandon för öppning för Windows-skal	Obehöriga ändringar av kommandon för öppning för Windows-skal, som gör att maskar och andra skadliga program kan köras på datorn.
Schemaläggare för delade aktiviteter	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan utföra register- och filändringar i schemaläggare för delade aktiviteter, vilket medför att potentiellt skadliga filer kan köras när du startar datorn.
Windows Messenger Service	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan utföra registerändringar i Windows meddelandetjänst, vilket medför att oönskade annonser och fjärrstyrda program kan köras på datorn.
Windows Win.ini-filen	Spionprogram, reklamprogram och andra eventuellt oönskade program som kan införa ändringar i Win.ini-filen, vilket medför att misstänkta program kan köras när du startar datorn.

Browser SystemGuards

Med hjälp av tekniken i Browser SystemGuards förhindras obehörig webbläsaraktivitet, t.ex. att du omdirigeras till misstänkta webbplatser, att inställningar och alternativ för webbläsaren ändras utan din vetskap och att misstänkta webbplatser utan ditt godkännande ses som tillförlitliga.

SystemGuard	Upptäcker ...
Browser Helper Objects	Spionprogram, annonsprogram och andra potentiellt oönskade program som kan använda webbläsarobjekt för att spåra surfvanor på nätet och visa oönskad reklam.
Internet Explorer Bars	Obehöriga registerändringar i Internet Explorer Bar-program, t.ex. Sök och Favoriter, kan påverka Internet Explorers utseende och funktioner.
Internet Explorer-tillägg	Spionprogram, annonsprogram och andra potentiellt oönskade program som kan installera Internet Explorer-tillägg för att spåra surfvanor på nätet och visa oönskad reklam.
Internet Explorer ShellBrowser	Obehöriga registerändringar i Internet Explorer ShellBrowser kan påverka webbläsarens utseende och funktioner.
Internet Explorer WebBrowser	Obehöriga registerändringar i Internet Explorer WebBrowser kan påverka webbläsarens utseende och funktioner.
Hooks för URL-sökning i Internet Explorer	Spionprogram, annonsprogram och andra potentiellt oönskade program som kan göra registerändringar i Hooks för URL-sökning i Internet Explorer, så att webbläsaren omdirigeras till misstänkta webbplatser när du söker på nätet.
Internet Explorer URL:er	Spionprogram, annonsprogram och andra potentiellt oönskade program som kan göra registerändringar i Internet Explorer-webbadresser som påverkar webbläsarens inställningar.
Internet Explorer-begränsningar	Spionprogram, annonsprogram och andra potentiellt oönskade program som kan göra registerändringar i Internet Explorer-begränsningar som påverkar webbläsarens inställningar och alternativ.
Säkerhetszoner för Internet Explorer	Spionprogram, annonsprogram och andra potentiellt oönskade program som kan göra registerändringar i säkerhetszonerna för Internet Explorer så att skadliga filer kan köras när du startar datorn.

Tillförlitliga platser i Internet Explorer	Spionprogram, annonsprogram och andra potentiellt oönskade program som kan göra registerändringar i Tillförlitliga platser i Internet Explorer, så att webbläsaren litar på misstänkta webbplatser.
Internet Explorer-princip	Spionprogram, annonsprogram och andra potentiellt oönskade program kan göra registerändringar i Internet Explorer-principer, som påverkar webbläsarens utseende och funktioner.

Använda listor med tillförlitliga objekt

Om du kör VirusScan och en fil- eller en registerändring (SystemGuard), ett program eller ett buffertspill upptäcks uppmanas du att ange det som tillförlitligt eller ta bort det. Om du anser att objektet är tillförlitligt och anger att du inte vill få fler meddelanden om dess aktiviteter läggs objektet till i en lista med tillförlitliga objekt. Då upptäcks det inte längre när du kör VirusScan och du får inga meddelanden om dess aktiviteter. Om ett objekt har lagts till i en lista med tillförlitliga objekt kan du ändå välja att blockera dess aktivitet. Om du blockerar ett objekt kan det inte köras eller göra några ändringar på datorn utan att du meddelas vid varje försök. Du kan också ta bort det från listan med tillförlitliga objekt. Om du tar bort objektet kan dess aktivitet återigen upptäckas när du kör VirusScan.

Hantera listor med tillförlitliga objekt

Använd fönstret Listor med tillförlitliga objekt när du vill ange objekt som tillförlitliga eller blockera objekt som tidigare upptäckts och angetts som tillförlitliga. Du kan också ta bort det från listan med tillförlitliga objekt så att det återigen kan upptäckas när du kör VirusScan.

1 Öppna fönstret Listor med tillförlitliga objekt.

Hur?

1. Klicka på **Hem** under **Vanliga uppgifter**.
2. Klicka på **Dator och filer** på Hem-panelen i SecurityCenter.
3. Klicka på **Konfigurera** i fältet Dator och filer.
4. Kontrollera att virusskyddet är aktiverat på panelen Dator- och filkonfiguration och klicka sedan på **Avancerat**.
5. Klicka på **Listor med tillförlitliga objekt** i rutan Virusskydd.

2 Välj någon av följande listor med tillförlitliga objekt:

- **Program SystemGuards**
- **Windows SystemGuards**
- **Browser SystemGuards**
- **Betrodda program**
- **Betrodda buffertspill**

3 Under **Jag vill** väljer du något av följande alternativ:

- Om du vill tillåta att dett upptäckta objektet gör ändringar i Windows register eller viktiga systemfiler på datorn utan att du meddelas, klicka på **Lita på**.

- Om du vill blockera det upptäckta objektet så att inga ändringar kan göras i Windows register eller viktiga systemfiler på datorn utan att du meddelas, klicka på **Blockera**.
- Om du vill ta du bort det upptäckta objektet från listorna med tillförlitliga objekt klickar du på **Ta bort**.

4 Klicka på **OK**.

Obs! Mer information om olika listor med tillförlitliga objekt hittar du i Om olika listor med tillförlitliga objekt (sida 54).

Om olika listor med tillförlitliga objekt

I SystemGuards i fönstret Listor med tillförlitliga objekt visas tidigare obehöriga register- och filändringar som har upptäckts när du kört VirusScan, men som du efter en varning eller från panelen Resultat av genomsökning har valt att tillåta. Det finns fem olika listor med tillförlitliga objekt som du kan hantera i fönstret Listor med tillförlitliga objekt: Programmet SystemGuards, Windows SystemGuards, Browser SystemGuards, Betrodda program och Betrodda buffertspill.

Alternativ	Beskrivning
Program SystemGuards	I Program SystemGuards i fönstret Listor med tillförlitliga objekt visas tidigare obehöriga register- och filändringar som har upptäckts när du kört VirusScan, men som du efter en varning eller från panelen Resultat av genomsökning har valt att tillåta. Med hjälp av Programmet SystemGuards upptäcks obehöriga register- och filändringar som har att göra med ActiveX-installationer, startobjekt, hook-program i Windows-skalet och aktiviteter i Shell Service Object Delay Load. Dessa typer av obehöriga register- och filändringar kan skada datorn, äventyra säkerheten och skada viktiga systemfiler.
Windows SystemGuards	I Windows SystemGuards i fönstret Listor med tillförlitliga objekt visas tidigare obehöriga register- och filändringar som har upptäckts när du kört VirusScan, men som du efter en varning eller från panelen Resultat av genomsökning har valt att tillåta. Med hjälp av Windows SystemGuards upptäcks obehöriga register- och filändringar som har att göra med hanterare för snabbmenyer, appInit DLL-filer, hosts-filen i Windows, Winlogon-skalet, LSP (Winsock Layered Service Providers) m.m. Dessa typer av obehöriga register- och filändringar kan påverka hur datorn skickar och tar emot information på Internet, ändra programs utseende och funktioner och tillåta att misstänkta program körs på datorn.

Browser SystemGuards	I Browser SystemGuards i fönstret Listor med tillförlitliga objekt visas tidigare obehöriga register- och filändringar som har upptäckts när du kört VirusScan, men som du efter en varning eller från panelen Resultat av genomsökning har valt att tillåta. Med hjälp av Browser SystemGuards upptäcks obehöriga registerändringar och annat oönskat beteendede som har att göra med webbläsarobjekt, Internet Explorer-tillägg, Internet Explorer-webbadresser, säkerhetszoner i Internet Explorer m.m. Dessa typer av obehöriga registerändringar kan leda till oönskad webbläsaraktivitet, t.ex. att du omdirigeras till misstänkta webbplatser, att inställningar och alternativ för webbläsaren ändras och att misstänkta webbplatser ses som tillförlitliga.
Betrodda program	Betrodda program är eventuellt oönskade program som har upptäckts när du kört VirusScan, men som du efter en varning eller från panelen Resultat av genomsökning har valt att tillåta.
Betrodda buffertspill	Betrodda buffertspill är oönskade aktiviteter som har upptäckts när du kört VirusScan, men som du efter en varning eller från panelen Resultat av genomsökning har valt att tillåta. Buffertspill kan skada datorn och förstöra filer. Buffertspill inträffar när mängden information som misstänkta program eller processer lagrar i en buffert överskrider buffertens kapacitet.

KAPITEL 11

Genomsökning av datorn

Från dess att du startar SecurityCenter första gången skyddas datorn från skadliga virus, trojaner och andra säkerhetshot med hjälp av VirusScans realtidsvirusskydd. Om du inte inaktiverar realtidsvirusskyddet övervakas datorn konstant och genomsöks efter virusaktivitet med hjälp av VirusScan. Varje gång du eller datorn använder filer söks de igenom med det alternativ för realtidsgenomsökning som du valt. För att försäkra dig om att datorn är skyddad mot de senaste säkerhetshoten bör du ha realtidsvirusskyddet aktiverat och göra upp ett schema för regelbundna, mer heltäckande manuella genomsökningar. Mer information om hur du konfigurerar alternativ för realtidsgenomsökningar och manuella genomsökningar finns i Konfigurera virusskydd (sida 39).

I VirusScan finns mer detaljerade genomsökningsalternativ för manuellt virusskydd. Det gör att du med jämna mellanrum kan göra mer omfattande genomsökningar. Från SecurityCenter kan du göra manuella genomsökningar av specifika platser enligt ett schema. Du kan också göra manuella genomsökningar direkt i Utforskaren när du arbetar. Fördelen med genomsökningar i SecurityCenter är att du snabbt kan ändra genomsökningsalternativen. Genomsökningar från Utforskaren är dock ett praktiskt sätt att få datorsäkerhet.

Oavsett om du gör manuella genomsökningar från SecurityCenter eller Utforskaren kan du visa resultatet av genomsökningen när den är färdig. Du visar resultatet av en genomsökning med VirusScan för att avgöra om virus, trojaner, spionprogram, reklamprogram, cookies och andra eventuellt oönskade program har upptäckts, reparerats eller satts i karantän. Resultatet av en genomsökning kan visas på olika sätt. Du kan till exempel visa en grundlägande sammanfattning av genomsökningen eller visa detaljerad information, som infektionens status och typ. Du kan också visa allmän statistik för genomsökningar och upptäckter.

I detta kapitel

Genomsök datorn

Du kan göra manuella genomsökningar från antingen Avancerad meny eller Grundläggande meny i SecurityCenter. Från Avancerad meny har du möjlighet att bekräfta alternativen för manuella genomsökningar innan du startar genomsökningen. Från Grundläggande meny startas genomsökningen med VirusScan omedelbart, med de befintliga genomsökningsalternativen. Du kan också göra en genomsökning i Utforskaren med de befintliga genomsökningsalternativen.

- Välj någon av de följande åtgärderna:

  Genomsök i SecurityCenter

Om du vill..	Gör du så här...
Genomsöka med befintliga inställningar	Klicka på **Genomsök** på Grundläggande meny.
Genomsöka med ändrade inställningar	Klicka på **Genomsök** på Avancerad meny. Markera platser för genomsökning, välj genomsökningsalternativ och klicka på **Genomsök nu**.

  Genomsök i Utforskaren

  1. Öppna Utforskaren.
  2. Högerklicka på en fil, mapp eller enhet och klicka sedan på **Genomsök**.

Obs! Resultatet av genomsökningen visas i meddelandet Genomsökning slutförd. I resultatet kan du se antal objekt som genomsökts, upptäckts, reparerats, satts i karantän och tagits bort. Klicka på **Visa sökinformation** om du vill läsa mer om resultat av genomsökningen eller arbeta med infekterade objekt.

Visa resultat av genomsökning

När en manuell genomsökning är färdig kan du visa resultaten för att se vad som upptäckts under genomsökningen och utvärdera datorns aktuella skyddsstatus. I resultatet av genomsökningen med VirusScan ser du om virus, trojaner, spionprogram, reklamprogram, cookies och andra eventuellt oönskade program har upptäckts, reparerats eller satts i karantän.

- Klicka på **Genomsök** i Grundläggande meny eller Avancerad meny och gör något av följande:

Om du vill..	Gör du så här...
Visa resultat av genomsökning i varningen	Visa resultat av genomsökning i meddelandet Genomsökning slutförd.
Visa mer information om resultatet av genomsökningen	Klicka på **Visa sökinformation** i meddelandet Genomsökning slutförd.
Visa en snabbsammanfattning av resultatet av genomsökningen	Peka på **ikonen Genomsökning slutförd** i Aktivitetsfältets meddelandefält.
Visa statistik för genomsökningar och upptäckter	Dubbelklicka på ikonen **Genomsökning slutförd** i Aktivitetsfältets meddelandefält.
Visa information om upptäckta objekt, infektionsstatus och typ.	Dubbelklicka på ikonen **Genomsökning slutförd** i Aktivitetsfältets meddelandefält. Klicka sedan på **Visa resultat** i panelen Genomsökning – förlopp: Manuell genomsökning.

KAPITEL 12

Arbeta med resultat av genomsökning

Om VirusScan upptäcker ett säkerhetshot vid en manuell genomsökning eller genomsökning i realtid försöker tjänsten åtgärda hotet automatiskt utifrån typen av hot. Om VirusScan hittar t.ex. ett virus, en trojan eller en spårningscookie på din dator försöker programmet rensa den infekterade filen. Om filen inte kan rensas av VirusScan placerar programmet den i karantän.

Vissa säkerhetshot kan inte rensas eller placeras i karantän av VirusScan. I så fall får du en uppmaning från VirusScan att hantera hotet. Du kan vidta flera olika åtgärder beroende på vilken typ av hot det rör sig om. Om ett virus upptäcks i en fil och den inte kan rensas eller placeras i karantän av VirusScan, nekas åtkomst till den filen. Om spårningscookies upptäcks och de inte kan rensas eller placeras i karantän av VirusScan avgör du själv om du vill ta bort dem eller lita på dem. Om eventuellt oönskade program upptäcks vidtas ingen automatisk åtgärd av VirusScan utan du får själv avgöra om du vill placera programmet i karantän eller lita på det.

När objekt placeras i karantän av VirusScan krypteras de och isoleras sedan i en mapp för att förhindra att filerna, programmen eller cookie-filerna skadar din dator. Objekt som placerats i karantän kan återställas eller tas bort. I de flesta fall kan du ta bort en cookie som placerats i karantän utan att det påverkar din dator. Om ett program som du känner igen och använder har placerats i karantän av VirusScan bör du dock återställa det.

I detta kapitel

Arbeta med virus och trojaner

Om VirusScan hittar ett virus eller en trojan i en fil på din dator under en genomsökning i realtid försöker programmet rensa filen. Om filen inte kan rensas av VirusScan försöker programmet placera den i karantän. Om det också misslyckas nekas åtkomst till filen (endast vid genomsökningar i realtid).

1 Öppna panelen Resultat av genomsökning.

Hur?

1. Dubbelklicka på ikonen **Genomsökning slutförd** i meddelandefältet längst till höger på aktivitetsfältet.
2. Klicka på **Visa resultat** i panelen Genomsökning – förlopp, under Manuell genomsökning.

2 Klicka på **Virus och trojaner** i listan med resultat av genomsökningen.

Obs! Information om hur du kan arbeta med de filer som har placerats i karantän av VirusScan finns i Arbeta med filer i karantän (sida 62).

Arbeta med eventuellt oönskade program

Om VirusScan upptäcker ett eventuellt oönskat program på din dator under en genomsökning i realtid eller en manuell genomsökning, kan du antingen ta bort det eller lita på det. Om du tar bort det eventuellt oönskade programmet raderas det egentligen inte från din dator. Men om du tar bort programmet förhindras det att skada din dator eller dina filer.

1 Öppna panelen Resultat av genomsökning.

Hur?

1. Dubbelklicka på ikonen **Genomsökning slutförd** i meddelandefältet längst till höger på aktivitetsfältet.
2. Klicka på **Visa resultat** i panelen Genomsökning – förlopp, under Manuell genomsökning.

2 Klicka på **Eventuellt oönskade program** i listan med resultat av genomsökningen.

3 Välj ett eventuellt oönskat program.

4 Klicka på **Ta bort** eller **Lita på** under **Jag vill**.

5 Bekräfta det alternativ du valt.

Arbeta med filer i karantän

När filer placeras i karantän av VirusScan krypteras de och flyttas sedan till en mapp för att förhindra att de skadar din dator. Objekt som placerats i karantän kan återställas eller tas bort i efterhand.

1 Öppna panelen Filer i karantän.

Hur?

1. Klicka på **Avancerad meny** på den vänstra panelen.
2. Klicka på **Återställ**.
3. Klicka på **Filer**.

2 Välj en fil i karantän.

3 Välj någon av de följande åtgärderna:

- Klicka på **Återställ** om du vill reparera den infekterade filen och återställa den till dess ursprungliga plats på datorn.
- Klicka på **Ta bort** om du vill ta bort den infekterade filen från datorn.

4 Bekräfta ditt val genom att klicka på **Ja**.

Tips: Du kan återställa eller ta bort flera filer samtidigt.

Arbeta med program och cookies i karantän

När potentiellt oönskade program eller spårningscookies placeras i karantän av VirusScan krypteras de och flyttas sedan till en skyddad mapp för att förhindra att de skadar din dator. Objekt som placerats i karantän kan återställas eller tas bort i efterhand. I de flesta fall kan du ta bort ett objekt i karantän utan att det påverkar din dator.

1 Öppna panelen Program och spårningscookies i karantän

Hur?

1. Klicka på **Avancerad meny** på den vänstra panelen.
2. Klicka på **Återställ**.
3. Klicka på **Program och cookies**.

2 Markera ett program eller en cookie i karantän.

3 Välj någon av de följande åtgärderna:

- Klicka på **Återställ** om du vill reparera den infekterade filen och återställa den till dess ursprungliga plats på datorn.
- Klicka på **Ta bort** om du vill ta bort den infekterade filen från datorn.

4 Bekräfta ditt val genom att klicka på **Ja**.

Tips: Du kan återställa eller ta bort flera program och cookies samtidigt.

KAPITEL 13

McAfee Personal Firewall

Personal Firewall ger avancerat skydd för din dator och dina personuppgifter. Personal Firewall upprättar en spärr mellan datorn och Internet samt övervakar diskret Internet-trafiken för att komma åt misstänkt aktivitet.

Obs! SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician.

I detta kapitel

Funktioner i Personal Firewall

Personal Firewall erbjuder följande funktioner.

Standard och anpassad skyddsnivå

Skydda emot intrång och misstänkt aktivitet med Firewalls standardinställningar eller anpassade skyddsinställningar.

Realtidsrekommendationer

Du kan dynamiskt få rekommendationer som kan hjälpa dig att välja huruvida program ska få tillgång till Internet eller om nätverkstrafik ska anses vara tillförlitlig.

Intelligent tillgångshantering för program

Hantera Internettillgång för program genom varningar och händelseloggar, eller konfigurera tillgångsnivåer för specifika program.

Spelskydd

Förhindrar att varningar om intrång och andra misstänkta aktiviteter stör medan du spelar i helskärmsläge.

Skydd vid datorstart

Så snart Windows startar skyddar Firewall din dator från intrångsförsök, oönskade program och nätverkstrafik.

Kontroll av systemtjänstport

Hantera öppna och stängda systemtjänstportar som krävs av vissa program.

Hantera datoranslutningar

Tillåt och blockera fjärranslutningar mellan andra datorer och din egen.

HackerWatch informationsintegration

Följ globala hackar- och intrångsmönster via HackerWatchs webbplats, som också innehåller aktuell säkerhetsinformation om program på din dator, global säkerhetsstatistik och Internetportsstatistik.

Lås brandvägg

Blockerar omedelbart all inkommande och utgående nätverkstrafik mellan datorn och Internet.

Återställ Firewall

Återställer direkt originalinställningarna för Firewall.

Avancerad identifiering av trojaner

Upptäck och blockera potentiellt skadliga program, t.ex. trojaner, från att vidarebefordra dina personliga data till Internet.

Händelseloggning

Spåra de senaste inkommande och utgående händelserna och intrången.

Övervaka Internettrafik

Visa kartor som visar källan till fientliga attacker och fientlig trafik över hela världen. Du kan också visa detaljerad information om kontakt/ägare och geografiska data om de ursprungliga IP-adresserna. Analysera ingående och utgående trafik, övervaka programbandbredd och programaktivitet.

