McAfee®

VirusScan® Plus

AntiVirus, Firewall & AntiSpyware

Brukerhåndbok

Innhold

KAPITTEL 1

Innledning

Beskytt datamaskinen med en kombinasjon av McAfees teknologier for brannmur, virusskanning og beskyttelse mot spionprogrammer. Du kan bruke VirusScan Plus til å beskytte datamaskinen mot virus, overvåke Internett-trafikk med tanke på mistenkelig aktivitet og blokkere spionvare som kan skade integriteten til personlig informasjon.

I dette kapitlet

KAPITTEL 2

McAfee SecurityCenter

McAfee SecurityCenter lar deg overvåke sikkerhetsstatusen til datamaskinen din, øyeblikkelig finne ut om din datamaskins tjenester for virus-, spionprogram-, e-post- og brannmurbeskyttelse er oppdatert, og reparere potensielle sikkerhetshull. Det gir deg navigeringsverktøyene og kontrollene du trenger for å koordinere og administrere alle områder av din datamaskins beskyttelse.

Før du starter konfigurering og administrering av din datamaskins beskyttelse, gå gjennom SecurityCenter-grensesnittet og forsikre deg om at du forstår forskjellen mellom beskyttelsesstatus, beskyttelseskategorier og beskyttelsestjenester. Oppdater deretter SecurityCenter for å forsikre deg om at du har den siste tilgjengelige beskyttelsen fra McAfee.

Etter at de første konfigurasjonsoppgavene er fullført, bruker du SecurityCenter til å overvåke beskyttelsesstatusen til din datamaskin. Hvis SecurityCenter oppdager et beskyttelsesproblem varsler det deg slik at du enten kan fikse eller ignorere problemet (avhengig av hvor alvorlig det er). Du kan også gå gjennom hendelser i SecurityCenter, som konfigurasjonsendringer i virusskanning, i en hendelseslogg.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

SecurityCenter-funksjoner

Forenklet beskyttelsesstatus

Gjør det enkelt å gå gjennom datamaskinens sikkerhetsstatus, se etter oppdateringer og fikse sikkerhetsproblemer.

Kontinuerlige oppdateringer og oppgraderinger

SecurityCenter laster automatisk ned oppdateringer til programmene og installerer dem. Når en ny versjon av et McAfee-program er tilgjengelig, leveres det automatisk til datamaskinen så lenge abonnementet ditt er gyldig, slik at du alltid er sikret den mest oppdaterte beskyttelsen.

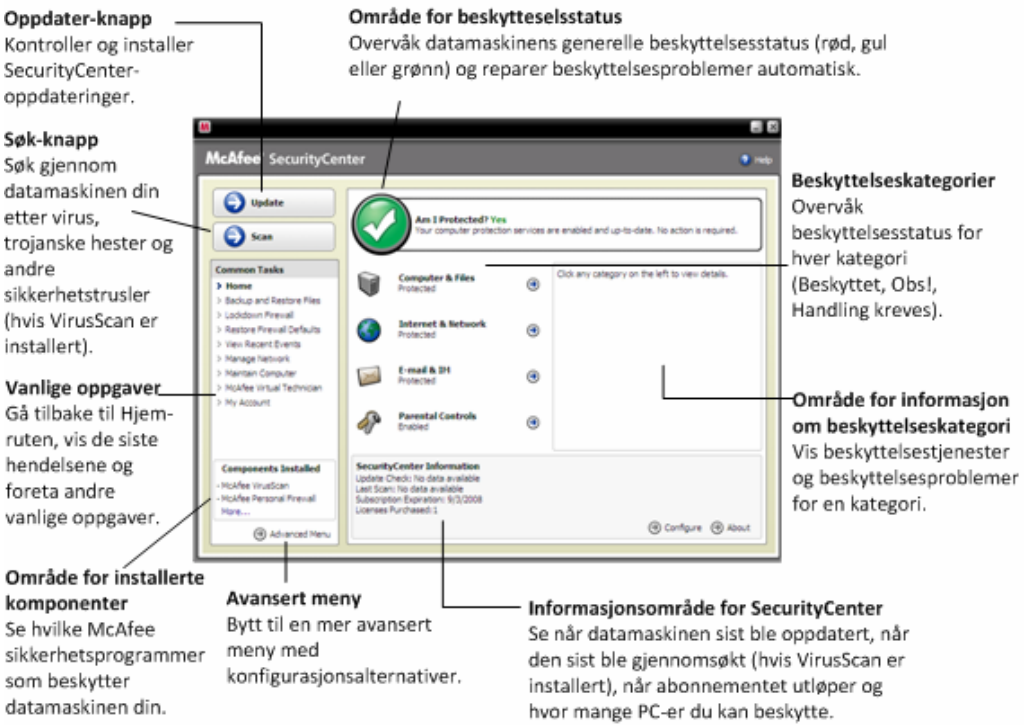
Sanntidsvarsler

Sikkerhetsvarsler advarer deg om kritiske virusutbrudd og sikkerhetstrusler.

KAPITTEL 3

Bruke SecurityCenter

Før du begynner å bruke SecurityCenter, gå gjennom komponentene og konfigurasjonsområdene du skal bruke til å administrere datamaskinens beskyttelsesstatus. For mer informasjon om terminologien som er brukt i dette bildet, se Forstå beskyttelsesstatus (side 8) og Forstå beskyttelseskategorier (side 9). Du kan deretter gå gjennom kontoinformasjonen din for McAfee og bekrefte abonnementet ditt.



I dette kapitlet

Forstå beskyttelsesstatus

Beskyttelsesstatusen til datamaskinen din vises i området for beskyttelsesstatus i Hjem-ruten i SecurityCenter. Den viser om datamaskinen din er fullstendig beskyttet mot de siste sikkerhetstruslene og kan påvirkes av ting som eksterne sikkerhetsangrep, andre sikkerhetsprogrammer og programmer som har tilgang til Internett.

Beskyttelsesstatusen til din datamaskin kan være rød, gul eller grønn.

Beskyttelses-status	Beskrivelse
Rød	Datamaskinen er ikke beskyttet. Området for beskyttelsesstatus i Hjem-ruten i SecurityCenter er rød og viser at du ikke er beskyttet. SecurityCenter rapporterer om minst ett kritisk sikkerhetsproblem. For å oppnå fullstendig beskyttelse må du reparere alle kritiske sikkerhetsproblemer i hver beskyttelseskategori (problemkategoriens status er satt til **Handling kreves**, også i rødt). For informasjon om hvordan du reparerer beskyttelsesproblemer, se Løse beskyttelsesproblemer (side 18).
Gul	Datamaskinen er delvis beskyttet. Området for beskyttelsesstatus i Hjem-ruten i SecurityCenter er gul og viser at du ikke er beskyttet. SecurityCenter rapporterer om minst ett ikke-kritisk sikkerhetsproblem. For å oppnå fullstendig beskyttelse må du reparere eller ignorere de ikke-kritiske sikkerhetsproblemene i hver beskyttelseskategori. For informasjon om hvordan du reparerer eller ignorerer beskyttelsesproblemer, se Løse eller ignorere beskyttelsesproblemer (side 17).
Grønn	Datamaskinen er fullstendig beskyttet. Området for beskyttelsesstatus i Hjem-ruten i SecurityCenter er grønn og viser at du er beskyttet. SecurityCenter rapporterer ikke om noen kritiske eller ikke-kritiske sikkerhetsproblemer. Hver beskyttelseskategori oppgir tjenestene som beskytter datamaskinen din.

Forstå beskyttelseskategorier

SecurityCenters beskyttelsestjenester er delt inn i fire kategorier: Datamaskin og filer, Internett og nettverk, E-post og direktemeldinger og Foreldrestyring. Disse kategoriene hjelper deg å bla gjennom og konfigurere sikkerhetstjenestene som beskytter datamaskinen din.

Klikk et kategorinavn for å konfigurere beskyttelsestjenestene og se sikkerhetsproblemer som er oppdaget for disse tjenestene. Hvis beskyttelsesstatusen til datamaskinen din er rød eller gul, vil en eller flere kategorier vise beskjeden *Handling kreves* eller *Obs*, som indikerer at SecurityCenter har oppdaget et problem med kategorien. For mer informasjon om beskyttelsesstatus, se Forstå beskyttelsesstatus (side 8).

Beskyttelseskategori	Beskrivelse
Datamaskin og filer	Kategorien Datamaskin og filer lar deg konfigurere følgende beskyttelsestjenester: ▪ Virusbeskyttelse ▪ Spionprogrambeskyttelse ▪ SystemGuards ▪ Windows-beskyttelse ▪ PC-helse
Internett og nettverk	Kategorien Internett og nettverk lar deg konfigurere følgende beskyttelsestjenester: ▪ Brannmurbeskyttelse ▪ Beskyttelse mot phishing ▪ Identitetsbeskyttelse
E-post og direktemeldinger	Kategorien E-post og direktemeldinger lar deg konfigurere følgende beskyttelsestjenester: ▪ E-postvirusbeskyttelse ▪ Virusbeskyttelse for direktemeldinger ▪ Spionprogrambeskyttelse for e-post ▪ Spionprogrambeskyttelse for direktemeldinger ▪ Spambeskyttelse
Foreldrestyring	Kategorien Foreldrestrying lar deg konfigurere følgende beskyttelsestjenester: ▪ Innholdsblokkering

Forstå beskyttelsestjenester

Beskyttelsestjenester er de ulike kjernesikkerhetskomponentene som du konfigurerer til å beskytte datamaskinen din. Beskyttelsestjenester korresponderer direkte med McAfee-programmer. For eksempel, når du installerer VirusScan, blir følgende beskyttelsestjenester tilgjengelig: Virusbeskyttelse, Spionprogrambeskyttelse, SystemGuards og skriptsøking. For detaljert informasjon om disse bestemte beskyttelsestjenestene, se Hjelp for VirusScan.

Som standardinnstilling er alle beskyttelsestjenester tilknyttet et program aktivert når du installerer programmet. Du kan imidlertid deaktivere en beskyttelsestjeneste når som helst. Hvis du for eksempel installerer Foreldrestyring, vil både Innholdsblokkering og Identitetsbeskyttelse være aktivert. Hvis du ikke har tenkt å bruke beskyttelsestjenesten Innholdsblokkering, kan du deaktivere den fullstendig. Du kan også midlertidig deaktivere en beskyttelsestjeneste mens du utfører installasjon eller vedlikeholdsoppgaver.

Administrere abonnementer

Til hvert McAfee-beskyttelsesprodukt du kjøper, følger det et abonnement som lar deg bruke produktet på et bestemt antall datamaskiner i en bestemt periode. Lengden på abonnementet varierer avhengig av kjøpet ditt, men abonnementet starter normalt når du aktiverer produktet. Aktivering er enkelt og kostnadsfritt – du behøver bare en Internett-tilkobling – men det er svært viktig, fordi det gir deg rett til å motta jevnlige, automatiske produktoppdateringer som beskytter datamaskinen mot de nyeste truslene.

Aktivering skjer normalt når produktet blir installert, men hvis du vil vente (for eksempel hvis du ikke har Internett-tilkobling), kan du gjøre det innen 15 dager. Hvis du ikke aktiverer innen 15 dager, vil ikke produktene lenger motta viktige oppdateringer eller utføre søk. Du vil også bli varslet med jevne mellomrom (med meldinger på skjermen) når abonnementet er i ferd med å utløpe. På den måten kan du unngå avbrudd i beskyttelsen ved å fornye det tidligere eller ved å opprette automatisk fornyelse på webområdet vårt.

Hvis du ser en kobling i SecurityCenter som ber deg om å aktivere, er ikke abonnementet aktivert. Du finner utløpsdatoen for abonnementet på kontosiden din.

Få tilgang til McAfee-kontoen

Du kan enkelt få tilgang til informasjonen i McAfee-kontoen din (kontosiden) fra SecurityCenter.

1 Under **Vanlige oppgaver** klikker du **Min konto**.

2 Logg på din McAfee-konto.

Aktivere produktet

Aktivering skjer normalt når du installerer produktet. Hvis dette ikke skjer, vises en kobling i SecurityCenter som ber deg om å aktivere. Du blir også varslet med jevne mellomrom.

- I Hjem-ruten i SecurityCenter klikker du **Aktiver abonnementet ditt** under **SecurityCenter-informasjon**.

Tips: Du kan også aktivere fra varselet som vises med jevne mellomrom.

Bekreft abonnementet

Du bekrefter abonnementet for å kontrollere at det ikke har gått ut.

- Høyreklikk SecurityCenter-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, og klikk deretter på **Bekreft abonnement**.

Fornye abonnementet

Kort tid før abonnementet utløper, vises en kobling i SecurityCenter som ber deg om å fornye det. Du blir også varslet med jevne mellomrom om at abonnementet snart utløper.

- Klikk **Forny** i Hjem-ruten i SecurityCenter under **SecurityCenter-informasjon**.

Tips: Du kan også fornye produktet fra varselsmeldingen som vises med jevne mellomrom. Alternativt kan du gå til kontosiden din, der du kan fornye eller opprette automatisk fornyelse.

KAPITTEL 4

Oppdatere SecurityCenter

SecurityCenter sørger for at dine registrerte McAfee-programmer er oppdaterte ved å se etter og installere oppdateringer på nettet hver fjerde time. Avhengig av programmene du har installert og aktivert, kan oppdateringer fra Internett inkludere de siste virusdefinisjonene og oppgraderinger for hacker-, spam-, spionprogram- og personvernbeskyttelse. Hvis du ønsker å se etter oppdateringer innenfor firetimersperioden som er standard, kan du gjøre dette når som helst. Mens SecurityCenter ser etter oppdateringer, kan du fortsette å utføre andre oppgaver.

Selv om det ikke anbefales, kan du endre måten SecurityCenter ser etter eller installerer oppdateringer. For eksempel kan du konfigurere SecurityCenter til å laste ned, men ikke installere oppdateringer, eller si ifra før det laster ned eller installerer oppdateringer. Du kan også deaktivere automatisk oppdatering.

Merk: Hvis du installerte McAfee-produktet fra en CD, må du aktivere innen 15 dager, ellers vil ikke produktene lenger motta viktige oppdateringer eller utføre søk.

I dette kapitlet

Se etter oppdateringer

Som standardinnstilling ser SecurityCenter automatisk etter oppdateringer hver fjerde time når datamaskinen din er tilkoblet Internett; hvis du imidlertid ønsker å se etter oppdateringer innenfor firetimersperioden kan du gjøre dette. Hvis du har deaktivert automatiske oppdateringer er det ditt ansvar å se etter oppdateringer med jevne mellomrom.

- Klikk **Oppdater** i Hjem-ruten i SecurityCenter.

Tips: Du kan se etter oppdateringer uten å starte SecurityCenter ved å høyreklikke SecurityCenter-ikonet i systemstatusfeltet helt til høyre på oppgavelinjen, og så klikke på **Oppdateringer**.

Konfigurere automatiske oppdateringer

Som standardinnstilling ser SecurityCenter automatisk etter oppdateringer og installerer dem hver fjerde time når du er tilkoblet Internett. Hvis du ønsker å endre denne standardinnstilingen kan du konfigurere SecurityCenter til å automatisk laste ned oppdateringer og gi beskjed når oppdateringene er klare til å installeres, eller gi beskjed før oppdateringer lastes ned.

Merknad: SecurityCenter gir deg beskjed via varsler når oppdateringer er klare til å lastes ned eller installeres. Fra varslene kan du enten laste ned eller installere oppdateringene, eller utsette oppdateringene. Når du oppdaterer programmene fra et varsel, kan det hende du må bekrefte abonnementet ditt før du kan laste ned og installere. For mer informasjon, se Arbeide med varsler (side 21).

1. Åpne konfigurasjonsruten for SecurityCenter

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.

2. I konfigurasjonsruten for SecurityCenter, under **Automatiske oppdateringer er deaktiverte**, klikk på **På**, og klikk deretter på **Avansert**.
3. Klikk én av følgende knapper:
   - **Installer oppdateringene automatisk, og varsle meg når tjenestene er oppdatert (anbefales)**
   - **Last ned oppdateringene automatisk, og varsle meg når de er klare til å installeres**
   - **Varsle meg før oppdateringer lastes ned**
4. Klikk **OK**.

Deaktivere automatiske oppdateringer

Hvis du deaktiverer automatiske oppdateringer er det ditt ansvar å se etter oppdateringer med jevne mellomrom; hvis ikke vil ikke datamaskinen ha den siste sikkerhetsbeskyttelsen. For informasjon om hvordan du ser etter oppdateringer manuelt, se Se etter oppdateringer (side 13).

1 Åpne konfigurasjonsruten for SecurityCenter

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.

2 I konfigurasjonsruten for SecurityCenter, under **Automatiske oppdateringer er aktivert**,klikker du **Av**.

3 I bekreftelsesdialogboksen klikker du **Ja**.

Tips: Du aktiverer automatiske oppdateringer ved å klikke **På**-knappen eller ved å fjerne merket for **Deaktiver automatisk oppdatering og la meg se etter oppdateringer manuelt** i ruten for Oppdateringsalternativer.

KAPITTEL 5

Reparere eller ignorere beskyttelsesproblemer

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Kritiske beskyttelsesproblemer krever øyeblikkelig handling og kan sette din beskyttelsesstatus på spill (endre fargen til rød). Ikke-kritiske beskyttelsesproblemer krever ikke øyeblikkelig handling og kan kanskje sette din beskyttelsesstatus på spill (avhengig av hva slags type problem det dreier seg om). For å oppnå grønn beskyttelsesstatus må du reparere alle kritiske problemer og enten reparere eller ignorere alle ikke-kritiske problemer. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtuell Tekniker. For mer informasjon om McAfee Virtuell tekniker, se Hjelp for McAfee Virtuell tekniker.

I dette kapitlet

Løse beskyttelsesproblemer

De fleste sikkerhetsproblemer kan løses automatisk, men noen problemer kan kreve at du foretar deg noe. Hvis for eksempel Brannmurbeskyttelse er deaktivert, kan SecurityCenter aktivere det automatisk, men hvis Brannmurbeskyttelse ikke er installert, må du installere det. Følgende tabell beskriver noen andre handlinger du kanskje må utføre for å løse beskyttelsesproblemer manuelt:

Problem	Handling
Det er ikke fullført et fullstendig søk på datamaskinen de siste 30 dagene.	Kjør søk på datamaskinen manuelt. Se Hjelp for VirusScan for mer informasjon.
Oppdagelsessignaturfilene (DAT-filene) er foreldet.	Oppdater beskyttelsen manuelt. Se Hjelp for VirusScan for mer informasjon.
Et program er ikke installert.	Installer programmet fra McAfees webområde eller CD.
Et program mangler komponenter.	Installer programmet på nytt fra McAfees webområde eller CD.
Et program er ikke aktivert, og kan ikke motta fullstendig beskyttelse.	Aktiver programmet på McAfees webområde.
Abonnementet er utløpt.	Kontroller kontostatusen på McAfees webområde. Du finner mer informasjon i Administrere abonnementer (side 10).

Merk: Ofte vil ett enkelt beskyttelsesproblem ha innvirkning på flere beskyttelseskategorier. I så fall fjernes problemer fra de andre kategoriene når du løser det i én kategori.

Løse beskyttelsesproblemer automatisk

SecurityCenter kan løse de fleste beskyttelsesproblemene automatisk. Konfigurasjonsendringene som SecurityCenter gjør når det løser beskyttelsesproblemer automatisk, blir ikke registrert i hendelsesloggen. For mer informasjon om varsler, se Om varsler (side 27).

1 Under **Vanlige oppgaver** klikker du **Hjem**.

2 I området for beskyttelsesstatus i Hjem-ruten i SecurityCenter klikker du **Reparer**.

Løse beskyttelsesproblemer manuelt

Hvis ett eller flere beskyttelsesproblemer vedvarer etter at du har forsøkt å løse dem automatisk, kan du løse problemene manuelt.

1 Under **Vanlige oppgaver** klikker du **Hjem**.

2 I Hjem-ruten i SecurityCenter klikker du på den beskyttelseskategorien SecurityCenter rapporterer om problemet i.

3 Klikk på koblingen etter beskrivelsen av problemet.

Ignorere beskyttelsesproblemer

Hvis SecurityCenter oppdager et ikke-kritisk problem kan du enten løse eller ignorere det. Andre ikke-kritiske problemer (f.eks. hvis Anti-Spam eller Foreldrestyring ikke er installert) ignoreres automatisk. Ignorerte problemer vises ikke i informasjonsområdet for beskyttelseskategorier i Hjem-ruten i SecurityCenter med mindre beskyttelsesstatusen til datamaskinen er grønn. Hvis du ignorerer et problem, men senere vil at det skal vises i informasjonsområdet for beskyttelseskategorier selv når beskyttelsesstatusen til datamaskinen ikke er grønn, kan du vise det ignorerte problemet.

Ignorere et beskyttelsesproblem

Hvis SecurityCenter oppdager et ikke-kritisk problem du ikke har planer om å løse, kan du ignorere det. Når du ignorerer problemet fjernes det fra informasjonsområdet for beskyttelseskategorier i SecurityCenter.

1 Under **Vanlige oppgaver** klikker du **Hjem**.

2 I Hjem-ruten i SecurityCenter klikker du på den beskyttelseskategorien SecurityCenter rapporterer om problemet i.

3 Klikk på **Ignorer** -koblingen ved siden av beskyttelsesproblemet.

Vis eller skjul ignorerte problemer

Du kan vise eller skjule et ignorert beskyttelsesproblem, avhengig av hvor alvorlig det er.

1 Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.

2 I ruten SecurityCenter-konfigurasjon klikker du på **Ignorerte problemer**.

3 I ruten Ignorerte problemer gjør du følgende:

   - Hvis du vil ignorere et problem merker du av i avmerkingsboksen.
   - Hvis du vil rapportere et problem i informasjonsområdet for beskyttelseskategorier, fjerner du merket i avmerkingsboksen.

4 Klikk **OK**.

Tips: Du kan også ignorere et problem ved å klikke på **Ignorer**-koblingen ved siden av det rapporterte problemet i informasjonsområdet for beskyttelseskategorier.

KAPITTEL 6

Arbeide med varsler

Varsler er små popup-dialogbokser som vises i nederste høyre hjørne av skjermen når SecurityCenter-hendelser oppstår. Et varsel viser detaljert informasjon om en hendelse, samt anbefalinger og valg for å løse problemer som kan være tilkyttet hendelsen. Noen varsler inneholder også koblinger til ytterligere informasjon om hendelsen. Disse koblingene lar deg starte McAfees globale webområde eller sende informasjon til McAfee for feilsøking.

Det finnes tre typer varsler: rød, gul og grønn.

Varseltype	Beskrivelse
Rød	Et rødt varsel er en kritisk melding som krever en handling fra deg. Røde varsler oppstår når SecurityCenter ikke kan fastslå hvordan det kan løse et problem automatisk.
Gul	Et gult varsel er en ikke-kritisk melding som vanligvis krever en handling fra deg.
Grønn	Et grønt varsel er en ikke-kritisk melding som ikke krever en handling fra deg. Grønne varsler gir deg grunnleggende informasjon om en hendelse.

Siden varsler er svært viktige når du overvåker og administrerer beskyttelsesstatusen, kan du ikke deaktivere dem. Du kan imidlertid bestemme om visse typer informasjonsvarsler skal vises og konfigurere noen andre varslingsvalg (f.eks. om SecurityCenter skal spille av en lyd med et varsel eller vise McAfees velkomstskjerm ved oppstart).

I dette kapitlet

Vise og skjule informasjonsvarsler

Informasjonsvarsler gir deg beskjed når det oppstår hendelser som ikke utgjør en trussel mot datamaskinens sikkerhet. Hvis du f.eks. har installert Brannmurbeskyttelse vises som standard et informasjonsvarsel hver gang et program på datamaskinen blir gitt tilgang til Internett. Hvis du ikke vil at en bestemt type informasjonsvarsler skal vises, kan du skjule dem. Hvis du ikke vil at noen informasjonsvarsler skal vises, kan du skjule alle. Du kan også skjule alle informasjonsvarsler når du spiller spill i fullskjermmodus på datamaskinen. Når du er ferdig med spillet og går ut av fullskjermmodus fortsetter SecurityCenter å vise informasjonsvarsler.

Hvis du skjuler et informasjonsvarsel ved et uhell, kan du vise det igjen når som helst. Som standardinnstilling viser SecurityCenter alle informasjonsvarsler.

Vise eller skjule informasjonsvarsler

Du kan konfigurere SecurityCenter til å vise noen informasjonsvarsler og skjule andre, eller til å skjule alle informasjonsvarsler.

1 Åpne ruten Varslingsalternativer.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
3. Under **Varsler** klikker du **Avansert**.

2 I ruten SecurityCenter-konfigurasjon klikker du på **Informasjonsvarsler**.

3 I ruten Informasjonsvarsler gjør du følgende:

- Hvis du vil vise et informasjonsvarsel, fjerner du merket i avmerkingsboksen.
- Hvis du vil skjule et informasjonsvarsel, merker du av i avmerkingsboksen.
- Hvis du vil skjule alle informasjonsvarsler merker du av i boksen **Ikke vis informasjonsvarsler**.

4 Klikk **OK**.

Tips: Du kan også skjule et informasjonsvarsel ved å merke av i boksen **Ikke vis dette varslet igjen** i selve varslet. Hvis du gjør dette kan du vise informasjonsvarslet igjen ved å fjerne merket i den korresponderende avmerkingsboksen i ruten Informasjonsvarsler.

Vise eller skjule informasjonsvarsler når du spiller

Du kan skjule informasjonsvarsler når du spiller spill i fullskjermmodus på datamaskinen. Når du er ferdig med spillet og går ut av fullskjermmodus fortsetter SecurityCenter å vise informasjonsvarsler igjen.

1 Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.

2 I ruten Varslingsalternativer merker du av eller fjerner merket i boksen **Show informational alerts when gaming mode is detected**.

3 Klikk **OK**.

Konfigurere varslingsalternativer

Varslenes visning og hyppighet konfigureres av SecurityCenter; du kan imidlertid justere noen grunnleggende varslingsalternativer. Du kan f.eks. spille av en lyd med varsler eller skjule velkomstskjermvarslet når Windows starter. Du kan også skjule varsler som melder fra om virusutbrudd og andre sikkerhetstrusler i Internett-samfunn.

Spille av en lyd med varsler

Hvis du vil ha en hørbar indikasjon på at et varsel har oppstått, kan du konfigurere SecurityCenter til å spille av en lyd med hvert varsel.

1 Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.

2 Under **Lyd** i ruten Varslingsalternativer merker du av i boksen for **Spill av en lyd når det oppstår varsler**.

Skjule velkomstskjermen ved oppstart

Som standardinnstilling vises McAfees velkomstskjerm kort når Windows starter, for å informere deg om at SecurityCenter beskytter datamaskinen. Du kan imidlertid skjule velkomstskjermen hvis du ikke vil at den skal vises.

1 Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.

2 Under **Velkomstskjerm** i ruten Varslingsalternativer fjerner du merket i boksen for **Vis McAfees velkomstskjerm når Windows starter**.

Tips: Du kan når som helst vise velkomstskjermen igjen ved å merke av i boksen for **Vis McAfees velkomstskjerm når Windows starter**.

Skjule virusutbrudd-varsler

Du kan skjule varsler som melder fra om virusutbrudd og andre sikkerhetstrusler i Internett-samfunn.

1 Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.

2 I ruten Varslingsalternativer fjerner du merket i boksen **Varsle meg når det oppstår et virus eller en sikkerhetstrussel**.

Tips: Du kan vise virusutbrudd-varsler når som helst ved å merke av i boksen **Varsle meg når det oppstår et virus eller en sikkerhetstrussel**.

Skjule sikkerhetsmeldinger

Du kan skjule sikkerhetsvarsler om å beskytte flere datamaskiner på hjemmenettverket. Disse meldingene gir informasjon om abonnementet, antall datamaskiner du kan beskytte med abonnementet og hvordan du kan utvide abonnementet til å beskytte enda flere datamaskiner.

1 Åpne ruten Varslingsalternativer.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
3. Under **Varsler** klikker du **Avansert**.

2 I ruten Varslingsalternativer fjerner du merket i boksen **Vis virusveiledninger eller andre sikkerhetsmeldinger**.

Tips: Du kan vise disse sikkerhetsmeldingene når som helst ved å merke av for **Vis virusveiledninger eller andre sikkerhetsmeldinger**.

KAPITTEL 7

Vise hendelser

En hendelse er en handling eller konfigurasjonsendring som oppstår i en beskyttelseskategori og dens tilknyttede beskyttelsestjenester. Ulike beskyttelsestjenester registrerer ulike typer hendelser. For eksempel registrerer SecurityCenter en hendelse hvis en beskyttelsestjeneste blir aktivert eller deaktivert; Virusbeskyttelse registrerer en hendelse hver gang et virus blir oppdaget og fjernet, og Brannmurbeskyttelse registrerer en hendelse hver gang et forsøk på å koble til Internett blir blokkert. For mer informasjon om beskyttelseskategorier, se Forstå beskyttelseskategorier (side 9).

Du kan se hendelser når du foretar feilsøking i konfigureringsspørsmål og går gjennom handlinger utført av andre brukere. Mange foreldre bruker hendelsesloggen til å overvåke barnas oppførsel på Internett. Hvis du kun vil undersøke de siste 30 hendelsene som har oppstått, viser du nyeste hendelser. Hvis du vil undersøke en omfattende liste over alle hendelser som har oppstått, viser du alle hendelser. Når du viser alle hendelser, åpner SecurityCenter hendelsesloggen, som sorterer hendelser etter beskyttelseskategoriene de oppsto i.

