

McAfee®

Wireless Protection 2007

Käyttöopas

Sisältö

| | |
|--|-----------|
| McAfee Wireless Protection | 5 |
| <hr/> | |
| McAfee SecurityCenter | 7 |
| <hr/> | |
| Ominaisuudet | 8 |
| SecurityCenterin käyttäminen | 9 |
| Otsikko | 9 |
| Vasen sarake | 9 |
| Pääikkuna | 10 |
| SecurityCenterin kuvakkeiden toiminta | 11 |
| Suojauksen tilan toiminta | 13 |
| Suojausongelmien korjaaminen | 19 |
| SecurityCenterin tietojen tarkasteleminen | 20 |
| Lisävalikon käyttäminen | 20 |
| SecurityCenterin asetusten määrittäminen | 21 |
| Suojauksen tilan asetusten määrittäminen | 22 |
| Käyttäjäasetusten määrittäminen | 23 |
| Päivitysasetusten määrittäminen | 26 |
| Hälytysasetusten määrittäminen | 31 |
| Yleisten tehtävien suorittaminen | 33 |
| Suorita yleisiä tehtäviä | 33 |
| Tarkastele äskettäisiä tapahtumia | 34 |
| Ylläpidä tietokonetta automaattisesti | 35 |
| Ylläpidä tietokonetta manuaalisesti | 36 |
| Hallitse verkkoa | 38 |
| Hanki lisätietoja viruksista | 38 |
| | |
| McAfee QuickClean | 39 |
| <hr/> | |
| QuickClean-ohjelman toiminnot | 40 |
| Ominaisuudet | 40 |
| Tietokoneen puhdistaminen | 41 |
| QuickClean-ohjelman käyttäminen | 43 |
| | |
| McAfee Shredder | 45 |
| <hr/> | |
| Shredder-ohjelman toiminnot | 46 |
| Ominaisuudet | 46 |
| Ei-toivottujen tiedostojen poistaminen Shredder-ohjelmalla | 47 |
| Shredder-ohjelman käyttäminen | 48 |

| | |
|--|------------|
| McAfee Network Manager | 49 |
| Ominaisuudet | 50 |
| Network Managerin kuvakkeiden toiminta | 51 |
| Hallitun verkon määrittäminen | 53 |
| Verkkokartan käyttäminen | 54 |
| Hallittuun verkkoon liittyminen | 57 |
| Verkon etähallinta..... | 61 |
| Tilan ja oikeuksien valvonta | 62 |
| Tietoturvan puutteiden korjaaminen | 65 |
| | |
| McAfee Wireless Network Security | 67 |
| Ominaisuudet | 68 |
| Wireless Network Securityn ottaminen käyttöön..... | 70 |
| Ota Wireless Network Security käyttöön | 70 |
| Poista Wireless Network Security käytöstä..... | 71 |
| Langattomien verkkojen suojaaminen..... | 73 |
| Suojattujen langattomien verkkojen määrittäminen | 74 |
| Lisää tietokoneita suojattuun langattomaan verkkoon..... | 86 |
| Langattomien verkkojen hallinnointi..... | 91 |
| Langattomien verkkojen hallinta | 92 |
| Langattoman verkon suojauksen hallinta..... | 103 |
| Suojausasetusten määrittäminen | 104 |
| Verkkoavainten hallinta..... | 109 |
| Langattomien verkkojen valvonta | 119 |
| Langattomien verkkoyhteyksien valvonta..... | 120 |
| Suojattujen langattomien verkkojen valvonta | 125 |
| Vianmääritys..... | 131 |
| | |
| McAfee EasyNetwork | 147 |
| Ominaisuudet | 148 |
| EasyNetworkin asentaminen | 149 |
| EasyNetworkin käynnistäminen | 150 |
| Hallittuun verkkoon liittyminen | 151 |
| Hallitusta verkosta poistuminen..... | 155 |
| Tiedostojen jakaminen ja lähettäminen | 157 |
| Tiedostojen jakaminen | 158 |
| Tiedostojen lähettäminen toisiin tietokoneisiin..... | 161 |
| Tulostinten jakaminen | 163 |
| Jaettujen tulostinten käyttäminen | 164 |

| | |
|----------|-----|
| Liitteet | 167 |
|----------|-----|

| | |
|---------|-----|
| Sanasto | 168 |
|---------|-----|

| | |
|-------------------|-----|
| Tietoja McAfeesta | 185 |
|-------------------|-----|

| | |
|----------------|-----|
| Copyright..... | 186 |
|----------------|-----|

| | |
|-----------|-----|
| Hakemisto | 187 |
|-----------|-----|

LUKU 1

McAfee Wireless Protection

McAfee Wireless Protection Suite poistaa verkko-ongelmat ja langattoman verkon riskit. Sen luotettava suoja torjuu hakkerien hyökkäykset langattomaan verkkoosi, suojaa henkilötietosi ja tietoliikenteesi sekä estää muita käyttämästä verkkoasi Internet-yhteyden muodostamiseen - kaiken tämän yhdellä napsautuksella. McAfee Wireless Network Securityn vahvat, kierrätettävät salausavaimet estävät päättäväisimpienkin hakkereiden hyökkäykset. Wireless Protection sisältää myös McAfee EasyNetworkin, joka helpottaa tiedostojen ja tulostinten jakamista verkossa. Se sisältää myös McAfee Network Managerin, joka valvoo verkkosi tietokoneita tietoturvariskien varalta ja helpottaa mahdollisten tietoturva-aukkojen korjaamista.

Wireless Protection sisältää seuraavat ohjelmat:

- SecurityCenter
- Wireless Network Security
- Network Manager
- EasyNetwork

L U K U 2

McAfee SecurityCenter

McAfee SecurityCenter on helppokäyttöinen ympäristö, jossa McAfeen käyttäjät voivat ottaa tietoturvatilauksensa käyttöön, hallita sitä ja määrittää sen asetukset.

SecurityCenter on myös tietopankki, jossa on tietoja virushälytyksistä, tuotteista, tuesta ja tilauksista, ja se mahdollistaa McAfeen Web-sivustossa olevien työkalujen käytön ja uutisten lukemisen yhdellä näppäimen painalluksella.

Tässä luvussa

| | |
|--|----|
| Ominaisuudet..... | 8 |
| SecurityCenterin käyttäminen | 9 |
| SecurityCenterin asetusten määrittäminen | 21 |
| Yleisten tehtävien suorittaminen..... | 33 |

Ominaisuudet

McAfee SecurityCenter tarjoaa seuraavat uudet toiminnot ja edut:

Uudelleensuunniteltu suojaustila

Voit helposti tarkastaa tietokoneesi suojaustilan, etsiä päivityksiä ja korjata mahdollisia tietoturva-aukkoja.

Jatkuvat päivitykset ja uudet tuoteversiot

Asenna päivittäiset päivitykset automaattisesti. Kun uusi McAfee-ohjelmistoversio on saatavilla, tilaajana saat sen automaattisesti ilman lisäkustannuksia, jotta suojauksesi on aina ajan tasalla.

Reaaliaikaiset hälytykset

Suojahälytykset ilmoittavat virusesiintymistä ja tietoturvauhista sekä tarjoavat toimintavaihtoehtoja uhkien poistamiseen ja neutralointiin sekä lisätietoja uhista.

Helppokäyttöinen suojaus

Useat uudistusvaihdot auttavat pitämään McAfee-suojauksesi ajan tasalla.

Suorituskykyökalut

Poista käyttämättömät tiedostot, eheyttä käytetyt tiedostot ja käytä järjestelmän palautusta, jotta voit pitää tietokoneen suorituskyvyn parhaana mahdollisena.

Oikeaa online-tukea

McAfeen tietoturva-ammattilaiset tarjoavat tukipalveluja puhelimen, sähköpostin ja Internet-keskusteluohjelmien välityksellä.

Suojatun selauksen suojaus

Jos McAfee SiteAdvisor -selainlaajennus on asennettu, se auttaa suojaamaan sinua vakoiluohjelmilta, roskapostilta, viruksilta ja verkkohuijauksilta arvioimalla Web-hakutuloksissa luetellut Web-sivustot tai sivut, joilla olet käynyt. Voit tarkastella yksityiskohtaisia turvallisuusarviomäärittelyjä, jotka näyttävät sivuston sähköpostikäytäntöjä, ladattavia tiedostoja, verkkoyhteyksiä sekä ponnahdusikkunoiden ja kolmansien osapuolten seurantaevästeiden kaltaisia häiriötekijöitä koskevien testien tulokset.

LUKU 3

SecurityCenterin käyttäminen

Voit käynnistää SecurityCenterin napsauttamalla McAfee SecurityCenterin kuvaketta , joka sijaitsee tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella tai Windowsin työpöydällä.

Kun avaat SecurityCenterin, Koti-ikkuna näyttää tietokoneen suojauksen tilan ja antaa mahdollisuuden päivitysten, tarkistusten (jos McAfee VirusScan on asennettu) ja muiden yleisten tehtävien nopeaan suorittamiseen:

Otsikko

Ohje

Tarkastele ohjelman ohjetiedostoa.

Vasen sarake

Päivitä

Suojaudu uusilta uhilta päivittämällä tuotteesi.

Tarkista

Jos McAfee VirusScan on asennettu, voit tarkistaa tietokoneen manuaalisesti.

Yleiset tehtävät

Suorita yleisiä tehtäviä: palaa Koti-ikkunaan, tarkastele äskettäisiä tapahtumia, hallitse tietokoneverkkoa (jos käytät verkon hallintaan kykenevää tietokonetta) ja ylläpidä tietokonetta. Jos McAfee Data Backup on asennettu, voit myös varmuuskopioida tietosi.

Asennetut komponentit

Katso, mitkä tietoturvapalvelut huolehtivat tietokoneesi turvallisuudesta.

Pääikkuna

Suojauksen tila

Olenko suojattu? -kohdassa voit tarkastella tietokoneen yleistä suojauksen tilaa. Sen alapuolella näet tilan eriteltynä suojausluokan ja -tyypin mukaan.

SecurityCenterin tiedot

Tarkista, koska tietokone on päivitetty viimeksi, koska se on tarkistettu viimeksi (jos McAfee VirusScan on asennettu) ja koska tilaus umpeutuu.

Tässä luvussa

| | |
|---|----|
| SecurityCenterin kuvakkeiden toiminta..... | 11 |
| Suojauksen tilan toiminta | 13 |
| Suojausongelmien korjaaminen | 19 |
| SecurityCenterin tietojen tarkasteleminen | 20 |
| Lisävalikon käyttäminen..... | 20 |

SecurityCenterin kuvakkeiden toiminta

SecurityCenterin kuvakkeet ilmestyvät tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle. Niiden avulla voit tarkistaa, onko tietokoneesi täysin suojattu, tarkastella käynnissä olevan tarkistuksen tilaa (jos McAfee VirusScan on asennettu), hakea päivityksiä, tarkastella äskettäisiä tapahtumia, ylläpitää tietokonetta ja pyytää tukea McAfeen Web-sivustosta.


Avaa SecurityCenter ja käytä lisäominaisuuksia

Kun SecurityCenter on käynnissä, tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle ilmestyy SecurityCenter M -kuvake .

SecurityCenterin avaaminen tai lisäominaisuuksien käyttäminen:

- Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella ja valitse yksi seuraavista:
 - Avaa SecurityCenter
 - Päivitykset
 - Pikalinkit
- Alivalikossa on linkit Koti-, Tarkastele äskettäisiä tapahtumia-, Verkonhallinta-, Ylläpidä tietokonetta- ja Data Backup -valikkovaihtoehtoihin (jos asennettu).
- Vahvista tilaus
- (Tämä kohde ilmestyy näyttöön sen jälkeen, kun ainakin yhden tuotteen tilaus on umpeutunut.)
- Päivityskeskus
 - Asiakastuki


Tarkista suojauksen tila

Jos tietokone ei ole täysin suojattu, tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle ilmestyy suojauksen tilan kuvake . Suojauksen tilan mukaan kuvake voi olla punainen tai keltainen.

Suojauksen tilan tarkistaminen:

- Avaa SecurityCenter napsauttamalla suojauksen tilan kuvaketta ja korjaa mahdolliset ongelmat.

Tarkista päivitysten tila

Jos olet hakemassa päivityksiä, tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle ilmestyy päivityskuvake .

Päivitysten tilan tarkistaminen:

- Napsauttamalla päivityskuvaketta voit tarkastella päivitysten tilaa työkaluvihjeenä.

Suojauksen tilan toiminta

Tietokoneen yleinen suojauksen tila on ilmoitettu Security Centerin **Olenko suojattu?** -kohdassa.

Suojauksen tila ilmaisee, onko tietokone täysin suojattu uusia tietoturvahaukia vastaan, kuten myös sen, vaativatko ongelmat huomiota ja miten ne voi ratkaista. Jos ongelma vaikuttaa useampaan suojausluokkaan, ongelman ratkaiseminen voi palauttaa useamman luokan täysin suojattuun tilaan.

Suojauksen tilaan vaikuttavat muun muassa ulkoiset tietoturvahauhat, tietokoneeseen asennetut tietoturvatuotteet, Internetiä käyttävät tuotteet sekä kyseisten tietoturva- ja Internet-tuotteiden asetukset.

Oletusarvoisesti nämä ei-kriittiset suojausongelmat ohitetaan automaattisesti ja niitä ei seurata yleisessä suojauksen tilassa, jos roskapostin torjuntaa ja sisällön estämistä ei ole asennettu. Jos suojausongelman perässä on **Ohita**-linkki, voit halutessasi ohittaa ongelman, jos olet varma, että et halua korjata sitä.

Olenko suojattu?

SecurityCenterin **Olenko suojattu?** -kohdassa voit tarkastella tietokoneen yleistä suojauksen tilaa:

- Näyttöön ilmestyy **Kyllä**, jos tietokoneesi on täysin suojattu (vihreä).
- Näyttöön ilmestyy **Ei**, jos tietokoneesi on osittain suojattu (keltainen) tai suojaamaton (punainen).

Voit ratkaista useimmat suojausongelmat automaattisesti valitsemalla suojauksen tilan vierestä **Korjaa**. Jos yksi tai useampi suojausongelma ei ratkea ja vaatii toimenpiteitä, napsauta ongelman perässä olevaa linkkiä ja suorita suositeltu toimenpide.

Suojausluokkien ja -tyyppien toiminta

SecurityCenterin **Olenko suojattu?** -kohdassa voit tarkastella suojauksen tilaa seuraavien suojausluokkien ja -tyyppien mukaan jaoteltuna:

- Tietokone ja tiedostot
- Internet ja verkko
- Sähköposti ja pikaviesti
- Käytönvalvonta-asetukset

SecurityCenterissä näkyvät suojaustyypit vaihtelevat asennettujen tuotteiden mukaan. Esimerkiksi Tietokoneen kunto -suojaustyyppi ilmestyy näyttöön silloin, kun McAfee Data Backup -ohjelmisto on asennettu.

Jos luokalla ei ole suojausongelmia, se on vihreässä tilassa. Jos valitset vihreän luokan, oikealle ilmestyy käyttöön otettujen suojaustyyppien luettelo, jota seuraa ohitettujen ongelmien luettelo. Jos ongelmia ei ole, niiden tilalla näkyy virusilmoitus. Voit myös muuttaa kyseisen luokan asetuksia valitsemalla **Määritä**.

Jos luokan kaikki suojaustyypit ovat vihreässä tilassa, myös luokan tila on vihreä. Samalla tavalla yleinen suojauksen tila on vihreä, jos kaikki suojausluokat ovat vihreässä tilassa.

Jos jokin suojausluokka on keltaisessa tai punaisessa tilassa, voit ratkaista suojausongelmat korjaamalla tai ohittamalla ne. Tällöin tila muuttuu vihreäksi.

Tietokone ja tiedostot -suojausten toiminta

Tietokone ja tiedostot -suojausluokka muodostuu seuraavista suojaustyypeistä:

- **Virustorjunta** – Reaaliaikainen tarkistussuojaus suojaa tietokonetta viruksia, matoja, Troijan hevosia, epäilyttäviä komentosarjoja, sekahyökkäyksiä ja muita uhkia vastaan. Se tarkistaa ja yrittää puhdistaa tiedostot (muun muassa .exe-muotoiset pakatut tiedostot, käynnistyslohkon, muistin ja kriittiset tiedostot) automaattisesti, kun sinä tai tietokone yritätte käyttää niitä.
- **Vakoiluohjelmien torjunta** – Vakoiluohjelmien torjunta havaitsee, estää ja poistaa vakoiluohjelmat, mainosohjelmat ja muut mahdollisesti ilman lupaasi henkilökohtaisia tietoja keräävät ja lähettävät ohjelmat nopeasti.
- **SystemGuards** – SystemGuards havaitsee tietokoneeseen tehdyt muutokset ja varoittaa niistä. Voit tämän jälkeen tarkastella muutoksia ja päättää, haluatko sallia ne.
- **Windows-suojaus** – Windows-suojaus näyttää tietokoneen Windows-päivitysten tilan. Jos McAfee VirusScan on asennettu, puskurin ylivuotosuojaus on myös käytettävissä.

Yksi Tietokone ja tiedostot -suojaukseen vaikuttavista tekijöistä on ulkoiset virusuhat. Esimerkiksi suojaako käyttämäsi virustorjuntaohjelmisto sinua virusesiintymiltä? Muita tekijöitä ovat virustorjuntaohjelmiston asetukset ja se, onko tietokone päivitetty uusimmilla tunnistusallekirjoitustiedostoilla, jotka auttavat suojaamaan tietokonetta uusilta uhilta.

Avaa Tietokone ja tiedostot -asetusikkuna

Jos **Tietokone ja tiedostot** -luokassa ei ole ongelmia, voit avata asetusiikkunan tietoikkunasta.

Tietokone ja tiedostot -asetusiikkunan avaaminen:

- 1 Valitse Koti-ikkunasta **Tietokone ja tiedostot**.
- 2 Valitse oikeasta ikkunasta **Määritä**.

Internet ja verkko -suojauksen toiminta

Internet ja verkko -suojaluokka muodostuu seuraavista suojaustyypeistä:

- **Palomuurisuojaus** – Firewall suojaa tietokonetta tietomurroilta ja ei-toivotulta tietoliikenteeltä. Se auttaa hallitsemaan saapuvia ja lähteviä Internet-yhteyksiä.
- **Langaton suojaus** – Langaton suojaus suojaa kodin langatonta verkkoa tietomurroilta ja tietojen sieppaamiselta. Jos olet muodostanut yhteyden ulkoiseen langattomaan verkkoon, suojauksesi taso vaihtelee kuitenkin kyseisen verkon suojaustason mukaan.
- **Web Browsing Protection** – Web-selauksen suojaus piilottaa mainokset, ponnahdusikkunat ja piilojäljitteet tietokoneella Internetiä selattaessa.
- **Phishing-huijausten torjunta** – Phishing-huijausten torjunta auttaa estämään petolliset Web-sivustot, jotka tavoittelevat henkilökohtaisia tietoja sähköpostiviestien ja pikaviestiohjelmien hyperlinkkien avulla, sekä ponnahdusikkunoiden ja muiden keinojen avulla.
- **Henkilökohtaisten tietojen suojaus** – Henkilökohtaisten tietojen suojaus estää arkaluonteisten ja luottamuksellisten tietojen julkistamisen Internetissä.

Avaa Internet ja verkko -asetusikkuna

Jos **Internet ja verkko** -luokassa ei ole ongelmia, voit avata asetussikkunan tietoikkunasta.

Internet ja verkko -asetusikkunan avaaminen:

- 1 Valitse Koti-ikkunasta **Internet ja tiedostot**.
- 2 Valitse oikeasta ikkunasta **Määritä**.

Sähköposti ja pikaviesti -suojauksen toiminta

Sähköposti ja pikaviesti -suojausluokka muodostuu seuraavista suojaustyypeistä:

- **Sähköpostisuojaus** – Sähköpostisuojaus tarkistaa saapuvat ja lähtevät sähköpostiviestit ja liitteet automaattisesti ja yrittää poistaa niissä olevat virukset, vakoiluohjelmat ja mahdolliset uhat.
- **Roskapostin torjunta** – Roskapostin torjunta auttaa estämään ei-toivottujen sähköpostiviestien toimittamisen Saapuvat-kansioosi.
- **Pikaviestisuojaus** – Pikaviestisuojaus tarkistaa saapuvien pikaviestien liitteet automaattisesti ja yrittää poistaa niissä olevat virukset, vakoiluohjelmat ja mahdolliset uhat. Se estää myös pikaviestipalvelimia vaihtamasta haitallisia sisältöjä tai henkilökohtaisia tietoja Internetissä.
- **Suojatun selauksen suojaus** – Jos McAfee SiteAdvisor -selainlaajennus on asennettu, se auttaa suojaamaan sinua vakoiluohjelmilta, roskapostilta, viruksilta ja verkkohuijauksilta arvioimalla vierailemasi tai Web-hakutuloksissa luetellut Web-sivustot. Voit tarkastella yksityiskohtaisia turvallisuusarviomäärittäjiä, jotka näyttävät sivuston sähköpostikäytäntöjä, ladattavia tiedostoja, verkkoyhteyksiä sekä ponnahdusikkunoiden ja kolmansien osapuolten seurantaevästeiden kaltaisia häiriötekijöitä koskevien testien tulokset.

Avaa Sähköposti ja pikaviesti -asetusikkuna

Jos **Sähköposti ja pikaviesti** -luokassa ei ole ongelmia, voit avata asetusiikkunan tietoikkunasta.

Sähköposti ja pikaviesti -asetusiikkunan avaaminen:

- 1 Valitse Koti-ikkunasta **Sähköposti ja pikaviesti**.
- 2 Valitse oikeasta ikkunasta **Määritä**.

Käytönvalvonta-asetukset-suojauksen toiminta

Käytönvalvonta-asetukset-suojausluokka muodostuu seuraavasta suojaustyyppistä:

- **Käytönvalvonta-asetukset** – Käytönvalvonta-asetukset estävät käyttäjiä katselemasta ei-toivottuja Internet-sisältöjä estämällä mahdollisesti vahingolliset Web-sivustot. Käyttäjien Internet-tapahtumia ja -käyttöä voidaan myös valvoa ja rajoittaa.

Avaa Käytönvalvonta-asetukset-asetusikkuna

Jos **Käytönvalvonta-asetukset**-luokassa ei ole ongelmia, voit avata asetussikkunan tietoikkunasta.

Käytönvalvonta-asetukset-asetusikkunan avaaminen:

- 1 Valitse Koti-ikkunasta **Käytönvalvonta-asetukset**.
- 2 Valitse oikeasta ikkunasta **Määritä**.

Suojausongelmien korjaaminen

Useimmat suojausongelmat voidaan ratkaista automaattisesti. Jos yksi tai useampi ongelma ei kuitenkaan poistu, ne on ratkaistava.

Korjaa suojausongelmat automaattisesti

Useimmat suojausongelmat voidaan ratkaista automaattisesti.

Suojausongelmien korjaaminen automaattisesti:

- Valitse suojauksen tilan vierestä **Korjaa**.

Korjaa suojausongelmat manuaalisesti

Jos yksi tai useampi suojausongelma ei ratkea automaattisesti, napsauta ongelman perässä olevaa linkkiä ja suorita suositeltu toimenpide.

Suojausongelmien korjaaminen manuaalisesti:

- Valitse yksi seuraavista vaihtoehdoista:
 - Jos tietokoneelle ei ole suoritettu täydellistä tarkistusta viimeisen 30 päivän aikana, tarkista tietokone manuaalisesti valitsemalla suojauksen tilan pääikkunan vasemmalta puolelta **Tarkista**. (Tämä valikkovaihtoehto ilmestyy näyttöön, jos McAfee VirusScan on asennettu.)
 - Jos tunnistusallekirjoitustiedostot (DAT) ovat vanhentuneet, päivitä suojauksesi valitsemalla suojauksen tilan pääikkunan vasemmalta puolelta **Päivitä**.
 - Jos ohjelmaa ei ole asennettu, asenna se valitsemalla **Hanki täydellinen suojaus**.
 - Jos ohjelmasta puuttuu osia, asenna se uudelleen.
 - Jos täydellinen suojaus edellyttää ohjelman rekisteröintiä, rekisteröi se valitsemalla **Rekisteröi nyt**. (Tämä valikkokohde ilmestyy näyttöön, jos yksi tai useampi ohjelma on vanhentunut.)
 - Jos ohjelma on vanhentunut, tarkista tilisi tila valitsemalla **Vahvista tilaus nyt**. (Tämä valikkokohde ilmestyy näyttöön, jos yksi tai useampi ohjelma on vanhentunut.)

SecurityCenterin tietojen tarkasteleminen

Suojauksen tila -ikkunan alaosassa olevassa SecurityCenterin tiedot -kohdassa voit määrittää SecurityCenterin asetukset ja tarkastella McAfeen tuotteiden viimeistä päivitystä, viimeistä tarkistusta (jos McAfee VirusScan on asennettu) ja tilauksen päättymiseen liittyviä tietoja.

Avaa SecurityCenter-asetusikkuna

Käytön helpottamiseksi voit muuttaa asetuksiasi Koti-ikkunasta, kun avaat SecurityCenter-asetusikkunan.

SecurityCenter-asetusikkunan avaaminen:

- Valitse Koti-ikkunassa olevasta **SecurityCenterin tiedot** -kohdasta **Määritä**.

Tarkastele asennettujen tuotteiden tietoja

Voit tarkastella asennettujen tuotteiden luetteloa, jossa näkyvät tuoteversiot ja viimeisten päivitysten ajankohdat.

McAfeen tuotteiden tietojen tarkasteleminen

- Avaa tuotetietoikkuna valitsemalla Koti-ikkunassa olevasta **SecurityCenter-tiedot** -kohdasta **Näytä tiedot**.

Lisävalikon käyttäminen

Kun avaat SecurityCenterin ensimmäisen kerran, Perusvalikko avautuu vasemmalla olevaan sarakkeeseen. Jos olet kokenut käyttäjä, voit avata sen sijaan yksityiskohtaisemman komentovalikon valitsemalla **Lisävalikko**-vaihtoehdon. Käytön helpottamiseksi viimeksi käytetty valikko näytetään SecurityCenterissä, kun se avataan seuraavan kerran.

Lisävalikossa on seuraavat kohteet:

- Koti
- Raportit ja lokitiedostot (sisältää äskettäisten tapahtumien luettelon ja lokit viimeisen 30, 60 ja 90 päivän ajalta)
- Määritä
- Palauta
- Työkalut

LUKU 4

SecurityCenterin asetusten määrittäminen

SecurityCenter näyttää tietokoneen yleisen suojauksen tilan, mahdollistaa McAfee-käyttäjätilien luomisen, asentaa automaattisesti uusimmat tuotepäivitykset ja ilmoittaa sinulle julkisista virusesiintymistä, tietoturvauhista ja tuotepäivityksistä automaattisesti hälytyksellä ja merkkiäänellä.

SecurityCenter-asetukset-ikkunassa voit muuttaa seuraavia Security Centerin asetuksia:

- Suojauksen tila
- Käyttäjät
- Automaattiset päivitykset
- Hälytykset

Tässä luvussa

| | |
|---|----|
| Suojauksen tilan asetusten määrittäminen..... | 22 |
| Käyttäjäasetusten määrittäminen..... | 23 |
| Päivitysasetusten määrittäminen..... | 26 |
| Hälytysasetusten määrittäminen | 31 |

Suojauksen tilan asetusten määrittäminen

Tietokoneen yleinen suojauksen tila on ilmoitettu Security Centerin **Olenko suojattu?** -kohdassa.

Suojauksen tila ilmaisee, onko tietokone täysin suojattu uusia tietoturvauhkia vastaan, kuten myös sen, vaativatko ongelmat huomiota ja miten ne voi ratkaista.

Oletusarvoisesti nämä ei-kriittiset suojausongelmat ohitetaan automaattisesti ja niitä ei seurata yleisessä suojauksen tilassa, jos roskapostin torjuntaa ja sisällön estämistä ei ole asennettu. Jos suojausongelman perässä on **Ohita**-linkki, voit halutessasi ohittaa ongelman, jos olet varma, että et halua korjata sitä. Jos päätät myöhemmin korjata aikaisemmin ohitetun ongelman, voit lisätä sen suojauksen tilaan seurantaan varten.