Förebyggande av intrång

Skydda din integritet från möjliga Internethot. McAfee använder sig av en typ av heuristisk funktion med ett tredje skyddslager som blockerar objekt som uppvisar symptom på attacker eller liknar hackarförsök.

Sofistikerad trafikanalys

Gå igenom ingående och utgående Internettrafik och programkopplingar, även de som aktivt lyssnar efter öppna anslutningar. Detta gör att du kan visa och göra något åt program som kan vara mottagliga för intrång.

KAPITEL 14

Starta Firewall

Så fort du har installerat Firewall är datorn skyddad mot intrång och oönskad nätverkstrafik. Dessutom kan du hantera varningar samt inkommande och utgående Internetåtkomst för kända och okända program. Smarta rekommendationer och säkerhetsnivån Tillförlitlig (med alternativet att endast tillåta program utgående Internetanslutningar) aktiveras automatiskt.

Du kan inaktivera Firewall på panelen Internet- och nätverkskonfiguration, men tänk på att datorn då inte längre är skyddad mot intrång och oönskad nätverkstrafik, och du kan inte heller hantera inkommande och utgående Internetanslutningar effektivt. Inaktivera inte brandväggsskyddet om det inte är nödvändigt, och då bara tillfälligt. Du kan även aktivera Firewall igen på panelen Internet- och nätverkskonfiguration.

Firewall inaktiverar automatiskt Windows-brandväggen och blir standardbrandvägg på datorn.

Obs! När du vill konfigurera Firewall öppnar du först panelen Nätverks- och Internetkonfiguration.

I detta kapitel

Aktivera brandväggsskydd

Genom att aktivera Firewall kan du skydda datorn mot intrång och oönskad nätverkstrafik samt hantera inkommande och utgående Internet-anslutningar.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **På** under **Brandväggsskydd är inaktiverat** på panelen Internet- och nätverkskonfiguration.

Stänga av brandväggsskydd

Du kan inaktivera Firewall om du inte vill skydda datorn mot intrång och oönskad nätverkstrafik. Utan brandväggsskydd kan du inte hantera inkommande och utgående Internet-anslutningar.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Av** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.

KAPITEL 15

Arbeta med varningar

I Firewall används en varningsmatris som hjälper dig hantera säkerheten. Dessa varningar kan delas in i tre grundtyper:

- Röd varning
- Gul varning
- Grön varning

Varningar kan också innehålla information som hjälper dig bestämma hur varningar ska hanteras eller hämta information om program som körs på datorn.

I detta kapitel

Om varningar

Firewall innehåller tre grundläggande varningstyper. Dessutom innehåller vissa varningar information som hjälper dig att lära mer eller att hämta information om program som körs på datorn.

Röd varning

Den röda varningen visas när Firewall upptäcker och blockerar en Trojan på din dator. Du blir också rekommenderad att genomsöka datorn efter flera hot. Trojaner verkar vara tillförlitliga program men kan störa och skada datorn eller ge obehöriga åtkomst till den. Den här varningen visas på varje säkerhetsnivå, utom Öppna.

Gul varning

Den vanligaste varningen är en gul varning, som informerar dig om att Firewall har upptäckt en programaktivitet eller nätverkshändelse. När det händer beskriver varningen programaktiviteten eller nätverkshändelsen, följt av ett eller flera alternativ som du måste svara på. Exempelvis visas varningen **Nytt nätverk upptäckt** när en dator med Firewall ansluts till ett nytt nätverk. Du kan välja att lita på eller inte lita på nätverket. Om du litar på nätverket tillåter Firewall trafik från alla datorer i nätverket och det läggs till i Betrodda IP-adresser. Om smarta rekommendationer har aktiverats läggs program till i panelen Programtillstånd.

Grön varning

I de flesta fall innehåller en grön varning basinformation om en händelse och kräver ingen åtgärd. Gröna varningar inträffar vanligen när säkerhetsnivåerna Standard, Tillförlitlig, Hög eller Smygläge har angetts.

Användarhjälp

Många Firewall-varningar innehåller ytterligare information som hjälper dig hantera datorns säkerhet, vilket inkluderar följande:

- **Mer information om det här programmet**: Starta McAfees globala säkerhetswebbplats och hämta information om ett program som Firewall har upptäckt på datorn.
- **Informera McAfee om detta program**: Skicka information till McAfee om en okänd fil som Firewall har upptäckt på datorn.
- **McAfee rekommenderar**: Råd för hantering av varningar. En varning kan t.ex. rekommendera att du beviljar åtkomst för ett program.

KAPITEL 16

Hantera informationsvarningar

Med Firewall kan du visa eller dölja informationsvarningar när intrångsförsök eller misstänkt aktivitet upptäcks under vissa händelser, t.ex. vid spel i helskärmsläge.

I detta kapitel

Visa varningar vid spel

Du kan ställa in att Firewall ska visa informationsvarningar när intrångsförsök eller misstänkt aktivitet upptäcks vid spel i helskärmsläge.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Konfigurera**.
3. Klicka på **Avancerat** under **Varningar** i panelen Konfigurering av SecurityCenter.
4. I panelen Varningsalternativ väljer du **Visa informationsvarningar när spelläge upptäcks**.
5. Klicka på **OK**.

Dölja informationsvarningar

Du kan hindra att informationsvarningar från Firewall visas när Firewall upptäcker intrångsförsök eller misstänkt aktivitet.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Konfigurera**.
3. Klicka på **Avancerat** under **Varningar** i panelen Konfigurering av SecurityCenter.
4. Klicka på **Informationsvarningar** på panelen Konfigurera SecurityCenter.
5. I panelen Informationsvarningar gör du något av följande:
   - Välj **Visa inga informationsvarningar** om du vill dölja alla informationsvarningar.
   - Avmarkera den informationsvarning du vill dölja.
6. Klicka på **OK**.

KAPITEL 17

Konfigurera skydd med Firewall

Det finns ett flertal sätt att hantera säkerheten och specialanpassa svar på säkerhetshändelser och varningar i Firewall.

Efter att du har installerat Firewall för första gången är datorns säkerhetsnivå inställd på Tillförlitlig och programmen tillåts endast utgående Internetåtkomst. Du kan dock välja andra nivåer i Firewall, från mycket strikta till mycket tillåtande.

Du kan också välja att få rekommendationer om varningar och Internetåtkomst för program.

I detta kapitel

Säkerhetsnivåer i Firewall

Firewalls säkerhetsnivåer styr i vilken grad du vill hantera och ge respons på varningar. Varningarna visas när Firewall upptäcker oönskad nätverkstrafik samt inkommande och utgående Internetanslutningar. Som standard är säkerhetsnivån i Firewall Tillförlitlig, med endast utgående åtkomst.

När Tillförlitlig säkerhet gäller och smarta rekommendationer har aktiverats, visas gula varningar där du kan välja att bevilja eller blockera åtkomst för okända program som begär inkommande åtkomst. När kända program upptäcks visas gröna informationsvarningar och åtkomst beviljas automatiskt. Om åtkomst beviljas kan programmet skapa utgående anslutningar och lyssna efter ej efterfrågade inkommande anslutningar.

I allmänhet gäller att ju striktare säkerhetsnivå du väljer (Smygläge eller Hög), desto fler alternativ och varningar måste du hantera.

Tabellen nedan beskriver de sex säkerhetsnivåerna i Firewall, i ordning från striktast till mest tillåtande:

Nivå	Beskrivning
Lås	Blockerar alla inkommande och utgående nätverksanslutningar, inklusive åtkomst till webbplatser, e-post och säkerhetsuppdateringar. Denna säkerhetsnivå har samma effekt som att koppla bort anslutningen till Internet. Du kan använda den här inställningen för att blockera portar som du har konfigurerat som öppna på panelen Systemtjänster.
Smygläge	Blockerar alla inkommande Internetanslutningar utom öppna portar, och döljer datorns närvaro på Internet. Brandväggen varnar dig när nya program försöker skapa utgående Internetanslutningar eller ta emot begäranden om inkommande anslutningar. Blockerade och tillagda program visas på panelen Programtillstånd.
Hög	Varnar dig när nya program försöker skapa utgående Internetanslutningar eller ta emot begäranden om inkommande anslutningar. Blockerade och tillagda program visas på panelen Programtillstånd. Säkerhetsnivån Hög innebär att ett program endast begär den typ av åtkomst som det behöver just då, t.ex. endast utgående, vilket du kan välja att bevilja eller blockera. Om programmet senare begär både inkommande och utgående anslutningar kan du bevilja fullständig åtkomst för programmet på panelen Programtillstånd.
Standard	Övervakar inkommande och utgående anslutningar och frågar vad du vill göra när nya program försöker komma åt Internet. Blockerade och tillagda program visas på panelen Programtillstånd.

Tillförlitlig	Tillåter program att antingen ha inkommande och utgående åtkomst (fullständig) eller endast utgående Internetåtkomst. Standardnivån för säkerhet är Tillförlitlig med alternativet att endast tillåta utgående åtkomst valt. Om ett program får fullständig åtkomst litar Firewall automatiskt på det och lägger till det i listan över tillåtna program på panelen Programtillstånd. Om ett program endast tillåts utgående åtkomst, litar Firewall automatiskt på det endast när en utgående Internetanslutning upprättas. Firewall litar inte automatiskt på en inkommande anslutning.
Öppna	Alla inkommande och utgående Internetanslutningar tillåts.

Du kan om du vill omedelbart återställa säkerhetsnivån till Tillförlitlig (och tillåta endast utgående åtkomst) på panelen Återställ brandväggsskyddets standardinställningar.

Säkerhetsnivån Lås

Du kan ställa in säkerhetsnivån Lås i Firewall om du vill blockera alla inkommande och utgående nätverksanslutningar.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Flytta reglaget på panelen Säkerhetsnivå tills **Lås** visas som aktuell nivå.
4. Klicka på **OK**.

Säkerhetsnivån Smygläge

Du kan ställa in säkerhetsnivån i Firewall till Smygläge om du vill blockera alla inkommande nätverksanslutningar, utom öppna portar, för att dölja datorn på Internet.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Flytta reglaget på panelen Säkerhetsnivå tills **Smygläge** visas som aktuell nivå.
4. Klicka på **OK**.

Obs! I Smygläge visas varningar när nya program försöker ansluta till Internet eller nås av inkommande anslutningsförsök.

Säkerhetsnivån Hög

Vid säkerhetsnivån Hög i Firewall visas meddelanden när ett nytt program försöker ansluta till Internet eller nås av inkommande anslutningsförsök.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Flytta reglaget på panelen Säkerhetsnivå tills **Hög** visas som aktuell nivå.
4. Klicka på **OK**.

Obs! Säkerhetsnivån Hög innebär att ett program endast begär den typ av åtkomst som det behöver just då, t.ex. endast utgående, vilket du kan välja att bevilja eller blockera. Om programmet senare begär både inkommande och utgående anslutningar kan du bevilja fullständig åtkomst för programmet på panelen Programtillstånd.

Säkerhetsnivån Standard

Du kan ställa in säkerhetsnivån till Standard om du vill övervaka inkommande och utgående anslutningar och bli varnad när nya program försöker ansluta till Internet.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Flytta reglaget på panelen Säkerhetsnivå tills **Standard** visas som aktuell nivå.
4. Klicka på **OK**.

Säkerhetsnivån Tillförlitlig

Du kan ställa in säkerhetsnivån i Firewall till Tillförlitlig för att antingen tillåta fullständig åtkomst eller endast utgående nätverksåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Flytta reglaget på panelen Säkerhetsnivå tills **Tillförlitlig** visas som aktuell nivå.
4. Välj någon av de följande åtgärderna:
   - Om du vill tillåta full inkommande och utgående nätverksåtkomst väljer du **Tillåt fullständig åtkomst**.

- Om du bara vill tillåta utgående nätverksåtkomst väljer du **Tillåt endast utgående åtkomst**.

5 Klicka på **OK**.

Obs! Tillåt endast utgående åtkomst är standardalternativet.

Säkerhetsnivån Öppna

Du kan ställa in säkerhetsnivån Öppna i Firewall om du vill tillåta alla inkommande och utgående nätverksanslutningar.

1 Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.

2 Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.

3 Flytta reglaget på panelen Säkerhetsnivå tills **Öppna** visas som aktuell nivå.

4 Klicka på **OK**.

Konfigurera smarta rekommendationer i varningar

Du kan välja om rekommendationer ska tas med, inte tas med eller endast visas i Firewall-varningar när program försöker ansluta till Internet. Smarta rekommendationer ger dig hjälp att hantera varningar.

När smarta rekommendationer är aktiverade (och säkerhetsnivån är Tillförlitlig med endast utgående åtkomst aktiverad) kommer Firewall automatiskt att tillåta eller blockera kända program samt visa en varning med en rekommenderad åtgärd när ett potentiellt skadligt program upptäcks..

När smarta rekommendationer är inaktiverade kommer Firewall inte att tillåta eller blockera Internet-åtkomst och inte heller visa några rekommendationer.

När du väljer Visa endast för smarta rekommendationer, visas en varning med ett förslag på åtgärd, men du väljer själv att bevilja eller blockera åtkomst.

Aktivera smarta rekommendationer

Du kan aktivera smarta rekommendationer för att tillåta eller blockera program automatiskt med Firewall och varna dig om okända och eventuellt farliga program.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Säkerhetsnivå och välj **Aktivera smarta rekommendationer** under **Smarta rekommendationer**.
4. Klicka på **OK**.

Inaktivera smarta rekommendationer

Du kan inaktivera smarta rekommendationer för att tillåta eller blockera program med Firewall och varna dig om okända och eventuellt farliga program. Varningarna visar dock inga rekommendationer om att hantera åtkomst för program. Om Firewall upptäcker ett nytt program som är misstänkt eller skadligt, blockeras programmet automatiskt från åtkomst till Internet.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Säkerhetsnivå och välj **Inaktivera smarta rekommendationer** under **Smarta rekommendationer**.
4. Klicka på **OK**.

Visa endast smarta rekommendationer

Du kan visa smarta rekommendationer för varningarna för att endast visa rekommendationer så att du kan avgöra om du vill tillåta eller blockera okända och eventuellt farliga program.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Säkerhetsnivå och välj **Visa endast** under **Smarta rekommendationer**.
4. Klicka på **OK**.

Optimera säkerheten med Firewall

Skyddet för din dator kan hotas på många olika sätt. Vissa program kan t.ex. försöka ansluta till Internet innan Windows® startas. Ett annat problem är att kunniga datoranvändare kan spåra (eller pinga) din dator i syfte att se om den är ansluten till ett nätverk. Med Firewall kan du skydda dig mot båda dessa intrångstyper genom att aktivera skydd vid start och blockera pingningar. Den första inställningen blockerar program från att ansluta till Internet när Windows startas. Den andra blockerar pingningar som andra användare kan skicka för att hitta din dator i ett nätverk.

Standardinställningarna efter installationen inkluderar automatisk identifiering av de vanligaste intrångsförsöken, t.ex. Denial of Service-attacker och utnyttjanden. Om du använder standardinställningarna innebär det att du är skyddad mot dessa attacker, men du kan inaktivera automatisk identifiering av en eller flera typer av attacker eller genomsökningar genom att använda panelen för intrångsidentifiering.

Skydda datorn vid start

Du kan skydda datorn när Windows startar för att blockera nya program som inte hade och nu behöver Internetåtkomst vid starten. Firewall visar varningar om program som har försökt ansluta till Internet under start, och du kan då välja att tillåta eller blockera dessa. Det här alternativet går inte att välja om säkerhetsnivån är Öppna eller Lås.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Säkerhetsnivå och välj **Aktivera skydd vid start** under **Säkerhetsinställningar**.
4. Klicka på **OK**.

Obs! Blockerade anslutningar och intrång loggas inte medan skydd vid start är aktiverat.

Inställningar för pingningar

Du kan tillåta eller förhindra att andra datoranvändare upptäcker din dator på nätverket.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gör något av följande under **Säkerhetsinställningar** på panelen Säkerhetsnivå:
   - Markera **Tillåt begäran om ICMP-pingning** om du vill att andra ska kunna upptäcka din dator i nätverket genom pingningar.
   - Avmarkera **Tillåt begäran om ICMP-pingning** om du vill att andra inte ska kunna upptäcka din dator i nätverket genom pingningar.
4. Klicka på **OK**.

Konfigurera intrångsdetektering

Du kan upptäcka intrångsförsök för att skydda datorn mot attacker och obehöriga genomsökningar. Standardinställningen i Firewall upptäcker automatiskt de vanligaste intrångsförsöken, t.ex. Denial of Service-attacker eller utnyttjanden. Du kan dock inaktivera automatisk upptäckt av en eller flera attacker eller genomsökningar.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Upptäckt av intrång**.
4. Under **Upptäck intrångsförsök** gör du något av följande:
   - Markera ett namn om du vill aktivera automatisk upptäckt av angrepp eller genomsökning.
   - Radera ett namn om du vill inaktivera automatisk upptäckt av angrepp eller genomsökning.
5. Klicka på **OK**.

Konfigurera inställningar för Firewalls skyddsstatus

Du kan ställa in att Firewall ska ignorera att specifika problem på datorn inte rapporteras till SecurityCenter.

1. Klicka på **Konfigurera** under **SecurityCenter – information** på panelen McAfee SecurityCenter.
2. Klicka på **Avancerat** under **Skyddsstatus** i panelen Konfigurering av SecurityCenter.
3. I panelen Ignorerade problem väljer du ett eller flera av följande alternativ:
   - **Brandväggsskyddet är inaktiverat.**
   - **Brandväggen är inställd på öppen säkerhetsnivå.**
   - **Brandväggstjänsten körs inte.**
   - **Det finns ingen brandvägg på datorn.**
   - **Windows-brandväggen är inaktiverad.**
   - **Det finns ingen brandvägg för utgående trafik på datorn.**
4. Klicka på **OK**.

Låsa och återställa brandvägg

Vid låsning blockeras omedelbart all inkommande och utgående nätverkstrafik så att du kan isolera och felsöka ett problem på datorn.

Låsa brandväggen direkt

Du kan låsa Firewall om du direkt vill blockera all nätverkstrafik mellan datorn och Internet.

1. Klicka på **Lås brandvägg** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
2. I panelen Lås brandvägg klickar du på **Lås**.
3. Bekräfta genom att klicka på **Ja**.

Tips: Du kan också låsa Firewall genom att högerklicka på SecurityCenter-ikonen i meddelandefältet till höger om aktivitetsfältet och sedan klicka på **Snabblänkar** och sedan på **Lås brandvägg**.

Låsa upp brandväggen direkt

Du kan låsa upp Firewall om du direkt vill tillåta all nätverkstrafik mellan datorn och Internet.

1. Klicka på **Lås brandvägg** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
2. I panelen Lås aktiverat klickar du på **Lås upp**.
3. Bekräfta genom att klicka på **Ja**.

Återställa inställningar för brandvägg

Du kan snabbt återställa brandväggen till de ursprungliga skyddsinställningarna. Återställningen återställer säkerhetsnivån till Tillförlitlig och tillåter endast utgående nätverksåtkomst, aktiverar smarta rekommendationer, återställer listan över standardprogram och deras behörigheter i panelen Programtillstånd, tar bort tillförlitliga och förbjudna IP-adresser och återställer systemtjänster, inställningar för händelseloggar och intrångsupptäckt.

1. Klicka på **Återställ brandväggens standardinställningar** på panelen McAfee SecurityCenter.
2. I panelen Återställ brandväggsskyddets standardinställningar klickar du på **Återställ standardvärden**.
3. Bekräfta genom att klicka på **Ja**.

Tips: Du kan också återställa standardinställningarna i Firewall genom att högerklicka på SecurityCenter-ikonen i meddelandefältet till höger om aktivitetsfältet och sedan klicka på **Snabblänkar** och sedan på **Återställ brandväggens standardinställningar**.

KAPITEL 18

Hantera program och tillstånd

Med Firewall kan du hantera och skapa åtkomsttillstånd för befintliga och nya program som begär inkommande och utgående Internetanslutningar. Du kan välja att tillåta fullständig eller endast utgående åtkomst för program. Du kan även blockera åtkomst för programmen.

I detta kapitel

Tillåta Internetåtkomst för program

Vissa program, t.ex. webbläsare, behöver kunna ansluta till Internet för att fungera som de ska.

På sidan Programtillstånd i Firewall kan du göra följande:

- Tillåta åtkomst för program
- Tillåta endast utgående åtkomst för program
- Blockera åtkomst för program

Du kan också tillåta fullständig eller endast utgående åtkomst för ett program från loggarna Utgående händelser och De senaste händelserna.

Tillåt fullständig åtkomst för ett program

Du kan tillåta att ett befintligt blockerat program på datorn ska få fullständig inkommande och utgående Internetåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Firewall och klicka på **Programtillstånd**.
4. Under **Programtillstånd** markerar du ett program med tillståndet **Blockerat** eller **Endast utgående åtkomst**.
5. Klicka på **Tillåt åtkomst** under **Åtgärd**.
6. Klicka på **OK**.

