

McAfee[®]
VirusScan[®] 2008

Virus and Spyware Protection

Brugerhåndbog

Indhold

McAfee VirusScan	3
McAfee SecurityCenter	5
Funktioner i SecurityCenter	6
Brug af SecurityCenter	7
Opdatere SecurityCenter	13
Løse eller ignorere beskyttelsesproblemer	17
Arbejde med alarmer	23
Vise hændelser	29
McAfee VirusScan	31
Funktioner i VirusScan	32
Starte virusbeskyttelse i realtid	33
Starte yderligere beskyttelse	35
Konfigurere virusbeskyttelse	39
Scanne computeren	57
Arbejde med scanningsresultater	61
McAfee QuickClean	65
Funktioner i QuickClean.....	66
Rense computeren	67
Defragmentering af din computer	70
Planlæg en opgave.....	71
McAfee Shredder.....	77
Funktioner i Shredder	78
Makulerer filer og indholdet af mapper og diske.....	79
McAfee Network Manager.....	81
Funktioner i Network Manager.....	82
Forklaring af ikoner i Network Manager.....	83
Konfigurere et administreret netværk	85
Administrere netværket eksternt	93
Reference.....	98
Ordliste	99
Om McAfee	113
Copyright	113
Licens	114
Kundeservice og teknisk support.....	115
Brug af McAfee Virtual Technician	116
Support og downloads	117
Indeks	126

KAPITEL 1

McAfee VirusScan

VirusScan med SiteAdvisor tilbyder avancerede registrerings- og beskyttelsestjenester for at optimere computerens forsvar mod de nyeste sikkerhedstrusler, herunder virus, trojanske heste, sporingscookies, spyware, adware og andre potentielt uønskede programmer. Med VirusScan udvides beskyttelsen ud over filerne og mapperne på den stationære eller bærbare computer og målrettes mod trusler fra forskellige indgange, herunder e-mail, onlinemeddelelser og internettet. McAfee SiteAdvisors sikkerhedsbedømmelser hjælper dig med at undgå usikre websteder.

I dette kapitel

McAfee SecurityCenter	5
McAfee VirusScan	31
McAfee QuickClean.....	65
McAfee Shredder	77
McAfee Network Manager	81
Reference	98
Om McAfee	113
Kundeservice og teknisk support	115

KAPITEL 2

McAfee SecurityCenter

McAfee SecurityCenter giver dig mulighed for at overvåge computerens sikkerhedsstatus, øjeblikkeligt få oplyst, om computerens virus-, spyware-, e-mail- og firewall-beskyttelsestjenester er opdaterede, og reagere over for potentielle sikkerhedssårbarheder. Det indeholder de navigationsværktøjer og kontrolelementer, du skal bruge til at koordinere og administrere alle områder af computerens beskyttelse.

Inden du begynder at konfigurere og administrere computerens beskyttelse, bør du gennemgå grænsefladen i SecurityCenter og sikre, at du forstår forskellen mellem beskyttelsesstatus, beskyttelseskategorier og beskyttelsestjenester. Opdater derefter SecurityCenter for at sikre, at du har den sidste nye beskyttelse fra McAfee.

Når du har udført indledende konfigurationsopgaver, kan du bruge SecurityCenter til at overvåge computerens beskyttelsesstatus. Hvis SecurityCenter registrerer et beskyttelsesproblem, advarer det dig, så du kan løse eller ignorere problemet (afhængigt af dets alvor). Du kan gennemgå SecurityCenter-hændelser, som f.eks. ændringer i konfigurationen af virusscanning, i en hændelseslogfil.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i SecurityCenter	6
Brug af SecurityCenter	7
Opdatere SecurityCenter	13
Løse eller ignorere beskyttelsesproblemer	17
Arbejde med alarmer	23
Vise hændelser	29

Funktioner i SecurityCenter

SecurityCenter indeholder følgende funktioner:

Forenklet beskyttelsesstatus

Se hurtigt computerens beskyttelsesstatus, søg efter opdateringer, og løs potentielle beskyttelsesproblemer.

Automatiske opdateringer og opgraderinger

Download og installerer automatisk opdateringer af registrerede programmer. Når en ny version af et registreret McAfee-program er tilgængelig, får du den gratis i din abonnementsperiode, og du er derved altid sikret opdateret beskyttelse.

Alarmer i realtid

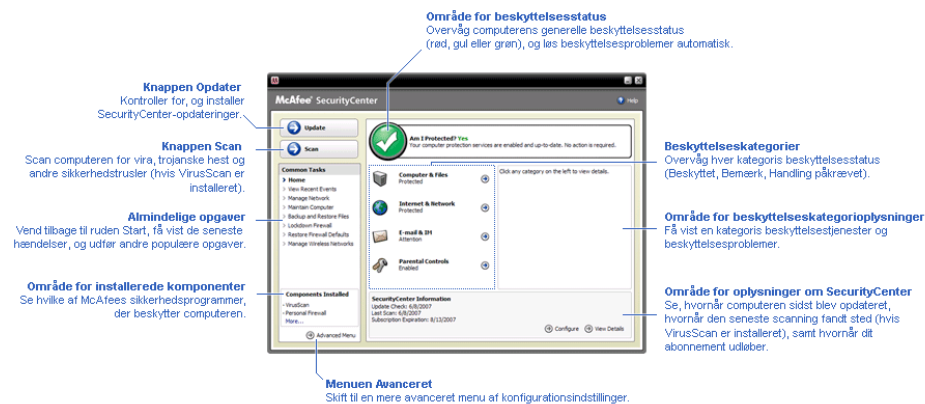
Sikkerhedsalarmer underretter dig om virusudbrud og sikkerhedstrusler og giver dig mulighed for at fjerne, neutralisere eller få mere at vide om de enkelte trusler.

KAPITEL 3

Brug af SecurityCenter

Inden du begynder at bruge SecurityCenter, skal du gennemgå de komponenter og konfigurationsområder, du vil bruge til at administrere computerens beskyttelsesstatus. Flere oplysninger om den terminologi, der bruges i dette billede, finder du under

Forklaring af beskyttelsesstatus (side 8) og Forklaring af beskyttelseskategorier (side 9). Derefter kan du gennemgå dine McAfee-kontooplysninger og kontrollere gyldigheden af dit abonnement.



I dette kapitel

Forklaring af beskyttelsesstatus	8
Forklaring af beskyttelseskategorier	9
Forklaring af beskyttelsestjenester	10
Administrere din McAfee-konto	11

Forklaring af beskyttelsesstatus

Computerens beskyttelsesstatus vises i beskyttelsesstatusområdet i startruden til SecurityCenter. Det angives, om computeren er fuldt beskyttet mod de seneste sikkerhedstrusler og kan påvirkes af ting, som f.eks. eksterne sikkerhedsangreb, andre sikkerhedsprogrammer og programmer, der benytter internettet.

Computerens beskyttelsesstatus kan være rød, gul eller grøn.

Beskyttelsesstatus	Beskrivelse
Rød	<p>Din computer er ikke beskyttet. Beskyttelsesstatusområdet i startruden til SecurityCenter er rødt og angiver, at computeren ikke er beskyttet. SecurityCenter rapporterer mindst ét kritisk sikkerhedsproblem.</p> <p>For at opnå fuld beskyttelse skal du løse alle kritiske sikkerhedsproblemer i hver beskyttelseskategori (kategoristatus for problem er indstillet til Handling påkrævet, også med rødt). Oplysninger om, hvordan du løser beskyttelsesproblemer, finder du under Løsning af beskyttelsesproblemer (side 18).</p>
Gul	<p>Din computer er delvist beskyttet. Beskyttelsesstatusområdet i startruden til SecurityCenter er gult og angiver, at computeren ikke er beskyttet. SecurityCenter rapporterer mindst ét ikke-kritisk sikkerhedsproblem.</p> <p>For at opnå fuld beskyttelse skal du løse eller ignorere de ikke-kritiske sikkerhedsproblemer i hver beskyttelseskategori. Oplysninger om, hvordan du løser eller ignorerer beskyttelsesproblemer, finder du under Løse eller ignorere beskyttelsesproblemer (side 17).</p>
Grøn	<p>Din computer er fuldt beskyttet. Beskyttelsesstatusområdet i startruden til SecurityCenter er grønt og angiver, at computeren er beskyttet. SecurityCenter rapporterer ingen kritiske eller ikke-kritiske sikkerhedsproblemer.</p> <p>I hver beskyttelseskategori vises de tjenester, der beskytter computeren.</p>

Forklaring af beskyttelseskategorier

Beskyttelsestjenesterne i SecurityCenter er opdelt i fire kategorier: Computer & filer, Internet & netværk, E-mail & IM og Forældrestyring. Disse kategorier hjælper dig med at gennemse og konfigurere de sikkerhedstjenester, der beskytter computeren.

Du kan klikke på et kategorinavn for at konfigurere beskyttelsestjenesterne og få vist de sikkerhedsproblemer, der evt. er registreret for disse tjenester. Hvis computerens beskyttelsesstatus er rød eller gul, vises meddelelsen *Handling påkrævet* eller *Bemærk* i en eller flere kategorier for at vise, at SecurityCenter har registreret et problem i kategorien. Flere oplysninger om beskyttelsesstatus finder du under Forklaring af beskyttelsesstatus (side 8).

Beskyttelses-kategori	Beskrivelse
Computer & filer	Kategorien Computer & filer giver dig mulighed for at konfigurere følgende beskyttelsestjenester: <ul style="list-style-type: none"> ▪ Virusbeskyttelse ▪ PUP-beskyttelse ▪ Systemovervågning ▪ Windows-beskyttelse
Internet & netværk	Kategorien Internet & netværk giver dig mulighed for at konfigurere følgende beskyttelsestjenester: <ul style="list-style-type: none"> ▪ Firewall-beskyttelse ▪ Identitetsbeskyttelse
E-mail & IM	Kategorien E-mail & IM giver dig mulighed for at konfigurere følgende beskyttelsestjenester: <ul style="list-style-type: none"> ▪ E-mail-beskyttelse ▪ Spambeskyttelse
Forældrestyring	Kategorien Forældrestyring giver dig mulighed for at konfigurere følgende beskyttelsestjenester: <ul style="list-style-type: none"> ▪ Indholdsblokering

Forklaring af beskyttelsestjenester

Beskyttelsestjenester er kernekomponenterne i SecurityCenter, som du konfigurerer for at beskytte computeren. Beskyttelsestjenester svarer direkte til McAfee-programmer. Når du installerer VirusScan, bliver følgende beskyttelsestjenester f.eks. tilgængelige: Virusbeskyttelse, PUP-beskyttelse, Systemovervågning og Windows-beskyttelse. Flere oplysninger om disse beskyttelsestjenester finder du i VirusScan Hjælp.

Som standard aktiveres alle de beskyttelsestjenester, der er knyttet til et program, når du installerer programmet. Du kan dog til enhver tid deaktivere en beskyttelsestjeneste. Hvis du f.eks. installerer Privacy Service, aktiveres både Indholdsblokering og Identitetsbeskyttelse. Hvis du ikke vil bruge beskyttelsestjenesten Indholdsblokering, kan du deaktivere den. Du kan også midlertidigt deaktivere en beskyttelsestjeneste, mens du udfører opsætnings- eller vedligeholdelsesopgaver.

Administrere din McAfee-konto

Du kan administrere din McAfee-konto fra SecurityCenter, hvor du nemt kan få adgang til og gennemgå dine kontooplysninger og kontrollere din aktuelle abonnementsstatus.

Bemærk! Hvis du har installeret McAfee-programmerne fra en cd, skal du registrere dem på McAfee-webstedet for at konfigurere eller opdatere din McAfee-konto. Først når du har gjort det, får du adgang til regelmæssige, automatiske programopdateringer.


Administrere din McAfee-konto

Du kan nemt få adgang til dine McAfee-kontooplysninger (Min konto) fra SecurityCenter.

- 1 Klik på **Min konto** under **Almindelige opgaver**.
- 2 Log ind på din McAfee-konto

Kontrollere dit abonnement

Du skal kontrollere dit abonnement for at sikre, at det endnu ikke er udløbet.

- Højreklik på ikonet SecurityCenter  i meddelelsesområdet længst til højre på proceslinjen, og klik derefter på **Bekræft abonnement**.

KAPITEL 4

Opdatere SecurityCenter

SecurityCenter sikrer, at dine registrerede McAfee-programmer er aktuelle, ved at søge efter og installere onlineopdateringer hver fjerde time. Afhængigt af de programmer, du har installeret og registreret, kan onlineopdateringer indeholde de nyeste virusdefinitioner og opgraderinger af beskyttelse mod virus, hackere, spam og spyware og af dine personlige oplysninger. Hvis du vil søge efter opdateringer mere end hver fjerde time, kan du gøre det på ethvert tidspunkt. Mens SecurityCenter søger efter opdateringer, kan du foretage andre opgaver i programmet.

Selvom det ikke anbefales, kan du ændre den måde, SecurityCenter søger efter og installerer opdateringer på. Du kan f.eks. konfigurere SecurityCenter til at downloade, men ikke installere opdateringer, eller underrette dig før download og installation af opdateringer. Du kan også deaktivere automatisk opdatering.

Bemærk! Hvis du har installeret McAfee-programmerne fra en cd, skal du registrere dem på McAfee-webstedet for at modtage regelmæssige, automatisk opdateringer til disse programmer.

I dette kapitel

Søge efter opdateringer	13
Konfigurere automatiske opdateringer	14
Deaktivere automatiske opdateringer	14

Søge efter opdateringer

Som standard søger SecurityCenter automatisk efter opdateringer hver fjerde time, når computeren har forbindelse til internettet. Hvis du vil søge efter opdateringer mere end hver fjerde time, kan du gøre det. Hvis du har deaktiveret automatiske opdateringer, er du ansvarlig for regelmæssigt at søge efter opdateringer.

- Klik derefter på **Opdater** i startruden til SecurityCenter.

Tip! Du kan søge efter opdateringer uden at starte SecurityCenter ved at højreklikke på ikonet SecurityCenter  i meddelelsesområdet på proceslinjen og derefter klikke på **Opdateringer**.

Konfigurere automatiske opdateringer

Som standard søger SecurityCenter automatisk efter og installerer opdateringer hver fjerde time, når computeren har forbindelse til internettet. Hvis du vil ændre denne standardfunktion, kan du konfigurere SecurityCenter til automatisk at downloade opdateringer og derefter give dig besked, når opdateringerne er parate til at blive installeret, eller give dig besked, inden opdateringerne downloades.

Bemærk! SecurityCenter underretter dig, når opdateringer er parate til at blive downloadet eller installeret, ved hjælp af alarmer. Fra disse alarmer kan du enten downloade eller installere opdateringerne eller udskyde opdateringerne. Når du opdaterer programmer fra en alarm, bliver du bedt om at bekræfte dit abonnement, inden programmerne downloades og installeres. Flere oplysninger finder du under Arbejde med alarmer (side 23).

- 1 Åbn ruden Konfiguration af SecurityCenter.
Hvordan?
 1. Klik på **Start** under **Almindelige opgaver**.
 2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
- 2 Klik på **Til** under **Automatiske opdateringer er deaktiveret** i ruden Konfiguration af SecurityCenter, og klik derefter på **Avanceret**.
- 3 Klik på en af følgende knapper:
 - **Installer opdateringerne automatisk, og giv mig besked, når mine tjenester er opdateret (anbefales)**
 - **Download opdateringerne automatisk, og giv mig besked, når de er klar til at blive installeret**
 - **Giv besked før download af opdateringer**
- 4 Klik på **OK**.

Deaktivere automatiske opdateringer

Hvis du deaktiverer automatiske opdateringer, er du ansvarlig for regelmæssigt at søge efter opdateringer. Ellers har din computer ikke den nyeste sikkerhedsbeskyttelse. Flere oplysninger om at søge efter opdateringer finder du under Søge efter opdateringer (side 13).

- 1 Åbn ruden Konfiguration af SecurityCenter.
Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
 2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
- 2** Klik på **Fra** under **Automatiske opdateringer er aktiveret** i ruden Konfiguration af SecurityCenter.

Tip! Du kan aktivere automatiske opdateringer ved at klikke på knappen **Til** eller fjerne markeringen af **Deaktiver automatisk opdatering, og lad mig kontrollere for opdateringer manuelt** i ruden Opdateringsindstillinger.

KAPITEL 5

Løse eller ignorere beskyttelsesproblemer

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Kritiske beskyttelsesproblemer kræver øjeblikkelig handling og kompromitterer din beskyttelsesstatus (ændrer farven til rød). Ikke-kritiske beskyttelsesproblemer kræver ikke øjeblikkelig handling og muligvis kompromittere din beskyttelsesstatus (afhængigt af typen af problem). For at opnå grøn beskyttelsesstatus skal du løse alle kritiske problemer og enten løse eller ignorere alle ikke-kritiske problemer. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician. Se Hjælp i McAfee Virtual Technician for at få flere oplysninger om McAfee Virtual Technician.

I dette kapitel

Løse beskyttelsesproblemer	18
Ignorere beskyttelsesproblemer	20

Løse beskyttelsesproblemer

De fleste sikkerhedsproblemer kan løses automatisk. Nogle problemer kræver dog, at du foretager en handling. Hvis Firewall-beskyttelse f.eks. er deaktiveret, kan SecurityCenter aktivere den automatisk. Hvis Firewall-beskyttelse ikke er installeret, skal du dog installere den. I følgende tabel beskrives nogle af de handlinger, du kan foretage, når du løser beskyttelsesproblemer manuelt:

Problem	Handling
Der er ikke udført en komplet scanning af computeren inden for de sidste 30 dage.	Scan computeren manuelt. Flere oplysninger findes i VirusScan Hjælp.
Dine virussignaturfiler er forældede.	Opdater beskyttelsen manuelt. Flere oplysninger findes i VirusScan Hjælp.
Et program er ikke installeret.	Installer programmet fra McAfees websted eller en cd.
Komponenter mangler i et program.	Installer programmet igen fra McAfees websted eller en cd.
Et program er ikke registreret og kan ikke modtage fuld beskyttelse.	Registrer programmet på McAfees websted.
Et program er udløbet.	Kontroller din kontostatus på McAfees websted.

Bemærk! Ofte påvirker et enkelt beskyttelsesproblem mere end én beskyttelseskategori. I dette tilfælde fjernes problemet fra alle andre beskyttelseskategorier, når du løser det.

Løse beskyttelsesproblemer automatisk

SecurityCenter kan løse de fleste beskyttelsesproblemer automatisk. De konfigurationsændringer, som SecurityCenter foretager, når beskyttelsesproblemer løses automatisk, registreres ikke i hændelseslogfilen. Flere oplysninger om hændelser finder du under **Vise hændelser** (side 29).

- 1 Klik på **Start** under **Almindelige opgaver**.
- 2 Klik på **Reparer** i i beskyttelsesstatusområdet i startruden til SecurityCenter.

Løse beskyttelsesproblemer manuelt

Hvis et eller flere beskyttelsesproblemer stadig forekommer, når du har forsøgt at løse dem automatisk, kan du løse problemerne manuelt.

- 1 Klik på **Start** under **Almindelige opgaver**.
- 2 Klik på den beskyttelseskategori, SecurityCenter har rapporteret problemet i, i starttruden til SecurityCenter.
- 3 Klik på linket efter beskrivelsen af problemet.