Määritä ohitettujen ongelmien asetukset

Voit ottaa ongelmat huomioon tai jättää ne huomiotta seurattessasi tietokoneen yleistä suojauksen tilaa. Jos suojausongelman perässä on **Ohita**-linkki, voit halutessasi ohittaa ongelman, jos olet varma, että et halua korjata sitä. Jos päätät myöhemmin korjata aikaisemmin ohitetun ongelman, voit lisätä sen suojauksen tilaan seurantaan varten.

Ohitettujen ongelmien asetusten määrittäminen:

- 1 Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Laajenna **Suojauksen tila** -ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
- 3 Toimi Ohitetut ongelmat -ikkunassa seuraavasti:
 - Jos haluat ottaa aikaisemmin ohitetut ongelmat suojauksen tilassa huomioon, poista niiden valintaruutujen valinnat.
 - Jos haluat jättää aikaisemmin ohitetut ongelmat suojauksen tilassa huomiotta, valitse niiden valintaruudut.
- 4 Valitse **OK**.

Käyttäjäasetusten määrittäminen

Jos käytät McAfeen ohjelmia, jotka vaativat tiettyjä käyttöoikeuksia, kyseiset käyttöoikeudet vastaavat oletusasetuksena tietokoneen Windows-käyttäjätilien käyttöoikeuksia. Voit yksinkertaistaa näiden ohjelmien käyttäjien hallintaa siirtymällä milloin tahansa käyttämään McAfee-käyttäjätilejä.

Jos siirryt käyttämään McAfee-käyttäjätilejä, Käytönvalvonta-asetukset-ohjelmassa olevat käyttäjänimet ja käyttöoikeudet tuodaan automaattisesti. Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinun on kuitenkin luotava järjestelmänvalvojan tili. Sen jälkeen voit luoda uusia McAfee-käyttäjätilejä ja määrittää niiden asetukset.

Siirry McAfee-käyttäjätileihin

Oletusarvoisesti käytät Windows-käyttäjätilejä. Voit kuitenkin siirtyä käyttämään McAfee-käyttäjätilejä, jolloin uusia Windows-käyttäjätilejä ei enää tarvitse luoda.

Siirtyminen McAfee-käyttäjätileihin:

- 1 Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Laajenna **Käyttäjät**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
- 3 Jos haluat käyttää McAfee-käyttäjätilejä, valitse **Vaihda**.

Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinun on luotava järjestelmänvalvojan tili (sivu 23).

Luo järjestelmänvalvojan tili

Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinua kehoitetaan luomaan järjestelmänvalvojan tili.

Järjestelmänvalvojan tilin luominen:

- 1 Kirjoita salasana **Salasana**-tekstiruutuun ja kirjoita se uudelleen **Vahvista salasana** -tekstiruutuun.
- 2 Valitse salasanan palautuskysymys luettelosta ja kirjoita salaisen kysymyksen vastaus **Vastaus**-tekstiruutuun.
- 3 Valitse **Käytä**.

Kun olet valmis, käyttäjätilin tyyppi päivitetään ikkunassa lisäämällä siihen mahdolliset

Käytönvalvonta-asetukset-ohjelman käyttäjänimet ja käyttöoikeudet. Jos olet määrittämässä käyttäjätilien asetuksia ensimmäisen kerran, näyttöön ilmestyy Hallitse käyttäjiä -ikkuna.

Määritä käyttäjäasetukset

Jos siirryt käyttämään McAfee-käyttäjätilejä, Käytönvalvonta-asetukset -ohjelmassa olevat käyttäjänimet ja käyttöoikeudet tuodaan automaattisesti. Kun siirryt käyttämään McAfee-käyttäjätilejä ensimmäisen kerran, sinun on kuitenkin luotava järjestelmänvalvojan tili. Sen jälkeen voit luoda uusia McAfee-käyttäjätilejä ja määrittää niiden asetukset.

Käyttäjäasetusten määrittäminen

- 1 Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Laajenna **Käyttäjät**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
- 3 Valitse **Käyttäjätilit**-kohdasta **Lisää**.
- 4 Kirjoita käyttäjänimi **Käyttäjänimi**-tekstiruutuun.
- 5 Kirjoita salasana **Salasana**-tekstiruutuun ja kirjoita se uudelleen **Vahvista salasana** -tekstiruutuun.
- 6 Valitse **Aloituskäyttäjä**-valintaruutu, jos haluat uuden käyttäjän kirjautuvan automaattisesti sisään, kun SecurityCenter käynnistyy.
- 7 Valitse **Käyttäjätilin tyyppi** -kohdasta kyseiselle käyttäjälle tilin tyyppi ja valitse **Luo**.


Huomaa: Kun olet luonut käyttäjätilin, sinun on määritettävä sille Käytönvalvonta-asetukset-kohdasta rajoitetun käyttäjän asetukset.

- 8 Jos haluat muokata käyttäjän salasanaa, automaattista sisäänkirjausta tai tilin tyyppiä, valitse luettelosta käyttäjän nimi ja sitten **Muokkaa**.
- 9 Kun olet valmis, valitse **Käytä**.

Palauta järjestelmänvalvojan salasana

Jos unohdat järjestelmänvalvojan salasanan, voit palauttaa sen.

Järjestelmänvalvojan salasanan palauttaminen:

- 1 Napsauta SecurityCenter M -kuvaketta  hiiren kakkospainikkella ja valitse **Vaihda käyttäjää**.
- 2 Valitse **Käyttäjänimi**-luettelosta **Järjestelmänvalvoja** ja sitten **Unohditko salasanasasi?**
- 3 Anna vastaus salaiseen kysymykseen, jonka valitsit järjestelmänvalvojan salasanan luomisen yhteydessä.
- 4 Valitse **Lähetä**.

Unohdettu järjestelmänvalvojan salasanasasi ilmestyy näyttöön.

Muuta järjestelmänvalvojan salasanaa

Jos sinun on vaikeata muistaa järjestelmänvalvojan salasanaa tai epäilet sen joutuneen väärin käsiin, voit muuttaa sen.

Järjestelmänvalvojan salasanan muuttaminen:

- 1 Napsauta SecurityCenter M -kuvaketta  hiiren kakkospainikkeella ja valitse **Vaihda käyttäjää**.
- 2 Valitse **Käyttäjänimi**-luettelosta **Järjestelmänvalvoja** ja sitten **Vaihda salasana**.
- 3 Kirjoita nykyinen salasanasi **Vanha salasana** -tekstiruutuun.
- 4 Kirjoita uusi salasanasi **Salasana**-tekstiruutuun ja kirjoita se uudelleen **Vahvista salasana** -tekstiruutuun.
- 5 Valitse **OK**.

Päivitysasetusten määrittäminen

Kun olet muodostanut yhteyden Internetiin, SecurityCenter hakee päivityksiä automaattisesti kaikille McAfee-palveluille neljän tunnin välein ja asentaa uudet tuotepäivitykset automaattisesti. Voit kuitenkin hakea päivityksiä myös manuaalisesti napsauttamalla SecurityCenter-kuvaketta, joka sijaitsee tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella.

Hae päivityksiä automaattisesti

Kun olet muodostanut yhteyden Internetiin, SecurityCenter hakee päivityksiä automaattisesti neljän tunnin välein. Voit kuitenkin määrittää SecurityCenterin antamaan ilmoituksen ennen päivitysten lataamista tai asentamista.

Päivitysten automaattinen hakeminen:

- 1 Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Laajenna **Automaattiset päivitykset ovat käytössä** -ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
- 3 Valitse Päivitysvalinnat-ikkunasta yksi seuraavista:
 - Asenna päivitykset automaattisesti ja ilmoita, kun tuote päivitetään (suositus) (sivu 27)
 - Lataa päivitykset automaattisesti ja ilmoita, kun ne ovat valmiina asennettaviksi (sivu 28)
 - Ilmoita ennen päivitysten lataamista (sivu 28)
- 4 Valitse **OK**.

Huomaa: Parhaan mahdollisen suojan takaamiseksi McAfee suosittelee, että annat SecurityCenterin hakea ja asentaa päivitykset automaattisesti. Jos haluat kuitenkin päivittää tietoturvapalvelut vain manuaalisesti, voit poistaa automaattiset päivitykset käytöstä (sivu 29).

Lataa ja päivitä päivitykset automaattisesti

Jos valitset SecurityCenterin Päivitysvalinnat-kohdasta **Asenna päivitykset automaattisesti ja ilmoita, kun palvelut päivitetään (suositus)**, SecurityCenter lataa ja asentaa päivitykset automaattisesti.

Lataa päivitykset automaattisesti

Jos valitset SecurityCenterin Päivitysvalinnat-kohdasta **Lataa päivitykset automaattisesti ja ilmoita, kun ne ovat valmiina asennettaviksi**, SecurityCenter lataa päivitykset automaattisesti ja ilmoittaa sinulle, kun ne ovat valmiina asennettaviksi. Voit tällöin halutessasi asentaa päivityksen tai siirtää päivitystä (sivu 29).

Automaattisesti ladatun päivityksen asentaminen:

- 1 Valitse hälytyksen saatuasi **Päivitä tuotteet nyt** ja sitten **OK**.

Kehotettaessa sinun on kirjaututtava Web-sivustoon ja vahvistettava tilauksesi ennen latauksen aloittamista.

- 2 Kun tilauksesi on vahvistettu, lataa ja asenna päivitys valitsemalla Päivitykset-ikkunasta **Päivitä**. Jos tilauksesi on umpeutunut, valitse hälytyksen saatuasi **Uudista tilaukseni** ja toimi kehoitteiden mukaan.

Huomaa: Joissakin tapauksissa sinua kehoitetaan viimeistelemään päivitys käynnistämällä tietokone uudelleen. Tallenna työt ja sulje kaikki ohjelmat ennen uudelleenkäynnistystä.

Ilmoita ennen päivitysten lataamista

Jos valitset Päivitysvalinnat-ikkunasta **Ilmoita ennen päivitysten lataamista**, SecurityCenter ilmoittaa sinulle ennen päivitysten lataamista. Voit tällöin halutessasi ladata ja asentaa tietoturvapalveluiden päivityksen hyökkäysuhan välttämiseksi.

Päivityksen lataaminen ja asentaminen:

- 1 Valitse hälytyksen saatuasi **Päivitä tuotteet nyt** ja sitten **OK**.

- 2 Kirjaudu kehotettaessa Web-sivustoon.

Päivitys latautuu automaattisesti.

- 3 Valitse hälytyksen saatuasi **OK**, kun päivitys on asennettu.

Huomaa: Joissakin tapauksissa sinua kehoitetaan viimeistelemään päivitys käynnistämällä tietokone uudelleen. Tallenna työt ja sulje kaikki ohjelmat ennen uudelleenkäynnistystä.

Poista automaattiset päivitykset käytöstä

Parhaan mahdollisen suojan takaamiseksi McAfee suosittelee, että annat SecurityCenterin hakea ja asentaa päivitykset automaattisesti. Jos haluat kuitenkin päivittää tietoturvapalvelut vain manuaalisesti, voit poistaa automaattiset päivitykset käytöstä.

Huomaa: Muista hakea päivitykset manuaalisesti (sivu 30) ainakin kerran viikossa. Jos et hae päivityksiä, uusimmat tietoturvapäivitykset eivät suojaa tietokonettasi.

Automaattisten päivitysten poistaminen käytöstä:

- 1 Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Laajenna **Automaattiset päivitykset ovat käytössä** -ikkuna napsauttamalla sen vieressä olevaa nuolta.
- 3 Valitse **Ei käytössä**.
- 4 Vahvista muutos valitsemalla **Kyllä**.

Tila päivitetään otsikkoon.

Jos et hae päivityksiä manuaalisesti seitsemään päivään, saat tästä muistuttavan hälytyksen.

Siirrä päivitykset

Jos olet liian kiireinen etkä ehdi päivittää tietoturvapalveluita juuri silloin, kun saat hälytyksen, voit pyytää myöhempää muistutusta tai ohittaa hälytyksen.

Päivityksen siirtäminen:


- Toimi seuraavasti:
 - Valitse hälytyksen saatuasi **Muistuta myöhemmin** ja sitten **OK**.
 - Valitse **Sulje tämä hälytys** ja sulje hälytys ryhtymättä toimenpiteisiin valitsemalla **OK**.

Hae päivityksiä manuaalisesti

Kun olet muodostanut yhteyden Internetiin, SecurityCenter hakee päivityksiä automaattisesti neljän tunnin välein ja asentaa uudet tuotepäivitykset. Voit kuitenkin hakea päivityksiä myös manuaalisesti napsauttamalla SecurityCenter-kuvaketta, joka sijaitsee tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella.

Huomaa: Parhaan mahdollisen suojan takaamiseksi McAfee suosittelee, että annat SecurityCenterin hakea ja asentaa päivitykset automaattisesti. Jos haluat kuitenkin päivittää tietoturvapalvelut vain manuaalisesti, voit poistaa automaattiset päivitykset käytöstä (sivu 29).

Päivitysten manuaalinen hakeminen:

- 1 Varmista, että tietokoneesi on muodostanut yhteyden Internetiin.
- 2 Napsauta SecurityCenter M -kuvaketta  hiiren kakkospainikkeella tehtäväpalkin oikeassa reunassa olevalla Windowsin ilmaisinalueella ja napsauta sitten **Päivitykset**-kohtaa.

Sillä välin kun SecurityCenter tarkistaa päivityksiä, voit suorittaa sillä muita tehtäviä.

Käytön helpottamiseksi tuotteen kuvake ilmestyy tehtäväpalkin oikeassa reunassa olevalle Windowsin ilmaisinalueelle. Kun SecurityCenter on valmis, kuvake katoaa automaattisesti.

- 3 Kirjaudu kehotettaessa Web-sivustoon ja vahvista tilauksesi.

Huomaa: Joissakin tapauksissa sinua kehoitetaan viimeistelemään päivitys käynnistämällä tietokone uudelleen. Tallenna työt ja sulje kaikki ohjelmat ennen uudelleenkäynnistystä.

Hälytysasetusten määrittäminen

SecurityCenter ilmoittaa julkisista virusesiintymistä, tietoturvahkista ja tuotepäivityksistä automaattisesti hälytyksellä ja merkkiäänellä. Voit kuitenkin määrittää SecurityCenterin näyttämään vain välitöntä huomiota vaativat hälytykset.

Määritä hälytysasetukset

SecurityCenter ilmoittaa julkisista virusesiintymistä, tietoturvahkista ja tuotepäivityksistä automaattisesti hälytyksellä ja merkkiäänellä. Voit kuitenkin määrittää SecurityCenterin näyttämään vain välitöntä huomiota vaativat hälytykset.

Hälytysasetusten määrittäminen:

- 1 Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Laajenna **Hälytykset**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
- 3 Valitse Hälytysasetukset-ikkunasta yksi seuraavista:
 - **Hälytä julkisista virusesiintymistä tai tietoturvahkista**
 - **Näytä tiedottavat hälytykset, kun tietokoneen havaitaan olevan pelitilassa**
 - **Soita ääni hälytyksen esiintyessä**
 - **Näytä McAfee-aloitusnäyttö Windowsin käynnistyessä**
- 4 Valitse **OK**.

Huomaa: Jos haluat poistaa tulevat tiedottavat hälytykset käytöstä itse hälytyksestä, valitse **Älä näytä tätä hälytystä uudelleen** -valintaruutu. Voit ottaa ne myöhemmin uudelleen käyttöön Tiedottavat hälytykset -ikkunassa.

Määritä tiedottavien hälytysten asetukset

Tiedottavat hälytykset ilmoittavat tapahtumista, jotka eivät vaadi välitöntä huomiota. Jos poistat tulevat tiedottavat hälytykset käytöstä itse hälytyksestä, voit ottaa ne Tiedottavat hälytykset -ikkunassa uudelleen käyttöön.

Tiedottavien hälytysten asetusten määrittäminen:

- 1 Valitse **SecurityCenterin tiedot** -kohdasta **Määritä**.
- 2 Laajenna **Hälytykset**-ikkuna napsauttamalla sen vieressä olevaa nuolta ja valitse **Lisäasetukset**.
- 3 Valitse **SecurityCenter-asetukset**-ikkunasta **Tiedottavat hälytykset**.
- 4 Poista **Pilota tiedottavat hälytykset** -kohdan valinta ja poista sitten luettelosta niiden hälytysten valintaruutujen valinnat, jotka haluat näyttää.
- 5 Valitse **OK**.

LUKU 5

Yleisten tehtävien suorittaminen

Voit suorittaa yleisiä tehtäviä: palata Koti-ikkunaan, tarkastella äskettäisiä tapahtumia, hallita tietokoneverkkoa (jos käytät verkon hallintaan kykenevää tietokonetta) ja ylläpitää tietokonetta. Jos McAfee Data Backup on asennettu, voit myös varmuuskopioida tietosi.

Tässä luvussa

| | |
|--|----|
| Suorita yleisiä tehtäviä..... | 33 |
| Tarkastele äskettäisiä tapahtumia | 34 |
| Ylläpidä tietokonetta automaattisesti..... | 35 |
| Ylläpidä tietokonetta manuaalisesti | 36 |
| Hallitse verkkoa..... | 38 |
| Hanki lisätietoja viruksista | 38 |

Suorita yleisiä tehtäviä

Voit suorittaa yleisiä tehtäviä: palata Koti-ikkunaan, tarkastella äskettäisiä tapahtumia, ylläpitää tietokonetta, hallita tietokoneverkkoa (jos käytät verkon hallintaan kykenevää tietokonetta) ja varmuuskopioida tietosi (jos McAfee Data Backup on asennettu).

Yleisten tehtävien suorittaminen:

- Toimi Perusvalikon **Yleiset tehtävät** -kohdassa seuraavasti:
 - Jos haluat palata Koti-ikkunaan, valitse **Koti**.
 - Jos haluat tarkastella tietoturvaohjelmiston äskettäin havaitsemia tapahtumia, valitse **Äskettäiset tapahtumat**.
 - Jos haluat poistaa käyttämättömiä tiedostoja, eheyttää tietoja ja palauttaa tietokoneen aikaisemmat asetukset, valitse **Ylläpidä tietokonetta**.
 - Jos haluat hallita tietokoneverkkoa, valitse **Verkonhallinta**, jos käytät verkon hallintaan kykenevää tietokonetta.
 Network Manager tarkkailee verkkosi tietokoneita mahdollisten tietoturva-aukkojen varalta, ja sen avulla voit tunnistaa verkon tietoturvaongelmat helposti.
 - Jos haluat luoda tiedostoistaisi varmuuskopioita, valitse **Data Backup**, jos McAfee Data Backup on asennettu.

Automaattinen varmuuskopointitoiminto tallentaa salatut kopiot tärkeimmistä tiedostoistasi CD- ja DVD-levyille, USB-asetuille sekä ulkoisille kiintolevyasetuille ja verkkoasetuille.

Vihje: Käytön helpottamiseksi voit suorittaa yleisiä tehtäviä myös kahdesta muusta paikasta (Lisävalikon **Koti**-kohdasta ja tehtäväpalkin oikeassa reunassa olevan SecurityCenter M -kuvakkeen **Pikalinkit**-valikosta). Voit myös tarkastella äskettäisiä tapahtumia ja yksityiskohtaisia lokeja tyypeittäin Lisävalikon **Raportit ja lokit** -kohdassa.

Tarkastele äskettäisiä tapahtumia

Äskettäiset tapahtumat kirjataan, kun tietokoneessa tapahtuu muutoksia. Esimerkkejä tästä ovat suojaustyyppin ottaminen käyttöön tai poistaminen käytöstä, uhan poistaminen tai Internet-yhteysyrityksen estäminen. Voit tarkastella 20:tä viimeisintä tapahtumaa ja niiden tietoja.

Lisätietoja tapahtumista on kunkin tuotteen ohjetiedostossa.

Äskettäisten tapahtumien tarkasteleminen:

- 1 Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Tarkastele äskettäisiä tapahtumia**.
Äskettäiset tapahtumat ilmestyvät luetteloon yhdessä päiväyksen ja lyhyen kuvauksen kanssa.
- 2 Valitse **Äskettäiset tapahtumat** -kohdasta tapahtuma, jota haluat tarkastella tarkemmin Lisätiedot-ikkunassa.
Mahdolliset toimenpiteet ilmestyvät **Haluan**-kohtaan.
- 3 Jos haluat tarkastella tapahtumien yksityiskohtaisempaa luetteloa, valitse **Tarkastele lokia**.

Ylläpidä tietokonetta automaattisesti

Voit vapauttaa arvokasta kiintolevytilaa ja optimoida tietokoneen suorituskyvyn ajoittamalla tietokoneen suorittamaan QuickClean- ja levyn eheytystehtävät säännöllisin väliajoin. Näiden tehtävien avulla voit poistaa, tuhota ja eheyttää tiedostoja ja kansioita.

Tietokoneen automaattinen ylläpito:

- 1 Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Ylläpidä tietokonetta**.
- 2 Valitse **Tehtävien ajoitus** -kohdasta **Käynnistä**.
- 3 Valitse toimintojen luettelosta **QuickClean** tai **Levyn eheyty**.
- 4 Toimi seuraavasti:
 - Jos haluat muuttaa olemassa olevaa tehtävää, valitse se ja sitten **Muokkaa**. Toimi näytön ohjeiden mukaan.
 - Jos haluat luoda uuden tehtävän, kirjoita sen nimi **Tehtävän nimi** -tekstiruutuun ja valitse **Luo**. Toimi näytön ohjeiden mukaan.
 - Jos haluat poistaa tehtävän, valitse se ja sitten **Poista**.
- 5 **Tehtävän yhteenveto** -kohdassa voit tarkastella, koska tehtävä on suoritettu viimeksi, koska se suoritetaan seuraavan kerran ja mikä sen tila on.

Ylläpidä tietokonetta manuaalisesti

Manuaalisia ylläpitotehtäviä suorittamalla voit poistaa käyttämättömiä tiedostoja, eheyttää tietoja tai palauttaa tietokoneen aikaisemmat asetukset.

Tietokoneen manuaalinen ylläpito:

- Toimi seuraavasti:
 - Jos haluat käyttää QuickClean-toimintoa, napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit**, sitten **Ylläpidä tietokonetta** ja lopuksi **Käynnistä**.
 - Jos haluat käyttää levyn eheytysoimintoa, napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit**, sitten **Ylläpidä tietokonetta** ja lopuksi **Analysoi**.
 - Jos haluat käyttää järjestelmän palautustoimintoa, valitse Lisävalikosta **Työkalut**, sitten **Järjestelmän palautus** ja lopuksi **Käynnistä**.

Poista käyttämättömiä tiedostoja ja kansioita

QuickClean-toiminnolla voit vapauttaa arvokasta kiintolevytilaa ja optimoida tietokoneen suorituskyvyn.

Käyttämättömien tiedostojen ja kansioden poistaminen:

- 1 Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Ylläpidä tietokonetta**.
- 2 Valitse **QuickClean**-kohdasta **Käynnistä**.
- 3 Toimi näytön ohjeiden mukaan.

Eheyttä tiedostoja ja kansioita

Tiedostot pirstoutuvat, kun tiedostoja ja kansioita poistetaan ja uusia tiedostoja lisätään. Pirstoutuminen hidastaa levyn käyttöä ja heikentää tietokoneen yleistä suorituskykyä, vaikka yleensä ei kovinkaan merkittävästi.

Levyn eheytyä käyttämällä voit kirjoittaa tiedoston uudelleen kiintolevyn peräkkäisille sektoreille ja siten nopeuttaa käyttöä ja hakua.

Tiedostojen ja kansioiden eheyttäminen:

- 1 Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Ylläpidä tietokonetta**.
- 2 Valitse **Levyn eheyty** -kohdasta **Analysoi**.
- 3 Toimi näytön ohjeiden mukaan.

Palauta tietokoneen aikaisemmat asetukset

Palautuspisteet ovat tilannevedoksia tietokoneesta, jotka Windows tallentaa säännöllisin väliajoin ja aina merkittävien tapahtumien yhteydessä (esimerkiksi kun ohjelma tai ohjain asennetaan). Voit kuitenkin luoda myös omia palautuspisteitä ja nimetä ne milloin tahansa.

Palautuspisteiden avulla voit kumota tietokoneelle vahinkoa aiheuttaneet muutokset ja palauttaa aikaisemmat asetukset.

Tietokoneen aikaisempien asetusten palauttaminen:

- 1 Valitse Lisävalikosta **Työkalut** ja sitten **Järjestelmän palautus**.
- 2 Valitse **Järjestelmän palautus** -kohdasta **Käynnistä**.
- 3 Toimi näytön ohjeiden mukaan.

Hallitse verkkoa

Jos tietokoneesi kykenee verkon hallintaan, Network Managerin avulla voit tarkkailla verkkosi tietokoneita mahdollisten tietoturva-aukkojen varalta, ja sen avulla voit tunnistaa verkon tietoturvaongelmat helposti.

Jos tietokoneen suojauksen tilaa ei valvota tässä verkossa, tietokone ei kuulu verkkoon tai se on verkon laite, joka ei kuulu hallinnan piiriin. Lisätietoja on Network Managerin ohjetiedostossa.

Verkon hallinta:

- 1 Napsauta SecurityCenter-kuvaketta hiiren kakkospainikkeella, valitse **Pikalinkit** ja sitten **Verkonhallinta**.
- 2 Napsauta verkkokartassa tätä tietokonetta esittävää kuvaketta.
- 3 Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.

Hanki lisätietoja viruksista

Virustietokanta ja viruskartta tarjoavat useita mahdollisuuksia:

- Lisätietoja viimeisimmistä viruksista, sähköpostivirushuijauksista ja muista tietoturvauhkista.
- Hanki ilmaisia virusten poistotyökaluja, joiden avulla voit korjata tietokoneesi.
- Saat reaaliaikaisia karttanäkymiä siitä, miten viimeisimmät virukset leviävät tietokoneissa maailman ympäri.

Lisätietojen hankkiminen viruksista:

- 1 Valitse Lisävalikosta **Työkalut** ja sitten **Virustietoja**.
- 2 Toimi seuraavasti:
 - Tutki viruksia maksuttoman McAfee-virustietokannan avulla.
 - Tutki viruksia McAfeen Web-sivustossa olevan maailman viruskartan avulla.

L U K U 6

McAfee QuickClean

Kun surffaat Internetissä, tietokoneeseen kertyy nopeasti ylimääräistä roskamateriaalia. Turvaa tietosuojasi ja poista Internetin sekä sähköpostin kautta tuleva tarpeeton materiaali QuickClean-pikapuhdistusohjelman avulla. QuickClean tunnistaa ja poistaa tiedostoja, joita kerääntyy surffatessa, esimerkiksi evästeitä, sähköposteja, latauksia ja henkilötietoja sisältäviä historiatietoja. Ohjelma parantaa tietosuojaasi tarjoamalla turvallisen tavan poistaa näitä tietoja.

QuickClean poistaa myös ei-toivottuja ohjelmia. Määritä poistettavat tiedostot, niin voit poistaa turhan materiaalin ja säilyttää tarpeelliset tiedot.

Tässä luvussa

| | |
|------------------------------------|----|
| QuickClean-ohjelman toiminnot..... | 40 |
| Tietokoneen puhdistaminen..... | 41 |

QuickClean-ohjelman toiminnot

Tässä osassa kuvaillaan QuickClean-ohjelman toimintoja.

Ominaisuudet

QuickClean-ohjelma on tehokas ja helppokäyttöinen työkalu, joka poistaa turvallisesti digitaalisen roskamateriaalin. Voit vapauttaa arvokasta levytilaa ja saat käyttöön tietokoneen parhaan mahdollisen suorituskyvyn.

LUKU 7

Tietokoneen puhdistaminen

QuickClean-ohjelman avulla voit turvallisesti poistaa tiedostoja ja kansioita.

Kun selaat Internetiä, selain kopioi jokaisen Internet-sivun ja sen kuvat kiintolevyllä olevaan välimuistiin. Tämän jälkeen selain voi ladata sivun nopeasti, jos palaat siihen. Tiedostojen tallentaminen välimuistiin on käytännöllistä, jos käyt usein samoilla Internet-sivuilla, eikä niiden sisältö muutu usein. Useimmiten välimuistiin tallennetut tiedostot eivät kuitenkaan ole hyödyllisiä, ja ne voi poistaa.

Voit poistaa useita eri kohteita seuraavilla puhdistusohjelmilla.