I dette kapitlet

Vise nylige hendelser

Hvis du kun vil undersøke de siste 30 hendelsene som har oppstått, viser du nyeste hendelser.

- Under **Vanlige oppgaver,** klikker du **Vis nyeste hendelser**.

Vise alle hendelser

Hvis du vil undersøke en omfattende liste over alle hendelser som har oppstått, viser du alle hendelser.

1. Under **Vanlige oppgaver,** klikker du **Vis nyeste hendelser**.
2. Klikk **Vis logg** i ruten Nylige hendelser.
3. I hendelsesloggens venstre rute klikker du hvilke typer hendelser du vil vise.

KAPITTEL 8

McAfee VirusScan

VirusScan tilbyr avanserte tjenester for oppdagelse og beskyttelse som forsvarer deg og din datamaskin mot de siste sikkerhetstruslene, inkludert virus, trojanske hester, informasjonskapsler for sporing, spion- og reklameprogrammer og andre potensielt uønskede programmer. Med VirusScan rekker beskyttelsen lenger enn filene og mappene på din stasjonære eller bærbare datamaskin, og programmet går etter trusler fra ulike inngangspunkt, inkludert e-post, direktemeldinger og Internett.

Med VirusScan er beskyttelsen av datamaskinen din øyeblikkelig og konstant (krever ingen langtekkelig administrering). Mens du arbeider, spiller, surfer på Internett eller leser e-post kjører det i bakgrunnen og overvåker, søker etter og oppdager potensielle skader i sanntid. Omfattende søk gjennomføres etter tidsskjema og sjekker datamaskinen din jevnlig ved bruk av et avansert sett alternativer. VirusScan gir deg fleksibilitet til å tilpasse hvordan programmet skal fungere, men selv om du ikke gjør det vil datamaskinen din likevel være beskyttet.

Ved normal bruk av datamaskinen kan virus, ormer og and potensielle trusler infiltrere datamaskinen. Dersom dette skjer varsler VirusScan deg om trusselen, men vil vanligvis ta seg av den for deg ved å fjerne eller isolere infiserte elementer før skade oppstår. Selv om det er sjelden, kan videre handling noen ganger være nødvendig. I slike tilfeller lar VirusScan deg bestemme hva du skal gjøre (søke på nytt neste gang du slår på datamaskinen, beholde det oppdagede elementet eller fjerne det oppdagede elementet).

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

VirusScan-funksjoner

Omfattende virusbeskyttelse

Forsvar deg selv og datamaskinen mot de nyeste sikkerhetstruslene, inkludert virus, trojanske hester, sporingsinformasjonskapsler, spionprogrammer, reklameprogrammer og andre potensielt uønskede programmer. Beskyttelsen rekker lenger enn filene og mappene på din datamaskin, og programmet går etter trusler fra ulike inngangspunkt, inkludert e-post, direktemeldinger og Internett. Krever ingen langtekkelig administrering.

Ressursbevisste søkealternativer

Du kan tilpasse søkealternativene hvis du ønsker, men selv om du ikke gjør det vil datamaskinen din likevel være beskyttet. Hvis du opplever lav søkehastighet kan du deaktivere alternativet for minimal bruk av datamaskinressurser, men husk at virusbeskyttelse vil bli høyere prioritert enn andre oppgaver.

Automatiske reparasjoner

Hvis VirusScan oppdager en sikkerhetstrussel under et søk, vil det automatisk forsøke å behandle trusselen etter hvilken type trussel det er. På denne måten kan de fleste trusler oppdages og nøytraliseres uten at du trenger å gjøre noe. Selv om det er sjelden, hender det at VirusScan ikke kan nøytralisere en trussel selv. I slike tilfeller lar VirusScan deg bestemme hva du skal gjøre (søke på nytt neste gang du slår på datamaskinen, beholde det oppdagede elementet eller fjerne det oppdagede elementet).

Midlertidig stans av oppgaver i fullskjermmodus

Når du gjør ting som å se film, spille dataspill eller annen aktivitet som opptar hele dataskjermen, stopper VirusScan midlertidig en rekke oppgaver, inkludert manuelle søk.

KAPITTEL 9

Gjennomsøke datamaskinen

Selv før du starter SecurityCenter første gang, begynner sanntidsvirusbeskyttelsen i VirusScan å beskytte datamaskinen mot potensielt skadelige virus, trojanske hester og andre sikkerhetstrusler. Dersom du ikke deaktiverer sanntidsvirusbeskyttelse, vil VirusScan kontinuerlig overvåke datamaskinen for virusaktivitet og gjennomsøke filer hver gang du eller datamaskinen åpner dem ved å bruke alternativene for sanntidssøk som du har valgt. Du bør la sanntidsvirusbeskyttelse være på og lage en tidsplan for faste, mer omfattende manuelle søk for å sikre at datamaskinen er beskyttet mot de siste sikkerhetstruslene. For mer informasjon om innstilling av søkealternativer, kan du se Konfigurere virusbeskyttelse (side 45).

VirusScan tilbyr et detaljert sett søkealternativer for virusbeskyttelse, som lar deg utføre mer omfattende søk regelmessig. Du kan kjøre fulle, raske, egendefinerte eller planlagte søk fra SecurityCenter. Du kan også utføre manuelle søk i Windows Utforsker mens du arbeider. Søking i SecurityCenter har den fordelen at du kan endre søkealternativer i full fart. Søking fra Windows Utforsker tilbyr imidlertid en praktisk tilnærming til datasikkerhet.

Uansett om du utfører søk fra SecurityCenter eller Windows Utforsker kan du se søkeresultatene når søket er ferdig. Du kan bruke søkeresultatene for å se om VirusScan har oppdaget, reparert eller isolert virus, trojanske hester, spion- og reklameprogrammer, informasjonskapsler og andre potensielt uønskede programmer. Søkeresultatene kan vises på flere måter. Du kan for eksempel se et sammendrag av søkeresultatene eller detaljert informasjon, som f.eks. infeksjonens status og type. Du kan også se generell statistikk for søk og oppdagelser.

I dette kapitlet

Gjennomsøke PC-en

VirusScan inneholder et fullstendig sett søkealternativer for virusbeskyttelse, inkludert sanntidssøk (som konstant overvåker PC-en for trusselaktivitet), manuelt søk fra Windows Utforsker, samt fullstendig, raskt, egendefinert eller planlagt søk fra SecurityCenter.

For å...	Gjør dette ...
Starte sanntidssøk for konstant å overvåke datamaskinen for virusaktivitet og gjennomsøke filer hver gang du eller datamaskinen bruker dem	1. Åpne konfigurasjonsruten for Datamaskin og filer Hvordan? 1. Klikk på **Avansert meny** i den venstre ruten. 2. Klikk på **Konfigurer**. 3. Klikk **Datamaskin og filer** i Konfigurer-ruten. 2. Klikk **På** under **Virusbeskyttelse**. **Merk**: Sanntidssøk er som standard deaktivert.
Starte Hurtigskanning for raskt å se etter trusler på datamaskinen	1. Klikk **Søk** i Grunnleggende-menyen. 2. Klikk **Start** under Hurtigskanning i ruten Søkealternativer.
Starte Komplett skanning for grundig å se etter trusler på datamaskinen	1. Klikk **Søk** i Grunnleggende-menyen. 2. Klikk **Start** under Komplett skanning i ruten Søkealternativer.
Starte Egendefinert skanning basert på dine egne innstillinger	1. Klikk **Søk** i Grunnleggende-menyen. 2. Klikk **Start** under La meg velge i ruten Søkealternativer. 3. Tilpass søket ved å merke eller fjerne merket for følgende: **Alle trusler i alle filer** **Ukjente virus** **Arkivfiler** **Spionprogrammer og potensielle trusler** **Sporingsinformasjonskapsler** **Skjulte programmer** 4. Klikk **Start**.

For å...	Gjør dette ...
Starte Manuell skanning for å se etter trusler i filer, mapper eller stasjoner	1. Åpne Windows Utforsker. 2. Høyreklikk en fil, mappe eller stasjon og klikk deretter **Søk**.
Starte Planlagt skanning som med jevne mellomrom søker etter trusler på datamaskinen	1. Åpne ruten for Planlagt søk. Hvordan? 1. Under **Vanlige oppgaver** klikker du **Hjem**. 2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter. 3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**. 4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**. 5. Klikk på **Planlagt søk** i ruten Virusbeskyttelse. 2. Velg **Aktiver planlagt søk**. 3. For å redusere mengden prosessorkraft som vanligvis brukes til søking, velger du **Utfør søk med minimal bruk av datamaskinressurser**. 4. Velg en eller flere dager. 5. Spesifiser starttidspunkt. 6. Klikk **OK**.

Søkeresultatene vises i varselet for Søk fullført. Resultatene består av antallet gjennomsøkte, oppdagede, reparerte, ignorerte og fjernede elementer. Klikk **Vis søkedetaljer** for å lese mer om søkeresultatene eller arbeide med infiserte elementer.

Merk: Se Søketyper (side 38) for å lære mer om søkealternativer.

Vise søkeresultater

Når et søk er ferdig kan du vise resultatene for å se hva søket fant og for å analysere datamaskinens gjeldende beskyttelsesstatus. Søkeresultatene forteller deg om VirusScan har oppdaget, reparert eller isolert virus, trojanske hester, spion- og reklameprogrammer, informasjonskapsler og andre potensielt uønskede programmer.

I Grunnleggende- eller Avansert-meny klikker du **Søk** og gjør så ett av følgende:

For å...	Gjør dette ...
Vise søkeresultater i varslet	Vise søkeresultater i varslet for Søk fullført.
Vise mer informasjon om søkeresultater	Klikk **Vis søkedetaljer** i varslet for Søk fullført.
Vise et kort sammendrag av søkeresultatene	Pek på ikonet for **Søk fullført** i systemstatusfeltet på oppgavelinjen.
Vise statistikk for søk og oppdagelse	Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen på oppgavelinjen.
Vise detaljer om oppdagede elementer, infeksjonsstatus og -type	1. Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen på oppgavelinjen. 2. Klikk **Detaljer** i ruten Komplett skanning, Hurtigskanning, Egendefinert skanning eller Manuell skanning.
Vise detaljer om det siste søket	Dobbeltklikk ikonet **Søk fullført** i systemstatusfeltet på oppgavelinjen, og vis detaljene for det siste søket under Ditt søk i ruten Komplett skanning, Hurtigskanning, Egendefinert skanning eller Manuell skanning.

KAPITTEL 10

Arbeide med søkeresultater

Hvis VirusScan oppdager en sikkerhetstrussel under et søk, vil det automatisk forsøke å behandle trusselen etter hvilken type trussel det er. Hvis VirusScan for eksempel oppdager et virus, trojansk hest eller informasjonskapsel for sporing på datamaskinen, forsøker det å rense den infiserte filen. VirusScan isolerer alltid en fil før det blir utført et renseforsøk. Hvis filen ikke kan renses, blir den isolert.

Noen sikkerhetstrusler kan det hende VirusScan ikke kan rense eller isolere. Hvis dette skjer, vil VirusScan be deg om å behandle trusselen. Du kan foreta ulike handlinger avhengig av typen trussel. Hvis for eksempel et virus blir oppdaget i en fil, og VirusScan ikke kan rense eller isolere filen, nekter den adgang til filen. Hvis informasjonskapsler for sporing blir oppdaget, og VirusScan ikke kan rense eller isolere informasjonskapslene, kan du bestemme om de skal fjernes eller klareres. Hvis potensielt uønskede programmer blir oppdaget, foretar ikke VirusScan seg noe umiddelbart. I stedet lar det deg bestemme om programmet skal isoleres eller klareres.

Når VirusScan isolerer elementer, krypterer og isolerer det elementene i en mappe for å hindre filene, programmene eller informasjonskapslene fra å skade datamaskinen. Du kan gjenopprette eller fjerne de isolerte elementene. I de fleste tilfeller kan du slette en isolert informasjonskapsel uten å påvirke systemet. Hvis VirusScan derimot har isolert et program du gjenkjenner og bruker, bør du vurdere å gjenopprette det.

I dette kapitlet

Arbeide med virus og trojanske hester

Hvis VirusScan oppdager et virus eller en trojansk hest på datamaskinen, forsøker det å rense filen. Hvis filen ikke kan renses, forsøker VirusScan å isolere den. Hvis dette heller ikke går, nektes det adgang til filen (kun i sanntidssøk).

1 Åpne ruten Søkeresultater.

Hvordan?

1. Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen helt til høyre på oppgavelinjen.
2. I Søkeframdrift: Ruten Manuelt søk, klikk på **Vis resultater**.

2 I listen over søkeresultater klikker du **Virus og trojanske hester**.

Merk: Hvis du vil arbeide med filene VirusScan har isolert, se Arbeide med isolerte filer (side 36).

Arbeide med potensielt uønskede programmer

Hvis VirusScan oppdager et potensielt uønsket program på datamaskinen, kan du enten fjerne eller klarere programmet. Hvis du ikke gjenkjenner programmet, bør du vurdere å fjerne det. Å fjerne et potensielt uønsket program sletter det ikke fra systemet. I stedet isoleres programmet for å hindre at det skader datamaskinen eller filer.

1 Åpne ruten Søkeresultater.

Hvordan?

1. Dobbelklikk **Søk fullført**-ikonet i informasjonsdelen helt til høyre på oppgavelinjen.
2. I Søkeframdrift: Ruten Manuelt søk, klikk på **Vis resultater**.

2 I listen over søkeresultater klikker du **Potensielt uønskede programmer.**

3 Velg et potensielt uønsket program.

4 Under **Jeg vil** klikker du enten **Fjern** eller **Klarer**.

5 Bekreft valget.

Arbeide med isolerte filer

Når VirusScan isolerer infiserte filer, krypterer og flytter det filene til en mappe for å hindre dem i å skade datamaskinen. Du kan deretter gjenopprette eller fjerne de isolerte elementene.

1 Åpne ruten Isolerte filer.

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Gjenopprett**.
3. Klikk på **Filer**.

2 Velg en isolert fil.

3 Gjør ett av følgende:

- Hvis du vil reparere den infiserte filen og flytte den tilbake til sin opprinnelige plassering på datamaskinen, klikker du **Gjenopprett**.
- Hvis du vil fjerne den infiserte filen fra datamaskinen klikker du **Fjern**.

4 Klikk **Ja** for å bekrefte valget.

Tips: Du kan gjenopprette eller fjerne flere filer samtidig.

Arbeide med isolerte programmer og informasjonskapsler

Når VirusScan isolerer potensielt uønskede programmer eller informasjonskapsler for sporing, krypterer og flytter det dem til en beskyttet mappe for å hindre programmene eller informasjonskapslene i å skade datamaskinen. Du kan gjenopprette eller fjerne de isolerte elementene. I de fleste tilfeller kan du slette et isolert element uten at det påvirker systemet.

1 Åpne ruten Isolerte programmer og informasjonskapsler for sporing.

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Gjenopprett**.
3. Klikk på **Programmer og informasjonskapsler**.

2 Velg et isolert program eller informasjonskapsel.

3 Gjør ett av følgende:

- Hvis du vil reparere den infiserte filen og flytte den tilbake til sin opprinnelige plassering på datamaskinen, klikker du **Gjenopprett**.
- Hvis du vil fjerne den infiserte filen fra datamaskinen klikker du **Fjern**.

4 Klikk **Ja** for å bekrefte handlingen.

Tips: Du kan gjenopprette eller fjerne flere programmer og informasjonskapsler samtidig.

Søketyper

VirusScan inneholder et fullstendig sett søkealternativer for virusbeskyttelse, inkludert sanntidssøk (som konstant overvåker PC-en for trusselaktivitet), manuelt søk fra Windows Utforsker, samt muligheten til å kjøre et fullstendig, raskt, egendefinert søk fra SecurityCenter, eller angi når planlagte søk skal skje. Søking i SecurityCenter har den fordelen at du kan endre søkealternativer i full fart.

Sanntidssøk:

Sanntidsvirusbeskyttelse overvåker konstant datamaskinen for virusaktivitet, og gjennomsøker filer hver gang du eller datamaskinen din bruker dem. Du bør la sanntidsvirusbeskyttelse være på og lage en tidsplan for faste, mer omfattende manuelle søk for å sikre at datamaskinen er beskyttet mot de siste sikkerhetstruslene.

Du kan angi standardalternativer for sanntidssøk, som inkluderer søk etter ukjente virus og søk etter trusler i sporingsinformasjonskapsler og på nettverksstasjoner. Du kan også dra nytte av beskyttelse mot bufferoverløp, som er aktivert som standard (bortsett fra hvis du bruker et 64-bits Windows Vista-operativsystem). Se Konfigurere søkealternativer i sanntid (side 46) hvis du vil lære mer.

Hurtigskanning

Med Hurtigskanning kan du se etter trusselaktivitet i prosesser, viktige Windows-filer og andre utsatte områder på datamaskinen.

Komplett skanning

Med Komplett skanning kan du grundig sjekke hele datamaskinen for virus, spionprogrammer og andre sikkerhetstrusler overalt på PC-en.

Egendefinert skanning

Med Egendefinert skanning kan du velge egne søkeinnstillinger for sjekk etter trusselaktivitet på PC-en. Alternativene for Egendefinert skanning inkluderer søk etter trusler i alle filer, i arkivfiler samt i informasjonskapsler, i tillegg til søk etter ukjente virus, spionvare og skjulte programmer.

Du kan angi standardalternativer for egendefinerte søk, som inkluderer søk etter ukjente virus, arkivfiler, spionvare og potensielle trusler, sporingsinformasjonskapsler og skjulte programmer. Du kan også søke ved å bruke minimale datamaskinressurser. Se Konfigurere alternativer for egendefinert søk (side 48) hvis du vil lære mer.

Manuell skanning

Med Manuell skanning kan du raskt se etter trusler i filer, mapper og stasjoner fra Windows Utforsker.

Planlagt skanning

Planlagte søk gjennomfører grundige søk på datamaskinen etter virus og andre trusler hvilken som helst dag og tidspunkt i uken. Planlagte søk gjennomsøker alltid hele datamaskinen ved å bruke standardinnstillingene for søk. Som standardinnstilling utfører VirusScan et planlagt søk en gang i uken. Hvis du opplever lav søkehastighet kan du deaktivere alternativet for minimal bruk av datamaskinressurser, men husk at virusbeskyttelse vil bli høyere prioritert enn andre oppgaver. Se Planlegge et søk (side 51) hvis du vil lære mer.

Merk: Se Gjennomsøke PC-en (side 32) for å lære hvordan du starter søkealternativet som passer best for deg.

KAPITTEL 11

Bruke tilleggsbeskyttelse

I tillegg til sanntidsvirusbeskyttelse gir VirusScan avansert beskyttelse mot skript, spionprogrammer og potensielt skadelige vedlegg til e-post og direktemeldinger. Som standardinnstilling er skriptsøking, spionprogram-, e-post- og direktemeldingsbeskyttelse slått på og beskytter datamaskinen.

Skriptsøkbeskyttelse

Skriptsøkbeskyttelse oppdager potensielt skadelige skript og hindrer dem i å kjøre på datamaskinen eller i webleseren. Den overvåker datamaskinen for mistenkelig skriptaktivitet, slik som skript som oppretter, kopierer eller sletter filer eller åpner Windows-registeret, og varsler deg før det oppstår skade.

Spionprogrambeskyttelse

Spionprogrambeskyttelse oppdager spionprogrammer og andre potensielt uønskede programmer. Spionprogrammer er programvare som installeres på datamaskinen i hemmelighet for å overvåke din atferd, samle inn personlig informasjon og til og med forstyrre din kontroll over datamaskinen ved å installere tilleggsprogramvare eller omdirigere webleseraktivitet.

E-postbeskyttelse

E-postbeskyttelse oppdager mistenkelig aktivitet i e-post og vedlegg du sender.

Direktemeldingsbeskyttelse

Direktemeldingsbeskyttelse oppdager potensielle sikkerhetstrusler fra direktemeldingsvedlegg du mottar. Den hindrer også direktemeldingsprogrammer i å dele personlig informasjon.

I dette kapitlet

Starte skriptsøkbeskyttelse

Slå på skriptsøkbeskyttelse for å oppdage potensielt skadelige skript og hindre dem i å kjøre på datamaskinen din. Skriptsøkbeskyttelse varsler deg når et skript forsøker å lage, kopiere eller slette filer på datamaskinen eller gjøre endringer i Windows-registret.

1 Åpne konfigurasjonsruten for Datamaskin og filer

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **På** under **Skriptsøkbeskyttelse**.

Merk: Selv om du kan slå av skriptsøkbeskyttelse når som helst, vil det gjøre at datamaskinen er sårbar overfor skadelige skript.

Starte spionprogrambeskyttelse

Slå på spionprogrambeskyttelse for å oppdage og fjerne spion- og reklameprogrammer og andre potensielle uønskede programmer som samler og overfører informasjon uten at du vet det eller har tillat det.

1 Åpne konfigurasjonsruten for Datamaskin og filer

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **På** under **Skriptsøkbeskyttelse**.

Merk: Selv om du kan slå av spionprogrambeskyttelse når som helst, vil det gjøre at datamaskinen er sårbar overfor skadelige skript.

Starte e-postbeskyttelse

Slå på e-post-beskyttelse for å oppdage både ormer og potensielle trusler i utgående (SMTP) og innkommende (POP) e-postmeldinger og vedlegg.

1 Åpne konfigurasjonsruten for E-post og direktemeldinger

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **E-post og direktemeldinger** i ruten Konfigurer.

2 Under **E-postbeskyttelse** klikker du **På**.

Merk: Selv om du kan slå av e-post-beskyttelse når som helst, vil det gjøre at datamaskinen er sårbar overfor e-posttrusler.

Starte beskyttelse av direktemeldinger

Slå på beskyttelse av direktemeldinger for å oppdage sikkerhetstrusler som kan være inkludert i innkommende direktemeldingsvedlegg.

1 Åpne konfigurasjonsruten for E-post og direktemeldinger

Hvordan?

1. Klikk på **Avansert meny** i den venstre ruten.
2. Klikk på **Konfigurer**.
3. Klikk **E-post og direktemeldinger** i ruten Konfigurer.

2 Under **Beskyttelse av direktemeldinger** klikker du **På**.

Merk: Selv om du kan slå av beskyttelse av direktemeldinger når som helst, vil det gjøre at datamaskinen er sårbar overfor skadelige direktemeldingsvedlegg.

KAPITTEL 12

Konfigurere virusbeskyttelse

Du kan angi ulike alternativer for planlagt søk, egendefinert søk og sanntidssøk. For eksempel, siden sanntidsbeskyttelse kontinuerlig overvåker datamaskinen, kan du velge et bestemt sett grunnleggende søkealternativer og reservere et mer omfattende sett søkealternativer for manuell beskyttelse på forespørsel.

Du kan også bestemme hvordan VirusScan skal overvåke og behandle potensielle uautoriserte eller uønskede endringer på PC-en ved hjelp av SystemGuards og klarerte lister. Systemguards overvåker, logger, rapporterer og administrerer potensielle uautoriserte endringer som er gjort i Windows-registeret eller kritiske systemfiler på datamaskinen. Uautoriserte endringer i register og filer kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler. Du kan bruke Klarerte lister til å bestemme om du vil klarere eller fjerne regler som finner fil- eller registerendringer (SystemGuard), programmer eller bufferoverløp. Hvis du klarerer elementet og sier at du ikke vil motta flere meldinger om elementets aktivitet, blir elementet lagt til i en klarert liste og VirusScan vil ikke lenger oppdage det eller melde fra om aktiviteten til det.

I dette kapitlet

Konfigurere søkealternativer i sanntid

Når du starter sanntids virusbeskyttelse bruker VirusScan standardinnstilte alternativer for å gjennomsøke filer; du kan imidlertid endre standardinnstillingene slik at de passer ditt behov.

For å endre sanntids søkealternativer må du bestemme hva VirusScan skal se etter under et søk, samt plasseringen og filtypene det skal gjennomsøke. For eksempel kan du bestemme om VirusScan søker etter ukjente virus eller informasjonskapsler som brukes av webområder til å spore din atferd, og om det skal søke på nettverkstasjoner som er tilordnet datamaskinen din eller bare lokale stasjoner. Du kan også bestemme hva slags type filer som skal gjennomsøkes (alle filer, eller kun programfiler og dokumenter, siden det er der det oppdages flest virus).

Når du endrer sanntids søkealternativer må du også bestemme om det er viktig for datamaskinen å ha beskyttelse mot bufferoverløp. En buffer er en del av minnet som brukes til å midlertidig lagre datainformasjon. Bufferoverløp kan forekomme når mengden informasjon mistenkelige programmer eller prosesser lagrer i en buffer overstiger bufferens kapasitet. Når dette skjer, blir datamaskinen din mer sårbar overfor sikkerhetsangrep.

Konfigurere alternativer for sanntidssøk

Du konfigurerer alternativer for sanntidssøk for å tilpasse hva VirusScan søker etter under et sanntidssøk, samt plasseringene og filtypene det gjennomsøker. Alternativer inkluderer å søke etter ukjente virus og informasjonskapsler for sporing, samt beskytte mot bufferoverløp. Du kan også konfigurere sanntidssøk til å gjennomsøke nettverksstasjoner som er tilordnet datamaskinen din.

1 Åpne ruten for Sanntidssøk.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.

2 Spesifiser alternativene for sanntidssøk og klikk deretter **OK**.

For å...	Gjør dette ...
Oppdage ukjente virus og nye varianter av kjente virus	Velg **Søk etter ukjente virus**.
Oppdage informasjonskapsler	Velg **Søk etter og fjern informasjonskapsler for sporing**.
Oppdage virus og andre potensielle trusler på stasjoner som er tilkoblet nettverket ditt	Velg **Søk gjennom nettverksstasjoner**.
Beskytte datamaskinen mot bufferoverløp	Velg **Aktiver beskyttelse mot bufferoverløp**.
Angi hvilke typer filer som skal gjennomsøkes	Klikk enten **Alle filer (anbefales)** eller **Bare programfiler og dokumenter**.

Stoppe sanntidsvirusbeskyttelse

Selv om det er sjelden, kan det hende at du ønsker å midlertidig stoppe sanntidssøking (for eksempel for å endre søkealternativer eller utføre feilsøking angående et ytelsesproblem). Når sanntidsvirusbeskyttelse er deaktivert, er ikke datamaskinen din beskyttet og beskyttelsesstatusen i SecurityCenter er rød. For mer informasjon om beskyttelsesstatus, se Forstå beskyttelsesstatus i Hjelp for SecurityCenter.

Du kan slå av sanntidsvirusbeskyttelse midlertidig og bestemme når den skal starte igjen. Du kan automatisk gjenoppta beskyttelse etter 15, 30, 45 eller 60 minutter, når du slår på datamaskinen igjen eller aldri.

1 Åpne konfigurasjonsruten for Datamaskin og filer

   Hvordan?

   1. Klikk på **Avansert meny** i den venstre ruten.
   2. Klikk på **Konfigurer**.
   3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **Av** under **Virusbeskyttelse**.

3 I dialogboksen velger du når sanntidssøking skal gjenopptas.

4 Klikk **OK**.

Konfigurere alternativer for egendefinert søk

Med egendefinert virusbeskyttelse kan du gjennomsøke filer på forespørsel. Når du starter et egendefinert søk, gjennomsøker VirusScan datamaskinen for virus og andre potensielt skadelige elementer ved å bruke et mer omfattende sett søkealternativer. Hvis du vil endre alternativene for egendefinert søk, må du bestemme hva VirusScan skal se etter under et søk. Du kan for eksempel bestemme om VirusScan skal se etter ukjente virus, potensielt uønskede programmer som f.eks. spion- eller reklameprogrammer, skjulte programmer og rootkits (som kan gi uautorisert tilgang til datamaskinen), og informasjonskapsler som webområder kan bruke til å spore atferden din. Du må også bestemme hvilke typer filer som skal gjennomsøkes. For eksempel kan du bestemme om VirusScan skal gjennomsøke alle filer eller bare programfiler og dokumenter (siden det er her det oppdages flest virus). Du kan også bestemme om komprimerte filer (f.eks. .zip-filer) skal inkluderes i søket.

Som standard gjennomsøker VirusScan alle stasjoner og mapper på datamaskinen og alle nettverksstasjoner hver gang det kjører et egendefinert søk. Du kan imidlertid endre standardplasseringene slik at de passer til ditt behov. Du kan for eksempel gjennomsøke bare viktige PC-filer, elementer på skrivebordet eller elementer i Programfiler-mappen. Hvis du ikke vil ha ansvaret for å starte hvert egendefinerte søk selv, kan du lage en fast tidsplan for søk. Planlagte søk gjennomsøker alltid hele datamaskinen ved å bruke standardinnstillingene for søk. Som standardinnstilling utfører VirusScan et planlagt søk en gang i uken.

Hvis du opplever lav søkehastighet kan du deaktivere alternativet for minimal bruk av datamaskinressurser, men husk at virusbeskyttelse vil bli høyere prioritert enn andre oppgaver.

Merk: Når du gjør ting som å se film, spille dataspill eller annen aktivitet som opptar hele dataskjermen, stopper VirusScan midlertidig en rekke oppgaver, inkludert automatiske oppdateringer og egendefinerte søk.