Tillåt fullständig åtkomst för ett nytt program

Du kan tillåta att ett nytt program på datorn ska få fullständig inkommande och utgående Internetåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Firewall och klicka på **Programtillstånd**.
4. Under **Programtillstånd** klickar du på **Lägg till tillåtet program**.
5. Dialogrutan **Lägg till program** öppnas. Bläddra till och markera det program du vill lägga till och klicka på **Öppna**.

Obs! Du kan ändra tillstånd för ett program som du har lagt till precis som för andra program – genom att markera programmet och sedan klicka på **Tillåt endast utgående åtkomst** eller **Blockera åtkomst** under **Åtgärd**.

Tillåt fullständig åtkomst från loggen för senaste händelser

Du kan tillåta att ett befintligt blockerat program som visas i loggen för senaste händelser ska få fullständig inkommande och utgående Internetåtkomst.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Under **De senaste händelserna** markerar du händelsebeskrivningen och klickar sedan på **Tillåt åtkomst**.
4. I dialogrutan Programtillstånd klickar du på **Ja** för att bekräfta.

Närliggande information

- Visa utgående händelser (sida 115)

Tillåt fullständig åtkomst från loggen för utgående händelser

Du kan tillåta att ett befintligt blockerat program som visas i loggen för utgående händelser ska få fullständig inkommande och utgående Internetåtkomst.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Klicka på **Visa logg** under **De senaste händelserna**.
4. Klicka på **Internet och nätverk** och sedan **Utgående händelser**.
5. Välj ett program och klicka på **Tillåt åtkomst** under **Jag vill**.
6. I dialogrutan Programtillstånd klickar du på **Ja** för att bekräfta.

Tillåta endast utgående åtkomst för program

Vissa program på datorn kräver utgående Internetåtkomst. I Firewall kan du tillåta program endast utgående åtkomst till Internet.

Tillåt endast utgående åtkomst för program

Du kan tillåta att ett program endast ska få utgående Internetåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Firewall och klicka på **Programtillstånd**.
4. Under **Programtillstånd** markerar du ett program med tillståndet **Blockerat** eller **Fullständig åtkomst**.
5. Klicka på **Tillåt endast utgående åtkomst** under **Åtgärd**.
6. Klicka på **OK**.

Tillåt endast utgående åtkomst från loggen för senaste händelser

Du kan tillåta att ett befintligt blockerat program som visas i loggen för de senaste händelserna ska få endast utgående Internetåtkomst.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Under **De senaste händelserna** markerar du händelsebeskrivningen och klickar sedan på **Tillåt endast utgående åtkomst**.
4. I dialogrutan Programtillstånd klickar du på **Ja** för att bekräfta.

Tillåt endast utgående åtkomst från loggen för utgående händelser

Du kan tillåta att ett befintligt blockerat program som visas i loggen för utgående händelser ska få endast utgående Internetåtkomst.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Klicka på **Visa logg** under **De senaste händelserna**.
4. Klicka på **Internet och nätverk** och sedan **Utgående händelser**.
5. Välj ett program och klicka på **Tillåt endast utgående åtkomst** under **Jag vill**.
6. I dialogrutan Programtillstånd klickar du på **Ja** för att bekräfta.

Blockera Internetåtkomst för program

Med Firewall kan du blockera program från att ansluta till Internet. Kontrollera först att blockering av ett visst program inte kommer att störa nätverksanslutningen eller något annat program som behöver Internetåtkomst för att fungera korrekt.

Blockera åtkomst för program

Du kan blockera ett program från inkommande eller utgående Internetåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Firewall och klicka på **Programtillstånd**.
4. Under **Programtillstånd** markerar du ett program med tillståndet **Fullständig åtkomst** eller **Endast utgående åtkomst**.
5. Klicka på **Blockera åtkomst** under **Åtgärd**.
6. Klicka på **OK**.

Blockera åtkomst för ett nytt program

Du kan blockera ett nytt program från inkommande eller utgående Internetåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Firewall och klicka på **Programtillstånd**.
4. Under **Programtillstånd** klickar du på **Lägg till blockerat program**.
5. Dialogrutan Lägg till program öppnas. Bläddra till och markera det program du vill lägga till och klicka på **Öppna**.

Obs! Du kan ändra tillstånd för ett program som du har lagt till genom att markera programmet och sedan klicka på **Tillåt endast utgående åtkomst** eller **Tillåt åtkomst** under **Åtgärd**.

Blockera åtkomst från loggen för senaste händelser

Du kan blockera ett program som visas i loggen för senaste händelser från inkommande och utgående Internetåtkomst.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Under **De senaste händelserna** markerar du händelsebeskrivningen och klickar sedan på **Blockera åtkomst**.
4. I dialogrutan Programtillstånd klickar du på **Ja** för att bekräfta.

Ta bort åtkomsttillstånd för program

Innan du tar bort åtkomsttillståndet för ett program bör du kontrollera att ändringen inte påverkar datorns funktioner eller nätverksanslutningen.

Ta bort ett programtillstånd

Du kan ta bort ett program från all inkommande eller utgående Internetåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Firewall och klicka på **Programtillstånd**.
4. Markera ett program under **Programtillstånd**.
5. Klicka på **Ta bort programtillstånd** under **Åtgärd**.
6. Klicka på **OK**.

Obs! För vissa program är vissa åtgärder nedtonade eftersom de inte kan utföras.

Information om program

Om du är osäker på vilket programtillstånd du ska välja kan du läsa mer om programmet på McAfee-webbplatsen HackerWatch.

Visa programinformation

Du kan få programinformation från McAfees webbplats HackerWatch för att avgöra om du bör tillåta eller blockera från inkommande och utgående Internetåtkomst.

Obs! Se till att datorn är ansluten till Internet så att webbläsaren kan ansluta till McAfee-webbplatsen HackerWatch, där du hittar aktuell information om program, säkerhetshot och villkor för Internetåtkomst.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. Gå till panelen Firewall och klicka på **Programtillstånd**.
4. Markera ett program under **Programtillstånd**.
5. Klicka på **Läs mer** under **Åtgärd**.

Hämta programinformation från loggen för utgående händelser

Från loggen för utgående händelser kan du få programinformation från McAfees webbplats HackerWatch för att avgöra vilka program som du bör tillåta eller blockera från inkommande och utgående Internetåtkomst.

Obs! Se till att datorn är ansluten till Internet så att webbläsaren kan ansluta till McAfee-webbplatsen HackerWatch, där du hittar aktuell information om program, säkerhetshot och villkor för Internetåtkomst.

1. Klicka på **Avancerad meny** på panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Under De senaste händelserna väljer du en händelse och klickar sedan på **Visa logg**.
4. Klicka på **Internet och nätverk** och sedan **Utgående händelser**.
5. Markera en IP-adress och klicka sedan på **Mer information**.

KAPITEL 19

Hantera systemtjänster

Om vissa program, till exempel webbservrar och serverprogram för fildelning, ska kunna fungera korrekt måste de godkänna oönskade anslutningar från andra datorer via avsedda systemtjänstportar. Oftast stängs de här systemtjänstportarna av Firewall eftersom de representerar den vanligaste källan till osäkerheter i systemet. Om anslutningar från fjärrdatorer ska kunna godkännas måste systemtjänstportarna emellertid öppnas.

I detta kapitel

Konfigurera systemtjänstportar

Systemtjänstportar kan konfigureras för att tillåta eller blockera fjärråtkomst till en tjänst på datorn.

Listan nedan visar de vanligaste systemtjänsterana och tillhörande portar:

- File Transfer Protocol (FTP) 20-21
- Mail Server (IMAP) 143
- Mail Server (POP3) 110
- Mail Server (SMTP) 25
- Microsoft Directory Server (MSFT DS) 445
- Microsoft SQL Server (MSFT SQL) 1433
- Network Time Protocol 123
- Remote Desktop / Remote Assistance / Terminal Server (RDP) 3389
- Remote Procedure Calls (RPC) 135
- Secure Web Server (HTTPS) 443
- Universal Plug and Play (UPNP) 5000
- Web Server (HTTP) 80
- Windows File Sharing (NETBIOS) 137-139

Systemtjänstportar kan också konfigureras för att tillåta en dator att dela Internetanslutning med andra datorer som är anslutna till den via samma nätverk. Den anslutningen, som kallas Internetanslutningsdelning (ICS), gör att datorn som delar anslutningen kan fungera som gateway till Internet för den andra nätverksanslutna datorn.

Obs! Om datorn har ett program som accepterar webb- eller FTP-serveranslutningar, kan datorn som delar anslutningen behöva öppna den associerade systemtjänstporten och tillåta att inkommande anslutningar för de portarna vidarebefordras.

Tillåta åtkomst till en befintlig systemtjänstport

Du kan öppna en befintlig port om du vill tillåta fjärråtkomst till en tjänst på din dator.

Obs! En öppen systemtjänstport kan göra datorn sårbar för hot mot säkerheten i Internet. Öppna därför bara en port om det är nödvändigt.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Systemtjänster**.
4. Under **Öppna systemtjänstport** markerar du en systemtjänst om du vill öppna en port.
5. Klicka på **OK**.

Blockera åtkomst till en befintlig systemtjänstport

Du kan stänga en befintlig port om du vill blockera fjärråtkomst till en tjänst på din dator.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Systemtjänster**.
4. Under **Öppna systemtjänstport** avmarkerar du en systemtjänst om du vill stänga en port.
5. Klicka på **OK**.

Konfigurera en ny systemtjänstport

Du kan konfigurera en ny nätverkstjänstport på datorn som du kan öppna eller stänga för att tillåta eller blockera fjärråtkomst på datorn.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Systemtjänster**.
4. Klicka på **Lägg till**.
5. Ange följande på panelen Systemtjänster under **Portar och systemtjänster**:
   - Programnamn
   - Inkommande TCP/IP-portar

- Utgående TCP/IP-portar
- Inkommande UDP-portar
- Utgående UDP-portar

6 Om du vill skicka portens aktivitetsinformation till en annan nätverksansluten Windows-dator som delar Internetanslutningen, väljer du **Vidarebefordra nätverksaktivitet på den här porten till nätverksanvändare som använder Internetanslutningsdelning**.

7 Välj om du vill beskriva den nya konfigureringen.

8 Klicka på **OK**.

Obs! Om datorn har ett program som accepterar webb- eller FTP-serveranslutningar, kan datorn som delar anslutningen behöva öppna den associerade systemtjänstporten och tillåta att inkommande anslutningar för de portarna vidarebefordras. Om du använder Internetanslutningsdelning (ICS) måste du också lägga till en tillförlitlig datoranslutning på listan Tillförlitliga IP-adresser. Mer information finns under Lägga till en betrodd datoranslutning.

Ändra en systemtjänstport

Du kan ändra inkommande och utgående nätverksåtkomstinformation om en befintlig systemtjänstport.

Obs! Om felaktig portinformation anges fungerar inte systemtjänsten.

1 Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.

2 Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.

3 I Firewall-panelen klickar du på **Systemtjänster**.

4 Markera en systemtjänst och klicka på **Redigera**.

5 Ange följande på panelen Systemtjänster under **Portar och systemtjänster**:

- Programnamn
- Inkommande TCP/IP-portar
- Utgående TCP/IP-portar
- Inkommande UDP-portar
- Utgående UDP-portar

6 Om du vill skicka portens aktivitetsinformation till en annan nätverksansluten Windows-dator som delar Internetanslutningen, väljer du **Vidarebefordra nätverksaktivitet på den här porten till**

nätverksanvändare som använder Internetanslutningsdelning.

7 Välj om du vill beskriva den ändrade konfigureringen.

8 Klicka på **OK**.

Ta bort en systemtjänstport

Du kan ta bort en befintlig systemtjänstport från datorn. Efter att du tagit bort systemtjänstporten kan fjärrdatorer inte längre komma åt nätverkstjänsten i din dator.

1 Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.

2 Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.

3 I Firewall-panelen klickar du på **Systemtjänster**.

4 Markera en systemtjänst och klicka sedan på **Ta bort**.

5 Klicka på **Ja** för att bekräfta.

KAPITEL 20

Hantera datoranslutningar

Med hjälp av Firewall kan du hantera enskilda fjärranslutningar till datorn genom att skapa regler som baseras på IP-adresser för fjärranslutna datorer. Datorer med IP-adresser som du litar på kan få tillstånd att ansluta till din dator, medan IP-adresser som är okända eller misstänkta kan förbjudas att ansluta till datorn.

När du tillåter en anslutning måste du vara säker på att den dator du tillåter är säker. Om en dator som du anger att du litar på är infekterad av en mask eller liknande kan din dator också utsättas för infektion. McAfee rekommenderar också att datorer du litar på ska skyddas av en brandvägg och ett uppdaterat antivirusprogram. Firewall loggar inte trafik och genererar inte händelsevarningar från IP-adresser i listan Betrodda IP-adresser.

Datorer associerade med okända, misstänkta eller ej tillförlitliga IP-adresser kan förbjudas att ansluta till din dator.

Firewall blockerar all oönskad trafik. Därför är det normalt onödigt att förbjuda en IP-adress. Du ska bara förbjuda en IP-adress när du är säker på att en Internetanslutning innebär ett visst hot. Blockera inte viktiga IP-adresser, till exempel för DNS- eller DHCP-servern, eller andra servrar hos din Internetleverantör. Beroende på dina säkerhetsinställningar kan Firewall varna dig när den upptäcker en händelse från en förbjuden dator.

I detta kapitel

Betrodda datoranslutningar

Du kan lägga till, ändra och ta bort tillförlitliga IP-adresser under **Tillförlitliga IP-adresser** på panelen Tillförlitliga och förbjudna IP-adresser.

Listan **Tillförlitliga IP-adresser** i Tillförlitliga och förbjudna IP-adresser-panelen gör att du kan tillåta all trafik från en dator till din dator. Firewall loggar inte trafik och genererar inte händelsevarningar från IP-adresser i listan **Betrodda IP-adresser**.

Alla IP-adresser som är markerade i denna lista anses som betrodda av Firewall. Trafik från en betrodd IP-adress tillåts alltid via alla portar. Aktiviteter mellan en dator med betrodd IP-adress och din dator filtreras inte och analyseras inte av Firewall. Som standard visar Tillförlitliga IP-adresser det första privata nätverk som Firewall hittar.

När du tillåter en anslutning måste du vara säker på att den dator du tillåter är säker. Om en dator som du anger att du litar på är infekterad av en mask eller liknande kan din dator också utsättas för infektion. McAfee rekommenderar också att datorer du litar på ska skyddas av en brandvägg och ett uppdaterat antivirusprogram.

Lägga till en betrodd datoranslutning

Du kan lägga till en betrodd datoranslutning och dess IP-adress.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Betrodda och förbjudna IP-adresser**.
4. På panelen Betrodda och förbjudna IP-adresser väljer du **Betrodda IP-adresser** och klickar sedan på **Lägg till**.
5. Under **Lägg till regel om betrodd IP-adress** gör du något av följande:
   - Välj **En enda IP-adress** och ange önskad IP-adress.
   - Välj **IP-adressintervall** och ange sedan intervallets inledande och avslutande IP-adress i rutorna **Från IP-adress** och **Till IP-adress**.

6 Om en systemtjänst använder Internetanslutningsdelning (ICS), kan du lägga till följande IP-adressintervall: 192.168.0.1 till 192.168.0.255.

7 Om du vill kan du markera **Regeln slutar gälla** och ange hur många dagar regeln ska gälla.

8 Du kan ange en beskrivning av regeln om du vill.

9 Klicka på **OK**.

10 I dialogrutan **Betrodda och förbjudna IP-adresser** klickar du på **Ja** för att bekräfta.

Obs! Mer information om Internetanslutningsdelning (ICS) finns i Konfigurera en ny systemtjänst.

Lägga till en tillförlitlig dator från loggen för inkommande händelser

Du kan lägga till en tillförlitlig datoranslutning med tillhörande IP-adress från loggen för inkommande händelser.

1 Klicka på **Avancerad meny** under Vanliga uppgifter i panelen McAfee SecurityCenter.

2 Klicka på **Rapporter och loggar**.

3 Klicka på **Visa logg** under **De senaste händelserna**.

4 Klicka på **Internet och nätverk** och sedan **Inkommande händelser**.

5 Välj en käll-IP-adress och klicka på **Lita på denna adress** under **Jag vill**.

6 Bekräfta genom att klicka på **Ja**.

Ändra en betrodd datoranslutning

Du kan redigera en betrodd datoranslutning och dess IP-adress.

1 Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.

2 Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.

3 I Firewall-panelen klickar du på **Betrodda och förbjudna IP-adresser**.

4 På panelen Betrodda och förbjudna IP-adresser väljer du **Betrodda IP-adresser**.

5 Markera en IP-adress och klicka sedan på **Redigera**.

6 Under **Redigera tillförlitlig IP-adress** gör du något av följande:

- Välj **En enda IP-adress** och ange önskad IP-adress.

- Välj **IP-adressintervall** och ange sedan intervallets inledande och avslutande IP-adress i rutorna **Från IP-adress** och **Till IP-adress**.

7 Om du vill kan du markera **Regeln slutar gälla** och ange hur många dagar regeln ska gälla.

8 Du kan ange en beskrivning av regeln om du vill.

9 Klicka på **OK**.

Obs! Du kan inte redigera de standarddatoranslutningar som Firewall automatiskt lade till från ett tillförlitligt privat nätverk.

Ta bort en betrodd datoranslutning

Du kan välja att ta bort en betrodd datoranslutning och dess IP-adress.

1 Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.

2 Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.

3 I Firewall-panelen klickar du på **Betrodda och förbjudna IP-adresser**.

4 På panelen Betrodda och förbjudna IP-adresser väljer du **Betrodda IP-adresser**.

5 Välj en IP-adress och klicka sedan på **Ta bort**.

6 I dialogrutan **Betrodda och förbjudna IP-adresser** klickar du på **Ja** för att bekräfta.

Förbjudna datoranslutningar

Du kan lägga till, ändra och ta bort förbjudna IP-adresser under **Förbjudna IP-adresser** på panelen Tillförlitliga och förbjudna IP-adresser.

Datorer associerade med okända, misstänkta eller ej tillförlitliga IP-adresser kan förbjudas att ansluta till din dator.

Firewall blockerar all oönskad trafik. Därför är det normalt onödigt att förbjuda en IP-adress. Du ska bara förbjuda en IP-adress när du är säker på att en Internetanslutning innebär ett visst hot. Blockera inte viktiga IP-adresser, till exempel för DNS- eller DHCP-servern, eller andra servrar hos din Internetleverantör. Beroende på dina säkerhetsinställningar kan Firewall varna dig när den upptäcker en händelse från en förbjuden dator.

Lägga till en förbjuden datoranslutning

Du kan lägga till en förbjuden datoranslutning och dess IP-adress.

Obs! Blockera inte viktiga IP-adresser, till exempel för DNS- eller DHCP-servern, eller andra servrar hos din Internetleverantör.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Betrodda och förbjudna IP-adresser**.
4. På panelen Tillförlitliga och förbjudna IP-adresser väljer du **Förbjudna IP-adresser** och klickar sedan på **Lägg till**.
5. Gör något av följande under **Lägg till regel om förbjuden IP-adress**:
   - Välj **En enda IP-adress** och ange önskad IP-adress.
   - Välj **IP-adressintervall** och ange sedan intervallets inledande och avslutande IP-adress i rutorna **Från IP-adress** och **Till IP-adress**.
6. Om du vill kan du markera **Regeln slutar gälla** och ange hur många dagar regeln ska gälla.
7. Du kan ange en beskrivning av regeln om du vill.
8. Klicka på **OK**.
9. I dialogrutan **Betrodda och förbjudna IP-adresser** klickar du på **Ja** för att bekräfta.

Redigera en förbjuden datoranslutning

Du kan redigera en förbjuden datoranslutning och dess IP-adress.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Betrodda och förbjudna IP-adresser**.
4. På panelen Tillförlitliga och förbjudna IP-adresser väljer du **Förbjudna IP-adresser** och klickar sedan på **Redigera**.
5. Under **Redigera förbjuden IP-adress** gör du något av följande:
   - Välj **En enda IP-adress** och ange önskad IP-adress.
   - Välj **IP-adressintervall** och ange sedan intervallets inledande och avslutande IP-adress i rutorna **Från IP-adress** och **Till IP-adress**.
6. Om du vill kan du markera **Regeln slutar gälla** och ange hur många dagar regeln ska gälla.
7. Du kan ange en beskrivning av regeln om du vill.
8. Klicka på **OK**.

Ta bort en förbjuden datoranslutning

Du kan ta bort en förbjuden datoranslutning och dess IP-adress.

1. Klicka på **Internet och nätverk** i panelen McAfee SecurityCenter och klicka sedan på **Konfigurera**.
2. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
3. I Firewall-panelen klickar du på **Betrodda och förbjudna IP-adresser**.
4. I panelen Betrodda och förbjudna IP-adresser väljer du **Förbjudna IP-adresser**.
5. Välj en IP-adress och klicka sedan på **Ta bort**.
6. I dialogrutan **Betrodda och förbjudna IP-adresser** klickar du på **Ja** för att bekräfta.

Förbjuda en dator från loggen för inkommande händelser

Du kan förbjuda en datoranslutning med tillhörande IP-adress från loggen för inkommande händelser.