- Roskakorin tyhjennysohjelma: Tyhjentää Windows-roskakorin.
- Väliaikaisten tiedostojen poisto-ohjelma: Poistaa väliaikaisten tiedostojen kansioihin tallennetut tiedostot.
- Pikakuvakkeiden puhdistusohjelma: Poistaa rikkinäiset pikakuvakkeet ja pikakuvakkeet, joihin ei liity mitään ohjelmaa.
- Hävinneiden tiedostopirstaleiden puhdistusohjelma: Poistaa kadonneet tiedostopirstaleet tietokoneesta.
- Rekisterin puhdistusohjelma: Poistaa Windows-rekisteritiedot ohjelmista, jotka on poistettu tietokoneesta.
- Välimuistin tyhjennysohjelma: Poistaa välimuistiin tallennetut tiedostot, joita kertyy Internetiä selatessa. Tämäntyyppiset tiedostot tallentuvat tavallisesti väliaikaisina Internet-tiedostoina.
- Evästeiden poisto-ohjelma: Poistaa evästeet. Tämäntyyppiset tiedostot tallentuvat tavallisesti väliaikaisina Internet-tiedostoina. Evästeet ovat pieniä tiedostoja, joita Web-selain tallentaa tietokoneeseen Web-palvelimen pyynnöstä. Aina kun avaat Web-sivun Web-palvelimelta, selaimesi lähettää evästeen takaisin palvelimeen. Nämä evästeet voivat toimia tunnisteinä, joiden avulla Web-palvelin voi jäljittää avaamasi sivut sekä sen, kuinka usein käyt niillä.
- Selainhistorian tyhjennysohjelma: Poistaa selaimen historiatiedot.
- Outlook Express- ja Outlook-ohjelmien poistettujen ja lähetettyjen sähköpostien poisto-ohjelma: Poistaa sähköpostit lähetettyjen ja poistettujen sähköpostien kansioista Outlook-ohjelmissa.

- Viimeksi käytettyjen kohteiden poisto-ohjelma: Poistaa tietokoneeseen tallentuneet viimeksi käytetyt kohteet, kuten Microsoft Office -asiakirjat.
- ActiveX- ja Plug-in-laajennusten poisto-ohjelma: Poistaa ActiveX- ja Plug-in-laajennukset.
ActiveX on teknologia, jota käytetään ohjelman komponenttien suorittamiseen. ActiveX-komponentti voi lisätä painikkeen ohjelman käyttöliittymään. Useimmat komponentit ovat harmittomia, mutta jotkut henkilöt voivat hyödyntää ActiveX-tekniikkaa tietojen kaappaamiseen tietokoneesta.
Plug-in-laajennukset ovat pieniä ohjelmia, jotka kytkeytyvät suurempiin sovelluksiin ja lisäävät niihin toimintoja. Plug-in-laajennukset antavat Web-selaimen käyttää ja suorittaa HTML-asiakirjoihin upotettuja tiedostoja, jotka ovat selaimen tunnistamattomassa muodossa (esimerkiksi animaatio-, video- ja äänitiedostot).
- Järjestelmän palautuspisteiden poisto-ohjelma: Poistaa vanhat järjestelmän palautuspisteet tietokoneesta.

Tässä luvussa

QuickClean-ohjelman käyttäminen.....43

QuickClean-ohjelman käyttäminen

Tässä osassa kerrotaan, kuinka QuickClean-pikapuhdistusohjelmaa käytetään.

Tietokoneen puhdistaminen

Voit poistaa käyttämättömät tiedostot ja kansiot, vapauttaa levytilaa ja tehostaa tietokoneen toimintaa.

Tietokoneen puhdistaminen:

- 1 Valitse Lisävalikosta **Työkalut**.
- 2 Valitse **Ylläpidä tietokonetta** ja valitse sitten **McAfee QuickClean - Käynnistä**.
- 3 Tee toinen seuraavista:
 - Hyväksy luettelon oletuspuhdistusohjelmat valitsemalla **Seuraava**.
 - Valitse tai poista haluamasi puhdistusohjelmat ja valitse sitten **Seuraava**. Valitsemalla Viimeksi käytettyjen kohteiden poisto-ohjelma -kohdasta **Asetukset** voit poistaa käytöstä haluamasi puhdistusohjelmat.
 - Palauta oletuspuhdistusohjelmat valitsemalla **Palauta oletusasetukset** ja valitse sitten **Seuraava**.
- 4 Kun analyysi on suoritettu, vahvista tiedostojen poistaminen valitsemalla **Seuraava**. Voit laajentaa luetteloa, jotta näet puhdistettavat tiedostot ja niiden sijainnin.
- 5 Valitse **Seuraava**.
- 6 Tee jokin seuraavista:
 - Hyväksy oletusasetus **Ei, haluan poistaa tiedostot perinteisellä Windowsin poistomenetelmällä** valitsemalla **Seuraava**.
 - Valitse **Kyllä, haluan poistaa tiedostot turvallisesti käyttämällä Shredder-ohjelmaa** ja määritä tyhjennyskerrat. Shredder-ohjelmalla poistettuja tiedostoja ei voi palauttaa.
- 7 Valitse **Valmis**.
- 8 Tarkasta **Pikatyhjennyksen yhteenveto** -näytöstä poistettujen rekisteritiedostojen määrä ja puhdistuksen vapauttama levytila.

LUKU 8

McAfee Shredder

Poistetut tiedostot voi palauttaa tietokoneeseen vielä roskakorin tyhjentämisen jälkeenkin. Kun poistat tiedoston, Windows merkitsee tilan levyasemaan vapaaksi levytilaksi, mutta tiedosto on yhä asemassa. Tietokoneen jäljitystyökalujen avulla voit palauttaa verotiedot, työhakemuksen ansioluettelot ja muut poistamasi asiakirjat. Shredder-ohjelma parantaa tietosuojaaasi poistamalla ei-toivotut tiedostot turvallisesti ja pysyvästi.

Jos haluat poistaa tiedoston pysyvästi, aiempi tiedosto on korvattava uusilla tiedoilla. Microsoft® Windows ei poista tiedostoja turvallisesti, sillä kaikki tiedostotoiminnot ovat erittäin hitaita. Asiakirjan hävittäminen ei aina takaa, ettei tiedostoa voisi palauttaa, sillä jotkut ohjelmat tekevät avoimista asiakirjoista väliaikaisia piilokopioita. Jos hävität vain asiakirjat, jotka näkyvät Windowsin® Resurssienhallinnassa, asiakirjoista voi yhä olla väliaikaisia kopioita.

Huomaa: Shredder-ohjelmalla poistettuja tiedostoja ei varmuuskopioida. Et voi enää palauttaa tiedostoja, jotka on poistettu Shredder-ohjelmalla.

Tässä luvussa

| | |
|--|----|
| Shredder-ohjelman toiminnot | 46 |
| Ei-toivottujen tiedostojen poistaminen | |
| Shredder-ohjelmalla | 47 |

Shredder-ohjelman toiminnot

Tässä osassa kuvaillaan Shredder-ohjelman toimintoja.

Ominaisuudet

Shredder-ohjelmalla voit poistaa roskakorin sisällön, väliaikaiset Internet-tiedostot, Web-sivuhistorian, tiedostoja ja kansioita sekä tyhjentää levyasemia.

LUKU 9

Ei-toivottujen tiedostojen poistaminen Shredder-ohjelmalla

Shredder-ohjelma parantaa tietosuojasi poistamalla turvallisesti ja pysyvästi ei-toivotut tiedostot, kuten roskakorin sisällön, väliaikaiset Internet-tiedostot ja Web-sivuhistorian. Voit valita tiedostoja ja kansioita poistettavaksi tai selata niitä.

Tässä luvussa

Shredder-ohjelman käyttäminen.....48

Shredder-ohjelman käyttäminen

Tässä osassa kerrotaan, kuinka Shredder-ohjelmaa käytetään.

Tiedostojen ja kansioiden poistaminen sekä levyasemien tyhjentäminen

Tiedostot voivat yhä sijaita tietokoneessa, vaikka tyhjennät roskakorin. Shredder-ohjelma kuitenkin poistaa tiedot pysyvästi, eivätkä hakkerit pääse niihin käsiksi.

Tiedostojen ja kansioiden poistaminen ja levyasemien tyhjentäminen:

- 1 Valitse Lisävalikosta **Työkalut - Shredder**.
- 2 Tee jokin seuraavista:
 - Poista tiedostoja ja kansioita valitsemalla **Poistaa tiedostoja ja kansioita**.
 - Poista levyasemia valitsemalla **Tyhjentää koko levyn**.
- 3 Valitse jokin seuraavista poistamistasoista:
 - **Nopea:** Poistaa valitut kohteet kerran.
 - **Perusteellinen:** Poistaa valitut kohteet 7 kertaa.
 - **Mukautettu:** Poistaa valitut kohteet 10 kertaa. Mitä suurempi poistomäärä, sitä parempi tiedostojen poiston tietosuoja on.
- 4 Valitse **Seuraava**.
- 5 Tee jokin seuraavista:
 - Jos olet poistamassa tiedostoja, valitse **Valitse tuhottava(t) tiedosto(t)** -luettelosta **Roskakorin sisältö, Väliaikaiset Internet-tiedostot** tai **Web-sivustohistoria**. Jos olet tyhjentämässä levyasemaa, napsauta asemaa.
 - Valitse **Selaa**, siirry poistettavien tiedostojen kohdalle ja valitse ne.
 - Kirjoita poistettavien tiedostojen polku **Valitse tuhottava(t) tiedosto(t)** -luetteloon.
- 6 Valitse **Seuraava**.
- 7 Suorita toiminto loppuun valitsemalla **Valmis**.
- 8 Valitse **Valmis**.

LUKU 10

McAfee Network Manager

McAfee® Network Manager esittää graafisen näkymän kotiverkon tietokoneista ja osista. Network Managerin avulla voit valvoa kunkin verkkosi hallitun tietokoneen suojauksen tilaa ja korjata raportoituja tietoturvan puutteita.

Voit tutustua Networkin Managerin suosituimpiin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on Network Managerin ohjeessa.

Tässä luvussa

| | |
|--|----|
| Ominaisuudet..... | 50 |
| Network Managerin kuvakkeiden toiminta | 51 |
| Hallitun verkon määrittäminen | 53 |
| Verkon etähallinta..... | 61 |

Ominaisuudet

Network Manager tarjoaa seuraavat ominaisuudet:

Graafinen verkkokartta









Network Managerin verkkokartta tarjoaa graafisen näkymän muiden tietokoneiden ja kotiverkon osien suojaustilasta. Kun teet muutoksia verkkoosi (esimerkiksi lisäät siihen tietokoneen), verkkokartta tunnistaa muutokset. Voit päivittää verkkokarttaa, nimetä sen uudelleen ja mukauttaa näkymää näyttämällä tai piilottamalla verkkokartan osia. Voit myös tarkastella verkkokartassa näkyviin osiin liittyviä tietoja.

Etähallinta

Voit hallita kotiverkkosi tietokoneiden suojaustilaa Network Managerin verkkokartan avulla. Voit kutsua tietokoneen hallittuun verkkoon, valvoa hallitun tietokoneen suojaustilaa ja korjata tunnettuja tietoturvan puutteita verkkosi etätietokoneelta.

Network Managerin kuvakkeiden toiminta

Seuraavassa taulukossa kuvataan Network Managerin verkkokartassa yleisesti käytettyjä kuvakkeita.

| Kuvake | Kuvaus |
|---|--|
|  | Kuvaa verkossa olevaa hallittua tietokonetta |
|  | Kuvaa hallittua tietokonetta, joka ei ole verkossa |
|  | Kuvaa hallinnan piiriin kuulumatonta tietokonetta, johon on asennettu McAfee 2007 -tietoturvaohjelmisto |
|  | Kuvaa hallinnan piiriin kuulumatonta tietokonetta, joka ei ole verkossa |
|  | Kuvaa verkossa olevaa tietokonetta, johon ei ole asennettu McAfee 2007 -tietoturvaohjelmistoa, tai tuntematonta verkkolaitetta |
|  | Kuvaa tietokonetta, joka ei ole verkossa ja johon ei ole asennettu McAfee 2007 -tietoturvaohjelmistoa, tai tuntematonta verkkolaitetta, joka ei ole verkossa |
|  | Määrittää, että vastaava kohde on suojattu ja kytketty |
|  | Määrittää, että vastaava kohde vaatii huomiota |
|  | Määrittää, että vastaava kohde vaatii huomiota ja yhteys on katkaistu |
|  | Kuvaa langatonta kotireititintä |
|  | Kuvaa tavallista kotireititintä |
|  | Kuvaa Internetiä, kun yhteys on muodostettu |
|  | Kuvaa Internetiä, kun yhteys on katkaistu |

LUKU 11

Hallitun verkon määrittäminen

Voit määrittää hallitun verkon käyttämällä verkkokartan kohteita ja lisäämällä jäseniä (tietokoneita) verkkoon.

Tässä luvussa

| | |
|---------------------------------------|----|
| Verkkokartan käyttäminen | 54 |
| Hallittuun verkkoon liittyminen | 57 |

Verkkokartan käyttäminen

Aina kun kytket tietokoneen verkkoon, Network Manager analysoi verkon tilan ja määrittää reitittimen asetukset, Internet-tilan ja sen, onko verkossa jäseniä (hallittuja tai hallinnan piiriin kuulumattomia). Ellei jäseniä löydy, Network Manager olettaa, että nyt kytkettävä tietokone on verkon ensimmäinen tietokone ja tekee tietokoneesta automaattisesti järjestelmänvalvojan oikeuksin varustetun jäsenen. Oletusarvoisesti verkon nimeen sisältyy ensimmäisen verkkoon liittyvän tietokoneen, johon on asennettu McAfee 2007 -tietoturvaohjelmisto, työryhmän tai toimialueen nimi. Voit kuitenkin nimetä verkon uudelleen milloin tahansa.

Kun teet muutoksia verkkoosi (esimerkiksi lisäät siihen tietokoneen), voit mukauttaa verkkokarttaa. Voit esimerkiksi päivittää verkkokarttaa, nimetä sen uudelleen ja mukauttaa näkymää näyttämällä tai piilottamalla verkkokartan osia. Voit myös tarkastella verkkokartassa näkyviin osiin liittyviä tietoja.

Verkkokartan käyttäminen

Voit käyttää verkkokarttaa käynnistämällä Network Managerin SecurityCenterin yleisten tehtävien luettelosta. Verkkokartta on graafinen esitys kotiverkon tietokoneista ja osista.

Verkkokartan käyttäminen:

- Valitse Perus- tai Lisävalikosta **Verkonhallinta**. Verkkokartta näkyy oikeanpuoleisessa ikkunassa.

Huomaa: Kun käytät verkkokarttaa ensimmäistä kertaa, sinua pyydetään luottamaan verkon muihin tietokoneisiin, ennen kuin verkkokartta tulee näkyviin.

Päivitä verkkokartta

Voit päivittää verkkokartan milloin tahansa, esimerkiksi kun toinen tietokone liittyy hallittuun verkkoon.

Verkkokartan päivittäminen:

- 1 Valitse Perus- tai Lisävalikosta **Verkonhallinta**. Verkkokartta näkyy oikeanpuoleisessa ikkunassa.
- 2 Valitse **Haluan**-kohdasta **Päivitä verkkokartta**.

Huomautus: Päivitä verkkokartta -linkki on käytettävissä vain, kun verkkokartalta ei ole valittu kohteita. Voit poistaa kohteen valinnan napsauttamalla valittua kohdetta tai napsauttamalla verkkokartan valkoista kohtaa.

Verkon nimeäminen uudelleen

Oletusarvoisesti verkon nimeen sisältyy ensimmäisen verkkoon liittyvän tietokoneen, johon on asennettu McAfee 2007 -tietoturvaohjelmisto, työryhmän tai toimialueen nimi. Voit vaihtaa nimeä, ellei se ole soveltuva.

Verkon nimeäminen uudelleen:

- 1 Valitse Perus- tai Lisävalikosta **Verkonhallinta**. Verkkokartta näkyy oikeanpuoleisessa ikkunassa.
- 2 Valitse **Haluan**-kohdasta **Verkon nimeäminen uudelleen**.
- 3 Kirjoita verkon nimi **Nimeä verkko uudelleen** -ruutuun.
- 4 Valitse **OK**.

Huomautus: Nimeä verkko uudelleen -linkki on käytettävissä vain, kun verkkokartalta ei ole valittu kohteita. Voit poistaa kohteen valinnan napsauttamalla valittua kohdetta tai napsauttamalla verkkokartan valkoista kohtaa.

Verkkokartan kohteiden näyttäminen ja piilottaminen

Oletusarvoisesti kaikki kotiverkkosi tietokoneet ja osat näkyvät verkkokartalla. Jos sinulla on piilotettuja kohteita, saat ne näkyviin milloin tahansa. Vain hallinnan piiriin kuulumattomat kohteet voidaan piilottaa, hallittuja tietokoneita ei voi piilottaa.

| | |
|---------------------------------------|---|
| Jos haluat saada... | Valitse Perus- tai Lisävalikosta Verkonhallinta ja tee näin... |
| ...kohteen piilotettua verkkokartalta | Napsauta verkkokartalla näkyvää kohdetta ja valitse Haluan -kohdasta Piilota tämä . Valitse vahvistusvalintaikkunasta Kyllä . |
| ...kohteen näkyviin verkkokartalle | Valitse Haluan -kohdasta Näytä piilotetut kohteet . |

Kohteen tietojen tarkasteleminen

Voit tarkastella yksityiskohtaisia tietoja mistä tahansa verkkosi kohteesta valitsemalla kohteen verkkokartalta. Näitä tietoja ovat muun muassa osan nimi, sen suojauksen tila ja muut osan hallintaan tarvittavat tiedot.

Kohteen tietojen tarkasteleminen:

- 1 Napsauta verkkokartalla näkyvää kohteen kuvaketta.
- 2 **Tiedot**-kohdassa voit tarkastella kohteen tietoja.

Hallittuun verkkoon liittyminen

Tietokoneen täytyy olla verkon luotettu jäsen, ennen kuin sitä voidaan etähallita tai sille voidaan myöntää oikeus etähallita toisia verkon tietokoneita. Verkon jäsenyyden uusille tietokoneille myöntää verkossa jo oleva jäsen, jolla on järjestelmänvalvojan käyttöoikeudet. Jotta varmistetaan, että vain luotetut tietokoneet voivat liittyä verkkoon, täytyy sekä myöntävän että liittyvän tietokoneen todentaa toisensa.

Kun tietokone liittyy verkkoon, järjestelmä pyytää sitä paljastamaan McAfee-suojaustilansa muille verkon tietokoneille. Jos tietokone suostuu paljastamaan suojaustilansa, siitä tulee verkon *hallittu* jäsen. Jos tietokone ei suostu paljastamaan suojaustilaansa, siitä tulee *hallinnan piiriin kuulumaton* verkon jäsen. Hallinnan piiriin kuulumattomat verkon jäsenet ovat tavallisesti vierailevia tietokoneita, jotka haluavat käyttää muita verkon ominaisuuksia (kuten tiedostojen tai tulostinten jakamista).

Huomaa: Jos tietokoneeseen on asennettu muita McAfee-verkko-ohjelmia, kuten McAfee Wireless Network Security tai EasyNetwork, tietokone tunnistetaan hallittavaksi tietokoneeksi myös näiden ohjelmien osalta. Network Managerissa määritetty oikeustaso koskee kaikkia McAfee-verkko-ohjelmia. Lisätietoja vieraan käyttöoikeuksista, täysistä käyttöoikeuksista ja järjestelmänvalvojan käyttöoikeuksista McAfee-verkko-ohjelmissa on ohjelmien mukana toimitetuissa käyttöohjeissa.

Hallittuun verkkoon liittyminen

Kun saat kutsun liittyä verkkoon, voit joko hyväksyä tai hylätä kutsun. Voit määrittää myös, haluatko tämän ja muiden tietokoneiden valvovan toistensa suojausasetuksia (esimerkiksi ovatko tietokoneen virustorjuntapalvelut ajan tasalla).

Hallittuun verkkoon liittyminen:

- 1 Valitse kutsun valintaikkunasta **Salli tämän ja muiden tietokoneiden valvoa toistensa suojausasetuksia** -valintaruutu, jos haluat toisten hallitun verkon tietokoneiden valvovan tietokoneesi suojausasetuksia.
- 2 Valitse **Liity**.
Kun hyväksyt kutsun, kaksi pelikorttia tulee näkyviin.
- 3 Vahvista, että kortit ovat samat kuin sinut hallittuun verkkoon kutsuneella tietokoneella näkyvät kortit.
- 4 Valitse **Vahvista**.

Huomaa: Jos sinut hallittuun verkkoon kutsuneen tietokoneen näytössä näkyvät kortit eivät ole samat kuin suojausvarmistuksen valintaikkunassa näkyvät kortit, hallitun verkon turvallisuus on uhattuna. Verkkoon liittyminen saattaa altistaa tietokoneesi turvallisuusriskeille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää**.

Tietokoneen kutsuminen hallittuun verkkoon

Jos hallittuun verkkoon lisätään tietokone tai verkossa on hallinnan piiriin kuulumaton tietokone, voit kutsua ne liittymään hallittuun verkkoon. Vain tietokoneet, joilla on järjestelmänvalvojan oikeudet verkossa, voivat kutsua toisia tietokoneita liittymään verkkoon. Kun lähetät pyynnön, määrität samalla liittyvälle tietokoneelle myönnettävän oikeustason.

Tietokoneen kutsuminen liittymään hallittuun verkkoon:

- 1 Napsauta verkkokartalla näkyvää hallinnan piiriin kuulumattoman tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.
- 3 Valitse Kutsu tietokone liittymään hallittuun verkkoon -valintaikkunasta jokin seuraavista:
 - **Myönnä vieraan käyttöoikeudet**
Vieraan käyttöoikeuksilla tietokone voi käyttää verkkoa.
 - **Myönnä täydelliset käyttöoikeudet kaikkiin hallitun verkon sovelluksiin**
Täydellisillä käyttöoikeuksilla (kuten vieraan käyttöoikeuksilla) tietokone voi käyttää verkkoa.

- **Myönnä järjestelmänvalvojan käyttöoikeudet kaikkiin hallitun verkon sovelluksiin**

Järjestelmänvalvojan käyttöoikeuksilla tietokone voi käyttää verkkoa järjestelmänvalvojan oikeuksin. Niillä varustettu tietokone voi myös myöntää käyttöoikeuden muille tietokoneille, jotka haluavat liittyä hallittuun verkkoon.

4 Valitse **Kutsu**.

Kutsu liittyä hallittuun verkkoon lähetään tietokoneelle. Kun tietokone hyväksyy kutsun, kaksi pelikorttia tulee näkyviin.

5 Vahvista, että kortit ovat samat kuin hallittuun verkkoon kutsutussa tietokoneessa näkyvät kortit.

6 Valitse **Myönnä käyttöoikeudet**.

Huomaa: Jos hallittuun verkkoon kutsutun tietokoneen näytössä näkyvät kortit eivät ole samat kuin suojausvarmistuksen valintaikkunassa näkyvät kortit, hallitun verkon turvallisuus on uhattuna. Käyttöoikeuden myöntäminen tälle tietokoneelle saattaa altistaa toiset tietokoneet vaaroille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää**.

Lakkaa luottamasta verkon tietokoneisiin

Jos olet vahingossa suostunut luottamaan toiseen verkon tietokoneeseen, voit lopettaa luottamisen.

Verkon tietokoneeseen luottamisen lopettaminen:

- Valitse **Haluan**-kohdasta **Lopeta tämän verkon tietokoneisiin luottaminen**.

Huomaa: Lopeta tämän verkon tietokoneisiin luottaminen
-linkki on valittavissa vain, jos verkkoon ei ole liittynyt muita hallittuja tietokoneita.

LUKU 12

Verkon etähallinta

Kun olet asentanut hallitun verkon, voit etähallita verkon tietokoneita ja osia Network Managerin avulla. Voit valvoa tietokoneiden ja osien tilaa ja oikeustasoja sekä korjata tietoturvan puutteita.

Tässä luvussa

| | |
|--|----|
| Tilan ja oikeuksien valvonta | 62 |
| Tietoturvan puutteiden korjaaminen | 65 |

Tilan ja oikeuksien valvonta

Hallitussa verkossa on kahdentyyppisiä jäseniä: hallittuja jäseniä ja hallinnan piiriin kuulumattomia jäseniä. Hallitut jäsenet sallivat muiden verkon tietokoneiden valvoa

McAfee-suojaustasoaan, hallinnan piiriin kuulumattomat eivät. Hallinnan piiriin kuulumattomat verkon jäsenet ovat tavallisesti vierailevia tietokoneita, jotka haluavat käyttää muita verkon ominaisuuksia (kuten tiedostojen tai tulostinten jakamista). Toinen hallitun verkon tietokone voi kutsua hallinnan piiriin kuulumattoman tietokoneen hallituksi tietokoneeksi. Samoin hallitusta tietokoneesta voidaan tehdä hallinnan piiriin kuulumaton milloin tahansa.

Hallituilla tietokoneilla on joko järjestelmänvalvojan, täydet tai vieraan käyttöoikeudet. Järjestelmänvalvojan oikeuksilla hallitut tietokoneet voivat hallita toisten hallittujen tietokoneiden suojaustilaa verkossa ja myöntää toisille tietokoneille verkon jäsenyyksiä. Täysillä käyttöoikeuksilla ja vieraan käyttöoikeuksilla tietokoneet voivat vain käyttää verkkoa. Voit muokata tietokoneen oikeustasoa milloin tahansa.

Hallittuun verkkoon kuuluu myös laitteita (esimerkiksi reitittimiä), joita voit myös hallita Network Managerin avulla. Voit myös määrittää ja muokata laitteen näytön ominaisuuksia verkkokartalla.

Tietokoneen suojauksen tilan valvominen

Jos tietokoneen suojauksen tilaa ei valvota verkossa (joko koska tietokone ei ole verkon jäsen tai se ei kuulu hallinnan piiriin), sen valvontaa voi pyytää.

Tietokoneen suojauksen tilan valvominen:

- 1 Napsauta verkkokartalla näkyvää hallinnan piiriin kuulumattoman tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Valvo tätä tietokonetta**.

Tietokoneen suojausten tilan valvomisen lopettaminen

Voit lopettaa yksityisen verkon hallitun tietokoneen suojausten tilan valvomisen. Tietokoneesta tulee tällöin hallinnan piiriin kuulumaton.

Tietokoneen suojausten tilan valvomisen lopettaminen:

- 1 Napsauta verkkokartalla näkyvää hallitun tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Lopeta tämän tietokoneen valvonta**.
- 3 Valitse vahvistusvalintaikkunasta **Kyllä**.

Hallitun tietokoneen oikeuksien muokkaaminen

Voit muokata hallitun tietokoneen oikeuksia milloin tahansa. Oikeuksien avulla voit määrittää, mitkä tietokoneet valvovat toisten verkon tietokoneiden suojausten tilaa (suojausasetuksia).

Hallitun tietokoneen oikeuksien muokkaaminen

- 1 Napsauta verkkokartalla näkyvää hallitun tietokoneen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Muuta tämän tietokoneen käyttöoikeuksia**.
- 3 Määritä, voivatko hallitun verkon tietokoneet valvoa toistensa suojausten tilaa valitsemalla tai poistamalla valinta käyttöoikeuksien muuttamisen valintaikkunan valintaruudusta.
- 4 Valitse **OK**.

Laitteen hallitseminen

Voit hallita laitetta käyttämällä sen hallinnan Web-sivua Network Managerista käsin.

Laitteen hallitseminen:

- 1 Napsauta verkkokartalla näkyvää laitteen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Ota tämä laite hallintaan**. Laitteen hallinnan Web-sivu aukeaa selaimeen.
- 3 Kirjoita kirjautumistietosi selaimeen ja määritä laitteen suojausasetukset.

Huomaa: Jos laite on Wireless Network Securityn suojaama langaton reititin tai yhteyspiste, sen suojausasetusten määrittämiseen on käytettävä Wireless Network Securityä.

Laitteen näytön ominaisuuksien muokkaaminen

Kun muokkaat laitteen näytön ominaisuuksia, voit muuttaa laitteen näyttönimeä verkossa ja määrittää, onko laite langaton reititin.

Laitteen näytön ominaisuuksien muokkaaminen:

- 1 Napsauta verkkokartalla näkyvää laitteen kuvaketta.
- 2 Valitse **Haluan**-kohdasta **Muokkaa laitteen ominaisuuksia**.
- 3 Voit määrittää laitteen näyttönimen kirjoittamalla nimen **Nimi**-ruutuun.
- 4 Voit määrittää laitteen tyyppin napsauttamalla toista seuraavista:
 - **Reititin**
Tämä vastaa tavallista kotireititintä.
 - **Langaton reititin**
Tämä vastaa langatonta kotireititintä.
- 5 Valitse **OK**.