Ignorere beskyttelsesproblemer

Hvis SecurityCenter registrerer et ikke-kritiske problem, kan du løse det eller ignorere det. Andre ikke-kritiske problemer (hvis f.eks. Anti-Spam eller Privacy Service ikke er installeret) ignoreres automatisk. Ignorerede problemer vises ikke i området med oplysninger om beskyttelseskategori i startruden til SecurityCenter, medmindre computerens beskyttelsesstatus er grøn. Hvis du ignorerer et problem, men senere beslutter, at det skal vises i området med oplysninger om beskyttelseskategori, selvom computerens beskyttelsesstatus ikke er grøn, kan du få vist det ignorerede problem.

Ignorere et beskyttelsesproblem

Hvis SecurityCenter registrerer et ikke-kritiske problem, som du ikke vil løse, kan du ignorere det. Når et problem ignoreres, fjernes det fra området med oplysninger om beskyttelseskategori i SecurityCenter.

- 1 Klik på **Start** under **Almindelige opgaver**.
- 2 Klik på den beskyttelseskategori, SecurityCenter har rapporteret problemet i, i startruden til SecurityCenter.
- 3 Klik på linket **Ignorer** ud for beskyttelsesproblemet.

Vise eller skjule ignorerede problemer

Afhængigt af alvoren kan du vise eller skjule et ignoreret beskyttelsesproblem.

- 1 Åbn ruden Alarmindstillinger.
Hvordan?
 1. Klik på **Start** under **Almindelige opgaver**.
 2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
 3. Under **Alarmer** skal du klikke på **Avanceret**.
- 2 Klik på **Ignorerede problemer** i ruden Konfiguration af SecurityCenter .
- 3 I ruden Ignorerede problemer skal du foretage en af følgende handlinger:
 - Marker dets afkrydsningsfelt for at ignorere et problem.
 - Fjern markeringen fra dets afkrydsningsfelt i området med oplysninger om beskyttelseskategori for at rapportere et problem.

4 Klik på **OK**.

Tip! Du kan også ignorere et problem ved at klikke på linket **Ignorer** ud for det rapporterede problem i området med oplysninger om beskyttelseskategori.

KAPITEL 6

Arbejde med alarmer

Alarmer er små pop-up-dialogbokse, som vises i skærmens nederste højre hjørne, når bestemte SecurityCenter-hændelser forekommer. En alarm indeholder detaljerede oplysninger om en hændelse samt anbefalinger og indstillinger, der kan løse de problemer, der evt. er knyttet til hændelsen. Nogle alarmer indeholder også links til yderligere oplysninger om hændelsen. Med disse links kan du gå til McAfees globale websted eller sende oplysninger til McAfee til fejlfinding.

Der findes følgende tre typer alarmer: rød, gul og grøn.

Alarmtype	Beskrivelse
Rød	En rød alarm er en kritisk besked, som kræver, at du reagerer. Røde alarmer forekommer, når SecurityCenter ikke kan afgøre, hvordan et beskyttelsesproblem kan løses automatisk.
Gul	En gul alarm er en ikke-kritisk besked, som ofte kræver, at du reagerer.
Grøn	En grøn alarm er en ikke-kritisk besked, som ikke kræver, at du reagerer. Grønne alarmer giver grundlæggende oplysninger om en hændelse.

Alarmer spiller en vigtig rolle i forbindelse med overvågning og administration af din beskyttelsesstatus, og derfor kan du ikke deaktivere dem. Du kan dog kontrollere, om visse typer oplysningsalarmer skal vises, og konfigurere andre alarmindstillinger (f.eks. om SecurityCenter skal afspille en lyd sammen med en alarm eller vise McAfee-velkomstbilledet ved opstart).

I dette kapitel

Vise og skjule oplysningsalarmer	24
Konfigurere alarmindstillinger.....	26

Vise og skjule oplysningsalarmer

Oplysningsalarmer giver dig besked om hændelser, som ikke udgør nogen trusler mod din sikkerhed. Hvis du f.eks. har konfigureret Firewall-beskyttelse, vises en oplysningsalarm som standard, når et program på computeren gives adgang til internettet. Hvis du ikke ønsker at få vist en bestemt type oplysningsalarm, kan du skjule den. Hvis du ikke ønsker at få vist nogen oplysningsalarmer, kan du skjule dem alle. Du kan også skjule alle oplysningsalarmer, når du spiller et spil i fuldskærmstilstand på computeren. Når du er færdig med at spille spillet og afslutter fuldskærmstilstand, viser SecurityCenter oplysningsalarmer igen.

Hvis du ved en fejl skjuler en oplysningsalarm, kan du til enhver tid få den vist igen. Som standard viser SecurityCenter alle oplysningsalarmer.

Vise eller skjule oplysningsalarmer

Du kan konfigurere SecurityCenter til at vise nogle oplysningsalarmer og skjule andre eller til at skjule alle oplysningsalarmer.

1 Åbn ruden Alarmindstillinger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Klik på **Oplysningsalarmer** i ruden Konfiguration af SecurityCenter.

3 I Oplysningsalarmer skal du foretage en af følgende handlinger:

- Hvis du vil vise en oplysningsalarm, skal du fjerne markeringerne i dens afkrydsningsfelt.
- Hvis du vil skjule en oplysningsalarm, skal du markere dens afkrydsningsfelt.
- Hvis du vil skjule alle oplysningsalarmer, skal du markere afkrydsningsfeltet **Vis ikke oplysningsalarmer**.

4 Klik på **OK**.

Tip! Du kan også skjule en oplysningsalarm ved at markere afkrydsningsfeltet **Vis ikke denne advarsel igen** i selve alarmen. Hvis du gør det, kan du få vist oplysningsalarmen igen ved at fjerne markeringen i det pågældende afkrydsningsfelt i ruden Oplysningsalarmer.

Vise eller skjule oplysningsalarmer under spil

Du kan også skjule oplysningsalarmer, når du spiller et spil i fuldskærmstilstand på computeren. Når du er færdig med at spille spillet og afslutter fuldskærmstilstand, viser SecurityCenter oplysningsalarmer igen.

1 Åbn ruden Alarmindstillinger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Marker eller fjern markeringen i afkrydsningsfeltet **Vis oplysningsalarmer, når spilletilstand registreres** i ruden Alarmindstillinger.

3 Klik på **OK**.

Konfigurere alarmindstillinger

Alarmernes udseende og frekvens konfigureres af SecurityCenter. Du kan dog justere de grundlæggende alarmindstillinger. Du kan f.eks. afspille en lyd med alarmer eller skjule velkomstbilledalarmen, når Windows startes. Du kan også skjule alarmer, der giver dig besked om virusudbrud og andre sikkerhedstrusler på internettet.

Afspille en lyd med alarmer

Hvis du vil modtage en lydbesked, når en alarm forekommer, kan du konfigurere SecurityCenter til at afspille en lyd med hver alarm.

- 1 Åbn ruden Alarmindstillinger.
Hvordan?
 1. Klik på **Start** under **Almindelige opgaver**.
 2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
 3. Under **Alarmer** skal du klikke på **Avanceret**.
- 2 Marker afkrydsningsfeltet **Afspil en lyd, når der opstår en alarm** under **Lyd** i ruden Alarmindstillinger.

Skjule velkomstbilledet ved opstart

Som standard vises McAfee-velkomstbilledet kortvarigt, når Windows startes, og giver dig besked om, at SecurityCenter beskytter computeren. Du kan dog skjule velkomstbilledet, hvis du ikke ønsker at få den vist.

- 1 Åbn ruden Alarmindstillinger.
Hvordan?
 1. Klik på **Start** under **Almindelige opgaver**.
 2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
 3. Under **Alarmer** skal du klikke på **Avanceret**.
- 2 Fjern markeringen i afkrydsningsfeltet **Vis McAfee-velkomstkærmen, når Windows starter** under **Velkomstbillede** i ruden Alarmindstillinger.

Tip! Du kan til enhver tid få vist velkomstbilledet igen ved at markere afkrydsningsfeltet **Vis McAfee-velkomstkærmen, når Windows starter**.

Skjule alarmer om virusudbrud

Du kan skjule alarmer, der giver dig besked om virusudbrud og andre sikkerhedstrusler på internettet.

1 Åbn ruden Alarmindstillinger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Fjern markeringen i afkrydsningsfeltet **Alarmer, når der forekommer en virus eller sikkerhedstrussel** i ruden Alarmindstillinger.

Tip! Du kan til enhver tid få vist alarmer om virusudbrud ved at markere afkrydsningsfeltet **Alarmer, når der forekommer en virus eller sikkerhedstrussel**.

KAPITEL 7

Vise hændelser

En hændelse er en handling eller konfigurationsændring, der forekommer inden for en beskyttelseskategori og de tilknyttede beskyttelsestjenester. Forskellige beskyttelsestjenester registrerer forskellige typer hændelser. SecurityCenter registrerer en hændelse, hvis en beskyttelsestjeneste er aktiveret eller deaktiveret. Virusbeskyttelse registrerer en hændelse, hver gang en virus registreres og fjernes. Firewall-beskyttelse registrerer en hændelse, hver gang et forsøg på at oprette forbindelse til internettet blokeres. Flere oplysninger om beskyttelseskategorier finder du under Forklaring af beskyttelseskategorier (side 9).

Du kan få vist hændelser, når du foretager fejlfinding af konfigurationsproblemer og gennemgår handlinger, der er foretaget af andre brugere. Mange forældre bruger hændelseslogfilen til at overvåge børnenes adfærd på internettet. Du kan få vist nylige hændelser, hvis du kun ønsker at undersøge de sidste 30 hændelser, der er forekommet. Du kan få vist alle hændelser, hvis du vil undersøge en omfattende liste over alle de hændelser, der er forekommet. Når du får vist alle hændelser, starter SecurityCenter hændelsesloggen, som sorterer hændelser efter den beskyttelseskategori, de er forekommet i.

I dette kapitel

Vise de seneste hændelser	29
Vise alle hændelser.....	29

Vise de seneste hændelser

Du kan få vist nylige hændelser, hvis du kun ønsker at undersøge de sidste 30 hændelser, der er forekommet.

- Klik på **Vis seneste hændelser** under **Almindelige opgaver**.

Vise alle hændelser

Du kan få vist alle hændelser, hvis du vil undersøge en omfattende liste over alle de hændelser, der er forekommet.

- 1 Klik på **Vis seneste hændelser** under **Almindelige opgaver**.
- 2 Klik på **Vis logfil** i ruden Seneste hændelser.
- 3 Klik på den type hændelse, du ønsker at få vist.

KAPITEL 8

McAfee VirusScan

De avancerede registrerings- og beskyttelsestjenester i VirusScan forsvarer dig og din computer mod de nyeste sikkerhedstrusler, herunder virus, trojanske heste, sporingscookies, spyware, adware og andre potentielt uønskede programmer. Beskyttelsen udvides ud over filerne og mapperne på den stationære computer og målrettes mod trusler fra forskellige indgange, herunder e-mail, onlinemeddelelser og internettet.

Med VirusScan beskyttes computeren omgående og hele tiden (der kræves ingen langsommelig administration). Mens du arbejder, spiller, søger på internettet eller tjekker din e-mail, køres programmet i baggrunden og overvåger, scanner og registrerer potentiel skade i real tid. Omfattende scanninger gennemføres efter en plan, så computeren jævnlige kontrolleres ved hjælp af et mere avanceret sæt indstillinger. VirusScan giver dig fleksibilitet til at tilpasse denne funktion, hvis du ønsker det. Hvis du ikke ønsker det, forbliver computeren beskyttet.

Ved normal brug af en computer kan den blive infiltreret med virus, orm og andre potentielle trusler. Hvis det forekommer, giver VirusScan dig besked om truslen, men normalt håndterer programmer truslen for dig og renser eller sætter inficerede elementer i karantæne, inden der opstår skade. Selvom det er sjældent, kan der være nødvendigt med yderligere handling. I disse tilfælde lader VirusScan dig vælge, hvad du vil gøre (scanne igen, næste gang computeren startes, beholde det registrerede element eller fjerne det registrerede element).

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i VirusScan	32
Starte virusbeskyttelse i realtid	33
Starte yderligere beskyttelse	35
Konfigurere virusbeskyttelse	39
Scanne computeren	57
Arbejde med scanningsresultater	61

Funktioner i VirusScan

VirusScan indeholder følgende funktioner.

Omfattende virusbeskyttelse

De avancerede registrerings- og beskyttelsestjenester i VirusScan forsvarer dig og din computer mod de nyeste sikkerhedstrusler, herunder virus, trojanske heste, sporingscookies, spyware, adware og andre potentielt uønskede programmer. Beskyttelsen udvides ud over filerne og mapperne på den stationære computer og målrettes mod trusler fra forskellige indgange, herunder e-mail, onlinemeddelelser og internettet. Der kræves ingen langsommelig administration.

Ressourcebevidste scanningsindstillinger

Hvis du oplever langsom scanningshastighed, kan du deaktivere indstillingen for brug af færrest mulige computerressourcer. Du skal dog være opmærksom på, at virusbeskyttelse prioriteres højere end andre opgaver. VirusScan giver dig fleksibilitet til at tilpasse indstillingerne for realtidsscanning og manuel scanning, hvis du ønsker det. Hvis du ikke ønsker det, forbliver computeren beskyttet.

Automatiske reparationer

Hvis VirusScan registrerer en sikkerhedstrussel under en realtidsscanning eller en manuel scanning, forsøger programmet at håndtere truslen automatisk i overensstemmelse med trusselstypen. På den måde kan de fleste trusler registreres og neutraliseres uden din medvirken. Selvom det er sjældent, kan VirusScan ikke altid selv neutralisere en trussel. I disse tilfælde lader VirusScan dig vælge, hvad du vil gøre (scanne igen, næste gang computeren startes, beholde det registrerede element eller fjerne det registrerede element).

Afbryde opgaver midlertidigt i fuldskærmstilstand

Når du f.eks. ser film, spiller spil eller udfører andre aktiviteter på computeren, som fylder hele skærmen, standser VirusScan en række opgaver midlertidigt, herunder automatiske opdateringer og manuelle scanninger.

Starte virusbeskyttelse i realtid

VirusScan giver dig to typer virusbeskyttelse: realtidsbeskyttelse og manuel beskyttelse. Virusbeskyttelse i realtid overvåger konstant computeren for virusaktivitet og scanner filer, hver gang du eller din computer forsøger at åbne dem. Manuel virusbeskyttelse giver dig mulighed for at scanne filer, når du ønsker det. Hvis du vil sikre, at computeren altid er beskyttet mod de seneste sikkerhedstrusler, skal du lade virusbeskyttelse i realtid være aktiveret og oprette en plan for regelmæssige og mere omfattende manuelle scanninger. Som standard gennemfører VirusScan en planlagt scanning en gang om ugen. Flere oplysninger om realtidsscanning og manuel scanning finder du under Scanne computeren (side 57).

Selvom det er sjældent, kan der forekomme tilfælde, hvor du midlertidigt vil standse realtidsscanningen (f.eks. for at ændre scanningsindstillinger eller fejlfinde et effektivitetsproblem). Når virusbeskyttelse i realtid er deaktiveret, er din computer ikke beskyttet, og beskyttelsesstatus i SecurityCenter er rød. Flere oplysninger om beskyttelsesstatus finder du under "Forklaring af beskyttelsesstatus" i SecurityCenter Hjælp.

Starte virusbeskyttelse i realtid

Som standard er virusbeskyttelse i realtid aktiveret og beskytter computeren mod virus, trojanske heste og andre sikkerhedstrusler. Hvis du slår virusbeskyttelse i realtid fra, skal du slå den til igen for at beskytte computeren.

- 1 Åbn konfigurationsruden Computer & filer.
Hvordan?
 1. Klik på menuen **Avanceret** i den venstre røde.
 2. Klik på **Konfigurer**.
 3. Klik derefter på **Computer & filer** i ruden Konfigurer.
- 2 Under **Virusbeskyttelse** skal du klikke på **Til**.

Standse virusbeskyttelse i realtid

Du kan slå virusbeskyttelse i realtid fra midlertidigt og derefter angive, hvornår den skal genstartes. Du kan automatisk genstarte beskyttelse efter 15, 30, 45 eller 60 minutter, når computeren genstartes, eller aldrig.

- 1 Åbn konfigurationsruden Computer & filer.
Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **Computer & filer** i ruden Konfigurer.
- 2** Under **Virusbeskyttelse** skal du klikke på **Fra**.
- 3** Vælg, hvornår realtidsscanning skal genstartes, i dialogboksen.
- 4** Klik på **OK**.

KAPITEL 9

Starte yderligere beskyttelse

Ud over virusbeskyttelse i realtid giver VirusScan avanceret beskyttelse mod scripts, spyware og potentielt skadelige vedhæftede filer i e-mail og onlinemeddelelser. Som standard er scriptscanning samt spyware-, e-mail- og onlinemeddelelsesbeskyttelse aktiveret og beskytter computeren.

Scriptscanning

Scriptscanning registrerer potentielt skadelige scripts og forhindrer dem i at køre på din computer. Funktionen overvåger computeren for mistænkelig scriptaktivitet, f.eks. et script, der opretter, kopierer eller sletter filer, eller som åbner din Windows-registreringsdatabase, og giver dig besked, inden der opstår skade.

Spywarebeskyttelse

Spywarebeskyttelse registrerer spyware, adware og andre potentielt uønskede programmer. Spyware er software, der hemmeligt kan installeres på din computer for at overvåge dine aktiviteter, indsamle personlige oplysninger og endda gribe ind i din kontrol over computeren ved at installere yderligere software eller omdirigere browseraktivitet.

E-mail-beskyttelse

E-mail-beskyttelse registrerer mistænkelig aktivitet i de e-mail-beskeder og vedhæftede filer, du afsender og modtager.

Beskyttelse af onlinemeddelelser

Beskyttelse af onlinemeddelelser registrerer potentielle sikkerhedstrusler i vedhæftede filer i onlinemeddelelser, som du modtager. Funktionen forhindrer også IM-programmer i at dele personlige oplysninger.

I dette kapitel

Starte scriptscanning	36
Starte spywarebeskyttelse	36
Starte e-mail-beskyttelse	36
Starte beskyttelse af onlinemeddelelser	37

Starte scriptscanning

Slå scriptscanning til for at registrere potentielt skadelige scripts og forhindre dem i at køre på din computer. Scriptscanning giver dig besked, når et script forsøger at oprette, kopiere eller slette filer på computeren eller foretage ændringer i Windows-registreringsdatabasen.

1 Åbn konfigurationsruden Computer & filer.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **Computer & filer** i ruden Konfigurer.

2 Under **Scriptscanning** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå scriptscanning fra, men computeren bliver så sårbar over for skadelige scripts.

Starte spywarebeskyttelse

Slå spywarebeskyttelse til for at registrere og fjerne spyware, adware og andre potentielt uønskede programmer, som samler og sender data uden din viden eller tilladelse.

1 Åbn konfigurationsruden Computer & filer.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **Computer & filer** i ruden Konfigurer.

2 Under **Scriptscanning** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå spywarebeskyttelse fra, men computeren bliver så sårbar over for potentielt uønskede programmer.

Starte e-mail-beskyttelse

Slå e-mail-beskyttelse til for at registrere orm og potentielle trusler i indgående (POP3) og udgående (SMTP) e-mail-beskeder og vedhæftede filer.

1 Åbn konfigurationsruden E-mail & IM.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **E-mail & IM** i ruden Konfigurer.

2 Under **E-mail-beskyttelse** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå e-mail-beskyttelse fra, men computeren bliver så sårbar over for e-mail-trusler.

Starte beskyttelse af onlinemeddelelser

Slå beskyttelse af onlinemeddelelser til for at registrere sikkerhedstrusler i vedhæftede filer i indgående onlinemeddelelser.

1 Åbn konfigurationsruden E-mail & IM.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **E-mail & IM** i ruden Konfigurer.