Konfigurere alternativer for egendefinert søk

Du konfigurerer alternativer for egendefinert søk for å tilpasse hva VirusScan søker etter under et egendefinert søk, samt plasseringene og filtypene det gjennomsøker. Alternativer inkluderer søk etter ukjente virus, komprimerte filer, spionprogrammer og potensielt uønskede programmer, informasjonskapsler for sporing, rootkits og skjulte programmer. Du kan også angi en egendefinert plassering for søk for å bestemme hvor VirusScan skal søke etter virus og andre skadelige elementer under et egendefinert søk. Du kan gjennomsøke alle filer, mapper og stasjoner på datamaskinen eller du kan begrense søket til bestemte mapper og stasjoner.

1 Åpne ruten for egendefinert søk.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.
5. Klikk på **Manuelt søk** i ruten Virusbeskyttelse.

2 Spesifiser alternativene for egendefinert søk og klikk deretter **OK**.

For å...	Gjør dette ...
Oppdage ukjente virus og nye varianter av kjente virus	Velg **Søk etter ukjente virus**.
Oppdage og fjerne virus i ZIP-filer og andre komprimerte filer.	Velg **Søk i arkiverte filer**.
Oppdage spion- og reklameprogrammer og andre potensielle uønskede programmer.	Velg **Søk etter spionprogrammer og potensielle trusler**.
Oppdage informasjonskapsler	Velg **Søk etter og fjern informasjonskapsler for sporing**.
Oppdage rootkits og skjulte programmer som kan endre og utnytte eksisterende systemfiler for Windows	Velg **Søk etter skjulte programmer**.

For å...	Gjør dette ...
Bruke mindre prossessorkraft for søk og prioritere andre oppgaver høyere (som f.eks. weblesing eller åpning av dokumenter)	Velg **Søk som bruker minimale datamaskinressurser**.
Angi hvilke typer filer som skal gjennomsøkes	Klikk enten **Alle filer (anbefales)** eller **Bare programfiler og dokumenter**.

3 Klikk **Standard plassering som skal gjennomsøkes**, merk av eller fjern merket for plasseringer du vil gjennomsøke eller hoppe over, og klikk deretter **OK**:

For å...	Gjør dette ...
Gjennomsøke aller filer og mapper på datamaskinen	Velg **(Min)Datamaskin**.
Gjennomsøke bestemte filer, mapper og stasjoner på datamaskinen	Fjern merket i boksen for **(Min)Datamaskin** og velg en eller flere mapper eller stasjoner.
Gjennomsøke kritiske systemfiler	Fjern merket i boksen for **(Min)Datamaskin** og merk deretter av i boksen for **Kritiske systemfiler**.

Planlegge et søk

Planlegg søk for å gjennomføre et grundig søk av datamaskinen etter virus og andre trusler hvilken som helst dag og tidspunkt i uken. Planlagte søk gjennomsøker alltid hele datamaskinen ved å bruke standardinnstillingene for søk. Som standardinnstilling utfører VirusScan et planlagt søk en gang i uken. Hvis du opplever lav søkehastighet kan du deaktivere alternativet for minimal bruk av datamaskinressurser, men husk at virusbeskyttelse vil bli høyere prioritert enn andre oppgaver.

Planlegg søk som grundig gjennomsøker hele datamaskinen for virus og andre trusler ved å bruke standardinnstillingene for søk. Som standardinnstilling utfører VirusScan et planlagt søk en gang i uken.

1 Åpne ruten for Planlagt søk.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
   3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
   4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.
   5. Klikk på **Planlagt søk** i ruten Virusbeskyttelse.

2 Velg **Aktiver planlagt søk**.

3 For å redusere mengden prosessorkraft som vanligvis brukes til søking velger du **Utfør søk med minimal bruk av datamaskinressurser**.

4 Velg en eller flere dager.

5 Spesifiser starttidspunkt.

6 Klikk **OK**.

Tips: Du kan gjenopprette standardtidsplanen ved å klikke **Tilbakestill**.

Bruke alternativer for SystemGuards

Systemguards overvåker, logger, rapporterer og administrerer potensielle uautoriserte endringer som er gjort i Windows-registret eller kritiske systemfiler på datamaskinen. Uautoriserte endringer i register og filer kans kade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.

Endringer i register og filer er vanlig og oppstår regelmessig på datamaskinen. Siden mange er uskadelige, er SystemGuards' standardinnstillinger konfigurert til å sørge for pålitelig, intelligent og ekte beskyttelse mot uautoriserte endringer som kan være skadelige. For eksempel, når SystemGuards oppdager uvanlige endringer som kan være en mulig trussel, blir aktiviteten øyeblikkelig rapportert og registrert. Mer vanlige endringer som likevel kan være en trussel, blir kun registrert. Som standardinnstilling er imidlertid overvåking av standardendringer og endringer med lav risiko deaktivert. SystemGuards-teknologien kan konfigureres til å utvide beskyttelsen til et hvilket som helst miljø.

Det finnes tre typer SystemGuards: SystemGuards for programmer, SystemGuards for Windows og SystemGuards for webleser.

SystemGuards for programmer

SystemGuards for programmer oppdager potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. Disse viktige registerelementene og filene er bl.a. ActiveX-installasjoner, oppstartselementer, shell execute hooks i Windows og shell service object delay loads. Ved å overvåke disse stopper SystemGuards for programmer mistenkelige ActiveX-programmer (nedlastet fra Internett) i tillegg til spionprogrammer og potensielle uønskede programmer som kan starte automatisk når Windows starter.

SystemGuards for Windows

SystemGuards for Windows oppdager også potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. Disse viktige registerelementene og filene er bl.a. hurtigmenystyring, appInit DLLs og Windows Hosts-filen. Ved å overvåke disse hjelper SystemGuards for Windows til med å hindre at datamaskinen din sender og mottar uautorisert eller personlig informasjon over Internett. Det hjelper også til med å stoppe programmer som kan komme med uventede endringer i utseendet og atferden til programmer som er viktige for deg og din familie.

SystemGuards for webleser

Akkurat som SystemGuards for programmer og Windows oppdager også SystemGuards for webleser potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. SystemGuards for webleser overvåker derimot endringer i viktige registerelementer og filer som f.eks. Internet Explorer-tillegg, Internet Explorer URL-er og Internett Explorer sikkerhetssoner. Ved å overvåke disse, hjelper SystemGuards for webleser til med å hindre uautorisert webleseraktivitet, som f.eks. videresending til mistenkelige webområder, endringer i innstillinger og alternativer for webleser uten at du vet om det, og uønsket klarering av mistenkelige webområder.

Aktivere SystemGuards-beskyttelse

Aktiver SystemGuards-beskyttelse for å oppdage og bli varslet om potensielle uautoriserte endringer i Windows-register og filer på datamaskinen. Uautoriserte endringer i register og filer kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.

1 Åpne konfigurasjonsruten for Datamaskin og filer

   Hvordan?

   1. Klikk på **Avansert meny** i den venstre ruten.
   2. Klikk på **Konfigurer**.
   3. Klikk **Datamaskin og filer** i Konfigurer-ruten.

2 Klikk **På** under **SystemGuard-beskyttelse**.

Merknad: Du kan deaktivere SystemGuard-beskyttelse ved å klikke på **Av**.

Konfigurere alternativer for SystemGuards

Bruk ruten SystemGuards for å konfigurere beskyttelses-, logging- og varslingsalternativer mot uautoriserte register- og filendringer tilknyttet Windows-filer og -programmer og Internett Explorer. Uautoriserte endringer i register og filer kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.

1 Åpne ruten SystemGuards.

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at SystemGuard-beskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.

2 Velg en SystemGuards-type fra listen.

- **SystemGuards for programmer**
- **SystemGuards for Windows**
- **SystemGuards for webleser**

3 Under **Jeg vil** gjør du ett av følgende:

- Hvis du vil oppdage, logge og rapportere uautoriserte register- og filendringer tilknyttet SystemGuards for programmer, Windows og webleser, klikker du på **Vis varsler.**
- Hvis du vil oppdage og logge uautoriserte register- og filendringer tilknyttet SystemGuards for programmer, Windows og webleser, klikker du på **Bare logg endringer.**
- Hvis du vil deaktivere oppdaging av uautoriserte register- og filendringer tilknyttet SystemGuards for programmer, Windows og webleser, klikker du på **Deaktiver SystemGuard.**

Merk: For mer informasjon om SystemGuards-typer, se Om SystemGuards-typer (side 55).

Om SystemGuards-typer

SystemGuards oppdager potensielle uautoriserte endringer i datamaskinens register og andre kritiske filer som er viktige for Windows. Det finnes tre typer SystemGuards: SystemGuards for programmer, SystemGuards for Windows og SystemGuards for webleser.

SystemGuards for programmer

SystemGuards for programmer stopper mistenkelige ActiveX-programmer (nedlastet fra Internett) i tillegg til spionprogrammer og potensielle uønskede programmer som kan starte automatisk når Windows starter.

SystemGuard	Oppdager...
ActiveX-installasjoner	Uautoriserte registerendringer i ActiveX-installasjoner som kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.
Oppstartselementer	Spion- og reklameprogrammer og andre potensielle uønskede programmer som kan installere filendringer i oppstartselementer og lar mistenkelige programmer kjøre når du starter datamaskinen.
Shell Execute Hooks i Windows	Spion- og reklameprogrammer eller andre potensielt uønskede programmer som kan installere shell execute hooks for å hindre at sikkerhetsprogrammer kjøres.
Shell Service Object Delay Load	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i shell service object delay load og la skadelige filer kjøre når du starter datamaskinen.

SystemGuards for Windows

SystemGuards for Windows hjelper til med å hindre at datamaskinen din sender og mottar uautorisert eller personlig informasjon over Internett. Det hjelper også til med å stoppe programmer som kan komme med uventede endringer i utseendet og atferden til programmer som er viktige for deg og din familie.

SystemGuard	Oppdager...
Hurtigmenystyring	Uautoriserte registerendringer i Windows hurtigmenystyring som kan påvirke utseendet og atferden til Windows-menyer. Hurtigmenyer lar deg utføre handlinger på datamaskinen, som f.eks. å høyreklikke filer.

SystemGuard	Oppdager...
AppInit DLLs	Uautoriserte registerendringer i Windows appInit DLLs som kan tillate potensielt skadelige filer å kjøre når du starter datamaskinen.
Windows Hosts-fil	Spion- og reklameprogrammer og potensielt uønskede programmer som kan skape uautoriserte endringer i Windows hosts-filen, tillate webleseren å omdirigeres til mistenkelige webområder og blokkere programoppdateringer.
Winlogon-skall	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Winlogon-skallet og tillate andre programmer å erstatte Windows Utforsker.
Winlogon User Init	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Winlogon user init og lar mistenkelige programmer kjøre når du logger på Windows.
Windows-protokoller	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Windows-protokoller og påvirke måten datamaskinen sender og mottar informasjon over Internett på.
Winsock Layered Service Providers	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan installere registerendringer i Winsock Layered Service Providers (LSPs) for å fange opp og endre informasjon du sender og mottar over Internett.
Windows Shell Open Commands	Uautoriserte endringer i Windows shell open commands som kan tillate ormer og andre skadelige programmer å kjøre på datamaskinen.
Shared Task Scheduler	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape register- og filendringer i shared task scheduler og la potensielt skadelige filer kjøre når du starter datamaskinen.

SystemGuard	Oppdager...
Windows Messenger-tjenesten	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Windows Messenger-tjenesten og tillate uønskede reklamer og kjøre eksterne programmer på datamaskinen.
Windows Win.ini-fil	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape endringer i Win.ini-filen og la mistenkelige programmer kjøre når du starter datamaskinen.

SystemGuards for webleser

SystemGuards for webleser hjelper til med å hindre uautorisert webleseraktivitet, som f.eks. videresending til mistenkelige webområder, endringer i innstillinger og alternativer for webleser uten at du vet om det, og uønsket klarering av mistenkelige webområder.

SystemGuard	Oppdager...
Hjelpeobjekter for weblesere	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan bruke hjelpeobjekter for webleser til å spore weblesing og vise uønsket reklame.
Internet Explorer-verktøylinjer	Uautoriserte registerendringer i programmer for Internet Explorer-verktøylinjer, som f.eks. Søk og Favoritter, som kan påvirke utseendet og atferden til Internet Explorer.
Tillegg for Internet Explorer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan installere tillegg for Internet Explorer til å spore weblesing og vise uønsket reklame.
Internet Explorer ShellBrowser	Uautoriserte registerendringer i Internet Explorer shell browser som kan påvirke utseendet og atferden til webleseren.
Internet Explorer WebBrowser	Uautoriserte registerendringer i Internet Explorer Webleser som kan påvirke utseendet og atferden til webleseren.

SystemGuard	Oppdager...
Internet Explorer-bindinger for URL-søk	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer-bindinger for URL-søk og tillate webleseren å bli omdirigert til mistenkelige webområder når du søker på nettet.
Internet Explorer-URLer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer URL-er og påvirke innstillingene for webleseren.
Internet Explorer-begrensninger	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer URL-er og påvirke innstillingene og alternativene for webleseren.
Sikkerhetssoner i Internet Explorer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i sikkerhetssoner i Internet Explorer og la potensielt skadelige filer kjøre når du starter datamaskinen.
Klarerte områder i Internet Explorer	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i klarerte områder i Internet Explorer og tillate webleseren å klarere mistenkelige webområder.
Internet Explorer-policy	Spion- og reklameprogrammer og andre potensielt uønskede programmer som kan skape registerendringer i Internet Explorer-policyer og påvirke utseendet og atferden til webleseren.

Bruke klarerte lister

Hvis VirusScan oppdager endringer i filer eller register (SystemGuard), program eller bufferoverløp, blir du bedt om å klarere eller fjerne det. Hvis du klarerer elementet og sier at du ikke vil motta flere meldinger om elementets aktivitet, blir elementet lagt til i en klarert liste og VirusScan vil ikke lenger oppdage det eller melde fra om aktiviteten til det. Hvis et element har blitt lagt til i en klarert liste, men du ønsker å blokkere aktiviteten, kan du gjøre det. Å blokkere hindrer elementet fra å kjøre eller foreta endringer på datamaskinen uten å melde fra hver gang det blir gjort et forsøk. Du kan også fjerne et element fra en klarert liste. Å fjerne et element gjør at VirusScan kan oppdage elementets aktivitet igjen.

Behandle klarerte lister

Bruk ruten Klarerte lister for å klarere eller blokkere elementer som tidligere har blitt oppdaget og klarert. Du kan også fjerne et element fra en klarert liste slik at VirusScan kan oppdage det igjen.

1 Åpne ruten Klarerte lister

Hvordan?

1. Under **Vanlige oppgaver** klikker du **Hjem**.
2. Klikk **Datamaskin og filer** i Hjem-ruten i SecurityCenter.
3. I informasjonsdelen for Datamaskin og filer klikker du **Konfigurer**.
4. Kontroller at virusbeskyttelse er aktivert i ruten for Datamaskin og filer, og klikk deretter **Avansert**.
5. Klikk på **Klarerte lister** i ruten Virusbeskyttelse.

2 Velg en av følgende typer klarerte lister:

- **SystemGuards for programmer**
- **SystemGuards for Windows**
- **SystemGuards for webleser**
- **Klarerte programmer**
- **Klarerte bufferoverløp**

3 Under **Jeg vil** gjør du ett av følgende:

- Hvis du vil tillate det oppdagede elementet å foreta endringer i Windows-registret eller kritiske systemfiler på datamaskinen uten å melde fra, klikker du på **Klarer**.
- Hvis du vil blokkere det oppdagede elementet fra å foreta endringer i Windows-registret eller kritiske systemfiler på datamaskinen uten å melde fra, klikker du på **Blokker**.
- For å fjerne det oppdagede elementet fra klarerte lister, klikker du på **Fjern**.

4 Klikk **OK**.

Merk: For mer informasjon om typer av klarerte lister, se Om typer av klarerte lister (side 60).

Om typer av klarerte lister

SystemGuards i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. Det finnes fem typer klarerte lister som du kan administrere i ruten Klarerte lister: SystemGuards for programmer, SystemGuards for Windows, SystemGuards for webleser, Klarerte programmer og Klarerte bufferoverløp.

Alternativer	Beskrivelse
SystemGuards for programmer	SystemGuards for programmer i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. SystemGuards for programmer oppdager uautoriserte register- og filendringer tilknyttet ActiveX-installasjoner, oppstartselementer, shell execute hooks i Windows og aktivitet i shell service object delay load. Slike typer uautoriserte endringer i register og filer kan skade datamaskinen, sette sikkerheten på spill og skade verdifulle systemfiler.

Alternativer	Beskrivelse
SystemGuards for Windows	SystemGuards for programmer i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. SystemGuards for Windows oppdager uautoriserte register- og filendringer tilknyttet hurtigmenystyring, appInit DLLs, Windows hosts-filen, Winlogon-skallet, Winsock Layered Service Providers (LSPs) osv. Slike typer uautoriserte register- og filendringer kan påvirke måten datamaskinen sender og mottar informasjon over Internett på, endre utseendet og atferden til programmer og tillate mistenkelige programmer å kjøre på datamaskinen.
SystemGuards for webleser	SystemGuards for webleser i ruten Klarerte lister viser tidligere uautoriserte register- og filendringer som VirusScan har oppdaget, men som du kan ha valgt å tillate fra et varsel eller fra ruten Søkeresultater. SystemGuards for webleser oppdager uautoriserte registerendringer og annen uønsket atferd tilknyttet hjelpeobjekter for weblesere, Internet Explorer-tillegg, Internet Explorer URL-er, sikkerhetssoner i Internet Explorer osv. Slike typer uautoriserte registerendringer kan resultere i uønsket webleseraktivitet, slik som omdirigering til mistenkelige webområder, endringer i webleserens innstillinger og alternativer og klarering av mistenkelige webområder.
Klarerte programmer	Klarerte programmer er potensielt uønskede programmer som VirusScan tidligere har oppdaget, men som du har valgt å klarere fra et varsel eller fra ruten Søkeresultater.
Klarerte bufferoverløp	Klarerte bufferoverløp er potensielt uønsket aktivitet som VirusScan tidligere har oppdaget, men som du har valgt å klarere fra et varsel eller fra ruten Søkeresultater. Bufferoverløp kan skade datamaskinen og ødelegge filer. Bufferoverløp forekommer når mengden informasjon mistenkelige programmer eller prosesser lagrer i en buffer overstiger bufferens kapasitet.

KAPITTEL 13

McAfee Personal Firewall

Personal Firewall gir avansert beskyttelse til datamaskinen og dine personlige opplysninger. Personal Firewall oppretter en barriere mellom datamaskinen og Internett og overvåker all Internett-trafikk i bakgrunnen.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Personal Firewall-funksjoner

Standard og egendefinert beskyttelsesnivå	Beskyttelse mot inntrenging og mistenkelig aktivitet ved å bruke Firewalls standard egendefinerte beskyttelsesinnstillinger
Anbefalinger i sanntid	Motta dynamiske anbefalinger som hjelper deg å bestemme om programmer skal få Internett-tilgang eller om du kan stole på nettverkstrafikk.
Intelligent tilgangsadministrasjon for programmer	Håndter Internett-tilgang for programmer via varsler og hendelseslogger, og konfigurer tilgangstillatelser for spesifikke programmer.
Spillebeskyttelse	Forhindrer at varsler om inntrengingsforsøk og mistenkelige aktiviteter distraherer deg mens du spiller i fullskjermmodus.
Beskyttelse ved oppstart	Beskytter datamaskinen mot inntrengingsforsøk, uønskede programmer og nettverkstrafikk når Windows® starter.
Kontroll av systemtjenesteport	Administrerer åpne og lukkede systemtjenesteporter som kreves av visse programmer.
Administrerer datamaskintilkoblinger	Tillater og blokkerer eksterne tilkoblinger mellom andre datamaskiner og din datamaskin.
Integrasjon av HackerWatch-informasjon	Sporer global hacking- og inntrengingsmønstre via HackerWatch's webområde, som også gir oppdatert sikkerhetsinformasjon om programmer på datamaskinen din og statistikk om globale sikkerhetshendelser og Internett-port.
Sperr brannmur	Blokkerer all innkommende og utgående trafikk umiddelbart mellom datamaskinen og Internett.
Gjenopprette Firewall	Gjenoppretter umiddelbart Firewalls originale beskyttelsesinnstillinger.
Avanserte funksjoner for oppdagelse av trojanske hester	Oppdager og blokkerer potensielt skadelige programmer, som for eksempel trojanske hester, fra å videresende dine personlige opplysninger over Internett.
Hendelseslogging	Sporer nylig innkommende, utgående og inntrengingshendelser.
Overvåke Internett-trafikk	Gå gjennom kart som viser kilden til aggressive angrep og aggressiv trafikk over hele verden. I tillegg kan du få detaljert eierinformasjon og geografiske data om de opprinnelige IP-adressene. Analyserer også innkommende og utgående trafikk og overvåker programbåndbredde og programaktivitet.
Inntrengingshindring	Beskytter ditt personvern fra mulige Internett-trusler. Ved hjelp av heuristisklignende funksjonalitet tilbyr vi et tertiært beskyttelseslag som blokkerer elementer som viser tegn på angrep eller de samme karakteristikkene som hackerangrep.
Avansert trafikkanalyse	Gjennomgår både innkommende og utgående Internett-trafikk og programtilkoblinger, deriblant de som aktivt lytter etter åpne tilkoblinger. Dette gir deg anledning til å se hvilke programmer som kan være åpne for inntrenging, slik at du kan handle deretter.

KAPITTEL 14

Starte Firewall

Så snart du har installert Firewall, er datamaskinen din beskyttet mot inntrenging og uønsket nettverkstrafikk. I tillegg er du klar til å håndtere varsler og administrere innkommende og utgående Internett-tilgang for kjente og ukjente programmer. Smarte anbefalinger og automatisk sikkerhetsnivå (med alternativet satt til å tillate programmer kun utgående tilgang til Internett) aktiveres automatisk.

Du kan deaktivere Firewall i ruten Internett- og nettverkskonfigurasjon, men da vil ikke datamaskinen din lenger være beskyttet mot inntrenging og uønsket nettverkstrafikk, og du kan ikke administrere innkommende og utgående Internett-tilkoblinger på en effektiv måte. Hvis du må deaktivere brannmurbeskyttelsen, bør du gjøre det midlertidig og bare når det er nødvendig. Du kan også aktivere Firewall i panelet Internett- og nettverkskonfigurasjon.

Firewall deaktiverer automatisk Windows® Firewall og angir seg selv som standard brannmur.

Merk: Hvis du vil konfigurere Firewall, åpner du ruten Internett- og nettverkskonfigurasjon.

I dette kapitlet

Starte brannmurbeskyttelse

Du kan aktivere Firewall til å beskytte datamaskinen mot inntrenging og uønsket trafikk i tillegg til at du får hjelp til å administrere innkommende og utgående Internett-tilkoblinger.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse deaktivert**, klikker du på **På**.

Stoppe brannmurbeskyttelse

Du kan deaktivere Firewall hvis du ikke ønsker å beskytte datamaskinen fra inntrenging og uønsket trafikk. Hvis Firewall er deaktivert, kan du ikke administrere innkommende eller utgående Internett-tilkoblinger.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Av**.

KAPITTEL 15

Arbeide med varsler

Firewall benytter et bredt spekter av varsler for å hjelpe deg å administrere sikkerheten. Disse varslene kan grupperes i tre grunnleggende typer:

- Rødt varsel
- Gult varsel
- Grønt varsel

Varsler kan også inneholde informasjon som hjelper deg å finne ut hvordan du skal håndtere varsler eller hvordan du kan få informasjon om programmer som kjører på datamaskinen.

I dette kapitlet

Om varsler

Firewall har tre grunnleggende varseltyper. Noen varsler inneholder også informasjon som hjelper deg å lære eller få informasjon om programmer som kjører på datamaskinen din.

Rødt varsel

Et rødt varsel vises når Firewall oppdager og deretter blokkerer en trojansk hest på datamaskinen din og anbefaler at du foretar et søk etter flere trusler. Trojanere ser ut til å være legitime programmer, men kan avbryte, skade eller gi uautorisert tilgang til datamaskinen. Dette varselet forekommer på alle sikkerhetsnivåer.

Gult varsel

Den vanligste varseltypen er et gult varsel. Det informerer deg om en programaktivitet eller nettverkshendelse oppdaget av Firewall. Når dette forekommer, beskriver varselet programaktiviteten eller nettverkshendelsen, og gir deg deretter ett eller flere alternativer som krever en handling fra deg. Varselet **Ny nettverkstilkobling** vises for eksempel når en datamaskin med Firewall installert kobles til et nytt nettverk. Du kan angi sikkerhetsnivået du vil tilordne dette nye nettverket, og det vises deretter i Nettverk-listen. Hvis Smarte anbefalinger er aktivert, legges kjente programmer automatisk til i ruten for programtillatelser.

Grønt varsel

I de fleste tilfeller gir et grønt varsel grunnleggende informasjon om en hendelse uten at det er nødvendig å handle. Grønne varsler deaktiveres som standard.

Brukerhjelp

Mange Firewall-varsler inneholder tilleggsinformasjon som hjelper deg å administrere datamaskinens sikkerhet, noe som omfatter følgende:

- **Finn ut mer om dette programmet**: Start McAfees globale webområde om sikkerhet for å få informasjon om et program som Firewall har oppdaget på datamaskinen.
- **Fortell McAfee om dette programmet**: Send informasjon til McAfee om en ukjent fil som Firewall har oppdaget på datamaskinen.
- **McAfee anbefaler**: Råd om hvordan du håndterer varsler. Et varsel kan for eksempel anbefale at du gir tilgang til et program.

KAPITTEL 16

Håndtere informasjonsvarsler

Med Firewall kan du vise eller skjule informasjonsvarsler når inntrengingsforsøk eller mistenkelige aktiviteter oppdages under bestemte hendelser, for eksempel under fullskjermspilling.

I dette kapitlet

Vise varsler når du spiller

Med Firewall kan du la informasjonsvarsler vises når inntrengingsforsøk eller mistenkelig aktivitet oppdages under fullskjermspilling.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på **Konfigurer**.
3. I ruten SecurityCenter-konfigurasjon klikker du **Varsler** under **Avansert**.
4. I ruten Alternativer for varslinger velger du **Vis informasjonsvarsler når spillmodus er oppdaget**.
5. Klikk **OK**.

Skjule informasjonsvarsler

Du kan forhindre at Firewall-informasjonsvarsler vises når inntrengingsforsøk eller mistenkelig aktivitet oppdages.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på **Konfigurer**.
3. I ruten SecurityCenter-konfigurasjon klikker du **Varsler** under **Avansert**.
4. I ruten SecurityCenter-konfigurasjon klikker du på **Informasjonsvarsler**.
5. I ruten Informasjonsvarsler gjør du ett av følgende:
   - Velg **Ikke vis informasjonsvarsler** for å skjule alle informasjonsvarsler.
   - Velg et varsel du vil skjule.
6. Klikk **OK**.

KAPITTEL 17

Konfigurere Firewall-beskyttelse

Firewall tilbyr en rekke metoder for å administrere sikkerheten og skreddersy måten du vil følge opp sikkerhetshendelser og varsler på.

Når du installerer Firewall for første gang, settes beskyttelsesnivået til Automatisk, og programmene tillates kun utgående Internett-tilgang. Firewall tilbyr imidlertid andre nivåer, fra svært restriktiv til svært lite restriktiv.

Firewall gir deg også muligheten til å motta anbefalinger om varsler og Internett-tilgang for programmer.

I dette kapitlet

Administrere sikkerhetsnivåer i Firewall

Firewalls sikkerhetsnivåer kontrollerer i hvilken grad du vil administrere og reagere på varsler. Disse varslene vises når Firewall oppdager uønsket nettverkstrafikk og innkommende og utgående Internett-tilkoblinger Som standardinnstilling settes Firewalls sikkerhetsnivå til Automatisk, med kun utgående tilgang.

Når sikkerhetsnivået Automatisk er angitt og Smarte anbefalinger er aktivert, gir gule varsler deg muligheten til å tillate eller blokkere tilgang for ukjente programmer som krever innkommende tilgang. Selv om grønne varsler er deaktiverte som standard, vises de når kjente programmer oppdages og det gis automatisk tilgang. Et program som gis tilgang, kan opprette utgående tilkoblinger og lytte etter uanmodede innkommende tilkoblinger.

Generelt sett er det slik at jo mer restriktivt sikkerhetsnivået (Skjult og Standard) er, jo flere alternativer og varsler vises, som du så må håndtere.

Den følgende tabellen beskriver Firewalls tre sikkerhetsnivåer, fra det mest restriktive til det minst restriktive nivået:

Nivå	Beskrivelse
Skjult	Blokkerer alle inngående Internett-tilkoblinger, bortsett fra åpne porter, og skjuler datamaskinen din på Internett. Brannmuren varsler deg når nye programmer gjør forsøk på utgående Internett-tilkoblinger eller mottar forespørsler om inngående tilkobling. Blokkerte programmer og programmer som er lagt til, vises i ruten for programtillatelser.
Standard	Overvåker innkommende og utgående tilkoblinger og varsler når nye programmer prøver å få Internett-tilgang. Blokkerte programmer og programmer som er lagt til, vises i ruten for programtillatelser.
Automatisk	Tillater programmene å ha enten innkommende og utgående (full) eller bare utgående Internett-tilgang. Standard sikkerhetsnivå er Automatisk med alternativet å kun tillate programmer utgående tilgang. Hvis et program tillates full tilgang, vil Firewall automatisk klarere det og legge det til listen over tillatte programmer i ruten Programtillatelser. Hvis et program kun er tillatt utgående tilgang, vil Firewall automatisk klarere det kun når det gjør en utgående Internett-tilkobling. En inngående forbindelse klareres ikke automatisk.