Tietoturvan puutteiden korjaaminen

Järjestelmänvalvojan oikeuksilla varustetut tietokoneet voivat valvoa verkossa olevien toisten hallittujen tietokoneiden McAfee-suojaustasoa ja korjata raportoituja tietoturvan puutteita. Jos esimerkiksi hallitun tietokoneen McAfee-suojaustaso ilmaisee, ettei virustorjunta ole käytössä, toinen järjestelmävalvojan oikeuksin varustettu hallittu tietokone voi *korjata* tämän tietoturvan puutteen ottamalla virustorjunnan käyttöön etäyhteyden kautta.

Kun korjaat tietoturvan puutteita etäyhteyden kautta, Network Manager korjaa useimmat raportoidut ongelmat automaattisesti. Tietyt tietoturvan puutteet saattavat kuitenkin vaatia manuaalisia toimia paikalliselta tietokoneelta. Tässä tapauksessa Network Manager korjaa ne ongelmat, jotka se pystyy korjaamaan etäyhteyden kautta, ja pyytää korjaamaan loput ongelmat kirjautumalla kyseisessä tietokoneessa SecurityCenteriin ja noudattamalla tarjottuja suosituksia. Joissakin tapauksissa suositeltava korjaustapa on McAfee 2007 -tietoturvaohjelmiston asentaminen etätietokoneeseen tai verkon tietokoneisiin.

Korjaa tietoturvan puutteet

Network Managerin avulla voit korjata automaattisesti useimmat hallittujen tietokoneiden tietoturvan puutteet etäyhteyttä käyttäen. Jos esimerkiksi virustorjunta on poistettu käytöstä etätietokoneesta, voit ottaa sen automaattisesti käyttöön Network Managerin avulla.

Tietoturvan puutteiden korjaaminen:

- 1 Napsauta verkkokartalla näkyvää kohteen kuvaketta.
- 2 Kohteen suojauksen tila näkyy **Lisätiedot**-kohdassa.
- 3 Valitse **Haluan**-kohdasta **Tietoturvan puutteiden korjaaminen**.
- 4 Kun tietoturvan puutteet on korjattu, napsauta **OK**-painiketta.

Huomaa: Vaikka Network Manager korjaa automaattisesti useimmat tietoturvan puutteet, joidenkin puutteiden korjaus edellyttää SecurityCenterin käynnistämistä kyseisessä tietokoneessa ja tarjottujen suositusten noudattamista.

McAfee-tietoturvaohjelmiston asentaminen etätietokoneisiin

Jos yksi tai useampi verkkosi tietokone ei käytä McAfee 2007 -tietoturvaohjelmistoa, niiden suojauksen tilaa ei voida valvoa etäyhteyden kautta. Jos haluat valvoa kyseisiä tietokoneita etäyhteydettä käyttäen, niihin täytyy asentaa McAfee-tietoturvaohjelmisto.

McAfee-tietoturvaohjelmiston asentaminen etätietokoneisiin:

- 1 Siirry etätietokoneen selaimella osoitteeseen <http://download.mcafee.com/us/>.
- 2 Asenna McAfee 2007 -tietoturvaohjelmisto tietokoneeseen noudattamalla näytössä näkyviä ohjeita.

LUKU 13

McAfee Wireless Network Security

Wireless Network Security tarjoaa standardinmukaisen automaattisen suojauksen tietomurtoja ja luvaton verkkon käyttöä vastaan. Suojaus toimii helposti vain yhdellä hiiren napsautuksella. Wireless Network Security salaa henkilökohtaiset ja yksityiset tietosi, kun ne lähetetään langattoman verkkoyhteyden kautta, ja estää hakkereilta pääsyn langattomaan verkkoosi.

Wireless Network Security estää hakkereita murtautumasta langattomaan verkkoosi, sillä se

- estää luvattomien yhteyksien muodostamisen langattomaan verkkoon
- estää langattoman verkon kautta lähetettyjen tietojen sieppaamisen
- havaitsee langattomaan verkkoon kohdistuvat yhteydenottoyritykset.

Wireless Network Securityssa on sekä helppokäyttöisiä toimintoja, kuten verkon välitön lukitus ja mahdollisuus lisätä luvallisia käyttäjiä verkkoon, että tehokkaita suojausominaisuuksia, kuten salausavainten automaattinen luominen ja ajoitettu avainten kierrätys.

Tässä luvussa

| | |
|--|-----|
| Ominaisuudet..... | 68 |
| Wireless Network Securityn ottaminen käyttöön..... | 70 |
| Langattomien verkkojen suojaaminen..... | 73 |
| Langattomien verkkojen hallinnointi..... | 91 |
| Langattoman verkon suojauksen hallinta..... | 103 |
| Langattomien verkkojen valvonta..... | 119 |

Ominaisuudet

Wireless Network Security tarjoaa seuraavat ominaisuudet.

Aina käynnissä -suojaus

Wireless Network Security havaitsee automaattisesti ja suojaa havaitsemiaan haavoittuvia langattomia verkkoja, joihin olet kytkeytynyt.

Helppo käyttöliittymä

Suojaa verkkoa vaatimatta hankalia päätöksiä tai teknisten termien tietämystä.

Vahva automaattinen salaus

Sallii vain ystävien ja perheenjäsenten käyttää verkkoasi ja suojaa tietojasi niitä siirrettäessä.

Ohjelmistopohjainen tietoturvaratkaisu

Wireless Network Security toimii yhdessä tavallisen langattoman reitittimen tai yhteyspisteen sekä tietoturvaohjelmiston kanssa. Sinun ei tarvitse hankkia lisälaitteita.

Automaattinen verkkoavaimen kierrätys

Päätäväisimmätkään hakkerit eivät pysty sieppaamaan tietojasi, koska verkkoavainta kierrätetään jatkuvasti.

Verkkokäyttäjien lisääminen

Voit helposti myöntää ystäville ja perheenjäsenille käyttöoikeuden verkkoosi. Voit lisätä käyttäjiä langattomasti tai siirtämällä ohjelmia USB-aseman kautta.

Helppokäyttöinen yhdistämistyökalu

Langattoman yhteyden työkalu on helppokäyttöinen ja informatiivinen. Siinä näkyy tietoja signaalinvoimakkuudesta ja suojauksen tilasta.

Tapahutumien kirjaaminen lokiin ja hälytykset

Helposti ymmärrettävät raportit ja hälytykset tarjoavat kokeneille käyttäjille tietoja langattomasta verkosta.

Keskeytystila

Keskeyttää väliaikaisesti verkkoavaimen kierrätyksen, jotta tietyt sovellukset voidaan suorittaa keskeytyksettä.

Yhteensopivuus muiden laitteiden kanssa

Wireless Network Security päivittää itsensä automaattisesti uusimpien langattomien reititin- ja yhteyspiste-moduulien kanssa, kuten Linksys®, NETGEAR®, D-Link®, Belkin®, TRENDnet® ja muiden valmistajien laitteiden.

Wireless Network Securityn ottaminen käyttöön

Wireless Network Security otetaan asennuksen jälkeen automaattisesti käyttöön, joten sitä ei tarvitse käynnistää manuaalisesti. Halutessasi voit kuitenkin ottaa langattoman verkon suojauksen käyttöön ja poistaa sen käytöstä myös manuaalisesti.

Kun olet asentanut Wireless Network Securityn, tietokone yrittää muodostaa yhteyden langattomaan reitittimeen. Kun yhteys on muodostettu, tietokone ohjelmoi salausavaimen langattomaan reitittimeen. Jos oletussalasana on muuttunut, sinua kehoitetaan antamaan salasana, jotta Wireless Network Security voi määrittää langattoman reitittimen asetukset lisäämällä siihen jaetun salausavaimen ja ottamalla vahvan suojaustilan käyttöön. Suojattu langaton yhteys muodostetaan käyttämällä samaa jaettua avainta ja salaustilaa myös tietokoneessa.

Ota Wireless Network Security käyttöön

Wireless Network Security otetaan oletusarvoisesti käyttöön, mutta voit kuitenkin ottaa langattoman verkon suojauksen käyttöön ja poistaa sen käytöstä myös manuaalisesti.

Ottamalla langattoman verkon suojauksen käyttöön voit suojata langatonta verkkoa tietomurroilta ja tietojen kaappaamiselta. Jos olet muodostanut yhteyden ulkoiseen langattomaan verkkoon, suojauksesi taso vaihtelee kuitenkin kyseisen verkon suojaustason mukaan.

Langattoman verkon suojauksen ottaminen manuaalisesti käyttöön:

- 1 Toimi McAfee SecurityCenter -ikkunassa seuraavasti:
 - Valitse **Internet ja verkko** ja sitten **Määritä**.
 - Valitse **Lisävalikko**, sitten **Koti**-valikosta **Määritä** ja lopuksi **Internet ja verkko**.
- 2 Valitse **Internet- ja verkkomääritykset** -ikkunan **Langaton suojaus** -kohdasta **Käytössä**.

Huomaa: Wireless Network Security otetaan automaattisesti käyttöön, jos tietokoneessa on yhteensopiva langaton verkkosovitin.

Poista Wireless Network Security käytöstä

Wireless Network Security otetaan oletusarvoisesti käyttöön, mutta voit kuitenkin ottaa langattoman verkon suojauksen käyttöön ja poistaa sen käytöstä myös manuaalisesti.

Langattoman verkon suojauksen poistaminen käytöstä altistaa verkon tietomurroille ja tietojen kaappaamiselle.

Langattoman verkon suojauksen poistaminen käytöstä:

- 1 Toimi McAfee SecurityCenter -ikkunassa seuraavasti:
 - Valitse **Internet ja verkko** ja sitten **Määritä**.
 - Valitse **Lisävalikko**, sitten **Koti**-valikosta **Määritä** ja lopuksi **Internet ja verkko**.
- 2 Valitse **Internet- ja verkkomääritykset** -ikkunan **Langaton suojaus** -kohdasta **Ei käytössä**.

LUKU 14

Langattomien verkkojen suojaaminen

Wireless Network Security suojaa verkkoa käyttämällä langatonta salausta (WEP-, WPA- tai WPA2-salausta laitteiston mukaan). Se ohjelmoi automaattisesti voimassa olevat ja salausavaimen perustuvat käyttöoikeustiedot asiakkaisiin ja langattomiin reitittämiin, ja käyttöoikeuksien perusteella langaton reititin myöntää tietokoneille luvan yhteyden muodostamiseen. Salausavaimella suojatut verkot estävät luvattomia käyttäjiä käyttämästä langatonta verkkoa ja suojaavat langattoman verkon kautta lähetettyjä tietoja. Wireless Network Security tekee tämän

- luomalla ja jakamalla pitkän, vahvan, sattumanvaraisen ja jaetun salausavaimen
- kierrättämällä salausavainta säännöllisin väliajoin
- määrittämällä jokaiselle langattomalle laitteelle salausavaimen.

Tässä luvussa

| | |
|---|----|
| Suojattujen langattomien verkkojen määrittäminen | 74 |
| Lisää tietokoneita suojattuun langattomaan verkkoon | 86 |

Suojattujen langattomien verkkojen määrittäminen

Kun Wireless Network Security asennetaan, se kehottaa sinua automaattisesti suojaamaan käyttämäsi suojaamattoman langattoman yhteyden tai liittymään jo suojattuun langattomaan verkkoon.

Jos et ole muodostanut yhteyttä langattomaan verkkoon, Wireless Network Security hakee McAfeen suojaamaa verkkoa, jonka signaali on voimakas, ja kehottaa käyttäjää liittymään verkkoon. Jos suojattuja verkkoja ei ole käytettävissä, Wireless Network Security hakee suojaamattomia verkkoja, joiden signaali on voimakas, ja jos sellainen löytyy, kehottaa käyttäjää liittymään kyseiseen verkkoon.

Jos langaton verkko ei ole McAfee Wireless Network Securityn suojaama, McAfee katsoo langattomat verkot "suojaamattomiksi", vaikka niissä käytettäisiin muita langattoman verkon suojausmekanismeja, kuten WEP- ja WPA-salausta.

Jos langaton verkko ei ole McAfee Wireless Network Securityn suojaama, McAfee katsoo verkon suojaamattomaksi, vaikka siinä käytettäisiin muita langattoman verkon suojausmekanismeja, kuten WEP- ja WPA-salausta.

Tietoja käyttöoikeustypeistä

Suojatun langattoman verkon voivat luoda kaikki langattomat tietokoneet, joihin on asennettu Wireless Network Security. Ensimmäiselle reitittimen suojanneelle ja suojatun langattoman verkon luoneelle tietokoneelle myönnetään automaattisesti kyseisen verkon järjestelmänvalvojan käyttöoikeudet. Olemassa oleva käyttäjä, jolla on järjestelmänvalvojan käyttöoikeudet, voi myöntää myöhemmin verkkoon liittyville tietokoneille järjestelmänvalvojan käyttöoikeudet, täydelliset käyttöoikeudet tai vieraan käyttöoikeudet.

Tietokoneet, joissa on järjestelmänvalvojan käyttöoikeudet ja täydelliset käyttöoikeudet, voivat suorittaa seuraavat tehtävät:

- suojata ja poistaa reitittimen tai yhteyspisteen
- kierrättää salausavaimia
- muuttaa verkon suojausasetuksia
- korjata verkkoja
- myöntää tietokoneille oikeudet verkon käyttöön
- evätä oikeudet suojatun langattoman verkon käyttöön
- muuttaa tietokoneen hallintatasoa.

Tietokoneet, joissa on vieraan käyttöoikeudet, voivat suorittaa verkossa seuraavat tehtävät:

- muodostaa yhteyden verkkoon
- liittyä verkkoon
- muokata vierastietokoneen asetuksia.

Huomaa: Tietokoneilla voi olla järjestelmänvalvojan käyttöoikeudet yhdessä verkossa, mutta vieraan käyttöoikeudet tai täydelliset käyttöoikeudet toisessa verkossa. Tietokone, jolla on vieraan käyttöoikeudet tai täydelliset käyttöoikeudet verkossa, voi luoda uuden verkon.

Vastaavat aiheet

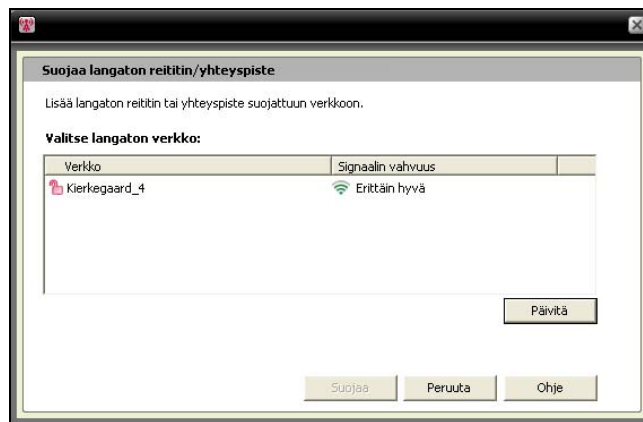
- Liity suojattuun langattomaan verkkoon (sivu 78)
- Myönnä tietokoneille järjestelmänvalvojan käyttöoikeudet (sivu 83)
- Evää oikeudet verkon käyttöön (sivu 101)

Luo suojattuja langattomia verkkoja

Jos haluat luoda suojatun langattoman verkon, sinun on ensin lisättävä langattoman verkon langaton reititin tai yhteyspiste.

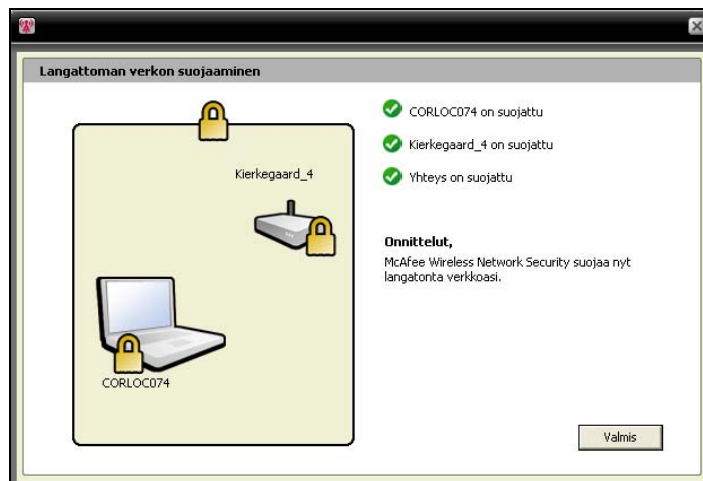
Langattoman reitittimen tai yhteyspisteen lisääminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Suojaustyökalut-ruudun **Suojaa langaton reititin tai yhteyspiste** -kohdasta **Suojaa**.
- 4 Valitse Suojaa langaton reititin tai yhteyspiste -ruudusta suojattava langaton verkko ja valitse sitten **Suojaa**.



Näyttöön ilmestyy Langattoman verkon suojaus -ruutu, kun Wireless Network Security yrittää suojata tietokonetta, reititintä ja verkkoyhteyttä.

Suojaamalla kaikki nämä tekijät voidaan varmistaa, että langaton verkko on täydellisesti suojattu.



5 Valitse **Valmis**.

Huomaa: Kun olet suojannut verkon, Seuraavat vaiheet -valintaikkunassa sinua kehoitetaan asentamaan Wireless Network Security jokaiseen langattomaan tietokoneeseen, jotta ne voivat liittyä verkkoon.

Jos olet jo aikaisemmin määrittänyt reitittimelle tai yhteyspisteelle esijaetun avaimen tai yhteyspisteen, mutta yhteyttä ei muodostettu, kun yritit suojata reitittimen tai yhteyspisteen, sinun on kirjoitettava avain myös WEP-avain-ruutuun ja valittava Yhdistä. Jos olet aikaisemmin muuttanut langattoman reitittimen järjestelmänvalvojan käyttäjänimeä tai salasanaa, sinua kehoitetaan antamaan nämä tiedot ennen reitittimen tai yhteyspisteen suojaamista.

Vastaavat aiheet

- Suojaa muut langattomat laitteet (sivu 84)
- Lisää tietokoneita suojattuun langattomaan verkkoon (sivu 86)

Liity suojattuihin langattomiin verkkoihin

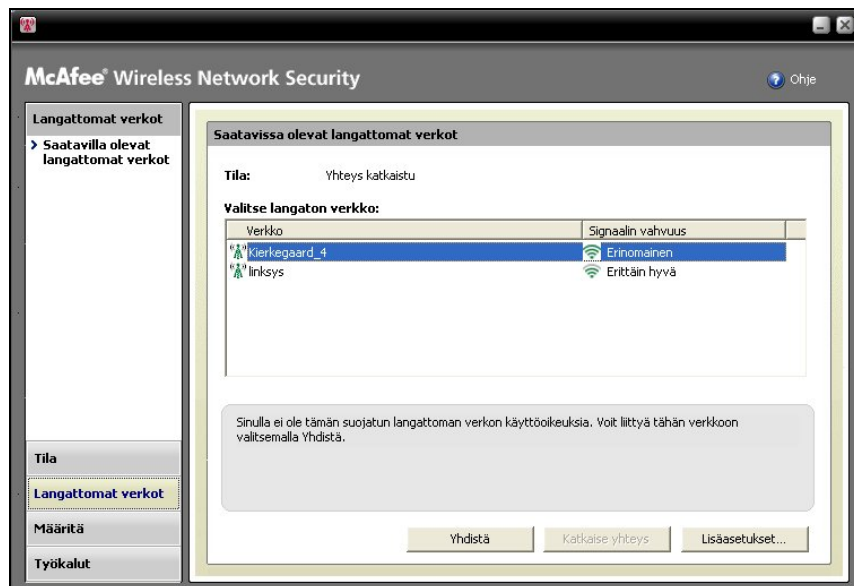
Suojattu langaton verkko estää hakkereita kaappaamasta verkon kautta lähetettyjä tietoja ja muodostamasta yhteyttä verkkoon. Valtuutettujen tietokoneiden on liityttävä suojattuun langattomaan verkkoon ennen kuin ne voivat käyttää sitä.

Kun tietokone pyytää oikeutta liittyä hallittuun verkkoon, muille verkon järjestelmänvalvonnasta vastaaville tietokoneille lähetetään viesti. Järjestelmänvalvojana tehtävänäsi on päättää, mikä käyttöoikeustyyppi tietokoneelle myönnetään: vieras, täydet oikeudet tai järjestelmänvalvoja.

Ennen kuin voit liittyä suojattuun verkkoon, sinun on asennettava Wireless Network Security ja muodostettava sitten yhteys suojattuun langattomaan verkkoon. Nykyisen verkon käyttäjän, jolla on järjestelmänvalvojan oikeudet, on annettava sinulle lupa suojatun langattoman verkon käyttöön. Kun olet liittynyt verkkoon, sinun ei tarvitse liittyä siihen uudelleen, kun muodostat uudelleen yhteyden. Sekä käyttöoikeuden myöntäjällä että verkkoon liittyjällä on oltava aktiivinen langaton yhteys. Myöntäjän on oltava järjestelmänvalvonnasta vastaava tietokone, joka on yhteydessä verkkoon.

Suojattuun langattomaan verkkoon liittyminen:

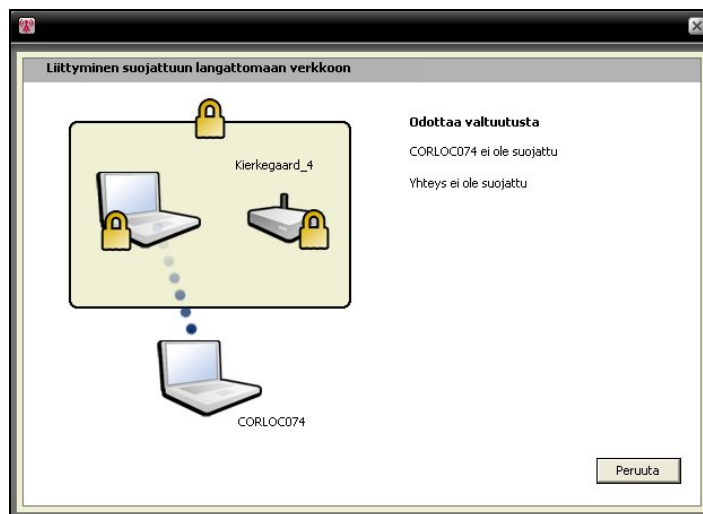
- 1 Napsauta hiiren kakkospainikkeella suojaamattoman tietokoneen Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä langattomat verkot**.
- 3 Valitse verkko Käytettävissä olevat langattomat verkot -ruudusta ja valitse **Yhdistä**.



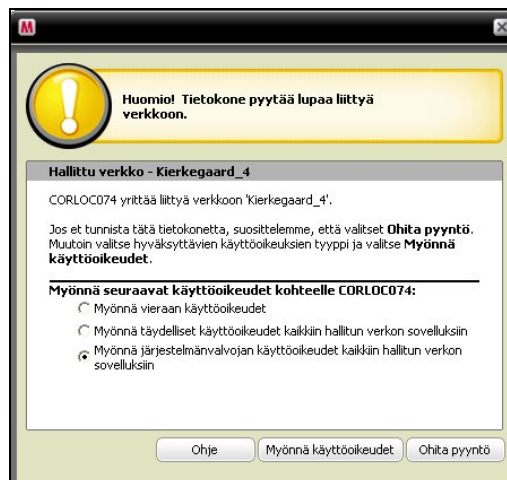
4 Liity verkkoon valitsemalla Liity suojattuun langattomaan verkkoon -valintaikkunasta **Kyllä**.



Kun Wireless Network Security pyytää lupaa saada liittyä verkkoon, verkkoon liittymistä yrittävään tietokoneeseen ilmestyy Liitytään suojattuun langattomaan verkkoon -ruutu.



5 Liity verkkoon -ruutu ilmestyy järjestelmänvalvonnasta vastaavaan tietokoneeseen, josta voidaan myöntää vieraan käyttöoikeudet, täydelliset käyttöoikeudet tai järjestelmänvalvojan käyttöoikeudet.



Valitse Liity verkkoon -valintaikkunasta yksi seuraavista vaihtoehtoista:

| | |
|--|---|
| <p>Myönnä vieraan käyttöoikeudet</p> | <p>Sallii tietokoneen lähettää tiedostoja muihin langattomassa verkossa oleviin tietokoneisiin, mutta ei salli tiedostojen jakamista McAfee EasyNetworkin kautta.</p> |
| <p>Myönnä täydelliset käyttöoikeudet kaikkiin hallitun verkon sovelluksiin</p> | <p>Sallii tietokoneen lähettää ja jakaa tiedostoja McAfee EasyNetworkin kautta.</p> |
| <p>Myönnä järjestelmänvalvojan käyttöoikeudet kaikkiin hallitun verkon sovelluksiin</p> | <p>Sallii tietokoneen lähettää ja jakaa tiedostoja McAfee EasyNetworkin kautta, myöntää käyttöoikeuden muiden tietokoneiden käyttöön ja mahdollistaa muiden langattomassa verkossa olevien tietokoneiden käyttöoikeustason muuttamisen.</p> |

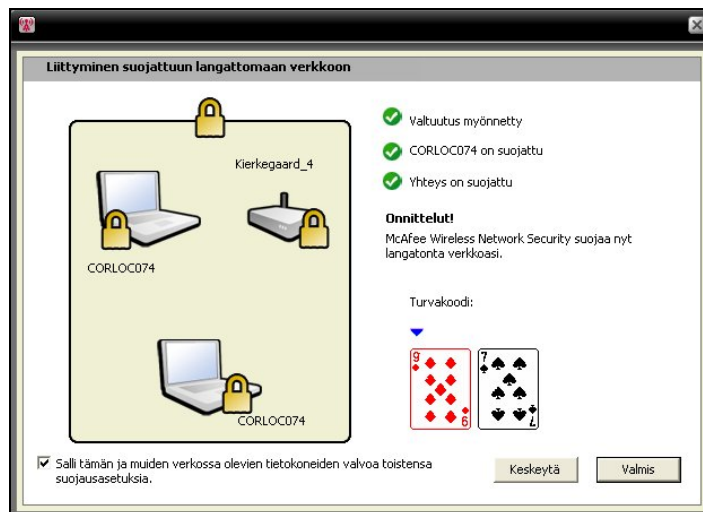
6 Valitse **Myönnä käyttöoikeudet**.

7 Vahvista, että Myönnetään käyttöoikeuksia verkkoon -ruudussa näkyvät kortit vastaavat langattomaan verkkoon liittymistä yrittävän tietokoneen kortteja. Jos kortit vastaavat toisiaan, valitse **Myönnä käyttöoikeudet**.

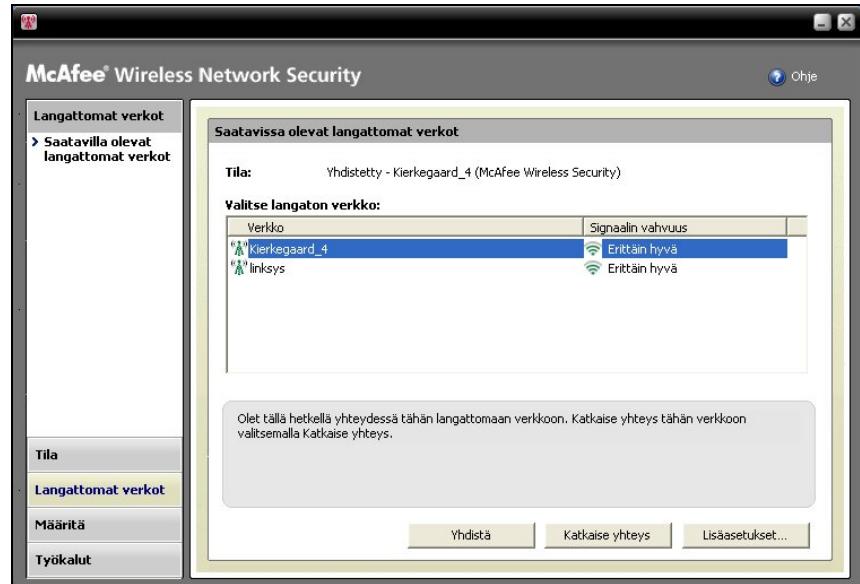
Jos tietokoneiden kortit ovat erilaiset, tietoturva on mahdollisesti uhattuna. Verkon käyttöoikeuden myöntäminen kyseiselle tietokoneelle voi vaarantaa tietokoneen turvallisuuden. Jos haluat estää tietokonetta käyttämästä langatonta verkkoa, valitse **Hylkää käyttöoikeudet**.