IP-adresser som visas i loggen för inkommande händelser blockeras. Att förbjuda en adress ger alltså inget ökat skydd om inte datorn använder portar som avsiktligt öppnats eller innehåller ett program som beviljats åtkomst till Internet.

Lägg bara till en IP-adress i listan **Förbjudna IP-adresser** om du har en eller flera portar som är avsiktligen öppna och om du har anledning att tro att du måste blockera adressen från åtkomst till öppna portar.

Du kan använda sidan Inkommande händelser, som visar IP-adresser för all inkommande Internettrafik, när du vill förbjuda en IP-adress som du misstänker är källa till misstänkt eller oönskad Internetaktivitet.

1. Klicka på **Avancerad meny** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Klicka på **Visa logg** under **De senaste händelserna**.
4. Klicka på **Internet och nätverk** och sedan **Inkommande händelser**.
5. Välj en käll-IP-adress och klicka på **Förbjud denna adress** under **Jag vill**.
6. I dialogrutan **Lägg till regel om förbjuden IP-adress** klickar du på **Ja** för att bekräfta.

Förbjuda en dator från loggen för upptäckt av intrångshändelser

Du kan förbjuda en datoranslutning med tillhörande IP-adress från loggen för upptäckt av intrångshändelser.

1. Klicka på **Avancerad meny** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
2. Klicka på **Rapporter och loggar**.
3. Klicka på **Visa logg** under **De senaste händelserna**.
4. Klicka på **Internet och nätverk** och sedan på **Upptäckt av intrångshändelser**.
5. Välj en käll-IP-adress och klicka på **Förbjud denna adress** under **Jag vill**.
6. I dialogrutan **Lägg till regel om förbjuden IP-adress** klickar du på **Ja** för att bekräfta.

KAPITEL 21

Logga, övervaka och analysera

I Firewall finns omfattande och lättläst loggning, övervakning och analys av Internethändelser och trafik. Om du förstår Internettrafiken och händelserna blir det lättare för dig att hantera Internetanslutningarna.

I detta kapitel

Händelseloggning

I Firewall kan du aktivera eller inaktivera loggning och välja vilka händelsetyper som ska loggas (om loggning har aktiverats). Med händelseloggning kan du visa senaste inkommande och utgående händelser och intrångshändelser.

Konfigurera inställningar för händelseloggen

Du kan ange och konfigurera vilka typer av Firewall-händelser som ska loggas. Som standard är händelseloggning aktiverad för alla händelser och aktiviteter.

1. Välj **Avancerat** under **Brandväggsskydd är aktiverat** på panelen Internet- och nätverkskonfiguration.
2. I Firewall-panelen klickar du på **Inställningar för händelselogg**.
3. Om det inte redan är valt väljer du **Aktivera händelseloggning**.
4. Under **Aktivera händelseloggning** markerar eller avmarkerar du de händelsetyper du vill eller inte vill logga. Händelsetyper är bl.a. följande:
   - Blockerade program
   - ICMP-pingningar
   - Trafik från förbjudna IP-adresser
   - Händelser på systemtjänstportar
   - Händelser på okända portar
   - Intrångsdetekteringshändelser
5. Om du vill förhindra loggning på vissa portar väljer du **Logga inte händelser på följande portar** och ange sedan enstaka portnummer avgränsade med komma eller ange portintervall med bindestreck. Till exempel `137-139, 445, 400-5000`.
6. Klicka på **OK**.

Visa de senaste händelserna

Du kan visa senaste händelser om loggningen är aktiverad. I panelen De senaste händelserna visas datum för och en beskrivning av händelsen. Den visar aktiviteter från program vars åtkomst till Internet uttryckligen har blockerats.

- Gå till **Avancerad meny** under panelen Vanliga uppgifter och klicka på **Rapporter och loggar** eller **Visa senaste händelser**. Alternativt kan du klicka på **Visa senaste händelser** under panelen Vanliga uppgifter på Grundläggande meny.

Visa inkommande händelser

Du kan visa inkommande intrång om loggningen är aktiverad. Inkommande händelser innehåller datum och klockslag, källans IP-nummer, värdnamn samt information och händelsetyp.

1. Kontrollera att Avancerad meny är aktiverad. Klicka på **Rapporter och loggar** i panelen Vanliga uppgifter.
2. Klicka på **Visa logg** under **De senaste händelserna**.
3. Klicka på **Internet och nätverk** och sedan **Inkommande händelser**.

Obs! Du kan välja att lita på, förbjuda eller spåra en IP-adress i loggen Inkommande händelser.

Visa utgående händelser

Du kan visa utgående händelser om loggningen är aktiverad. Utgående händelser omfattar namnet på programmet som försökt upprätta en utgående anslutning, datum och klockslag för händelsen samt programmets plats på datorn.

1. Klicka på **Rapporter och loggar** i panelen Vanliga uppgifter.
2. Klicka på **Visa logg** under **De senaste händelserna**.
3. Klicka på **Internet och nätverk** och sedan **Utgående händelser**.

Obs! I loggen Utgående händelser kan du tillåta fullständig respektive endast utgående åtkomst för program. Dessutom kan du visa ytterligare information om programmet.

Visa upptäckta intrång

Du kan visa inkommande intrångshändelser om loggningen är aktiverad. Datum och klockslag, källans IP-nummer, värdnamn för intrånget och typ av intrång visas i Upptäckt av intrång.

1. Klicka på **Rapporter och loggar** i panelen Vanliga uppgifter.
2. Klicka på **Visa logg** under **De senaste händelserna**.
3. Klicka på **Internet och nätverk** och sedan på **Upptäckt av intrångshändelser**.

Obs! Du kan förbjuda och spåra IP-adresser från loggen Upptäckt av intrångshändelser.

Arbeta med statistik

Med Firewall förstärks säkerhetswebbplatsen för McAfees HackerWatch för att ge statistik om globala Internetsäkerhetshändelser och portaktivitet.

Visa global händelsestatistik för säkerhet

Med HackerWatch spåras världsomspännande säkerhetshändelser på Internet, vilka du kan visa i SecurityCenter. Spårad information visar problem som rapporterats till HackerWatch under de senaste 24 timmarna, 7 respektive 30 dagarna.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. I Verktygspanelen klickar du på **HackerWatch**.
3. Visa händelsestatistik för säkerhet under Event Tracking (Händelsespårning).

Visa global Internetportsaktivitet

Med HackerWatch spåras världsomspännande säkerhetshändelser på Internet, vilka du kan visa i SecurityCenter. Visad information inkluderar de vanligast förekommande händelseportarna som rapporterats till HackerWatch under de senaste sju dagarna. Vanligen visas portinformation om HTTP, TCP och UDP.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. I Verktygspanelen klickar du på **HackerWatch**.
3. Visa de vanligast förekommande händelseportarna under **Recent Port Activity (Senaste portaktivitet)**.

Spåra Internettrafik

I Firewall finns ett antal alternativ för spårning av Internettrafik. Med de här alternativen kan du geografiskt spåra en nätverksdator, hämta domän- och nätverksinformation och spåra datorer från händelseloggarna för inkommande händelser och intrångsdetektering.

Geografiskt spåra en nätverksdator

Du kan använda Visual Tracer om du geografiskt vill spåra en dator som ansluter, eller försöker ansluta, till din dator med hjälp av namnet eller IP-adressen. Du kan också komma åt nätverks- och registreringsinformation med hjälp av Visual Tracer. När du kör Visual Tracer visas en världskarta med den troligaste rutten för data från källdatorn till din dator.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. I Verktygspanelen klickar du på **Visual Tracer**.
3. Ange datorns IP-adress och klicka på **Trace (Spåra)**.
4. Under **Visual Tracer** väljer du **Map View (Kartvy)**.

Obs! Du kan inte spåra händelser relaterade till loopade, privata eller ogiltiga IP-adresser.

Hämta datorregistreringsinformation

Du kan hämta en dators registreringsinformation från SecurityCenter med hjälp av Visual Tracer. Informationen inkluderar domännamnet, namn och adress till den som registrerat samt den administrativa kontakten.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. I Verktygspanelen klickar du på **Visual Tracer**.
3. Ange datorns IP-adress och klicka sedan på **Spåra**.
4. Under **Visual Tracer** väljer du **Registreringsvy**.

Hämta datorns nätverksinformation

Du kan hämta en dators nätverksinformation från SecurityCenter med hjälp av Visual Tracer. Nätverksinformationen innehåller detaljer om det nätverk som domänen finns på.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. I Verktygspanelen klickar du på **Visual Tracer**.
3. Ange datorns IP-adress och klicka sedan på **Spåra**.
4. Under **Visual Tracer** väljer du **Nätverksvy**.

Spåra en dator från loggen för inkommande händelser

I panelen Inkommande händelser kan du spåra en IP-adress som visas i loggen Inkommande händelser.

1. Kontrollera att Avancerad meny är aktiverad. Klicka på **Rapporter och loggar** i panelen Vanliga uppgifter.
2. Klicka på **Visa logg** under **De senaste händelserna**.
3. Klicka på **Internet och nätverk** och sedan **Inkommande händelser**.
4. I panelen Inkommande händelser markerar du en käll-IP-adress och klickar sedan på **Spåra denna adress**.
5. I panelen Visual Tracer klickar du på något av följande:
   - **Kartvy**: Geografiskt placera en dator med hjälp av markerad IP-adress.
   - **Registreringsvy**: Hitta domäninformation med hjälp av markerad IP-adress.
   - **Nätverksvy**: Hitta nätverksinformation med hjälp av markerad IP-adress.
6. Klicka på **Klar**.

Spåra en dator från loggen för upptäckt av intrångshändelser

I panelen Upptäckt av intrångshändelser kan du spåra en IP-adress som visas i loggen för upptäckt av intrångshändelser.

1. Klicka på **Rapporter och loggar** i panelen Vanliga uppgifter.
2. Klicka på **Visa logg** under **De senaste händelserna**.
3. Klicka på **Internet och nätverk** och sedan på **Upptäckt av intrångshändelser**. I panelen Upptäckt av intrångshändelser markerar du en käll-IP-adress och klickar sedan på **Spåra denna adress**.
4. I panelen Visual Tracer klickar du på något av följande:
   - **Kartvy**: Geografiskt placera en dator med hjälp av markerad IP-adress.
   - **Registreringsvy**: Hitta domäninformation med hjälp av markerad IP-adress.
   - **Nätverksvy**: Hitta nätverksinformation med hjälp av markerad IP-adress.
5. Klicka på **Klar**.

Spåra en övervakad IP-adress

Du kan spåra en övervakad IP-adress om du vill se en geografisk översikt över den troligaste rutten för de data som har färdats från källdatorn till din dator. Dessutom kan du visa registrerings- och nätverksinformation om IP-adressen.

1. Kontrollera att Avancerad meny är aktiverad och klicka sedan på **Verktyg**.
2. Klicka på **Trafikövervakning** på verktygspanelen.
3. Under **Trafikövervakning** klickar du på **Aktiva program**.
4. Markera ett program och sedan IP-adressen som visas nedanför programnamnet.
5. Klicka på **Spåra den här IP-adressen** under **Programaktivitet**.
6. Under **Visual Tracer** kan du se en karta som visar den sannolikaste vägen som data har färdats från källdatorn till din dator. Dessutom kan du visa registrerings- och nätverksinformation om IP-adressen.

Obs! Klicka på **Uppdatera** under **Visual Tracer** om du vill se aktuell statistik.

Övervaka Internettrafik

I Firewall finns ett antal olika sätt att övervaka din Internettrafik, inklusive följande:

- **Trafikanalysdiagram**: Visar senaste inkommande och utgående Internettrafik.
- **Trafikanvändningsdiagram**: Visar hur många procent av bandbredden som använts av de mest aktiva programmen under den senaste 24-timmarsperioden.
- **Aktiva program**: Visar de program som för tillfället använder de flesta nätverksanslutningarna i din dator och de IP-adresser som programmen använder.

Om trafikanalysdiagrammet

Diagrammet för trafikövervakning är en numerisk och grafisk framställning av inkommande och utgående Internettrafik. Med trafikövervakningen visas också de program som för närvarande använder flest nätverksanslutningar på datorn och de IP-adresser som programmen har åtkomst till.

I panelen Trafikanalys kan du visa den senaste inkommande och utgående Internettrafiken: aktuell, genomsnittlig och maximal överföringshastighet. Du kan också visa trafikvolym, inklusive hur mycket trafik som förekommit sedan du startade Firewall och total trafik för aktuell och föregående månad.

I panelen Trafikanalys visas Internetaktivitet i datorn i realtid, inklusive volym och hastighet för senaste inkommande och utgående Internettrafik i din dator, anslutningshastighet och totalt antal byte som överförts över Internet.

Den heldragna gröna linjen motsvarar aktuell överföringshastighet för inkommande trafik. Den prickade gröna linjen motsvarar genomsnittlig överföringshastighet för inkommande trafik. Om den aktuella och den genomsnittliga överföringshastigheten är samma visas inte den prickade linjen i diagrammet. Den heldragna linjen motsvarar då både genomsnittlig och aktuell överföringshastighet.

Den heldragna röda linjen motsvarar aktuell överföringshastighet för utgående trafik. Den prickade röda linjen motsvarar genomsnittlig överföringshastighet för utgående trafik. Om den aktuella och den genomsnittliga överföringshastigheten är samma visas inte den prickade linjen i diagrammet. Den heldragna linjen motsvarar då både genomsnittlig och aktuell överföringshastighet.

Analysera inkommande och utgående trafik

Diagrammet för trafikövervakning är en numerisk och grafisk framställning av inkommande och utgående Internettrafik. Med trafikövervakningen visas också de program som för närvarande använder flest nätverksanslutningar på datorn och de IP-adresser som programmen har åtkomst till.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. Klicka på **Trafikövervakning** på verktygspanelen.
3. Under **Trafikövervakning** klickar du på **Trafikanalys**.

Tips: Klicka på **Uppdatera** under **Trafikanalys** om du vill se aktuell statistik.

Övervaka programmens bandbredd

Du kan visa ett cirkeldiagram som avslöjar ungefär hur mycket bandbredd i procent som använts av de mest aktiva programmen på datorn under de senaste 24 timmarna. I cirkeldiagrammet kan du se den relativa bandbreddsmängden som används av de olika programmen.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. Klicka på **Trafikövervakning** på verktygspanelen.
3. Under **Trafikövervakning** klickar du på **Trafikanvändning**.

Tips: Klicka på **Uppdatera** under **Trafikanvändning** om du vill se aktuell statistik.

Övervaka programmens aktiviteter

Du kan visa programmens inkommande och utgående aktiviteter. Då visas bl.a. fjärranslutningar till andra datorer och portar.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. Klicka på **Trafikövervakning** på verktygspanelen.
3. Under **Trafikövervakning** klickar du på **Aktiva program**.
4. Du kan visa följande information:
   - Programaktivitetsdiagram. Välj ett program så visas ett diagram över dess aktiviteter.
   - Lyssnande anslutning. Välj ett lyssningsobjekt under programnamnet.
   - Datoranslutning: Välj en IP-adress under programnamnet, systemprocessen eller tjänsten.

Obs! Klicka på **Uppdatera** under **Aktiva program** om du vill se aktuell statistik.

KAPITEL 22

Mer information om Internetsäkerhet

Med Firewall förstärks säkerhetswebbplatsen för McAfee HackerWatch för att tillhandahålla uppdaterad information om program och global Internetaktivitet. HackerWatch innehåller också en självstudiekurs om Firewall i HTML-format.

I detta kapitel

Starta HackerWatch-vägledningen

Om du vill veta mer om Firewall kan du öppna HackerWatch-vägledningen i SecurityCenter.

1. Se till att Avancerat-menyn är aktiverad och klicka sedan på **Verktyg**.
2. I Verktygspanelen klickar du på **HackerWatch**.
3. Under **HackerWatch-resurser** klickar du på **Visa vägledning**.

KAPITEL 23

McAfee QuickClean

QuickClean förbättrar datorns prestanda genom att radera filer som kan överbelasta datorn. Det tömmer Papperskorgen och raderar tillfälliga filer, genvägar, förlorade filfragment, registerfiler, cachelagrade filer, cookies, webbläsarhistorik, skickad och borttagen e-post, listor över senast använda filer, Active-X-filer och filer för systemåterställningspunkter. QuickClean skyddar också dina privata uppgifter genom att använda komponenten McAfee Shredder för att säkert och permanent radera objekt som kan innehålla känslig personlig information, t.ex. namn och adress. Se McAfee Shredder för mer information om att rensa filer.

Diskdefragmenteraren ordnar filer och mappar på datorn så att de inte sprids ut (eller fragmenteras) när de sparas på hårddisken. Genom att defragmentera hårddisken med jämna mellanrum ser du till att fragmenterade filer och mappar sammanfogas så att det går snabbt att hämta dem senare.

Om du inte vill underhålla datorn manuellt kan du schemalägga att både QuickClean och Diskdefragmenteraren ska köras automatiskt som oberoende åtgärder med valfria mellanrum.

Obs! SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician.

I detta kapitel

Funktioner i QuickClean

QuickClean innehåller olika rensningsfunktioner som tar bort onödiga filer säkert och effektivt. Genom att ta bort sådana filer ökar du utrymmet på datorns hårddisk och förbättrar dess prestanda.

Rensa datorn

QuickClean raderar filer som kan överbelasta datorn. Det tömmer Papperskorgen och raderar tillfälliga filer, genvägar, förlorade filfragment, registerfiler, cachelagrade filer, cookies, webbläsarhistorik, skickad och borttagen e-post, listor över senast använda filer, Active-X-filer och filer för systemåterställningspunkter. QuickClean raderar dessa objekt utan att påverka annan viktig information.

Du kan använda någon av QuickCleans rengöringsfunktioner för att ta bort onödiga filer från datorn. Följande tabell beskriver rensningsfunktionerna i QuickClean:

Namn	Funktion
Rensning av papperskorgen	Tar bort filer i Papperskorgen.
Rensning av temporära filer	Raderar filer lagrade i temporära mappar.
Rensning av genvägar	Raderar brutna genvägar och genvägar som inte har ett tillhörande program.
Rensning av förlorade filfragment	Raderar förlorade filfragment på datorn.
Registerrensning	Raderar information i Windows-registret för program som inte längre finns i datorn. Registret är en databas där Windows lagrar konfigurationsinformation. Registret innehåller profiler för varje användare och information om datorns maskinvara, installerade program och egenskapsinställningar. Windows använder informationen hela tiden under driften.
Rensning av cacheminnet	Raderar cachelagrade filer som samlas när du söker dig fram på webbsidor. Filerna lagras vanligtvis som temporära filer i en cachemapp. En cachemapp är ett tillfälligt lagringsområde på datorn. För att det ska gå snabbare och bli mer effektivt att surfa på webben, kan webbläsaren hämta en webbsida från cacheminnet (istället för från en fjärransluten server) nästa gång du vill se den.

Cookierensning	Raderar cookies. Filerna lagras vanligtvis som tillfälliga filer. En cookie är en liten fil som innehåller information, vanligen ett användarnamn och aktuellt datum och tid, som lagras på datorn hos någon som surfar på webben. Cookies används främst av webbplatser för att identifiera användare som tidigare har registrerat sig på eller besökt webbplatsen. De kan dock också användas av hackare för att utvinna information.
Rensning av webbläsarhistorik	Raderar webbläsarhistoriken.
E-postrensning för Outlook Express och Outlook (skickade och raderade objekt)	Raderar skickad och borttagen e-post från Outlook® och Outlook Express.
Rensning av senast använda	Raderar senast använda filer som skapats med något av följande program: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows-historik ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX-rensning	Raderar ActiveX-kontroller. ActiveX är en programvarukomponent som används av program eller webbsidor för att lägga till funktioner som smälter in och visas som en normal del av programmet eller webbsidan. De flesta ActiveX-kontroller är oskadliga, men vissa kan samla in information från datorn.
Rensning av systemåterställningspunkter	Raderar gamla systemåterställningspunkter (utom den senaste) från datorn. Systemåterställningspunkter skapas av Windows för att markera ändringar som görs på datorn så att du kan återgå till ett tidigare tillstånd om några problem skulle uppstå.

Rensa datorn

Du kan använda någon av QuickCleans rengöringsfunktioner för att ta bort onödiga filer från datorn. Under **QuickClean-sammanfattning** ser du när du är klar hur mycket diskutrymme som frigjordes efter rensningen, hur många filer som raderades samt datum och tid för när den senaste QuickClean-åtgärden kördes på datorn.

1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
2. Under **McAfee QuickClean** klickar du på **Starta**.
3. Välj någon av de följande åtgärderna:
   - Klicka på **Nästa** för att acceptera standardrensningsfunktionerna i listan.
   - Markera eller avmarkera rensningsfunktionerna och klicka sedan på **Nästa**.Om du väljer Rensning av senast använda kan du klicka på **Egenskaper** för att markera eller avmarkera filer som skapats nyligen med programmen i listan och sedan klicka på **OK**.
   - Klicka på **Återställ standardvärden** om du vill återställa standardrensningsfunktionerna och klicka därefter på **Nästa.**
4. När analysen är klar klickar du på **Nästa**.
5. Klicka på **Nästa** för att bekräfta borttagningen.
6. Välj någon av de följande åtgärderna:
   - Klicka på **Nästa** för att acceptera standardalternativet **Nej, jag vill ta bort filerna med vanlig Windows-borttagning**.
   - Klicka på **Ja, jag vill radera mina filer på ett säkert sätt med Shredder**, ange antal pass (upp till 10) och klicka sedan på **Nästa**. Det kan ta ett tag att rensa filer om det är mycket information som rensas.
7. Om några filer eller objekt var låsta under rensningen kan du uppmanas att starta om datorn. Klicka på **OK** för att stänga uppmaningen.
8. Klicka på **Slutför**.