Med Firewall kan du også umiddelbart tilbakestille sikkerhetsnivået til Automatisk (og tillate kun utgående tilgang) i ruten Gjenopprett standardinnstillinger for brannmur.

Angi sikkerhetsnivået til Skjult

Du kan stille Firewalls sikkerhetsnivå til Skjult for å blokkere alle inngående nettverkstilkoblinger, bortsett fra åpne porter, for å skjule datamaskinen din på Internett.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Skjult** vises som gjeldende nivå.
4. Klikk **OK**.

Merk: I Skjult-modusen vil Firewall varsle deg når nye programmer ber om utgående Internett-tilkobling eller mottar forespørsler om inngående tilkoblinger.

Angi sikkerhetsnivået til Standard

Du kan angi sikkerhetsnivået til Standard for å overvåke innkommende og utgående tilkoblinger og varsler når nye programmer prøver å få Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Standard** vises som gjeldende nivå.
4. Klikk **OK**.

Angi sikkerhetsnivået til Automatisk

Du kan sette sikkerhetsnivået for brannmuren til Automatisk for å tillate enten full tilgang eller bare utgående nettverkstilgang.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Sikkerhetsnivå-ruten flytter du glidebryteren slik at **Automatisk** vises som gjeldende nivå.

4 Gjør ett av følgende:
   - Velg **Tillat full tilgang** for å tillate full inngående og utgående nettverkstilgang.
   - Velg **Tillat bare utgående tilgang** for å tillate bare utgående nettverkstilgang.

5 Klikk **OK**.

Merk: Standardinnstillingen er **Tillat bare utgående tilgang**.

Konfigurere Smarte anbefalinger for varsler

Du kan konfigurere Firewall slik at varsler inkluderer, utelukker eller viser anbefalinger når programmer prøver å få tilgang til Internett. Ved å aktivere Smarte anbefalinger får du hjelp til å finne ut hvordan du skal håndtere varsler.

Når Smarte anbefalinger er aktivert (og sikkerhetsnivået er satt til Automatisk med kun utgående tilgang aktivert), tillater brannmuren automatisk kjente programmer og blokkerer potensielt farlige programmer.

Når Smarte anbefalinger er deaktivert, vil brannmuren hverken tillate eller blokkere Internett-tilgang og heller ikke gi anbefalinger i varslet.

Når Smarte anbefalinger er satt til Vis, vil et varsel be deg om å tillate eller blokkere tilgang og anbefale en handlingsplan i varselet.

Aktivere Smarte anbefalinger

Du kan aktivere Smarte anbefalinger for Firewall til å automatisk tillate eller blokkere programmer, og varsle deg om ukjente og potensielt farlige programmer.

1 Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.

3 I Sikkerhetsnivå-ruten velger du **Bruk Smarte anbefalinger** under **Smarte anbefalinger**.

4 Klikk **OK**.

Deaktivere Smarte anbefalinger

Du kan deaktivere Smarte anbefalinger for Firewall til å tillate eller blokkere programmer og varsle deg om ukjente og potensielt farlige programmer. Varslene vil imidlertid utelukke anbefalinger om tilgangshåndtering for programmer. Hvis Firewall oppdager et nytt program som er mistenkelig eller som er kjent for å være en mulig trussel, blokkeres programmet automatisk fra å få tilgang til Internett.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Sikkerhetsnivå-ruten velger du **Ikke bruk Smarte anbefalinger** under **Smarte anbefalinger**.
4. Klikk **OK**.

Vise smarte anbefalinger

Du kan vise Smarte anbefalinger for å vise bare en anbefaling i varslene, slik du kan bestemme om du vil tillate eller blokkere ukjente og potensielt farlige programmer.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Sikkerhetsnivå-ruten velger du **Vis Smarte anbefalinger** under **Smarte anbefalinger**.
4. Klikk **OK**.

Optimalisere Firewall-sikkerhet

Sikkerheten på datamaskinen din kan settes på spill på mange måter. Noen programmer kan for eksempel prøve å koble til Internett når Windows® starter. I tillegg kan sofistikerte datamaskinbrukere spore (eller pinge) datamaskinen for å finne ut om den er koblet til et nettverk. De kan også sende informasjon til datamaskinen din ved hjelp av UDP-protokollen i form av meldingsenheter (datagrammer). Firewall beskytter datamaskinen mot denne typen angrep ved å gjøre det mulig å blokkere programmer fra å få tilgang til Internett når Windows starter, blokkere pingforespørsler som hjelper andre brukere å oppdage datamaskinen din på et nettverk og forhindre andre brukere fra å sende informasjon til datamaskinen din i form av meldingsenheter (datagrammer).

Standard installasjonspolicy omfatter automatisk oppdagelse av de vanligste inntrengingsforsøkene, som tjenestenekt (Denial of Service) eller sikkerhetshull. Bruk av standard installasjonspolicy betyr at du beskyttes mot disse angrepene. Du kan imidlertid skru av automatisk oppdagelse for ett eller flere angrep eller søk i ruten for inntrengingsoppdagelse.

Beskytte datamaskinen under oppstart

Du kan beskytte datamaskinen når Windows starter opp ved å blokkere nye programmer som ikke hadde, og nå trenger, Internett-tilgang under oppstart. Firewall viser relevante varsler for programmer som har bedt om Internett-tilgang. Disse kan du tillate eller blokkere.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Sikkerhetsnivå-ruten velger du **Aktiver beskyttelse ved oppstart av Windows** under **Sikkerhetsinnstillinger**.
4. Klikk **OK**.

Merk: Blokkerte tilkoblinger og inntrenginger logges ikke når beskyttelse under oppstart er aktivert.

Konfigurere innstillinger for pingforespørsler

Du kan tillate eller forhindre at din datamaskin oppdages på nettverket av andre datamaskiner.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. Under **Sikkerhetsinnstillinger** i Sikkerhetsnivå-ruten gjør du ett av følgende:
   - Velg **Tillat ICMP-pingforespørsler** for å tillate at datamaskinen din oppdages på nettverket ved hjelp av pingforespørsler.
   - Fjern merket for **Tillat ICMP-pingforespørsler** for å hindre at datamaskinen din oppdages på nettverket ved hjelp av pingforespørsler.
4. Klikk **OK**.

Konfigurere UDP-innstillinger

Du kan tillate at andre brukere av nettverksdatamaskiner sender meldingsenheter (datagrammer) til datamaskinen din, ved hjelp av UDP-protokollen. Du kan imidlertid bare gjøre dette hvis du også har lukket en systemtjenesteport for å blokkere denne protokollen.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. Under **Sikkerhetsinnstillinger** i Sikkerhetsnivå-ruten gjør du ett av følgende:
   - Velg **Aktiver UDP-sporing** for å gjøre det mulig for andre datamaskinbrukere å sende meldingsenheter (datagrammer) til din datamaskin.
   - Fjern avmerkingen for **Aktiver UDP-sporing** for å forhindre andre datamaskinbrukere fra å sende meldingsenheter (datagrammer) til din datamaskin.
4. Klikk **OK**.

Konfigurere inntrengingsoppdagelse

Du kan beskytte datamaskinen fra angrep og uautoriserte søk ved å oppdage inntrengningsforsøk. Standardinnstilling for Firewall inkluderer automatisk oppdagelse av de mest vanlige inntrengningsforsøkene, som Denial of Service-angrep eller sikkerhetshull. Du kan imidlertid deaktivere automatisk oppdagelsen for et eller flere angrep, eller søk.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Inntrengingsoppdagelse**.
4. Under **Oppdag forsøk på inntrenging** gjør du ett av følgende:
   - Velg et navn for å oppdage angrepet eller foreta et søk automatisk.
   - Fjern merket for et navn hvis du vil deaktivere automatisk angrepsoppdagelse eller søk.
5. Klikk **OK**.

Konfigurere beskyttelsesstatusinnstillinger for Firewall

Du kan konfigurere Firewall til å ignorere at spesifikke problemer på datamaskinen ikke rapporteres til SecurityCenter.

1. Klikk **Konfigurer** i ruten McAfee SecurityCenter under **SecurityCenter-informasjon**.
2. I ruten SecurityCenter-konfigurasjon klikker du **Beskyttelsesstatus** under **Avansert**.
3. I ruten Ignorer problemene velger du ett eller flere av følgende alternativer:
   - **Brannmurbeskyttelse er deaktivert.**
   - **Brannmurtjeneste kjører ikke.**
   - **Brannmurbeskyttelse er ikke installert på datamaskinen.**
   - **Windows-brannmur er deaktivert.**
   - **Utgående brannmur er ikke installert på datamaskinen.**
4. Klikk **OK**.

Sperre og gjenopprette Firewall

Sperring blokkerer øyeblikkelig alle inngående og utgående nettverkstilkoblinger, inkludert tilgang til webområder, e-post og sikkerhetsoppdateringer. Sperring gir det samme resultatet som å koble fra nettverkskablene på datamaskinen. Du kan bruke denne innstillingen til å blokkere åpne porter i Systemtjenester-ruten og til å hjelpe deg å isolere og feilsøke et problem på datamaskinen din.

Sperre brannmur øyeblikkelig

Du kan sperre brannmuren for øyeblikkelig å blokkere all nettverkstrafikk mellom datamaskinen og et hvilket som helst nettverk, inkludert Internett.

1. Klikk **Sperr Firewall** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. I ruten for brannmursperring klikker du **Aktiver brannmursperring**.
3. Klikk **Ja** for å bekrefte.

Tips: Du kan også sperre Firewall ved å høyreklikke SecurityCenter-ikonet i systemstatusfeltet til høyre for oppgavelinjen. Klikk deretter **Hurtiglinker** og deretter **Sperr Firewall**.

Oppheve sperring av brannmuren øyeblikkelig

Du kan oppheve brannmuren for øyeblikkelig å tillate all nettverkstrafikk mellom datamaskinen og et hvilket som helst nettverk, inkludert Internett.

1. Klikk **Sperr Firewall** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. I ruten Sperrefunksjon aktivert klikker du **Deaktiver brannmursperring**.
3. Klikk **Ja** for å bekrefte.

Gjenopprette Firewall-innstillinger

Du kan raskt gjenopprette Firewalls opprinnelige beskyttelsesinnstillinger. Dette gjenoppretter sikkerhetsnivået til Automatisk og tillater bare utgående nettverkstilgang, aktiverer Smarte anbefalinger, gjenoppretter listen over standardprogrammer og deres tillatelser i ruten Programtillatelser, fjerner klarerte og utestengte IP-adresser, og gjenoppretter systemtjenester, innstillinger for hendelseslogg og inntrengingsoppdagelse.

1. I ruten McAfee SecurityCenter klikker du **Gjenopprett standardinnstillinger for Firewall**.
2. I ruten Gjenopprett standardinnstillinger for brannmurbeskyttelse klikker du **Gjenopprett standardinnstillingene**.
3. Klikk **Ja** for å bekrefte.
4. Klikk **OK**.

KAPITTEL 18

Administrere programmer og tillatelser

Firewall lar deg administrere og opprette tilgangstillatelser for eksisterende og nye programmer som krever innkommende og utgående Internett-tilgang. Med Firewall kan du kontroller om programmer skal gis full eller bare utgående tilgang. Du kan også blokkere tilgang for programmer.

I dette kapitlet

Tillat Internett-tilgang for programmer

Enkelte programmer, for eksempel Internett-lesere, trenger tilgang til Internett for å fungere skikkelig.

Firewall lar deg bruke siden for programtillatelser for å:

- Tillat tilgang for programmer
- Tillat bare utgående tilgang til programmer
- Blokkere tilgang for programmer

Du kan også tillate et program full og bare utgående tilgang fra loggene for utgående hendelser og nylige hendelser.

Gi full tilgang til et program

Du kan gi et eksisterende blokkert program på datamaskinen full inngående og utgående tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program med **Blokkert** eller **Bare utgående tilgang**.
5. Under **Handling** klikker du **Tillat tilgang**.
6. Klikk **OK**.

Gi full tilgang til nytt et program

Du kan gi et nytt program på datamaskinen full inngående og utgående tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** klikker du **Legg til tillatt program**.
5. I dialogboksen **Legg til program** blar du etter og velger programmet du vil legge til, og klikker deretter på **Åpne**.

Merk: Du kan endre tillatelsene for et program du har lagt til, på samme måte som for et eksisterende program. Dvs. du velger programmet, og deretter klikker du **Gi bare utgående tilgang** eller **Blokker tilgang** under **Handling**.

Gi full tilgang fra loggen for nylige hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Nylige hendelser full inngående og utgående Internett-tilgang.

1 I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2 Klikk på**Rapporter og logger**.
3 Under **Nylige hendelser**, velger du hendelsesbeskrivelsen, og deretter klikker du **Tillat tilgang**.
4 I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Beslektede emner

- Vise utgående hendelser (side 105)

Gi full tilgang fra loggen Utgående hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Utgående hendelser full inngående og utgående Internett-tilgang.

1 I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2 Klikk på**Rapporter og logger**.
3 I **Nylige hendelser** klikker du på **Vis logg**.
4 Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.
5 Velg et program, og klikk **Tillat tilgang** under **Jeg vil**.
6 I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Tillat bare utgående tilgang til programmer

Noen programmer på datamaskinen krever utgående Internett-tilgang. Med Firewall kan du konfigurere programtillatelser til å tillate bare utgående Internett-tilgang.

Tillat bare utgående tilgang for et program

Du kan gi et program bare utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program med **Blokkert** eller **Full tilgang**.
5. Under **Handling** klikker du **Tillat bare utgående tilgang**.
6. Klikk **OK**.

Tillat bare utgående tilgang fra loggen Nylige hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Nylige hendelser bare utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. Under **Nylige hendelser**, velger du hendelsesbeskrivelsen, og deretter klikker du **Tillat bare utgående tilgang**.
4. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Tillat bare utgående tilgang fra loggen for utgående hendelser

Du kan gi et eksisterende blokkert program som vises i loggen Utgående hendelser bare utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. I **Nylige hendelser** klikker du på **Vis logg**.
4. Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.
5. Velg et program, og klikk **Tillat bare utgående tilgang** under **Jeg vil**.
6. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Blokkere Internett-tilgang for programmer

Med Firewall kan du blokkere programmer fra å få tilgang til Internett. Kontroller at ikke nettverkstilkoblingen avbrytes eller at et annet program som krever tilgang til Internett for å fungere skikkelig, forstyrres når du blokkerer et program.

Blokkere tilgang for et program

Du kan blokkere et program fra å ha inngående og utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program med **Full tilgang** eller **Bare utgående tilgang**.
5. Under **Handling** klikker du **Blokker tilgang**.
6. Klikk **OK**.

Blokkere tilgangen for et nytt program

Du kan blokkere et nytt program fra å ha inngående og utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** klikker du **Legg til blokkert program**.
5. I dialogboksen Legg til program, blar du etter og velger programmet du vil legge til, og klikker deretter på **Åpne**.

Merk: Du kan endre tillatelsene for et program du har lagt til ved å velge programmet, og deretter klikke på **Tillat bare utgående tilgang** eller **Tillat tilgang** under **Handling**.

Blokkere tilgang fra loggen for nylige hendelser

Du kan blokkere et program som vises i loggen Nylige hendelser slik at det ikke vil ha inngående og utgående Internett-tilgang.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. Under **Nylige hendelser**, velger du hendelsesbeskrivelsen, og deretter klikker du **Blokker tilgang**.
4. I dialogboksen Programtillatelser, klikker du **Ja** for å bekrefte.

Fjerne tilgangstillatelser for programmer

Før du fjerner en programtillatelse, må du forsikre deg om at fraværet av dette programmet ikke påvirker datamaskinens funksjonalitet eller nettverkstilkoblingen din.

Fjerne en programtillatelse

Du kan fjerne et program fra å ha inngående eller utgående Internett-tilgang.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program.
5. Under **Handling** klikker du **Fjern programtillatelse**.
6. Klikk **OK**.

Merk: Firewall hindrer deg i å endre enkelte programmer ved å tone ned og deaktivere visse handlinger.

Lære om programmer

Hvis du er usikker på hvilken programtillatelse du skal bruke, kan du få informasjon om programmet på McAfees webområde HackerWatch.

Få programinformasjon

Du kan få programinformasjon for å avgjøre om du skal tillate eller blokkere inngående og utgående Internett-tilgang på McAfees webområde HackerWatch.

Merknad: Pass på at du er koblet til Internett slik at webleseren kan starte McAfees HackerWatch-webområde, som gir oppdatert informasjon og programmer, Internett-tilgangskrav og sikkerhetstrusler.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Programtillatelser**.
4. Under **Programtillatelser** velger du et program.
5. Under **Handling** klikker du **Mer informasjon**.

Få programinformasjon fra loggen for utgående hendelser

Du kan få programinformasjon fra loggen Utgående hendelser for å avgjøre for hvilke programmer du skal tillate eller blokkere inngående og utgående Internett-tilgang på McAfees webområde HackerWatch.

Merknad: Pass på at du er koblet til Internett slik at webleseren kan starte McAfees HackerWatch-webområde, som gir oppdatert informasjon og programmer, Internett-tilgangskrav og sikkerhetstrusler.

1. I ruten McAfee SecurityCenter klikker du på **Avansert meny**.
2. Klikk på**Rapporter og logger**.
3. Velg en hendelse under Nylige hendelser og klikk deretter på **Vis logg**.
4. Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.
5. Velg en IP-adresse, og klikk deretter **Lær mer**.

KAPITTEL 19

Administrere datamaskintilkoblinger

Du kan konfigurere Firewall til å administrere bestemte eksterne tilkoblinger til datamaskinen ved å opprette regler basert på Internett-protokolladresser (IP-adresser) som er tilknyttet eksterne datamaskiner. Datamaskiner som er tilknyttet klarerte IP-adresser, kan trygt tilkobles datamaskinen din, mens datamaskiner som er tilknyttet IP-adresser som er ukjente, mistenkelige eller mistrodde, kan bli utestengt fra å koble til datamaskinen din.

Når du tillater en tilkobling, må du passe på at datamaskinen du klarerer, er sikker. Hvis en klarert datamaskin er infisert med en orm eller en annen mekanisme, kan datamaskinen din være sårbar for infeksjon. McAfee anbefaler også at datamaskinen du klarerer, er beskyttet av en brannmur og et oppdatert antivirusprogram. Firewall logger ikke trafikk og genererer heller ikke hendelsesvarsler fra klarerte IP-adresser i **Nettverk**-listen.

Du kan utestenge datamaskiner som er forbundet med ukjente, mistenkelige eller mistrodde IP-adresser, fra å koble til datamaskinen din.

Ettersom Firewall blokkerer all uønsket trafikk, er det vanligvis ikke nødvendig å utestenge IP-adresser. Du bør bare utestenge en IP-adresse når du er sikker på at en Internett-tilkobling utgjør en trussel. Sørg for at du ikke blokkerer viktige IP-adresser, for eksempel DNS- eller DHCP-tjeneren eller andre ISP-tjenere.

I dette kapitlet

Om datamaskintilkoblinger

Datamaskintilkoblinger er tilkoblingene som du oppretter mellom andre datamaskiner i andre nettverk og ditt eget. Du kan legge til, redigere og fjerne IP-adresser på **Nettverk**-listen. Disse IP-adressene er tilknyttet nettverk som du ønsker å tilordne et sikkerhetsnivå for når de kobler til datamaskinen din: Klarert, Standard og Offentlig.

Nivå	Beskrivelse
Klarert	Firewall tillater trafikk fra en IP-adresse å nå datamaskinen via hvilken som helst port. Aktivitet mellom datamaskinen som er tilknyttet en klarert IP-adresse, og din datamaskin filtreres eller analyseres ikke av Firewall. Som standard vises det første nettverket Firewall finner, som Klarert i listen **Nettverk**. Et eksempel på et klarert nettverk er en datamaskin eller datamaskiner i ditt lokalnettverk eller hjemmenettverk.
Standard	Firewall kontrollerer trafikk fra en IP-adresse (men ikke fra andre datamaskiner i det nettverket) når den kobler til din datamaskin, og tillater eller blokkerer den i henhold til reglene listen **Systemtjenester**. Firewall logger trafikk og genererer hendelsesvarsler fra standard-IP-adresser. Et eksempel på et standardnettverk er en datamaskin eller datamaskiner i et bedriftsnettverk.
Offentlig	Firewall kontrollerer trafikk fra et offentlig nettverk i henhold til regelene i listen **Systemtjenester**. Et eksempel på et offentlig nettverk er et Internett-nettverk i en kafé, et hotell eller en flyplass.

Når du tillater en tilkobling, må du passe på at datamaskinen du klarerer, er sikker. Hvis en klarert datamaskin er infisert med en orm eller en annen mekanisme, kan datamaskinen din være sårbar for infeksjon. McAfee anbefaler også at datamaskinen du klarerer, er beskyttet av en brannmur og et oppdatert antivirusprogram.

Legge til en datamaskintilkobling

Du kan legge til en klarert, standard eller offentlig datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1 Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.

3 I Brannmur-ruten klikker du **Nettverk**.

4 I Nettverk-ruten klikker du **Legg til**.

5 Hvis datamaskintilkoblingen er på et IPv6-nettverk, merker du av for **IPv6**.

6 Under **Legg til regel** gjør du ett av følgende:

- Velg **Enkel**, og angi deretter IP-adressen i boksen **IP-adresse**.
- Velg **Område** og angi deretter start- og slutt-IP-adresser i boksene **Fra IP-adresse** og **Til IP-adresse**. Hvis datamaskintilkoblingen er på et IPv6-nettverk, angir du start-IP-adressen og prefikslengden i boksene **Fra IP-adresse** og **Prefikslengde**.

7 Under **Type** gjør du ett av følgende:

- Velg **Klarert** for å angi at denne datamaskintilkoblingen er klarert (for eksempel en datamaskin i et hjemmenettverk).
- Velg **Standard** for å angi at denne datamaskintilkoblingen (og ikke de andre datamaskinene i det samme nettverket), er klarert (for eksempel en datamaskin i et bedriftsnettverk).
- Velg **Offentlig** for å angi at denne datamaskintilkoblingen er offentlig (for eksempel en datamaskin i en Internett-kafé, et hotell eller på en flyplass).

8 Hvis en systemtjeneste bruker deling av Internett-tilkobling (ICS), kan du legge til følgende IP-adresseområde: 192.168.0.1 til 192.168.0.255.

9 Velg eventuelt **Regel utløper om** og angi hvor mange dager regelen skal gjelde.

10 Skriv eventuelt inn en beskrivelse av regelen.

11 Klikk **OK**.

Merk: Du finner mer informasjon om deling av Internett-tilkobling (ICS) i Konfigurere en ny systemtjeneste.

Legge til en datamaskin fra loggen for innkommende hendelser

Du kan legge til en klarert eller standard datamaskintilkobling og koblingens tilknyttede IP-adresse fra loggen for innkommende hendelser.

1. Klikk **Avansert meny** under Vanlige oppgaver i ruten McAfee SecurityCenter.
2. Klikk **Rapporter og logger**.
3. I **Nylige hendelser** klikker du **Vis logg**.
4. Klikk **Nettverk og Internett** og deretter **Innkommende hendelser**.
5. Velg en kilde-IP-adresse og gjør ett av følgende under **Jeg vil**:
   - Klikk **Legg til denne IP-adressen som klarert** for å legge til denne datamaskinen som Klarert i listen **Nettverk**.
   - Klikk **Legg til denne IP-adressen som standard** for å legge til denne datamaskintilkoblingen som Standard i listen **Nettverk**.
6. Klikk **Ja** for å bekrefte.

Redigere en datamaskintilkobling

Du kan redigere en klarert, standard eller offentlig datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Nettverk**.
4. I Nettverk-ruten velger du en IP-adresse, og klikker deretter **Rediger**.
5. Hvis datamaskintilkoblingen er på et IPv6-nettverk, merker du av for **IPv6**.
6. Under **Rediger regel** gjør du ett av følgende:
   - Velg **Enkel**, og angi deretter IP-adressen i boksen **IP-adresse**.
   - Velg **Område** og angi deretter start- og slutt-IP-adresser i boksene **Fra IP-adresse** og **Til IP-adresse**. Hvis datamaskintilkoblingen er på et IPv6-nettverk, angir du start-IP-adressen og prefikslengden i boksene **Fra IP-adresse** og **Prefikslengde**.

7 Under **Type** gjør du ett av følgende:

- Velg **Klarert** for å angi at denne datamaskintilkoblingen er klarert (for eksempel en datamaskin i et hjemmenettverk).
- Velg **Standard** for å angi at denne datamaskintilkoblingen (og ikke de andre datamaskinene i det samme nettverket), er klarert (for eksempel en datamaskin i et bedriftsnettverk).
- Velg **Offentlig** for å angi at denne datamaskintilkoblingen er offentlig (for eksempel en datamaskin i en Internett-kafé, et hotell eller på en flyplass).

8 Merk eventuelt av for **Regel utløper om**, og angi hvor mange dager regelen skal gjelde.

9 Skriv eventuelt inn en beskrivelse av regelen.

10 Klikk **OK**.

Merk: Du kan ikke redigere standard datamaskintilkobling som Firewall automatisk har lagt til fra et klarert privat nettverk.

Fjerne en datamaskintilkobling

Du kan fjerne en klarert, standard eller offentlig datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1 Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.

2 I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.

3 I Brannmur-ruten klikker du **Nettverk**.

4 I Nettverk-ruten velger du en IP-adresse, og klikker deretter **Fjern**.

5 Klikk **Ja** for å bekrefte.

Stenge ute datamaskintilkoblinger

Du kan legge til, redigere og fjerne utestengte IP-adresser i ruten Utestengte IP-adresser.

Du kan utestenge datamaskiner som er forbundet med ukjente, mistenkelige eller mistrodde IP-adresser, fra å koble til datamaskinen din.

Ettersom Firewall blokkerer all uønsket trafikk, er det vanligvis ikke nødvendig å utestenge IP-adresser. Du bør bare utestenge en IP-adresse når du er sikker på at en Internett-tilkobling utgjør en trussel. Sørg for at du ikke blokkerer viktige IP-adresser, for eksempel DNS- eller DHCP-tjeneren eller andre ISP-tjenere.

Legge til en utestengt datamaskintilkobling

Du kan legge til en utestengt datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

Merk: Sørg for at du ikke blokkerer viktige IP-adresser, for eksempel DNS- eller DHCP-tjeneren eller andre ISP-tjenere.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Utestengte IP-adresser**.
4. I ruten Utestengte IP-adresser klikker du **Legg til**.
5. Hvis datamaskintilkoblingen er på et IPv6-nettverk, merker du av for **IPv6**.
6. Under **Legg til regel** gjør du ett av følgende:
   - Velg **Enkel**, og angi deretter IP-adressen i boksen **IP-adresse**.
   - Velg **Område** og angi deretter start- og slutt-IP-adresser i boksene **Fra IP-adresse** og **Til IP-adresse**. Hvis datamaskintilkoblingen er på et IPv6-nettverk, angir du start-IP-adressen og prefikslengden i boksene **Fra IP-adresse** og **Prefikslengde**.
7. Velg eventuelt **Regel utløper om** og angi hvor mange dager regelen skal gjelde.
8. Skriv eventuelt inn en beskrivelse av regelen.
9. Klikk **OK**.
10. Klikk **Ja** for å bekrefte.

Redigere en utestengt datamaskintilkobling

Du kan redigere en utestengt datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Utestengte IP-adresser**.
4. I ruten Utestengte IP-adresser klikker du **Rediger**.
5. Hvis datamaskintilkoblingen er på et IPv6-nettverk, merker du av for **IPv6**.
6. Under **Rediger regel** gjør du ett av følgende:
   - Velg **Enkel**, og angi deretter IP-adressen i boksen **IP-adresse**.
   - Velg **Område** og angi deretter start- og slutt-IP-adresser i boksene **Fra IP-adresse** og **Til IP-adresse**. Hvis datamaskintilkoblingen er på et IPv6-nettverk, angir du start-IP-adressen og prefikslengden i boksene **Fra IP-adresse** og **Prefikslengde**.
7. Velg eventuelt **Regel utløper om** og angi hvor mange dager regelen skal gjelde.
8. Skriv eventuelt inn en beskrivelse av regelen.
9. Klikk **OK**.

Fjerne en utestengt datamaskintilkobling

Du kan fjerne en utestengt datamaskintilkobling og tilkoblingens tilknyttede IP-adresse.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Utestengte IP-adresser**.
4. I ruten Utestengte IP-adresser velger du en IP-adresse, og klikker deretter **Fjern**.
5. Klikk **Ja** for å bekrefte.

Stenge ute en datamaskin fra loggen for innkommende hendelser

Du kan stenge ute en datamaskintilkobling og tilkoblingens tilknyttede IP-adresse fra loggen for innkommende hendelser. Bruk denne loggen, som viser IP-adressene til all innkommende Internett-trafikk, til å stenge ute en IP-adresse du tror er kilden til mistenkelig eller uønsket Internett-aktivitet.

Legg til en IP-adresse i listen **Utestengte IP-adresser** hvis du vil blokkere all innkommende Internett-trafikk fra denne IP-adressen, uansett om systemtjenesteportene er åpne eller lukkede.