- 8 Myöntetään käyttöoikeuksia verkkoon -ruutu vahvistaa, että Wireless Network Security suojaa uutta tietokonetta. Jos haluat valvoa toisten tietokoneiden suojausasetuksia ja haluat niiden valvovan oman tietokoneesi suojausasetuksia, valitse **Salli tämän ja muiden tietokoneiden valvoa toistensa suojausasetuksia.**



- 9 Valitse **Valmis**.
- 10 Käytettävissä olevat langattomat verkot -ruutu osoittaa, että olet muodostanut yhteyden suojattuun langattomaan verkkoon.



Vastaavat aiheet

- Lisää tietokoneita suojattuun langattomaan verkkoon (sivu 86)

Muodosta yhteys suojattuihin langattomiin verkkoihin

Jos olet jo liittynyt suojattuun langattomaan verkkoon, mutta yhteytesi katkesi eikä käyttöoikeuksiasi ole evätty, voit muodostaa yhteyden uudelleen milloin tahansa ilman uudelleenliittymistä.

Yhteyden muodostaminen suojattuun langattomaan verkkoon:

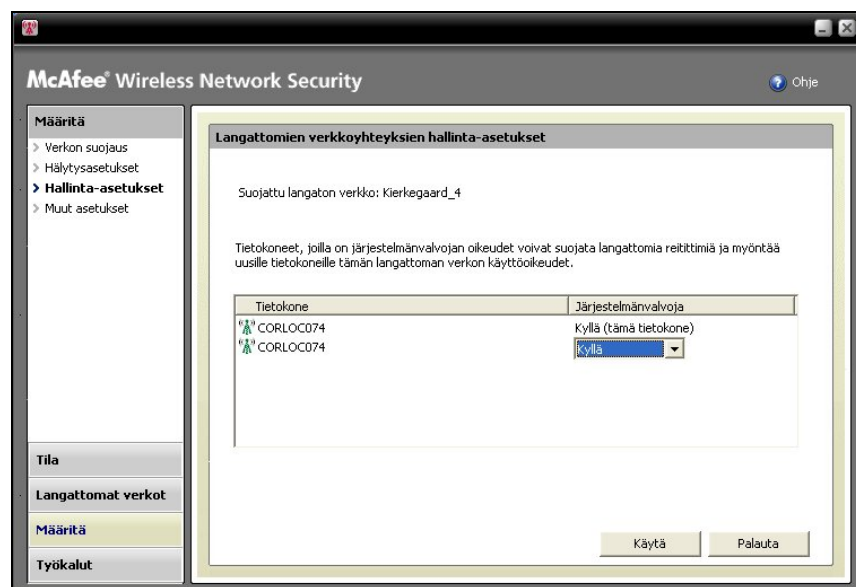
- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä langattomat verkot**.
- 3 Valitse verkko Käytettävissä olevat langattomat verkot -ruudusta ja valitse **Yhdistä**.

Myönnä tietokoneille järjestelmänvalvojan käyttöoikeudet

Tietokoneet, joissa on järjestelmänvalvojan käyttöoikeudet, voivat suojata langattomia reitittimiä, muuttaa suojaustiloja ja myöntää uusille tietokoneille käyttöoikeudet suojatun langattoman verkon käyttöön.

Järjestelmänvalvojan käyttöoikeuksien määrittäminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Valitse Määritä-ruudusta **Hallinta-asetukset**.
- 4 Valitse Langattoman hallinnan asetukset -ruudusta **Kyllä** tai **Ei** ja määritä, haluatko myöntää järjestelmänvalvojan käyttöoikeudet.



- 5 Valitse **Käytä**.

Vastaavat aiheet

- Tietoja käyttöoikeustyypeistä (sivu 75)
- Evää oikeudet verkon käyttöön (sivu 101)

Suojaa muut langattomat laitteet

Wireless Network Securityn avulla voit lisätä yhden tai useamman langattoman tulostimen, tulostinpalvelimen tai pelikonsolin verkkoon.

Langattoman tulostimen, tulostinpalvelimen tai pelikonsolin lisääminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Suojaustyökalut-ruudun **Suojaa muu kuin yhteyspistettä käyttävä laite** -kohdasta **Suojaa**.
- 4 Valitse Suojaa langaton laite -ruudusta langaton laite ja sitten **Suojaa**.
- 5 Muu kuin yhteyspistettä käyttävä laite suojattu -hälytys vahvistaa, että laite on lisätty verkkoon.

Yhteyden muodostaminen verkkoihin, joissa SSID-lähetys on poistettu käytöstä

Voit muodostaa yhteyden langattomiin verkkoihin, joissa SSID-lähetys on poistettu käytöstä. Kun reititinten SSID-lähetys on poistettu käytöstä, ne eivät ilmesty Käytettävissä olevat langattomat verkot -ruutuun.

McAfee suosittelee, että et käytä Wireless Network Securitya sellaisten langattomien reititinten suojaamiseen, joissa SSID-lähetys on poistettu käytöstä.

Yhteyden muodostaminen langattomiin verkkoihin, joissa SSID-lähetys on poistettu käytöstä:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä langattomat verkot**.
- 3 Valitse Käytettävissä olevat langattomat verkot -ikkunasta **Lisäasetukset**.
- 4 Valitse Langattomat verkot -kohdasta **Lisää**.
- 5 Määritä seuraavat asetukset Lisää langaton verkko -ruudusta ja valitse **OK**.

| Asetus | Kuvaus |
|-------------------|---|
| Verkko | Verkon nimi. Jos muokkaat verkkoa, et voi muuttaa sen nimeä. |
| Suojaus-asetukset | Suojaamattoman verkon suojaus. Huomaa, että jos langaton verkkosovitin ei tue valittua tilaa, yhteyttä ei voi muodostaa. Suojaustilat ovat seuraavat: Ei käytössä, Avoin WEP, Jaettu WEP, Automaattinen WEP, WPA-PSK, WPA2-PSK. |
| Salaustila | Valitsemaasi suojaustilaan liittyvä salaustila. Salaustilat ovat seuraavat: WEP, TKIP, AES ja TKIP+AES. |

Huomaa: McAfee suosittelee, että et käytä Wireless Network Securitya sellaisten langattomien reititinten suojaamiseen, joissa SSID-lähetys on poistettu käytöstä. Jos sinun on välttämättä käytettävä toimintoa, käytä sitä vain silloin, kun SSID-lähetys on poistettu käytöstä.

Lisää tietokoneita suojattuun langattomaan verkkoon

Voit lisätä tietokoneita suojattuun langattomaan verkkoon käyttämällä siirrettävää laitetta, kuten USB flash -asemaa, tallentavaa CD-levyä tai Windows Connect Now -tekniikkaa.

Lisää tietokoneita käyttämällä siirrettävää laitetta

Wireless Network Securityn ja USB flash -aseman tai tallentavan CD-levyn avulla voit lisätä suojattuun langattomaan verkkoon muita tietokoneita, jotka eivät käytä Wireless Network Securityä.

Tietokoneen lisääminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Suojaustyökalut-ruudun **Suojaa tietokone** -kohdasta **Suojaa**.
- 4 Valitse Suojaa toinen tietokone -ruudusta **Kopioi Wireless Network Security siirrettävään laitteeseen, kuten USB-avaimeen**.



- 5 Valitse CD-aseman tai USB flash -aseman sijainti, jonne haluat kopioida Wireless Network Securityn.
- 6 Valitse **Kopioi**.
- 7 Kun kaikki tiedostot on kopioitu CD-levylle tai USB flash -asemalle, aseta siirrettävä laite suojattavaan tietokoneeseen. Jos ohjelma ei käynnisty automaattisesti, käytä Resurssienhallintaa ja valitse siirrettävästä tallennusvälineestä **Install.exe**.
- 8 Toimi näytön ohjeiden mukaan.

Huomaa: Voit lisätä tietokoneen suojattuun langattomaan verkkoon myös käyttämällä Windows Connect Now -tekniikkaa.

Vastaavat aiheet

- Lisää tietokoneita käyttämällä Windows Connect Now -tekniikkaa (sivu 88)

Lisää tietokoneita käyttämällä Windows Connect Now -tekniikkaa

Wireless Network Securityn ja Windows Connect Now -tekniikan avulla voit lisätä verkkoon muita tietokoneita, jotka eivät käytä Wireless Network Securityä.

Tietokoneiden lisääminen käyttämällä Windows Connect Now -tekniikkaa:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Suojaustyökalut-ruudun **Suojaa tietokone** -kohdasta **Suojaa**.
- 4 Valitse Suojaa toinen tietokone -ruudusta **Luo Windows Connect Now -levy**
- 5 Valitse sijainti, jonne haluat kopioida Windows Connect Now -tiedot.
- 6 Valitse **Kopioi**.
- 7 Aseta Windows Connect Now -levy suojattavaan tietokoneeseen
- 8 Jos levy ei käynnisty automaattisesti, valitse yksi seuraavista vaihtoehdoista:
 - Asenna Wireless Connect Now -tekniikka: Valitse Windowsin tehtäväriviltä **Käynnistä** ja valitse sitten Ohjauspaneeli. Jos käytät Ohjauspaneelin luokkanäkymää, valitse **Verkko- ja Internet-yhteydet** ja sitten **Ohjattu langattoman verkon asennus**. Jos käytät Ohjauspaneelin perinteistä näkymää, valitse **Ohjattu langattoman verkon asennus**. Toimi näytön ohjeiden mukaan.
 - Avaa setupSNK.exe Windows Connect -levyltä ja kopioi ja liitä avain langattoman verkon valintaan käytettävään asiakastietokoneeseen.

Huomaa: Keskeytä avainten kierrätys, jos muodostat yhteyden langattomaan verkkoon Windows Connect -tekniikan avulla, sillä muuten verkkoyhteys epäonnistuu. Yhteys epäonnistuu, sillä avainten kierrätys luo uuden avaimen, joka on erilainen kuin Windows Connect Now -tekniikan käyttämä avain.

Voit lisätä tietokoneita suojattuun langattomaan verkkoon myös käyttämällä siirrettävää laitetta, kuten tallentavaa CD-levyä tai USB flash -asemaa.

Vastaavat aiheet

- Lisää tietokoneita käyttämällä siirrettävää laitetta (sivu 86)

LUKU 15

Langattomien verkkojen hallinnointi

Wireless Network Security tarjoaa lukuisia hallintatyökaluja langattoman verkon hallintaan ja ylläpitoon.

Tässä luvussa

Langattomien verkkojen hallinta92

Langattomien verkkojen hallinta




Kun olet yhteydessä suojattuun langattomaan verkkoon, lähetetyt ja vastaanotetut tiedot salataan. Hakkerit eivät voi purkaa suojatun verkon kautta lähetettyjä tietoja, eivätkä he voi muodostaa yhteyttä verkkoosi. Wireless Network Security tarjoaa useita työkaluja verkon hallintaan, joiden avulla tietomurrot voidaan estää.

Tietoa Wireless Network Securityn kuvakkeista

Wireless Network Securityssa käytetään kuvakkeita, jotka esittävät eri verkkoyhteystyyppä ja signaalivoimakkuuksia.





Verkkoyhteyuskuvakkeet

Seuraavassa taulukossa kuvataan Wireless Network Securityn kuvakkeet, joita käytetään yleisesti Langattoman verkon tila-, Suojaustyökalut- ja Käytettävissä olevat langattomat verkot -ruuduissa. Kuvakkeet esittävät erilaisia verkkoyhteyden ja suojauksen tiloja.

| Kuvake | Tilaruudut | Suojausruudut |
|---|--|---|
|  | Tietokone on yhdistetty valittuun suojattuun langattomaan verkkoon. | Wireless Network Security suojaa laitetta. |
|  | Tietokone voi käyttää suojattua langatonta verkkoa, mutta sitä ei ole tällä hetkellä yhdistetty verkkoon. | Laite käyttää WEP- tai WPA-salausta. |
|  | Tietokone on aikaisemmin kuulunut suojattuun langattomaan verkkoon, mutta sen käyttöoikeudet evättiin, kun tietokone katkaisi yhteyden verkkoon. | Wireless Network Security ei ole laitteessa käytössä. |

Signaalinvoimakkuuden kuvakkeet

Seuraavassa taulukossa kuvataan Wireless Network Securityn kuvakkeet, joita käytetään verkkojen signaalinvoimakkuuden esittämiseen.

| Kuvake | Kuvaus |
|---|-----------------------------------|
|  | Erinomainen signaalinvoimakkuus |
|  | Erittäin hyvä signaalinvoimakkuus |
|  | Hyvä signaalinvoimakkuus |
|  | Heikko signaalinvoimakkuus |

Vastaavat aiheet

- Näytä verkon signaalinvoimakkuus (sivu 123)
- Näytä tällä hetkellä suojatut tietokoneet (sivu 129)
- Näytä verkon suojaustila (sivu 121)

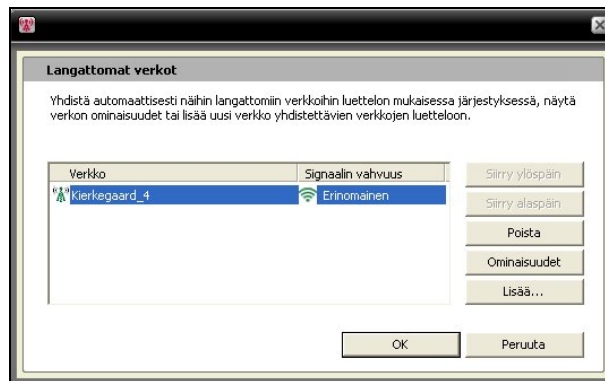
Luettele suositut verkot

Wireless Network Securityn avulla voit määrittää suosittuja verkkoja. Näin voit määrittää niiden verkkojen järjestyksen, joihin tietokone ottaa automaattisesti yhteyttä. Wireless Network Security yrittää muodostaa yhteyden luettelossa ensimmäisenä olevaan verkkoon.

Tämä toiminto on hyödyllinen esimerkiksi silloin, kun yrität muodostaa automaattisesti yhteyden ystäväsi langattomaan verkkoon, kun olet hänen alueellaan. Voit siirtää toisen verkon luettelon alkuun.

Suosittujen verkkojen luetteleminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä langattomat verkot**.
- 3 Valitse Käytettävissä olevat langattomat verkot -ikkunasta **Lisäasetukset**.
- 4 Valitse verkko, jonka järjestyksestä haluat säätää, ja valitse **Siirrä ylös** tai **Siirrä alas**.



- 5 Valitse **OK**.

Vastaavat aiheet

- Poista suositut langattomat verkot (sivu 95)

Poista suositut langattomat verkot

Wireless Network Securityn avulla voit poistaa suositut verkot.

Tämä on hyödyllistä esimerkiksi silloin, kun haluat poistaa luettelosta vanhentuneen verkon.

Suosittujen verkkojen poistaminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä langattomat verkot**.
- 3 Valitse Käytettävissä olevat langattomat verkot -ikkunasta **Lisäasetukset**.
- 4 Valitse verkko Langattomat verkot -ruudusta ja valitse sitten **Poista**.
- 5 Valitse **OK**.

Vastaavat aiheet

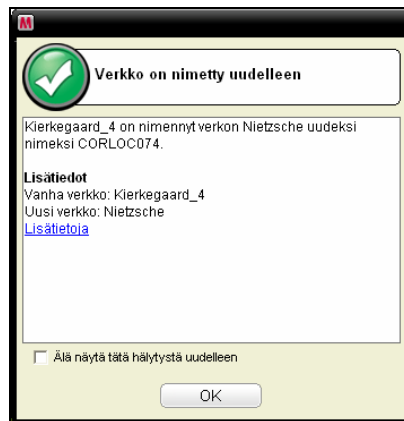
- Luettele suositut verkot (sivu 94)

Nimeä suojatut langattomat verkot uudelleen

Wireless Network Securityn avulla voit nimetä nykyisen suojatun langattoman verkon uudelleen.

Verkon nimeäminen uudelleen voi olla hyödyllistä esimerkiksi silloin, kun naapurisi käyttää täysin tai melkein samannimistä verkkoa, tai jos haluat luoda ainutkertaisen ja helposti tunnistettavan nimen.

Suojattuun langattomaan verkkoon yhteydessä olevat tietokoneet on mahdollisesti yhdistettävä manuaalisesti uudelleen. Saat ilmoituksen, jos verkon nimi muuttuu.



Jos verkko on nimetty uudelleen, uusi nimi ilmestyy Suojattu langaton reititin tai yhteyspiste -ruutuun.

Suojatun langattoman verkon nimen muokkaaminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Kirjoita uusi nimi Verkon suojaus -ruudussa olevaan **Suojatun langattoman verkon nimi** -ruutuun.
- 4 Valitse **Käytä**.

Päivitetään verkkosuojauksen asetukset -valintaikkuna ilmestyy näyttöön, kun Wireless Network Security muuttaa suojatun langattoman verkon nimen. Tietokoneen asetusten ja signaalinvoimakkuuden mukaan verkon nimi muuttuu alle minuutissa.

Huomaa: Turvallisuussyistä McAfee suosittelee, että nimeät reitittimen tai yhteyspisteen SSID-oletustunnuksen uudelleen. Vaikka Wireless Network Security tukee SSID-oletustunnuksia, kuten linksys, belkin54g tai NETGEAR, nimeämällä SSID-tunnukset uudelleen voit suojautua yhteyspisteisiin kohdistuvia uhkia vastaan.

Määritä hälytysasetukset

Wireless Network Securityn avulla voit määrittää hälytysasetukset siten, että hälytykset näytetään tietyissä tilanteissa, kuten esimerkiksi jos uusi tietokone muodostaa yhteyden verkkoon.

Hälytysten toimintatavan määrittäminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Valitse **Hälytysasetukset**.
- 4 Valitse yksi tai useampi seuraavista tapahtumista tai poista niiden valinnat ja valitse sitten **Käytä**:

| Hälytysasetus | Kuvaus |
|--|--|
| Suojatun langattoman verkon verkkoavain on kierrätetty | Näyttää Verkkoavain on kierrätetty -hälytyksen sen jälkeen, kun olet kierrättänyt verkkoavaimen manuaalisesti tai automaattisesti. Avainta kierrättämällä voit estää hakkereita kaappaamasta tietoja ja muodostamasta yhteyttä verkkoon. |
| Toinen suojattu tietokone muodostaa tai katkaisee yhteyden verkkoon | Näyttää Tietokone on muodostanut yhteyden- tai Tietokone on katkaissut yhteyden -hälytyksen sen jälkeen, kun tietokone on muodostanut tai katkaissut yhteyden suojattuun langattomaan verkkoon. Verkossa olevien tietokoneiden tiedot on nyt suojattu tietomurtoja ja tietojen sieppaamista vastaan. |
| Toiselle tietokoneelle myönnetään oikeudet suojatun langattoman verkon käyttöön | Näyttää Tietokoneelle on myönnetty oikeudet verkon käyttöön -hälytyksen sen jälkeen, kun järjestelmänvalvonnasta vastaava tietokone on sallinut toisen tietokoneen liittyä suojattuun langattomaan verkkoon. Myöntämällä tietokoneelle oikeudet suojatun verkon käyttöön voit estää hakkereita kaappaamasta tietoja. |
| Suojatun langattoman verkon avainten kierrätys on keskeytetty tai sitä on jatkettu | Näyttää Avainten kierrätys on keskeytetty- tai Avainten kierrätystä on jatkettu -hälytyksen sen jälkeen, kun olet manuaalisesti keskeyttänyt avainten kierrätyksen tai jatkanut sitä. Avainta kierrättämällä voit estää hakkereita kaappaamasta tietoja ja muodostamasta yhteyttä verkkoon. |
| Kaikkien verkkoyhteyden katkaissien tietokoneiden käyttöoikeudet on evätty | Näyttää Käyttöoikeudet on evätty -hälytyksen sen jälkeen, kun muiden kuin verkossa olevien tietokoneiden käyttöoikeudet on evätty. Verkkoyhteyden katkaissien tietokoneiden on liityttävä uudelleen verkkoon. |
| Suojattuun langattomaan verkkoon on lisätty tai siitä on poistettu reititin | Näyttää Reititin tai yhteyspiste on lisätty verkkoon- tai Reititin tai yhteyspiste on suojaamaton -hälytyksen sen jälkeen, kun suojattuun langattomaan verkkoon on lisätty tai siitä on poistettu reititin. |

| | |
|--|---|
| Suojatun langattoman reitittimen kirjautumistiedot muuttuvat | Näyttää Reitittimen tai yhteyspisteen kirjautumistiedot ovat muuttuneet -hälytyksen sen jälkeen, kun Wireless Network Securityn järjestelmänvalvoja on muuttanut reitittimen tai yhteyspisteen käyttäjänimeä tai salasanaa. |
| Suojatun langattoman verkon nimi tai suojausasetus muuttuu | Näyttää Verkon asetukset ovat muuttuneet- tai Verkko on nimetty uudelleen -hälytyksen sen jälkeen, kun olet nimennyt suojatun langattoman verkon uudelleen tai olet muuttanut sen suojausasetuksia. |
| Suojatun langattoman verkon asetukset on korjattu | Näyttää Verkko on korjattu -hälytyksen sen jälkeen, kun verkon langattomien reitittinten tai yhteyspisteiden suojausasetukset on korjattu. |

Huomaa: Jos haluat valita tai tyhjentää kaikki hälytysasetukset, valitse **Valitse kaikki** tai **Tyhjennä kaikki**. Jos haluat palauttaa Wireless Network Securityn hälytysasetukset, valitse **Palauta oletusasetukset**.

Vastaavat aiheet

- Kierrätä avaimia automaattisesti (sivu 110)
- Liity suojattuun langattomaan verkkoon (sivu 78)
- Muodosta yhteys suojattuihin langattomiin verkkoihin (sivu 82)
- Katkaise yhteys suojattuihin langattomiin verkkoihin (sivu 100)
- Keskeytä avainten automaattinen kierrätys (sivu 113)
- Evää oikeudet verkon käyttöön (sivu 101)
- Poista langattomia reitittimiä tai yhteyspisteitä (sivu 99)
- Muuta langattomien laitteiden käyttöoikeustietoja (sivu 107)
- Nimeä suojatut langattomat verkot uudelleen (sivu 95)
- Korjaa verkon suojausasetukset (sivu 108)

Näytä yhteysilmoitukset

Voit määrittää Wireless Network Securityn ilmoittamaan, kun tietokone muodostaa yhteyden langattomaan verkkoon.

Ilmoituksen näyttäminen, kun muodostat yhteyden langattomaan verkkoon:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Valitse **Muut asetukset**.
- 4 Valitse **Näytä ilmoitusviesti, kun langattomaan verkkoon muodostetaan yhteys**.
- 5 Valitse **Käytä**.

Vastaavat aiheet

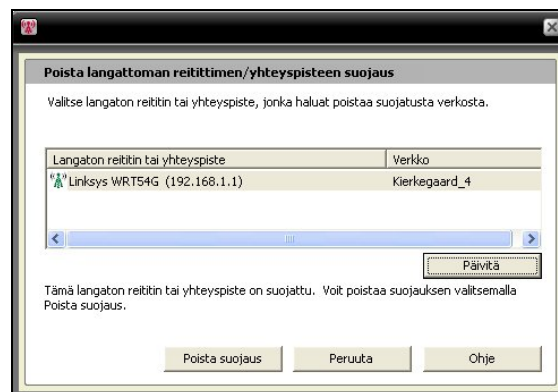
- Muodosta yhteys suojattuihin langattomiin verkkoihin (sivu 82)

Poista langattomia reitittimiä tai yhteyspisteitä

Wireless Network Securityn avulla voit poistaa yhden tai useamman reitittimen tai yhteyspisteen suojatusta verkosta.

Langattoman reitittimen tai yhteyspisteen poistaminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Suojaustyökalut-ruudun **Poista laitteen suojaus**-kohdasta **Poista suojaus**.
- 4 Valitse Poista langattoman reitittimen tai yhteyspisteen suojaus -ruudusta suojatusta verkosta poistettava langaton reititin tai yhteyspiste ja valitse sitten **Poista suojaus**.



- 5 Valitse Langattoman reitittimen tai yhteyspisteen suojaus on poistettu -ruudusta **OK** ja vahvista, että langaton reititin tai yhteyspiste on poistettu verkosta.

Vastaavat aiheet

- Luo suojattuja langattomia verkkoja (sivu 76)

Katkaise yhteys suojattuihin langattomiin verkkoihin

Wireless Network Securityn avulla voit katkaista tietokoneen yhteyden verkkoon.

Tämä on hyödyllistä esimerkiksi silloin, kun tietokoneesi on muodostanut yhteyden verkkoon, joka on samanniminen kuin oma verkkosi. Voit katkaista yhteyden verkkoon ja muodostaa uuden yhteyden omaan verkkoosi.

Tämä toiminto on hyödyllinen myös silloin, kun yhteyspisteen voimakkaan signaalin tai radiohäiriöiden vuoksi muodostat vahingossa yhteyden väärään verkkoon.

Yhteyden katkaiseminen suojattuun langattomaan verkkoon:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä langattomat verkot**.
- 3 Valitse verkko Käytettävissä olevat langattomat verkot -ruudusta ja valitse **Katkaise yhteys**.

Vastaavat aiheet

- Evää oikeudet verkon käyttöön (sivu 101)
- Poistu suojatuista langattomista verkoista (sivu 102)

Evää oikeudet verkon käyttöön

Wireless Network Securityn avulla voit evätä sellaisten tietokoneiden käyttöoikeudet, jotka eivät ole yhteydessä verkkoon. Uusi verkkoavainten kierrätysaikataulu otetaan käyttöön: tietokoneet, jotka eivät ole yhteydessä suojattuun langattomaan verkkoon, menettävät oikeudet sen käyttöön, mutta saavat käyttöoikeudet takaisin liittymällä uudelleen verkkoon. Verkossa olevien tietokoneiden käyttöoikeudet säilyvät.

Wireless Network Securityn avulla voit esimerkiksi evätä vieraan tietokoneen käyttöoikeudet yhteyden katkaisemisen jälkeen. Aikuinen voi myös evätä lapsen käyttämän tietokoneen käyttöoikeudet käyttäessään käytönvalvonta-asetuksia Internet-käytön valvontaan. Tietokoneelle epähuomiossa myönnetty käyttöoikeudet voidaan myös evätä.

Kaikkien suojattuun verkkoon yhteyden katkaisseiden tietokoneiden käyttöoikeuksien evääminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Työkalut-ikkunasta Ylläpitotyökalut.
- 4 Valitse Ylläpitotyökalut-ruudun **Evää käyttöoikeudet** -kohdasta **Evää**.
- 5 Valitse Evää käyttöoikeudet -ruudusta **Evää**.
- 6 Valitse Wireless Network Security -valintaikkunasta **OK**.

Vastaavat aiheet

- Katkaise yhteys suojattuihin langattomiin verkkoihin (sivu 100)
- Poistu suojaetuista langattomista verkoista (sivu 102)

Poistu suojatuista langattomista verkoista

Wireless Network Securityn avulla voit peruuttaa oikeudet suojatun verkon käyttöön.

Poistuminen verkosta:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Valitse Määritä-ruudusta **Muut asetukset**.
- 4 Valitse Muut asetukset -ruudun Suojatun verkon käyttöoikeudet -kohdasta verkko, josta haluat poistua, ja valitse **Poistu verkosta**.
- 5 Poistu verkosta valitsemalla Katkaise yhteys verkkoon -kohdasta **Kyllä**.

Huomaa: Kun poistut verkosta, toisen käyttäjän on myönnettävä sinulle oikeudet suojatun verkon käyttöön, ennen kuin voit liittyä siihen uudelleen.

Vastaavat aiheet

- Katkaise yhteys suojattuihin langattomiin verkkoihin (sivu 100)
- Evää oikeudet verkon käyttöön (sivu 101)

LUKU 16

Langattoman verkon suojauksen hallinta

Wireless Network Security tarjoaa lukuisia työkaluja langattoman verkon suojausominaisuuksien hallintaan.

Tässä luvussa

| | |
|--------------------------------------|-----|
| Suojausasetusten määrittäminen | 104 |
| Verkkoavainten hallinta..... | 109 |

Suojausasetusten määrittäminen

Kun olet muodostanut yhteyden suojattuun langattomaan verkkoon, Wireless Network Security suojaa verkkoa automaattisesti. Voit kuitenkin määrittää uusia suojausasetuksia milloin tahansa.