2 Under **Beskyttelse af onlinemeddelelser** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå beskyttelse af onlinemeddelelser fra, men computeren bliver så sårbar over for skadelige vedhæftede filer i onlinemeddelelser.

KAPITEL 10

Konfigurere virusbeskyttelse

VirusScan giver dig to typer virusbeskyttelse: realtidsbeskyttelse og manuel beskyttelse. Virusbeskyttelse i realtid scanner filer, hver gang du eller din computer forsøger at åbne dem. Manuel virusbeskyttelse giver dig mulighed for at scanne filer, når du ønsker det. Du kan angive forskellige indstillinger for hver type beskyttelse. Da realtidsbeskyttelse konstant overvåger computeren, kan du f.eks. vælge et bestemt sæt grundlæggende scanningsindstillinger og reservere et mere omfattende sæt scanningsindstillinger til manuel, on-demand-beskyttelse.

I dette kapitel

Vælge indstillinger for realtidsscanning.....	40
Vælge indstillinger for manuel scanning.....	42
Brug af indstillinger for systembeskyttelse.....	46
Brug af lister, der er tillid til	53

Vælge indstillinger for realtidsscanning

Når du starter virusbeskyttelse i realtid, bruger VirusScan et standardsæt indstillinger til at scanne filer. Du kan dog ændre standardindstillingerne, så de opfylder dine behov.

Hvis du vil ændre indstillingerne for realtidsscanning, skal du vælge, hvad VirusScan skal kontrollere for under en scanning, og de placeringer og filtyper, der skal scannes. Du kan f.eks. vælge, om VirusScan skal kontrollere for ukendte virus eller cookies, som websteder kan bruge til at registrere dine aktiviteter, og om programmet skal scanne netværksdrev, der er tilknyttet computeren, eller kun lokale drev. Du kan også vælge, hvilke typer filer der skal scannes (alle filer eller kun programfiler og dokumenter, da de fleste virus registreres i disse filer).

Når du ændrer indstillingerne for realtidsscanning, skal du også afgøre, om det er vigtigt for computeren, at beskyttelse for bufferoverløb er aktiveret. En buffer er en del af hukommelsen, som midlertidigt lagrer computerinformation. Bufferoverløb kan forekomme, når den mængde oplysninger, som mistænkelig programmer eller processer lagrer i en buffer, overstiger bufferens kapacitet. Hvis det sker, bliver computeren sårbar over for sikkerhedsangreb.

Vælge indstillinger for realtidsscanning

Du kan angive indstillinger for realtidsscanning for at tilpasse, hvad VirusScan skal kontrollere for under en scanning, og de placeringer og filtyper, der skal scannes. Indstillingerne omfatter scanning for ukendte virus og sporingscookies samt beskyttelse mod bufferoverløb. Du kan også konfigurere realtidsscanning til at kontrollere netværksdrev, der er tilknyttet på computeren.

1 Åbn ruden Scanning i realtid.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.

2 Angiv de ønskede indstillinger for realtidsscanning, og klik derefter på **OK**.

For at...	Skal du...
Registrere ukendte virus og nye varianter af kendte virus	Markere afkrydsningsfeltet Scan for ukendte virus ved hjælp af heuristik .

Registrere cookies	Markere afkrydningsfeltet Scan og fjern sporingscookies.
Registrere virus og andre potentielle trusler på drev, der er tilsluttet netværket	Markere afkrydningsfeltet Scan netværksdrev.
Beskytte computeren mod bufferoverløb	Markere afkrydningsfeltet Aktiver beskyttelse for bufferoverløb.
Angive de filtyper, der skal scannes	Klikke på Alle filer (anbefales) eller Kun programfiler og dokumenter.

Vælge indstillinger for manuel scanning

Manuel virusbeskyttelse giver dig mulighed for at scanne filer, når du ønsker det. Når du starter en manuel scanning, kontrollerer VirusScan computeren for virus og andre potentielt skadelige elementer ved hjælp af et mere omfattende sæt scanningsindstillinger. Hvis du vil ændre indstillingerne for manuel scanning, skal du vælge, hvad VirusScan skal kontrollere for under en scanning. Du kan f.eks. bestemme, om VirusScan skal søge efter ukendte virus, potentielt uønskede programmer, f.eks. spyware eller adware, skjulte programmer, f.eks. rootkits, der kan give uautoriseret adgang til computeren, og cookies, som websteder kan bruge til at spore dine aktiviteter. Du skal også vælge, hvilke filtyper der skal kontrolleres. Du kan f.eks. vælge, om VirusScan skal kontrollere alle filer eller kun programfiler og dokumenter (da de fleste virus registreres i disse filer). Du kan også vælge, om komprimerede filer (f.eks. .zip-filer) skal medtages i scanningen.

Som standard kontrollerer VirusScan alle drev og mapper på computeren, hver gang programmet kører en manuel scanning. Du kan dog ændre standardplaceringerne, så de opfylder dine behov. Du kan f.eks. vælge kun at scanne vigtige systemfiler, elementer på skrivebordet eller elementer i mappen Programmer. Medmindre du selv vil starte alle manuelle scanninger, kan du definere en tidsplan for scanningerne. Planlagte scanninger kontrollerer altid hele computeren ved hjælp af standardindstillingerne for scanning. Som standard gennemfører VirusScan en planlagt scanning en gang om ugen.

Hvis du oplever langsom scanningshastighed, kan du deaktivere indstillingen for brug af færrest mulige computerressourcer. Du skal dog være opmærksom på, at virusbeskyttelse prioriteres højere end andre opgaver.

Bemærk! Når du f.eks. ser film, spiller spil eller udfører andre aktiviteter på computeren, som fylder hele skærmen, standser VirusScan en række opgaver midlertidigt, herunder automatiske opdateringer og manuelle scanninger.

Vælge indstillinger for manuel scanning

Du kan angive indstillinger for manuel scanning for at tilpasse, hvad VirusScan skal kontrollere for under en scanning, og de placeringer og filtyper, der skal scannes. Indstillinger omfatter scanning for ukendte virus, filarkiver, spyware og potentielt uønskede programmer, sporingscookies, rootkits og skjulte programmer.

1 Åbn ruden Manuel scanning.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
 2. Klik på **Computer & filer** i startruden for SecurityCenter.
 3. Klik på **Konfigurer** i området Computer & filer.
 4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.
 5. Klik på **Manuel scanning** i ruden Virusbeskyttelse.
- 2 Angiv de ønskede indstillinger for manuel scanning, og klik derefter på **OK**.

For at...	Skal du...
Registrere ukendte virus og nye varianter af kendte virus	Markere afkrydsningsfeltet Scan for ukendte virus ved hjælp af heuristik .
Registrere og fjerne virus i .zip-filer og andre komprimerede filer	Markere afkrydsningsfeltet Scan .zip-filer og andre komprimerede filer .
Registrere spyware, adware og andre potentielt uønskede programmer	Markere afkrydsningsfeltet Scan for spyware og potentielt uønskede programmer .
Registrere cookies	Markere afkrydsningsfeltet Scan og fjern springscookies .
Registrere rootkits og skjulte programmer, der kan ændre og udnytte eksisterende Windows-systemfiler	Markere afkrydsningsfeltet Scan for rootkits og andre skjulte programmer .
Bruge mindre processorkraft til scanninger, hvilket giver højere prioritet til andre opgaver (f.eks. surfing på internettet eller åbning af dokumenter)	Markere afkrydsningsfeltet Scan ved brug af færrest mulige computerressourcer .
Angive de filtyper, der skal scannes	Klikke på Alle filer (anbefales) eller Kun programfiler og dokumenter .

Vælge placering til manuel scanning

Du angiver placeringer til manuel scanning for at bestemme, hvor VirusScan skal søge efter virus og andre skadelige elementer under en manuel scanning. Du kan scanne alle filer, mapper og drev på computeren, eller du kan begrænse scanningen til bestemte mapper og drev.

1 Åbn ruden Manuel scanning.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.
5. Klik på **Manuel scanning** i ruden Virusbeskyttelse.

2 Klik på **Standardplacering, der skal scannes**.

3 Angiv placeringen til manuel scanning, og klik derefter på **OK**.

For at...	Skal du...
Scanne alle filer og mapper på computeren	Markere afkrydsningsfeltet (Min) computer .
Scanne bestemte filer, mapper og drev på computeren	Fjerne markeringen i afkrydsningsfeltet (Min) computer og markere en eller flere mapper eller et eller flere drev.
Scanne vigtige systemfiler	Fjerne markeringen i afkrydsningsfeltet (Min) computer og derefter markere afkrydsningsfeltet Vigtige systemfiler .

Planlægge en scanning

Planlæg scanninger for at tjekke din computer grundigt for virus og andre trusler på enhver dag og ethvert tidspunkt i løbet af ugen. Planlagte scanninger kontrollerer altid hele computeren ved hjælp af standardindstillingerne for scanning. Som standard gennemfører VirusScan en planlagt scanning en gang om ugen. Hvis du oplever langsom scanningshastighed, kan du deaktivere indstillingen for brug af færrest mulige computerressourcer. Du skal dog være opmærksom på, at virusbeskyttelse prioriteres højere end andre opgaver.

1 Åbn ruden Planlagt scanning.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i starttruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.
5. Klik på **Planlagt scanning** i ruden Virusbeskyttelse.

2 Vælg **Aktiver planlagt scanning**.

3 Hvis du vil reducere den mængde processorkraft, der normalt bruges til scanning, skal du vælge **Scan ved brug af færrest mulige computerressourcer**.

4 Vælg en eller flere dage.

5 Angiv et starttidspunkt.

6 Klik på **OK**.

Tip! Du kan gendanne standardplanen ved at klikke på **Nulstil**.

Brug af indstillinger for systembeskyttelse

Systembeskyttelse overvåger, logger, rapporterer og administrerer potentielt uautoriserede ændringer i Windows-databasen eller vigtige systemfiler på computeren. Uautoriserede ændringer i registreringsdatabasen kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.

Ændringer i registreringsdatabase og filer er almindelige og kan forekomme regelmæssigt på computeren. Da mange af ændringerne er uskadelige, er standardindstillingerne for systembeskyttelse konfigureret til at sikre pålidelig, intelligent og virkelig beskyttelse mod uautoriserede ændringer, der potentielt kan medføre betydelig skade. Når systembeskyttelse f.eks. registrerer ændringer, der er ualmindelige og repræsenterer en potentielt væsentlig trussel, rapporteres og logges aktiviteten omgående. Ændringer, der er mere almindelige, men som stadig repræsenterer en potentiel skade, registreres kun i logfilen. Overvågning for standardændringer med lav risiko er dog som standard slået fra. Systembeskyttelsesteknologien kan konfigureres, så dens beskyttelse udvides til ethvert miljø, du ønsker.

Der findes tre typer systembeskyttelser: Program-systembeskyttelse, Windows-systembeskyttelse og Browser-systembeskyttelse.

Program-systembeskyttelse

Program-systembeskyttelse registrerer potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Disse vigtige registreringsdatabaseelementer og filer omfatter ActiveX-installationer, opstartselementer, Windows Shell Execute Hooks og Shell Service Object Delay Loads. Ved at overvåge disse standser Program-systembeskyttelse mistænkelige ActiveX-programmer (downloadet fra internettet) samt spyware og potentielt uønskede programmer, som automatisk kan startes, når Windows startes.

Windows-systembeskyttelse

Windows-systembeskyttelse registrerer også potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Disse vigtige registreringsdatabaseelementer og filer omfatter håndtering af genvejsmenuer, appInit DLL-filer og Windows-værtsfilen. Ved at overvåge disse hjælper Windows-systembeskyttelse med at forhindre computeren i at sende og modtage uautoriserede eller personlige oplysninger over internettet. Den hjælper også med at stoppe mistænkelige programmer, der kan forårsage uønskede ændringer i udseendet og funktionaliteten af de programmer, som er vigtige for dig og din familie.

Browser-systembeskyttelse

Ligesom Program- og Windows-systembeskyttelse registrerer Browser-systembeskyttelse også potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Browser-systembeskyttelse overvåger dog ændringer i vigtige registreringsdatabaseelementer og filer, som f.eks. Internet Explorer-tilføjelsesprogrammer, Internet Explorer-webadresser og Internet Explorer-sikkerhedszoner. Ved at overvåge disse hjælper Browser-systembeskyttelse med at forhindre uautoriseret browseraktivitet, som f.eks. omdirigering til mistænkelige websteder, ændringer i browserindstillinger uden din viden og uønsket tillid til mistænkelige websteder.

Aktivere systembeskyttelse

Aktiver systembeskyttelse for at registrere og få besked om potentielt uautoriserede ændringer i Windows-registreringsdatabasen og filer på computeren. Uautoriserede ændringer i registreringsdatabasen kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.

1 Åbn konfigurationsruden Computer & filer.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **Computer & filer** i ruden Konfigurer.

2 Under **Systembeskyttelse** skal du klikke på **Til**.

Bemærk! Du kan deaktivere systembeskyttelse ved at klikke på **Fra**.

Konfigurere indstillinger for systembeskyttelse

Brug ruden Systembeskyttelse til at konfigurere indstillinger for beskyttelse, logføring og alarmer vedrørende uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Windows-filer, programmer og Internet Explorer. Uautoriserede ændringer i registreringsdatabasen kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.

1 Åbn ruden Systembeskyttelse.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i starttruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at systembeskyttelse er aktiveret i konfigurationsruden Computer & Filer, og klik derefter på **Avanceret**.

2 Vælg en type systembeskyttelse på listen.

- **Program-systembeskyttelse**
- **Windows-systembeskyttelse**
- **Browser-systembeskyttelse**

3 Under **Jeg ønsker at** skal du udføre en af følgende handlinger:

- Hvis du vil registrere, logføre og rapportere uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Program-, Windows- og Browser-systembeskyttelser, skal du klikke på **Vis alarmer**.
- Hvis du vil registrere og logføre uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Program-, Windows- og Browser-systembeskyttelser, skal du klikke på **Logfør kun ændringer**.
- Hvis du vil deaktivere registrering af uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Program-, Windows- og Browser-systembeskyttelser, skal du klikke på **Deaktiver systembeskyttelse**.

Bemærk! Flere oplysninger om systembeskyttelsestyper finder du under Om systembeskyttelsestyper (side 49).

Om systembeskyttelsestyper

Systembeskyttelse registrerer potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Der findes tre typer systembeskyttelser: Program-systembeskyttelse, Windows-systembeskyttelse og Browser-systembeskyttelse.

Program-systembeskyttelse

Program-systembeskyttelse standser mistænkelige ActiveX-programmer (downloadet fra internettet) samt spyware og potentielt uønskede programmer, som automatisk kan startes, når Windows startes.

Systembeskyttelse	Registrerer...
ActiveX-installationer	Uautoriserede ændringer i ActiveX-installationer, der kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.
Opstartselementer	Spyware, adware og andre potentielt uønskede programmer, der kan kan installere fil- eller registreringsdatabaseændringer til startelementer, så mistænkelige programmer kan køres, når du starter din computer.
Windows Shell Execute Hooks	Spyware, adware og andre potentielt uønskede programmer, der kan installere Windows Shell Execute Hooks for at forhindre sikkerhedsprogrammer i at køre korrekt.
Shell Service Object Delay Load	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabase i forbindelse med Shell Service Object Delay Load, så skadelige filer kan afvikles, når du starter din computer.

Windows-systembeskyttelse

Windows-systembeskyttelse hjælper med at forhindre computeren i at sende og modtage uautoriserede eller personlige oplysninger over internettet. Den hjælper også med at stoppe mistænkelige programmer, der kan forårsage uønskede ændringer i udseendet og funktionaliteten af de programmer, som er vigtige for dig og din familie.

System- beskyttelse	Registrerer...
Håndtering af genvejsmenu	Uautoriserede ændringer i registreringsdatabasen i forbindelse med håndtering af genvejsmenuer i Windows, der kan påvirke udseendet og funktionen af Windows-menuerne. Med genvejsmenuer kan du udføre handlinger på din computer, f.eks. højreklikke på filer.
AppInit DLL-filer	Uautoriserede ændringer i registreringsdatabasen i forbindelse med Windows AppInit_DLL-filer, der kan medføre, at potentielt skadelige filer kan afvikles, når du starter din computer.
Windows værtsfiler	Spyware, adware og potentielt uønskede programmer, der kan foretage uautoriserede ændringer i din Windows-værtsfil, hvilket gør det muligt, at din browser kan om dirigere dig til mistænkelige websteder og blokere softwareopdateringer.
Winlogon Shell	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Winlogon Shell, så andre programmer kan erstatte Windows Stifinder.
Winlogon Userinit	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Winlogon User Init, så mistænkelige programmer kan køre, når du logger på Windows.
Windows-protokoller	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Windows-protokoller, så den måde, hvorpå din computer sender og modtager oplysninger via internettet, påvirkes.
Winsock Layered Service Providers	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Winsock Layered Service Providers (LSP'er) for på den måde at opfange og ændre de oplysninger, som du sender og modtager via internettet.

Windows Shell-åbningskommandoer	Uautoriserede ændringer i Windows Shell-åbningskommandoer, der kan give mulighed for, at orme og andre skadelige programmer kan køre på din computer.
SharedTaskScheduler	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Shared Task Scheduler, så skadelige filer kan afvikles, når du starter din computer.
Windows Messenger Service	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Windows Messenger Service, så uopfordrede reklamer og eksternt afviklede programmer kan køre på din computer.
Windows-filen win.ini	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i Win.ini-filen, så mistænkelige programmer kan køres, når du starter din computer.

Browser-systembeskyttelse

Browser-systembeskyttelse hjælper med at forhindre uautoriseret browseraktivitet, som f.eks. omdirigering til mistænkelige websteder, ændringer i browserindstillinger uden din viden og uønsket tillid til mistænkelige websteder.

Systembeskyttelse	Registrerer...
Browserhjelpeobjekter	Spyware, adware og andre potentielt uønskede programmer, der kan bruge browserhjelpeobjekter til at spore surfing på internettet og vise uopfordrede reklamer.
Værktøjslinjer i Internet Explorer	Uautoriserede ændringer i registreringsdatabasen i forbindelse med programmer på Internet Explorer-værktøjslinjen, f.eks. Søg og Foretrukne, der kan påvirke udseendet og funktionen af Internet Explorer.
Internet Explorer-tilføjelsesprogrammer	Spyware, adware og andre potentielt uønskede programmer, der kan installere Internet Explorer-tilføjelsesprogrammer til at spore surfing på internettet og vise uopfordrede reklamer.
Internet Explorer ShellBrowser	Uautoriserede ændringer i registreringsdatabasen i forbindelse med Internet Explorer ShellBrowser, der kan påvirke udseendet og funktionen af din webbrowser.

Internet Explorer WebBrowser	Uautoriserede ændringer i registreringsdatabasen i forbindelse med Internet Explorer-webbrowseren, der kan påvirke udseendet og funktionen af din webbrowser.
Internet Explorer URL Search Hooks	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Internet Explorer URL Search Hook, så din browser kan omdirigeres til mistænkelige websteder, når du søger på internettet.
Internet Explorer URLer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Internet Explorer URLer, som påvirker browserindstillingerne.
Begrænsninger af Internet Explorer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med begrænsninger af Internet Explorer, som påvirker browserindstillingerne og -muligheder.
Sikkerhedszoner i Internet Explorer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Sikkerhedszoner i Internet Explorer, så potentielt skadelige filer kan afvikles, når du starter din computer.
Websteder, der har tillid til i Internet Explorer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Websteder, du har tillid til i Internet Explorer, så din browser har tillid til mistænkelige websteder.
Internet Explorer-regler	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med politikker i Internet Explorer, som browserens udseende og funktion.