1. Klikk **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. Klikk **Rapporter og logger**.
3. I **Nylige hendelser** klikker du **Vis logg**.
4. Klikk **Nettverk og Internett** og deretter **Innkommende hendelser**.
5. Velg en kilde-IP-adresse, og klikk **Utesteng denne IP-adressen** under **Jeg vil**.
6. Klikk **Ja** for å bekrefte.

Stenge ute en datamaskin fra loggen for inntrengingsoppdagelseshendelser

Du kan stenge ute en datamaskintilkobling og tilkoblingens tilknyttede IP-adresse fra loggen for inntrengingsoppdagelseshendelser.

1. Klikk **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
2. Klikk **Rapporter og logger**.
3. I **Nylige hendelser** klikker du **Vis logg**.
4. Klikk **Nettverk og Internett**, og klikk deretter **Inntrengingsoppdagelseshendelser**.
5. Velg en kilde-IP-adresse, og klikk **Utesteng denne IP-adressen** under **Jeg vil**.
6. Klikk **Ja** for å bekrefte.

KAPITTEL 20

Behandle systemtjenester

For at enkelte programmer (for eksempel webtjenere og tjenerprogrammer for fildeling) skal fungere riktig, må de godta uanmodede tilkoblinger fra andre datamaskiner via angitte systemtjenesteporter. Vanligvis lukker Firewall disse systemtjenesteportene fordi de utgjør den største kilden til sikkerhetshull og sårbarheter i systemet. For å godta tilkoblinger fra eksterne datamaskiner må imidlertid systemtjenesteportene være åpne.

I dette kapitlet

Konfigurere systemtjenesteporter

Systemtjenesteporter kan konfigureres til å tillate eller blokkere ekstern nettverkstilgang til en tjeneste på din datamaskin. Disse systemtjenesteportene kan åpnes eller lukkes for datamaskiner som er oppført som Klarert, Standard eller Offentlig i listen **Nettverk**.

Listen nedenfor viser de vanlige systemtjenestene og dere tilknyttede porter.

- Vanlig operativsystemport 5357
- Filoverføringsprotokollporter (FTP) 20-21
- E-posttjenerport (IMAP) 143
- E-posttjenerport (POP3) 110
- E-posttjenerport (SMTP) 25
- Microsofts katalogtjenerport (MSFT DS) 445
- Microsoft SQL Server-port (MSFT SQL) 1433
- Network Time Protocol Port 123
- Port 3389 for Remote Desktop / Remote Assistance / Terminal Server (RDP)
- RPC-kallport (Remote Procedure Calls) 135
- Sikker webtjenerport (HTTPS) 443
- Universal Plug and Play-port (UPNP) 5000
- Webtjenerport (HTTP) 80
- Fildelingsporter i Windows (NETBIOS) 137-139

Systemtjenesteporter kan også konfigureres til å tillate at en datamaskin deler Internett-tilkoblingene med andre datamaskiner koblet til den gjennom det samme nettverket. Denne forbindelsen, kjent som ICS (Internet Connection Sharing), tillater at datamaskinen deler forbindelsen for å fungere som en gateway til Internett for de andre datamaskinene i nettverket.

Merk: Hvis datamaskinen har et program som tillater enten Internett- eller FTP-servertilkoblinger, må datamaskinen som deler tilkoblingen, åpne den tilknyttede systemtjenesteporten og tillate videresending av innkommende tilkoblinger for disse portene.

Tillate tilgang til en eksisterende systemtjenesteport

Du kan åpne en eksisterende port for å tillate ekstern nettverkstilgang til en systemtjeneste på datamaskinen.

Merk: En åpen systemtjenesteport kan gjøre datamaskinen sårbar for Internett-sikkerhetstrusler. Åpne derfor bare en port hvis det er nødvendig.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Under **Åpne systemtjenesteport** velger du en systemtjeneste for å åpne porten for tjenesten.
5. Klikk **Rediger**.
6. Gjør ett av følgende:
   - Hvis du vil åpne porten på en datamaskin i et klarert, standard eller offentlig nettverk (for eksempel et hjemmenettverk, et bedriftsnettverk eller et Internett-nettverk), velger du **Klarert, Standard og Offentlig**.
   - Hvis du vil åpne porten på en datamaskin på et standard nettverk (for eksempel et bedriftsnettverk), velger du **Standard (inkluderer Klarert)**.
7. Klikk **OK**.

Blokkere tilgang til en eksisterende systemtjenesteport

Du kan lukke en eksisterende port for å blokkere ekstern nettverkstilgang til en systemtjeneste på datamaskinen.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Under **Åpne systemtjenesteport** fjerner du avmerkingen for systemtjenesteporten du vil lukke.
5. Klikk **OK**.

Konfigurere en ny systemtjenesteport

Du kan konfigurere en ny nettverkstjenesteport på datamaskinen som du kan åpne eller lukke for å tillate eller blokkere ekstern tilgang på datamaskinen.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Klikk **Legg til**.
5. I ruten for systemtjenester, under **Legg til regel i Systemtjenester**, legger du inn følgende:
   - Systemtjenestenavn
   - Systemtjenestekategori
   - Lokale TCP/IP-porter
   - Lokale UDP-porter
6. Gjør ett av følgende:
   - Hvis du vil åpne porten på en datamaskin i et klarert, standard eller offentlig nettverk (for eksempel et hjemmenettverk, et bedriftsnettverk eller et Internett-nettverk), velger du **Klarert, Standard og Offentlig**.
   - Hvis du vil åpne porten på en datamaskin på et standard nettverk (for eksempel et bedriftsnettverk), velger du **Standard (inkluderer Klarert)**.
7. Hvis du vil sende aktivitetsinformasjonen for denne porten til en annen datamaskin i Windows-nettverket som deler din Internett-tilkobling, velger du **Videresend nettverksaktivitet på denne porten til nettverkdatamaskiner som bruker Deling av Internett-tilkobling**.
8. Beskriv eventuelt den nye konfigurasjonen.
9. Klikk **OK**.

Merk: Hvis datamaskinen har et program som tillater enten Internett- eller FTP-servertilkoblinger, må datamaskinen som deler tilkoblingen, åpne den tilknyttede systemtjenesteporten og tillate videresending av innkommende tilkoblinger for disse portene. Hvis du bruker deling av Internett-tilkobling (ICS), må du også legge til en klarert dataforbindelse i listen **Nettverk**. Se Legg til en datamaskintilkobling for mer informasjon.

Endre en systemtjenesteport

Du kan endre informasjonen om inngående og utgående nettverkstilgang for en eksisterende systemtjenesteport.

Merk: Hvis portinformasjonen angis på feil måte, mislykkes systemtjenesten.

1. Klikk **Internett og nettverk** i ruten McAfee SecurityCenter, og klikk deretter **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Brannmurbeskyttelse er aktivert**, klikker du **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Klikk en avmerkingsboks ved siden av en systemtjeneste, og klikk deretter **Rediger**.
5. I ruten for systemtjenester, under **Legg til regel i Systemtjenester**, endrer du følgende:
   - Systemtjenestenavn
   - Lokale TCP/IP-porter
   - Lokale UDP-porter
6. Gjør ett av følgende:
   - Hvis du vil åpne porten på en datamaskin i et klarert, standard eller offentlig nettverk (for eksempel et hjemmenettverk, et bedriftsnettverk eller et Internett-nettverk), velger du **Klarert, Standard og Offentlig**.
   - Hvis du vil åpne porten på en datamaskin på et standard nettverk (for eksempel et bedriftsnettverk), velger du **Standard (inkluderer Klarert)**.
7. Hvis du vil sende aktivitetsinformasjonen for denne porten til en annen datamaskin i Windows-nettverket som deler din Internett-tilkobling, velger du **Videresend nettverksaktivitet på denne porten til nettverkdatamaskiner som bruker Deling av Internett-tilkobling**.
8. Beskriv eventuelt den endrede konfigurasjonen.
9. Klikk **OK**.

Fjerne en systemtjenesteport

Du kan fjerne en eksisterende systemtjenesteport fra datamaskinen. Etter at porten er fjernet, har ikke lenger eksterne datamaskiner tilgang til nettverkstjenesten på din datamaskin.

1. Klikk på **Internett- og nettverk** i ruten McAfee SecurityCenter, og klikk deretter på **Konfigurer**.
2. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
3. I Brannmur-ruten klikker du **Systemtjenester**.
4. Velg en systemtjeneste, og klikk deretter **Fjern**.
5. Når du blir spurt, klikk **Ja** for å bekrefte.

KAPITTEL 21

Logge, overvåke og analysere

Firewall tilbyr omfattende og lettlest logging, overvåking og analyse for Internett-hendelser og -trafikk. Å forstå Internett-trafikk og -hendelser kan være til hjelp når du skal administrere Internett-tilkoblingene dine.

I dette kapitlet

Hendelseslogging

Firewall lar deg aktivere eller deaktivere logging og hvilke hendelsestyper som skal logges når logging er aktivert. Hendelseslogging lar deg vise de siste innkommende og utgående hendelsene samt inntrengningshendelser.

Konfigurere innstillinger for hendelseslogg

Du kan angi og konfigurere alle typer Firewall-hendelser for logging. Som standardinnstilling er hendelseslogg aktivert for alle hendelser og aktiviteter.

1. I ruten Internett- og nettverkskonfigurasjon, under **Firewall-beskyttelse aktivert**, klikker du på **Avansert**.
2. I Brannmur-ruten klikker du **Innstillinger for hendelseslogg**.
3. Velg **Aktiver hendelseslogging** hvis det ikke allerede er valgt.
4. Under **Aktiver hendelseslogging** velger eller sletter du hendelsestyper som du ønsker eller ikke ønsker å logge. Hendelsestypene omfatter følgende:
   - Blokkerte programmer
   - ICMP-pinger
   - Trafikk fra utestengte IP-adresser
   - Hendelser på systemtjenesteporter
   - Hendelser på ukjente porter
   - Inntrengingsoppdagelseshendelser (IDS)
5. Hvis du vil hindre logging på bestemte porter, velger du **Ikke logg hendelser på følgende port(er)**, og deretter angir du enkelte portnumre atskilt med kommaer, eller portområder med bindestreker. For eksempel `137-139, 445, 400-5000`.
6. Klikk **OK**.

Vise nylige hendelser

Hvis logging er aktivert, kan du vise de nyeste hendelsene. Ruten Nylige hendelser viser datoen for og en beskrivelse av hendelsen. Det viser aktivitet for programmer som tilgang til Internett er blokkert for.

- Under Vanlige oppgaver på **Avansert meny** klikker du **Rapporter og logger** eller **Vis nyeste hendelser**. Du kan eventuelt klikke **Vis nyeste hendelser** under ruten Vanlige oppgaver fra Grunnleggende meny.

Vise innkommende hendelser

Hvis logging er aktivert, kan du vise innkommende hendelser. Innkommende hendelser inkluderer dato og tidspunkt, kildt-IP-adresse, vertsnavn og informasjon og hendelsestype.

1. Pass på at den avanserte menyen er aktivert. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk på **Nettverk & Internett** og deretter på **Innkommende hendelser**.

Merk: Du kan klarere, stenge ute og spore en IP-adresse fra loggen for innkommende hendelser.

Vise utgående hendelser

Hvis logging er aktivert, kan du vise utgående hendelser. Utgående hendelser omfatter navnet på programmet som prøver å få utgående tilgang, dato og klokkeslett for hendelsen og programmets plassering på datamaskinen.

1. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk på **Nettverk & Internett**, og klikk deretter på **Utgående hendelser**.

Merk: Du kan gi full tilgang og bare utgående tilgang til et program fra loggen for utgående hendelser. Du kan også finne tilleggsinformasjon om programmet.

Vise inntrengingsoppdagelseshendelser

Hvis logging er aktivert, kan du vise innkommende inntrengingshendelser. Inntrengingsoppdagelseshendelser viser dato og klokkeslett, kilde-IP, vertsnavnet for hendelsen og hendelsestypen.

1. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk **Nettverk & og Internett**, og klikk deretter **Inntrengingsoppdagelseshendelser**.

Merk: Du kan stenge ute og spore en IP-adresse fra loggen for inntrengingsoppdagelseshendelser.

Arbeide med statistikk

Firewall benytter McAfees HackerWatch-webområde om sikkerhet for å gi deg statistikk om globale Internett-sikkerhetshendelser og portaktivitet.

Vise statistikk for globale sikkerhetshendelser

HackerWatch sporer globale Internett-sikkerhetshendelser som du kan vise fra SecurityCenter. Sporet informasjon omfatter hendelser som er rapportert til HackerWatch de siste 24 timene, 7 dagene og 30 dagene.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **HackerWatch**.
3. Vis statistikk for sikkerhetshendelser under Event Tracking.

Vise global Internett-portaktivitet

HackerWatch sporer globale Internett-sikkerhetshendelser som du kan vise fra SecurityCenter. Informasjonen som vises, inkluderer portene med høyest hendelsesforekomst rapportert til HackerWatch de siste sju dagene. Vanligvis vises HTTP-, TCP- og UDP-informasjon.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **HackerWatch**.
3. Vis portene med høyest hendelsesforekomst under **Recent Port Activity** (Nyeste portaktivitet).

Spore Internett-trafikk

Firewall tilbyr en rekke alternativer for å spore Internett-trafikk. Disse alternativene lar deg spore en nettverksdatamaskin geografisk, få domene- og nettverksinformasjon samt spore datamaskiner fra loggene for innkommende hendelser og inntrengingsoppdagelseshendelser.

Spore en nettverksdatamaskin geografisk

Du kan bruke Visuell sporing til å finne ut hvor en datamaskin som kobler seg til eller prøver å koble seg til datamaskinen din, befinner seg geografisk, ved hjelp av navnet eller IP-adressen. Du kan også få tilgang til nettverks- og registreringsinformasjon ved hjelp av Visuell sporing. Når du kjører Visuell sporing, vises et verdenskart som viser den mest sannsynlige ruten data har tatt fra kildedatamaskinen til din maskin.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Visuell sporing**.
3. Skriv inn datamaskinens IP-adresse, og klikk **Spor**.
4. Under **Visuell sporing** velger du **Kartvisning**.

Merk: Du kan ikke spore private eller ugyldige IP-hendelser eller hendelser som går i løkke.

Få registreringsinformasjonen til en datamaskin

Du kan få registreringsinformasjonen til en datamaskin fra SecurityCenter ved hjelp av Visuell sporing. Informasjon inneholder domenenavnet, registrertes navn og adresse og administrasjonskontakt.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Visuell sporing**.
3. Skriv inn datamaskinens IP-adresse, og klikk deretter **Spor**.
4. Under **Visuell sporing** velger du **Registreringsvisning**.

Få nettverksinformasjonen til en datamaskin

Du kan få nettverksinformasjonen til en datamaskin fra SecurityCenter ved hjelp av Visuell sporing. Nettverksinformasjon inneholder detaljer om nettverket der domenet ligger.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Visuell sporing**.
3. Skriv inn datamaskinens IP-adresse, og klikk deretter **Spor**.
4. Under **Visuell sporing** velger du **Nettverksvisning**.

Spore en datamaskin fra loggen for innkommende hendelser

I ruten for innkommende hendelser kan du spore en IP-adresse som vises i loggen for innkommende hendelser.

1. Pass på at den avanserte menyen er aktivert. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk på **Nettverk & Internett** og deretter på **Innkommende hendelser**.
4. I ruten Innkommende hendelser velger du en kilde-IP-adresse, og klikker deretter **Spor denne IP-adressen**.
5. I ruten Visuell sporing klikker du én av følgende:
   - **Kartvisning**: Finne en datamaskin geografisk ved hjelp av den valgte IP-adressen.
   - **Registreringsvisning**: Finne domeneinformasjon ved hjelp av den valgte IP-adressen.
   - **Nettverksvisning**: Finne nettverksinformasjon ved hjelp av den valgte IP-adressen.
6. Klikk **Fullført**.

Spore en datamaskin fra loggen for inntrengingsoppdagelseshendelser

I ruten for inntrengingsoppdagelseshendelser kan du spore en IP-adresse som vises i loggen for inntrengingsoppdagelseshendelser.

1. I Vanlige oppgaver-ruten klikker du på **Rapporter og logger**.
2. I **Nylige hendelser** klikker du på **Vis logg**.
3. Klikk **Nettverk & og Internett**, og klikk deretter **Inntrengingsoppdagelseshendelser**.I ruten for inntrengingsoppdagelseshendelser velger du en kilde-IP-adresse, og klikker deretter **Spor denne IP-adressen**.
4. I ruten Visuell sporing klikker du én av følgende:
   - **Kartvisning**: Finne en datamaskin geografisk ved hjelp av den valgte IP-adressen.
   - **Registreringsvisning**: Finne domeneinformasjon ved hjelp av den valgte IP-adressen.
   - **Nettverksvisning**: Finne nettverksinformasjon ved hjelp av den valgte IP-adressen.
5. Klikk **Fullført**.

Spore en overvåket IP-adresse

Du kan spore en overvåket IP-adresse for å få en geografisk visning som viser den mest sannsynlige ruten for data fra kildedatamaskinen til din egen. I tillegg kan du få registrerings- og nettverksinformasjon om IP-adressen.

1. Kontroller at Avansert meny er aktivert, og klikk **Verktøy**.
2. I Verktøy-ruten klikker du **Trafikkovervåking**.
3. Under **Trafikkovervåking** klikker du **Aktive programmer**.
4. Velg et program og deretter IP-adressen som vises under programnavnet.
5. Under **Programaktivitet** klikker du **Spor denne IP-adressen**.
6. Under **Visuell sporing** kan du vise et kart som viser den mest sannsynlige ruten for data fra kildedatamaskinen til din egen. I tillegg kan du få registrerings- og nettverksinformasjon om IP-adressen.

Merk: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Visuell sporing**.

Overvåke Internett-trafikk

Firewall inneholder en rekke metoder for å overvåke Internett-trafikken, inkludert følgende:

- **Diagrammet Trafikkanalyse**: Viser nylig innkommende og utgående Internett-trafikk.
- **Diagrammet Trafikkbruk**: Viser prosentandelen av båndbredden brukt av de mest aktive programmene den siste 24-timersperioden.
- **Aktive programmer**: Viser de programmene som for øyeblikket bruker flest nettverkstilkoblinger på datamaskinen, og IP-adressene som programmene har tilgang til.

Om diagrammet Trafikkanalyse

Trafikkanalysediagrammet er en numerisk og grafisk representasjon av innkommende og utgående Internett-trafikk. I tillegg viser Trafikkovervåking programmene som bruker flest nettverkstilkoblinger på datamaskinen, og IP-adressene som programmene har tilgang til.

I Trafikkanalyse-ruten kan du vise den siste innkommende og utgående Internett-trafikken samt gjeldende, gjennomsnittlige og maksimale overføringshastigheter. Du kan også vise trafikkvolum, inkludert trafikkmengden siden du startet Firewall, og den totale trafikken for gjeldende måned og tidligere måneder.

Trafikkanalyse-ruten viser Internett-aktivitet på datamaskinen i sanntid, inkludert volumet og hastigheten på den nylig innkommende og utgående Internett-trafikken på datamaskinen, tilkoblingshastighet og totalt antall byte som er overført over Internett.

Den heltrukne grønne streken representerer gjeldende overhøringshastighet for innkommende trafikk. Den prikkete grønne streken representerer gjennomsnittlig overføringshastighet for innkommende trafikk. Hvis gjeldende overføringshastighet og gjennomsnittlig overføringshastighet er den samme, vises ikke den prikkete streken på diagrammet. Den heltrukne streken representerer både gjennomsnittlig og gjeldende overføringshastighet.

Den heltrukne røde streken representerer gjeldende overføringshastighet for utgående trafikk. Den røde prikkete streken representerer gjennomsnittlig overføringshastighet for utgående trafikk. Hvis gjeldende overføringshastighet og gjennomsnittlig overføringshastighet er den samme, vises ikke den prikkete streken på diagrammet. Den heltrukne streken representerer både gjennomsnittlig og gjeldende overføringshastighet.

Analysere innkommende og utgående trafikk

Trafikkanalysediagrammet er en numerisk og grafisk representasjon av innkommende og utgående Internett-trafikk. I tillegg viser Trafikkovervåking programmene som bruker flest nettverkstilkoblinger på datamaskinen, og IP-adressene som programmene har tilgang til.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Trafikkovervåking**.
3. Under **Trafikkovervåking** klikker du **Trafikkanalyse**.

Tips: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Trafikkanalyse**.

Overvåke båndbredden for et program

Du kan vise sektordiagrammet som viser hvor stor omtrentlig prosentandel av båndbredden som de mest aktive programmene på datamaskinen har brukt i løpet av de siste 24 timene. Sektordiagrammet gir en visuell presentasjon av den relative delen av båndbredden som brukes av programmene.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Trafikkovervåking**.
3. Under **Trafikkovervåking** klikker du **Trafikkbruk**.

Tips: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Trafikkbruk**.

Overvåke programaktivitet

Du kan vise innkommende og utgående programaktivitet, som viser tilkoblinger og porter for eksterne datamaskiner.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **Trafikkovervåking**.
3. Under **Trafikkovervåking** klikker du **Aktive programmer**.

4 Du kan vise følgende informasjon:

- Diagram for programaktivitet: Velg et program for å vise et diagram over programmets aktivitet.
- Lyttende tilkobling: Velg et lyttende element under programnavnet.
- Datamaskintilkobling: Velg en IP-adresse under programnavnet, systemprosessen eller tjenesten.

Merk: Hvis du vil vise den mest oppdaterte statistikken, klikker du **Oppdater** under **Aktive programmer**.

KAPITTEL 22

Lære om Internett-sikkerhet

Firewall benytter McAfees webområde om sikkerhet, HackerWatch, til å gi oppdatert informasjon om programmer og global Internett-aktivitet. HackerWatch inneholder også en HTML-brukeropplæring om Firewall.

I dette kapitlet

Starte HackerWatch-brukeropplæringen

Hvis du vil lære mer om Firewall, kan du åpne HackerWatch-opplæringen fra SecurityCenter.

1. Kontroller at Avansert meny er aktivert, og klikk deretter **Verktøy**.
2. I Verktøy-ruten klikker du **HackerWatch**.
3. Under **HackerWatch Resources** (HackerWatch-ressurser) klikker du **View Tutorial** (Vis brukeropplæring).

KAPITTEL 23

McAfee QuickClean

QuickClean forbedrer datamaskinens yteevne ved å slette filer som kan skape rot på datamaskinen. Programmet tømmer papirkurven og sletter midlertidige filer, snarveier, tapte filfragmenter, registerfiler, hurtiglagrede filer, informasjonskapsler, loggfiler i webleseren, sendt og slettet e-post, nylig brukte filer, Active-X-filer og filer med systemgjenopprettingspunkter. QuickClean ivaretar dessuten personvernet ved å bruke McAfee Shredder-programmet til trygt og permanent å slette elementer som kan inneholde følsomme personopplysninger som navn og adresse. Se McAfee Shredder for å lese mer om makulering av filer.

Diskdefragmentering rydder i filer og mapper på datamaskinen for å sikre at de ikke blir spredt (dvs. fragmentert) når de lagres på datamaskinens harddisk. Med regelmessig defragmentering av harddisken kan disse fragmenterte filene og mappene raskt hentes frem igjen senere.

Ønsker du ikke å vedlikeholde datamaskinen manuelt, er det mulig å planlegge det slik at både QuickClean og diskdefragmenteringen går automatisk og uavhengig uansett hyppighet.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

QuickClean-funksjoner

Renseprogram for filer

Slett unødvendige filer trygt og effektivt ved hjelp av ulike rensefunksjoner. Plassen på datamaskinens harddisk blir dermed større og yteevnen bedre.

KAPITTEL 24

Rens av datamaskinen

QuickClean sletter filer som kan lage rot på datamaskinen. Programmet tømmer papirkurven og sletter midlertidige filer, snarveier, tapte filfragmenter, registerfiler, hurtiglagrede filer, informasjonskapsler, loggfiler i nettleseren, sendt og slettet e-post, nylig brukte filer, Active-X-filer og filer med systemgjenopprettingspunkter. QuickClean sletter disse elementene uten at det får betydning for annen sentral informasjon.

Alle rensefunksjonene i QuickClean kan brukes til å slette unødvendige filer fra datamaskinen. Følgende tabell beskriver rensefunksjonene i QuickClean:

Navn	Funksjon
Papirkurvrens	Sletter filer i papirkurven.
Rens for midlertidige filer	Sletter filer som er lagret i midlertidige mapper.
Snarveirens	Sletter ødelagte snarveier eller snarveier uten tilknyttet program.
Rens for tapte filfragmenter	Sletter tapte filfragmenter på datamaskinen.
Registerrens	Sletter registerinformasjon i Windows® for programmer som ikke lenger finnes på maskinen. Registeret er en database der Windows lagrer konfigurasjonsinformasjon. Registeret inneholder profiler for hver datamaskinbruker og informasjon om maskinvare, installerte programmer og egenskapsinnstillinger. Windows forsyner denne informasjonen med kontinuerlige henvisninger mens systemet kjører.
Hurtiglagerrens	Sletter hurtiglagrede filer som hoper seg opp under Internett-surfing. Disse filene lagres vanligvis som midlertidige filer i en hurtiglagermappe. En hurtiglagermappe er et midlertidig lagringsområde på datamaskinen. Nettleseren kan hente en nettside fra hurtiglageret (istedenfor en ekstern server) neste gang siden skal åpnes, og dermed sørge for raskere og mer effektiv navigering.

Navn	Funksjon
Informasjonskapselrens	Sletter informasjonskapsler. Disse filene er som regel lagret som midlertidige filer. En informasjonskapsel er en liten fil som inneholder informasjon, vanligvis med brukernavn og gjeldende dato og klokkeslett, som en person som navigerer på nettet, har lagret på maskinen. Informasjonskapsler brukes i all hovedsak av webområder til å identifisere brukere som tidligere har registrert seg på eller besøkt området, men de kan også være en kilde til informasjon for hackere.
Loggrens	Sletter loggen i nettleseren.
Rens av Outlook Express og Outlook E-mail (sendte og slettede elementer):	Sletter sendt og slettet e-post fra Outlook® og Outlook Express.
Nylig brukt rens	Sletter nylig brukte filer som er opprettet med et av disse programmene: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX-rens	Sletter ActiveX-kontroller. Active X er en programvarekomponent som programmer eller nettsider bruker til å tilføye funksjonalitet som glir inn og fremstår som en normal del av programmet eller nettsiden. De fleste ActiveX-kontrollene er harmløse, men noen kan innhente informasjon fra datamaskinen.

Navn	Funksjon
Rens for systemgjenopprettingspunkt	Sletter gamle systemgjenopprettingspunkter (bortsett fra de nyeste) fra datamaskinen. Windows oppretter systemgjenopprettingspunkter for å markere endringer på datamaskinen. Datamaskinen kan dermed gå tilbake til en tidligere tilstand hvis det oppstår problemer.

I dette kapitlet

Rens av datamaskinen

Alle rensefunksjonene i QuickClean kan brukes til å slette unødvendige filer fra datamaskinen. Etterpå er det under **Sammendrag av QuickClean** mulig å vise hvor mye diskplass som er igjen etter rensen, hvor mange filer som ble slettet, og dato og klokkeslett for når QuickClean sist ble kjørt på maskinen.

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **MacAfee QuickClean**.
3. Gjør ett av følgende:
   - Klikk på **Neste** for å godta standardrensefunksjonene i listen.
   - Velg eller fjern de ønskede rensefunksjonene, og klikk deretter på **Neste.** Hvis "Nylig brukt rensefunksjon" velges, er det mulig å klikke på **Egenskaper** for å velge eller fjerne filene som nylig ble opprettet med programmene i listen, og deretter klikke på **OK**.
   - Klikk på **Gjenopprett standardinnstillingene** for å gjenopprette standardrensefunksjonene, og klikk deretter på **Neste**.
4. Klikk på **Neste** når analysen er fullført.
5. Klikk på **Neste** for å bekrefte filslettingen.

6 Gjør ett av følgende:

- Klikk på **Neste** for å godta standardvalget **Nei, jeg vil slette filene med standard Windows-sletting**.
- Klikk på **Ja, jeg vil utføre sikker fjerning med Shredder**, oppgi antall omganger (opptil 10) og klikk deretter på **Neste**. Det kan ta lang tid å makulere filer hvis mye informasjon er slettet.

7 Hvis filer eller elementer var låst under rensen, kan det hende datamaskinen må startes på nytt. Klikk på **OK** for å lukke meldingen.

8 Klikk på **Fullfør**.

Merknad: Filer som slettes med Shredder, kan ikke gjenopprettes. Se McAfee Shredder for å lese mer om makulering av filer.

KAPITTEL 25

Defragmentering av datamaskinen

Diskdefragmentering rydder i filer og mapper på datamaskinen for å sikre at de ikke blir spredt (dvs. fragmentert) når de lagres på datamaskinens harddisk. Med regelmessig defragmentering av harddisken kan disse fragmenterte filene og mappene raskt hentes frem igjen senere.

Defragmentering av datamaskinen

Datamaskinen kan defragmenteres, slik at det blir bedre tilgang til filer og mapper.

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Analyser** under **Diskdefragmentering**.
3. Følg instruksene på skjermen.

Merknad: Se Windows-hjelpen for å lese mer om diskdefragmentering.