Suojaustilojen määrittäminen

Voit määrittää suojatun langattoman verkon suojaustilan. Suojaustilat määrittävät tietokoneen ja reitittimen tai yhteyspisteen välisen salauksen.

Kun suojaat verkkosi, WEP-salaus määritetään automaattisesti. McAfee suosittelee kuitenkin, että käytät suojaustilana WPA2- tai WPA-PSK AES -salausta. Wireless Network Security käyttää aluksi WEP-salausta siksi, että kaikki reitittimet ja langattomat verkkosovittimet tukevat tätä tilaa. Useimmat uudet reitittimet ja langattomat verkkosovittimet toimivat kuitenkin turvallisemmassa WPA-tilassa.

Suojatun langattoman verkon suojaustilan muuttaminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Valitse Verkon suojaus -ruudusta suojaustyyppi, jonka haluat ottaa käyttöön **Suojaustila**-ruudusta, ja valitse **Käytä**.

Seuraavassa taulukossa kuvataan käytettävissä olevat suojaustilat:

| Voimakkuus | Tila | Kuvaus |
|-----------------|--------------------------|--|
| Heikoin | WEP | Wired Equivalent Privacy (WEP) kuuluu osana WLAN-standardiin IEEE 802.11, jota käytetään langattomien IEEE 802.11 -verkkojen suojaamiseen. WEP-salauksen suojaustaso on riittävä estämään taitamattoman nuuskinnan, mutta se ei tavallisesti anna yhtä hyvää suojaa kuin WPA-PSK-salaus. Vaikka Wireless Network Securityssa käytetään vahvaa (vaikeasti arvattavaa ja pitkää) avainta, McAfee suosittelee WPA-suojaustilan käyttöä. |
| Keskinkertainen | WPA-PSK TKIP | Wi-Fi Protected Access (WPA) on 802.11i-tietoturvastandardin aikaisempi versio. TKIP-protokolla on suunniteltu WPA-salausta varten, ja sen tarkoituksena on parantaa WEP-salausta. TKIP-protokollan ominaisuuksiin kuuluvat sanoman yhtenäisyyden tarkistus, avainten kierrätysmahdollisuus ja pakettikohtainen avaimen hajautus. |
| Vahva | WPA-PSK AES | Tämä suojaustila yhdistää WPA- ja AES-tilat. Advanced Encryption Standard (AES) on Yhdysvaltain hallituksen käyttämä lohkosalausstandardi. |
| Vahvempi | WPA2- PSK AES | Tämä suojaustila yhdistää WPA2- ja AES-tilat. WPA2 on 802.11i-verkkojen viimeisin tietoturvastandardi. WPA2 käyttää Counter Mode CBC MAC -protokollaa (CCMP), joka on TKIP-salausta turvallisempi ja skaalattavampi ratkaisu. Tämä on vahvin kuluttajien käytettävissä oleva suojaustila. |
| Vahvin | WPA2- PSK TKIP+AES | Tämä suojaustila yhdistää WPA2-, AES ja WPA-PSK TKIP -tilat. Se on muita suojaustiloja joustavampi ratkaisu, johon voidaan liittää sekä vanhat että uudet langattomat verkkosovittimet. |

Huomaa: Suojaustilan muuttamisen jälkeen sinun on mahdollisesti muodostettava yhteys uudelleen.

Vastaavat aiheet

- Korjaa verkon suojausasetukset (sivu 108)
- Näytä verkon suojaustila (sivu 121)

Määritä verkon suojausasetukset

Voit muuttaa Wireless Network Securityn suojaamien verkkojen ominaisuuksia. Tämä on hyödyllistä esimerkiksi silloin, kun haluat päivittää suojauksen WEP-salauksesta WPA-salaukseen.

McAfee suosittelee, että muokkaat verkon suojausasetuksia, jos hälytys kehottaa sinua tekemään niin.

Suojaamattoman verkon ominaisuuksien määrittäminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä langattomat verkot**.
- 3 Valitse Käytettävissä olevat langattomat verkot -ikkunasta **Lisäasetukset**.
- 4 Valitse Langattomat verkot -kohdasta **Asetukset**.
- 5 Muuta seuraavia asetuksia Langattoman verkon ominaisuudet -ruudussa ja valitse sitten **OK**:

| Asetus | Kuvaus |
|-------------------|---|
| Verkko | Verkon nimi. Jos muokkaat verkkoa, et voi muuttaa sen nimeä. |
| Suojaus-asetukset | Suojaamattoman verkon suojaus. Huomaa, että jos langaton verkkosovitin ei tue valittua tilaa, yhteyttä ei voi muodostaa. Suojaustilat ovat seuraavat: Ei käytössä, Avoin WEP, Jaettu WEP, Automaattinen WEP, WPA-PSK, WPA2-PSK. |
| Salaustila | Valitsemaasi suojaustilaan liittyvä salaustila. Salaustilat ovat seuraavat: WEP, TKIP, AES ja TKIP+AES. |

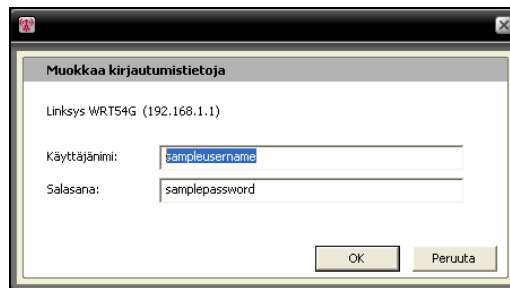
Muuta langattomien laitteiden käyttöoikeustietoja

Voit muuttaa langatonta reititintä tai yhteyspistettä käyttävän laitteen käyttäjänimeä tai salasanaa. Laitteiden luettelo on kohdassa **Suojatun langattoman verkon laitteet**.

McAfee suosittelee, että muutat käyttöoikeustietojasi, sillä useimmissa saman valmistajan langattomissa laitteissa käytetään samoja sisäänkirjautumistietoja. Muuttamalla sisäänkirjautumistietoja voit estää muita käyttämästä langatonta reititintä tai yhteyspistettä sekä muuttamasta niiden asetuksia.

Suojatun langattoman verkon laitteen käyttäjänimen tai salasanan muuttaminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Valitse Verkon suojaus -ruudun **Suojatun langattoman verkon laitteet** -kohdasta langaton reititin tai yhteyspiste ja valitse **Muuta käyttäjänimi tai salasana**.



- 4 Anna kirjautumistietosi ja valitse Wireless Network Security -valintaikkunasta **OK**.

Uusi käyttäjänimi ja salasana ilmestyvät **Suojatun langattoman verkon laitteet** -kohtaan.

Huomaa: Jotkin reitittimet eivät tue käyttäjänimiä, ja siksi käyttäjänimi ei ilmesty **Suojatun langattoman verkon laitteet** -kohtaan.

Korjaa verkon suojausasetukset

Jos sinulla on ongelmia suojausasetusten tai asetusten määrittämisen kanssa, Wireless Network Securityn avulla voit korjata reitittimen tai yhteyspisteen asetukset.

Suojausasetusten korjaaminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Työkalut-ikkunasta **Ylläpitotyökalut**.
- 4 Valitse **Korjaa verkon suojausasetukset** -kohdasta **Korjaa**.
- 5 Valitse Korjaa verkon suojausasetukset -kohdasta **Korjaa**.
Wireless Network Security -hälytys ilmoittaa, onko verkkoa korjattu vai ei.

Huomaa: Jos verkon korjaus epäonnistuu, muodosta yhteys verkkoon kaapelilla ja yritä uudelleen. Jos reitittimen tai yhteyspisteen salasana on muuttunut, salasana on annettava uudelleen yhteyden muodostamiseksi.

Verkkoavainten hallinta

Wireless Network Security luo pitkiä, vahvoja ja satunnaisia salausavaimia satunnaislukugeneraattorin avulla. WEP-salausta käytettäessä avain muunnetaan 26-lukaiseksi heksadesimaaliarvoksi (104 bitille entropiaa eli vahvuutta, joka on 128-bittisen WEP-salauksen enimmäisvahvuus), kun taas WPA-salauksessa avain on 63-merkkinen ASCII-merkkijono. Jokaisella merkillä on 64 mahdollista arvoa (6 bittiä), joissa on entropiaa 384 bittiä. Tämä on enemmän kuin WAP-avaimen 256 bitin vahvuus.

Kun hallitset verkkoavaimia, voit näyttää suojaamattomien yhteyspisteiden avaimet tavallisena tekstinä tai tähtimerkkeinä, hylätä suojaamattomien yhteyspisteiden tallennetut avaimet, ottaa verkkoavainten kierrätyksen käyttöön tai poistaa sen käytöstä, muuttaa avainten kierrätyksen tiheyttä, kierrättää avaimia manuaalisesti ja keskeyttää avainten kierrätyksen.

Kun avaimia kierrätetään automaattisesti, hakkereiden työkalut eivät pysty sieppaamaan tietoja, sillä avain muuttuu jatkuvasti.

Jos yhdistät verkkoon langattomia laitteita (esimerkiksi langattoman kämmentietokoneen), joita Wireless Network Security ei tue, sinun on kirjoitettava avain muistiin, lopetettava avainten kierrätys ja annettava avain laitteessa.

Näytä nykyiset avaimet

Wireless Network Securityn avulla langattoman verkon suojaukseen liittyvät tiedot, kuten suojatun langattoman verkon nykyinen avain, ovat nopeasti käytettävissä.

Nykyisen avaimen näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.
- 3 Valitse Langattoman verkon tila -ruudun Suojattu langaton verkko -ruudusta **Nykyinen avain**.

Verkolle määritetty avain ilmestyy Avaimen määrittäminen -valintaikkunaan.

Vastaavat aiheet

- Näytä avainten kierrätyskertojen määrä (sivu 126)

Kierrätä avaimia automaattisesti

Avainten automaattinen kierrätys otetaan automaattisesti käyttöön. Jos keskeytät avainten kierrätyksen, voit ottaa sen kuitenkin myöhemmin uudelleen käyttöön tietokoneesta, jossa on järjestelmänvalvojan oikeudet.

Voit määrittää Wireless Network Securityn kierrättämään suojatun langattoman verkon verkkoavainta automaattisesti.

Wireless Network Security luo automaattisesti vahvojen avainten jatkuvan sarjan, joka synkronoidaan verkossa. Langaton yhteys voi lyhyesti katketa, kun langaton reititin käynnistyy uudelleen uuden verkkoavaimen määrittämisen jälkeen, mutta verkon käyttäjät tavallisesti havaitsevat tämän.

Jos verkossa ei ole yhtäkään tietokonetta, avainta kierrätetään sen jälkeen, kun ensimmäinen tietokone on muodostanut yhteyden verkkoon.

Avainten automaattisen kierrätyksen ottaminen käyttöön:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Valitse Verkon suojaus -ruudusta **Ota automaattinen avainten kierrätys käyttöön**.
Voit jatkaa avainten kierrätystä myös Langattoman verkon tila -ruudusta.
- 4 Valitse **Käytä**.

Huomaa: Automaattinen avainten kierrätys suoritetaan oletusarvoisesti kolmen tunnin välein, mutta voit säätää avainten kierrätyksen tiheyttä tietoturvaan liittyvien vaatimustesi mukaan.

Vastaavat aiheet

- Säädä avainten kierrätyksen tiheyttä (sivu 111)
- Jatka avainten kierrätystä (sivu 111)
- Näytä avainten kierrätyskertojen määrä (sivu 126)

Jatka avainten kierrätystä

Avainten automaattinen kierrätys otetaan oletusarvoisesti käyttöön. Jos kierrätystoiminto keskeytetään, se voidaan ottaa uudelleen käyttöön tietokoneesta, jossa on järjestelmänvalvojan oikeudet.

Avainten kierrätyksen jatkaminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä tila**.
- 3 Valitse Langattoman verkon tila -kohdasta **Jatka avainten kierrätystä**.

Avainten kierrätys on aloitettu- ja Verkkoavain on kierrätetty -hälytykset vahvistavat, että avainten kierrätys on käynnistetty ja että se onnistui.

Vastaavat aiheet

- Kierrätä avaimia automaattisesti (sivu 110)
- Keskeytä avainten automaattinen kierrätys (sivu 113)
- Näytä avainten kierrätyskertojen määrä (sivu 126)

Säädä avainten kierrätyksen tiheyttä

Jos Wireless Network Security on määritetty kierrättämään suojatun langattoman verkon verkkoavainta automaattisesti, voit säätää kierrätyksen aikavälin 15 minuutin ja 15 päivän välillä.

McAfee suosittelee, että verkkoavainta kierrätetään päivittäin.

Avainten automaattisen kierrätyksen tiheyden säätäminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä ja määritä**.
- 3 Vahvista Verkon suojaus -ruudusta, että avainten automaattinen kierrätys on otettu käyttöön, ja siirrä **Tiheys**-liukusäädin yhteen seuraavista asetuksista:
 - **15 minuutin välein**
 - **30 minuutin välein**
 - **1 tunnin välein**
 - **3 tunnin välein**
 - **12 tunnin välein**
 - **1 päivän välein**

- **7 päivän välein**
- **15 päivän välein**

4 Valitse **Käytä**.

Huomaa: Varmista ennen avainten kierrätyksen tiheyden määrittämistä, että automaattinen avainten kierrätys on otettu käyttöön.

Vastaavat aiheet

- Ota avainten automaattinen kierrätys käyttöön (sivu 110)
- Näytä avainten kierrätyskertojen määrä (sivu 126)

Keskeytä avainten automaattinen kierrätys

Avainten kierrätyksen voi keskeyttää mikä tahansa verkossa oleva tietokone. Avainten kierrätyksen keskeyttäminen saattaa olla tarpeen, kun haluat

- myöntää vieraalle oikeudet verkon käyttöön, ja Wireless Network Security ei ole asennettuna.
- myöntää muulle kuin Windows-järjestelmälle, kuten Macintoshille, Linuxille tai TiVolle, oikeudet verkon käyttöön. Kun lopetat avainten kierrätyksen, laita avain muistiin ja kirjoita se uuteen laitteeseen.
- myöntää tietyille ohjelmille, kuten online-peleille, langaton yhteys, jota avainten kierrätys ei keskeytä.
- Automaattista avainten kierrätystä tulisi jatkaa mahdollisimman pian, jotta verkko olisi täysin suojattu hakkereilta.

Nykyisen avaimen näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä tila**.
- 3 Valitse Langattoman verkon tila -ruudun Suojattu langaton verkko -ruudusta **Nykyinen avain**. Laita Avaimen määritykset -valintaikkunassa näkyvä avain muistiin. Muut tietokoneet, joihin Wireless Network Securitya ei ole asennettu, voivat muodostaa tämän avaimen avulla yhteyden suojattuun langattomaan verkkoon.
- 4 Valitse Avaimen määritykset -valintaikkunasta **Keskeytä avainten kierrätys**.
- 5 Jatka työskentelyä valitsemalla Avainten kierrätys on keskeytetty -valintaikkunasta **OK**.

Varoitus: Jos avainten kierrätystä ei ole keskeytetty, manuaalisesti verkkoon liitetyt yhteensopimattomat laitteet katkaisevat yhteyden verkkoon, kun avainta kierrätetään.

Voit luoda Windows Connect Now -levyn ja kopioida avaimen toiseen tietokoneeseen ja laitteeseen käyttämällä tekstitiedostoa.

Vastaavat aiheet

- Ota avainten automaattinen kierrätys käyttöön (sivu 110)
- Lisää tietokoneita käyttämällä Windows Connect Now -tekniikkaa (sivu 88)
- Jatka avainten kierrätystä (sivu 111)
- Kierrätä avaimia automaattisesti (sivu 110)
- Näytä avainten kierrätyskertojen määrä (sivu 126)

Kierrätä verkkoavaimia manuaalisesti

Wireless Network Securityn avulla voit kierrättää verkkoavainta manuaalisesti myös silloin, kun avainten automaattinen kierrätys on otettu käyttöön.

Verkkoavaimen manuaalinen kierrätys:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse **Näytä työkalut**.
- 3 Valitse Työkalut-ikkunasta **Ylläpitotyökalut**.
- 4 Valitse Ylläpitotyökalut-sivun **Kierrätä verkkoavainta manuaalisesti** -kohdasta **Kierrätä**.

Näyttöön ilmestyy Avainten kierrätys on aloitettu -hälytys ja vahvistaa, että avainten kierrätys on aloitettu. Kun verkkoavain on kierrätetty, näyttöön ilmestyy Verkkoavain on kierrätetty -hälytys ja vahvistaa, että avaimen kierrätys onnistui.

Huomaa: Voit helpottaa verkkoavainten hallintaa ottamalla avainten kierrätyksen Verkon suojaus -ruudussa automaattisesti käyttöön.

Jos langattomassa verkossa ei ole yhtäkään tietokonetta, avainta kierrätetään automaattisesti sen jälkeen, kun ensimmäinen tietokone on muodostanut yhteyden verkkoon.

Vastaavat aiheet

- Ota avainten automaattinen kierrätys käyttöön (sivu 110)
- Säädä avainten kierrätyksen tiheyttä (sivu 111)
- Näytä avainten kierrätyskertojen määrä (sivu 126)

Näytä avaimet tähtimerkkeinä

Avaimet näytetään oletusarvoisesti tähtimerkkeinä, mutta voit määrittää Wireless Network Securityn näyttämään avaimet tavallisena tekstinä verkoissa, jotka eivät ole Wireless Network Securityn suojaamia.

Wireless Network Securityn suojaamissa verkoissa avain näkyy tavallisena tekstinä.

Avainten näyttäminen tähtimerkkeinä:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele määritystä**.
- 3 Valitse **Muut asetukset**.
- 4 Poista **Näytä avaimet tavallisena tekstinä** -ruudun valinta.
- 5 Valitse **Käytä**.

Vastaavat aiheet

- Näytä avaimet tavallisena tekstinä (sivu 116)

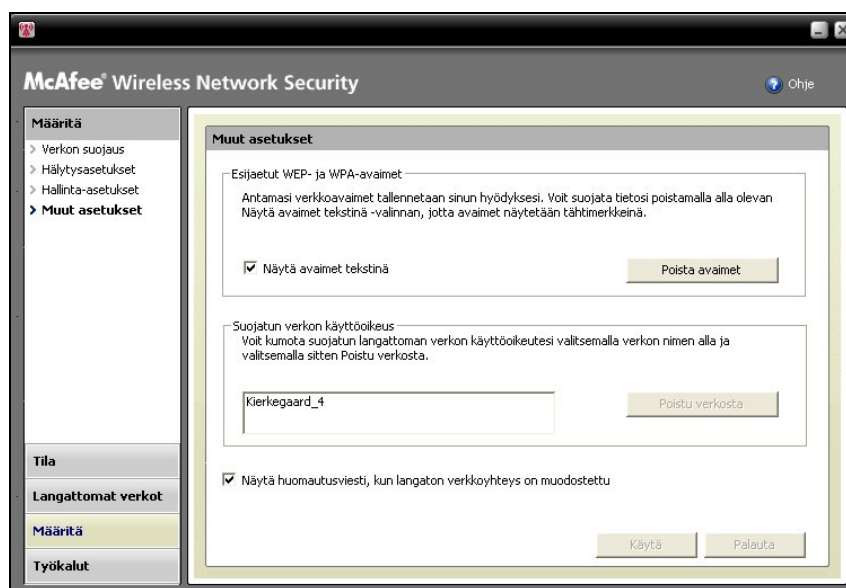
Näytä avaimet tavallisena tekstinä

Avaimet näytetään oletusarvoisesti tähtimerkkeinä, mutta voit määrittää Wireless Network Securityn näyttämään avaimet tavallisena tekstinä verkoissa, jotka eivät ole Wireless Network Securityn suojaamia.

Wireless Network Securityn suojaamissa verkoissa avain näkyy tavallisena tekstinä.

Avainten näyttäminen tavallisena tekstinä:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele määrittystä**.
- 3 Valitse **Muut asetukset**.



- 4 Valitse **Näytä avaimet tavallisena tekstinä** -ruutu.
- 5 Valitse **Käytä**.

Vastaavat aiheet

- Näytä avaimet tähtimerkkeinä (sivu 115)

Poista verkkoavaimet

Wireless Network Security tallentaa esijaetut WEP- ja WPA-avaimet automaattisesti, mutta voit poistaa ne milloin tahansa.

Kaikkien verkkoavainten poistaminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele määritystä**.
- 3 Valitse **Määritä**-ruudusta **Muut asetukset**.
- 4 Valitse **Muut asetukset** -ruudun **Esijaetut WEP- ja WPA-avaimet** -kohdasta **Poista avaimet**.
- 5 Valitse Tyhjennä avaimet -valintaikkunasta **Kyllä**, jos olet varma, että haluat poistaa kaikki tallennetut esijaetut WEP- ja WPA-avaimet.

Varoitus: Jos poistat avaimet, ne poistetaan tietokoneesta lopullisesti. Kun olet poistanut verkkoavaimet, sinun on annettava oikea avain, ennen kuin voit muodostaa yhteyden WEP- ja WPA-verkkoon.

LUKU 17

Langattomien verkkojen valvonta

Wireless Network Securityn avulla voit valvoa langattoman verkon tilaa ja siihen yhteydessä olevia tietokoneita.

Tässä luvussa

| | |
|---|-----|
| Langattomien verkkoyhteyksien valvonta | 120 |
| Suojattujen langattomien verkkojen valvonta | 125 |
| Vianmääritys..... | 131 |

Langattomien verkkoyhteyksien valvonta

Langattoman verkon tila -ruudusta voit tarkastella verkkoyhteyden tilaa, suojaustilaa, nopeutta, kestoaa, signaalinvoimakkuutta ja tietoturvaraporttia.



Seuraavassa taulukossa kuvataan langattomien verkkoyhteyksien tilanilmaisimet.

| Tila | Kuvaus | Tiedot |
|---------------------|---|---|
| Tila | Näyttää, onko tietokone yhteydessä verkkoon ja mihin verkkoon se on yhteydessä. | Näytä yhteyden tila (sivu 121) |
| Suojaus | Näyttää sen verkon suojaustilan, johon olet muodostanut yhteyden. Näytössä näkyy Wireless Network Security, jos olet Wireless Network Securityn suojaama. | Näytä verkon suojaustila (sivu 122) |
| Nopeus | Näyttää verkossa olevan tietokoneen yhteysnopeuden. | Näytä verkon yhteysnopeus (sivu 122) |
| Kesto | Näyttää ajan, jonka tietokone on ollut yhteydessä verkkoon. | Näytä verkkoyhteyden kesto (sivu 122) |
| Signaalinvoimakkuus | Näyttää verkon suhteellisen signaalinvoimakkuuden. | Näytä verkon signaalinvoimakkuus (sivu 124) |
| Tietoturvatarkistus | Valitsemalla Tietoturvatarkistus -asetuksen voit tarkastella tietoturvaan liittyviä tietoja, kuten langattoman verkon tietoturva-aukkoja, suorituskykyä ja langattoman verkon tilaa. | Näytä online-tietoturvaraportti (sivu 124) |

Vastaavat aiheet

- Tietoa Wireless Network Securityn kuvakkeista (sivu 92)

Näytä yhteyden tila

Langattoman verkon tila -ruudussa voit tarkastella langattoman yhteyden tilaa ja tarkistaa, oletko yhteydessä verkkoon vai onko verkkoyhteys katkaistu.

Langattoman yhteyden tilan näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.

Suojatussa langattomassa verkossa olevat tietokoneet sekä kellonaika ja päivämäärä, jolloin kukin tietokone on muodostanut yhteyden verkkoon, on ilmoitettu Langattoman verkon tila -ruudun **Tietokoneet**-kohdassa.

Vastaavat aiheet

- Langattomien verkkoyhteyksien valvonta (sivu 120)
- Näytä verkon suojaustila (sivu 122)
- Näytä verkon yhteysnopeus (sivu 122)
- Näytä verkkoyhteyden kesto (sivu 122)
- Näytä verkon signaalivoimakkuus (sivu 124)
- Näytä online-tietoturvaraportti (sivu 124)

Näytä verkon suojaustila

Langattoman verkon tila -ruudussa voit tarkastella verkkoyhteyden suojaustilaa.

Verkon suojaustilan näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.

Suojaustila näkyy Langattoman verkon tila -ruudun **Suojaus**-ruudussa.

Näytössä näkyy Wireless Network Security, jos langaton verkko on Wireless Network Securityn suojaama.

Vastaavat aiheet

- Langattomien verkkoyhteyksien valvonta (sivu 120)
- Näytä yhteyden tila (sivu 121)
- Näytä verkon yhteysnopeus (sivu 122)
- Näytä verkkoyhteyden kesto (sivu 122)
- Näytä verkon signaalivoimakkuus (sivu 124)
- Näytä online-tietoturvaraportti (sivu 124)

Näytä verkon yhteysnopeus

Langattoman verkon tila -ruudussa voit tarkastella verkon yhteysnopeutta.

Verkon yhteysnopeuden näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.

Yhteysnopeus näkyy Langattoman verkon tila -ruudun **Nopeus**-ruudussa.

Vastaavat aiheet

- Langattomien verkkoyhteyksien valvonta (sivu 120)
- Näytä yhteyden tila (sivu 121)
- Näytä verkon suojaustila (sivu 122)
- Näytä verkkoyhteyden kesto (sivu 122)
- Näytä verkon signaalinvoimakkuus (sivu 124)
- Näytä online-tietoturvaraportti (sivu 124)

Näytä verkkoyhteyden kesto

Langattoman verkon tila -ruudussa voit tarkastella, kuinka kauan olet ollut yhteydessä verkkoon.

Verkkoyhteyden keston näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.

Aika, jonka tietokone on ollut yhteydessä langattomaan verkkoon, näkyy **Kesto**-ruudussa.

Vastaavat aiheet

- Langattomien verkkoyhteyksien valvonta (sivu 120)
- Näytä yhteyden tila (sivu 121)
- Näytä verkon suojaustila (sivu 122)
- Näytä verkon yhteysnopeus (sivu 122)
- Näytä verkon signaalinvoimakkuus (sivu 124)
- Näytä online-tietoturvaraportti (sivu 124)

Näytä verkon signaalivoimakkuus

Langattoman verkon tila -ruudussa voit tarkastella verkon signaalivoimakkuutta.

Signaalivoimakkuuden näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.
Signaalin laatu näkyy **Signaalivoimakkuus**-ruudussa.

Vastaavat aiheet

- Langattomien verkkoyhteyksien valvonta (sivu 120)
- Näytä yhteyden tila (sivu 121)
- Näytä verkon suojaustila (sivu 122)
- Näytä verkon yhteysnopeus (sivu 122)
- Näytä verkkoyhteyden kesto (sivu 122)
- Näytä online-tietoturvaraportti (sivu 124)

Näytä online-tietoturvaraportti

Langattoman verkon tila -ruudussa voit tarkastella langatonta yhteyttä kuvaavaa raporttia ja määrittää, onko yhteys turvallinen vai ei.

McAfee Wi-FiScan -sivustossa on tietoja langattoman verkon tietoturva-aukoista, suorituskyvystä ja langattoman verkon tilasta, mutta se antaa myös suojausratkaisuehdotuksen ja osoittaa, onko yhteytesi suojattu vai ei.

Varmista ennen raportin tarkastelemista, että Internet-yhteytesi toimii.

Verkkoa kuvaavan online-tietoturvaraportin näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.
- 3 Valitse Langattomat verkot -kohdasta **Tietoturvatarkistus**.

Kun selain aukeaa, sinun on ladattava ja asennettava ActiveX-komponentti. Selain saattaa estää hallinnan sen mukaan, mitkä sen asetukset ovat. Salli selaimen ladata komponentti ja aloita tarkistus suorittamalla se. Tarkistamiseen käytettävä aika vaihtelee Internet-yhteyden mukaan.

Huomaa: Lisätietoja ActiveX-komponenttien lataamisesta on selaimen ohjeissa.

McAfeen Wi-FiScan tukee Internet Explorer 5.5:n ja sen uudempien versioiden käyttöä.