Obs! Filer som har tagits bort med Shredder kan inte återskapas. Se McAfee Shredder för mer information om att rensa filer.

Defragmentera datorn

Diskdefragmenteraren ordnar filer och mappar på datorn så att de inte sprids ut (eller fragmenteras) när de sparas på hårddisken. Genom att defragmentera hårddisken med jämna mellanrum ser du till att fragmenterade filer och mappar sammanfogas så att det går snabbt att hämta dem senare.

Defragmentera datorn

Du kan defragmentera datorn för att förbättra prestanda när datorn skriver och läser filer och mappar.

1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
2. Under **Diskdefragmenteraren** klickar du på **Analysera**.
3. Följ anvisningarna på skärmen.

Obs! Mer information om Diskdefragmenteraren finns i hjälpen till Windows.

Schemalägga en åtgärd

Med Schemaläggaren kan du automatisera hur ofta QuickClean eller Diskdefragmenteraren ska köras på datorn. Du kan t.ex. schemalägga att QuickClean ska tömma Papperskorgen varje söndag 18.00 eller att Diskdefragmenteraren ska defragmentera hårddisken den sista dagen i varje månad. Du kan skapa, ändra eller ta bort en åtgärd när som helst. Du måste vara inloggad på datorn för att en schemalagd åtgärd ska köras. Om en åtgärd inte körs av någon anledning ändras tiden till fem minuter efter att du loggar in igen.

Schemalägg en QuickClean-åtgärd

Du kan schemalägga att en QuickClean-åtgärd ska rensa datorn automatiskt med en eller flera rensningsfunktioner. När åtgärden har slutförts kan du se datum och tid för när den är schemalagd att köras igen under **QuickClean-sammanfattning**.

1 Öppna panelen Schemaläggaren.

   Hur?

   1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i McAfee SecurityCenter.
   2. Under **Schemaläggaren** klickar du på **Starta**.

2 I listan **Välj en åtgärd som ska schemaläggas** klickar du på **McAfee QuickClean**.

3 Skriv in ett namn för åtgärden i rutan **Aktivitetsnamn** och klicka sedan på **Skapa**.

4 Välj någon av de följande åtgärderna:

   - Klicka på **Nästa** för att acceptera rensningsfunktionerna i listan.
   - Markera eller avmarkera rensningsfunktionerna och klicka sedan på **Nästa**. Om du väljer Rensning av senast använda kan du klicka på **Egenskaper** för att markera eller avmarkera filer som skapats nyligen med programmen i listan och sedan klicka på **OK**.
   - Klicka på **Återställ standardvärden** om du vill återställa standardrensningsfunktionerna och klicka därefter på **Nästa**.

5 Välj någon av de följande åtgärderna:

   - Klicka på **Schema** för att acceptera standardalternativet **Nej, jag vill ta bort filerna med vanlig Windows-borttagning**.

- Klicka på **Ja, jag vill radera mina filer på ett säkert sätt med Shredder**, ange antal pass (upp till 10) och klicka sedan på **Schema**.

6 I dialogrutan **Schema** väljer du hur ofta du vill att åtgärden ska utföras. Klicka sedan på **OK**.

7 Om du ändrade egenskaperna för Rensning av senast använda kan du bli uppmanad att starta om datorn. Klicka på **OK** för att stänga uppmaningen.

8 Klicka på **Slutför**.

Obs! Filer som har tagits bort med Shredder kan inte återskapas. Se McAfee Shredder för mer information om att rensa filer.

Ändra en QuickClean-åtgärd

Du kan ändra en schemalagd QuickClean-åtgärd för att ändra de rensningsfunktioner den använder eller hur ofta den ska köras automatiskt på datorn. När åtgärden har slutförts kan du se datum och tid för när den är schemalagd att köras igen under **QuickClean-sammanfattning**.

1 Öppna panelen Schemaläggaren.

Hur?

1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i McAfee SecurityCenter.
2. Under **Schemaläggaren** klickar du på **Starta**.

2 I listan **Välj en åtgärd som ska schemaläggas** klickar du på **McAfee QuickClean**.

3 Markera åtgärden i listan **Välj en befintlig uppgift** och klicka sedan på **Ändra**.

4 Välj någon av de följande åtgärderna:

- Klicka på **Nästa** för att acceptera rensningsfunktionerna som valts för åtgärden.
- Markera eller avmarkera rensningsfunktionerna och klicka sedan på **Nästa**. Om du väljer Rensning av senast använda kan du klicka på **Egenskaper** för att markera eller avmarkera filer som skapats nyligen med programmen i listan och sedan klicka på **OK**.
- Klicka på **Återställ standardvärden** om du vill återställa standardrensningsfunktionerna och klicka därefter på **Nästa.**

5 Välj någon av de följande åtgärderna:

- Klicka på **Schema** för att acceptera standardalternativet **Nej, jag vill ta bort filerna med vanlig Windows-borttagning**.

- Klicka på **Ja, jag vill radera mina filer på ett säkert sätt med Shredder**, ange antal pass (upp till 10) och klicka sedan på **Schema**.

6 I dialogrutan **Schema** väljer du hur ofta du vill att åtgärden ska utföras. Klicka sedan på **OK**.

7 Om du ändrade egenskaperna för Rensning av senast använda kan du bli uppmanad att starta om datorn. Klicka på **OK** för att stänga uppmaningen.

8 Klicka på **Slutför**.

Obs! Filer som har tagits bort med Shredder kan inte återskapas. Se McAfee Shredder för mer information om att rensa filer.

Ta bort en QuickClean-åtgärd

Du kan ta bort en schemalagd QuickClean-åtgärd om du inte längre vill att den ska köras automatiskt.

1 Öppna panelen Schemaläggaren.

Hur?

1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i McAfee SecurityCenter.
2. Under **Schemaläggaren** klickar du på **Starta**.

2 I listan **Välj en åtgärd som ska schemaläggas** klickar du på **McAfee QuickClean**.

3 Välj åtgärden i listan **Välj en befintlig uppgift**.

4 Klicka på **Ta bort** och sedan på **Ja** för att bekräfta borttagningen.

5 Klicka på **Slutför**.

Schemalägg en åtgärd med Diskdefragmenteraren

Du kan schemalägga en åtgärd med Diskdefragmenteraren om du vill ställa in hur ofta datorns hårddisk ska defragmenteras automatiskt. När åtgärden har slutförts kan du se datum och tid för när den är schemalagd att köras igen under **Diskdefragmenteraren**.

1 Öppna panelen Schemaläggaren.

Hur?

1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i McAfee SecurityCenter.
2. Under **Schemaläggaren** klickar du på **Starta**.

2 I listan **Välj en åtgärd som ska schemaläggas** klickar du på **Diskdefragmenteraren**.

3 Skriv in ett namn för åtgärden i rutan **Aktivitetsnamn** och klicka sedan på **Skapa**.

4 Välj någon av de följande åtgärderna:

- Klicka på **Schema** om du vill acceptera standardalternativet **Utför defragmentering även om mängden ledigt utrymme är låg**.
- Avmarkera alternativet **Utför defragmentering även om mängden ledigt utrymme är låg** och klicka sedan på **Schema**.

5 I dialogrutan **Schema** väljer du hur ofta du vill att åtgärden ska utföras. Klicka sedan på **OK**.

6 Klicka på **Slutför**.

Ändra en åtgärd med Diskdefragmenteraren

Du kan ändra en schemalagd Diskdefragmenteraren-åtgärd om du vill ändra hur ofta den ska köras automatiskt på datorn. När åtgärden har slutförts kan du se datum och tid för när den är schemalagd att köras igen under **Diskdefragmenteraren**.

1 Öppna panelen Schemaläggaren.

Hur?

1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i McAfee SecurityCenter.
2. Under **Schemaläggaren** klickar du på **Starta**.

2 I listan **Välj en åtgärd som ska schemaläggas** klickar du på **Diskdefragmenteraren**.

3 Markera åtgärden i listan **Välj en befintlig uppgift** och klicka sedan på **Ändra**.

4 Välj någon av de följande åtgärderna:

- Klicka på **Schema** om du vill acceptera standardalternativet **Utför defragmentering även om mängden ledigt utrymme är låg**.
- Avmarkera alternativet **Utför defragmentering även om mängden ledigt utrymme är låg** och klicka sedan på **Schema**.

5 I dialogrutan **Schema** väljer du hur ofta du vill att åtgärden ska utföras. Klicka sedan på **OK**.

6 Klicka på **Slutför**.

Ta bort en åtgärd med Diskdefragmenteraren

Du kan ta bort en schemalagd Diskdefragmenteraren-åtgärd om du inte längre vill att den ska köras automatiskt.

1. Öppna panelen Schemaläggaren.

   Hur?

   1. Klicka på **Underhåll datorn** under **Vanliga uppgifter** i McAfee SecurityCenter.
   2. Under **Schemaläggaren** klickar du på **Starta**.

2. I listan **Välj en åtgärd som ska schemaläggas** klickar du på **Diskdefragmenteraren**.
3. Välj åtgärden i listan **Välj en befintlig uppgift**.
4. Klicka på **Ta bort** och sedan på **Ja** för att bekräfta borttagningen.
5. Klicka på **Slutför**.

KAPITEL 24

McAfee Shredder

McAfee Shredder raderar (eller rensar) objekt permanent från datorns hårddisk. Även om du tar bort filer och mappar, tömmer Papperskorgen eller raderar mappen Tillfälliga Internet-filer manuellt, kan du ändå komma åt informationen med rätt verktyg. Det kan också gå att återskapa en raderad fil eftersom vissa program gör tillfälliga osynliga kopior av öppna filer. Med Shredder kan du skydda dina privata uppgifter genom att på ett säkert sätt radera filer som du inte längre vill ha kvar. Det är viktigt att känna till att rensade filer inte går att återställa

Obs! SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician.

I detta kapitel

Funktioner i Shredder

Shredder raderar objekt från datorns hårddisk så att informationen i dem inte kan återskapas. Programmet skyddar din privata information genom att fullständigt radera filer och mappar, objekt i Papperskorgen och tillfälliga Internetfiler, samt innehållet på hela diskar, t.ex. återskrivbara cd-skivor, externa hårddiskar och disketter.

Rensa filer, mappar och diskar

Shredder ser till att informationen i raderade filer och mappar i Papperskorgen och i Tillfälliga Internet-filer inte går att återskapa ens med specialverktyg. Med Shredder kan du ange hur många gånger (upp till 10) du vill att ett objekt ska rensas. Ett högre rensningsvärde ökar tryggheten för en säker filradering.

Rensa filer och mappar

Du kan rensa filer och mappar från datorns hårddisk, inklusive objekt i Papperskorgen och mappen för tillfälliga Internetfiler.

1 Öppna **Shredder**.

   Hur?

   1. Klicka på **Avancerad meny** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
   2. Klicka på **Verktyg** i den vänstra panelen.
   3. Klicka på **Shredder**.

2 Under **Jag vill** i rutan Rensa filer och mappar klickar du på **Radera filer och mappar**.

3 Under **Rensningsnivå** väljer du någon av följande rensningsnivåer:

   - **Snabb**: rensar valda objekt en gång.
   - **Grundlig**: rensar valda objekt sju gånger.
   - **Anpassa**: rensar valda objekt upp till tio gånger.

4 Klicka på **Nästa**.

5 Välj någon av de följande åtgärderna:

   - I listan **Välj filer att rensa** klickar du antingen på **Innehåll i Papperskorgen** eller **Tillfälliga Internet-filer**.
   - Klicka på **Bläddra** för att navigera till de filer som du vill rensa, markera dem och klicka på **Öppna**.

6 Klicka på **Nästa**.

7 Klicka på **Start** .

8 När Shredder är klart klickar du på **Klar**.

Obs! Arbeta inte med några filer tills Shredder har slutfört rensningen.

Rensa en hel disk

Du kan rensa hela innehållet på en disk på en gång. Det går bara att rensa flyttbara enheter, t.ex. externa hårddiskar, återskrivbara cd-skivor och disketter.

1 Öppna **Shredder**.

   Hur?

   1. Klicka på **Avancerad meny** under **Vanliga uppgifter** i panelen McAfee SecurityCenter.
   2. Klicka på **Verktyg** i den vänstra panelen.
   3. Klicka på **Shredder**.

2 Under **Jag vill** i rutan Rensa filer och mappar klickar du på **Radera en hel disk**.

3 Under **Rensningsnivå** väljer du någon av följande rensningsnivåer:

   - **Snabb**: rensar den valda enheten en gång.
   - **Grundlig**: rensar den valda enheten sju gånger.
   - **Anpassa**: rensar den valda enheten upp till tio gånger.

4 Klicka på **Nästa**.

5 I listan **Välj disk** klickar du på den enhet du vill rensa.

6 Klicka på **Nästa** och sedan på **Ja** för att bekräfta.

7 Klicka på **Start**.

8 När Shredder är klart klickar du på **Klar**.

Obs! Arbeta inte med några filer tills Shredder har slutfört rensningen.

KAPITEL 25

McAfee Network Manager

Network Manager ger en grafisk vy över de datorer och komponenter som utgör ditt hemnätverk. Du kan använda Network Manager för att fjärrstyra skyddsstatusen för varje hanterad dator i ditt nätverk, eller för att fjärråtgärda rapporterade säkerhetsproblem på datorerna.

Innan du använder Network Manager kan du bekanta dig med några av funktionerna. Information om hur du konfigurerar och använder dessa funktioner hittar du i Network Manager-hjälpen.

Obs! SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician.

I detta kapitel

Network Manager-funktioner

Network Manager tillhandahåller följande funktioner.

Grafisk nätverkskarta

Network Managers nätverkskarta ger en grafisk överblick över skyddstillståndet för de datorer och komponenter som utgör ditt hemnätverk. När du gör ändringar i nätverket (till exempel lägger till en ny dator) identifierar nätverkskartan dessa ändringar. Du kan uppdatera nätverkskartan, ändra namn på nätverket, och visa eller dölja komponenter på nätverkskartan för att anpassa översikten. Du kan också visa information om komponenterna som visas på nätverkskartan.

Fjärrhantering

Använd Network Managers nätverkskarta när du vill hantera skyddsstatusen för de datorer som utgör ditt hemnätverk. Du kan bjuda in en dator att gå med i det hanterade nätverket, övervaka den hanterade datorns skyddsstatus och korrigera kända säkerhetsproblem från en fjärrdator på nätverket.

Förstå Network Manager-ikoner

Följande tabell beskriver de vanligaste ikonerna som används i Network Managers nätverkskarta.

Ikon	Beskrivning
	Representerar en hanterad dator som är online
	Representerar en hanterad dator som är offline
	Representerar en ohanterad dator som har SecurityCenter installerat
	Representerar en ohanterad dator som är offline
	Representerar en dator som är online men inte har SecurityCenter installerat, eller en okänd nätverksenhet
	Representerar en dator som är offline men inte har SecurityCenter installerat, eller en okänd nätverksenhet som är offline
	Visar att motsvarande objekt är anslutet och skyddat
	Visar att motsvarande objekt kan kräva din uppmärksamhet
	Visar att motsvarande objekt kräver din omedelbara uppmärksamhet
	Representerar en trådlös router
	Representerar en vanlig router
	Representerar Internet, när du är ansluten
	Representerar Internet, när du inte är ansluten

KAPITEL 26

Konfigurera ett hanterat nätverk

Du konfigurerar ett hanterat nätverk genom att arbeta med objekten i nätverkskartan och lägga till medlemmar (datorer) i nätverket. Innan en dator kan bli fjärrstyrd eller ges tillåtelse att fjärrstyra andra datorer i nätverket måste den bli en tillförlitlig medlem av nätverket. Medlemskap i nätverket ges till nya datorer av nätverksmedlemmar (datorer) med administrativ behörighet.

Du kan visa information om komponenterna som visas på nätverkskartan, även efter du gjort ändringar i nätverket (till exempel lagt till en ny dator).

I detta kapitel

Arbeta med nätverkskartan

När du ansluter en dator till nätverket analyserar Network Manager nätverket för att fastställa om det finns några hanterade eller ohanterade medlemmar, vilka routerattributen är och Internetstatusen. Om inga medlemmar hittas antar Network Manager att den nu anslutande datorn är den första datorn på nätverket och gör då datorn till en hanterad medlem med administrationsbehörighet. Som standard innehåller nätverksnamnet arbetsgrupp- eller domännamnet på den första datorn som ansluter till nätverket och som har SecurityCenter installerad, men du kan ändra namn på nätverket när du vill.

När du gör ändringar i nätverket (till exempel lägger till en ny dator) kan du anpassa nätverkskartan. Du kan till exempel uppdatera nätverkskartan, ändra namn på nätverket, och visa eller dölja komponenter på nätverkskartan för att anpassa översikten. Du kan också visa information om komponenterna som visas på nätverkskartan.

Få tillgång till nätverkskartan

Nätverkskartan ger en grafisk representation av datorerna och komponenterna som utgör ditt hemmanätverk.

- Klicka på **Hantera nätverket** på Grundläggande meny eller Avancerad meny.

Obs! Första gången du använder nätverkskartan uppmanas du lita på de andra datorerna i nätverket.

Uppdatera nätverkskartan

Du kan uppdatera nätverkskartan när du vill, till exempel efter att en dator har gått med i det hanterade nätverket.

1. Klicka på **Hantera nätverket** på Grundläggande meny eller Avancerad meny.
2. Klicka på **Uppdatera nätverkskartan** under **Jag vill**.

Obs! Länken **Uppdatera nätverkskartan** är bara tillgänglig när inga andra objekt är markerade på nätverkskartan. Om du vill avmarkera ett objekt klickar du på det, eller klicka på det vita området på nätverkskartan.

Byta namn på nätverket

Som standard innehåller nätverksnamnet arbetsgrupp eller domännamnet på den första datorn som ansluter till nätverket och har SecurityCenter installerad. Om du föredrar ett annat namn kan du ändra det.

1. Klicka på **Hantera nätverket** på Grundläggande meny eller Avancerad meny.
2. Klicka på **Byt namn på nätverket** under **Jag vill**.
3. Ange namnet på nätverket i rutan **Nätverksnamn**.
4. Klicka på **OK**.

Obs! Länken **Byt namn på nätverket** är bara tillgänglig när inga andra objekt är markerade på nätverkskartan. Om du vill avmarkera ett objekt klickar du på det, eller klicka på det vita området på nätverkskartan.

Visa eller dölj ett föremål på nätverkskartan

Som standard visas alla datorer och komponenter i ditt hemnätverk på nätverkskartan. Om du har dolda objekt kan du visa dem igen när du vill. Det går bara att dölja ohanterade objekt, inte hanterade datorer.

Om du vill..	Klicka på **Hantera nätverket** på Grundläggande-menyn eller Avancerad-menyn, och gör sedan detta...
Dölja ett objekt på nätverkskartan	Klicka på ett objekt i nätverkskartan och klicka sedan på **Dölj det här objektet** under **Jag vill**. Klicka sedan på **Ja** i dialogrutan för bekräftelse.
Visa dolda föremål på nätverkskartan	Under **Jag vill** klickar du på **Visa dolda objekt**.

Visa information om objekt

Du kan visa detaljerad information om komponenter i nätverket genom att markera komponenten på nätverkskartan. Denna information innehåller komponentens namn, dess skyddsstatus och annan information som är nödvändig för att hantera den.

1. Klicka på ikonen för ett objekt på nätverkskartan
2. Information om objektet visas under **Detaljer**.

Gå med i det hanterade nätverket

Innan en dator kan bli fjärrstyrd eller ges tillåtelse att fjärrstyra andra datorer i nätverket måste den bli en tillförlitlig medlem av nätverket. Medlemskap i nätverket ges till nya datorer av nätverksmedlemmar (datorer) med administrativ behörighet. För att se till att endast betrodda datorer går med i nätverket måste användare på både datorn som går med och den beviljande datorn autentisera varandra.

När en dator går med i ett nätverk uppmanas den att visa sin McAfee-skyddsstatus för övriga datorer i nätverket. Om en dator går med på att visa sin skyddsstatus blir den en hanterad medlem i nätverket. Om en dator inte går med på att visa sin skyddsstatus blir den en ej hanterad medlem i nätverket. Ohanterade medlemmar i nätverket är vanligtvis gästdatorer som vill komma åt andra nätverksfunktioner (till exempel skicka filer eller dela skrivare).

Obs! Om du har andra McAfee-nätverksprogram installerade (till exempel EasyNetwork) så identifieras datorn också som en hanterad dator i dessa program. Behörighetsnivån som tilldelas en dator i Network Manager gäller också för andra McAfee-nätverksprogram. Mer information om vad gäst, full eller administrativ behörighet innebär i andra McAfee-nätverksprogram finns dokumentationen för relevant program.