Brug af lister, der er tillid til

Hvis VirusScan registrerer en fil- eller registreringsdatabaseændring (systembeskyttelse), program eller bufferoverløb, bliver du spurgt, om du har tillid til elementet eller vil fjerne det. Hvis du har tillid til elementet og angiver, at du ikke ønsker at modtage besked om dets aktivitet i fremtiden, føjes elementet til en liste over elementer, der er tillid til. Derefter registrerer VirusScan det ikke længere og giver dig ikke besked om dets aktivitet. Hvis et element er føjet til en liste, du har tillid til, men du ønsker at blokere dets aktivitet, kan du gøre det. Blokering forhindrer elementet i at køre eller foretage ændringer i computeren, uden at du får besked, hver gang der gøres et forsøg. Du kan også fjerne et element fra en liste over elementer, der er tillid til. Når du fjerner et element, kan VirusScan registrere dets aktiviteter igen.

Administrere lister over elementer, der er tillid til

Brug ruden Lister, der er tillid til, til at tillade eller blokere elementer, der tidligere er registreret og tilladt. Du kan også fjerne et element fra en liste over elementer, der er tillid til, så VirusScan registrerer det igen.

1 Åbn ruden Lister, der er tillid til.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.
5. Klik på **Lister, der er tillid til** i ruden Virusbeskyttelse.

2 Marker en af følgende typer af lister, der er tillid til:

- **Program-systembeskyttelse**
- **Windows-systembeskyttelse**
- **Browser-systembeskyttelse**
- **Programmer, der er tillid til**
- **Bufferoverløb, der er tillid til**

3 Under **Jeg ønsker at** skal du udføre en af følgende handlinger:

- Hvis du vil tillade, at det registrerede element foretager ændringer i Windows-registreringsdatabase eller vigtige systemfiler på computeren uden at give dig besked, skal du klikke på **Hav tillid til**.

- Hvis du vil forhindre, at det registrerede element foretager ændringer i Windows-registreringsdatabasen eller vigtige systemfiler på computeren uden at give dig besked, skal du klikke på **Bloker**.
- Hvis du vil fjerne det registrerede element fra listen over elementer, der er tillid til, skal du klikke på **Fjern**:

4 Klik på **OK**.

Bemærk! Flere oplysninger om typer af lister, der er tillid til, finder du under Om typer af lister, der er tillid til (side 54).

Om typer af lister, der er tillid til

Systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater. Der findes fem typer af lister, der er tillid til, som du kan administrere i ruden Lister, der er tillid til: Program-systembeskyttelse, Windows-systembeskyttelse, Browser-systembeskyttelse, Programmer, der er tillid til, og Bufferoverløb, der er tillid til.

Indstilling	Beskrivelse
Program-systembeskyttelse	<p>Program-systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater.</p> <p>Program-systembeskyttelse registrerer uautoriserede registreringsdatabase- og filændringer i forbindelse med ActiveX-installationer, opstartselementer, Windows Shell Execute Hooks og Shell Service Object Delay Loads. Disse typer uautoriserede registreringsdatabase- og filændringer kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.</p>

<p>Windows-systembeskyttelse</p>	<p>Windows-systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater.</p> <p>Windows-systembeskyttelse registrerer uautoriserede registreringsdatabase- og filændringer i forbindelse med håndtering af genvejsmenuer i Windows, appInit DLL-filer, Windows-værtsfilen, Winlogon Shell, Winsock Layered Service Providers (LSP'er) osv. Disse typer uautoriserede registreringsdatabase- og filændringer kan påvirke den måde, computeren sender og modtager information via internettet på, ændre programmets udseende og funktion og tillade, at mistænkelige programmer køres på computeren.</p>
<p>Browser-systembeskyttelse</p>	<p>Browser-systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater.</p> <p>Browser-systembeskyttelse overvåger uautoriserede registreringsdatabaseændringer og andre uønskede aktiviteter i forbindelse med browserhjelpeobjekter, Internet Explorer-tilføjelsesprogrammer, Internet Explorer URLer, Internet Explorer-sikkerhedszoner osv. Disse typer uautoriserede registreringsdatabaseændringer kan resultere i uønsket browseraktivitet, som f.eks. omdirigering til mistænkelige websteder, ændringer i browserindstillinger uden din viden og uønsket tillid til mistænkelige websteder.</p>
<p>Programmer, der er tillid til</p>	<p>Programmer, der er tillid til, er potentielt uønskede programmer, som VirusScan tidligere har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater.</p>
<p>Bufferoverløb, der er tillid til</p>	<p>Bufferoverløb, der er tillid til, er tidligere uønsket aktivitet, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater.</p> <p>Bufferoverløb kan skade din computer og beskadige filer. Bufferoverløb sker, når den mængde oplysninger, som mistænkelig programmer eller processer lagrer i en buffer, overstiger bufferens kapacitet.</p>

KAPITEL 11

Scanne computeren

Første gang du starter SecurityCenter, begynder virusbeskyttelsen i VirusScan at beskytte computeren mod potentielt skadelige virus, trojanske heste og andre sikkerhedstrusler i realtid. Medmindre du deaktiverer virusbeskyttelse i realtid, overvåger VirusScan konstant computeren for virusaktivitet og scanner filer, hver gang du eller din computer forsøger at åbne dem, ved hjælp af de indstillinger for realtidsscanning, du vælger. Hvis du vil sikre, at computeren altid er beskyttet mod de seneste sikkerhedstrusler, skal du lade virusbeskyttelse i realtid være aktiveret og oprette en plan for regelmæssige og mere omfattende manuelle scanninger. Flere oplysninger om realtidsscanning og manuel scanning finder du under Konfigurere virusbeskyttelse (side 39).

VirusScan indeholder et mere detaljeret sæt scanningsindstillinger for manuel virusbeskyttelse, som giver dig mulighed for regelmæssigt at køre mere omfattende scanninger. Du kan køre manuelle scanninger fra SecurityCenter og målrette mod bestemte placeringer i henhold til en angivet plan. Du kan også køre manuelle scanninger direkte i Windows Stifinder, mens du arbejder. Ved scanning i SecurityCenter kan du skifte scanningsindstillinger undervejs. Scanning fra Windows Stifinder gør det dog nemt for dit at beskytte computerens sikkerhed.

Uanset om du kører en manuel scanning fra SecurityCenter eller Windows Stifinder, kan du få vist scanningsresultaterne efter scanningen. Vis resultaterne af en scanning for at finde ud af, om VirusScan har registreret, repareret eller sat virus, trojanske heste, spyware, adware, cookies og andre potentielt uønskede programmer i karantæne. Du kan få vist resultaterne af en scanning på forskellige måder. Du kan f.eks. få vist et grundlæggende resume af scanningsresultaterne eller detaljerede oplysninger, som f.eks. infektionsstatus og -type. Du kan også få vist generel scannings- og registreringsstatistik.

I dette kapitel

Scanne computeren	58
Vise scanningsresultater	58

Scanne computeren

Du kan køre en manuel scanning fra menuen Avanceret eller Grundlæggende i SecurityCenter. Hvis du kører en scanning fra menuen Avanceret, kan du bekræfte indstillingerne for manuel scanning, inden scanningen startes. Hvis du kører en scanning fra menuen Grundlæggende, starter VirusScan scanningen med det samme ved brug af de eksisterende scanningsindstillinger. Du kan også køre en scanning i Windows Stifinder ved brug af de eksisterende scanningsindstillinger.

- Nu kan du gøre følgende:

Scanne i SecurityCenter

For at...	Skal du...
Scanne ved brug af eksisterende indstillinger	Klikke på Scan i menuen Grundlæggende.
Scanne ved brug af ændrede indstillinger	Klikke på Scan i menuen Avanceret, vælge de placeringer, der skal scannes, vælge scanningsindstillinger og derefter klikke på Scan nu .

Scanne i Windows Stifinder

- Åbn Windows Stifinder.
- Højreklik på en fil, en mappe eller et drev, og klik derefter på **Scan**.

Bemærk! Scanningsresultaterne vises i alarmen Scanning fuldført. Resultaterne omfatter antallet af scannede, registrerede og fjernede elementer og antallet af elementer i karantæne. Klik på **Vis scanningsoplysninger** for at få flere oplysninger om scanningsresultaterne eller bearbejde de inficerede elementer.

Vise scanningsresultater

Når en manuel scanning er udført, kan du få vist resultaterne for at finde ud af, hvad scanningen har fundet, og for at analysere computerens beskyttelsesstatus. Scanningsresultaterne fortæller dig, om VirusScan har registreret, repareret eller sat virus, trojanske heste, spyware, adware, cookies og andre potentielt uønskede programmer i karantæne.

- Klik på **Scan** i menuen Grundlæggende eller Avanceret, og gør derefter følgende:

For at...	Skal du...
Få vist scanningsresultater i alarmen	Vise scanningsresultater i alarmen Scanning fuldført.

Få vist flere oplysninger om scanningsresultater	Klikke på Vis scanningsoplysninger i alarmen Scanning fuldført.
Få vist en hurtig oversigt over scanningsresultaterne	Pege på ikonet Scanning fuldført i meddelelsesområdet på proceslinjen.
Få vist scannings- og registreringsstatistik	Dobbeltklikke på ikonet Scanning fuldført i meddelelsesområdet på proceslinjen.
Få vist detaljer om registrerede elementer, infektionsstatus og type.	Dobbeltklikke på ikonet Scanning fuldført i meddelelsesområdet på proceslinjen. Klik derefter på Vis resultater i ruden Status for scanning: Manuel scanning.

KAPITEL 12

Arbejde med scanningsresultater

Hvis VirusScan registrerer en sikkerhedstrussel under en realtidsscanning eller en manuel scanning, forsøger programmet at håndtere truslen automatisk i overensstemmelse med trusselstypen. Hvis VirusScan f.eks. registrerer en virus, trojansk hest eller sporingscookie på computeren, forsøger programmet at rense den inficerede fil. Hvis VirusScan ikke kan rense filen, sættes den i karantæne.

Ved nogle sikkerhedstrusler kan VirusScan evt. ikke rense en fil eller sætte den i karantæne. I det tilfælde giver VirusScan dig besked om, at du skal håndtere truslen. Du kan foretage forskellige handlinger, afhængigt af trusselstypen. Hvis VirusScan f.eks. har registreret en virus i en fil, men ikke kan rense den eller sætte den i karantæne, tillades der ikke yderligere adgang til filen. Hvis VirusScan registrerer sporingscookies, men ikke kan rense dem eller sætte dem i karantæne, kan du vælge at fjerne dem eller have tillid til dem. Hvis VirusScan registrerer potentielt uønskede programmer, foretager VirusScan ingen automatiske handlinger. I stedet får du mulighed for at vælge, om programmet skal i karantæne, eller du har tillid til det.

Når VirusScan sætter elementer i karantæne, krypteres og isoleres de i en mappe for at forhindre disse filer, programmer eller cookies i at beskadige computeren. Du kan gendanne eller fjerne elementer i karantæne. I de fleste tilfælde kan du slette en cookie i karantæne, uden at det påvirker systemet. Hvis VirusScan har sat et program, som du genkender og bruger, i karantæne, kan du overveje at gendanne det.

I dette kapitel

Arbejde med virus og trojanske heste	61
Arbejde med potentielt uønskede programmer	62
Arbejde med filer i karantæne	62
Arbejde med programmer og cookies i karantæne...	63

Arbejde med virus og trojanske heste

Hvis VirusScan registrerer en virus eller trojansk hest i en fil på computeren under en realtidsscanning eller en manuel scanning, forsøger programmet at rense filen. Hvis VirusScan ikke kan rense filen, sættes den i karantæne. Hvis det mislykkes, tillades adgang til filen ikke (kun ved realtidsscanning).

1 Åbn ruden Scanningsresultater.

Hvordan?

1. Dobbeltklik på ikonet **Scanning fuldført** i meddelelsesområdet længst til højre på proceslinjen.
2. I ruden Status for scanning: Manuel scanning skal du klikke på **Vis resultater**.

- 2 Klik på **Virus og trojanske heste** i ruden Scanningsresultater.

Bemærk! Hvis du vil arbejde med filer, som VirusScan har sat i karantæne, finder du flere oplysninger under Arbejde med filer i karantæne (side 62).

Arbejde med potentielt uønskede programmer

Hvis VirusScan registrerer et potentielt uønsket program på computeren under en realtidsscanning eller en manuel scanning, kan du fjerne eller have tillid til programmet. Fjernelse af et potentielt uønsket program sletter det ikke fra systemet. I stedet sættes det i karantæne, så det ikke kan beskadige computeren eller dine filer.

- 1 Åbn ruden Scanningsresultater.
Hvordan?
 1. Dobbeltklik på ikonet **Scanning fuldført** i meddelelsesområdet længst til højre på proceslinjen.
 2. I ruden Status for scanning: Manuel scanning skal du klikke på **Vis resultater**.
- 2 Klik på **Potentielt uønskede programmer** i ruden Scanningsresultater.
- 3 Vælg et potentielt uønsket program.
- 4 Under **Jeg ønsker at**, skal du klikke på **Fjern** eller **Hav tillid til**.
- 5 Bekræft den valgte indstilling.

Arbejde med filer i karantæne

Når VirusScan sætter inficerede filer i karantæne, krypteres og isoleres de i en mappe for at forhindre disse filer i at beskadige computeren. Du kan derefter gendanne eller fjerne filerne i karantæne.

- 1 Åbn ruden Filer i karantæne.
Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
 2. Klik på **Gendan**.
 3. Klik på **Filer**.
- 2 Vælg en fil, der er sat i karantæne.
 - 3 Nu kan du gøre følgende:
 - Hvis du vil reparere den inficerede fil og flytte den tilbage til dens oprindelige placering på computeren, skal du klikke på **Gendan**.
 - Hvis du vil fjerne den inficerede fil fra computeren, skal du klikke på **Fjern**.
 - 4 Klik på **Ja** for at bekræfte den valgte indstilling.

Tip! Du kan gendanne eller fjerne flere filer på én gang.

Arbejde med programmer og cookies i karantæne

Når VirusScan sætter potentielt uønskede programmer eller sporingscookies i karantæne, krypteres de og flyttes derefter til en beskyttet mappe for at forhindre disse programmer eller cookies i at beskadige computeren. Du kan derefter gendanne eller fjerne elementerne i karantæne. I de fleste tilfælde kan du slette et element i karantæne, uden at det påvirker systemet.

- 1 Åbn ruden Programmer og sporingscookies i karantæne.
Hvordan?
 1. Klik på menuen **Avanceret** i den venstre rude.
 2. Klik på **Gendan**.
 3. Klik på **Programmer og Cookies**.
- 2 Vælg et program eller en cookie, der er sat i karantæne.
- 3 Nu kan du gøre følgende:
 - Hvis du vil reparere den inficerede fil og flytte den tilbage til dens oprindelige placering på computeren, skal du klikke på **Gendan**.
 - Hvis du vil fjerne den inficerede fil fra computeren, skal du klikke på **Fjern**.
- 4 Klik på **Ja** for at bekræfte handlingen.

Tip! Du kan gendanne eller fjerne flere programmer og cookies på én gang.

KAPITEL 13

McAfee QuickClean

QuickClean forbedrer din computers ydeevne ved at slette filer, som kan skabe rod på din computer. Det tømmer din papirkurv og sletter midlertidige filer, genveje, mistede filfragmenter, registreringsdatabasefiler, cachelagrede filer, cookies, webstedshistorik, sendte og slettede e-mails, filer brugt for nylig, Active-X-filer og systemgendannelsespunktfiler. QuickClean beskytter desuden dit privatliv ved at bruge McAfee Shredder-komponenter til sikkert og permanent at slette elementer, der kan indeholde følsomme personlige oplysninger, som f.eks. dit navn og din adresse. Flere oplysninger om makulering af filer finder du under McAfee Shredder.

Disk Defragmenter arrangerer filer og mapper på din computer for at sikre, at de ikke bliver spredt (dvs. fragmenteret), når du gemmer på din computers harddisk. Ved at defragmentere din harddisk med jævne mellemrum sikrer du, at disse fragmenterede filer og mapper konsolideres, så de senere hurtigt kan hentes.

Hvis du ikke ønsker at vedligeholde din computer manuelt, kan du indstille både QuickClean og Disk Defragmenter til at køre automatisk som uafhængige opgaver med de mellemrum, som du vil have.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i QuickClean	66
Rense computeren	67
Defragmentering af din computer	70
Planlæg en opgave	71

Funktioner i QuickClean

QuickClean tilbyder forskellige oprydningssfunktioner, der gør det muligt at slette unødvendige filer på en sikker og effektiv måde. Ved at slette disse filer kan du øge pladsen på din computers harddisk og forbedre dens ydeevne.

Rense computeren

QuickClean sletter filer, der kan skabe rod på din computer. Det tømmer din Papirkurv og sletter midlertidige filer, genveje, mistede filfragmenter, registreringsdatabasefiler, cachelagrede filer, cookies, webstedshistorik, sendte og slettede e-mails, filer brugt for nylig, Active-X-filer og systemgendannelsespunktfiler. QuickClean sletter disse filer, uden at det påvirker andre vigtige oplysninger.

Du kan anvende alle oprydningssfunktionerne i QuickClean til at slette unødvendige filer på din computer. Følgende tabel beskriver de forskellige oprydningssfunktioner i QuickClean:

Navn	Funktion
Rensning af Papirkurv	Sletter filer i Papirkurv.
Rensning af midlertidige filer	Sletter filer, som er gemt i midlertidige mapper.
Genvejsrensning	Sletter ødelagte genveje og genveje uden et associeret program.
Rensning af tabt filfragment	Sletter tabte filfragmenter på din computer.
Rensning af registreringsdatabase	Sletter Windows®-registreringsdatabaseoplysninger for programmer, der ikke længere eksisterer på computeren. Registreringsdatabasen er en database, hvori Windows gemmer sine konfigurationsoplysninger. Registreringsdatabasen indeholder profiler for hver bruger af computeren og oplysninger om systemhardware, installerede programmer og egenskabsindstillinger. Windows anvender konstant disse informationer.
Cacherensning	Sletter de cache-filer, som akkumuleres, når du besøger på websider. Disse filer gemmes normalt som midlertidige filer i en cache-mappe. En cache-mappe er et midlertidigt opbevaringsområde på din computer. Hastigheden og effektiviteten på din internetsøgning kan øges ved, at din browser henter en webside fra sin cache-mappe (i stedet for fra en fjernserver) næste gang, du vil have den vist.

Cookie-rensning	<p>Sletter cookies. Disse filer gemmes normalt som midlertidige filer.</p> <p>En cookie er en lille fil, der indeholder oplysninger om f.eks. brugernavn og den aktuelle dato og tid, som gemmes på computer, når der søges på internettet. Cookies bruges hovedsagelig af websider til at identificere brugere, som tidligere har registreret sig på eller besøgt siden. De kan dog også fungere som en informationskilde for hackere.</p>
Rensning af browser-historik	Sletter din browsers webhistorik.
Outlook Express- og Outlook E-mail Cleaner (sendte og slettede elementer)	Sletter sendte og slettede e-mails fra Outlook® og Outlook Express.
Seneste rensning	<p>Sletter seneste filer, der er blevet oprettet med et hvilket som helst af disse programmer:</p> <ul style="list-style-type: none"> ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX Cleaner	<p>Sletter ActiveX-objekter.</p> <p>ActiveX er en softwarekomponent, der bruges af programmer eller websider til at tilføje funktionalitet, som kan indgå og fremstå som en normal del af programmet eller websiden. De fleste ActiveX-objekter er harmløse, men der er dog nogle, som kan opsnappe oplysninger fra din computer.</p>
Rensning af systemgendannelsespunkt	<p>Sletter gamle systemgendannelsespunkter (på nær de seneste) fra computeren.</p> <p>Systemgendannelsespunkter oprettes ved hjælp af Windows for at markere eventuelle ændringer, der er foretaget på din computer, så du kan gå tilbage til en tidligere indstilling, hvis der opstår problemer.</p>

Rensning af din computer

Du kan anvende alle oprydningsskærmen i QuickClean til at slette unødvendige filer på din computer. Når oprydningen er afsluttet, kan du under **Oversigt over QuickClean** se den mængde diskplads, der blev frigjort, antallet af filer som blev slettet og den dato og det tidspunkt, QuickClean sidst blev brugt på din computer.