Vastaavat aiheet

- Langattomien verkkoyhteyksien valvonta (sivu 120)
- Näytä yhteyden tila (sivu 121)
- Näytä verkon suojaustila (sivu 122)
- Näytä verkon yhteysnopeus (sivu 122)
- Näytä verkkoyhteyden kesto (sivu 122)
- Näytä verkon signaalivoimakkuus (sivu 124)

Suojattujen langattomien verkkojen valvonta

Wireless Network Securityn avulla voit tarkastella Langattoman verkon tila -ruudussa yhteyksien, avainten kierrätysten ja suojattujen tietokoneiden määrää. Voit tarkastella myös verkkotapahtumia, nykyistä avainta ja tällä hetkellä suojattuja tietokoneita.



Seuraavassa taulukossa kuvataan suojattujen langattomien verkkoyhteyksien tilanilmaisimet.

| Tila | Kuvaus | Tiedot |
|-----------------------------------|--|---|
| Avainten kierrätykset tänään | Näyttää suojatun langattoman verkon avainten kierrätyskertojen päivittäisen määrän. | Näytä avainten kierrätyskertojen määrä (sivu 127) |
| Yhteydet tänään | Näyttää suojatun verkon yhteyskertojen päivittäisen määrän. | Näytä päivän aikana muodostettujen yhteyksien määrä (sivu 127) |
| Tässä kuussa suojatut tietokoneet | Näyttää kuluvan kuukauden aikana suojattujen tietokoneiden määrän. | Näytä kuukauden aikana suojattujen tietokoneiden määrä (sivu 127) |
| Verkko-tapahtumat | Napsauttamalla Verkkotapahtumat -vaihtoehtoa voit tarkastella verkkoon, yhteyteen ja avainten kierrätykseen liittyviä tapahtumia. | Näytä suojatun langattoman verkon tapahtumat (sivu 128) |

| | | |
|-------------|---|--|
| Tietokoneet | Näyttää suojatussa langattomassa verkossa olevien tietokoneiden määrän ja ajankohdan, jolloin kukin tietokone on muodostanut yhteyden verkkoon. | Näytä tällä hetkellä suojatut tietokoneet (sivu 129) |
|-------------|---|--|

Näytä avainten kierrätyskertojen määrä

Wireless Network Securityn avulla voit tarkastella suojatussa verkossa suoritettujen avainten kierrätyskertojen määrää ja avaimen edellisen kierrätyskerran ajankohtaa.

Avainten kierrätyskertojen päivittämisen määrän näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.

Yhteyksien kokonaismäärä ja edellinen avainten kierrätyskerta näkyvät Langattoman verkon tila -ruudussa olevan **Suojattu langaton verkko** -kohdan **Avainten kierrätykset tänään** -kentässä.

Vastaavat aiheet

- Suojattujen langattomien verkkojen valvonta (sivu 125)
- Näytä päivän aikana muodostettujen yhteyksien määrä (sivu 127)
- Näytä kuukauden aikana suojattujen tietokoneiden määrä (sivu 127)
- Näytä suojatun langattoman verkon tapahtumat (sivu 128)
- Näytä tällä hetkellä suojatut tietokoneet (sivu 129)
- Verkkoavainten hallinta (sivu 109)
- Kierrätä avaimia automaattisesti (sivu 110)
- Kierrätä verkkoavaimia manuaalisesti (sivu 114)

Näytä päivän aikana muodostettujen yhteyksien määrä

Wireless Network Securityn avulla voit tarkastella suojattuun verkkoon päivän aikana muodostettujen yhteyksien määrää.

Suojatun langattoman verkon yhteyksien näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.
Yhteyksien kokonaismäärä näkyy Langattoman verkon tila -ruudussa olevan **Suojattu langaton verkko** -kohdan **Yhteydet tänään** -kentässä.

Vastaavat aiheet

- Suojattujen langattomien verkkojen valvonta (sivu 125)
- Näytä kuukauden aikana suojattujen tietokoneiden määrä (sivu 127)
- Näytä suojatun langattoman verkon tapahtumat (sivu 128)
- Näytä tällä hetkellä suojatut tietokoneet (sivu 129)

Näytä kuukauden aikana suojattujen tietokoneiden määrä

Wireless Network Securityn avulla voit tarkastella kuluvan kuukauden aikana suojattujen tietokoneiden määrää.

Kuluvan kuukauden aikana suojattujen tietokoneiden määrän näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.
- 3 Kuluvan kuukauden aikana suojattujen tietokoneiden kokonaismäärä näkyy Langattoman verkon tila -ruudussa olevan **Suojattu langaton verkko** -kohdan **Tässä kuussa suojatut tietokoneet** -kentässä.

Vastaavat aiheet

- Suojattujen langattomien verkkojen valvonta (sivu 125)
- Näytä avainten kierrätyskertojen määrä (sivu 127)
- Näytä päivän aikana muodostettujen yhteyksien määrä (sivu 127)
- Näytä suojatun langattoman verkon tapahtumat (sivu 128)
- Näytä tällä hetkellä suojatut tietokoneet (sivu 129)

Näytä suojatun langattoman verkon tapahtumat

Wireless Network Security kirjaa langattoman verkon tapahtumat, kuten sen, milloin verkkoavaimet kierrätetään, milloin muut tietokoneet muodostavat yhteyden McAfeen suojaamaan verkkoon ja milloin muut tietokoneet liittyvät McAfeen suojaamaan verkkoon.

Wireless Network Securityn avulla voit tarkastella verkon tapahtumia kuvaavaa raporttia. Voit määrittää näytettävien tapahtumien tyytit ja lajitella tapahtumatiedot päivämäärän, tapahtuman tai tietokoneen mukaan.

Verkkotapahtumien näyttäminen:

- 1 Napsauta hiiren kakkospainikkeella Windowsin ilmoitusalueella olevaa Wireless Network Security -kuvaketta.
- 2 Valitse jokin seuraavista:

| Toiminto | Toimenpide |
|--|---|
| Näytä verkko-tapahtumat Langattoman verkon tila -ruudussa | 1. Valitse Näytä tila . 2. Valitse Langattoman verkon tila -ruudun Suojattu langaton verkko -ruudusta Verkkotapahtumat . |
| Näytä verkko-tapahtumat Langattoman verkon tila -ruudussa | 1. Valitse Näytä työkalut . 2. Valitse Työkalut-ikkunasta Ylläpitotyökalut . 3. Valitse Ylläpitotyökalut-ruudun Näytä tapahtumaloki -kohdasta Näytä . |

- 3 Valitse näytettäväksi yksi tai useampi seuraavista tapahtumista:
 - **Verkkotapahtumat:** Näyttää tietoja verkon toiminnasta, kuten langattoman reitittimen tai yhteyspisteen suojauksen.
 - **Yhteystapahtumat:** Näyttää tietoja verkkoyhteyksistä, kuten kellonajan ja päivämäärän, jolloin tietokone on muodostanut yhteyden verkkoon.
 - **Avainten kierrätystapahtumat:** Näyttää verkkoavainten kierrätysten päivämäärät ja kellonajat.

4 Valitse **Sulje**.

Vastaavat aiheet

- Suojattujen langattomien verkkojen valvonta (sivu 125)
- Näytä avainten kierrätyskertojen määrä (sivu 127)
- Näytä päivän aikana muodostettujen yhteyksien määrä (sivu 127)
- Näytä päivän aikana muodostettujen yhteyksien määrä (sivu 127)
- Näytä tällä hetkellä suojatut tietokoneet (sivu 129)

Näytä tällä hetkellä suojatut tietokoneet

Voit tarkastella suojatussa langattomassa verkossa olevien tietokoneiden määrää ja ajankohtaa, jolloin kukin tietokone on muodostanut viimeksi yhteyden verkkoon.

Suojattuun verkkoon yhteyden muodostaneiden tietokoneiden tarkasteleminen:

- 1 Napsauta hiiren kakkospainikkeella Wireless Network Security -kuvaketta Windowsin ilmaisinalueella.
- 2 Valitse **Tarkastele tilaa**.
- 3 Suojatussa langattomassa verkossa olevat tietokoneet sekä kellonaika ja päivämäärä, jolloin kukin tietokone on viimeksi muodostanut yhteyden verkkoon, on ilmoitettu Langattoman verkon tila -ruudun **Tietokoneet**-kohdassa.

Vastaavat aiheet

- Suojattujen langattomien verkkojen valvonta (sivu 125)
- Näytä avainten kierrätyskertojen määrä (sivu 127)
- Näytä päivän aikana muodostettujen yhteyksien määrä (sivu 127)
- Näytä kuukauden aikana suojattujen tietokoneiden määrä (sivu 127)
- Näytä suojatun langattoman verkon tapahtumat (sivu 128)

LUKU 18

Vianmääritys

Wireless Securitya ja muiden valmistajien laitteita käytettäessä voit ratkaista seuraavan kaltaisia ongelmia:

- Asennukseen liittyvät ongelmat
- Verkkoa ei voi suojata tai määrittää
- Tietokoneita ei voi liittää verkkoon
- Verkkoon tai Internetiin ei voi muodostaa yhteyttä
- Muut ongelmat

Tässä luvussa

| | |
|--|-----|
| Wireless Network Securityn asentaminen | 132 |
| Verkon suojaaminen tai määrittäminen | 134 |
| Tietokoneiden liittäminen verkkoon | 137 |
| Yhteyden muodostaminen Internetiin ja verkkoon . | 139 |
| Muut ongelmat..... | 144 |

Wireless Network Securityn asentaminen

Voit määrittää seuraavat asennukseen liittyvät ongelmat:

- Mihin tietokoneeseen ohjelmisto on asennettava
- Langatonta verkkosovitinta ei havaita
- Useita langattomia verkkosovittimia
- Langattomiin tietokoneisiin ei voi ladata, sillä verkko on jo suojattu

Mihin tietokoneeseen ohjelmisto on asennettava

Asenna Wireless Network Security jokaiseen verkossa olevaan tietokoneeseen (toisin kuin muut McAfeen ohjelmat, tämän ohjelmiston voi asentaa useampaan tietokoneeseen). Noudata hankitun ohjelmiston käyttöoikeussopimusta. Joissakin tapauksissa on mahdollisesti hankittava lisää käyttöluvia.

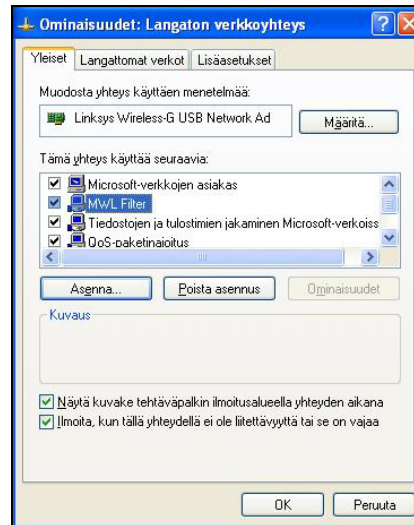
Halutessasi voit asentaa ohjelmiston myös tietokoneisiin, joissa ei ole langatonta verkkosovitinta, mutta ohjelmisto ei ole näissä tietokoneissa aktiivinen, sillä ne eivät tarvitse langatonta suojausta.

Wireless Network Security on tällä hetkellä yhteensopiva Windows XP- ja Windows 2000 -käyttöjärjestelmien kanssa.

Yhteensopivaa langatonta verkkosovitinta ei havaita

Jos langatonta verkkosovitinta ei havaita, kun se asennetaan ja otetaan käyttöön, käynnistä tietokone uudelleen. Jos verkkosovitinta ei havaita senkään jälkeen, kun tietokone on käynnistetty uudelleen, toimi seuraavien ohjeiden mukaan.

- 1 Käynnistä Windowsin Langaton verkkoyhteys -ominaisuusvalintaikkuna.
- 2 Valitse Windowsin perinteisestä Käynnistä-valikosta **Käynnistä**, sitten **Asetukset** ja lopuksi **Verkkoyhteydet**.
- 3 Napsauta **Langaton verkkoyhteys** -kuvaketta.
- 4 Valitse Langattoman verkkoyhteyden tila -valintaikkunasta **Asetukset**.
- 5 Poista Langaton verkkoyhteys -ominaisuusvalintaikkunasta **MWL-suodatin**-kohdan valinta ja valitse se sitten uudelleen.



- 6 Valitse **OK**.

Jos tämä ei ratkaise ongelmaa, suorita WiFi Scan. Jos langattoman verkon tarkistus toimii, verkkosovitin on yhteensopiva. Jos ei, päivitä verkkosovittimen ohjain (käytä Windows Update -palvelua tai käy valmistajan Web-sivustossa) tai osta uusi laite.

Vastaavat aiheet

- Näytä online-tietoturvaraportti (sivu 124)

Useita langattomia verkkosovittimia

Jos saat virhesanoman, että olet asentanut useita langattomia verkkosovittimia, yksi niistä on poistettava käytöstä tai irrotettava. Wireless Home Network Security toimii vain yhdellä langattomalla verkkosovittimella.

Lataus epäonnistuu suojattua verkkoa käytettäessä

Jos sinulla on asennus-CD-levy, asenna Wireless Network Security CD-levyltä kaikkiin langattomiin tietokoneisiin.

Jos asensit ohjelmiston yhteen langattomaan tietokoneeseen ja suojasit verkon, ennen kuin asensit ohjelmiston muihin langattomiin tietokoneisiin, voit valita seuraavista vaihtoehdoista.

- Poista verkon suojaus. Lataa sen jälkeen ohjelmisto ja asenna se kaikkiin langattomiin tietokoneisiin. Suojaa verkko uudelleen.
- Tarkista verkkoavain. Muodosta sen jälkeen yhteys verkkoon kirjoittamalla avain langattomaan tietokoneeseen. Lataa ja asenna ohjelmisto ja liity langattomasta tietokoneesta verkkoon.
- Lataa suoritettava tiedosto tietokoneeseen, joka on jo muodostanut yhteyden verkkoon, ja tallenna se USB flash -asemalle tai kirjoita se CD-levylle, jotta voit asentaa sen muihin tietokoneisiin.
- Suorita Windows Connect Now -tekniikka.

Vastaavat aiheet

- Poista langattomia reitittämiä tai yhteyspisteitä (sivu 99)
- Näytä nykyiset avaimet (sivu 109)
- Lisää tietokoneita käyttämällä siirrettävää laitetta (sivu 86)
- Lisää tietokoneita käyttämällä Windows Connect Now -tekniikkaa (sivu 88)

Verkon suojaaminen tai määrittäminen

Voit ratkaista seuraavat ongelmat, jotka liittyvät verkon suojaamiseen ja määrittämiseen.

- Yhteensopimaton reititin tai yhteyspiste
- Päivitä reitittimen tai yhteyspisteen laiteohjelmisto
- Kahden järjestelmänvalvojan virhe
- Verkko vaikuttaa suojaamattomalta
- Ei voi korjata

Yhteensopimaton reititin tai yhteyspiste

Jos saat virhesanoman, että langaton reititin tai yhteyspiste ei ole yhteensopiva, Wireless Network Security ei ole voinut määrittää laitetta, sillä sitä ei tunnistettu tai löydetty.

Pyydä päivitystä ja varmista, että käytössäsi on Wireless Network Securityn uusin versio (McAfee lisää jatkuvasti uusien reititinten ja yhteyspisteiden tukea). Jos reititin tai yhteyspiste on edelleen yhteensopivien reititinten luettelossa, mutta saat edelleen kyseisen virhesanoman, tietokoneen ja reitittimen tai yhteyspisteen välillä on yhteysvirhe.

Vastaavat aiheet

- Yhteensopivat langattomat reitittimet
<http://www.mcafee.com/router>

Päivitä reitittimen tai yhteyspisteen laiteohjelmisto

Jos saat virhesanoman, että langattoman reitittimen tai yhteyspisteen laiteohjelmisto ei ole yhteensopiva, laite on yhteensopiva, mutta sen laiteohjelmisto ei. Pyydä päivitystä ja varmista, että käytössäsi on Wireless Network Securityn uusin versio (McAfee lisää jatkuvasti uusien laiteohjelmistojen tukea).

Jos käytät Wireless Network Securityn uusinta versiota, tarkista reitittimen tai yhteyspisteen tiedot valmistajan Web-sivustosta tai tukiorganisaatiosta ja asenna yhteensopivien reititinten luettelossa mainittu laiteohjelmisto.

Vastaavat aiheet

- Yhteensopivat langattomat reitittimet
<http://www.mcafee.com/router>

Kahden järjestelmänvalvojan virhe

Kun olet määrittänyt reitittimen tai yhteyspisteen asetukset, sinun on kirjauduttava ulos hallintaliittymästä. Jos et kirjaudu ulos, joissakin tapauksissa reititin tai yhteyspiste käyttäytyy aivan kuin toinen tietokone olisi edelleen määrittämässä sitä, ja saat virhesanoman.

Jos et pysty kirjautumaan ulos, irrota reititin tai yhteyspiste verkosta ja liitä se uudelleen verkkoon.

Avainten kierrätys epäonnistui

Avainten kierrätys epäonnistui seuraavista syistä:

- Reitittimen tai yhteyspisteen kirjautumistiedot ovat muuttuneet.
- Reitittimen tai yhteyspisteen laiteohjelmiston versio on muuttunut versioksi, jota ei tueta.
- Reititin tai yhteyspiste ei ole käytettävissä. Varmista, että reitittimeen tai yhteyspisteeseen on kytketty virta ja että se on liitetty verkkoon.
- Kahden järjestelmänvalvojan virhe.
- Joissakin langattomissa reitittimissä McAfee-asiakas ei välttämättä pysty kierrättämään salausavainta käyttämällä hallintaliittymää, jos toinen tietokone on kirjautunut manuaalisesti langattoman reitittimen Web-liittymään.

Vastaavat aiheet

- Muuta langattomien laitteiden käyttöoikeustietoja (sivu 107)
- Kierrätä avaimia automaattisesti (sivu 110)

Reititintä tai yhteyspistettä ei voi korjata

Jos korjaus epäonnistuu, kokeile seuraavia toimenpiteitä. Huomaa, että toimenpiteet ovat toisistaan riippumattomia.

- Muodosta verkkoyhteys kaapelilla ja yritä korjausta uudelleen.
- Irrota reititin tai yhteyspiste verkosta, liitä se uudelleen verkkoon ja yritä muodostaa yhteys uudelleen.
- Palauta langattoman reitittimen tai yhteyspisteen asetukset ja korjaa se. Tämä palauttaa langattomat asetukset alkuperäisiin asetuksiinsa. Palauta sen jälkeen Internet-yhteyden asetukset.
- Siirry lisäasetuksiin, katkaise kaikista tietokoneista yhteys verkkoon, palauta langattoman reitittimen tai yhteyspisteen asetukset ja suojaa se. Tämä palauttaa langattomat asetukset alkuperäisiin asetuksiinsa. Palauta sen jälkeen Internet-yhteyden asetukset.

Vastaavat aiheet

- Korjaa verkon suojausasetukset (sivu 108)

Verkko vaikuttaa suojaamattomalta

Jos verkko näkyy suojaamattomana, sitä ei ole suojattu. Turvallisuussyistä verkko on suojattava. Huomaa, että Wireless Network Security toimii vain yhteensopivien reititinten ja yhteyspisteiden kanssa.

Vastaavat aiheet

- Luo suojattuja langattomia verkkoja (sivu 76)
- Yhteensopivat langattomat reitittimet
<http://www.mcafee.com/router>

Tietokoneiden liittäminen verkkoon

Voit ratkaista seuraavat ongelmat, jotka liittyvät tietokoneiden liittämiseen verkkoon.

- Odotetaan käyttöoikeuksien todentamista
- Käyttöoikeuksien myöntäminen tuntemattomalle tietokoneelle

Odotetaan käyttöoikeuksien todentamista

Jos yrität liittyä suojattuun verkkoon ja koneesi jää käyttöoikeuksien todentamista odottavaan tilaan, tarkista seuraavat seikat.

- Langaton tietokone, jolla on jo oikeudet verkon käyttöön, kytketään päälle ja liitetään verkkoon.
- Joku läsnäoleva antaa tietokoneelle käyttöoikeudet, kun se ilmestyy näkyviin.
- Tietokoneet ovat toisistaan langattoman kantaman päässä.

Jos **Myönnä käyttöoikeudet** ei ilmesty tietokoneeseen, jolla on jo oikeudet verkon käyttöön, yritä myöntää käyttöoikeudet toisesta tietokoneesta.

Jos muita tietokoneita ei ole käytettävissä, poista verkon suojaus tietokoneesta, jolla on jo käyttöoikeudet, ja suojaa verkko tietokoneesta, jolla ei ole vielä käyttöoikeuksia. Liity sen jälkeen verkkoon tietokoneesta, joka aikaisemmin suojasi verkkoa.

Voit käyttää myös Suojaa toinen tietokone -toimintoa.

Vastaavat aiheet

- Liity suojattuun langattomaan verkkoon (sivu 78)
- Poistu suojatuista langattomista verkoista (sivu 102)
- Poista langattomia reitittäjiä tai yhteyspisteitä (sivu 99)
- Lisää tietokoneita suojattuun langattomaan verkkoon (sivu 86)

Käyttöoikeuksien myöntäminen tuntemattomalle tietokoneelle

Kun saat toisesta tietokoneesta käyttöoikeuksien myöntämistä koskevan pyynnön, evää pyyntö, kunnes pystyt varmistamaan sen aitouden. Joku saattaa yrittää käyttää verkkoa ilman lupaasi.

Yhteyden muodostaminen Internetiin ja verkkoon

Voit ratkaista seuraavat ongelmat, jotka liittyvät yhteyden muodostamiseen verkkoon tai Internetiin.

- Huono Internet-yhteys
- Yhteys katkeaa hetkeksi
- Laitteet (ei tietokone) menettävät yhteyden
- Kehotus antaa WEP-, WPA- tai WPA2-avain
- Yhteyttä ei voi muodostaa
- Päivitä langaton verkkosovitin
- Heikko signaalitaso
- Windows ei voi määrittää langatonta yhteyttä
- Windows näyttää, että yhteyttä ei ole

Internetiin ei voi muodostaa yhteyttä

Jos et pysty muodostamaan yhteyttä, yritä liittyä verkkoon kaapelin avulla ja muodosta Internet-yhteys sen jälkeen. Jos et edelleenkään pysty muodostamaan yhteyttä, tarkista seuraavat seikat:

- Modeemiin on kytketty virta
- PPPoE-asetukset ovat oikein
- DSL- tai kaapeliyhteys on aktiivinen

Langattoman verkon häiriöt voivat aiheuttaa myös yhteysongelmia ja vaikuttaa nopeuteen tai signaalinvoimakkuuteen. Yritä ratkaista ongelma seuraavasti:

- Vaihda langattoman puhelimen kanavaa
- Poista mahdolliset häiriölähteet
- Vaihda langattoman reitittimen, yhteyspisteen tai tietokoneen sijoituspaikkaa
- Vaihda reitittimen tai yhteyspisteen kanavaa. Pohjois- ja Etelä-Amerikassa suositellaan kanavien 1, 4, 7 ja 11 käyttöä. Muissa maissa suositellaan kanavien 1, 4, 7 ja 13 käyttöä. Monet reitittimet on oletusarvoisesti asetettu käyttämään kanavaa 6.
- Varmista, että reititin ja langaton verkkosovitin (erityisesti langaton USB-verkkosovitin) eivät ole seinän vieressä.
- Varmista, että langaton USB-verkkosovitin ei ole langattoman yhteyspisteen tai reitittimen vieressä.
- Sijoita reititin kauas seinistä ja metalliesineistä.

Yhteys on katkennut

Jos yhteys katkeaa hetkeksi (esimerkiksi online-pelin aikana), syynä saattaa olla avainten kierrätys. Voit välttää ongelman estämällä avainten kierrätyksen.

McAfee suosittelee, että jatkat avainten kierrätystä mahdollisimman pian, jotta verkko olisi täysin suojattu hakkereilta.

Vastaavat aiheet

- Kierrätä avaimia automaattisesti (sivu 110)
- Jatka avainten kierrätystä (sivu 111)
- Keskeytä avainten automaattinen kierrätys (sivu 113)
- Kierrätä verkkoavaimia manuaalisesti (sivu 114)

Laitteet menettävät yhteyden

Jos jotkin laitteet menettävät yhteyden, kun käytät Wireless Network Securitya, yritä korjata ongelma seuraavasti:

- Keskeytä avainten kierrätys
- Päivitä langattoman verkkosovittimen ohjain
- Poista verkkosovittimen asiakashallinta

Vastaavat aiheet

- Keskeytä avainten automaattinen kierrätys (sivu 113)

Kehotus antaa WEP-, WPA- tai WPA2-avain

Jos sinun on annettava WEP-, WPA- tai WPA2-avain, jotta voit muodostaa yhteyden suojattuun langattomaan verkkoon, todennäköisesti et ole asentanut ohjelmistoa tietokoneeseen.

Toimiakseen kunnolla Wireless Network Security on asennettava verkon jokaiseen langattomaan tietokoneeseen.

Vastaavat aiheet

- Wireless Network Securityn ottaminen käyttöön (sivu 70)
- Lisää tietokoneita suojattuun langattomaan verkkoon (sivu 86)

Langattomaan verkkoon ei voi muodostaa yhteyttä

Jos et pysty muodostamaan yhteyttä verkkoon, kokeile seuraavia toimenpiteitä. Huomaa, että toimenpiteet ovat toisistaan riippumattomia.

- Jos et ole muodostamassa yhteyttä suojattuun verkkoon, varmista, että sinulla on oikea avain, ja anna se uudelleen.
- Irrota langaton verkkosovitin verkosta ja liitä se uudelleen verkkoon, tai poista se käytöstä ja ota se uudelleen käyttöön.
- Sammuta reititin tai yhteyspiste, käynnistä se uudelleen ja yritä muodostaa yhteys.
- Varmista, että langaton reititin tai yhteyspiste on liitetty, ja korjaa suojausasetukset.
- Käynnistä tietokone uudelleen.
- Päivitä langaton verkkosovitin tai osta uusi. On esimerkiksi mahdollista, että verkkosi käyttää WPA-PSK TKIP -salausta, ja langaton verkkosovitin ei välttämättä tue verkon suojaustilaa (verkkojen asetukseksi näytetään WEP-salaus, vaikka niissä käytetään WPA-salausta).
- Jos et pysty muodostamaan yhteyttä senkään jälkeen, kun olet päivittänyt langattoman reitittimen tai yhteyspisteen, olet mahdollisesti päivittänyt sen versioon, jota ei tueta. Tarkista reitittimen tai yhteyspisteen yhteensopivuus. Jos sitä ei tueta, vaihda se yhteensopivaan versioon tai odota, kunnes Wireless Security -päivitys on saatavilla.

Vastaavat aiheet

- Korjaa verkon suojausasetukset (sivu 108)
- Langattoman verkkosovittimen päivittäminen (sivu 142)

Päivitä langaton verkkosovitin

Wireless Network Securityn käyttö saattaa edellyttää langattoman verkkosovittimen päivittämistä.

Verkkosovittimen päivittäminen:

- 1 Valitse työpöydältä **Käynnistä**, sitten **Asetukset** ja lopuksi **Ohjauspaneeli**.
- 2 Kaksoisnapsauta **Järjestelmä**-kuvaketta. **Ominaisuudet: Järjestelmä** -valintaikkuna ilmestyy näyttöön.
- 3 Valitse **Laitteisto**-välilehti ja sitten **Laitehallinta**.
- 4 Kaksoisnapsauta ohjainta Laitehallinta-luettelossa.
- 5 Valitse **Ohjain**-välilehti ja laita ohjain muistiin.
- 6 Siirry ohjaimen valmistajan sivustoon päivityksen hakemista varten. Ohjaimet löytyvät tavallisesti tuki- tai latausosasta. Jos käytät miniPCI-korttia, siirry tietokoneen (ei kortin) valmistajan sivustoon.
- 7 Jos ohjainpäivitys on saatavilla, lataa se Web-sivuston ohjeiden mukaan.
- 8 Siirry takaisin **Ohjain**-välilehdelle ja valitse **Päivitä ohjain**. Windowsin ohjattu toiminto ilmestyy näyttöön.
- 9 Asenna ohjain Web-sivuston ohjeiden mukaan.