KAPITTEL 26

Planlegging av oppgave

Oppgaveplanlegging sørger for at det går automatikk i hvor ofte QuickClean eller diskdefragmenteringen kjøres på maskinen. Eksempelvis kan det planlegges at en QuickClean-oppgave skal tømme papirkurven hver søndag kl. 9.00 eller at en diskdefragmenteringsoppgave skal gå gjennom harddisken siste dag i hver måned. Oppgaver kan opprettes, endres eller slettes når som helst. Det er nødvendig å være logget på datamaskinen for at en planlagt oppgave skal kjøres. Hvis en oppgave av en eller annen grunn ikke kjøres, blir den planlagt på nytt fem minutter etter neste pålogging.

Planlegging av QuickClean-oppgave

QuickClean-oppgaver kan planlegges slik at de automatisk renser datamaskinen med én eller flere rensefunksjoner. Når oppgaven er ferdig, er det under **Sammendrag av QuickClean** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1. Åpne "Oppgaveplanlegging"-ruten.

   Hvordan?

   1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
   2. Klikk på **Start** under **Oppgaveplanlegging**.

2. Klikk på **McAfee QuickClean** i **Velg operasjon du ønsker å planlegge**-listen.
3. Legg inn navn på oppgaven i **Oppgavenavn**-boksen, og klikk deretter på **Opprett**.
4. Gjør ett av følgende:
   - Klikk på **Neste** for å godta rensefunksjonene i listen.
   - Velg eller fjern de ønskede rensefunksjonene, og klikk deretter på **Neste**. Hvis "Nylig brukt rensefunksjon" velges, er det mulig å klikke på **Egenskaper** for å velge eller fjerne filene som nylig ble opprettet med programmene i listen, og deretter klikke på **OK**.
   - Klikk på **Gjenopprett standardinnstillingene** for å gjenopprette standardrensefunksjonene, og klikk deretter på **Neste**.
5. Gjør ett av følgende:
   - Klikk på **Planlegg** for å godta standardalternativet **Nei, jeg vil slette filene med standard Windows-sletting**.

- Klikk på **Ja, jeg vil utføre sikker fjerning med Shredder**, oppgi antall omganger (opptil 10) og klikk deretter på **Planlegg**.

6 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

7 Hvis egenskapene for "Nylig brukte rensefunksjoner" ble endret, kan det hende at datamaskinen må startes på nytt. Klikk på **OK** for å lukke meldingen.

8 Klikk på **Fullfør**.

Merknad: Filer som slettes med Shredder, kan ikke gjenopprettes. Se McAfee Shredder for å lese mer om makulering av filer.

Endring av QuickClean-oppgave

Planlagte QuickClean-oppgaver kan endres slik at andre rensefunksjoner brukes, eller slik at oppgaven ikke kjøres like ofte på maskinen. Når oppgaven er ferdig, er det under **Sammendrag av QuickClean** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1 Åpne "Oppgaveplanlegging"-ruten.

   Hvordan?

   1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
   2. Klikk på **Start** under **Oppgaveplanlegging**.

2 Klikk på **McAfee QuickClean** i **Velg operasjon du ønsker å planlegge**-listen.

3 Velg oppgave i **Velg en eksisterende oppgave**-listen, og klikk deretter på **Endre**.

4 Gjør ett av følgende:

- Klikk på **Neste** for å godta rensefunksjonene som er valgt til oppgaven.
- Velg eller fjern de ønskede rensefunksjonene, og klikk deretter på **Neste**. Hvis "Nylig brukt rensefunksjon" velges, er det mulig å klikke på **Egenskaper** for å velge eller fjerne filene som nylige ble opprettet med programmene i listen, og deretter klikke på **OK**.
- Klikk på **Gjenopprett standardinnstillingene** for å gjenopprette standardrensefunksjonene, og klikk deretter på **Neste**.

5 Gjør ett av følgende:

- Klikk på **Planlegg** for å godta standardalternativet **Nei, jeg vil slette filene med standard Windows-sletting**.

- Klikk på **Ja, jeg vil utføre sikker fjerning med Shredder**, oppgi antall omganger (opptil 10) og klikk deretter på **Planlegg**.

6 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

7 Hvis egenskapene for "Nylig brukte rensefunksjoner" ble endret, kan det hende at datamaskinen må startes på nytt. Klikk på **OK** for å lukke meldingen.

8 Klikk på **Fullfør**.

Merknad: Filer som slettes med Shredder, kan ikke gjenopprettes. Se McAfee Shredder for å lese mer om makulering av filer.

Sletting av QuickClean-oppgave

Planlagte QuickClean-oppgaver kan slettes hvis de ikke lenger skal kjøre automatisk.

1 Åpne "Oppgaveplanlegging"-ruten.

Hvordan?

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **Oppgaveplanlegging**.

2 Klikk på **McAfee QuickClean** i **Velg operasjon du ønsker å planlegge**-listen.

3 Velg oppgave i **Velg en eksisterende oppgave**-listen.

4 Klikk på **Slett** og deretter **Ja** for å bekrefte slettingen.

5 Klikk på **Fullfør**.

Planlegging av diskdefragmenteringsoppgave

Det er mulig å planlegge hvor ofte diskdefragmenteringsoppgaver skal kjøres automatisk på datamaskinen. Når oppgaven er ferdig, er det under **Diskdefragmentering** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1 Åpne "Oppgaveplanlegging"-ruten.

   Hvordan?

   1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
   2. Klikk på **Start** under **Oppgaveplanlegging**.

2 Klikk på **Diskdefragmentering** i **Velg operasjon du ønsker å planlegge**-listen.

3 Legg inn navn på oppgaven i **Oppgavenavn**-boksen, og klikk deretter på **Opprett**.

4 Gjør ett av følgende:

   - Klikk på **Planlegg** for å godta standardvalget **Kjør defragmentering selv om det er lite ledig plass**.
   - Fjern **Kjør defragmentering selv om det er lite ledig plass**-alternativet, og klikk deretter på **Planlegg**.

5 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

6 Klikk på **Fullfør**.

Endring av diskdefragmenteringsoppgave

Det er mulig å endre hvor ofte planlagte diskdefragmenteringsoppgaver skal kjøres automatisk på maskinen. Når oppgaven er ferdig, er det under **Diskdefragmentering** mulig å vise dato og klokkeslett for neste gang det er planlagt å kjøre oppgaven.

1 Åpne "Oppgaveplanlegging"-ruten.

   Hvordan?

   1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
   2. Klikk på **Start** under **Oppgaveplanlegging**.

2 Klikk på **Diskdefragmentering** i **Velg operasjon du ønsker å planlegge**-listen.

3 Velg oppgave i **Velg en eksisterende oppgave**-listen, og klikk deretter på **Endre**.

4 Gjør ett av følgende:

- Klikk på **Planlegg** for å godta standardvalget **Kjør defragmentering selv om det er lite ledig plass**.
- Fjern **Kjør defragmentering selv om det er lite ledig plass**-alternativet, og klikk deretter på **Planlegg**.

5 Velg hvor ofte oppgaven skal kjøres i dialogboksen **Planlegg**, og klikk deretter på **OK**.

6 Klikk på **Fullfør**.

Sletting av diskdefragmenteringsoppgave

Planlagte diskdefragmenteringsoppgaver kan slettes hvis de ikke lenger skal kjøres automatisk.

1 Åpne "Oppgaveplanlegging"-ruten.

Hvordan?

1. Klikk på **Vedlikehold datamaskin** under **Vanlige oppgaver** i "McAfee SecurityCenter"-ruten.
2. Klikk på **Start** under **Oppgaveplanlegging**.

2 Klikk på **Diskdefragmentering** i **Velg operasjon du ønsker å planlegge**-listen.

3 Velg oppgave i **Velg en eksisterende oppgave**-listen.

4 Klikk på **Slett** og deretter **Ja** for å bekrefte slettingen.

5 Klikk på **Fullfør**.

KAPITTEL 27

McAfee Shredder

McAfee Shredder sletter (eller makulerer) elementer permanent og fjerner dem fra datamaskinens harddisk. Selv når man sletter filer og mapper manuelt, tømmer papirkurven eller sletter mappen med midlertidige Internett-filer, er det fortsatt mulig å gjenopprette denne informasjonen med kriminaltekniske dataverktøy. Dessuten kan slettede filer gjenopprettes fordi noen programmer lager midlertidige, skjulte kopier av åpne filer. Shredder ivaretar personvernet ved å slette uønskede filer trygt og permanent. Det er viktig å huske på at makulerte filer ikke kan gjenopprettes.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Shredder-funksjoner

Slette valgte filer og mapper permanent

Fjern elementer fra datamaskinens harddisk slik at den tilknyttede informasjonen ikke kan gjenopprettes. Dette beskytter personvernet ved trygt og permanent å slette filer og mapper, elementer i papirkurven og mappen med midlertidige Internett-filer og alt innholdet på datadisker som skrivbare CD-er, eksterne harddisker og disketter.

Makulering av filer, mapper og disker

Shredder sørger for at informasjonen i slettede filer og mapper i papirkurven og i mappen med midlertidige Internett-filer ikke kan gjenopprettes, ikke engang med spesialverktøy. Med Shredder er det mulig å oppgi hvor mange ganger (opptil 10) et element skal makuleres. Jo flere ganger et element makuleres, desto tryggere er filslettingen.

Makulering av filer og mapper

Filer og mapper, deriblant elementer i papirkurven og mappen med midlertidige Internett-filer, kan makuleres og fjernes fra datamaskinens harddisk.

1 Åpne **Shredder**.

   Hvordan?

   1. Klikk på **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
   2. Klikk på **Verktøy** i den venstre ruten.
   3. Klikk på **Shredder**.

2 Klikk på **Slette filer og mapper** under **Jeg vil** i "Makuler filer og mapper"-ruten.

3 Klikk på ett av følgende makuleringsnivåer under **Makuleringsnivå**:

   - **Raskt**: Makulerer det eller de valgte elementene én gang.
   - **Omfattende**: Makulerer det eller de valgte elementene 7 ganger.
   - **Egendefinert**: Makulerer det eller de valgte elementene opptil 10 ganger.

4 Klikk på **Neste**.

5 Gjør ett av følgende:

   - Klikk enten på **Innhold i papirkurven** eller **Midlertidige Internett-filer** i **Velg filen(e) du vil makulere**-listen.
   - Klikk på **Bla gjennom**, naviger til filen som skal makuleres, velg den og klikk deretter på **Åpne**.

6 Klikk på **Neste**.

7 Klikk på **Start**.

8 Klikk på **Fullført** når Shredder er ferdig.

Merknad: Ikke arbeid med disse filene før Shredder har fullført oppgaven.

Makulering av hel disk

Det er mulig å slette alt innholdet på en disk i én operasjon. Bare flyttbare stasjoner som eksterne harddisker, skrivbare CD-er og disketter kan makuleres.

1 Åpne **Shredder**.

   Hvordan?

   1. Klikk på **Avansert meny** under **Vanlige oppgaver** i ruten McAfee SecurityCenter.
   2. Klikk på **Verktøy** i den venstre ruten.
   3. Klikk på **Shredder**.

2 Klikk på **Slette en hel disk** under **Jeg vil** i "Makuler filer og mapper"-ruten.

3 Klikk på ett av følgende makuleringsnivåer under **Makuleringsnivå**:

   - **Raskt**: Makulerer den valgte disken én gang.
   - **Omfattende**: Makulerer den valgte disken 7 ganger.
   - **Egendefinert**: Makulerer den valgte disken opptil 10 ganger.

4 Klikk på **Neste**.

5 Klikk på den disken i **Velg disk**-listen som skal makuleres.

6 Klikk på **Neste** og deretter **Ja** for å bekrefte.

7 Klikk på **Start**.

8 Klikk på **Fullført** når Shredder er ferdig.

Merknad: Ikke arbeid med disse filene før Shredder har fullført oppgaven.

KAPITTEL 28

McAfee Network Manager

Network Manager gir en grafisk visning av datamaskinen og andre enheter som hjemmenettverket ditt består av. Du kan bruke Network Manager til å eksternt å administrere beskyttelsesstatusen på hver administrerte datamaskin i nettverket, og eksternt reparere rapporterte sikkerhetsproblemer på de administrerte datamaskinene. Hvis du har installert McAfee Total Protection, kan Network Manager også overvåke nettverket med henblikk på inntrengere (datamaskiner eller enheter du ikke gjenkjenner eller har klarert) som prøver å koble til det.

Før du begynner å bruke Network Manager, kan du gjøre deg kjent med noen av funksjonene. Du finner mer informasjon om hvordan du konfigurerer og bruker disse funksjonene, i hjelpen for Network Manager.

Merk: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

Network Manager funksjoner

Grafisk nettverkskart

Vis en grafisk oversikt over beskyttelsesstatusen til datamaskinene og enhetene som utgjør hjemmenettverket ditt. Når du foretar endringer i nettverket (for eksempel legger til en ny datamaskin), gjenkjenner nettverkskartet disse endringene. Du kan oppdatere nettverkskartet, gi nettverket et nytt navn samt vise/skjule komponenter på nettverkskartet for å tilpasse visningen. Du kan også vise detaljer om enhetene som vises på nettverkskartet.

Ekstern administrasjon

Administrer beskyttelsesstatusen til datamaskinene som utgjør hjemmenettverket ditt. Du kan invitere en datamaskin til å koble seg til det administrerte nettverket, overvåke den administrerte datamaskinens beskyttelsesstatus samt fikse kjente sikkerhetshull for en ekstern datamaskin på nettverket.

Nettverksovervåking

Hvis du har Network Manager, kan det overvåke nettverkene og varsle deg når venner eller inntrengere kobler til. Nettverksovervåking er bare tilgjengelig hvis du har kjøpt McAfee Total Protection.

Forstå Network Manager-ikoner

Den følgende tabellen beskriver ikonene som oftest blir brukt i nettverkskartet i Network Manager.

Ikon	Beskrivelse
	Representerer en administrert datamaskin som er frakoblet
	Representerer en administrert datamaskin som er frakoblet
	Representerer en ikke-administrert datamaskin som har SecurityCenter installert
	Representerer en frakoblet datamaskin som ikke er administrert
	Representerer en tilkoblet datamaskin som ikke har SecurityCenter installert, eller en ukjent nettverksenhet
	Representerer en tilkoblet datamaskin som ikke har SecurityCenter installert, eller en ikke tilkoblet, ukjent nettverksenhet
	Betyr at det tilsvarende elementet er beskyttet og tilkoblet
	Betyr at det tilsvarende elementet kan kreve ditt tilsyn
	Betyr at det tilsvarende elementet krever umiddelbart ditt tilsyn
	Representerer en trådløs ruter
	Representerer en vanlig ruter
	Representerer Internett, når det er tilkoblet
	Representerer Internett, når det er frakoblet

KAPITTEL 29

Sette opp et administrert nettverk

Du konfigurerer et administrert nettverk ved å klarere nettverket (hvis du ikke allerede har gjort det) og legge til medlemmer (datamaskiner) i det. Før en datamaskin kan administreres eksternt, eller gis tillatelse til å administrere andre datamaskiner via nettverket, må den bli et klarert medlem av nettverket. Nettverksmedlemskap blir gitt nye datamaskiner av eksisterende nettverksmedlemmer (datamaskiner) med administrative rettigheter.

Du kan vise detaljer om elementene som vises på nettverkskartet, selv etter at du har foretatt endringer i nettverket (for eksempel lagt til en datamaskin).

I dette kapitlet

Arbeide med nettverkskartet

Når du kobler en datamaskin til nettverket, analyserer Network Manager nettverkets tilstand for å finne ut om det er noen administrerte eller ikke-administrerte medlemmer tilkoblet, hva ruterens egenskaper er, og Internett-status. Hvis ingen medlemmer er tilkoblet, tar Network Manager utgangspunkt i at den datamaskinen som for øyeblikket er koblet til, er den første datamaskinen i nettverket, og registrerer denne datamaskinen som et administrert medlem med administrative rettigheter. Nettverksnavnet inkluderer som standard navnet på den første datamaskinen som kobler seg til med SecurityCenter installert. Du kan imidlertid gi nettverket et nytt navn når som helst.

Når du endrer noe i nettverket (for eksempel hvis du legger til en datamaskin), kan du tilpasse nettverkskartet. Du kan for eksempel oppdatere nettverkskartet, gi nettverket nytt navn og tilpasse visningen ved å skjule eller vise elementer i nettverket. Du kan også vise detaljer om elementene som vises på nettverkskartet.

Få tilgang til nettverkskartet

Nettverkskartet gir en grafisk fremstilling av datamaskinene og enhetene som hjemmenettverket består av.

- Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.

Merk: Hvis du ikke allerede har klarert nettverket (ved hjelp av McAfee Personal Firewall), blir du bedt om å gjøre dette første gang du bruker nettverkskartet.

Oppdatere nettverkskartet

Du kan oppdatere nettverkskartet når som helst, for eksempel etter at en annen datamaskin har logget seg på det administrerte nettverket.

1. Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.
2. Klikk **Oppdater nettverkskart** under **Jeg vil**.

Merk: Koblingen **Oppdater nettverkskart** er bare tilgjengelig hvis ingen elementer er valgt på nettverkskartet. Hvis du vil oppheve valget av et element, klikker du det valgte elementet eller klikker i et blankt område på nettverkskartet.

Gi nettverket nytt navn

Nettverksnavnet inkluderer som standard navnet på den første datamaskinen som kobler seg til nettverket med SecurityCenter installert. Hvis du ønsker å bruke et annet navn, kan du endre det.

1 Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.

2 Klikk **Gi nettverket nytt navn** under **Jeg vil**.

3 Skriv inn navnet på nettverket i boksen **Nettverksnavn**.

4 Klikk **OK**.

Merk: Koblingen **Gi nettverket nytt navn** er bare tilgjengelig hvis ingen elementer er valgt på nettverkskartet. Hvis du vil oppheve valget av et element, klikker du det valgte elementet eller klikker i et blankt område på nettverkskartet.

Vise eller skjule et element på nettverkskartet

Alle datamaskiner og elementer i hjemmenettverket vises på nettverkskartet som standard. Du kan imidlertid vise elementer igjen som du har skjult tidligere. Kun ikke-administrerte elementer kan skjules. Administrerte datamaskiner kan ikke skjules.

For å...	Klikk Behandle nettverk på menyen Grunnleggende eller Avansert, og gjør deretter følgende...
Skjule et element på nettverkskartet	Klikk et element på nettverkskartet og klikk **Skjul dette elementet** under **Jeg vil**. Klikk **Ja** i bekreftelsesdialogboksen.
Vise skjulte elementer på nettverkskartet	Klikk **Vis skjulte elementer** under **Jeg vil**.

Vise detaljer for et element

Du kan vise detaljert informasjon om alle elementer i nettverket hvis du velger det på nettverkskartet. Denne informasjonen inkluderer elementnavnet, beskyttelsesstatusen og annen informasjon som er nødvendig for å administrere elementet.

1 Klikk elementets ikon på nettverkskartet.

2 Vis informasjonen om elementet under **Detaljer**.

Koble til det administrerte nettverket

Før en datamaskin kan administreres eksternt, eller gis tillatelse til å administrere andre datamaskiner via nettverket, må den bli et klarert medlem av nettverket. Nettverksmedlemskap blir gitt nye datamaskiner av eksisterende nettverksmedlemmer (datamaskiner) med administrative rettigheter. For å sikre at bare klarerte datamaskiner kobler seg til nettverket, må brukeren på datamaskinen som gir tilgang til nettverket, og brukeren på datamaskinen som kobler seg til nettverket, autentifisere hverandre.

Når en datamaskin kobles til nettverket, blir den bedt om å dele sin McAfee-beskyttelsesstatus med de andre datamaskinene i nettverket. Hvis en datamaskin går med på å dele beskyttelsesstatusen sin, blir den et administrert medlem av nettverket. Hvis en datamaskin ikke går med på å dele beskyttelsesstatusen sin, blir den et ikke-administrert medlem av nettverket. Ikke-administrerte nettverksmedlemmer er vanligvis gjestemaskiner som vil ha tilgang til andre nettverksfunksjoner (for eksempel sende filer eller dele skrivere).

Merk: Hvis du har andre McAfee-nettverksprogrammer installert (for eksempel EasyNetwork), blir datamaskinen også gjenkjent som et administrert medlem i disse programmene, etter at du har koblet den til. Tillatelsesnivået som er tildelt en datamaskin i Network Manager, gjelder for alle McAfee-nettverksprogrammer. Hvis du vil ha mer informasjon om hva gjestetilgang, full tilgang eller administrative rettigheter betyr i andre McAfee-nettverksprogrammer, kan du se i dokumentasjonen som følger med programmet.

Koble til et administrert nettverk

Når du får en invitasjon om å koble til et administrert nettverk, kan du godta den eller avslå den. Du kan også bestemme om du ønsker at de andre datamaskinene i nettverket skal kunne administrere sikkerhetsinnstillingene for denne datamaskinen.

1. I dialogboksen for det administrerte nettverket kontrollerer du at det er merket av for **Tillat enhver datamaskin i dette nettverket å administrere sikkerhetsinnstillinger**.
2. Klikk **Koble til**.
   Når du godtar invitasjonen, vises to spillekort.
3. Bekreft at det er de samme spillekortene som vises på datamaskinen som inviterte deg til å koble til det administrerte nettverket.
4. Klikk **OK**.

Merk: Hvis datamaskinen som inviterte deg til å koble til det administrerte nettverket, ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd i det administrerte nettverket. Det kan utgjøre en sikkerhetsrisiko for datamaskinen å koble til nettverket. Klikk derfor **Avbryt** i dialogboksen for det administrerte nettverket.

Invitere en datamaskin til å koble seg til det administrerte nettverket

Hvis en datamaskin blir lagt til i det administrerte nettverket, eller hvis det er en annen ikke-administrert datamaskin i nettverket, kan du invitere datamaskinen til å koble seg til det administrerte nettverket. Bare datamaskiner med administrative rettigheter til nettverket kan invitere andre datamaskiner til å koble seg til. Når du sender en invitasjon, spesifiserer du også tillatelsesnivået du ønsker å tildele det nye medlemmet.

1. Klikk ikonet til den ikke-administrerte datamaskinen på nettverkskartet.
2. Klikk **Administrer denne datamaskinen** under **Jeg vil**.
3. I dialogboksen for å invitere en datamaskin til å koble seg til det administrerte nettverket gjør du ett av følgende:
   - Klikk **Gi gjest tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket (du kan bruke dette alternativet for midlertidige brukere i ditt hjem).
   - Klikk **Gi full tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket.

- Klikk **Gi administrative rettigheter til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket med administrative rettigheter. Datamaskinen kan også gi tilgang til andre datamaskiner som vil bli med i det administrerte nettverket.

4 Klikk **OK**.
En invitasjon til å koble til det administrerte nettverket blir sendt til datamaskinen. Når datamaskinen godtar invitasjonen, vises to spillekort.

5 Bekreft at det er de samme spillekortene som vises på datamaskinen du inviterte til å koble seg til det administrerte nettverket.

6 Klikk **Gi tilgang**.

Merk: Hvis datamaskinen du inviterte til å koble til det administrerte nettverket, ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd i det administrerte nettverket. Det å gi datamaskinen tilgang til å koble til nettverket, kan utgjøre en sikkerhetsrisiko for andre datamaskiner. Klikk derfor **Nekt tilgang** i dialogboksen for sikkerhetsbekreftelse.

Slutte å stole på datamaskiner i nettverket

Hvis du stolte på andre datamaskiner i nettverket ved en feil, kan du stoppe å stole på dem.

- Klikk på**Slutt å stole på datamaskiner i dette nettverket** under **Jeg vil**.

Merk: Koblingen for å slutte å stole på datamaskiner i dette nettverket er ikke tilgjengelig hvis du har administrative rettigheter og det er andre administrerte datamaskiner i nettverket.

KAPITTEL 30

Administrere nettverket eksternt

Når du har konfigurert et administrert nettverk, kan du eksternt administrere datamaskinene og enhetene som hjemmenettverket består av. Du kan administrere statusen og tilgangsnivåene til datamaskinene og enhetene, samt løse de fleste sikkerhetshull eksternt.

I dette kapitlet

Administrere status og rettigheter

Et administrert nettverk har administrerte og ikke-administrerte medlemmer. Administrerte medlemmer tillater andre datamaskiner i nettverket å administrere deres McAfee-beskyttelsesstatus. Ikke-administrerte medlemmer gjør ikke det. Ikke-administrerte nettverksmedlemmer er vanligvis gjestemaskiner som vil ha tilgang til andre nettverksfunksjoner (for eksempel sende filer eller dele skrivere). En ikke-administrert datamaskin kan inviteres til å bli en administrert datamaskin når som helst av en annen administrert datamaskin med administrative rettigheter i nettverket. På samme måte kan en administrert datamaskin med administrative rettigheter, når som helst gjøre en annen administrert datamaskin ikke-administrert.

Administrerte datamaskiner har administrative rettigheter, full tilgang eller gjestetilgang. Administrative rettigheter gjør at den administrerte datamaskinen kan overvåke beskyttelsesstatusen til alle administrerte datamaskiner i nettverket, og gi andre datamaskiner tilgang til nettverket. Full tilgang og gjestetilgang gir kun datamaskinen tilgang til nettverket. Du kan endre tillatelsesnivået til en datamaskin når som helst.

Siden et administrert nettverk også kan ha enheter (for eksempel rutere), kan du bruke Network Manager til å administrere disse enhetene. Du kan også konfigurere og endre egenskapene til en enhet på nettverkskartet.

Administrere beskyttelsesstatusen til en datamaskin

Hvis en datamaskins beskyttelsesstatus ikke blir administrert på nettverket (datamaskinen er ikke et medlem, eller er et ikke-administrert medlem), kan du be om å administrere den.

1. Klikk ikonet til den ikke-administrerte datamaskinen på nettverkskartet.
2. Klikk **Administrer denne datamaskinen** under **Jeg vil**.

Slutte å administrere beskyttelsesstatusen til en datamaskin

Du kan slutte å administrere beskyttelsesstatusen til en administrert datamaskin i nettverket. Datamaskinen blir da ikke administrert, og du kan ikke administrere beskyttelsesstatusen eksternt.

1. Klikk ikonet til den administrerte datamaskinen på nettverkskartet.
2. Klikk **Stopp å administrere denne datamaskinen** under **Jeg vil**.
3. Klikk **Ja** i bekreftelsesdialogboksen.

Endre tillatelsene til en administrert datamaskin

Du kan endre tillatelsene til en datamaskin når som helst. Dette gjør at du kan endre hvilke datamaskiner som kan administrere beskyttelsesstatusen til andre datamaskiner i nettverket.

1. Klikk ikonet til den administrerte datamaskinen på nettverkskartet.
2. Klikk **Endre tillatelser for denne datamaskinen** under **Jeg vil**.
3. I dialogboksen for endring av tillatelser merker du av eller fjerner merket i boksen for å angi om denne og andre datamaskiner i det administrerte nettverket kan administrere hverandres beskyttelsesstatus.
4. Klikk **OK**.

Administrere en enhet

Du kan administrere en enhet ved å åpne administrasjonswebsiden fra nettverkskartet.

1. Klikk enhetens ikon på nettverkskartet.
2. Klikk **Behandle denne enheten** under **Jeg vil**.
   En webleser åpnes og viser enhetens administrasjonswebside.
3. Oppgi påloggingsinformasjon og konfigurer enhetens sikkerhetsinnstillinger i webleseren.

Merk: Hvis enheten er en trådløs ruter eller et tilgangspunkt som er beskyttet av Wireless Network Security, må du bruke McAfee Wireless Network Security til å konfigurere sikkerhetsinnstillingene for enheten.

Endre visningsegenskapene til en enhet

Når du endrer visningsegenskapene til en enhet, kan du endre enhetens visningsnavn på nettverkskartet og spesifisere om enheten er en trådløs ruter.

1. Klikk på enhetens ikon på nettverkskartet.
2. Klikk på **Endre enhetens egenskaper** under **Jeg vil**.
3. Skriv inn et navn i **Navn**-boksen for å spesifisere visningsnavnet for enheten.
4. Hvis du vil spesifisere enhetstype, klikk på **Standard Ruter** dersom den ikke er en trådløs ruter, eller **Trådløs Ruter** dersom den er trådløs.
5. Klikk **OK**.

Løse sikkerhetshull

Administrerte datamaskiner med administrative rettigheter kan administrere McAfee-beskyttelsesstatusen til andre administrerte datamaskiner i nettverket, og løse eventuelle innrapporterte sikkerhetshull eksternt. Hvis for eksempel McAfee-beskyttelsesstatusen til en administrert datamaskin viser at VirusScan er deaktivert, kan en annen administrert datamaskin med administrative rettigheter aktivere VirusScan eksternt.

Når du løser sikkerhetshull eksternt, løser Network Manager de fleste rapporterte problemer. Noen sikkerhetshull krever imidlertid manuell inngripen på den lokale maskinen. I dette tilfellet løser Network Manager de problemene som kan løses eksternt, og ber deg deretter løse de gjenværende problemene ved å logge deg på SecurityCenter på den utsatte maskinen og følge de anbefalingene som blir gitt. I noen tilfeller er den anbefalte løsningen på problemet å installere den nyeste versjonen av SecurityCenter på den eksterne maskinen eller på datamaskiner i nettverket.

Løse sikkerhetshull

Du kan bruke Network Manager til å løse de fleste sikkerhetshull på eksterne, administrerte datamaskiner. For eksempel, hvis VirusScan er deaktivert på en ekstern datamaskin, kan du aktivere den.