Gå med i ett hanterat nätverk

När du får en inbjudan att gå med i ett hanterat nätverk kan du acceptera eller avvisa den. Du kan också bestämma om du vill att den här datorn och andra datorer i nätverket ska övervaka varandras säkerhetsinställningar (till exempel om en dators virusskydd är uppdaterat).

1. Kontrollera att kryssrutan **Tillåt alla datorer i nätverket att övervaka säkerhetsinställningar** är markerad i dialogrutan Hanterat n'tverk.
2. Klicka på **Gå med**.
   När du accepterar inbjudan visas två spelkort.
3. Bekräfta att dessa två spelkort är desamma som visas på datorn som skickade inbjudan om att gå med i det hanterade nätverket.
4. Klicka på **OK**.

Obs! Om datorn som skickade inbjudan inte visar samma spelkort som i dialogrutan för säkerhetsbekräftelse, så har ett säkerhetsproblem uppstått i det hanterade nätverket. Att gå med i nätverket kan innebära en risk för din dator. Klicka därför på **Avbryt** i dialogrutan Hanterat nätverk.

Bjud in en dator att gå med i det hanterade nätverket

Om en dator läggs till det i hanterade nätverket eller om en annan ohanterad dator finns i nätverket kan du bjuda in den datorn till det hanterade nätverket. Endast datorer med administrativa behörigheter i nätverket kan bjuda in andra datorer. När du skickar inbjudan kan du också ange vilken behörighetsnivå du vill ge den dator som går med i nätverket.

1. Klicka på en ohanterad dators ikon på nätverkskartan.
2. Klicka på **Övervaka den här datorn** under **Jag vill**.
3. Gör något av följande i dialogrutan Bjud in en dator att gå med i det hanterade nätverket:
   - Ge datorn tillgång till nätverket genom att klicka på **Tillåt gäståtkomst till hanterade nätverksprogram** (du kan använda det här alternativet för tillfälliga användare i hemmet).
   - Ge datorn tillgång till nätverket genom att klicka på **Tillåt fullständig åtkomst till hanterade nätverksprogram**.
   - Ge datorn tillgång till nätverket med administratörsbehörighet genom att klicka på **Tillåt administrativ åtkomst till hanterade nätverksprogram**. Det gör att datorn kan bevilja åtkomst till andra datorer som vill gå med i det hanterade nätverket.
4. Klicka på **OK**.
   En inbjudan att gå med i det hanterade nätverket skickas nu till datorn. När datorn accepterar inbjudan visas två spelkort.
5. Bekräfta att dessa två spelkort är desamma som visas på datorn som du bjöd in om att gå med i det hanterade nätverket.
6. Klicka på **Bevilja åtkomst**.

Obs! Om datorn som du bjöd in inte visar samma spelkort som visas i dialogrutan för säkerhetsbekräftelse, så har ett säkerhetsproblem uppstått i det hanterade nätverket. Att låta datorn gå med i nätverket kan innebära en risk för andra datorer. Klicka därför på **Avvisa åtkomst** i dialogrutan för säkerhetsbekräftelse.

Sluta lita på datorer i nätverket

Om du av misstag litade på andra datorer i nätverket kan du sluta lita på dem.

- Klicka på **Sluta lita på datorer i det här nätverket** under **Jag vill**.

Obs! Länken **Sluta lita på datorer i det här nätverket** är inte tillgänglig om du har administrativ behörighet och det finns andra hanterade datorer i nätverket.

KAPITEL 27

Fjärrstyra nätverket

Efter att du konfigurerat ditt hanterade nätverk kan du fjärrstyra datorerna och komponenterna som utgör ditt nätverk. Du kan genom fjärrstyrning övervaka statusen och behörighetsnivån på datorerna och komponenterna samt åtgärda säkerhetsproblem.

I detta kapitel

Övervaka status och behörighet

Ett hanterat nätverk kan ha hanterade och ohanterade medlemmar. Hanterade medlemmar tillåter andra datorer på nätverket att övervaka deras McAfee-skyddsstatus, ohanterade medlemmar gör inte det. Ohanterade medlemmar är vanligtvis gästdatorer som vill komma åt andra nätverksfunktioner (till exempel skicka filer eller dela skrivare). Ohanterade medlemmar kan bli inbjudna att bli hanterade medlemmar när som helst av andra hanterade datorer i nätverket. En hanterad dator kan bli en ohanterad dator när som helst.

Hanterade datorer har gästbehörighet eller full eller administrativ behörighet. Med administrativ behörighet kan hanterade datorer hantera skyddsstatusen hos alla andra hanterade datorer i nätverket och ge andra datorer medlemskap i nätverket. Med full behörighet och gästbehörighet får datorn bara tillgång till nätverket. Du kan ändra en dators behörighetsnivå när som helst.

Ett hanterat nätverk kan också ha enheter (till exempel routrar), och du kan använda Network Manager för att hantera dem också. Du kan också konfigurera och ändra en enhets visningsegenskaper på nätverkskartan.

Övervaka en dators skyddsstatus

Om en dators skyddsstatus inte övervakas på nätverket (datorn är antingen inte medlem eller en ohanterad medlem) kan du skicka en begäran om att få övervaka den.

1. Klicka på en ohanterad dators ikon på nätverkskartan
2. Klicka på **Övervaka den här datorn** under **Jag vill**.

Sluta övervaka en dators skyddsstatus

Du kan sluta övervaka skyddsstatusen för en hanterad dator i ditt nätverk. Datorn blir då ohanterad och du kan inte övervaka dess skyddsstatus via fjärrstyrning.

1. Klicka på en hanterad dators ikon på nätverkskartan.
2. Klicka på **Sluta övervaka den här datorn** under **Jag vill**.
3. Klicka sedan på **Ja** i dialogrutan för bekräftelse.

Anpassa en hanterad dators behörighet

Du kan ändra en hanterad dators behörighetsnivå när som helst. Detta ger dig möjlighet att ändra vilka datorer som kan övervaka skyddsstatusen för andra datorer på nätverket.

1. Klicka på en hanterad dators ikon på nätverkskartan.
2. Klicka på **Ändra tillstånd för den här datorn** under **Jag vill**.
3. I dialogrutan för ändring av tillstånd markerar eller avmarkerar du kryssrutorna för att bestämma om den här

datorn och andra datorer på det hanterade nätverket kan övervaka varandras skyddsstatus.

4 Klicka på **OK**.

Hantera en enhet

Du kan hantera en enhet genom att ansluta till dess administrationswebbsida från Network Manager.

1 Klicka på en enhets ikon på nätverkskartan.

2 Klicka på **Hantera den här enheten** under **Jag vill**. En webbläsare öppnas och visar den här enhetens administrationswebbsida.

3 Ange dina inloggningsuppgifter i webbläsaren och konfigurera sedan enhetens säkerhetsinställningar.

Obs! Om enheten är en trådlös router eller åtkomstpunkt som skyddas av Wireless Network Security måste du använda Wireless Network Security för att konfigurera den här enhetens säkerhetsinställningar.

Anpassa en enhets visningsegenskaper

När du anpassar en enhets visningsegenskaper kan du ändra enhetens visningsnamn på nätverkskartan och ange om enheten är en trådlös router.

1 Klicka på en enhets ikon på nätverkskartan.

2 Klicka på **Ändra enhetsegenskaper** under **Jag vill**.

3 Om du vill ange enhetens visningsnamn skriver du ett namn i rutan **Namn**.

4 Ange enhetens typ genom att klicka på **Router av standardmodell** om den inte är trådlös, och **Trådlös outer** om den är det.

5 Klicka på **OK**.

Åtgärda säkerhetsproblem

Hanterade datorer med administrativ behörighet kan övervaka McAfee-skyddsstatusen hos andra hanterade datorer i nätverket och åtgärda rapporterade säkerhetsproblem via fjärrstyrning. Om exempelvis en hanterad dators McAfee-skyddsstatus visar att VirusScan är avslaget kan en annan hanterad dator med administrativ behörighet aktivera VirusScan via fjärrstyrning.

När du åtgärdar säkerhetssvagheter via fjärrstyrning reparerar Network Manager de flesta rapporterade felen. Vissa säkerhetssvagheter kan dock kräva att man ingriper manuellt på den lokala datorn. Network Manager åtgärdar i så fall de problem som kan åtgärdas via fjärrstyrning och uppmanar dig sedan att åtgärda de kvarstående problemen genom att logga in i SecurityCenter på den sårbara datorn och följa rekommendationerna som ges. I vissa fall rekommenderas att installera den senaste versionen av SecurityCenter på fjärrdatorn eller datorerna i ditt nätverk.

Åtgärda säkerhetsproblem

Du kan använda Network Manager för att åtgärda de vanligaste säkerhetsproblemen på hanterade fjärrdatorer. Om VirusScan till exempel är inaktiverat på en fjärrdator kan du aktivera det.

1. Klicka på ikonen för ett objekt på nätverkskartan
2. Visa föremålets skyddsstatus under **Detaljer**.
3. Klicka på **Åtgärda säkerhetsproblem** under **Jag vill**.
4. När säkerhetsproblemen har åtgärdats klickar du på **OK**.

Obs! Även om Network Manager automatiskt åtgärdar de flesta säkerhetsproblemen kräver vissa reparationer att du startar SecurityCenter på den sårbara datorn och sedan följer rekommendationerna som ges.

Installera McAfee säkerhetsprogramvara på fjärrdatorer

Skyddsstatusen för datorer i ditt nätverk som inte kör den senaste versionen av SecurityCenter kan inte övervakas via fjärrstyrning. Om du vill övervaka dessa datorer via fjärrstyrning måste den senaste versionen av SecurityCenter installeras på varje dator.

1. Öppna SecurityCenter på den dator där du vill installera säkerhetsprogramvaran.
2. Klicka på **Mitt konto** under **Vanliga uppgifter**.
3. Logga in med e-postadressen och lösenordet som du använde när du registrerade säkerhetsprogrammet första gången du installerade det.
4. Välj rätt produkt, klicka på ikonen **Hämta/installera** och följ instruktionerna på skärmen.

KAPITEL 28

McAfee EasyNetwork

Med EasyNetwork kan du dela filer på ett säkert sätt samt enklare överföra filer och dela skrivare mellan datorerna i hemnätverket. EasyNetwork måste vara installerat på datorerna i hemnätverket för att de ska kunna komma åt dess funktioner.

Innan du använder EasyNetwork kan du bekanta dig med några av funktionerna. Mer information om hur du konfigurerar och använder dessa funktioner hittar du i EasyNetwork-hjälpen.

Obs! SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician.

I detta kapitel

EasyNetwork-funktioner

EasyNetwork erbjuder följande funktioner.

Fildelning

Med EasyNetwork är det enkelt att dela filer med andra datorer i nätverket. När du delar filer ger du andra datorer tillåtelse att läsa dessa filer. Endast datorer som har full eller administrativ åtkomst till det hanterade nätverket (medlemmar) kan dela filer och ha åtkomst till filer delade av andra medlemmar.

Filöverföring

Du kan skicka filer till andra datorer som har full eller administrativ åtkomst till det hanterade nätverket (medlemmar). När du tar emot en fil hamnar den i EasyNetwork-inkorgen. Inkorgen är en tillfällig lagringsplats för alla filer som andra datorer i nätverket skickar till dig.

Automatisk skrivardelning

När du har gått med i ett hanterat nätverk kan du dela lokala skrivare kopplade till din dator med andra användare. Skrivarens aktuella namn används som det delade skrivarnamnet. Programmet identifierar också skrivare som delas av andra datorer i nätverket och gör det möjligt för dig att konfigurera och använda dessa skrivare.

KAPITEL 29

Konfigurera EasyNetwork

Innan du kan använda EasyNetwork måste du starta programmet och ansluta till ett hanterat nätverk. När du har anslutit till ett hanterat nätverk kan du söka efter, dela och skicka filer till andra datorer i nätverket. Du kan också dela skrivare. Du kan lämna nätverket när du vill.

I detta kapitel

Öppna EasyNetwork

Som standard uppmanas du att starta EasyNetwork efter installationen, men du kan också starta EasyNetwork senare.

- Klicka på **Start**-menyn, peka på **Program**, på **McAfee** och klicka sedan på **McAfee EasyNetwork**.

Tips: Om du skapade skrivbords- och snabbstartsikoner under installationen kan du starta EasyNetwork genom att dubbelklicka på McAfee EasyNetwork-ikonen på ditt skrivbord eller i meddelandefältet längst till höger i aktivitetsfältet.

Ansluta till ett hanterat nätverk

Om inga datorer i nätverket som du är anslutet till har SecurityCenter blir du medlem i nätverket och tillfrågas om nätverket är tillförlitligt. Eftersom din dator var den första som anslöt till nätverket ingår ditt datornamn i nätverksnamnet, men du kan byta namn på nätverket när du vill.

När en dator ansluter till nätverket skickar den en anslutningsbegäran till de andra datorerna i nätverket. Begäran kan godkännas av alla datorer med administratörsbehörighet i nätverket. Den som utfärdat godkännandet kan också välja behörighetsnivå för datorn som ansluter till nätverket, till exempel gäst (endast filöverföringsbehörighet) eller full/administrativ (filöverföring och fildelning). I EasyNetwork kan datorer med administrativ behörighet ändra andra datorers behörighet (höja eller sänka behörighet). Datorer med full behörighet kan inte utföra sådana administrativa uppgifter.

Obs! Om du har andra McAfee-nätverksprogram installerade (till exempel Network Manager) så identifieras datorn också som en hanterad dator i dessa program. Behörighetsnivån som tilldelas en dator i EasyNetwork gäller också för andra McAfee-nätverksprogram. Mer information om vad gäst, full eller administrativ behörighet innebär i andra McAfee-nätverksprogram finns dokumentationen för relevant program.

Ansluta till nätverket

När en dator ansluts till ett tillförlitligt nätverk för första gången efter installationen av EasyNetwork visas ett meddelande där du tillfrågas om du vill gå med i det hanterade nätverket. Om datorn går med i nätverket skickas en förfrågan till alla datorer i nätverket som har administrativ behörighet. Denna förfrågan måste beviljas innan datorn kan dela skrivare och filer samt skicka och kopiera filer i nätverket. Den första datorn i nätverket tilldelas automatiskt administratörsbehörigheter.

1. I fönstret Delade filer klickar du på **Ja, gå med nu**. När en administrativ dator i nätverket beviljar din begäran visas ett meddelande som frågar om den här och andra datorer på nätverket ska kunna ändra varandras säkerhetsinställningar.
2. Om du vill tillåta att den här datorn och andra datorer i nätverket ändrar varandras säkerhetsinställningar klickar du på **OK**. Klicka annars på **Avbryt**.
3. Bekräfta att den beviljande datorn visar de spelkort som visas i dialogrutan för säkerhetsbekräftelse, och klicka sedan på **OK**.

Obs! Om datorn som skickade inbjudan inte visar samma spelkort som i dialogrutan för säkerhetsbekräftelse, så har ett säkerhetsproblem uppstått i det hanterade nätverket. Att gå med i nätverket kan innebära en risk för din dator. Klicka därför på **Avbryt** i dialogrutan för säkerhetsbekräftelse.

Bevilja åtkomst till nätverket

När en dator begär att få gå med i det hanterade nätverket skickas ett meddelande till de andra datorerna i nätverket som har administrativ åtkomst. Den första datorn som svarar blir den beviljande. Som den beviljande ansvarar du för att bestämma vilken typ av behörighet datorn ska få: gäst, full eller administrativ.

1. Klicka på lämplig behörighetsnivå i varningsdialogrutan.
2. Gör något av följande i dialogrutan Bjud in en dator att gå med i det hanterade nätverket:
   - Ge datorn tillgång till nätverket genom att klicka på **Tillåt gäståtkomst till hanterade nätverksprogram** (du kan använda det här alternativet för tillfälliga användare i hemmet).
   - Ge datorn tillgång till nätverket genom att klicka på **Tillåt fullständig åtkomst till hanterade nätverksprogram**.

- Ge datorn tillgång till nätverket med administratörsbehörighet genom att klicka på **Tillåt administrativ åtkomst till hanterade nätverksprogram**. Det gör att datorn kan bevilja åtkomst till andra datorer som vill gå med i det hanterade nätverket.

3 Klicka på **OK**.

4 Bekräfta att datorn visar de spelkort som visas i dialogrutan för säkerhetsbekräftelse, och klicka sedan på **Bevilja åtkomst**.

Obs! Om datorn inte visar samma spelkort som visas i dialogrutan för säkerhetsbekräftelse så har ett säkerhetsproblem uppstått i det hanterade nätverket. Att bevilja den datorn tillgång till nätverket kan innebära en risk för din dator. Klicka därför på **Avvisa åtkomst** i dialogrutan för säkerhetsbekräftelse.

Byta namn på nätverket

Som standard innehåller nätverksnamnet namnet på den första datorn som gick med i nätverket, men du kan ändra nätverksnamnet när du vill. När du byter namn på nätverket ändrar du nätverksbeskrivningen som visas i EasyNetwork.

1. Klicka på **Konfigurera** på **Alternativ**-menyn.
2. Skriv namnet på nätverket i rutan **Nätverksnamn** i dialogrutan Konfigurera.
3. Klicka på **OK**.

Lämna ett hanterat nätverk

Om du går med i ett hanterat nätverk men sedan beslutar dig för att du inte vill vara medlem kan du lämna nätverket. När du har lämnat det hanterade nätverket kan du ansluta till det igen, men du måste få tillstånd på nytt. Mer information finns i Ansluta till ett hanterat nätverk (sida 160).

Lämna ett hanterat nätverk

Du kan lämna ett hanterat nätverk som du tidigare har gått med i.

1. Klicka på **Lämna Nätverk** på **Verktyg**-menyn.
2. Markera namnet på det nätverk du vill lämna i dialogrutan Lämna nätverk.
3. Klicka på **Lämna nätverk**.

KAPITEL 30

Dela och skicka filer

Med EasyNetwork är det enkelt att skicka filer och dela dem med andra datorer i nätverket. När du delar filer ger du andra datorer tillåtelse att läsa dem. Endast datorer som är medlemmar i det hanterade nätverket (full eller administrativ åtkomst) kan dela filer och ha åtkomst till filer delade av andra datorer.

Obs!Om du delar ett stort antal filer kan det påverka datorns resurser.

I detta kapitel

Dela filer

Endast datorer som är medlemmar i det hanterade nätverket (full eller administrativ åtkomst) kan dela filer och ha åtkomst till filer delade av andra datorer. Om du delar en mapp kommer alla filer i mappen och dess undermappar också delas, men filer som senare läggs till i mappen delas inte automatiskt. Om en delad fil eller mapp tas bort så försvinner den från fönstret Delade filer. Du kan sluta dela en fil när som helst.

Du kan komma åt en delad fil genom att öppna den direkt från EasyNetwork, eller genom att kopiera den till din dator och sedan öppna den därifrån. Om din lista över delade filer är lång och det är svårt att se var filen finns kan du söka efter den.

Obs! Filer som delas via EasyNetwork går inte att komma åt från andra datorer med Utforskaren eftersom fildelning via EasyNetwork måste ske över säkra anslutningar.

Dela en fil

När du delar en fil görs den tillgänglig för alla medlemmar med full eller administrativ åtkomst i det hanterade nätverket.

1. Hitta filen du vill dela i Utforskaren.
2. Dra filen från dess plats i Utforskaren till fönstret Delade filer i EasyNetwork.

Tips: Du kan också dela en fil genom att klicka på **Dela Filer** på **Verktyg**-menyn. Gå till mappen där filen du vill dela finns i dialogrutan Dela, markera filen och klicka sedan på **Dela**.

Sluta dela en fil

Om du delar en fil i det hanterade nätverket kan du sluta dela den när du vill. När du slutar dela en fil kan andra medlemmar i det hanterade nätverket inte komma åt den.

1. Klicka på **Stoppa delning av filer** på **Verktyg**-menyn.
2. I dialogrutan Stoppa delning av filer klickar du på de filer du inte längre vill dela.
3. Klicka på **OK**.

Kopiera en delad fil

Kopiera en delad fil om du vill ha kvar den när den inte längre är delad. Du kan kopiera en delad fil från andra datorer på det hanterade nätverket.

- Dra en fil från fönstret Delade filer i EasyNetwork till en plats i Utforskaren eller på skrivbordet.

Tips: Du kan också kopiera en delad fil genom att markera den i EasyNetwork och sedan klicka på **Kopiera till** på **Verktyg**-menyn. Navigera till mappen dit du vill kopiera filen i dialogrutan Kopiera till mapp, markera mappen och klicka sedan på **Spara**.

Söka efter en delad fil

Du kan söka efter en fil som delas av dig eller andra medlemmar i nätverket. Medan du skriver dina sökkriterier visar EasyNetwork motsvarande resultat i fönstret Delade filer.

1. Klicka på **Sök** i fönstret Delade filer.
2. Klicka på lämpligt alternativ (sida 167) i listan **Innehåll**.
3. Skriv en del eller hela av fil eller sökvägen i listan **Filnamn eller sökväg**.
4. Klicka på lämplig filtyp (sida 167) i listan **Filtyp**.
5. I listorna **Från** och **Till** klickar du på de datum som representerar datumintervallen då filen skapades.