- 1 I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
- 2 Klik på **Start** under **McAfee QuickClean**.
- 3 Nu kan du gøre følgende:
 - Klik på **Næste** for at acceptere standardrensningstyperne på listen.
 - Vælg eller fravælg de relevante rensninger, og klik derefter på **Næste**. Hvis du vælger Seneste rensning, kan du klikke på **Egenskaber** for at vælge eller rense de filer, der senest er blevet oprettet med et af programmerne på listen. Klik derefter på **OK**.
 - Klik på **Gendan standarder** for at gendanne standardrensningstyperne, og klik derefter på **Næste**.
- 4 Når analysen er udført, skal du klikke på **Næste**.
- 5 Klik på **Næste** for at bekræfte sletningen af filen.
- 6 Nu kan du gøre følgende:
 - Klik på **Næste** for at acceptere standardindstillingen **Nej, jeg vil slette filer med standard Windows-sletning**.
 - Klik på **Ja, jeg vil slette mine filer sikkert med Shredder**, angiv antallet af sletningsgennemløb (op til 10) og klik derefter på **Næste**. Makuleringen af filer kan tage lang tid, hvis det er en stor mængde oplysninger, der skal slettes.
- 7 I tilfælde af at visse filer eller elementer var låst under rensningen, kan du blive bedt om at genstarte din computer. Klik på **OK** for at lukke dialogboksen.
- 8 Klik på **Udfør**.

Bemærk! Filer, der slettes med Shredder, kan ikke gendannes. Yderligere oplysninger om makulering af filer finder du under McAfee Shredder.

Defragmentering af din computer

Disk Defragmenter arrangerer filer og mapper på din computer, så de ikke bliver spredt (dvs. fragmenteret), når du gemmer på din computers harddisk. Ved at defragmentere din harddisk med jævne mellemrum sikrer du, at disse fragmenterede filer og mapper konsolideres, så de senere hurtigt kan hentes.

Defragmentering af din computer

Du kan defragmentere din computer, hvis du vil forbedre din adgang til og søgning efter filer og mapper.

- 1 I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
- 2 Klik på **Analyser** under **Diskdefragmentering**.
- 3 Følg vejledningen på skærmen.

Bemærk! Yderligere oplysninger om Disk Defragmenter finder du under Hjælp i Windows.

Planlæg en opgave

Task Scheduler automatiserer den frekvens, som QuickClean eller Disk Defragmenter skal køre med på din computer. Du kan eksempelvis planlægge, at QuickClean skal tømme din papirkurv søndag kl. 21.00, eller at Disk Defragmenter skal defragmentere din computers harddisk sidste dag i hver måned. Du kan til enhver tid oprette, ændre eller stoppe en opgave. Du skal være logget på din computer, for at en planlagt opgave kan udføres. Hvis opgaven ikke udføres af en eller anden grund, vil den blive planlagt igen fem minutter efter, at du logger ind næste gang.

Planlæg en opgave i QuickClean

Du kan planlægge en opgave i QuickClean, så programmet automatisk renser din computer ved hjælp af en eller flere oprydningsskemaer. Når rensningen er udført, kan du under **Oversigt over QuickClean** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

- 1 Åbn ruden Task Scheduler.
 - Hvordan?
 1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
 2. Klik på **Start** under **Opgavestyring**.
- 2 Klik på **McAfee QuickClean** på listen **Vælg opgave, der skal planlægges**.
- 3 Angiv et navn på din opgave i boksen **Opgavenavn**, og klik derefter på **Opret**.
- 4 Nu kan du gøre følgende:
 - Klik på **Næste** for at acceptere oprydningsskemaerne på listen.
 - Vælg eller fravælg de relevante oprydningsskemaer, og klik derefter på **Næste**. Hvis du vælger Seneste rensning, kan du klikke på **Egenskaber** for at vælge eller rense de filer, der senest er blevet oprettet med et af programmerne på listen. Klik derefter på **OK**.
 - Klik på **Gendan standarder** for at gendanne standardrensningsstyperne, og klik derefter på **Næste**.
- 5 Nu kan du gøre følgende:
 - Klik på **Planlæg** for at acceptere standardindstillingen **Nej, jeg vil slette filer med standard Windows-sletning**.

- Klik på **Ja, jeg vil slette mine filer sikkert med Shredder**, angiv antallet af sletningsgennemløb (op til 10) og klik derefter på **Planlæg**.
- 6 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.
 - 7 Hvis du foretog ændringer i egenskaberne for Seneste rensning, kan du blive bedt om at genstarte computeren. Klik på **OK** for at lukke dialogboksen.
 - 8 Klik på **Udfør**.

Bemærk! Filer, der slettes med Shredder, kan ikke gendannes. Yderligere oplysninger om makulering af filer finder du under McAfee Shredder.

Lav ændringer i en opgave i QuickClean

Du kan ændre en planlagt opgave i QuickClean, så oprydningsskemaet ændres, eller frekvensen, som programmet er indstillet til på din computer, laves om. Når rensningen er udført, kan du under **Oversigt over QuickClean** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

- 1 Åbn ruden Task Scheduler.
Hvordan?
 1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
 2. Klik på **Start** under **Opgavestyling**.
- 2 Klik på **McAfee QuickClean** på listen **Vælg opgave, der skal planlægges**.
- 3 Marker opgaven på listen **Vælg en eksisterende opgave**, og klik derefter på **Rediger**.
- 4 Nu kan du gøre følgende:
 - Klik på **Næste** for at acceptere rensningstyperne for opgaven.
 - Vælg eller fravælg de relevante oprydningsskemaer, og klik derefter på **Næste**. Hvis du vælger Seneste rensning, kan du klikke på **Egenskaber** for at vælge eller rense de filer, der senest er blevet oprettet med et af programmerne på listen. Klik derefter på **OK**.
 - Klik på **Gendan standarder** for at gendanne standardrensningstyperne, og klik derefter på **Næste**.
- 5 Nu kan du gøre følgende:
 - Klik på **Planlæg** for at acceptere standardindstillingen **Nej, jeg vil slette filer med standard Windows-sletning**.

- Klik på **Ja, jeg vil slette mine filer sikkert med Shredder**, angiv antallet af sletningsgennemløb (op til 10) og klik derefter på **Planlæg**.
- 6 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.
 - 7 Hvis du foretog ændringer i egenskaberne for Seneste rensning, kan du blive bedt om at genstarte computeren. Klik på **OK** for at lukke dialogboksen.
 - 8 Klik på **Udfør**.

Bemærk! Filer, der slettes med Shredder, kan ikke gendannes. Yderligere oplysninger om makulering af filer finder du under McAfee Shredder.

Slet en opgave i QuickClean

Du kan slette en planlagt opgave i QuickClean, hvis du ikke længere ønsker, at den skal køre automatisk.

- 1 Åbn ruden Task Scheduler.
Hvordan?
 1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
 2. Klik på **Start** under **Opgavestyring**.
- 2 Klik på **McAfee QuickClean** på listen **Vælg opgave, der skal planlægges**.
- 3 Marker opgaven på listen **Vælg en eksisterende opgave**.
- 4 Klik på **Slet**, og klik derefter på **Ja** for at bekræfte sletningen.
- 5 Klik på **Udfør**.

Planlæg en opgave i Disk Defragmenter

Du kan planlægge en opgave i Disk Defragmenter for at indstille frekvensen, som din computer automatisk defragmenterer harddisken med. Når rensningen er udført, kan du under **Disk Defragmenter** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

- 1 Åbn ruden Task Scheduler.
Hvordan?

1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
2. Klik på **Start** under **Opgavestyring**.
- 2 Klik på **Disk Defragmenter** på listen **Vælg opgave, der skal planlægges**.
- 3 Angiv et navn på din opgave i boksen **Opgavenavn**, og klik derefter på **Opret**.
- 4 Nu kan du gøre følgende:
 - Klik på **Planlæg** for at acceptere standardindstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**.
 - Fravælg indstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**, og klik derefter **Planlæg**.
- 5 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.
- 6 Klik på **Udfør**.

Lav ændring i en opgave i Disk Defragmenter

Du kan ændre en planlagt opgave i Disk Defragmenter, så frekvensen, som programmet er indstillet til at køre med på din computer, laves om. Når rensningen er udført, kan du under **Disk Defragmenter** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

- 1 Åbn ruden Task Scheduler.

Hvordan?

 1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
 2. Klik på **Start** under **Opgavestyring**.
- 2 Klik på **Disk Defragmenter** på listen **Vælg opgave, der skal planlægges**.
- 3 Marker opgaven på listen **Vælg en eksisterende opgave**, og klik derefter på **Rediger**.
- 4 Nu kan du gøre følgende:
 - Klik på **Planlæg** for at acceptere standardindstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**.
 - Fravælg indstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**, og klik derefter **Planlæg**.
- 5 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.
- 6 Klik på **Udfør**.

Slet en opgave i Disk Defragmenter

Du kan slette en planlagt opgave i Disk Defragmenter, hvis du ikke længere ønsker, at den skal køre automatisk.

1 Åbn ruden Task Scheduler.

Hvordan?

1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
2. Klik på **Start** under **Opgavestyring**.

2 Klik på **Disk Defragmenter** på listen **Vælg opgave, der skal planlægges**.

3 Marker opgaven på listen **Vælg en eksisterende opgave**.

4 Klik på **Slet**, og klik derefter på **Ja** for at bekræfte sletningen.

5 Klik på **Udfør**.

KAPITEL 14

McAfee Shredder

McAfee Shredder sletter (eller makulerer) filer permanent fra din computers harddisk. Selv når du sletter filer og mapper manuelt, tømmer din Papirkurv eller sletter mappen Midlertidige internetfiler, kan du stadig genfinde disse data ved hjælp af computerens sporingsværktøjer. Ligeledes kan slettede filer genfindes, idet nogle programmer laver midlertidige, gemte kopier af åbnede filer. Shredder beskytter dine private oplysninger ved at slette disse uønskede filer permanent og sikkert. Det er vigtigt at huske, at makulerede filer ikke kan gendannes.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Shredder.....	78
Makulerer filer og indholdet af mapper og diske.....	79

Funktioner i Shredder

Shredder sletter filer fra din computers harddisk, så deres tilknyttede oplysninger ikke kan genfindes. Det beskytter dit privatliv ved sikkert og permanent at slette filer og mapper, elementer i din Papirkurv og mappen Midlertidige internetfiler og hele indholdet på computerdiske, som f.eks. genskrivbare cd'er, eksterne harddiske og disketter.

Makulerer filer og indholdet af mapper og diske.

Shredder sørger for at de data, der findes i slettede filer og mapper i din Papirkurv og i mappen Midlertidige internetfiler, ikke kan genfindes selv med specialværktøjer. Med Shredder kan du angive, hvor mange gange (op til 10) du ønsker, at et element skal makuleres. Et højere antal makuleringsgennemløb øger sikkerhedsniveauet for sletningen af filen.

Makuler filer og mapper

Du kan makulere filer og mapper på din computers harddisk inklusive elementer i din Papirkurv og i mappen Midlertidige internetfiler.

1 Åbn **Shredder**.

Hvordan?

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på menuen **Avanceret**.
2. Klik på **Værktøjer** i den venstre rude.
3. Klik på **Shredder**.

2 I ruden Makuler filer og mapper under **Jeg vil** skal du klikke på **Slet filer og mapper**.

3 Under **Makuleringsniveau** skal du klikke på et af følgende niveauer:

- **Hurtig**: Makulerer det markerede element(er) en gang.
- **Omfattende**: Makulerer det markerede element(er) 7 gange.
- **Brugerdefineret**: Makulerer det markerede element(er) op til 10 gange.

4 Klik på **Næste**.

5 Nu kan du gøre følgende:

- På listen **Marker de filer, der skal makuleres** skal du klikke enten på **Indhold i Papirkurv** eller **Midlertidige internetfiler**.
- Klik på **Gennemse**, og find den fil, du ønsker at makulere. Vælg derefter **Åbn**.

- 6 Klik på **Næste**.
- 7 Klik på **Start**.
- 8 Når Shredder er færdig, skal du klikke på **Udført**.

Bemærk! Du bør ikke arbejde med nogen filer, før Shredder har fuldført denne opgave.

Makulere en hel disk

Du kan makulere alt indholdet på en disk på en gang. Det er kun flytbare diske som f.eks. eksterne harddiske, skrivbare cd'er og disketter, der kan makuleres.

- 1 Åbn **Shredder**.
Hvordan?
 1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på menuen **Avanceret**.
 2. Klik på **Værktøjer** i den venstre rude.
 3. Klik på **Shredder**.
- 2 I ruden Makuler filer og mapper under **Jeg vil** skal du klikke på **Slet en hel disk**.
- 3 Under **Makuleringsniveau** skal du klikke på et af følgende niveauer:
 - **Hurtig**: Makulerer den markerede disk en gang.
 - **Omfattende**: Makulerer den markerede disk 7 gange.
 - **Brugerdefineret**: Makulerer den markerede disk op til 10 gange.
- 4 Klik på **Næste**.
- 5 På listen **Vælg disken** skal du klikke på det drev, du vil makulere.
- 6 Klik på **Næste**, og klik derefter på **Ja** for at bekræfte.
- 7 Klik på **Start**.
- 8 Når Shredder er færdig, skal du klikke på **Udført**.

Bemærk! Du bør ikke arbejde med nogen filer, før Shredder har fuldført denne opgave.

KAPITEL 15

McAfee Network Manager

Network Manager giver en grafisk oversigt over computere og komponenter i hjemmenetværket. Du kan bruge Network Manager til at fjernovervåge beskyttelsesstatussen for hver af de administrerede computere i netværket og fjernreparere rapporterede sikkerhedsproblemer på disse computere.

Før du bruger Network Manager, kan du sætte dig ind i nogle af funktionerne. Der findes detaljerede oplysninger om konfiguration og brug af disse funktioner i hjælpen til Network Manager.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Network Manager	82
Forklaring af ikoner i Network Manager	83
Konfigurere et administreret netværk	85
Administrere netværket eksternt	93

Funktioner i Network Manager

Network Manager indeholder følgende funktioner:

Grafisk netværkskort














Network Managers netværkskort giver dig en grafisk oversigt over sikkerhedsstatus for de computere og komponenter, der udgør dit hjemmenetværk. Når du foretager ændringer i netværket (f.eks. tilføjer en computer), registrerer netværkskortet disse ændringer. Du kan opdatere netværkskortet, omdøbe netværket og vise eller skjule komponenter i netværkskortet for at tilpasse visningen. Du kan også få vist oplysninger vedrørende en af de komponenter, der vises på netværkskortet.

Fjernstyring

Brug Network Managers netværkskort til at styre sikkerhedsstatus for de computere, der udgør dit hjemmenetværk. Du kan invitere en computer til at tilslutte til det administrerede netværk, overvåge en administreret computers beskyttelsesstatus og udbedre kendte sikkerhedsproblemer fra en fjerncomputer i netværket.

Forklaring af ikoner i Network Manager

Følgende tabel beskriver de almindeligt brugte ikoner på netværkskortet i Network Manager.

Ikon	Beskrivelse
	Repræsenterer en administreret computer, der er online
	Repræsenterer en administreret computer, der er offline
	Repræsenterer en ikke-administreret computer, som har SecurityCenter installeret
	Repræsenterer en ikke-administreret computer, der er offline
	Repræsenterer en computer, der er online, og som ikke har SecurityCenter installeret, eller en ukendt netværksenhed
	Repræsenterer en computer, der er offline, og som ikke har SecurityCenter installeret, eller en ukendt netværksenhed
	Angiver, at det tilsvarende element er beskyttet og tilsluttet
	Angiver, at det tilsvarende element evt. kræver din opmærksomhed
	Angiver, at det tilsvarende element kræver din opmærksomhed omgående
	Repræsenterer en trådløs hjemmerouter
	Repræsenterer en standardhjemmerouter
	Repræsenterer internettet, når der er oprettet forbindelse
	Repræsenterer internettet, når forbindelsen er afbrudt

KAPITEL 16

Konfigurere et administreret netværk

Du kan konfigurere et administreret netværk ved at arbejde med elementerne på netværkshortet og føje medlemmer (computere) til netværket. Hvis en computer skal kunne fjernadministreres eller selv skal fjernadministrere andre computere på netværket, skal den være et netværksmedlem, der er tillid til. Nye computere gøres til medlemmer af netværket af eksisterende netværksmedlemmer (computere), der har administratorrettigheder.

Du kan få vist oplysninger vedrørende en af de komponenter, der vises på netværkshortet, også efter at du har foretaget ændringer i netværket (f.eks. tilføjet en computer).

I dette kapitel

Arbejde med netværkshortet	86
Tilslutte computeren til det administrerede netværk	88

Arbejde med netværkskortet

Når du forbinder en computer til netværket, analyserer Network Manager netværkets status for at afgøre, om der er administrerede eller ikke-administrerede medlemmer, routerens attributter og internetstatussen. Hvis der ikke findes nogen medlemmer, vil Network Manager gå ud fra, at den computer, der er tilsluttet i øjeblikket, er den første computer i netværket, og gør computeren til et administreret medlem med administratorrettigheder. Navnet på netværket indeholder som standard navnet på arbejdsgruppen eller domænet for den første computer med SecurityCenter installeret, der slutes til netværket. Netværket kan dog til enhver tid omdøbes.

Når du foretager ændringer i netværket (f.eks. tilføjer en computer), kan du brugertilpasse netværkskortet. Du kan f.eks. opdatere netværkskortet, omdøbe netværket og tilpasse visningen ved at vise eller skjule komponenter på netværkskortet. Du kan også få vist oplysninger vedrørende en af de komponenter, der vises på netværkskortet.

Åbne netværkskortet

Netværkskortet giver en grafisk gengivelse af computere og komponenter på dit hjemmenetværk.

- Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.

Bemærk! Første gang, du anvender netværkskortet, bliver du bedt om at have tillid til de øvrige computere i netværket.

Opdatere netværkskortet

Du kan til enhver tid opdatere netværkskortet, f.eks. når der er blevet sluttet en ny computer til netværket.

- 1 Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.
- 2 Klik på **Opdater netværkskortet** under **Jeg ønsker at**.

Bemærk! Linket **Opdater netværkskortet** er kun tilgængeligt, når ingen af elementerne på netværkskortet er markeret. Hvis du vil fjerne markeringen fra et element, skal du klikke på det markerede element eller på et hvidt område på netværkskortet.

Omdøbe netværket

Navnet på netværket indeholder som standard navnet på arbejdsgruppen eller domænet for den første computer med SecurityCenter installeret, der slutes til netværket. Hvis du foretrækker et andet navn, kan du ændre det.

- 1 Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.
- 2 Klik på **Omdøb netværket** under **Jeg ønsker at**.
- 3 Skriv navnet på netværket i feltet **Netværksnavn**.
- 4 Klik på **OK**.