1. Klikk på elementets ikon på nettverkskartet.
2. Vis beskyttelsesstatusen til elementet under **Detaljer**.
3. Klikk på **Reparer sikkerhetshull** under **Jeg vil**.
4. Når sikkerhetshull har blitt løst, klikker du på **OK**.

Merk: Selv om Network Manager løser de fleste sikkerhetshull automatisk, krever noen reparasjoner at du åpner SecurityCenter på den utsatte datamaskinen og følger de anbefalingene som blir gitt.

Installere McAfee-sikkerhetsprogramvare på eksterne datamaskiner

Hvis en eller flere datamaskiner i nettverket ikke bruker en nyere versjon av SecurityCenter, kan ikke beskyttelsesstatusen deres administreres eksternt. Hvis du vil administrere disse datamaskinene eksternt, må du gå til hver enkelt datamaskin og installere en nyere versjon av SecurityCenter.

1. Sørg for at du følger disse instruksjonene på datamaskinen du vil administrere eksternt.
2. Ha påloggingsinformasjonen for McAfee i nærheten – dette er e-postadressen og passordet du brukte første gang McAfee-programvaren ble aktivert.
3. Gå til McAfee-webområdet i en webleser, logg på og klikk **Min konto**.
4. Finn produktet du vil installere, klikk **Last ned**, og følg deretter instruksjonene på skjermen.

Tips: Du kan også lære hvordan du installerer sikkerhetsprogramvare fra McAfee på eksterne datamaskiner ved å åpne nettverkskartet og klikke **Beskytt PC-ene mine** under **Jeg vil**.

KAPITTEL 31

Overvåke nettverkene

Hvis du har installert McAfee Total Protection, overvåker Network Manager også nettverkene med henblikk på inntrengere. Hver gang en ukjent datamaskin eller enhet kobler til nettverket, blir du varslet, slik at du kan avgjøre om datamaskinen eller enheten er en Venn eller en Inntrenger. En Venn er en datamaskin eller enhet som du gjenkjenner og klarerer, og en Inntrenger er en datamaskin eller enhet du ikke gjenkjenner eller klarerer. Hvis du markerer en datamaskin eller enhet som Venn, kan du avgjøre om du vil bli varslet hver gang den kobler til nettverket. Hvis du markerer en datamaskin eller enhet som Inntrenger, blir du automatisk varslet hver gang den kobler til.

Første gang du kobler til et nettverk etter installering eller oppgradering til denne versjonen av Total Protection, markeres hver datamaskin eller enhet automatisk som Venn, og du blir ikke varslet når de kobler til nettverket i fremtiden. Etter tre dager blir du varslet om hver ukjente datamaskin eller enhet som kobler til, slik at du kan markere dem selv.

Merk: Nettverksovervåking er en funksjon i Network Manager som bare er tilgjengelig med McAfee Total Protection. Du finner mer informasjon om Total Protection på webområdet vårt.

I dette kapitlet

Stopp overvåking av nettverk

Hvis du deaktiverer nettverksovervåking, blir du ikke lenger varslet hvis inntrengere kobler til hjemmenettverket eller andre nettverk du kobler til.

1 Åpne konfigurasjonsruten for Internett og nettverk.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. I Hjem-ruten for SecurityCenter klikker du **Internett og nettverk**.
   3. I informasjonsdelen for Internett og nettverk klikker du **Konfigurer**.

2 Klikk **Av** under **Nettverksovervåking**.

Aktivere varsler fra nettverksovervåking på nytt

Selv om du kan deaktivere varsler fra nettverksovervåking, anbefales det ikke. Hvis du gjør det, vil du ikke lenger bli varslet om ukjente datamaskiner eller inntrengere som kobler til nettverket. Hvis du ved et uhell deaktiverer disse varslene (hvis du for eksempel merker av for **Ikke vis dette varslet igjen** i et varsel), kan du aktivere dem på nytt når som helst.

1 Åpne ruten Varslingsalternativer.

   Hvordan?

   1. Under **Vanlige oppgaver** klikker du **Hjem**.
   2. Klikk **Konfigurer** i den høyre ruten under **SecurityCenter-informasjon**.
   3. Under **Varsler** klikker du **Avansert**.

2 I ruten SecurityCenter-konfigurasjon klikker du **Informasjonsvarsler**.

3 I ruten Informasjonsvarsler kontrollerer du at det ikke er merket av for følgende alternativer:

   - **Ikke vis varsler når nye PC-er eller enheter kobler seg til nettverket**
   - **Ikke vis varsler når inntrengere kobler seg til nettverket**
   - **Ikke vis varsler for venner som jeg vanligvis ønsker å bli varslet om**

- **Ikke påminn meg når ukjente PC-er eller enheter blir oppdaget**
- **Ikke varsle meg når McAfee er ferdig med å oppdage nye Venner.**

4 Klikk **OK**.

Markere som Inntrenger

Du bør markere en datamaskin eller enhet på nettverket som Inntrenger hvis du ikke gjenkjenner den eller vil klarere den. Du blir automatisk varslet neste gang den kobler til nettverket.

1 Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.

2 Klikk et element på nettverkskartet.

3 Klikk **Marker som Venn eller Inntrenger** under **Jeg vil**.

4 Klikk **En Inntrenger** i dialogboksen.

Markere som Venn

Du bør bare markere en datamaskin eller enhet på nettverket som Venn hvis du gjenkjenner den og vil klarere den. Når du markerer en datamaskin eller enhet som Venn, kan du også avgjøre om du vil bli varslet hver gang den kobler til nettverket.

1 Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.

2 Klikk et element på nettverkskartet.

3 Klikk **Marker som Venn eller Inntrenger** under **Jeg vil**.

4 Klikk **En Venn** i dialogboksen.

5 Hvis du vil bli varslet hver gang denne vennen kobler til nettverket, merker du av for **Varsle meg når denne datamaskinen eller enheten kobler seg til nettverket**.

Slutte å finne nye venner

De første tre dagene etter at du har koblet til et nettverk med denne versjonen av Total Protection installert, markeres hver datamaskin eller enhet automatisk som Venn som du ikke vil bli varslet om. Du kan når som helst innen disse tre dagene stoppe den automatiske markeringen, men du kan ikke starte den på nytt senere.

1 Klikk **Administrert nettverk** på den grunnleggende eller avanserte menyen.

2 Klikk **Slutt å finne nye venner** under **Jeg vil**.

KAPITTEL 32

McAfee EasyNetwork

Med Easy Network får du sikker fildeling, enkel filoverføring og alle datamaskinene i hjemmenettverket får tilgang til skriveren. Imidlertid må datamaskinene i ditt nettverk ha EasyNetwork installert for å ha tilgang til dets funksjoner.

Før du begynner å bruke EasyNetwork, kan du gjøre deg kjent med noen av funksjonene. EasyNetwork-hjelp har informasjon om å konfigurere og bruke disse funksjonene.

Merknad: SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtual Technician.

I dette kapitlet

EasyNetwork funksjoner

EasyNetwork har følgende funksjoner.

Fildeling

EasyNetwork gjør det enkelt å dele filer med andre datamaskiner i ditt nettverk. Når du deler filer, gir du de andre datamaskinene lesetilgang til disse filene. Kun datamaskiner som har full eller administrativ tilgang til ditt administrative nettverk (medlemmer), kan dele eller få tilgang til filer som deles av andre medlemmer.

Filoverføring

Du kan sende filer til andre datamaskiner som har full eller administrativ tilgang til ditt administrative nettverk (medlemmer). Når du mottar en fil, vises den i EasyNetwork-innboksen. Innboksen er en midlertidig lagringsplass for alle filene som sendes til deg fra andre datamaskiner i nettverket.

Automatisk skriverdeling

Når du blir med i et administrativt nettverk, kan du dele lokale skrivere som er koblet til datamaskinen din med andre medlemmer, og bruke skriverens gjeldende navn som det delte skrivernavnet. Den oppdager også skrivere som deles av andre datamaskiner på nettverket, og tillater deg å konfigurere og bruke disse skriverne.

KAPITTEL 33

Konfigurere EasyNetwork

Før du kan bruke EasyNetwork, må du åpne den og koble deg til et administrativt nettverk. Etter at du har koblet deg til et administrativt nettverk, kan du dele, søke etter, og sende filer til andre datamaskiner i nettverket. Du kan også dele skrivere. Dersom du bestemmer deg for å forlate nettverket, kan du gjøre dette når som helst.

I dette kapitlet

Åpne EasyNetwork

Du kan åpne EasyNetwork fra Start-menyen i Windows eller ved å klikke skrivebordsikonet.

- Gå til **Start**-menyen, velg **Programmer**, velg **McAfee**, og klikk deretter **McAfee EasyNetwork**.

Tips: Du kan også åpne EasyNetwork ved å dobbeltklikke McAfee EasyNetwork-ikonet på skrivebordet.

Logge seg på et administrativt nettverk

Hvis ingen datamaskiner i nettverket som du er koblet til har SecurityCenter, blir du medlem av nettverket og du blir spurt om nettverket er til å stole på. Hvis du er den første datamaskinen som blir med i nettverket, blir ditt datamaskinnavn med i nettverksnavnet. Du kan imidlertid endre navnet når som helst.

Når en datamaskin kobles til nettverket, sender den en påloggingsanmodning til de andre datamaskinene som er koblet til nettverket. Alle datamaskiner med administrative rettigheter i nettverket, kan gi tilgang. Godkjenneren kan også bestemme tillatelsesnivået til datamaskinen som ble koblet til nettverket, for eksempel gjest (kun filoverføring) eller full tilgang / administrativ (filoverføring og fildeling). Med EasyNetwork kan datamaskiner med administrative rettigheter gi tilgang til andre datamaskiner og administrere tillatelser (tillate eller ikke tillate). Datamaskiner med full tilgang kan ikke utføre disse administrative oppgavene.

Merk: Hvis du har andre McAfee-nettverksprogrammer installert (for eksempel Network Manager), blir datamaskinen også gjenkjent som et administrert medlem i disse programmene, etter at du har koblet den til. Tillatelsesnivået som angis til en datamaskin i EasyNetwork, gjelder for alle McAfees nettverksprogrammer. Hvis du vil ha mer informasjon om hva gjestetilgang, full tilgang eller administrative rettigheter betyr i andre McAfee-nettverksprogrammer, kan du se i dokumentasjonen som følger med programmet.

Logge på nettverket

Når en datamaskin kobler seg på et pålitelig nettverk for første gang etter at EasyNetwork er installert, vises en melding der du blir spurt om du vil logge deg på det administrative nettverket. Hvis datamaskinen godtar å logge seg på, sendes en anmodning til alle de andre nettverksdatamaskinene som har administrativ tilgang. Denne anmodningen må innvilges før datamaskinen kan dele skrivere eller filer, eller sende og kopiere filer på nettverket. Den første datamaskinen i nettverket blir automatisk gitt administrative rettigheter.

1. I vinduet for delte filer, klikker du på **Logg på dette nettverket**.
   Når en administrativ datamaskin i nettverket gir deg tilgang, vises en melding der du blir spurt om du vil la denne datamaskinen og andre datamaskiner i nettverket administrere hverandres sikkerhetsinnstillinger.
2. Hvis du vil la denne datamaskinen og andre datamaskiner i nettverket administrere hverandres sikkerhetsinnstillinger, klikker du på **OK**. I motsatt tilfelle klikker du på **Avbryt**.
3. Bekreft at datamaskinen viser spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, og klikk deretter på **OK**.

Merknad: Hvis datamaskinen som inviterte deg til å koble til det administrative nettverket, ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd i det administrative nettverket. Det kan utgjøre en sikkerhetsrisiko for din datamaskin. Klikk **Avbryt** i dialogboksen for sikkerhetsbekreftelse.

Gi tilgang til nettverket

Når en datamaskin anmoder om å logge seg på det administrative nettverket, sendes en melding til alle de andre nettverksdatamaskinene som har administrativ tilgang. Den første datamaskinen som svarer, blir godkjenneren. Når du er godkjenner, har du ansvaret for hvilken tilgangstype datamaskinen skal få: gjestetilgang, full tilgang eller administrativ tilgang.

1. Velg egnet tilgangsnivåer.
2. I dialogboksen for å invitere en datamaskin til å koble seg til det administrative nettverket gjør du ett av følgende:
   - Klikk på **Gi gjest tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket (du kan bruke dette alternativet for midlertidige brukere i ditt hjem).
   - Klikk på **Gi full tilgang til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket.

- Klikk på **Gi administrative rettigheter til administrerte nettverksprogrammer** for å gi datamaskinen tilgang til nettverket med administrative rettigheter. Datamaskinen kan også gi tilgang til andre datamaskiner som vil bli med i det administrative nettverket.

3 Klikk **OK**.

4 Bekreft at datamaskinen viser spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, og klikk deretter på **Gi Tilgang**.

Merk: Hvis datamaskinen ikke viser de samme spillekortene som vises i dialogboksen for sikkerhetsbekreftelse, har det oppstått et sikkerhetsbrudd på det administrative nettverket. Det kan være risikofylt å gi denne datamaskinen tilgang til nettverket, så du bør klikke på **Avvis** i dialogboksen for sikkerhetsbekreftelse.

Gi nettverket nytt navn

Nettverksnavnet inkluderer som standard navnet på den første datamaskinen som ble med i nettverket. Du kan imidlertid endre navnet når som helst. Når du gir nettverket et nytt navn, endrer du nettverksbeskrivelsen som vises i EasyNetwork.

1 Klikk på **Konfigurer** på **Alternativer**-menyen.

2 I konfigurasjonsboksen skriver du inn navnet på nettverket i boksen **Nettverksnavn**.

3 Klikk **OK**.

Forlate et administrativt nettverk

Hvis du logger deg på et administrativt nettverk men så bestemmer deg for ikke å være medlem, kan du forlate nettverket. Etter at du forlater det administrative nettverket, kan du alltid bli med igjen, men da må du få tillatelse til å logge deg på igjen. Du finner mer informasjon om å logge seg på i Logge seg på et administrativt nettverk (side 154).

Forlate et administrert nettverk

Du kan forlate et administrert nettverk som du tidligere logget deg på.

1 Koble datamaskinen fra nettverket.

2 I EasyNetwork klikker du **Forlat nettverk** på **Verktøy**-menyen.

3 I dialogboksen Forlat nettverk velger du navnet på nettverket du vil forlate.

4 Klikk **Forlat nettverk**.

KAPITTEL 34

Dele og sende filer

EasyNetwork gjør det enkelt å dele og sende filer til andre datamaskiner på nettverket. Når du deler filer, gir du de andre datamaskinene lesetilgang til disse. Kun datamaskiner som er medlemmer av det administrative nettverket (full eller administrativ tilgang), kan dele eller få tilgang til filer som deles av andre datamaskiner.

Merknad: Hvis du deler et stort antall av filer, kan ressursene til din datamaskin bli påvirket.

I dette kapitlet

Dele filer

Kun datamaskiner som er medlemmer av det administrative nettverket (full eller administrativ tilgang), kan dele eller få tilgang til filer som deles av andre datamaskiner. Hvis du deler en mappe, deles alle filene i den mappen og eventuelle undermapper. Filer som senere legges i den mappen, blir imidlertid ikke automatisk delt. Hvis en delt fil eller mappe slettes, fjernes den fra vinduet for delte filer. Du kan slutte å dele en fil når som helst.

Hvis du vil ha tilgang til en delt fil, åpne filen direkte fra EasyNetwork eller kopier den til din datamaskin, og så åpne den derfra. Hvis listen over delte filer blir lang og det vanskelig å se hvor filen er, kan du søke etter den.

Merknad: Andre datamaskiner som bruker Window Explorer, har ikke tilgang til filer som deles via EasyNetwork. Fildeling med EasyNetwork må foregå over sikre tilkoblinger.

Dele filer

Når du deler en fil, blir den tilgjengelig for alle medlemmer som har full eller administrativ tilgang til det administrative nettverket.

1. Finn filen du vil dele, i Windows Utforsker.
2. Dra filen fra Windows Utforsker til vinduet for delte filer i EasyNetwork.

Tips: Du kan også dele en fil dersom du klikker på **Dele filer** i **Verktøy**-menyen. I Dele-dialogboksen finner du filen du vil dele, velger den og klikker på **Dele**.

Stanse deling av fil

Hvis du deler en fil på det administrative nettverket, kan du stanse delingen når som helst. Når du stanser delingen av en fil, har ikke andre medlemmer av det administrative nettverket tilgang.

1. Klikk på **Stanse deling av filer** i **Verktøy**-menyen.
2. I dialogboksen for stans av fildeling velger du den filen du ikke lenger vil dele.
3. Klikk **OK**.

Kopiere en delt fil

Du kan kopiere en delt fil slik at du fortsatt har den når den ikke deles lenger. Du kan kopiere en delt fil fra enhver datamaskin i ditt administrative nettverk.

- Dra filen fra vinduet for delte filer i EasyNetwork til et sted på Windows Utforsker eller Windows Skrivebord.

Tips: Du kan også kopiere en delt fil dersom du velger filen i EasyNetwork, og deretter klikker på **Kopi til** på **Verktøy**-menyen. I Kopi til-dialogboksen navigerer du til mappen du vil kopiere filen til, velger den og klikker på **Lagre**.

Søke etter en delt fil

Du kan søke etter en fil som er delt av deg eller andre nettverksmedlemmer. Når du skriver inn søkekriteriene, viser EasyNetwork resultatet i vinduet for delte filer.

1. Klikk på **Søk** i vinduet for delte filer.
2. Klikk på ønsket alternativ (side 159) i listen **Innehold**.
3. Skriv inn hele eller deler av filnavnet eller banen i listen **Fil- eller banenavn**.
4. Klikk på ønsket filtype (side 159) i listen **Type**.
5. I listene **Fra** og **Til** klikker du på datoene som representerer når filen ble opprettet.

Søkekriterier

Følgende tabeller beskriver de søkekriterier som du kan oppgi når du søker etter delte filer.

Navn på filen eller bane

Inneholder:	Beskrivelse
Inneholder alle ordene	Søk etter en fil eller banenavn som inneholder alle ordene du har oppgitt i listen **Fil- eller banenavn**.
Inneholder et hvilket som helst av ordene	Søker etter en fil eller banenavn som inneholder ett eller flere av ordene du har oppgitt i **Fil- eller banenavn**-listen.
Inneholder nøyaktig streng	Søker etter en fil eller banenavn som inneholder den nøyaktige frasen du oppgav i **Fil- eller banenavn**-listen.

Filtype

Type	Beskrivelse
Alle	Søker alle delte filtyper.
Dokument	Søker alle delte dokumenter.
Bilde	Søker alle delte bildefiler.
Video	Søker alle delte videofiler.
Lyd	Søker alle delte lydfiler.
Komprimert	Søke alle komprimerte filer (for eksempel ZIP-filer).

Sende filer til andre datamaskiner

Du kan sende filer til andre datamaskiner som er medlemmer av det administrative nettverket. Før du sender en fil, bekrefter EasyNetwork at datamaskinen som skal motta filen, har nok tilgjengelig lagringsplass.

Når du mottar en fil, vises den i EasyNetwork-innboksen. Innboksen er en midlertidig lagringsplass for filer som sendes til deg fra andre datamaskiner i nettverket. Hvis EasyNetwork er åpen når du mottar en fil, vises filen øyeblikkelig i innboksen. Ellers vises en melding i systemstatusfeltet helt til høyre for din oppgavelinje. Hvis du ikke vil motta meldingen (for eksempel da de forstyrrer det du foretar deg), kan du skru denne funksjonen av. Hvis innboksen allerede har en fil med samme navn, får den nye filen et nytt navn med numerisk endelse. Filer blir i innboksen til du godtar dem (kopierer dem til datamaskinen din).

Sende en fil til en annen datamaskin

Du kan sende en fil til en annen datamaskin på det administrative nettverket uten å dele den. Før mottakeren kan se filen, må den lagres lokalt. Du finner mer informasjon i Godta en fil fra en annen datamaskin (side 161).

1. Finn filen du vil sende, i Windows Utforsker.
2. Dra filen fra Windows Utforsker til et aktivt dataikon i EasyNetwork.

Tips: Flere filer kan sendes til en datamaskin ved å trykke på CTRL-knappen når du velger filene. Du kan også sende filer ved å klikke på **Send** på **Verktøy**-menyen, velge filene og deretter klikke på **Send**.

Godta en fil fra en annen datamaskin.

Hvis en annen datamaskin i det administrative nettverket sender deg en fil, må du godta den ved å lagre den på datamaskinen din. Hvis EasyNetwork ikke kjører når en fil blir sendt til din datamaskin, vil du motta en melding i systemstatusfeltet helt til høyre for din oppgavelinje. Klikk på meldingen for å åpne EasyNetwork og få tilgang til filen.

- Klikk på **Mottatt**, og dra deretter filen fra EasyNetwork-innboksen til en mappe i Windows Utforsker.

Tips: Du kan også motta en fil fra en annen datamaskin ved å velge filen i EasyNetwork-innboksen og deretter klikke på **Godta** på **Verktøy**-menyen. I Godta-dialogboksen navigerer du til mappen der du vil lagre filen, velger den og klikker på **Lagre**.

Motta melding når en fil er sendt

Du kan motta en melding når en annen datamaskin i det administrative nettverket sender deg en fil. Hvis EasyNetwork ikke kjører, vil meldingen vises i systemstatusfeltet helt til høyre for din oppgavelinje.

1. Klikk på **Konfigurer** på **Alternativer**-menyen.
2. I Konfigurer-dialogboksen velger du boksen **Varsle meg når en annen datamaskin sender meg filer**.
3. Klikk **OK**.

KAPITTEL 35

Dele skrivere

Når du blir med i et administrativt nettverk, deler EasyNetwork lokale skrivere som er koblet til datamaskinen din, og bruker skriverens navn som det delte skrivernavnet. EasyNetwork oppdager også skrivere som deles av andre datamaskiner på nettverket, og tillater deg å konfigurere og bruke disse skriverne.

Hvis du har konfigurert en skriverdriver til å skrive ut gjennom en nettverksskriver (for eksempel en trådløs USB-skrivertjener), anser EasyNetwork skriveren som en lokal skriver, og deler den i nettverket. Du kan slutte å dele en skriver når som helst.

I dette kapitlet

Arbeide med delte skrivere

EasyNetwork oppdager skrivere som deles av datamaskinene i nettverket. Hvis EasyNetwork oppdager en ekstern skriver som ikke er koblet til datamaskinen din, vises lenken **Tilgjengelige nettverksskrivere** i vinduet for delte filer når du åpner EasyNetwork for første gang. Dermed kan du installere tilgjengelige skrivere, eller avinstallere skrivere som allerede er koblet til datamaskinen din. Du kan også oppdatere listen over skrivere for å sikre at du viser oppdatert informasjon.

Hvis du ikke er logget på det administrative nettverket, men er koblet til det, kan du bruke skriverkontrollpanelet i Windows til å få tilgang til de delte skriverne.

Stanse deling av en skriver

Når du stanser deling av en printer, kan medlemmene ikke bruke den.

1. Klikk på **Skrivere** på **Verktøy**-menyen.
2. I dialogboksen for behandling av nettverksskrivere, velger du den skriveren du ikke lenger vil dele.
3. Klikk på **Ikke del**.

Installere en tilgjengelig nettverksskriver

Hvis du er medlem av et administrativt nettverk, har du tilgang til skrivere som deles. Du må imidlertid installere skriverdriveren som brukes av skriveren. Hvis eieren av skriveren slutter å dele sin printer, kan du ikke bruke den.

1. Klikk på **Skrivere** på **Verktøy**-menyen.
2. Velg et skrivernavn i dialogboksen for tilgjengelige nettverksskrivere.
3. Klikk på **Installer**.

Referanse

Ordlisten inneholder og forklarer de mest brukte sikkerhetsrelaterte ord og uttrykk i McAfees produkter.

Liste

8

802.11

Et sett med standarder for å sende data over et trådløst nettverk. 802.11 er også kjent som Wi-Fi.

802.11a

En utvidelse av 802.11 som sender data opp til 54 Mbit/s på 5GHz-frekvens. Selv om overføringshastigheten er raskere enn 802.11b, er rekkevidden mye mindre.

802.11b

En utvidelse av 802.11 som sender data opp til 11 Mbit/s på 2,4 GHz-frekvens. Selv om overføringshastighten er lavere enn 802.11a, er rekkevidden større.

802.1x

En standard for godkjenning i kablede og trådløse nettverk. 802.1x brukes vanligvis med 802.11 trådløse nettverk. Se også godkjenning (side 168).

A

ActiveX-kontroller

En programvarekomponent som programmer eller nettsider bruker til å tilføye funksjonalitet som glir inn og fremstår som en normal del av programmet eller nettsiden. De fleste ActiveX-kontrollene er harmløse, men noen kan innhente informasjon fra datamaskinen.

aktiveringspunkt

En geografisk grense dekket av et Wi-Fi (802.11) tilgangspunkt (AP). Brukere som kommer inn i et aktiveringspunkt med en trådløs datamaskin kan koble til Internett dersom aktiveringspunktet signaliserer (varsler at det er der) og det ikke kreves godkjenning. Aktiveringspunkt finnes ofte på travle plasser som for eksempel flyplasser.

arkiv

For å opprette en kopi av viktige filer på CD, DVD, USB-stasjon, ekstern harddisk eller nettverksstasjon. Se også sikkerhetskopiering (side 174).

B

brannmur

Et system (maskinvare, programvare eller begge deler) som skal forhindre uautorisert tilgang til eller fra et privat nettverk. Brannmurer benyttes ofte til å forhindre at uautoriserte Internett-brukere får tilgang til private nettverk som er koplet til Internett, spesielt et intranett. Alle beskjeder som går inn eller ut av intranettet passerer gjennom brannmuren, som undersøker hver beskjed og blokkerer de som ikke tilfredsstiller oppsatte sikkerhetskriterier.

buffer

Et midlertidig lagringsområde på datamaskinen for data som brukes ofte eller som nettopp er brukt. Nettleseren kan for eksempel hente en nettside fra bufferen istedenfor en ekstern server neste gang siden skal åpnes, og dermed sørge for raskere og mer effektiv navigering.

bufferoverløp

En tilstand som oppstår i et operativsystem eller applikasjon når mistenkelige programmer eller prosesser forsøker å lagre mer data i en buffer (midlertidig lagringsområde) på datamaskinen enn det er plass til. Bufferoverløp ødelegger minnet eller overskriver data i nærliggende buffere.

båndbredde

Datamengden som kan overføres i en bestemt tidsperiode.

D

DAT

Oppdagelsesdefinisjonsfiler, også kalt signaturfiler, som inneholder definisjonene som identifiserer, oppdager og reparerer virus, trojanske hester, spion- og reklameprogramer og andre potensielt uønskede programmer (PUP).

dele

Å gi e-postmottakere tilgang til utvalgte, sikkerhetskopierte filer i et begrenset tidsrom. Når du deler en fil, sender du en sikkerhetskopi av filen til de e-postmottaker du velger. Mottakerne får en e-postmelding fra Sikkerhetskopier og gjenopprett som sier at filene er delt med dem. E-posten inneholder også en kobling til de delte filene.

delt hemmelighet

Streng eller nøkkel (vanligvis et passord) som deles mellom to kommuniserende parter før kommunikasjonen starter. Den brukes til å beskytte sensitive deler av RADIUS-meldinger. Se også RADIUS (side 173).

DNS

Domenenavnsystem. Et databasesystem som oversetter en IP-adresse, slik som 11.2.3.44, til et domenenavn, for eksempel www.mcafee.com.

domene

Et lokalt delnettverk eller en nøkkel for områder på Internett. På et lokalt nettverk (LAN) er et domene et delnettverk som består av klient- og servermaskiner som kontrolleres av en sikkerhetsdatabase. På Internett inneholder alle nettadresser et domenenavn. I www.mcafee.com, for eksempel, er mcafee domenet.

E

e-post

Elektronisk post. Beskjeder som sendes og mottas elektronisk over et datanettverk. Se også webmail (side 177).

e-postklient

Et program du kjører på datamaskinen for å sende og motta e-post (for eksempel Microsoft Outlook).

ekstern harddisk

En harddisk som lagres utenfor datamaskinen.

ESS

Extended Service Set. To eller flere nettverk som danner et enkelt delnettverk

F

filfragmenter

Filrester som er spredt på en stasjon. Filfragmentering oppstår når filer legges til eller slettes, og kan gjøre at datamaskinens ytelse blir langsommere.

G

godkjenning

Prosessen med å kontrollere den digitale identiteten til en sender av elektroniske data.

H

hendelse

I et datasystem eller -program er en hendelse noe som kan oppdages av sikkerhetsprogramvaren etter forhåndsdefinerte kriterier. Typisk utløser en hendelse en handling, som å sende et varsel eller skrive en ny post til en hendelseslogg.

hjemmenettverk

To eller flere datamaskiner som er koblet sammen i et hjem slik at de kan dele filer og Internett-tilgang. Se også LAN (side 170).

hviteliste

En liste over nettsteder eller e-postadresser som regnes som trygge. Nettstedene på en hviteliste er de som brukerne har lov til å besøke. E-postadressene på en hviteliste er fra klarerte avsendere som du ønsker å motta meldinger fra. Se også svarteliste (side 175).