Sökkriterier

I följande tabeller beskrivs de sökkriterier du kan ange när du söker efter delade filer.

Namn på filen eller sökväg

Innehåller	Beskrivning
Innehåller alla orden	Söker efter en fil eller sökväg vars namn innehåller alla orden du angett i listan **Filnamn eller sökväg** oberoende av ordning.
Innehåller något av orden	Söker efter en fil eller sökväg vars namn innehåller något av orden du angett i listan **Filnamn eller sökväg**.
Innehåller strängen	Söker efter en fil eller sökväg vars namn innehåller den exakta fras som du angett i listan **Filnamn eller sökväg**.

Typ av fil

Typ	Beskrivning
Valfritt	Söker igenom alla delade filtyper
Dokument	Söker igenom alla delade dokument.
Bild	Söker igenom alla delade bildfiler.
Video	Söker igenom alla delade videofiler.
Ljud	Söker igenom alla delade ljudfiler.
Komprimerade	Söker igenom alla komprimerade filer (t.ex. .zip-filer).

Skicka filer till andra datorer

Du kan skicka filer till andra datorer som är medlemmar i det hanterade nätverket. Innan du skickar en fil kontrollerar EasyNetwork att datorn som tar emot filen har tillräckligt med diskutrymme tillgängligt.

När du tar emot en fil hamnar den i EasyNetwork-inkorgen. Inkorgen är en temporär lagringsplats för filerna som andra datorer i nätverket skickar till dig. Om du har EasyNetwork uppe när du tar emot en fil visas filen direkt i din inkorg. Annars visas ett meddelande i meddelandefältet längst till höger i aktivitetsfältet. Om du inte vill få meddelanden (t.ex. om du blir avbruten i ditt arbete) kan du stänga av den funktionen. Om en fil med samma namn redan finns i inkorgen förses den nya filen med ett numeriskt tillägg efter filnamnet. Filerna ligger kvar i din inkorg tills du accepterar dem (kopierar dem till din dator).

Skicka en fil till en annan dator

Du kan skicka en fil till en annan dator på det hanterade nätverket utan att dela den. Innan en användare på den mottagande datorn kan använda filen måste den sparas på en lokal plats. Mer information finns i Acceptera en fil från en annan dator (sida 169).

1. Hitta filen du vill skicka i Utforskaren.
2. Dra filen från dess plats i Utforskaren till en aktiv datorikon i EasyNetwork.

Tips: Om du vill skicka flera filer till en dator kan du hålla ned CTRL när du markerar filer. Du kan också skicka filer genom att klicka på **Skicka** på **Verktyg**-menyn, välja filerna och sedan klicka på **Skicka**.

Acceptera en fil från en annan dator

Om en annan dator i det hanterade nätverket skickar en fil till dig måste du acceptera den genom att spara den på din dator. Om EasyNetwork inte körs när en fil skickas till din dator får du ett meddelande i meddelandefältet längst till höger på aktivitetsfältet. Om du vill öppna EasyNetwork och få tillgång till filen klickar du på meddelandet.

- Klicka på **Mottagna** och dra filen från din EasyNetwork-inkorg till en mapp i Utforskaren.

Tips: Du kan också ta emot en fil från en annan dator genom att markera filen i din EasyNetwork-inkorg och sedan klicka på **Acceptera** på **Verktyg**-menyn. Gå till mappen där du vill spara filerna du tar emot i dialogrutan Acceptera till mapp, markera den och klicka sedan på **Spara**.

Få ett meddelande när en fil skickas

Du kan få ett meddelande när en annan dator i det hanterade nätverket skickar en fil till dig. Om EasyNetwork inte körs visas meddelandet i meddelandefältet längst till höger på aktivitetsfältet.

1. Klicka på **Konfigurera** på **Alternativ**-menyn.
2. Markera kryssrutan **Meddela mig när en annan dator skickar filer till mig** i dialogrutan Konfigurera.
3. Klicka på **OK**.

KAPITEL 31

Dela skrivare

När du har gått med i ett hanterat nätverk delas lokala skrivare kopplade till din dator ut av EasyNetwork och skrivarens aktuella namn används som det delade skrivarnamnet. Skrivare som delas av andra datorer i nätverket identifieras också och du kan då konfigurera och använda dem.

Om du har konfigurerat en skrivardrivrutin för att skriva ut via en nätverksskrivarserver (till exempel en trådlös USB-skrivarserver) behandlas den som en lokal skrivare av EasyNetwork, som delar ut den i nätverket. Du kan också sluta dela en skrivare när som helst.

I detta kapitel

Arbeta med delade skrivare

EasyNetwork identifierar skrivarna som delas av datorerna i nätverket. Om en fjärrskrivare som inte är ansluten till din dator identifieras av EasyNetwork visas länken **Tillgängliga nätverksskrivare** i fönstret Delade filer när du öppnar EasyNetwork för första gången. Därefter kan du installera tillgängliga skrivare eller avinstallera skrivare som redan är anslutna till datorn. Du kan också uppdatera listan på skrivare för att vara säker på att informationen som visas är den senaste.

Om du inte har gått med i det hanterade nätverket men är ansluten till det kan du komma åt de delade skrivarna från Windows skrivarkontrollpanel.

Sluta dela en skrivare

När du slutar dela en skrivare kan användare inte använda den.

1. Klicka på **Skrivare** på **Verktyg**-menyn.
2. Klicka på namnet på den skrivare du inte längre vill dela i dialogrutan Hantera nätverksskrivare.
3. Klicka på **Dela inte**.

Installera en tillgänglig nätverksskrivare

Om du är medlem i ett hanterat nätverk kan du få tillgång till delade skrivare, men du måste installera den skrivardrivrutin som skrivaren använder. Om skrivarens ägare slutar dela skrivaren kan du inte använda den.

1. Klicka på **Skrivare** på **Verktyg**-menyn.
2. Klicka på ett skrivarnamn i dialogrutan Tillgängliga nätverksskrivare.
3. Klicka på **Installera**.

Referens

Termordlistan anger och definierar den vanligaste säkerhetsterminologin som används i McAfees produkter.

Ordlista

8

802.11

En uppsättning IEEE-standarder för att överföra data via trådlöst nätverk. 802.11 går allmänt under beteckningen Wi-Fi.

802.11a

Ett tillägg till 802.11 som möjliggör överföring av data med upp till 54 Mbit/s i 5 GHz-bandet. Trots att överföringshastigheten är högre än för 802.11b, täcker den ett mycket mindre område.

802.11b

Ett tillägg till 802.11 som möjliggör överföring av data med upp till 11 Mbit/s i 2,4 GHz-bandet. Trots att överföringshastigheten är lägre än för 802.11a, täcker den ett mycket större område.

802.1x

En IEEE-standard för autentisering i trådbundna och trådlösa nätverk. 802.11x används vanligtvis med 802.11 trådlöst nätverk.

A

ActiveX-kontroll

En programvarukomponent som används av program eller webbsidor för att lägga till funktioner som visas som en normal del av programmet eller webbsidan. De flesta ActiveX-kontroller är oskadliga, men vissa kan samla in information från datorn.

arkivera

Skapa en kopia av viktiga filer på en CD-, DVD- eller USB-enhet, en extern hårddisk eller en nätverksenhet.

autentisering

Process för identifiering av en användare, vanligtvis utifrån ett unikt namn och lösenord.

B

bandbredd

Den mängd data som kan överföras under en fastställd tidsperiod.

bevakade filtyper

De filtyper (bl.a. .doc och .xls) som säkerhetskopieras eller arkiveras i bevakningsplatserna med Data Backup.

bevakningsplatser

De mappar på datorn som Data Backup övervakar.

bibliotek

Ett onlineutrymme för filer som du har säkerhetskopierat och publicerat. Data backup-biblioteket är en webbplats som kan nås av alla med en Internet-uppkoppling.

bildfiltrering

Ett alternativ i Vuxenkontroll som blockerar potentiellt olämpliga bilder från att visas.

brandvägg

Ett system (maskinvara, programvara eller båda delarna) avsett för att förhindra obehörig åtkomst till eller från ett privat nätverk. Brandväggar används ofta för att förhindra att obehöriga Internetanvändare ska få åtkomst till privata nätverk anslutna till Internet, till exempel ett intranät. Alla meddelanden som kommer in i eller går ut från intranetet passerar genom brandväggen, som undersöker varje meddelande och blockerar de som inte uppfyller angivna säkerhetsvillkor.

buffertspill

Ett tillstånd som uppstår när misstänkta program eller processer försöker spara mer data i en buffert (tillfälligt datalagringsutrymme) på datorn än vad som får plats. Buffertspill skadar eller skriver över data i närliggande buffertar.

C

cache

Ett tillfälligt lagringsutrymme på datorn. För att det ska gå snabbare och bli mer effektivt att surfa på webben, kan webbläsaren t.ex. hämta en webbsida från cacheminnet (istället för från en fjärransluten server) nästa gång du vill se den.

cookie

En cookie är en liten fil som innehåller information, vanligen ett användarnamn och aktuellt datum och tid, som lagras på datorn hos någon som surfar på webben. Cookies används främst av webbplatser för att identifiera användare som tidigare har registrerat sig på eller besökt webbplatsen. De kan dock också användas av hackare för att utvinna information.

D

DAT

(datasignaturfiler) Filer som innehåller de definitioner som används när McAfee upptäcker virus, trojaner, spionprogram, reklamprogram och andra eventuellt oönskade program på datorn eller USB-enheten.

dela

En operation som gör att e-postmottagare får åtkomst till valda säkerhetskopierade filer under en begränsad tidsperiod. När du delar en fil skickar du den säkerhetskopierade kopian av filen till den e-postmottagare som du anger. Mottagaren erhåller ett e-brev från Data Backup som anger att filen har delats med dem. I e-brevet finns dessutom en länk till de delade filerna.

delad hemlighet

En sträng eller nyckel (vanligtvis ett lösenord) som har delats mellan två kommunicerande parter innan kommunikationen inleds. En delad hemlighet används för att skydda känsliga delar av RADIUS-meddelanden.

djup bevakningsplats

En mapp i datorn som Data Backup kontrollerar för att se om det sker några förändringar i den. Om du ställer in en djup bevakningsplats kommer Data Backup att säkerhetskopiera de bevakade filtyperna i mappen och undermapparna.

DNS

(Domain Name System) Ett system som konverterar värdnamn eller domännamn till IP-adresser. På webben används DNS för att konvertera läsbara webbadresser (t.ex. www.mittvardnamn.se) till IP-adresser (t.ex. 111.2.3.44) så att webbplatsen kan hämtas. Utan DNS skulle du behöva skriva in själva IP-adressen i webbläsaren.

DNS-server

(Domain Name System-server) En dator som returnerar den IP-adress som är knuten till ett värd- eller domännamn. Se även DNS.

domän

Ett lokalt undernätverk eller en beskrivare för Internetplatser.

I ett lokalt nätverk (LAN) är en domän ett undernätverk som består av klient- och serverdatorer som kontrolleras av en säkerhetsdatabas. I det här sammanhanget kan domäner förbättra prestanda. På Internet ingår en domän i varje webbadress (i exemplet www.abc.com är abc domänen).

DoS (Denial of Service)

En typ av attack som får nätverkstrafiken att gå långsammare eller avstanna helt. En DoS-attack innebär att nätverket översvämmas av så många extra förfrågningar att den vanliga trafiken går långsammare eller avbryts helt. Den leder vanligtvis inte till stöld av information eller andra säkerhetsluckor.

E

e-post

(elektronisk post) Meddelanden som skickas och tas emot elektroniskt via ett datornätverk. Se även webbaserad e-post.

e-postklient

Ett program som körs på datorn som gör att du kan skicka och ta emot e-post (t.ex. Microsoft Outlook).

ej registrerad åtkomstpunkt

En obehörig åtkomstpunkt. Ej registrerade åtkomstpunkter kan installeras i ett säkert företagsnätverk för att ge obehöriga åtkomst till nätverket. De kan också skapas för att en angripare ska kunna utföra en mannen-i-mitten-attack.

ESS

(Extended Service Set) En uppsättning av ett eller flera nätverk som utgör ett undernätverk.

eventuellt oönskat program (PUP)

Ett program som samlar in och vidarebefordrar personlig information utan din tillåtelse (t.ex. spionprogram och reklamprogram).

extern hårddisk

En hårddisk som är placerad utanför datorn.

F

filfragment

Rester efter en fil som ligger spridda på en skiva. Filfragmentering uppstår när filer läggs till eller tas bort från en skiva och kan försämra datorns prestanda.

fullständig arkivering

Alla data baserade på de filtyper och platser som du angivit arkiveras. Se även snabbarkivering.

G

genomsökning på begäran

En genomsökning som startas på begäran (dvs. när du startar åtgärden). Till skillnad från realtidsgenomsökning startar inte genomsökning på begäran automatiskt.

genväg

En fil som bara innehåller platsen för en annan fil på datorn.

grunda bevakningsplatser

En mapp i datorn som Data Backup kontrollerar för att se om det sker några förändringar i den. Om du ställer in en grund bevakningsplats kommer Data Backup att säkerhetskopiera de bevakade filtyperna i mappen, men inte i undermapparna.

H

hanterade nätverk

Ett hemnätverk med två typer av medlemmar: hanterade medlemmar och ohanterade medlemmar Hanterade medlemmar tillåter andra datorer på nätverket att övervaka deras skyddsstatus, ohanterade medlemmar gör inte det.

hotspot

En geografisk gräns som täcks av en åtkomstpunkt för Wi-Fi (802.11). Användare som befinner sig i en hotspot med en bärbar dator med trådlöst nätverk kan ansluta till Internet, under förutsättning att hotspoten fungerar som beacon (d.v.s. talar om att den finns) och att ingen autentisering krävs. Hotspots finns ofta där många människor rör sig, t.ex. på flygplatser.

händelse

En händelse som initieras av användaren, en enhet eller själva datorn och som utlöser ett svar. McAfee registrerar händelser i händelseloggen.

I

innehållsklassificeringsgrupp

Innehållsklassificieringsgrupper i Vuxenkontroll är olika åldersgrupper som en användare hör hemma i. Innehållet görs tillgängligt eller blockeras utifrån vilken innehållsklassificeringsgrupp som användaren tillhör. Innehållsklassificeringsgrupper kan vara: yngre barn, barn, yngre tonåringar, äldre tonåringar och vuxna.

integrerad gateway

En enhet som kombinerar funktionerna i en åtkomstpunkt, router och brandvägg. I vissa enheter kan det dessutom finnas säkerhetsförstärkningar och bryggfunktioner.

Internet

Internet består av ett enormt antal sammanlänkade nätverk som använder TCP/IP-protokoll för att lokalisera och överföra data. Internet utvecklades utifrån en sammanlänkning av datorer på amerikanska universitet och college (i slutet av 1960- och början av 1970-talet) som finansierades av USA:s försvarsdepartement och som kallades för ARPANET. Internet är idag ett globalt nätverk bestående av nästan 100 000 självständiga nätverk.

intranät

Ett privat datornätverk, vanligen inom en organisation, som endast auktoriserade användare kan komma åt.

IP-adress

En identifierare för en dator eller enhet i ett TCP/IP-nätverk. Nätverk som använder TCP/IP-protokollet skickar meddelanden utifrån målets IP-adress. Formatet för en IP-adress är en 32 bitars numerisk adress som skrivs som fyra tal som avgränsas med punkter. Varje tal kan vara från 0 till 255 (t.ex. 192.168.1.100).

IP-förfalskning

Förfalskning av IP-adresser i ett IP-paket. Detta används vid många typer av attacker inklusive sessionskapning. Det används också ofta för att förfalska en e-postrubrik med skräpdata så att den inte går att spåra.

K

karantän

Att isolera. T.ex. upptäcks misstänkta filer och placeras i karantän i VirusScan, så att de inte kan skada datorn eller filer.

klartext

Text som inte är krypterad. Se även kryptering.

klient

Ett program som körs på en dator eller arbetsstation och som är beroende av en server för att kunna fungera. Exempel: en e-postklient är ett program som gör att du kan skicka och ta emot e-brev.

komprimering

En metod med vilken storleken på filer minimeras så att de blir lättare att lagra eller överföra.

krypterad text

Krypterad text. Krypterad text kan inte läsas förrän den konverteras (dekrypteras) till vanlig text.

kryptering

En process där data överförs från text till kod och döljer på så sätt informationen så att personer som inte känner till hur man dekrypterar filen kan läsa innehållet. Krypterade data kallas också chiffertext.

L

lagringsplats för onlinesäkerhetskopiering

Den plats på onlineservern där filerna lagras sedan de säkerhetskopierats.

LAN

(Local Area Network eller lokalt nätverk) Ett datornätverk som omfattar ett tämligen litet område (t.ex. ett enstaka hus). Datorer i ett LAN kan kommunicera med varandra och dela resurser, t.ex. skrivare och filer.

lista med godkända objekt

En lista över webbplatser som anses säkra att besöka.

lista med tillförlitliga objekt

Innehåller objekt som du litar på och som inte upptäcks. Om du litar på ett objekt (t.ex. ett eventuellt oönskat program eller en registerändring) av misstag eller vill att det ska upptäckas igen, måste du ta bort det från listan.

lösenord

En kod (som oftast består av bokstäver och siffror) du använder för att få tillgång till din dator, till ett visst program eller till en webbplats.

Lösenordsvalv

Ett säkert lagringsutrymme för dina lösenord. Det gör att du kan lagra lösenord på ett sådant sätt att du kan känna dig säker på att ingen annan (inte ens administratörer) kan komma åt dem.

M

MAC-adress

(Media Access Control-adress) Ett unikt serienummer tilldelat till den fysiska enheten med nätverksåtkomst..

mannen-i-mitten-attack

En metod att komma åt och eventuellt ändra meddelanden mellan två parter utan att någon av dem vet att kommunikationslänken har brutits.

MAPI

(Messaging Application Programming Interface) En gränssnittsspecifikation från Microsoft som gör att olika meddelande- och arbetsgrupprogram (inklusive e-post, röstmeddelanden och fax) kan fungera med en klient, t.ex. en Exchange-klient.

mask

En "mask" är ett självreplikerande virus som är lagrat i det aktiva minnet och som kan skicka kopior av sig själv via e-post. Maskar replikerar och konsumerar systemresurser, försämrar prestandan eller avbryter tillfälligt aktiviteter.

meddelandeverifieringskod (message authentication code, MAC)

En säkerhetskod som används för att kryptera meddelanden som överförs mellan datorer. Meddelandet accepteras om datorn känner igen den avkrypterade koden som giltig.

modemkapningsprogram

Ett program som hjälper dig upprätta en Internetanslutning. När de används i skadligt syfte kan modemkapningsprogram styra om Internetanslutningar till någon annan än din vanliga Internetleverantör utan att informera dig om extra kostnader.

MSN

(Microsoft Network) En grupp webbaserade tjänster från Microsoft Corporation, t.ex. en sökmotor, e-post, chatt och en portal.

N

NIC

(Network Interface Card) Ett kort som sätts in i en bärbar dator eller annan enhet och ansluter enheten till det lokala nätverket.

nod

En enskild dator ansluten till ett nätverk.

nyckel

En serie bokstäver och siffror som används i två enheter för att autentisera kommunikationen mellan dessa. Båda enheterna måste innehålla nyckeln. Se även WEP, WPA, WPA2, WPA-PSK och WPA2- PSK.

nyckelord

Ett ord som du kan tilldela till en säkerhetskopierad fil för att skapa en relation eller anslutning till andra filer som har fått samma nyckelord tilldelade. Om du tilldelar nyckelord till filerna blir det enklare att söka efter filer som du publicerat på Internet.

nätverk

En samling åtkomstpunkter och de användare som hör till, motsvarande ett ESS.

nätverk i hemmet

Två eller fler datorer som är anslutna i hemmet så att de kan dela filer och Internetanslutning. Se även Lokalt nätverk.

nätverksenhet

En hårddisk eller bandenhet som är ansluten till en server i ett nätverk som delas av flera användare. Nätverksenheter kallas ibland även fjärrenheter.

nätverkskarta

En grafisk representation av datorerna och komponenterna som utgör ett hemnätverk.

O

ordboksangrepp

En typ av råstyrkeattack som använder vanliga ord för att försöka hitta ett lösenord.

P

Papperskorgen

En simulerad papperskorg för borttagna filer och mappar i Windows.

phishing

Ett Internetbedrägeri där någon försöker komma åt värdefull information som kreditkorts- och personnummer, använder-ID:n och lösenord från aningslösa användare i bedrägliga syften.

plugin

Ett litet program som läggs till ett större program för att ge det extra funktioner. Plugin-programmen gör t.ex. att en webbläsare kan användas för att få åtkomst till och köra inbäddade filer i HTML-dokument med ett format som webbläsaren vanligtvis inte kan hantera (t.ex. animeringar, videoklipp och ljudfiler).