Bemærk! Linket **Opdater netværkskortet** er kun tilgængeligt, når ingen af elementerne på netværkskortet er markeret. Hvis du vil fjerne markeringen fra et element, skal du klikke på det markerede element eller på et hvidt område på netværkskortet.

Vise eller skjule elementer på netværkskortet

Som standard vises alle hjemmenetværkets computere og komponenter på netværkskortet. Hvis der er skjulte elementer, kan du til enhver tid få dem vist igen. Kun ikke-administrerede elementer kan skjules. Administrerede computere kan ikke skjules.

For at...	Klik på Netværksadministration i menuen Grundlæggende eller Avanceret, og gør derefter følgende...
Skjule et element på netværkskortet	Klik på et element på netværkskortet, og klik derefter på Skjul dette element under Jeg ønsker at . Klik på Ja i dialogboksen til bekræftelse.
Vise skjulte elementer på netværkskortet	Klik på Vis skjulte elementer under Jeg ønsker at .

Få vist yderligere oplysninger om et element

Du kan få vist detaljerede oplysninger om hver enkelt komponent i netværket ved at markere komponenten på netværkskortet. Blandt de viste oplysninger er komponentens navn og beskyttelsesstatus samt andre oplysninger, der skal bruges for at kunne administrere komponenten.

- 1 Klik på ikonet for et element på netværkskortet.
- 2 Se oplysningerne om elementet under **Detaljer**.

Tilslutte computeren til det administrerede netværk

Hvis en computer skal kunne fjernadministreres eller selv skal fjernadministrere andre computere på netværket, skal den være et netværksmedlem, der er tillid til. Nye computere gøres til medlemmer af netværket af eksisterende netværksmedlemmer (computere), der har administratorrettigheder. For at sikre at kun computere, der er tillid til, deltager i netværket, skal brugerne på den adgangsgivende og den tilknyttende computer godkende hinanden.

Når en computer tilknyttes netværket, bliver den bedt om at vise sin beskyttelsesstatus i McAfee til de andre computere på netværket. Hvis en computer accepterer at vise sin beskyttelsesstatus, bliver den administreret medlem af netværket. Hvis en computer afviser at vise sin beskyttelsesstatus, bliver den ikke-administreret medlem af netværket. Ikke-administrerede medlemmer af netværket er sædvanligvis gæstecomputere, der ønsker adgang til andre netværksfunktioner (f.eks. fil- eller printerdeling).

Bemærk! Hvis computeren har andre McAfee-netværksprogrammer installeret (f.eks. EasyNetwork), vil computeren også blive anerkendt som administreret computer af disse programmer, når den er blevet medlem af netværket. Det tilladelsesniveau, som computeren tildeles i Network Manager, anvendes i alle McAfee-netværksprogrammer. Yderligere oplysninger om, hvad rettighedsniveauerne gæst, fuld og administrator betyder for andre McAfee-netværksprogrammer, finder du i den medfølgende dokumentation for det enkelte program.

Tilslutte computeren til et administreret netværk

Når du modtager en invitation til at slutte dig til et administreret netværk, kan du enten acceptere eller afvise den. Du kan også bestemme, om denne computer og andre computere på netværket skal kunne overvåge hinandens sikkerhedsindstillinger (f.eks. om en computers virusbeskyttelsestjeneste er opdateret).

- 1 Kontroller, at afkrydsningsfeltet **Tillad alle computere på dette netværk at overvåge sikkerhedsindstillingerne** er markeret i dialogboksen Administreret netværk.
- 2 Klik på **Deltag**.
Når du accepterer invitationen, vises to spillekort.
- 3 Bekræft, at spillekortene er de samme som dem, der vises på den computer, der har inviteret dig til at deltage i det administrerede netværk.
- 4 Klik på **OK**.

Bemærk! Hvis den computer, der inviterede dig til at deltage i det administrerede netværk, ikke viser de samme spillekort som i dialogboksen til bekræftelse af sikkerheden, er der sket et sikkerhedsbrud på det administrerede netværk. I sådanne tilfælde kan det være risikabelt at tilslutte computeren til netværket. Derfor skal du klikke på **Annuller** i dialogboksen til bekræftelse af sikkerheden.

Invitere en computer til at deltage i det administrerede netværk

Hvis en computer føjes til det administrerede netværk, eller hvis der findes en anden, ikke-administreret computer på netværket, kan du invitere denne computer til at deltage i det administrerede netværk. En computer kan kun invitere andre computere til at deltage i netværket, hvis den har administratorrettigheder på netværket. Når du sender invitationen, skal du også angive tilladelsesniveauet for den computer, der skal tilsluttes.

- 1 Klik på ikonet for en ikke-administreret computer på netværksskottet.
- 2 Klik på **Overvåg denne computer** under **Jeg ønsker at**.
- 3 I dialogboksen Inviter en computer til at deltage i dette administrerede netværk skal du gøre et af følgende:
 - Klik på **Giv gæsteadgang til administrerede netværksprogrammer** for at give computeren adgang til netværket (du kan bruge denne indstilling for midlertidige brugere i dit hjem).
 - Klik på **Giv fuld adgang til administrerede netværksprogrammer** for at give computeren adgang til netværket.

- Klik på **Giv administratoradgang til administrerede netværksprogrammer** for at give computeren adgang til netværket med administratorrettigheder. Det giver også computeren adgang til at tildele adgangstilladelser til andre computere, der ønsker at deltage i det administrerede netværk.
- 4 Klik på **OK**.
Der sendes en invitation til at deltage i det administrerede netværk til computeren. Når computeren accepterer invitationen, vises to spillekort.
 - 5 Bekræft, at spillekortene er de samme som dem, der vises på den computer, du har inviteret til at deltage i det administrerede netværk.
 - 6 Klik på **Tildel adgang**.

Bemærk! Hvis den computer, du har inviteret til at deltage i det administrerede netværk, ikke viser de samme spillekort som i dialogboksen til bekræftelse af sikkerheden, er der sket et sikkerhedsbrud på det administrerede netværk. Hvis computeren gives adgang til at deltage i netværket, kan de andre computere muligvis udsættes for risiko, og du skal derfor klikke på **Afvis adgang** i dialogboksen til bekræftelse af sikkerheden.

Stoppe med at stole på andre computere på netværket

Hvis du ved en fejl har haft tillid til andre computere på netværket, kan du annullere dette.

- Klik på **Stop med at stole på andre computere på dette netværk** under **Jeg ønsker at**.

Bemærk! Linket **Stop med at stole på andre computere på dette netværk** er ikke tilgængeligt, hvis du har administratorrettigheder, og der er andre administrerede computere på netværket.

KAPITEL 17

Administrere netværket eksternt

Når du konfigurerer det administrerede netværk, kan du administrere netværkets computere og komponenter eksternt. Du kan overvåge computerens status og tilladelsesniveauer og afhjælpe de fleste sikkerhedssårbarheder eksternt.

I dette kapitel

Overvåge status og tilladelser	94
Afhjælpe sikkerhedssårbarheder	96

Overvåge status og tilladelser

I et administreret netværk findes der administrerede og ikke-administrerede medlemmer. Administrerede medlemmer tildeler andre computere adgang til netværket for at overvåge deres beskyttelsesstatus i McAfee – det gør andre medlemmer ikke. Ikke-administrerede medlemmer er sædvanligvis gæstecomputere, der ønsker adgang til andre netværksfunktioner (f.eks. fil- eller printerdeling). En ikke-administreret computer kan til enhver tid inviteres til at blive administreret computer af en anden administreret computer på netværket. En administreret computer kan også til enhver tid gøres ikke-administreret.

Administrerede computere er enten tildelt tilladelsesniveauet administrator, fuld eller gæst. En administreret computer med administratorrettigheder kan administrere beskyttelsesstatusen for alle andre administrerede computere på netværket og kan tildele andre computere medlemskab af netværket. En computer med tilladelsesniveauet fuld eller gæst har kun adgang til netværket. Du kan til enhver tid redigere en computers tilladelsesniveau.

Da et administreret netværk også består af enheder (f.eks. routere), kan Network Manager også bruges til at administrere disse. Du kan også konfigurere og redigere displayegenskaber for en enhed på netværkskortet.

Overvåge en computers beskyttelsesstatus

Hvis en computers beskyttelsesstatus ikke overvåges på netværket (computeren ikke er medlem af netværket, eller computeren er ikke-administreret medlem), kan du anmode om at overvåge den.

- 1 Klik på ikonet for en ikke-administreret computer på netværkskortet.
- 2 Klik på **Overvåg denne computer** under **Jeg ønsker at**.

Indstille overvågning af en computers beskyttelsesstatus

Du kan standse overvågningen af beskyttelsesstatusen for en administreret computer på netværket. Computeren bliver så ikke-administreret, og du kan ikke fjernovervåge dens beskyttelsesstatus.

- 1 Klik på ikonet for en administreret computer på netværkskortet.
- 2 Klik på **Indstil overvågning af denne computer** under **Jeg ønsker at**.
- 3 Klik på **Ja** i dialogboksen til bekræftelse.

Redigere tilladelser for en administreret computer

Du kan til enhver tid redigere tilladelser for en administreret computer. Dette giver dig mulighed for at justere, hvilke computere der kan overvåge beskyttelsesstatussen (sikkerhedsindstillingerne) for andre computere på netværket.

- 1 Klik på ikonet for en administreret computer på netværkskortet.
- 2 Klik på **Rediger tilladelser for denne computer** under **Jeg ønsker at**.
- 3 Marker afkrydsningsfeltet i dialogboksen Rediger tilladelser for at bestemme, om denne computer eller andre computere på det administrerede netværk kan overvåge hinandens beskyttelsesstatus.
- 4 Klik på **OK**.

Administrere en enhed

Du kan administrere en enhed ved at åbne dens administrationswebside fra Network Manager.

- 1 Klik på ikonet for en enhed på netværkskortet.
- 2 Klik på **Administrer denne enhed** under **Jeg ønsker at**. Der åbnes en webbrowser, der viser enhedens administrationswebside.
- 3 Angiv dine loginoplysninger i webbrowseren og konfigurer enhedens sikkerhedsindstillinger.

Bemærk! Hvis enheden er en trådløs router eller et trådløst adgangspunkt, der er beskyttet med Wireless Network Security, skal du bruge Wireless Network Security til at konfigurere enhedens sikkerhedsindstillinger.

Redigere en enheds displayegenskaber

Når du redigerer en enheds displayegenskaber, kan du ændre enhedens viste navn på netværkskortet og angive, om enheden er en trådløs router.

- 1 Klik på ikonet for en enhed på netværkskortet.
- 2 Klik på **Rediger enhedsegenskaber** under **Jeg ønsker at**.
- 3 Hvis du vil angive enhedens viste navn, skal du angive et navn i feltet **Navn**.
- 4 Hvis du vil angive enhedstypen, skal du klikke på **Standardrouter**, hvis det ikke er en trådløs router, eller **Trådløs router**, hvis den er trådløs.
- 5 Klik på **OK**.

Afhjælp sikkerhedssårbarheder

Administrerede computere med administratorrettigheder kan overvåge statussen for McAfee-beskyttelsen på andre administrerede computere på netværket og afhjælpe eventuelle rapporterede sikkerhedssårbarheder eksternt. Hvis f.eks. en administreret computers status for McAfee-beskyttelse viser, at VirusScan er deaktiveret, kan en anden administreret computer med administratorrettigheder fjernaktivere VirusScan.

Når du fjernafhjælper sikkerhedssårbarheder, reparerer Network Manager automatisk de fleste rapporterede problemer. Visse sikkerhedssårbarheder kan dog kræve manuel indgriben på den lokale computer. I dette tilfælde afhjælper Network Manager de problemer, der kan repareres eksternt, og viser en besked, der beder dig afhjælpe de resterende problemer ved at logge på SecurityCenter på den berørte computer og følge den angivne vejledning. I nogle tilfælde foreslås det at afhjælpe problemet ved at installere SecurityCenter på en eller flere fjerncomputere på netværket.

Afhjælp sikkerhedssårbarheder

Du kan bruge Network Manager til automatisk at afhjælpe de fleste sikkerhedssårbarheder på administrerede fjerncomputere. Hvis f.eks. VirusScan er deaktiveret på en fjerncomputer, kan du aktivere programmet.

- 1 Klik på ikonet for et element på netværkskortet.
- 2 Få vist elementets beskyttelsesstatus under **Detaljer**.
- 3 Klik på **Afhjælp sikkerhedssårbarheder** under **Jeg ønsker at**.
- 4 Klik **OK**, når sikkerhedsproblemet er afhjulpet.

Bemærk! Selvom Network Manager kan afhjælpe de fleste sikkerhedssårbarheder automatisk, vil nogle reparationer muligvis kræve, at du starter SecurityCenter på den berørte computer og følger den angivne vejledning.

Installere McAfee sikkerhedssoftware på fjerncomputere

Hvis en eller flere computere på netværket ikke har den seneste version af SecurityCenter installeret, kan deres sikkerhedsstatus ikke fjernovervåges. Hvis du vil fjernovervåge disse computere, skal du installere den seneste version af SecurityCenter lokalt på hver enkelt computer.

- 1 Åbn SecurityCenter på den computer, som du ønsker at installere sikkerhedssoftwaren på.
- 2 Klik på **Min konto** under **Almindelige opgaver**.
- 3 Log på med den e-mail-adresse og adgangskode, du brugte til at registrere din sikkerhedssoftware, første gang du installerede den.
- 4 Vælg det relevante produkt, klik på ikonet **Download/Install**, og følg anvisningerne på skærmen.

Reference

Ordlisten viser og definerer de mest almindeligt anvendte sikkerhedstermer, der findes i McAfees produkter.

Ordliste

8

802.11

Et sæt af IEEE-standarder for overførsel af data via et trådløst netværk 802.11 kaldes ofte Wi-Fi.

802.11a

En udvidelse af 802.11, der overfører data med op til 54 Mbps over 5 GHz-båndet. Selvom overførselshastigheden er hurtigere end 802.11b, er den afstand, der dækkes, meget mindre.

802.11b

En udvidelse af 802.11, der overfører data med op til 11 Mbps over 2,4 GHz-båndet. Selvom overførselshastigheden er langsommere end 802.11a, er den afstand, der dækkes, større.

802.1x

En IEEE-standard for godkendelse på faste og trådløse netværk. 802.1x bruges ofte med 802.11 trådløst netværk.

A

ActiveX-objekt

En softwarekomponent, der bruges af programmer eller websider til at tilføje funktionalitet, der fremstår som en normal del af programmet eller websiden. De fleste ActiveX-objekter er harmløse, men der er dog nogle, som kan opsnappe oplysninger fra din computer.

adgangskode

En kode (der normalt består af bogstaver og tal), som du bruger til at få adgang til computeren, et program eller et websted.

Adgangskodeboks

Et sikkert lagringsområde til dine personlige adgangskoder. Den giver dig mulighed for at opbevare dine adgangskoder med tillid til, at ingen andre brugere kan få adgang til dem (heller ikke en administrator).

adgangspunkt

En netværksenhed (ofte kaldet en trådløs router), der tilsluttes en Ethernet-hub eller -switch for at udvide den fysiske tjenesteradius for en trådløs bruger. Når trådløse brugere roamer med deres mobile enheder, skifter overførslen fra et adgangspunkt (AP) til et andet for at opretholde forbindelsen.

administreret netværk

Et hjemmenetværk med to typer medlemmer: administrerede medlemmer og ikke-administrerede medlemmer. Administrerede medlemmer tildeler andre computere adgang til netværket for at overvåge deres beskyttelsesstatus i McAfee. Det gør ikke-administrerede medlemmer ikke.

almindelig tekst

Tekst, som ikke er krypteret. Se også kryptering.

arkivere

At oprette en kopi af vigtige filer på cd, dvd, USB-drev, ekstern harddisk eller netværksdrev.

B

bibliotek

Et onlinelager til filer, du har sikkerhedskopieret og udgivet. Databiblioteket er et websted på internettet, som er tilgængeligt for alle med internetadgang.

billedfiltrering

En indstilling under Forældrestyring, som blokerer potentielt upassende webbilleder.

browser

Et program, der bruges til at få vist websider på internettet. Populære webbrowsere omfatter Microsoft Internet Explorer og Mozilla Firefox.

bufferoverløb

En betingelse, der opstår, når mistænkelige programmer eller processer forsøger at gemme flere data i en buffer (opbevaringsområde for midlertidige data) på din computer, end den kan klare. Bufferoverløb kan beskadige eller overskrive data i nærliggende buffere.

båndbredde

Mængden af data, som kan transmitteres inden for et fastlagt tidsrum.

C

cache

Et midlertidigt opbevaringsområde på computeren. For at øge hastigheden og effektiviteten på din internetsøgning kan din browser f.eks. hente en webside fra sin cache-mappe (i stedet for fra en fjernserver) næste gang, du vil have den vist.

cookie

En lille fil, der indeholder oplysninger om f.eks. brugernavn og den aktuelle dato og tid, som gemmes på computer, når der søges på internettet. Cookies bruges hovedsagelig af websider til at identificere brugere, som tidligere har registreret sig på eller besøgt siden. De kan dog også fungere som en informationskilde for hackere.

D

DAT

(DatSignaturfiler) Filer, der indeholder de definitioner, der bruges til at registrere virus, trojanske heste, spyware, adware og andre potentielt uønskede programmer på computeren eller et USB-drev.

dele

At give e-mail-modtagere adgang til udvalgte sikkerhedskopierede filer i et begrænset stykke tid. Når du deler en fil, sender du sikkerhedskopien af filen til de e-mail-modtagere, som du angiver. Modtagerne får en e-mail fra Data Backup, som viser, at filer deles med dem. Denne e-mail indeholder også et link til de delte filer.

delt hemmelighed (shared secret)

En streng eller nøgle (normalt en adgangskode), som to parter, der kommunikerer med hinanden, har udvekslet, inden kommunikationen blev initieret. En delt hemmelighed bruges til at beskytte følsomme dele af RADIUS-meddelelser.

DNS

(Domain Name System) Et system, der konverterer værtsnavne eller domænenavne til IP-adresser. På internettet bruges DNS til at konvertere letlæselige webadresser (f.eks. www.minvaert.dk) til IP-adresser (f.eks. 111.2.3.44), så webstedet kan hentes. Uden DNS skal du indtaste selve IP-adressen i webbrowseren.

DNS-server

(Domain Name System-server) En computer, der returnerer den IP-adresse, der er knyttet til et værts- eller domænenavn. Se også DNS.

domæne

Et lokalt undernetværk eller en "descriptor" for websteder på internettet.

På et lokalt netværk (LAN) er et domæne et undernetværk bestående af klient- og servercomputere, der kontrolleres af én sikkerhedsdatabase. I den forbindelse kan domæner forbedre effektiviteten. På internettet er et domæne en del af hver webadresse (i www.abc.com er abc f.eks. domænet).

DoS (Denial of Service - Afvisning af service)

En type angreb, der sænker eller standser trafikken på et netværk. Et DoS-angreb forekommer, når et netværk oversvømmes af så mange anmodninger, at almindelig trafik sænkes eller afbrydes helt. Det resulterer normalt ikke i tyveri af information eller andre sikkerhedssårbarheder.

dyb overvågningsplacering

En mappe på computer, som bliver overvåget for ændringer af Data Backup. Hvis du angiver en dyb overvågningsplacering, opretter Data Backup en sikkerhedskopi af overvågningsfilerne i denne mappe og dens undermapper.

E

e-mail

(elektronisk mail) Meddelelser, der sendes og modtages elektronisk via et computernetværk. Se også Webmail.

e-mail-klient

Et program, du kører på computer for at sende og modtage e-mail (f.eks. Microsoft Outlook).

ekstern harddisk

En harddisk, som befinder sig uden for computeren.