I

informasjonskapsel

En liten tekstfil som mange nettsteder bruker til å lagre informasjon om nettsider du har vært på. Filen lagres på din datamaskin. Den kan inneholde påloggings- eller registreringsopplysninger, handlekurvinformasjon eller brukerinnstillinger. Informasjonskapsler brukes i all hovedsak av webområder til å identifisere brukere som tidligere har registrert seg på eller besøkt området, men de kan også være en kilde til informasjon for hackere.

innholdsklassifiseringsgrupper

I Foreldrestyring er det en aldersgruppe som en bruker tilhører. Innholdet er tilgjengelig eller blokkert basert på hvilken innholdsklassifiseringsgruppe brukeren tilhører. Innholdsklassifiseringsgrupper omfatter: Småbarn, Barn, Unge ungdommer, Eldre ungdommer og Voksne.

integrert gateway

En enhet som kombinerer funksjonene til et tilgangspunkt, en ruter og en brannmur. Noen enheter har også ekstra sikkerhet og mellomegenskaper.

intranett

Et privat nettverk av datamaskiner, vanligvis innen en organisasjon, som kun godkjente brukere har tilgang til.

IP-adresse

Internett-protokolladresse. En adresse som brukes til å identifisere en datamaskin eller enhet på et TCP/IP-nettverk. Formatet til en IP-adresse er en 32-biters numerisk adresse som skrives som fire numre atskilt med punktum. Hvert nummer kan være mellom 0 og 250 (for eksempel 192.168.1.100).

IP-forfalskning

Forfalske IP-adressene i en IP-pakke. Dette brukes i mange typer angrep, blant annet kapring. Det brukes også ofte til å forfalske e-posthoder i spampost slik at de ikke kan spores.

K

karantene

Tvungen isolering av en fil eller mappe som mistenkes å inneholde et virus, spam eller mistenkelig innhold, eller potensielt uønskede programmer (PUP), slik at filene eller mappene ikke kan åpnes eller kjøres.

klarert liste

En liste over elementer som du har klarert og som ikke oppdages. Hvis du har klarert et element ved en feiltakelse (for eksempel et potensielt uønsket program eller en registerendring), eller du vil at elementet skal kunne oppdages igjen, må du fjerne det fra listen.

klient

Et program som kjører på en PC eller arbeidsstasjon og er avhengig av en tjener for å utføre visse oppgaver. En e-postklient, for eksempel, er et program som gjør at du kan sende og motta e-post.

komprimering

En prosess som komprimerer filer til en form som minimerer plassen som kreves for lagring eller overføring.

kryptering

En metode for å kode informasjon, slik at uvedkommende ikke for tilgang til den. Ved kryptering bruker man en "nøkkel" og matematiske algoritmer. Kryptert informasjon kan ikke dekrypteres uten riktig nøkkel. Det hender at virus bruker kryptering for ikke å bli oppdaget.

krypteringstekst

Kryptert tekst. Krypteringstekst er uleselig før den konverteres til vanlig tekst (dekryptert). Se også kryptering (side 169).

L

LAN

Lokalnettverk. Et nettverk av datamaskiner som strekker seg over et relativt lite område (for eksempel en enkelt bygning). Datamaskiner på et LAN-nettverk kan kommunisere med hverandre og dele ressurser som skrivere og filer.

launchpad

En U3-grensesnittskomponent som fungerer som startpunkt for oppstart og administrasjon av U3 USB-programmer.

M

MAC-adresse

Media Access Control-adresse. Et unikt serienummer som er tildelt en fysisk enhet (NIC, nettverksgrensesnittkort) som har tilgang til nettverket.

man-in-the-middle-angrep

Metode for å fange opp og muligens endre beskjeder mellom to parter uten at noen av partene vet at kommunikasjonskoblingen har blitt brutt.

MAPI

Messaging Application Programming Interface. En spesifikasjon for et Microsoft-grensesnitt som gjør det mulig for ulike meldings- og arbeidsgruppeprogrammer (som e-post, talemelding og faks) å jobbe sammen via en enkelt klient, som Exchange.

message authentication code (MAC)

Sikkerhetskode som brukes til å kryptere meldinger som overføres mellom datamaskiner. Meldingen godkjennes hvis datamaskinen finner at den krypterte koden er gyldig.

midlertidig fil

En fil som er opprettet i minnet eller på en stasjon av operativsystemet eller et annet program. Den skal brukes i en økt, og deretter fjernes.

MSN

Microsoft Network. En gruppe webbaserte tjenester som tilbys av Microsoft Corporation, bl.a. søkemotor, e-post, direktemeldinger og portal.

N

nettleser

Et program som brukes til å vise nettsider på Internett. Populære nettlesere er bl.a. Microsoft Internet Explorer og Mozilla Firefox.

nettverk

En samling av IP-baserte systemer (som rutere, svitsjer, tjenere og brannmurer) som er gruppert som en logisk enhet. For eksempel kan et "økonominettverk" omfatte alle tjenere, rutere og systemer som brukes i en økonomiavdeling. Se også hjemmenettverk (side 168).

nettverkskart

Grafisk representasjon av datamaskinene og komponentene som utgjør et hjemmenettverk.

nettverksstasjon

En disk- eller båndstasjon som er koplet til en tjener på et nettverk som deles av flere brukere. Nettverkstasjoner kalles også "eksterne stasjoner".

NIC

Network Interface Card. Et kort som settes i en bærbar datamaskin eller en annen enhet, og kopler enheten til et lokalnett.

node

En enkelt datamaskin som er koblet til et nettverk.

nøkkel

En serie med bokstaver og siffer som brukes av to enheter til å autentisere kommunikasjonen. Begge enheter må ha nøkkelen. Se også WEP (side 177), WPA (side 178), WPA2 (side 178), WPA2-PSK (side 178), WPA-PSK (side 178).

O

oppringningsprogrammer

Programvare som omdirigerer Internett-forbindelser til en annen aktør enn brukerens internettleverandør i den hensikt å belaste ekstra tilkoblingsgebyrer til fordel for en innholdsleverandør, forhandler eller annen tredjepart.

oppsiktsfiler

Filtyper (for eksempel .doc og .xls) som Sikkerhetskopier og gjenopprett arkiverer eller sikkerhetskopierer i oppsiktsplasseringer.

oppsiktsplasseringer

Mappene på datamaskinen din som Sikkerhetskopier og gjenopprett overvåker.

ordbokangrep

En type brute force-angrep som benytter vanlige ord for å forsøke å oppdage et passord.

orm

Et virus som sprer seg ved å opprette kopier av seg selv på andre stasjoner, systemer eller nettverk. Masseutsendelsesormer er ormer som krever at brukere er med på å spre dem, f.eks. ved å åpne et vedlegg eller kjøre en nedlastet fil. De fleste e-postvirus i dag er ormer. En selvreproduserende orm formerer seg uten medvirkning fra brukere. Blaster og Sasser er eksempler på slike selvreproduserende ormer.

P

Papirkurv

Simulert søppelbøtte for slettede filer og mapper i Windows.

passord

Kode (består vanligvis av bokstaver og tall) som brukes til å få tilgang til datamaskinen, et program eller et webområde.

passordhvelv

Et sikkert lagringsområde for dine passord. Her kan du lagre passordene dine og være sikker på at ingen andre brukere (selv en administrator) kan få tilgang.

phishing

En metode for gjennom svindel å få tak i personopplysninger, som passord, personnummer og kredittkortopplysninger. Metoden går ut på å sende falske e-poster som ser ut som de kommer fra avsendere man stoler på, som banker eller andre legitime virksomheter. I typiske tilfeller ber en phishing-melding mottakeren om å klikke på en kobling for å bekrefte eller oppdatere kontakt- eller kredittkortopplysninger.

plugin-modul

Et lite program som legger til nye funksjoner eller forbedrer en mer omfattende programvare. For eksempel kan plugin-moduler gi nettleseren tilgang til å kjøre filer inne i HTML-dokumenter som er i formater som nettleseren vanligvis ikke kjenner igjen (for eksempel animasjons-, video- og lydfiler).

POP3

Post Office Protocol 3. Grensesnitt mellom et e-postprogram og e-posttjeneren. De fleste hjemmebrukere har en POP3 e-postkonto, også kjent som standard e-postkonto.

popup-vinduer

Små vinduer som vises over andre vinduer på dataskjermen. Popup-vinduer brukes ofte til å vise reklame i nettleseren.

port

Et maskinvaregrensesnitt som brukes til å formidle data inn og ut av en dataenhet. Personlige datamaskiner har flere typer porter, blant annet interne porter for tilkobling av harddisk, skjerm og tastatur, samt eksterne porter for tilkobling av modem, skriver, mus og annet periferiutstyr.

potensielt uønsket program (PUP)

Et dataprogram som kan være uønsket, til tross for at brukeren kanskje samtykket i at skulle bli lastet ned. Det kan endre innstillingene for sikkerhet eller personvern på datamaskinen hvis det blir installert. PUP-er kan inneholde spionprogrammer, reklameprogrammer og oppringningsprogrammer, og kan bli lastet ned sammen med et program som brukeren vil ha.

PPPoE

Point-to-Point Protocol Over Ethernet. En måte å bruke Point-to-Point Protocol (PPP) oppringningsprotoll på med Ethernet som transportkanal.

protokoll

Et sett med regler som gjør at datamaskiner eller andre enheter kan utveksle data. I en lagdelt nettverksarkitektur (Open Systems Interconnection-modellen) har hvert lag sine egne protokoller som definerer hvordan kommunikasjonen skal finne sted på det nivået. Datamaskinen eller enheten må støtte den rette protokollen hvis den skal kunne kommunisere med andre datamaskiner. Se også Open Systems Interconnection (OSI).

proxy

En datamaskin (eller programvaren som kjører på maskinen) som fungerer som en barriere mellom et nettverk og Internett ved å ha bare én enkelt nettverksadresse til eksterne områder. Ved å representere alle interne datamaskiner, beskytter proxyen nettverksidentiteter samtidig som den gir tilgang til Internett. Se også proxy-tjener (side 173).

proxy-tjener

En brannmurkomponent som styrer Internett-trafikk til og fra et lokalnett (LAN). En proxy-tjener kan forbedre ytelsen ved å levere data som brukerne ofte ber om, for eksempel en populær nettside, og den kan filtrere og forkaste forespørsler som eieren ikke ønsker, for eksempel forespørsler om uautorisert tilgang til proprietære filer.

publisere

Det å gjøre en sikkerhetskopiert fil tilgjengelig for allmennheten på Internett. Du kan få tilgang til publiserte filer ved å søke i biblioteket Sikkerhetskopier og gjenopprett.

R

RADIUS

Remote Access Dial-In User Service. En protokoll som gjør det mulig å godkjenne brukere, vanligvis i form av ekstern tilgang. Protokollen ble opprinnelig brukt for tjenere med ekstern tilgang via oppringning, men den brukes nå i en rekke godkjenningsmiljøer, som 802.1x-godkjenning av WLAN-brukeres delte hemmeligheter. Se også delt hemmelighet.

register

En database som Windows bruker til å lagre konfigurasjonsopplysninger for datamaskinens brukere, maskinvaren, installerte programmer og egenskapsinnstillinger. Databasen er inndelt i nøkler, som det settes verdier for. Uønskede programmer kan endre verdien i registernøkler eller opprette nye for å kjøre ondsinnet kode.

ren tekst

Tekst som ikke er kryptert. Se også kryptering (side 169).

roaming

Å gå fra et tilgangspunktområde til en annet uten brudd i tilkoblingen.

rootkit

En samling verktøy (programmer) som gir brukeren adgang til en datamaskin eller datamaskinnettverk på administrator-nivå. Rootkits kan inneholde spionprogrammer og andre potensielt uønskede programmer som kan medføre ytterligere risiko for datamaskinens sikkerhet og personopplysninger.

ruter

En nettverksenhet som videresender datapakker fra et nettverk til et annet. Rutere leser hver pakke som kommer inn, og bestemmer hvordan de skal videresendes på grunnlag av avsender og mottaker, samt trafikkforholdene. En ruter kalles av og til for et tilgangspunkt (AP).

råkraftsangrep (brute-force attack)

En hacking-metode som brukes til å finne passord eller krypteringsnøkler ved å prøve alle mulige tegnkombinasjoner helt til krypteringen knekkes.

S

sanntidssøk

Å skanne filer og mapper etter virus og annen aktivitet når de åpnes av deg eller datamaskinen.

sikkerhetskopi

For å opprette en kopi av viktige filer, oftest på en sikker, tilkoplet tjener. Se også arkiv (side 166).

skanning på forespørsel

En planlagt undersøkelse av utvalgte filer, programmer eller nettverksenheter for å finne en trusler, sårbarhet eller andre potensielt uønskede enheter. Den kan finne sted umiddelbart, på en fastsatt tidspunkt i fremtiden eller med fastsatte mellomrom. Jf. skanning ved tilgang. Se også sårbarhet.

skript

Liste over kommandoer som kan utføres automatisk (det vil si uten at bruker foretar seg noe). I motsetning til programmer lagres skript vanligvis som ren tekst og kompileres hver gang de kjøres. Makroer og batch-filer kalles også skript.

smartstasjon

Se USB-stasjon (side 177).

SMTP

Simple Mail Transfer Protocol. En TCP/IP-protokoll for å sende meldinger fra en datamaskin til en annen på et nettverk. Denne protokollen brukes på Internett til å distribuere e-post.

snarvei

Fil som inneholder kun plasseringen til en annen fil på datamaskinen.

sporingsbilder

Små grafikkfiler som kan skjule seg på HTML-sider og tillater en uautorisert kilde å legge til informasjonskapsler på datamaskinen din. Disse informasjonskapslene kan da overføre informasjon til den uautoriserte kilden. Sporingsbilder kalles også "skjulte/usynlige sporingsbilder" og "usynlige GIF-er".

SSID

Service Set Identifier. Et tegn (hemmelig nøkkel) som identifiserer et Wi-Fi (802.11) nettverk. SSID konfigureres av nettverksadministrator og må oppgis av brukere som vil koble seg til nettverket.

SSL

Secure Sockets Layer. En protokoll utviklet av Netscape for å sende private dokumenter via Internett. SSL bruker en offentlig nøkkel til å kryptere data som overføres over SSL-tilkoblingen. URL-er som krever en SSL-tilkobling, begynner med HTTPS istedenfor HTTP.

standard e-postkonto

Se POP3 (side 172).

svarteliste

I Anti-Spam er dette en liste over e-postadresser du ikke ønsker å motta meldinger fra, fordi du tror meldingene er spam, eller søppelpost. Innen phishing-beskyttelse, en liste over webområder som anses å være et middel for nettsvindel. Se også hviteliste (side 168).

synkronisere

Fjerne inkonsekvenser mellom sikkerhetskopierte filer og dem som er lagret på den lokale datamaskinen. Du synkroniserer filer når filversjonen i databasen for sikkerhetskopi på nettet er nyere enn filversjonen på de andre datamaskinene.

systemgjenopprettingspunkt

En kopi (bilde) av innholdet i datamaskinens minne eller en database. Windows lager gjenopprettingspunkter med jevne mellomrom og når det oppstår viktige systemhendelser, som når et program eller en driver blir installert. Du kan også opprette og sette navn på dine egne gjenopprettingspunkt når som helst.

SystemGuard

McAfee-varsler som oppdager uautoriserte endringer i datamaskinen og varsler deg når de oppstår.

T

tilgangspunkt (AP)

En nettverksenhet (vanligvis kalt en trådløs ruter) som kan kobles til en Ethernet-hub eller -svitsj for å utvide det fysiske serviceområdet til en trådløs bruker. Når trådløse brukere roamer med mobile enheter går overføringen fra ett tilgangspunkt til et annet for å opprettholde tilkoblingen.

tjener

En datamaskin eller et program som tar imot tilkoblinger fra andre datamaskiner eller programmer og gir korrekte svar. For eksempel kobler e-postprogrammet seg til en e-posttjener hver gang du sender eller mottar e-post.

tjenestenektangrep (DoS)

En type angrep mot en datamaskin, tjener eller et nettverk som stanser eller gjør trafikken i et nettverk langsommere. Det oppstår når et nettverk blir oversvømt av så mange tilleggsforespørsler at vanlig trafikk går langsommere eller avbrytes helt. Et tjenestenektangrep overvelder angrepsmålet med falske tilkoblingsforespørsler, slik at målet ignorerer legitime forespørsler.

TKIP

Temporal Key Integrity Protocol (uttales ti-kip). En del av 802.11i-krypteringsstandarden for trådløse lokalnettverk. TKIP er neste generasjon av WEP, som brukes til å kryptere trådløse lokalnettverk etter 802.11-standarden. TKIP veksler nøkkel for hver pakke, sjekker meldingers integritet og har en mekanisme for å tildele nøkkel på nytt, og retter dermed opp ulempene ved WEP.

trojansk hest

Et program som ikke reproduserer seg selv, men som utretter skade eller setter datamaskinens sikkerhet i fare. Oftest er det en enkeltperson som mailer en trojansk hest til deg, den mailer ikke seg selv. Du kan også laste ned trojanske hester fra et nettsted eller via peer-to-peer-nettverk uten å vite det.

trådløst kort

Enhet som gir en datamaskin eller PDA trådløs kapasitet. Det kobles til via en USB-port, spor for PC-kort (CardBus) eller minnekort, eller internt til PCI-bussen.

trådløst PCI-kort

Peripheral Component Interconnect. Et trådløst kort som kan settes inn i et utvidelsesspor inne i datamaskinen.

trådløst USB-kort

Kort for trådløs kommunikasjon som kan settes inn i USB-porten i datamaskinen.

U

U3

You: Simplified, Smarter, Mobile. Plattform for å kjøre programmer for Windows 2000 eller Windows XP direkte fra en USB-stasjon. U3 ble startet i 2004 av M-Systems og SanDisk og lar brukere kjøre U3-programmer på en datamaskin med Windows uten å installere eller lagre data eller innstillinger på datamaskinen.

uautorisert tilkoblingspunkt

Uautoriserte tilkoblingspunkter kan installeres i et sikkert firmanettverk for å gi uautoriserte parter tilgang til nettverket. De kan også lages for å la en angriper utføre et man-in-the-middle-angrep.

URL

Uniform Resource Locator. Standardformatet for Internett-adresser.

USB

Universal Serial Bus. Tilkoblingspunkt som finnes på de fleste datamaskiner og som kan brukes til å koble til en rekke enheter, fra tastaturer og mus til webkameraer, skannere og skrivere.

USB-stasjon

En liten minnestasjon som kan kobles til USB-porten på en datamaskin. En USB-enhet fungerer som en liten harddisk, og gjør det enkelt å overføre filer fra en datamaskin til en annen.

V

virus

Et dataprogram som kan kopiere seg selv og infisere en datamaskin uten at brukeren tillater eller vet det.

VPN

Virtual Private Network. Et privat kommunikasjonsnettverk som konfigureres via et vertsnettverk som for eksempel Internett. Dataene som sendes via en VPN-forbindelse, er kryptert og beskyttet av kraftige sikkerhetsfunksjoner.

W

wardriver

Person som søket etter Wi-Fi (802.11)-nettverk ved å kjøre gjennom byer utstyrt med en Wi-Fi-datamaskin og en spesiell type maskinvare eller programvare.

webpost

Web-basert e-post. Elektronisk posttjeneste som man bruker hovedsaklig via en nettleser og ikke en e-postklient på datamaskinen som Microsoft Outlook. Se også e-post (side 167).

WEP

Wired Equivalent Privacy. En krypterings- og godkjenningsprotokoll definert som del av Wi-Fi (802.11)-standarden. De første versjonene er basert på RC4-chiffer og har betydelige svakheter. WEP prøver å ivareta sikkerheten ved å kryptere data over radiobølger slik at dataene er beskyttet mens de sendes fra et punkt til et annet. Man har imidlertid funnet ut at WEP ikke er like sikkert som man trodde.

Wi-Fi

Wireless Fidelity. Et begrep som brukes av Wi-Fi Alliance når den referer til alle typer 802.11-nettverk.

Wi-Fi Alliance

En organisasjon bestående av ledende leverandører av trådløs maskin- og programvare. Wi-Fi Alliance bestreber seg på å sertifisere alle 802.11-baserte produkter for interoperabilitet og fremme begrepet Wi-Fi som det globale merkenavnet innenfor alle markeder for produkter for 802.11-baserte trådløse LAN-nettverk. Organisasjonen er et konsortium, testlaboratorium og finansinstitusjon for leverandører som vil fremme industrivekst.

Wi-Fi-godkjent

Å bli testet og godkjent av Wi-Fi Alliance. Wi-Fi-godkjente produkter anses å kunne brukes om hverandre, selv om de stammer fra forskjellige produsenter. En bruker med et Wi-Fi-godkjent produkt kan bruke tilkoblingspunkter (AP) fra et hvilket som helst merke med et annet klientmaskinvare-merke som også er godkjent.

WLAN

Trådløst lokalnettverk. Et lokalnettverk (LAN) som bruker trådløst tilkobling. Et WLAN bruker høyfrekvensbølger i stedet for kabler til å la datamaskiner kommunisere med hverandre.

WPA

Wi-Fi Protected Access. En spesifikasjonsstandard som gir økt databeskyttelse og tilgangskontroll for eksisterende og fremtidige trådløse LAN-systemer. WPA kjøres som en programvareoppgradering på eksisterende maskinvare, og er utledet fra og kompatibelt med 802.11i-standarden. Når WPA er installert på korrekt måte, kan brukere med trådløse lokalnettverk stole på at dataene deres er beskyttet, og at kun godkjente nettverksbrukere har tilgang til nettverket.

WPA-PSK

En spesiell WPA-modus utviklet for hjemmebrukere som ikke trenger like høy grad av sikkerhet som bedrifter, og som ikke har tilgang til godkjenningstjenere. I denne modusen oppgir hjemmebrukeren startpassordet manuelt for å aktivere WPA i modus for fohåndsdelt nøkkel, og bør endre passfrasen på hver trådløse datamaskin og hvert tilkoblingspunkt med jevne mellomrom. Se også WPA2-PSK (side 178), TKIP (side 176).

WPA2

En oppdatering til WPA-sikkerhetsstandarden, basert på 802.11i-standarden.

WPA2-PSK

En spesiell WPA-modus som ligner WPA-PSK og er basert på WPA2-standarden. En vanlig WPA2-PSK-funksjon er at enheten ofte støtter flere krypteringsmetoder (for eksempel AES, TKIP) samtidig, mens eldre enheter vanligvis kun støtter en krypteringsmetode av gangen (dvs. at alle klientene måtte bruke samme krypteringsmetode).

Om McAfee

McAfee, Inc., som har hovedkontor i Santa Clara i California og er verdensleder innen inntrengingsforhindring og håndtering av sikkerhetsrisikoer, leverer proaktive og dokumenterte løsninger og tjenester som ivaretar sikkerheten til systemer og nettverk over hele verden. Gjennom sin sikkerhetsekspertise og satsning på nyskaping gir McAfee hjemmebrukere, bedrifter, offentlig sektor og tjenesteleverandører mulighet til å stanse angrep, forhindre forstyrrelser og overvåke og forbedre sikkerheten kontinuerlig.

Lisens

Copyright

KAPITTEL 36

Kundestøtte og teknisk støtte

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer så snart det oppdager dem. Kritiske beskyttelsesproblemer krever øyeblikkelig handling og kan sette din beskyttelsesstatus på spill (endre fargen til rød). Ikke-kritiske beskyttelsesproblemer krever ikke øyeblikkelig handling og kan kanskje sette din beskyttelsesstatus på spill (avhengig av hva slags type problem det dreier seg om). For å oppnå grønn beskyttelsesstatus må du reparere alle kritiske problemer og enten reparere eller ignorere alle ikke-kritiske problemer. Hvis du trenger hjelp til å diagnostisere beskyttelsesproblemene, kan du kjøre McAfee Virtuell Tekniker. For mer informasjon om McAfee Virtuell tekniker, se Hjelp for McAfee Virtuell tekniker.

Hvis du kjøpte sikkerhetsprogramvaren fra en annen samarbeidspartner eller forhandler enn McAfee åpner du en webleser og går til www.mcafeehjelp.com. Deretter velger du samarbeidspartner eller forhandler under Samarbeidskoblinger for å få tilgang til McAfee Virtuell tekniker.

Merknad: For å installere og kjøre McAfee Virtuell tekniker må du logge inn på datamaskinen din som Windows-administrator. Hvis du ikke gjør det, kan det hende MVT ikke kan løse problemene dine. For informasjon om hvordan du logger inn som Windows-administrator, se Hjelp for Windows. I Windows Vista™ blir du bedt om det når du kjører MVT. Når dette skjer klikker du på **Godta**. Virtuell tekniker virker ikke med Mozilla® Firefox.

I dette kapitlet

Bruke McAfee Virtuell tekniker

I likhet med en personlig teknisk støtterepresentant, samler Virtuell tekniker informasjon om dine SecurityCenter-programmer, slik at den kan løse sikkerhetsproblemer på datamaskinen din. Når du kjører Virtuell tekniker sjekker det for å sikre at SecurityCenter-programmene dine virker som de skal. Hvis det oppdager problemer tilbyr Virtuell tekniker seg å fikse dem for deg eller gi deg mer detaljert informasjon om dem. Når den er ferdig, viser Virtuell tekniker resultatene av analysen og lar deg om nødvendig søke ytterligere teknisk støtte fra McAfee.

For å opprettholde sikkerheten og integriteten til datamaskinen og filene dine, samler ikke Virtuell tekniker inn personlig informasjon som kan identifisere deg.

Merknad: For mer informasjon om Virtuell tekniker, klikk **Hjelp** -ikonet i Virtuell tekniker.

Starte Virtual Technician

Virtual Technician samler informasjon om dine SecurityCenter-programmer slik at det kan hjelpe deg å løse dine beskyttelsesproblemer. For å sikre personvernet ditt inkluderer ikke denne informasjonen personlig identifiserbar informasjon.

1. Under **Vanlige oppgaver** klikker du **McAfee Virtual Technician**.
2. Følg instruksjonene på skjermen for å laste ned og kjøre Virtual Technician.

Se følgende tabeller for webområder for McAfee Støtte og nedlastinger, inkludert brukerhåndbøker, for ditt land eller region.

Støtte og nedlastinger

Land/region	McAfee-støtte	McAfee-nedlastinger
Australia	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasil	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?langid=48
Danmark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp

Finland	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Frankrike	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Hellas	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
Italia	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japan	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Kina (forenklet kinesisk)	www.mcafeehelp.com	cn.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
Russland	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
Slovakia	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
Spania	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Storbritannia	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Sverige	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tsjekkia	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Tyrkia	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Tyskland	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Ungarn	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
USA	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection - brukerhåndbøker

Land/region	McAfee-brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasil	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
Danmark	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Hellas	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/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
Nederland	download.mcafee.com/products/manuals/nl/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
Russland	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slovakia	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf

Storbritannia	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tsjekkia	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security - brukerhåndbøker

Land/region	McAfee-brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasil	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
Danmark	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Hellas	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/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
Nederland	download.mcafee.com/products/manuals/nl/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
Russland	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slovakia	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Storbritannia	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tsjekkia	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus - brukerhåndbøker

Land/region	McAfee-brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasil	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
Danmark	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Hellas	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/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
Nederland	download.mcafee.com/products/manuals/nl/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
Russland	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
Slovakia	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Storbritannia	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tsjekkia	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf

Tyskland	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan - brukerhåndbøker

Land/region	McAfee-brukerhåndbøker
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasil	download.mcafee.com/products/manuals/pt-br/VS_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
Danmark	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Frankrike	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Hellas	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
Italia	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/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
Nederland	download.mcafee.com/products/manuals/nl/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

Russland	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Slovakia	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Spania	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Storbritannia	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tsjekkia	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Tyrkia	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Se følgende tabell for webområder om McAfee Threat Center og Virusinformasjon i ditt land eller region.

Land/region	Sikkerhetshovedkontor	Virusinformasjon
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasil	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
Danmark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finland	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Frankrike	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo

Hellas	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Italia	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japan	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Kina (forenklet kinesisk)	www.mcafee.com/us/threat_center	cn.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
Nederland	www.mcafee.com/us/threat_center	nl.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
Russland	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slovakia	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Spania	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Storbritannia	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Sverige	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tsjekkia	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Tyrkia	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Tyskland	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Ungarn	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
USA	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Se følgende tabell for HackerWatch-webområder i ditt land eller region.

Land/region	HackerWatch
Australia	www.hackerwatch.org
Brasil	www.hackerwatch.org/?lang=pt-br
Canada (engelsk)	www.hackerwatch.org
Canada (fransk)	www.hackerwatch.org/?lang=fr-ca
Danmark	www.hackerwatch.org/?lang=da
Finland	www.hackerwatch.org/?lang=fi
Frankrike	www.hackerwatch.org/?lang=fr
Hellas	www.hackerwatch.org/?lang=el
Italia	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Kina (forenklet kinesisk)	www.hackerwatch.org/?lang=zh-cn
Korea	www.hackerwatch.org/?lang=ko
Mexico	www.hackerwatch.org/?lang=es-mx
Nederland	www.hackerwatch.org/?lang=nl
Norge	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Russland	www.hackerwatch.org/?lang=ru
Slovakia	www.hackerwatch.org/?lang=sk
Spania	www.hackerwatch.org/?lang=es
Storbritannia	www.hackerwatch.org
Sverige	www.hackerwatch.org/?lang=sv
Taiwan	www.hackerwatch.org/?lang=zh-tw
Tsjekkia	www.hackerwatch.org/?lang=cs
Tyrkia	www.hackerwatch.org/?lang=tr
Tyskland	www.hackerwatch.org/?lang=de
Ungarn	www.hackerwatch.org/?lang=hu
USA	www.hackerwatch.org

Indeks

L

M

N

O

P

Q

R

W

Å