POP3

(Post Office Protocol 3) Ett gränssnitt mellan ett klientprogram för e-post och e-postservern. De flesta hemanvändare har ett e-postkonto för POP3 (kallas även (standard-e-postkonto).

popup-fönster

Små fönster som öppnas över andra fönster på bildskärmen. Popup-fönster används ofta i webbläsare för att visa reklam.

port

Ett ställe där information går in i och/eller kommer ut ur datorn. Ett vanligt analogt modem ansluts till exempel till en seriell port.

PPPoE

(Point-to-Point Protocol Over Ethernet) En metod att använda det uppringda protokollet Point-to-Point Protocol (PPP) via Ethernet.

protokoll

Ett format (maskinvara eller programvara) för överföring av data mellan två enheter. Datorn eller enheten måste ha stöd för rätt protokoll för att kunna kommunicera med andra datorer.

proxy

En dator (eller programvaran som körs på den) som fungerar som en barriär mellan ett nätverk och Internet genom att endast visa upp en nätverksadress för externa platser. Genom att representera alla interna datorer skyddar proxyn identiteterna inom nätverket samtidigt som det ger åtkomst till Internet. Se även proxyserver.

proxyserver

En brandväggskomponent som hanterar Internettrafik till och från ett lokalt nätverk (LAN). En proxyserver kan förbättra prestandan genom att tillhandahålla information som är efterfrågad, till exempel populära webbsidor, och kan filtrera och förkasta begäranden som ägaren inte tycker är lämpliga, till exempel begäranden från obehöriga att få åtkomst till privata filer.

publicera

Ett sätt att göra en säkerhetskopierad fil tillgänglig för alla på Internet. Du kan komma åt publicerade filer genom att söka i Data Backup-biblioteket.

R

RADIUS

(Remote Access Dial-In User Service) Ett protokoll som används för att autentisera användare, exempelvis vid en fjärråtkomst. Definierades ursprungligen för att användas för uppringda servrar, men RADIUS-protokollet används numera i olika autentiseringsmiljöer, inklusive vid 802.1x-autentisering av delade hemligheter för WLAN-användare.

realtidssökning

Söka igenom filer och mappar efter virus och andra aktiviteter när du använder dem eller när de påträffas av datorn.

register

En databas där Windows lagrar konfigurationsinformation. Registret innehåller profiler för varje användare och information om datorns maskinvara, installerade program och egenskapsinställningar. Windows använder informationen hela tiden under driften.

roaming

Att flytta från ett åtkomstpunktsområde till ett annat utan att tjänsten avbryts eller att anslutningen bryts.

rootkit

En uppsättning verktyg (program) som ger en användare åtkomst på administratörsnivå till en dator eller ett nätverk. De kan innehålla spionprogram och andra eventuellt oönskade program som kan medföra ytterligare säkerhets- eller sekretessrisker för data och personlig information.

router

En nätverksenhet som vidarebefordrar datapaket från ett nätverk till ett annat. Med hjälp av interna dirigeringstabeller läser routern av varje inkommande paket och avgör hur det ska vidarebefordras, baserat på en kombination av käll- och måladresser samt av de aktuella trafikförhållandena (t.ex. belastning, linjekostnader och dåliga linjer). En router kallas ibland för en åtkomstpunkt.

råstyrkeattacker

En metod för att avkoda krypterade data, t.ex. lösenord, genom omfattande försök (råstyrkeattacker) och inte genom intellektuell strategi. Råstyrkeattacker anses vara en osviklig men tidsödande metod. Råstyrkeattacker kallas även råstyrkebrytning.

S

server

En dator eller ett program som tar emot anslutningar från andra datorer eller program och svarar på lämpligt sätt. Ett e-postprogram ansluter t.ex. till en e-postserver varje gång du skickar eller tar emot e-postmeddelanden.

skript

En lista över kommandon som kan utföras automatiskt (d.v.s utan interaktion från användaren). Till skillnad från program lagras skript vanligtvis som vanlig text och kompileras varje gång de körs. Makron och kommandofiler kallas också skript.

smart enhet

Se USB-enhet.

SMTP

(Simple Mail Transfer Protocol) Ett TCP/IP-protokoll för att skicka meddelanden från en dator till en annan i ett nätverk. Detta protokoll används på Internet för att dirigera e-post.

snabbarkivering

Med snabbarkivering arkiveras endast de filer som har ändrats sedan den senaste fullständiga arkiveringen eller snabbarkiveringen. Se även fullständig arkivering.

SSID

(Service Set Identifier) Ett tecken (hemlig nyckel) som identifierar ett Wi-Fi-nätverk (802.11). SSID ställs in av nätverksadministratören och måste tillhandahållas av användare som vill ansluta till nätverket.

SSL

(Secure Sockets Layer) Ett protokoll som utvecklats av Netscape för överföring av privata dokument via Internet. För SSL används en offentlig nyckel för att kryptera data som överförs över SSL-anslutningen. Webbadresser som kräver en SSL-anslutning börjar med https: och inte med http:.

standard-e-postkonto

Se POP3.

startpanel

En U3-gränssnittskomponent som fungerar som en startpunkt för att starta och hantera U3-USB-program.

svartlista

Vid antiphising, en lista med misstänkt falska webbplatser.

synkronisera

Ett sätt att lösa inkonsekvenser mellan säkerhetskopierade filer och filer sparade på den lokala datorn. Du synkroniserar filer när filen i onlinesäkerhetskopieringens lagringsplats är nyare än den version av filen som finns på de andra datorerna.

SystemGuard

McAfee-varningar som upptäcker obehöriga ändringar i datorn och varnar dig när de inträffar.

systemåterställningspunkt

En ögonblicksbild av innehållet i datorns minne eller i en databas. Windows skapar återställningspunkter vid viktiga systemhändelser (t.ex. när ett program eller en drivrutin installeras). Du kan också skapa och namnge egna återställningspunkter när som helst.

säkerhetskopiera

Skapa en kopia av viktiga filer på en säker onlineserver.

T

tillfällig fil

En fil som skapas i minnet eller på en skiva, av operativsystemet eller något annat program, och som är avsedd att användas under en session och sedan tas bort.

TKIP

(Temporal Key Integrity Protocol) Ett protokoll som inriktar sig på svagheterna i WEP-säkerhet, i synnerhet återanvändning av krypteringsnycklar. TKIP ändrar temporära nycklar efter 10 000 paket och möjliggör en dynamisk distributionsmetod som avsevärt ökar nätverkssäkerheten. TKIP-processen (säkerhetsprocessen) börjar med en 128-bitar lång temporär nyckel som delas mellan klienter och åtkomstpunkter. TKIP kombinerar den temporära nyckeln med klientdatorns MAC-adress och lägger sedan till en relativt stor 16-oktetters initieringsvektor för att skapa nyckeln för att kryptera data. Den här proceduren gör att varje station använder olika nyckelströmmar för att kryptera data. I TKIP används RC4 för att utföra krypteringen.

Trojan

Trojaner verkar vara tillförlitliga program men kan störa och skada datorn eller ge obehöriga åtkomst till den.

trådlösa PCI-kort

(Peripheral Component Interconnect) Ett trådlöst nätverkskort som ansluts till en PCI-kortplats inuti datorn.

trådlöst kort

En enhet som ger en dator eller handdator trådlösa funktioner. Den ansluts via en USB-port, PC Card-kortplats (CardBus), minneskortplats eller internt i PCI-bussen.

trådlöst USB-kort

Ett trådlöst nätverkskort som ansluts till en USB-port på datorn.

U

U3

(U: Simplified, Smarter, Mobile) En plattform för att köra Windows 2000- eller Windows XP-program direkt från en USB-enhet. U3-initiativet grundades 2004 av M-Systems och SanDisk och gör att användare kan köra U3-program på en Windows-dator utan att installera eller spara data eller inställningar på datorn.

URL

(Uniform Resource Locator) Standardformatet för Internetadresser.

USB

(Universal Serial Bus) Ett standardiserat seriellt datorgränssnitt som gör det möjligt att ansluta kringutrustning som tangentbord, styrspakar och skrivare till datorn.

USB-enhet

En liten minnesenhet som kan anslutas till datorns USB-port. En USB-enhet fungerar som en liten diskenhet och gör det enkelt att överföra filer från en dator till en annan.

W

wardriver

Någon som söker efter Wi-Fi-nätverk (802.11) genom att köra genom städer med en Wi-Fi-utrustad dator och specialgjord maskinvara eller programvara.

Webbaserad e-post

Meddelanden som skickas och tas emot elektroniskt via Internet. Se även e-post.

webbläsare

Ett program som används för att visa webbsidor på Internet. Microsoft Internet Explorer och Mozilla Firefox är exempel på populära webbläsare.

Webbuggar

Små grafiska filer som kan bäddas in på dina HTML-sidor och gör så att obehöriga kan lägga in cookies på din dator. Dessa cookies kan sedan sända information till den obehöriga källan. Webbuggar kallas även webbeacons, bildpunktstaggar, klara GIF-filer eller osynliga GIF-filer.

WEP

(Wired Equivalent Privacy) Ett krypterings- och autentiseringsprotokoll som ingår som en del av 802.11-standarden. De första versionerna basers på RC4-chiffer och innehåller stora svagheter. WEP försöker skapa säkerhet genom att kryptera data över radiolänkar så att de skyddas när de skickas från en slutpunkt till en annan. Det är emellertid så att säkerheten i WEP är inte så stor som man i det första skedet trodde.

Wi-Fi

(Wireless Fidelity) En term som används av Wi-Fi Alliance om alla typer av 802.11-nätverk.

Wi-Fi Alliance

En organisation bestående av de främsta tillverkarna av trådlös maskinvara och programvara. Wi-Fi Alliance har som mål att certifiera alla 802.11-baserade produkter så att de samverkar samt att främja användandet av termen Wi-Fi som ett globalt märkesnamn i alla marknadssegment som använder trådlösa 802.11-baserade nätverksprodukter. Organisationen fungerar som ett konsortium, testlaboratorium och en central för leverantörer som vill främja tillväxt inom branschen.

Wi-Fi Certified

En enhet som har testats och godkänts av Wi-Fi Alliance. Produkter som är märkta Wi-Fi Certified fungerar tillsammans med andra certifierade produkter även om de kommer från olika tillverkare. En användare med en Wi-Fi-certifierad produkt kan välja åtkomstpunkt och klientmaskinvara oberoende av märke bara den också är certifierad.?

V

virus

Självreplikerande program som kan ändra filer eller data. De verkar ofta komma från en tillförlitlig avsändare eller ha oskyldigt innehåll.

W

WLAN

(Wireless Local Area Network) Ett lokalt nätverk (LAN) som använder en trådlös anslutning. I ett trådlöst lokalt nätverk används högfrekventa radiovågor och inte trådar för att sköta kommunikationen mellan datorerna.

WPA

(Wi-Fi Protected Access) En specifikationsstandard som avsevärt ökar dataskyddet och åtkomstkontrollen i befintliga och framtida trådlösa lokala nätverk. Den är avsedd att användas i befintliga maskinvaror som en programuppdatering. WPA härstammar från och är kompatibelt med IEEE 802.11i-standarden. När det är installerat på korrekt sätt skänker det användarna i det trådlösa lokala nätverket den tryggheten att deras data är skyddade och att endast behöriga nätverksanvändare har åtkomst till nätverket.

WPA-PSK

Ett speciellt WPA-läge avsett för hemanvändare som inte har behov av samma säkerhetstänkande som stora företag och som inte har åtkomst till autentiseringsservrar. I detta läge anger hemanvändaren manuellt startlösenordet för att aktivera WPA i läget för förutdelad nyckel och måste sedan ändra lösenorden på varje trådlös dator och åtkomstpunkt med jämna mellanrum. Se även WPA2-PSK och TKIP.

WPA2

En uppdatering av säkerhetsstandarden WPA, baserad på 802.11i IEEE-standarden.

WPA2-PSK

Ett särskilt WPA-läge som liknar WPA-PSK och är baserat på WPA2-standarden. En vanlig funktion i WPA2-PSK är att enheter ofta har stöd för flera krypteringslägen (t.ex. AES och TKIP) samtidigt, medan äldre enheter vanligtvis bara stöder ett krypteringsläge åt gången (dvs. alla klienter måste använda samma krypteringsläge).

V

VPN

(Virtual Private Network) Ett privat nätverk som är konfigurerat inuti ett offentligt nätverk för att utnyttja administrationsfunktionerna i det offentliga nätverket. VPN används av företag för att skapa WAN-nätverk (Wide Area Network) som täcker stora geografiska områden, för att kunna erbjuda filialer plats-till-plats-anslutningar eller låta mobila användare ringa upp företagets lokala nätverk.

Vuxenkontroll

Inställningar som hjälper dig styra vad dina barn kan se och göra när de surfar på webben. Du kan ställa in Vuxenkontroll genom att aktivera och avaktivera bildfiltrering, välja en innehållsklassificeringsgrupp och ställa in tidsgränser för webbsurfning.

Å

återställa

Att återställa en kopia av en fil från onlinesäkerhetskopieringens lagringsplats eller ett arkiv.

Åtkomstpunkt

En nätverksenhet (vanligtvis kallad trådlös router) som ansluts till ett Ethernet-nav eller en Ethernet-växel för att utöka det trådlösa nätverkets fysiska område. När trådlösa användare förflyttar sig med sina mobila enheter, flyttas överföringen från en åtkomstpunkt till en annan för att anslutningen ska upprätthållas.

Om McAfee

McAfee, Inc. har sitt huvudkontor i Santa Clara i Kalifornien och är global marknadsledare inom intrångsskydd och säkerhetsriskhantering. McAfee levererar proaktiva och erkända lösningar och tjänster som skyddar system och nätverk världen över. Med oöverträffad säkerhetsexpertis och satsning på innovation ger McAfee hemanvändare, företag, den offentliga sektorn samt tjänsteleverantörer möjlighet att blockera angrepp, förhindra avbrott och ständigt granska och förbättra säkerheten.

Upphovsrätt

Licens

MEDDELANDE TILL ALLA ANVÄNDARE: LÄS NOGGRANT IGENOM DET LICENSAVTAL SOM MOTSVARAR DEN LICENS DU KÖPT OCH SOM ANGER DE ALLMÄNNA VILLKOREN FÖR ANVÄNDNING AV DEN LICENSIERADE PROGRAMVARAN. OM DU INTE VET VILKEN TYP AV LICENS DU HAR KÖPT KAN DU LÄSA SÄLJDOKUMENT, LICENSDOKUMENT ELLER ANDRA INKÖPSORDERDOKUMENT SOM MEDFÖLJDE PROGRAMMET ELLER SOM DU MOTTAGIT SEPARAT SOM EN DEL AV KÖPET (TILL EXEMPEL ETT HÄFTE, EN FIL PÅ CD-SKIVAN MED PRODUKTEN ELLER EN FIL FRÅN WEBBPLATSEN SOM DU HÄMTADE PROGRAMPAKETET FRÅN). INSTALLERA INTE PROGRAMVARAN OM DU INTE ACCEPTERAR ALLA VILLKOR SOM ANGES I AVTALET. OM DU INTE ACCEPTERAR ALLA VILLKOR KAN DU RETURNERA PRODUKTEN TILL MCAFEE, INC. ELLER INKÖPSSTÄLLET FÖR FULL ERSÄTTNING.

KAPITEL 32

Kundsupport och teknisk support

SecurityCenter rapporterar allvarliga och mindre allvarliga skyddsproblem så snart de upptäcks. Allvarliga skyddsproblem måste åtgärdas omedelbart eftersom de påverkar din skyddsstatus, som ändras till röd. Mindre allvarliga problem behöver inte åtgärdas med en gång och det är inte säkert att de påverkar din skyddsstatus (beroende på vilken typ av problem det rör sig om). Om du vill uppnå grön skyddsstatus måste du åtgärda alla allvarliga problem och antingen åtgärda eller ignorera mindre allvarliga problem. Om du behöver hjälp med att analysera skyddsproblemen kan du köra McAfee Virtual Technician. Mer information om McAfee Virtual Technician finns i hjälpen till McAfee Virtual Technician.

Om du har köpt säkerhetsprogramvaran från en annan leverantör än McAfee kan du öppna en webbläsare och gå till www.mcafeehjalp.com. Du får tillgång till McAfee Virtual Technician genom att välja din leverantör under Partner Links.

Obs! Om du vill installera och använda McAfee Virtual Technician måste du logga in på datorn som Windows-administratör. Om du inte gör det kanske du inte kan lösa problemen med hjälp av MVT. Mer information om hur du loggar in som Windows-administratör finns i Windows hjälpfunktion. I Windows Vista™ visas ett meddelande när du använder MVT. Klicka på **Godkänn** när det visas. Virtual Technician fungerar inte med Mozilla® Firefox.

I detta kapitel

Använda McAfee Virtual Technician

Virtual Technician fungerar som en personlig servicetekniker, som samlar in information om dina SecurityCenter-program för att kunna lösa datorns skyddsproblem åt dig. När du kör Virtual Technician kontrollerar funktionen att SecurityCenter-programmen fungerar som de ska. Om något problem skulle upptäckas åtgärdar Virtual Technician problemet åt dig eller ger dig mer information om vad du själv kan göra. När sökningen är slutförd visas analysresultaten och du kan vid behov söka ytterligare teknisk support från McAfee.

Virtual Technician samlar inte in personidentifierande uppgifter och dator och filer hålls skyddade och oskadda.

Obs! Om du vill veta mer om Virtual Technician klickar du på ikonen **Help** i Virtual Technician.

Starta Virtual Technician

Virtual Technician samlar in information om dina SecurityCenter-program så att du kan lösa eventuella skyddsproblem. För att skydda din identitet samlas inte personidentifierande uppgifter in.

1. Klicka på **McAfee Virtual Technician** under **Vanliga uppgifter**.
2. Följ anvisningarna på skärmen för att hämta och köra Virtual Technician.

Support och Hämta

Information om McAfees webbplatser för support och hämtning i landet där du bor, samt användarhandböcker, finns i följande tabeller:

Support och Hämta

Land	McAfee-support	McAfee-hämtningar
Australien	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasilien	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Kanada (engelska)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kanada (franska)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kina (förenklad kinesiska)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Kina (traditionell kinesiska)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tjeckien	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Danmark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finland	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Frankrike	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Tyskland	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Storbritannien	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italien	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japan	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexiko	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norge	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polen	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Spanien	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Sverige	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turkiet	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
USA	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection Användarhandböcker

Land	McAfee Användarhandböcker
Australien	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Kanada (engelska)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Kanada (franska)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Kina (förenklad kinesiska)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Kina (traditionell kinesiska)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tjeckien	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Nederländerna	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf

Japan	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turkiet	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security Användarhandböcker

Land	McAfee Användarhandböcker
Australien	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Kanada (engelska)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Kanada (franska)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Kina (förenklad kinesiska)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Kina (traditionell kinesiska)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tjeckien	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf

Frankrike	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Nederländerna	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turkiet	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus Användarhandböcker

Land	McAfee Användarhandböcker
Australien	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Kanada (engelska)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Kanada (franska)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Kina (förenklad kinesiska)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf

Kina (traditionell kinesiska)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tjeckien	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Nederländerna	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turkiet	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan Användarhandböcker

Land	McAfee Användarhandböcker
Australien	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf

Brasilien	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Kanada (engelska)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Kanada (franska)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Kina (förenklad kinesiska)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Kina (traditionell kinesiska)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tjeckien	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Nederländerna	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexiko	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turkiet	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf

USA	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Information om webbplatserna för McAfee Threat Center och Virusinformation i landet där du bor finns i följande tabeller:

Land	Huvudkontor för säkerhet	Virusinformation
Australien	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasilien	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Kanada (engelska)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kanada (franska)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kina (förenklad kinesiska)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Kina (traditionell kinesiska)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tjeckien	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Danmark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finland	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Frankrike	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Tyskland	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Storbritannien	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Nederländerna	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italien	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japan	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo

Mexiko	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norge	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polen	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Spanien	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Sverige	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turkiet	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
USA	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Information om webbplatsen för HackerWatch i landet där du bor finns i följande tabeller:

Land	HackerWatch
Australien	www.hackerwatch.org
Brasilien	www.hackerwatch.org/?lang=pt-br
Kanada (engelska)	www.hackerwatch.org
Kanada (franska)	www.hackerwatch.org/?lang=fr-ca
Kina (förenklad kinesiska)	www.hackerwatch.org/?lang=zh-cn
Kina (traditionell kinesiska)	www.hackerwatch.org/?lang=zh-tw
Tjeckien	www.hackerwatch.org/?lang=cs
Danmark	www.hackerwatch.org/?lang=da
Finland	www.hackerwatch.org/?lang=fi
Frankrike	www.hackerwatch.org/?lang=fr
Tyskland	www.hackerwatch.org/?lang=de
Storbritannien	www.hackerwatch.org
Nederländerna	www.hackerwatch.org/?lang=nl
Italien	www.hackerwatch.org/?lang=it

Japan	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Mexiko	www.hackerwatch.org/?lang=es-mx
Norge	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Spanien	www.hackerwatch.org/?lang=es
Sverige	www.hackerwatch.org/?lang=sv
Turkiet	www.hackerwatch.org/?lang=tr
USA	www.hackerwatch.org

Index

M

N

O

P

R

S

T

U

V,W

Å

Ä

Ö