ESS

(Extended Service Set) Et sæt af to eller flere netværk, som udgør et enkelt undernetværk.

F

filfragmenter

Rester af en fil, der er spredt ud over disken. Filfragmentering sker, når filer tilføjes eller slettes, og kan sænke computerens effektivitet.

firewall

Et system (hardware, software eller begge dele), som er designet til at blokere uønsket adgang til eller fra et privat netværk. Firewalls bliver ofte brugt til at forhindre uautoriserede internetbrugere i at få adgang til private netværk, der har forbindelse til internettet, specielt intranet. Alle meddelelser, der modtages eller sendes fra intranettet, går gennem firewallen, som undersøger hver meddelelse og blokerer dem, som ikke opfylder de angivne sikkerhedskrav.

flade overvågningsplaceringer

En mappe på computeren, som overvåges for ændringer af Data Backup. Hvis du angiver en dyb overvågningsplacering, opretter Data Backup en sikkerhedskopi af overvågningsfilerne i denne mappe, men inkluderer ikke dens undermapper.

Forældrestyring

Indstillinger, der hjælper med at regulere, hvad dine børn kan se og gøre, når de er på internettet. Under Forældrestyring kan du aktivere eller deaktivere billedfiltrering, vælge en indholdsbedømmelsesgruppe og angive tidsgrænser for surfing på internettet.

frit adgangspunkt

Et uautoriseret adgangspunkt Frie adgangspunkter kan installeres på et sikkert virksomhedsnetværk for at tildele netværksadgang til uautoriserede personer. De kan også oprettes for at tillade en angriber at gennemføre et smørklat-angreb.

fuld arkivering

At arkivere et komplet datasæt baseret på typerne af overvågningsfiler og de steder, som du har konfigureret. Se også hurtigarkivering.

G

gendanne

At gendanne en kopi af en fil fra onlinelageret til sikkerhedskopiering eller fra et arkiv.

genvej

En fil, der kun indeholder placeringen af en anden fil på computeren.

godkendelse

Den proces, hvormed man identificerer et individ, normalt baseret på et entydigt brugernavn og en entydig adgangskode.

H

hjemmenetværk

To eller flere computere, der er forbundet i et hjem, så de kan dele filer og internetadgang. Se også LAN.

hotspot

Et geografisk område, der er dækket af et Wi-Fi (802.11)-adgangspunkt (AP). Brugere, der går ind i et hotspot med en trådløs bærbar computer, kan oprette forbindelse til internettet, hvis det pågældende hotspot sender signaler (beaconing), dvs. annoncerer dets tilstedeværelse, og godkendelse ikke er påkrævet. Hotspots er ofte placeret i områder med mange mennesker, f.eks. lufthavne.

hurtigarkivering

At arkivere kun de filer, som er blevet ændret siden sidste komplette eller hurtige arkivering. Se også fuld arkivering.

hændelse

En handling, der er initieret af brugeren, en enhed eller computeren selv, og som udløser et svar. McAfee registrerer hændelser i hændelseslogfilen.

I

indholdsbedømmelsesgruppe

De aldersgrupper, som en bruger hører ind under, i Forældrestyring. Indhold gøres tilgængeligt eller blokeres ud fra den indholdsbedømmelsesgruppe, brugeren tilhører. Indholdsbedømmelsesgrupperne omfatter: små børn, større børn, ung teenager, ældre teenager og voksen.

integreret gateway

En enhed, som kombinerer funktionerne fra et adgangspunkt (AP), en router og en firewall. Visse enheder kan også indeholde sikkerhedsforbedringer og brobyggende funktioner.

Internet

Internettet består af et utal af indbyrdes forbundne netværk, der bruger TCP/IP-protokollerne til placering og overførsel af data. Internettet har udviklet sig fra at være en sammenkædning af computere på universiteter og højere læreanstalter (sidst i 1960'erne og først i 1970'erne) startet af U.S. Department of Defense under navnet ARPANET. Internettet i dag er et globalt netværk af knap 100.000 uafhængige netværk.

intranet

Et privat computernetværk normalt inden for en organisation, der kun kan benyttes af autoriserede brugere.

IP-adresse

Et id for en computer eller en enhed på et TCP/IP-netværk. Netværk, der anvender TCP/IP-protokollen, router meddelelser ud fra destinationens IP-adresse. En IP-adresses format er en 32-bit numerisk adresse, der er skrevet som fire tal adskilt af punktummer. Hvert tal kan være fra 0 til 255 (f.eks. 192.168.1.100).

IP-forfalskning

At forfalske IP-adresserne i en IP-pakke. Dette bliver brugt i mange typer angreb, som f.eks. sessionskapring. Det bliver også brugt til at forfalske meddelelsesoverskrifterne i spam-beskeder, så de ikke kan spores korrekt.

K

karantæne

At isolere. I VirusScan registreres mistænkelige filer og sættes i karantæne, så de ikke kan beskadige computeren eller filerne.

klient

En applikation, der kører på en pc eller en arbejdsstation, og som er afhængig af en server til visse opgaver. For eksempel er en e-mail-klient en applikation, der gør det muligt for dig at sende og modtage e-mail.

komprimering

En proces, hvor filer komprimeres til en form, der minimerer den plads, der kræves for at sende eller gemme dem.

krigschauffør (wardriver)

En person, der søger efter Wi-Fi (802.11)-netværk ved at køre gennem byer bevæbnet med en Wi-Fi-computer og speciel hardware eller software.

krypteret tekst

Krypterede data. Krypteret tekst er ulæselig, indtil den er blevet konverteret til almindelig tekst (dekrypteret).

kryptering

En proces, som transformerer data fra tekst til kode og dermed skjuler informationerne ved at gøre dem ulæselige for folk, som ikke ved, hvordan de skal dekrypteres. Krypterede data kaldes også krypteret tekst.

L

LAN

(Local Area Network) Et computernetværk, som dækker et relativt lille område, f.eks. en enkelt bygning. Computere på et LAN kan kommunikere indbyrdes og dele ressourcer, f.eks. printere og filer.

launchpad

En U3-grænsefladekomponent, der fungerer som startpunkt for start og administration af U3 USB-programmer.

liste, der er tillid til

Indeholder elementer, du har tillid til, og som ikke registreres. Hvis du kommer til at tilføje et element (f.eks. et potentielt uønsket program), eller du ønsker, at et program igen skal registreres, skal du fjerne det fra denne liste.

M

MAC-adresse

(Media Access Control-adresse) Et entydigt serienummer, som er knyttet til en fysisk enhed med adgang til netværket.

MAPI

(Messaging Application Programming Interface) En Microsoft-grænsefladespecifikation, som tillader forskellige meddelelssystemer og arbejdsgruppeapplikationer (herunder e-mail, voice mail og fax) at fungere gennem en enkelt klient, såsom Exchange-klienten.

message authentication code (MAC)

En sikkerhedskode, der bruges til at kryptere meddelelser, der sendes mellem computere. Meddelelsen accepteres, hvis computeren genkender den afkrypterede kode som gyldig.

midlertidig fil

En fil, der er oprettet i hukommelsen eller på disken af operativsystemet eller et andet program, og som skal bruges under en session og derefter kasseres.

MSN

(Microsoft Network) En gruppe af webbaserede tjenester fra Microsoft Corporation, herunder søgemaskine, e-mail, onlinemeddelelser og portal.

N

netværk

En samling adgangspunkter og deres tilknyttede brugere, svarende til et ESS.

netværksdrev

En disk eller et bånd, som er forbundet til en server eller et netværk, der deles af flere brugere. Netværksdrev kaldes nogle gange for fjerndrev.

netværkskort

En grafisk visning af de computere og komponenter, der udgør et hjemmenetværk.

NIC

(Network Interface Card) Et kort, som kan sættes i en bærbar computer eller en anden enhed, og som tilslutter enheden til LAN-netværket.

node

En enkelt computer, der er tilsluttet et netværk.

nøgle

En række bogstaver og tal, som bruges af to enheder til at godkende deres kommunikation. Begge enheder skal have nøglen. Se også WEP, WPA, WPA2, WPA-PSK og WPA2-PSK.

nøgleord

Et ord, som du kan tildele en sikkerhedskopieret fil for at etablere et forhold eller en forbindelse med andre filer, som deler det samme nøgleord. Det er nemmere at søge på filer, som du har offentliggjort på internettet, hvis du har givet dem nøgleord.

O

offentliggøre

At gøre en sikkerhedskopieret fil offentligt tilgængelig på internettet. Du kan få adgang til udgivne filer ved at søge i biblioteket Data Backup.

onlinesikkerhedskopieringslager

Det sted på onlineserveren, hvor dine filer gemmes, når der er taget en sikkerhedskopi af dem.

opkaldsprogram

Software, der hjælper med at etablere en internetforbindelse. Når opkaldsprogrammer bruges på en skadelig måde, kan de omdirigere dine internetforbindelser til en anden end din standard internetudbyder uden at oplyse dig om de ekstra omkostninger.

ordbogsangreb

En type råstyrkeangreb, der bruger almindelige ord til at afsløre en adgangskode.

orm

En orm er en virus, der ligger i computerens aktive hukommelse, og som kan kopiere sig selv og sende kopierne videre pr. e-mail. Orme replikerer sig selv og optager systemressourcer, hvilket gør computeren langsommere eller sætter opgaver helt i stå.

overvågede filtyper

De filtyper (f.eks. .doc, .xls osv.), som Data Backup sikkerhedskopierer eller arkiverer indenfor overvågningsplaceringerne.

overvågningsplaceringer

De mapper, som Data Backup overvåger på computeren.

P

Papirkurv

Et simuleret affaldsspand til slettede filer og mapper i Windows.

phishing

En internetscam, som er designet til at stjæle værdifulde oplysninger, f.eks. kreditkortnumre, sygesikringsoplysninger, bruger-id og adgangskoder, fra uvidende personer til bedrageriske formål.

plug-in

Et lille softwareprogram, der fungerer sammen med et større program for at øge funktionaliteten. Plug-ins giver f.eks. internetbrowseren mulighed for at indlæse og køre filer, der er integreret i HTML-dokumenter, og som er i formater, som browseren normalt ikke ville genkende (f.eks. animationer, video og lydfiler).

pop-ups

Små vinduer, som dukker op over andre vinduer på computerskærmen. Pop-up-vinduer bruges ofte i internetbrowsere til at vise reklamer.

POP3

(Post Office Protocol 3) En grænseflade mellem et e-mail-klientprogram og e-mail-serveren. De fleste hjemmebrugere har en POP3-e-mail-konto, der også kaldes en standard e-mail-konto.

port

Et sted, hvor oplysninger kommer ind i/ud af en computer. Et traditionelt analogt modem er f.eks. tilsluttet en seriel port.

positivliste

En liste over websider, som det er tilladt at besøge, fordi de ikke anses for at være bedrageriske.

potentielt uønsket program (PUP)

Et program, der indsamler og sender personlige oplysninger uden din tilladelse (f.eks. spyware og adware).

PPPoE

(Point-to-Point Protocol Over Ethernet) En metode til at bruge opkaldsprotokollen Point-to-Point Protocol (PPP) med Ethernet som transport.

protokol

Et format (hardware eller software) til overførsel af data mellem to enheder. Computeren eller enheden skal understøtte den korrekte protokol, hvis du vil kommunikere med andre computere.

proxy

En computer (eller den software, der kører på den), der fungerer som en barriere mellem et netværk og internettet ved kun at vise en enkelt netværksadresse for eksterne websteder. Ved at repræsentere alle interne computere beskytter proxy'en netværksidentiteter og giver samtidig adgang til internettet. Se også proxyserver.

proxyserver

En firewall-komponent, der styrer internettrafik til og fra et LAN (lokalnetværk). En proxyserver kan forbedre ydeevnen ved at levere data, der hyppigt anmodes om, f.eks. en populær webside, og kan filtrere og afvise anmodninger, ejeren ikke accepterer, f.eks. anmodninger om uautoriseret adgang til beskyttede filer.

R

RADIUS

(Remote Access Dial-In User Service) En protokol, som sørger for godkendelse af brugere, som regel i forbindelse med fjernadgang. Denne protokol blev oprindeligt udviklet til brug med eksterne opkaldsservere, men bruges nu til en række godkendelsesmiljøer, som f.eks. 802.1x-godkendelse af en WLAN-brugers "delte hemmelighed" (Shared Secret).

registreringsdatabase

En database, hvori Windows gemmer sine konfigurationsoplysninger. Registreringsdatabasen indeholder profiler for hver bruger af computeren og oplysninger om systemhardware, installerede programmer og egenskabsindstillinger. Windows anvender konstant disse informationer.

roaming

At gå fra dækningsområdet for et adgangspunkt til et andet uden afbrydelse i tjenesterne eller tab af forbindelse.

rootkit

En samling værktøjer (programmer), som giver en bruger administratoradgang til en computer eller et computernetværk. Rootkits kan indeholde spyware og andre skjulte programmer, der kan skabe yderligere sikkerheds- eller fortrolighedsrisici for data og personlige oplysninger på din computer.

router

En netværksenhed, som videresender datapakker fra et netværk til et andet. Ud fra interne routing-tabeller læser routere indgående pakker og bestemmer, hvordan de skal videresendes, baseret på en given kombination af kilde- og destinationsadresser samt de aktuelle trafikforhold (f.eks. belastning, linjeomkostninger og dårlige linjer). En router kaldes også et adgangspunkt (AP).

råstyrkeangreb (brute-force attack)

En metode til at afkode krypterede data, f.eks. adgangskoder, gennem råstyrke (brute force) i stedet for intellektuel strategi. Råstyrke anses for at være en ufejlbarlig, men tidskrævende metode. Råstyrkeangreb kaldes også råstyrkecracking (brute-force cracking).

S

scanning i realtid

At scanne filer og mapper for virus og andre aktiviteter, når de anvendes af dig eller din computer.

scanning på forespørgsel

En scanning, der startes på forespørgsel, dvs. når du starter handlingen. I modsætning til realtidsscanning startes scanning på forespørgsel ikke automatisk.

script

En liste over kommandoer, der kan udføres automatisk (dvs. uden brugerinteraktion). I modsætning til programmer lagres scripts oftest i almindeligt tekstformat og kompileres, hver gang de kører. Makroer og batchfiler kaldes også scripts.

servere

En computer eller et program, der accepterer forbindelser fra andre computere eller programmer og returnerer passende svar. Dit e-mail-program opretter f.eks. forbindelse til en e-mail-server, hver gang du sender eller modtager e-mail.

sikkerhedskopiere

At oprette en kopi af vigtige filer på en sikker onlineserver.

smart drive

Se USB-drev.

SMTP

(Simple Mail Transfer Protocol) En TCP/IP-protokol til at sende meddelelser fra en computer til en anden via et netværk. Denne protokol bruges på internettet til et route e-mail.

smørklat-angreb (man-in-the-middle attack)

En metode opfange og muligvis modificere meddelelser mellem to parter, uden at nogen af parterne ved, at deres kommunikationslink er blevet brudt.

sortliste

En liste over websteder, som bliver anset for at være bedragerisk, i forbindelse med antiphishing.

SSID

(Service Set Identifier) En token (hemmelig nøgle), der identificerer et Wi-Fi (802.11)-netværk. SSID konfigureres af netværksadministratoren og skal angives af brugere, der ønsker at komme på netværket.

SSL

(Secure Sockets Layer) En protokol, som Netscape har udviklet til at transmittere private dokumenter via internettet. SSL virker ved at bruge en offentlig nøgle til at kryptere data, som så overføres over SSL-forbindelsen. URL'er, der kræver en SSL-forbindelse, skal starte med https i stedet for http.

standard e-mail-konto

Se POP3.

synkronisere

At fjerne uoverensstemmelser mellem sikkerhedskopierede filer og de filer, der er gemt på den lokale computer. Du synkroniserer filer, når versionen i sikkerhedskopieringslagret er nyere end den version, som måtte findes på andre computere.

Systembeskyttelse

McAfee-alarmer, der registrerer uautoriserede ændringer på computeren og underretter dig, når de opstår.

systemgendannelsespunkt

Et øjebliksbillede af indholdet af computerens hukommelse eller en database. Windows opretter regelmæssigt gendannelsespunkter og ved vigtige systemhændelser (f.eks. når et program eller en driver installeres). Du kan også oprette og navngive dine egne gendannelsespunkter når som helst.

T

TKIP

(Temporal Key Integrity Protocol) En protokol, der overvinder de medfødte fejl i WEP-sikkerhed, specielt i forbindelse med genbrug af krypteringsnøgler. TKIP ændrer de tidsmæssige nøgler for hver 10.000 pakker, hvilket giver en dynamisk distributionsmetode, som forbedrer sikkerheden på netværket betragteligt. TKIP-sikkerhedsprocessen begynder med en 128-bit tidsmæssig nøgle, som deles mellem klienter og adgangspunkter. TKIP kombinerer den tidsmæssige nøgle med klientens MAC-adresse og tilføjer så en relativt stor 16-oktet initialiseringsvektor for at producere den nøgle, som krypterer dataene. Denne procedure sikrer, at hver enkelt station bruger forskellige nøgle-streams til at kryptere data. TKIP bruger RC4 til udføre krypteringen.

Trojansk hest

Et program, der ligner legitime programmer, men som kan beskadige værdifulde filer, forstyrre ydelsen og tillade uautoriseret adgang til din computer.

trådløs adapter

En enhed, der føjer trådløs funktionalitet til en computer eller PDA. Den tilsluttes via en USB-port, PC Card-slot (CardBus), hukommelseskortslot eller internt i PCI-bussen.

trådløse PCI adapterkort

(Peripheral Component Interconnect) Et trådløst kort, der sættes i en PCI-udvidelsesport inde i computeren.

trådløst USB-adapterkort

Et trådløst kort, der sættes i en USB-slot i computeren.

U

U3

(You: Simplified, Smarter, Mobile) En platform, der kører Windows 2000- eller Windows XP-programmer direkte fra et USB-drev. U3-initiativet blev grundlagt i 2004 af M-Systems og SanDisk og giver brugere mulighed for at køre U3-programmer på en Windows-computer uden at installere eller lagre data eller indstillinger på computeren.

URL-adresse

(Uniform Resource Locator) Standardformatet for internetadresser.

USB

(Universal Serial Bus) En standardiseret seriel computergrænseflade, som giver dig mulighed for at forbinde perifere enheder, f.eks. tastaturer, joysticks og printere, til computeren.

USB-drev

Et lille hukommelsesdrev, der sættes i en computers USB-port. Et USB-drev fungerer som et lille diskdrev og gør det nemt at overføre filer fra en computer til en anden.

V

virus

Programmer, der replicerer sig selv, og som kan ændre dine filer eller data. De lader ofte til at komme fra en afsender, der er tillid til, eller at indeholde gavnligt indhold.

VPN

(Virtual Private Network) Et privat netværk, der er konfigureret i et offentligt netværk for at udnytte administrationsfaciliteterne i det offentlige netværk. VPN'er bruges af virksomheder til at oprette WAN'er, der dækker store geografiske områder, for at oprette site-to-site-forbindelser til afdelingskontorer eller give mobile brugere mulighed for at oprette opkaldsforbindelse til deres virksomheds-LAN.

W

Web bugs

Små grafikfiler, som kan lejre sig i dine HTML-sider og give en uautoriseret kilde mulighed for at gemme cookies på din computer. Disse cookies kan overføre oplysninger til den uautoriserede kilde. Web bugs kendes også som websignaler, pixel tags, gennemsigtige GIF'er eller usynlige GIF'er.

Webmail

Meddelelser, der sendes og modtages elektronisk via internettet. Se også e-mail.

WEP

(Wired Equivalent Privacy) En protokol til kryptering og godkendelse, defineret som en del af Wi-Fi (802.11)-standarden. De første versioner er baseret på RC4-koder og har betydelige svagheder. WEP forsøger at give sikkerhed ved at kryptere data over radiobølger, så de bliver beskyttet under transmissionen fra et endepunkt til et andet. Det er imidlertid blevet opdaget, at WEP ikke er så sikkert, som man engang troede.

Wi-Fi

(Wireless Fidelity) Et term, der bruges af Wi-Fi Alliance for enhver type af 802.11-netværk.

Wi-Fi Alliance

En organisation, der udgøres af førende leverandører af trådløs hardware og software. Wi-Fi Alliance arbejder for at certificere alle 802.11-baserede produkter med hensyn til interoperabilitet og fremme termen Wi-Fi som det globale brand på tværs af alle markeder for alle 802.11-baserede trådløse LAN-produkter. Organisationen fungerer som konsortium, testlaboratorium og afregningskontor for forhandlere, som ønsker at promovere industriens vækst.

Wi-Fi Certified

At være testet og godkendt af Wi-Fi Alliance. Wi-Fi Certified-produkter betragtes som interoperable, selvom de kommer fra forskellige producenter. En bruger med et Wi-Fi Certified-produkt kan bruge adgangspunkter af alle mærker sammen med ethvert andet mærke af klienthardware, som også er certificeret.

WLAN

(Wireless Local Area Network) Et lokalt netværk, der forbindes via et trådløst medie. Et WLAN bruger højfrekvente radiobølger i stedet for ledninger til kommunikation mellem knudepunkter.

WPA

(Wi-Fi Protected Access) En specifikationsstandard, som kraftigt forøger sikkerheden omkring databeskyttelse og adgangskontrol, både i eksisterende og fremtidige trådløse LAN-systemer. WPA er designet til at køre på eksisterende hardware som en softwareopgradering og er udledt af og kompatibel med IEEE 802.11-standarden. Når den er installeret rigtigt, giver WPA-standarden trådløse LAN-brugere stor sikkerhed for, at deres data forbliver beskyttede, og at det kun er muligt for autoriserede netværksbrugere at få adgang til netværket.

WPA-PSK

En speciel WPA-tilstand udviklet til hjemmebrugere, som ikke kræver kraftfuld sikkerhed på virksomhedsniveau, og som ikke har adgang til godkendelsesservere. I denne tilstand kan hjemmebrugeren manuelt indtaste startadgangskoden, der aktiverer WPA i forhåndsdelte nøgletilstand, og bør regelmæssigt ændre adgangsfraasen på hver trådløs computer og hvert adgangspunkt. Se også WPA2-PSK og TKIP.

WPA2

En opdatering af WPA-sikkerhedsstandarden, som er baseret på 802.11i IEEE-standarden.

WPA2-PSK

En særlig WPA-tilstand, der minder om WPA-PSK og er baseret på WPA2-standarden. En udbredt funktion i WPA2-PSK er, at enheder ofte understøtter flere krypteringsmetoder (f.eks. AES, TKIP) samtidig, mens ældre enheder generelt kun understøttede en enkelt krypteringsmetode ad gangen (dvs. at alle klienter var tvunget til at bruge samme krypteringsmetode).

Om McAfee

McAfee, Inc., som har hovedsæde i Santa Clara i Californien, er førende på markedet for løsninger til beskyttelse mod indtrængen og styring af sikkerhedsrisici og leverer proaktive og gennemprøvede løsninger og tjenester til sikring af systemer og netværk i hele verden. Med udgangspunkt i denne uovertrufne sikkerhedsekspertise og vilje til innovation kan McAfee give hjemmebrugere, virksomheder, den offentlige sektor og internetudbydere mulighed for at blokere angreb, undgå nedbrud og løbende følge op på og forbedre sikkerheden.

Copyright

Copyright © 2007-2008 McAfee, Inc. Alle rettigheder forbeholdes. Ingen del af denne publikation må reproducere, overføres, afskrives, lagres på et hentningssystem, eller oversættes til noget sprog i nogen form eller på nogen måde uden skriftlig tilladelse fra McAfee, Inc. McAfee og/eller yderligere mærker heri er registrerede varemærker eller varemærker tilhørende McAfee, Inc. og/eller associerede selskaber i USA og/eller andre lande. Farven rød i forbindelse med sikkerhed er et kendetegn for McAfee-produkter. Alle andre nævnte registrerede og ikke registrerede varemærker, samt copyright-beskyttet materiale heri, tilhører udelukkende deres respektive ejere.

ANERKENDELSE AF VAREMÆRKER

AVERT, EPO, EPOLICY ORCHESTRATOR, FLASHBOX, FOUNDSTONE, GROUPSHIELD, HERCULES, INTRUSHIELD, INTRUSION INTELLIGENCE, LINUXSHIELD, MANAGED MAIL PROTECTION, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, MCAFEE.COM, NETSHIELD, PORTALSHIELD, PREVENTSYS, PROTECTION-IN-DEPTH STRATEGY, PROTECTIONPILOT, SECURE MESSAGING SERVICE, SECURITYALLIANCE, SITEADVISOR, THREATSCAN, TOTAL PROTECTION, VIREX, VIRUSSCAN.

Licens

ORIENTERING TIL ALLE BRUGERE: LÆS OMHYGGELIGT DEN JURIDISK BINDENDE AFTALE, DER ER RELEVANT FOR DEN LICENS, DU HAR ERHVERVET. AFTALEN INDEHOLDER DE GENERELLE VILKÅR OG BETINGELSER FOR BRUG AF DET LICENSEREDE PROGRAM. HVIS DU IKKE VED, HVILKEN TYPE LICENS DU HAR ERHVERVET, SE DA VENLIGST DE SALGSDOKUMENTER ELLER ANDRE RELATEREDE TILLADELSES- ELLER KØBSORDREDOKUMENTER, DER FØLGER MED PROGRAMPAKKEN, ELLER SOM DU HAR MODTAGET SEPARAT SOM EN DEL AF KØBET (I FORM AF ET HÆFTE, EN FIL PÅ PROGRAM-CD'EN ELLER EN FIL, DER ER TILGÆNGELIG PÅ DET WEBSTED, HVORFRA DU HAR HENTET PROGRAMPAKKEN). HVIS DU IKKE ACCEPTERER ALLE VILKÅRENE I AFTALEN, SKAL DU IKKE INSTALLERE PROGRAMMET. HVIS DET ER RELEVANT, KAN DU RETURNERE PRODUKTET TIL MCAFEE, INC. ELLER KØBSTEDET OG FÅ PENGENE TILBAGE.

KAPITEL 18

Kundeservice og teknisk support

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Kritiske beskyttelsesproblemer kræver øjeblikkelig handling og kompromitterer din beskyttelsesstatus (ændrer farven til rød). Ikke-kritiske beskyttelsesproblemer kræver ikke øjeblikkelig handling og muligvis kompromittere din beskyttelsesstatus (afhængigt af typen af problem). For at opnå grøn beskyttelsesstatus skal du løse alle kritiske problemer og enten løse eller ignorere alle ikke-kritiske problemer. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician. Se Hjælp i McAfee Virtual Technician for at få flere oplysninger om McAfee Virtual Technician.

Hvis du har købt din sikkerhedssoftware fra en partner eller en anden leverandør end McAfee, skal du åbne en webbrowser og gå til www.mcafeehelp.com. Under Partner Links skal du vælge din partner eller leverandør for at få adgang til McAfee Virtual Technician.

Bemærk! Hvis du vil installere og køre McAfee Virtual Technician, skal du logge ind på din computer som Windows Administrator. Hvis du ikke gør det, kan MVT evt. ikke løse dine problemer. Du kan finde oplysninger om at logge ind som Windows Administrator i Windows Hjælp. I Windows Vista™ vises en meddelelse, når du kører MVT. Hvis det sker, skal du klikke på **Accepter**. Virtual Technician fungerer ikke med Mozilla® Firefox.

I dette kapitel

Brug af McAfee Virtual Technician	116
Support og downloads	117

Brug af McAfee Virtual Technician

Som en personlig, teknisk supportmedarbejder indsamler Virtual Technician oplysninger om dine SecurityCenter-programmer for at hjælpe dig med at løse computerens sikkerhedsproblemer. Når du kører Virtual Technician, kontrollerer den, at dine SecurityCenter-programmer fungerer korrekt. Hvis den registrerer problemer, tilbyder Virtual Technician at løse dem for dig eller give dig flere detaljerede oplysninger om dem. Når Virtual Technician er færdig, vises resultaterne af analysen, og du kan søge yderligere teknisk support hos McAfee, hvis det er nødvendigt.

For at opretholde sikkerheden og integriteten for computeren og filerne indsamler Virtual Technician ikke personligt identificerbare oplysninger.

Bemærk! Klik på ikonet **Hjælp** i Virtual Technician for at få flere oplysninger om Virtual Technician.

Starte Virtual Technician

Virtual Technician indsamler oplysninger om dine SecurityCenter-programmer for at hjælpe dig med at løse computerens sikkerhedsproblemer. For at beskytte dine personlige oplysninger indeholder disse oplysninger ikke personligt identificerbare oplysninger.

- 1 Klik på **McAfee Virtual Technician** under **Almindelige opgaver**.
- 2 Følg anvisningerne på skærmen for at downloade og køre Virtual Technician.

Support og downloads

Se følgende tabeller for oplysninger om McAfee Support- og Download-websteder i dit land, herunder brugerhåndbøger.

Support og downloads

Land	McAfee Support	McAfee Downloads
Australien	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasilien	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (engelsk)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (fransk)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Kina (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Kina (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tjekkoslaviet	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
Frankrig	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
Mexico	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
Tyrkiet	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
USA	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection-brugerhåndbøger

Land	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Kina (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Kina (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tjekkoslavakiet	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
Frankrig	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
Nederlandene	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
Mexico	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
Tyrkiet	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-brugerhåndbøger

Land	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Kina (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Kina (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tjekkoslavakiet	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
Frankrig	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
Nederlandene	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
Mexico	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
Tyrkiet	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-brugerhåndbøger

Land	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Kina (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Kina (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tjekkioslovakiet	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
Frankrig	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
Nederlandene	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
Mexico	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
Tyrkiet	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan-brugerhåndbøger

Land	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Kina (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Kina (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tjekkosllovakiet	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
Frankrig	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
Nederlandene	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
Mexico	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
Tyrkiet	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Se følgende tabel for oplysninger om McAfee Threat Center- og Virus Information-websteder i dit land.

Land	Sikkerhedshovedkvarter	Virusoplysninger
Australien	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasilien	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (engelsk)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (fransk)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Kina (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Kina (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tjekkoslavaki et	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
Frankrig	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
Nederlandene	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
Mexico	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
Tyrkiet	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
USA	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Se følgende tabel for oplysninger om HackerWatch-websteder i dit land.

Land	HackerWatch
Australien	www.hackerwatch.org
Brasilien	www.hackerwatch.org/?lang=pt-br
Canada (engelsk)	www.hackerwatch.org
Canada (fransk)	www.hackerwatch.org/?lang=fr-ca
Kina (chn)	www.hackerwatch.org/?lang=zh-cn
Kina (tw)	www.hackerwatch.org/?lang=zh-tw
Tjekkioslovakiet	www.hackerwatch.org/?lang=cs
Danmark	www.hackerwatch.org/?lang=da
Finland	www.hackerwatch.org/?lang=fi
Frankrig	www.hackerwatch.org/?lang=fr
Tyskland	www.hackerwatch.org/?lang=de
Storbritannien	www.hackerwatch.org
Nederlandene	www.hackerwatch.org/?lang=nl
Italien	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Korea	www.hackerwatch.org/?lang=ko
Mexico	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
Tyrkiet	www.hackerwatch.org/?lang=tr

USA

www.hackerwatch.org

Indeks

8

802.11	99
802.11a.....	99
802.11b	99
802.1x.....	99

A

ActiveX-objekt.....	99
adgangskode	99
Adgangskodeboks.....	99
adgangspunkt	99
Administrere din McAfee-konto.....	11
Administrere en enhed.....	95
Administrere lister over elementer, der er tillid til	53
Administrere netværket eksternt.....	93
administreret netværk.....	100
Afhjælp sikkerhedssårbarheder.....	96
Afspille en lyd med alarmer	26
Aktivere systembeskyttelse	47
almindelig tekst	100
Arbejde med alarmer.....	14, 23
Arbejde med filer i karantæne	62
Arbejde med netværkskortet	86
Arbejde med potentielt uønskede programmer	62
Arbejde med programmer og cookies i karantæne.....	63
Arbejde med scanningsresultater.....	61
Arbejde med virus og trojanske heste ...	61
arkivere.....	100

B

bibliotek	100
billedfiltrering	100
browser.....	100
Brug af indstillinger for systembeskyttelse	46
Brug af lister, der er tillid til	53
Brug af McAfee Virtual Technician.....	116
Brug af SecurityCenter	7
bufferoverløb	100
båndbredde.....	100

C

cache.....	100
------------	-----

cookie	100
Copyright	113

D

DAT.....	101
Deaktivere automatiske opdateringer ...	14
Defragmentering af din computer	70
dele	101
delt hemmelighed (shared secret)	101
DNS	101
DNS-server.....	101
domæne	101
DoS (Denial of Service - Afvisning af service).....	101
dyb overvågningsplacering.....	101

E

ekstern harddisk.....	102
e-mail	102
e-mail-klient	102
ESS.....	102

F

filfragmenter	102
firewall.....	102
flade overvågningsplaceringer	102
Forklaring af beskyttelseskategorier ...	7, 9, 29
Forklaring af beskyttelsesstatus	7, 8, 9
Forklaring af beskyttelsestjenester.....	10
Forklaring af ikoner i Network Manager	83
Forældrestyring	102
frit adgangspunkt	102
fuld arkivering	102
Funktioner i Network Manager	82
Funktioner i QuickClean.....	66
Funktioner i SecurityCenter	6
Funktioner i Shredder	78
Funktioner i VirusScan	32
Få vist yderligere oplysninger om et element	87

G

gendannde	103
genvej	103
godkendelse.....	103

H

hjemmenetværk.....	103
hotspot	103
hurtigarkivering.....	103
hændelse	103

I

Ignorere beskyttelsesproblemer.....	20
Ignorere et beskyttelsesproblem	20
indholdsbedømmelsesgruppe.....	103
Indstille overvågning af en computers beskyttelsesstatus.....	94
Installere McAfee sikkerhedssoftware på fjerncomputere	97
integreret gateway	103
Internet.....	103
intranet.....	104
Invitere en computer til at deltage i det administrerede netværk	89
IP-adresse.....	104
IP-forfalskning	104

K

karantæne	104
klient.....	104
komprimering.....	104
Konfigurere alarmindstillinger	26
Konfigurere automatiske opdateringer..	14
Konfigurere et administreret netværk....	85
Konfigurere indstillinger for systembeskyttelse	48
Konfigurere virusbeskyttelse	39, 57
Kontrollere dit abonnement	11
krigschauffør (wardriver)	104
krypteret tekst	104
kryptering.....	104
Kundeservice og teknisk support	115

L

LAN.....	104
launchpad	105
Lav ændring i en opgave i Disk Defragmenter	74
Lav ændringer i en opgave i QuickClean	72
Licens	114
liste, der er tillid til.....	105
Løse beskyttelsesproblemer	8, 18
Løse beskyttelsesproblemer automatisk	18
Løse beskyttelsesproblemer manuelt	19
Løse eller ignorere beskyttelsesproblemer	8, 17

M

MAC-adresse	105
Makuler filer og mapper	79
Makulere en hel disk	80
Makulerer filer og indholdet af mapper og diske.....	79
MAPI.....	105
McAfee Network Manager	81
McAfee QuickClean.....	65
McAfee SecurityCenter	5
McAfee Shredder	77
McAfee VirusScan.....	3, 31
message authentication code (MAC) ...	105
midlertidig fil	105
MSN.....	105

N

netværk	105
netværksdrev	105
netværkskort.....	105
NIC	105
node	106
nøgle.....	106
nøgleord.....	106

O

offentliggøre	106
Om McAfee	113
Om systembeskyttelsestyper	48, 49
Om typer af lister, der er tillid til	54
Omdøbe netværket	87
onlinesikkerhedskopieringslager	106
Opdatere netværkskortet.....	86
Opdatere SecurityCenter	13
opkaldsprogram	106
ordbogsangreb	106
orm	106
Overvåge en computers beskyttelsesstatus	94
Overvåge status og tilladelser	94
overvågede filtyper	106
overvågningsplaceringer	106

P

Papirkurv.....	106
phishing	107
Planlæg en opgave.....	71
Planlæg en opgave i Disk Defragmenter	73
Planlæg en opgave i QuickClean	71
Planlægge en scanning	45
plug-in.....	107
POP3.....	107
pop-ups.....	107

port	107
positivliste	107
potentielt uønsket program (PUP)	107
PPPoE	107
protokol	107
proxy	107
proxyserver.....	108
R	
RADIUS	108
Redigere en enheds displayegenskaber	95
Redigere tilladelser for en administreret computer	95
Reference	98
registreringsdatabase	108
Rense computeren	67
Rensning af din computer	69
roaming.....	108
rootkit	108
router	108
råstyrkeangreb (brute-force attack)	108
S	
Scanne computeren	33, 57, 58
scanning i realtid	108
scanning på forespørgsel	108
script.....	109
servere	109
sikkerhedskopiere.....	109
Skjule alarmer om virusudbrud.....	27
Skjule velkomstbilledet ved opstart	26
Slet en opgave i Disk Defragmenter	75
Slet en opgave i QuickClean	73
smart drive	109
SMTP	109
smørklat-angreb (man-in-the-middle attack)	109
sortliste.....	109
SSID	109
SSL	109
standard e-mail-konto	109
Standse virusbeskyttelse i realtid	33
Starte beskyttelse af onlinemeddelelser	37
Starte e-mail-beskyttelse	36
Starte scriptscanning.....	36
Starte spywarebeskyttelse	36
Starte Virtual Technician	116
Starte virusbeskyttelse i realtid	33
Starte yderligere beskyttelse	35
Stoppe med at stole på andre computere på netværket	91
Support og downloads	117
synkronisere.....	109
Systembeskyttelse	110
systemgendannelsespunkt	110
Søge efter opdateringer.....	13, 14
T	
Tilslutte computeren til det administrerede netværk	88
Tilslutte computeren til et administreret netværk.....	89
TKIP	110
Trojansk hest	110
trådløs adapter	110
trådløse PCI adapterkort.....	110
trådløst USB-adapterkort	110
U	
U3	110
URL-adresse	110
USB.....	111
USB-drev.....	111
V	
virus.....	111
Vise alle hændelser.....	29
Vise de seneste hændelser	29
Vise eller skjule elementer på netværkskortet	87
Vise eller skjule ignorerede problemer	20
Vise eller skjule oplysningsalarmer	24
Vise eller skjule oplysningsalarmer under spil.....	25
Vise hændelser	18, 29
Vise og skjule oplysningsalarmer	24
Vise scanningsresultater	58
VPN.....	111
Vælg indstillinger for manuel scanning	42
Vælg indstillinger for realtidsscanning	40
Vælg placering til manuel scanning.....	44
W	
Web bugs.....	111
Webmail.....	111
WEP	111
Wi-Fi.....	111
Wi-Fi Alliance	111
Wi-Fi Certified	112
WLAN	112
WPA	112
WPA2	112
WPA2-PSK.....	112
WPA-PSK.....	112
Å	
Åbne netværkskortet	86