Heikko signaalitaso

Jos yhteys katkeaa tai se on hidas, signaali ei ehkä ole tarpeeksi voimakas. Yritä parantaa signaalia seuraavasti:

- Varmista, että langattomien laitteiden tiellä ei ole metalliesineitä, kuten lämmityslaitteita, putkia tai suuria laitteita. Langattomat signaalit eivät läpäise näitä esineitä hyvin.
- Jos signaali kulkee seinien läpi, varmista, että sen ei tarvitse kulkea loivassa kulmassa. Mitä pidemmän matkan signaalin on kuljettava seinässä, sitä enemmän se heikkenee.
- Jos reitittimelläsi tai langattomalla yhteyspisteelläsi on useampi kuin yksi antenni, yritä suunnata antennit siten, että ne ovat kohtisuoraan toisiaan vasten (esim. toinen ylöspäin ja toinen vaakatasossa, 90 asteen kulmassa toisiinsa nähden).
- Joillakin valmistajilla on vahvistavia antennoja. Suuntaavien antennien toimintasäde on suurempi, kun taas ympärisäteilevät antennit ovat kaikkein joustavimpia. Asenna antenni valmistajan ohjeiden mukaan.

Jos nämä toimenpiteet eivät auta, lisää verkkoon yhteyspiste, joka on lähempänä tietokonetta, johon yrität muodostaa yhteyden. Jos määrität toisen yhteyspisteen samalla verkon nimellä (SSID), mutta eri kanavalle, sovitimesi etsii automaattisesti vahvimman mahdollisen signaalin ja muodostaa yhteyden yhteyspisteeseen, jolla on vahvempi signaali.

Vastaavat aiheet

- Signaalivoimakkuuden kuvakkeet (sivu 93)
- Näytä verkon signaalivoimakkuus (sivu 123)

Windows ei tue langatonta yhteyttä

Jos Windows antaa virhesanoman, että se ei pysty määrittämään langatonta yhteyttä, voit jättää sen huomiotta. Muodosta yhteys langattomiin verkkoihin Wireless Network Securityn avulla ja käytä sitä myös langattomien verkkojen määrittämiseen.

Tarkista Windowsin Langaton verkkoyhteys -ominaisuusvalintaikkunan Langattomat verkot -välilehdeltä, että **Windows määrittää langattoman verkon automaattisesti** -valintaruudun valinta on poistettu.

Wireless Network Security mahdollistaa seuraavat toiminnot:

- Windows 2000 -käyttöjärjestelmää käyttäviin tietokoneisiin asennetut verkkosovittimet voivat muodostaa yhteyden WPA-verkkoihin, vaikka kortin asiakashallintaa ei tueta.
- Windows XP -käyttöjärjestelmää käyttäviin tietokoneisiin asennetut verkkosovittimet voivat muodostaa yhteyden

WPA2-verkkoihin ilman Win XP SP2 -hotfix-korjauksen hakemista ja asentamista.

- Windows XP SP1 -käyttöjärjestelmää käyttävät verkkosovittimet voivat muodostaa yhteyden WPA- ja WPA2-verkkoihin ilman Windows XP SP1:n kanssa yhteensopimattoman hotfix-korjauksen hakemista ja asentamista.

Windows näyttää, että yhteyttä ei ole

Jos olet muodostanut yhteyden, mutta Windowsin verkkokuvake näyttää X (ei yhteyttä), jätä tämä huomiotta. Sinulla on hyvä yhteys.

Muut ongelmat

Voit määrittää seuraavat ongelmat:

- Muita ohjelmia käytettäessä verkolla on toinen nimi
- Ongelmia langattomien reititinten tai yhteyspisteiden määrittämisen kanssa
- Vaihda tietokoneet
- Valitse toinen suojaustila
- Ohjelmisto ei toimi käyttöjärjestelmän päivityksen jälkeen

Muita ohjelmia käytettäessä verkolla on toinen nimi

On normaalia, että verkolla on toinen nimi, kun sitä tarkastellaan muista ohjelmista (esimerkiksi _SafeAaf on osa nimeä).

Wireless Network Security merkitsee suojatut verkot koodilla.

Langattomien reititinten tai yhteyspisteiden määrittäminen

Jos saat virhesanoman, kun olet määrittämässä reitittimen tai yhteyspisteen asetuksia tai olet lisäämässä useita reitittämiä verkkoon, varmista, että kaikilla reitittimillä ja yhteyspisteillä on erillinen IP-osoite.

Jos langattoman reitittimen tai yhteyspisteen nimi näkyy Suojaa langaton reititin tai yhteyspiste -ruudussa, mutta saat virhesanoman sen asetuksia määritettäessä, toimi seuraavasti: Tarkista reitittimen tai yhteyspisteen yhteensopivuus.

Jos reitittimen tai yhteyspisteen asetukset on määritetty, mutta se vaikuttaa olevan väärässä verkossa (et esimerkiksi näe muita lähiverkossa olevia tietokoneita), varmista, että olet määrittänyt oikean etkän esimerkiksi naapurisi reitittimen tai yhteyspisteen asetukset. Irrota reititin tai yhteyspiste verkosta ja varmista, että yhteys katkeaa. Jos olet määrittänyt väärän reitittimen tai yhteyspisteen asetukset, poista sen suojaus ja suoja oikea reititin tai yhteyspiste.

Jos et pysty määrittämään reitittimen tai yhteyspisteen asetuksia tai lisäämään sitä, vaikka se on yhteensopiva, olet mahdollisesti tehnyt muutoksia, jotka estävät sen asetusten oikean määrittämisen.

- Määritä langattoman reitittimen tai yhteyspisteen asetukset DHCP-palvelimelle sopiviksi tai määritä oikea IP-osoite valmistajan ohjeiden mukaan. Joissakin tapauksissa valmistajalta on saatavana määrittäjätyökalu tähän tarkoitukseen.
- Palauta reitittimen tai yhteyspisteen tehdasasetukset ja yritä korjata verkko uudelleen. Olet mahdollisesti muuttanut reitittimen tai yhteyspisteen hallintaporttia tai kytkenyt langattoman hallinnan pois päältä. Varmista, että käytät oletuskokoonpanoa ja että langaton kokoonpano on otettu käyttöön. Toinen mahdollisuus on se, että HTTP-hallinta on poistettu käytöstä. Tarkista tällöin, että HTTP-hallinta on otettu käyttöön. Varmista, että käytät hallintaan porttia 80.
- Jos langaton reititin tai yhteyspiste ei ilmesty niiden langattomien reititinten tai yhteyspisteiden luetteloon, jotka haluat suojata tai joihin haluat muodostaa yhteyden, ota SSID-lähetys käyttöön ja varmista, että näet reitittimen tai yhteyspisteen Wireless Network Securityn käytettävissä olevien langattomien verkkojen luettelossa.
- Jos yhteys katkeaa tai et pysty muodostamaan yhteyttä, MAC-suodatus on ehkä otettu käyttöön. Poista MAC-suodatus käytöstä.
- Jos et pysty suorittamaan verkkotoimintoja (esimerkiksi jakamaan tiedostoja tai tulostamaan jaetuille tulostimille) kahden tietokoneen välillä, joilla on langaton yhteys verkkoon, varmista, että et ole ottanut yhteyspisteen eristämistä käyttöön. Yhteyspisteen eristäminen estää

langattomia tietokoneita muodostamasta verkkoyhteyttä toisiinsa.

- Jos käytät muuta palomuuriohjelmia kuin McAfee Personal Firewallia, varmista aliverkon luotettavuus.

Vastaavat aiheet

- Yhteensopivat langattomat reitittimet
<http://www.mcafee.com/router>

Vaihda tietokoneet

Jos verkkoa aikaisemmin suojannut tietokone on vaihdettu ja jos ei ole muita tietokoneita, joilla on oikeudet verkon käyttöön (eli et pysty käyttämään verkkoa), palauta langattoman reitittimen tai yhteyspisteen tehdasasetukset ja suojaa verkko uudelleen.

Valitse toinen suojaustila

Jos saat virhesanoman, että olet valinnut suojaustilan, jota langaton verkkosovitin ei tue, sinun on valittava toinen suojaustila.

- Kaikki verkkosovittimet tukevat WEP-tilan käyttöä.
- Useimmissa WPA-tilaa tukevissa verkkosovittimissa voit käyttää myös WPA-PSK TKIP- ja WPA-PSK AES -suojaustilaa.
- WPA2-tilaa tukevissa verkkosovittimissa voit käyttää WPA-, WPA2-PSK TKIP-, WPA2-PSK AES- ja WPA2-PSK TKIP/AES -suojaustiloja.

Vastaavat aiheet

- Suojausasetusten määrittäminen (sivu 104)
- Näytä verkon suojaustila (sivu 121)

Ohjelmisto ei toimi käyttöjärjestelmän päivityksen jälkeen

Jos Wireless Network Security ei toimi käyttöjärjestelmän päivityksen jälkeen, poista ohjelmiston asennus ja asenna se uudelleen.

LUKU 19

McAfee EasyNetwork

McAfee® EasyNetwork mahdollistaa suojatun tiedostojen jakamisen, yksinkertaistaa tiedostonsiirtoa ja automatisoi tulostimen jakamisen kotiverkkosi tietokoneiden kesken.

Voit tutustua EasyNetworkin suosituimpiin ominaisuuksiin, ennen kuin alat käyttää sitä. Lisätietoja näiden ominaisuuksien määrittämisestä ja käyttämisestä on EasyNetworkin ohjeessa.

Tässä luvussa

| | |
|--|-----|
| Ominaisuudet..... | 148 |
| EasyNetworkin asentaminen | 149 |
| Tiedostojen jakaminen ja lähettäminen..... | 157 |
| Tulostinten jakaminen..... | 163 |

Ominaisuudet

EasyNetworkissä on seuraavat ominaisuudet.

Tiedostojen jakaminen

EasyNetworkin avulla voit helposti jakaa tietokoneessasi olevia tiedostoja toisiin verkon tietokoneisiin. Kun jaat tiedostoja, myönnät toisille tietokoneille lukuoikeuden kyseisiin tiedostoihin. Vain hallitun verkon jäsentietokoneet (eli täysillä tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja tai lukea toisten jäsentietokoneiden jakamia tiedostoja.

Tiedostonsiirto

Voit lähettää tiedostoja toisiin hallitun verkon jäsentietokoneisiin. Kun vastaanotat tiedoston, se näkyy EasyNetworkin Saapuneet-kansiossa. Saapuneet-kansio on väliaikainen tallennuspaikka kaikille tiedostoille, jotka on lähetetty sinulle toisista verkon tietokoneista.

Automaattinen tulostimen jakaminen

Kun olet liittynyt hallittuun verkkoon, EasyNetwork jakaa automaattisesti tietokoneeseesi liitetyt paikalliset tulostimet ja käyttää jaetun tulostimen nimenä tulostimen nykyistä nimeä. Se havaitsee myös toisten verkon tietokoneiden tulostimet ja sallii niiden tulostimien määrittämisen ja käyttämisen.

LUKU 20

EasyNetworkin asentaminen

Ennen kuin EasyNetworkin ominaisuuksia voi käyttää, ohjelma on käynnistettävä ja hallittuun verkkoon on liityttävä. Liittymisen jälkeen voit poistua verkosta milloin tahansa.

Tässä luvussa

| | |
|---------------------------------------|-----|
| EasyNetworkin käynnistäminen | 150 |
| Hallittuun verkkoon liittyminen | 151 |
| Hallitusta verkosta poistuminen..... | 155 |

EasyNetworkin käynnistäminen

Oletusarvoisesti järjestelmä kehottaa käynnistämään EasyNetworkin heti asennuksen jälkeen, mutta voit käynnistää EasyNetworkin myöhemminkin.

EasyNetworkin käynnistäminen

Oletusarvoisesti järjestelmä kehottaa käynnistämään EasyNetworkin heti asennuksen jälkeen, mutta voit kuitenkin käynnistää EasyNetworkin myöhemminkin.

EasyNetworkin käynnistäminen:

- Valitse **Käynnistä**-valikosta **Ohjelmat, McAfee** ja valitse **McAfee EasyNetwork**.

Vihje: Jos olet luonut asennuksen yhteydessä työpöytä- ja pikakäynnistyskuvakkeet, voit käynnistää EasyNetworkin myös kaksoisnapsauttamalla työpöydällä olevaa McAfee EasyNetwork -kuvaketta tai napsauttamalla tehtäväpalkin oikeassa reunassa sijaitsevalla ilmaisinalueella McAfee EasyNetwork -kuvaketta.

Hallittuun verkkoon liittyminen

SecurityCenterin asentamisen jälkeen tietokoneeseen lisätään taustalla suoritettava verkkoagentti. Verkkoagentti vastaa EasyNetworkissä kelvollisen verkkoyhteyden havaitsemisesta, jaettavien paikallisten tulostimien havaitsemisesta ja verkon tilan valvonnasta.

Ellei verkkoon, johon olet liittynyt, ole liittynyt muita verkkoagenttia suorittavia tietokoneita, järjestelmä tekee sinusta automaattisesti verkon jäsenen ja kehottaa sinua määrittämään, onko verkko luotettava. Ensimmäisenä verkkoon liittyvänä tietokoneena tietokoneesi nimi sisällytetään verkon nimeen. Voit kuitenkin muuttaa verkon nimeä milloin tahansa.

Kun tietokone liittyy verkkoon, kaikille muille verkon tietokoneille lähetetään erillinen liittymispyyntö. Pyyntö voidaan hyväksyä miltä tahansa tietokoneelta, jolla on verkonvalvojan oikeudet. Myöntäjä voi myös määrittää verkkoon liittyvien tietokoneiden oikeuksien tason, esimerkiksi vieraan käyttöoikeudet (vain tiedostonsiirto-oikeus) tai täydet/järjestelmänvalvojan käyttöoikeudet (tiedostonsiirto- ja tiedostonjako-oikeudet). Järjestelmänvalvojojaoikeuksin varustetut tietokoneet voivat myöntää EasyNetworkissä käyttöoikeudet muille tietokoneille ja hallita oikeuksia (eli ylentää tai alentaa tietokoneita). Täysillä käyttöoikeuksilla varustetut tietokoneet eivät voi suorittaa kyseisiä järjestelmänvalvojan tehtäviä. Lisäksi järjestelmä suorittaa tietokoneelle turvallisuustarkastuksen, ennen kuin se voi liittyä verkkoon.

Huomaa: Jos tietokoneeseen on asennettu muita McAfee-verkko-ohjelmia, kuten McAfee Wireless Network Security tai Network Manager, tietokone tunnistetaan hallittavaksi tietokoneeksi myös näiden ohjelmien osalta. Tietokoneelle määritetty oikeuksien taso koskee kaikkia McAfee-verkko-ohjelmia. Lisätietoja vieraan käyttöoikeuksista, täysistä käyttöoikeuksista ja järjestelmänvalvojan käyttöoikeuksista McAfee-verkko-ohjelmissa on ohjelmien mukana toimitetuissa käyttöohjeissa.

Verkkoon liittyminen

Kun tietokone liittyy luotettavaan verkkoon ensimmäistä kertaa EasyNetworkin asentamisen jälkeen, näyttöön tulee kehoitusikkuna, jossa kysytään, haluatko liittyä hallittuun verkkoon. Kun tietokone hyväksyy liittymiskutsun, lähetetään pyyntö kaikille verkon tietokoneille, joilla on järjestelmänvalvojan oikeudet. Pyyntöön tarvitaan hyväksyntä, ennen kuin tietokone voi jakaa tulostimia ja tiedostoja tai lähettää ja kopioida tiedostoja verkossa. Jos tietokone on verkon ensimmäinen tietokone, se saa automaattisesti verkon järjestelmänvalvojan oikeudet.

Verkkoon liittyminen:

- 1 Valitse Jaetut tiedostot -ikkunasta **Kyllä, liity verkkoon nyt**. Kun verkon järjestelmänvalvoja-tietokone hyväksyy pyyntösi, näyttöön tulee viesti, jossa kysytään sallitaanko tämän ja muiden verkon tietokoneiden hallita toistensa suojausasetuksia.
- 2 Jos haluat sallia tietokoneen ja muiden verkon tietokoneiden keskinäisen suojausasetusten hallitsemisen, valitse **Kyllä**, muussa tapauksessa valitse **Ei**.
- 3 Varmista, että myöntävän tietokoneen näytössä näkyvät samat pelikortit kuin suojausvarmistuksen valintaikkunassa ja valitse **Vahvista**.

Huomaa: Jos myöntävän tietokoneen näytössä näkyvät kortit eivät vastaa suojausvarmistuksen valintaikkunassa näkyviä kortteja, hallitun verkon turvallisuus on uhattuna. Verkkoon liittyminen saattaa altistaa tietokoneesi turvallisuusriskeille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää**.

Verkon käyttöoikeuksien myöntäminen

Kun tietokone pyytää oikeutta liittyä hallittuun verkkoon, muille verkon järjestelmänvalvojatietokoneille lähetetään viesti. Ensimmäisenä viestiin vastaavasta tietokoneesta tulee myöntäjä. Myöntäjä päättää tietokoneelle myönnettävän käyttöoikeustyyppin: vieras, täydet oikeudet tai järjestelmänvalvoja.

Verkon käyttöoikeuksien myöntäminen:

- 1 Valitse jokin seuraavista valintaruuduista:
 - **Myönnä vieraan käyttöoikeudet:** Sallii käyttäjän lähettää tiedostoja muihin tietokoneisiin, mutta ei salli tiedostojen jakamista.
 - **Myönnä täydelliset käyttöoikeudet kaikkiin hallitun verkon sovelluksiin:** Sallii käyttäjän lähettää ja jakaa tiedostoja.

- **Myönnä järjestelmänvalvojan käyttöoikeudet kaikkiin hallitun verkon sovelluksiin:** Sallii käyttäjän lähettää ja jakaa tiedostoja, myöntää käyttöoikeuksia toisille tietokoneille ja muuttaa toisten tietokoneiden oikeuksien tasoja.

2 Valitse **Myönnä käyttöoikeudet.**

3 Varmista, että tietokoneen näytössä näkyvät samat pelikortit kuin suojausvarmistuksen valintaikkunassa ja valitse **Vahvista.**

Huomaa: Jos tietokoneen näytössä näkyvät kortit eivät vastaa suojausvarmistuksen valintaikkunassa näkyviä kortteja, hallitun verkon turvallisuus on uhattuna. Käyttöoikeuden myöntäminen kyseiselle tietokoneelle saattaa altistaa tietokoneesi tietoturvariskeille, joten valitse suojausvarmistuksen valintaikkunasta **Hylkää.**

Nimeä verkko uudelleen

Oletusarvoisesti verkon nimi sisältää ensimmäisen siihen liittyneen tietokoneen nimen, mutta voit kuitenkin muuttaa verkon nimeä milloin tahansa. Kun nimeät verkon uudelleen, EasyNetworkissä näkyvä verkon kuvaus muuttuu.

Verkon nimeäminen uudelleen:

- 1 Valitse **Valinnat**-valikosta **Määritä**.
- 2 Kirjoita verkon nimi Määritä-valintaikkunan **Verkon nimi**-ruutuun.
- 3 Valitse **OK**.

Hallitusta verkosta poistuminen

Jos liityt hallittuun verkkoon ja päätät, ettet enää halua kuulua verkkoon, voit poistua verkosta. Voit liittyä verkkoon uudelleen milloin tahansa jäsenyydestäsi luovuttuasi. Tarvitset kuitenkin uuden liittymisluvan ja turvallisuustarkastus suoritetaan uudelleen. Lisätietoja on kohdassa Hallittuun verkkoon liittyminen (sivu 151).

Hallitusta verkosta poistuminen

Voit poistua hallitusta verkosta, johon olet aiemmin liittynyt.

Hallitusta verkosta poistuminen:

- 1** Valitse **Työkalut**-valikosta **Poistu Verkosta**.
- 2** Valitse Poistu verkosta -valintaikkunasta sen verkon nimi, josta haluat poistua.
- 3** Valitse **Poistu verkosta**.

LUKU 21

Tiedostojen jakaminen ja lähettäminen

EasyNetworkin avulla voit helposti jakaa ja lähettää tietokoneessasi olevia tiedostoja toisiin verkon tietokoneisiin. Kun jaat tiedostoja, myönnyt toisille tietokoneille lukuoikeuden kyseisiin tiedostoihin. Vain hallitun verkon jäsentietokoneet (eli täysillä tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja ja lukea toisten jäsentietokoneiden jakamia tiedostoja.

Tässä luvussa

| | |
|--|-----|
| Tiedostojen jakaminen | 158 |
| Tiedostojen lähettäminen toisiin tietokoneisiin..... | 161 |

Tiedostojen jakaminen

EasyNetworkin avulla voit jakaa tietokoneessasi olevia tiedostoja helposti toisiin verkon tietokoneisiin. Kun jaat tiedostoja, myönnyt toisille tietokoneille lukuoikeuden kyseisiin tiedostoihin. Vain hallitun verkon jäsentietokoneet (eli täysillä tai järjestelmänvalvojan oikeuksilla varustetut tietokoneet) voivat jakaa tiedostoja ja lukea toisten jäsentietokoneiden jakamia tiedostoja. Jos jaat kansion, järjestelmä jakaa automaattisesti kaikki kansion sisältämät tiedostot ja alikansiot. Kansioon myöhemmin lisättäviä tiedostoja ei kuitenkaan jaeta. Jos jaettu kansio poistetaan, se poistuu myös Jaetut tiedostot -ikkunasta. Voit lopettaa tiedoston jakamisen milloin tahansa.

Voit käyttää jaettua tiedostoa kahdella tavalla: avaamalla tiedoston suoraan EasyNetworkistä tai kopiaamalla tiedoston tietokoneeseesi ja avaamalla sen sitten. Jos jaettujen tiedostojen luettelo on pitkä, voit hakea jaettua tiedostoa tai tiedostoja, joita haluat käyttää.

Huomautus: EasyNetworkillä jaettuja tiedostoja ei voi käyttää toisesta tietokoneesta käsin Windowsin Resurssienhallinnan avulla. EasyNetworkin tiedostojen jakaminen suoritetaan suojattuja yhteyksiä pitkin.

Tiedoston jakaminen

Kun jaat tiedoston, se on niiden hallitun verkon jäsentietokoneiden saatavilla, joilla on täydet tai järjestelmänvalvojan oikeudet.

Tiedoston jakaminen:

- 1 Etsi Windowsin Resurssienhallinnassa tiedosto, jonka haluat jakaa.
- 2 Vedä tiedosto Windowsin Resurssienhallinnasta EasyNetworkin Jaetut tiedostot -kansioon.

Vihje: Voit jakaa tiedoston myös valitsemalla **Työkalut**-valikosta **Jaa tiedostot**. Siirry Jakaminen-valintaikkunassa kansioon, jossa jaettava tiedosto sijaitsee, valitse tiedosto ja valitse sitten **Jaa**.

Tiedoston jakamisen lopettaminen

Jos jaat tiedostoa hallitussa verkossa, voit lopettaa jakamisen milloin tahansa. Kun lopetat tiedoston jakamisen, toiset hallitun verkon tietokoneet eivät voi enää käyttää sitä.

Tiedoston jakamisen lopettaminen:

- 1 Valitse **Työkalut**-valikosta **Lopeta tiedostojen jakaminen**.
- 2 Valitse Lopeta jakaminen -valintaikkunasta tiedosto, jonka jakamisen haluat lopettaa.
- 3 Napsauta **Älä jaa** -painiketta.

Jaetun tiedoston kopioiminen

Voit kopioida jaettuja tiedostoja mistä tahansa hallitun verkon tietokoneesta omaan tietokoneeseesi. Tällöin käytössäsi on kopio tiedostosta, vaikka tiedostoa jakanut tietokone lopettaisi jakamisen.

Tiedoston kopioiminen:

- Vedä tiedosto EasyNetworkin Jaetut tiedostot -ikkunasta Windowsin Resurssienhallintaan tai Windowsin työpöydälle.

Vihje: Voit kopioida jaetun tiedoston myös valitsemalla sen EasyNetworkissä ja valitsemalla sitten **Työkalut**-valikosta **Kopioi kohteeseen**. Siirry Kopioi kohteeseen -valintaikkunassa kansioon, johon haluat kopioida tiedoston, valitse se ja napsauta **Tallenna**-painiketta.

Jaetun tiedoston hakeminen

Voit hakea tiedostoa, joka on ollut jaettuna joko omassa tietokoneessasi tai jossakin toisessa verkon jäsentietokoneessa. Kun kirjoitat hakuehtoja, Jaetut tiedostot -ikkunassa näkyvät hakuasi vastaavat tulokset.

Jaetun tiedoston hakeminen:

- 1 Valitse Jaetut tiedostot -ikkunasta **Haku**.
- 2 Valitse **Sisältää**-luettelosta jokin seuraavista vaihtoehdoista:
 - **Sisältää sanat:** Hakee tiedostojen tai tiedostopolkujen nimiä, jotka sisältävät kaikki **Tiedoston tai tiedostopolun nimi** -luettelossa määrittämäsi sanat missä tahansa järjestyksessä.
 - **Sisältää minkä tahansa sanoista:** Hakee tiedostojen tai tiedostopolkujen nimiä, jotka sisältävät **Tiedoston tai tiedostopolun nimi** -luettelossa määrittämiäsi sanoja missä tahansa järjestyksessä.

- **Sisältää merkkijonon:** Hakee tiedostojen tai polkujen nimiä, jotka sisältävät **Tiedoston tai tiedostopolun nimi** -luettelossa määrittämäsi koko lauseen.
- 3 Kirjoita tiedoston tai tiedostopolun nimi osittain tai kokonaan **Tiedoston tai tiedostopolun nimi** -luetteloon.
 - 4 Valitse **Tyyppi**-luettelosta jokin seuraavista tiedostotyypeistä:
 - **Mikä tahansa:** Hakee kaikkia jaettuja tiedostotyyppisiä.
 - **Asiakirja:** Hakee kaikkia jaettuja asiakirjoja.
 - **Kuvatiedosto:** Hakee kaikkia jaettuja kuvatiedostoja.
 - **Videoleike:** Hakee kaikkia jaettuja videoleiketiedostoja.
 - **Äänitiedosto:** Hakee kaikkia jaettuja äänitiedostoja.
 - 5 Valitse **Mistä**- ja **Mihin**-luetteloiden avulla aikaväli, jonka aikana tiedosto on luotu.

Tiedostojen lähettäminen toisiin tietokoneisiin

Voit lähettää tiedostoja toisiin hallitun verkon jäsentietokoneisiin. Ennen tiedoston lähettämistä EasyNetwork tarkistaa, että vastaanottavassa tietokoneessa on riittävästi vapaata levytilaa.

Kun vastaanotat tiedoston, se näkyy EasyNetworkin Saapuneet-kansiossa. Saapuneet-kansio on väliaikainen tallennuspaikka kaikille toisista verkon tietokoneista sinulle lähetetyille tiedostoille. Jos EasyNetwork on auki, kun vastaanotat tiedoston, tiedosto näkyy heti Saapuneet-kansiossa. Muussa tapauksessa viesti näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla Windowsin ilmaisinalueella. Jos et halua nähdä vastaanoton ilmoitusviestejä, voit ottaa ne pois käytöstä. Jos Saapuneet-kansiossa on jo samanniminen tiedosto, uuden tiedoston nimen perään lisätään numeerinen erotin. Tiedostot säilyvät Saapuneet-kansiossa, kunnes hyväksyt ne (eli kopioit ne tietokoneeseesi).

Tiedoston lähettäminen toiseen tietokoneeseen

Voit lähettää tiedoston suoraan toiseen hallitun verkon tietokoneeseen jakamatta sitä. Ennen kuin vastaanottavan tietokoneen käyttäjä voi katsella tiedostoa, se täytyy tallentaa paikalliseen sijaintiin. Lisätietoja on kohdassa Tiedoston hyväksyminen toisesta tietokoneesta (sivu 162).

Tiedoston lähettäminen toiseen tietokoneeseen:

- 1 Etsi Windowsin Resurssienhallinnassa tiedosto, jonka haluat lähettää.
- 2 Vedä tiedosto Windowsin Resurssienhallinnasta EasyNetworkissä aktiivisena olevan tietokoneen kuvakkeen päälle.

Vihje: Voit lähettää tietokoneeseen useita tiedostoja painamalla CTRL-näppäintä tiedostoja valitessasi. Voit lähettää tiedostoja myös valitsemalla **Työkalut**-valikosta **Lähetä**, valitsemalla tiedostot ja napsauttamalla sitten **Lähetä**-painiketta.

Tiedoston hyväksyminen toiselta tietokoneelta

Jos toinen hallitun verkon tietokone lähettää sinulle tiedoston, sinun täytyy hyväksyä se (tallentamalla se johonkin tietokoneessasi olevaa kansioon). Jos EasyNetwork ei ole auki tai näkyvässä kun tietokoneeseesi lähetetään tiedosto, saat ilmoitusviestin, joka näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla Windowsin ilmaisinalueella. Avaa EasyNetwork napsauttamalla ilmoitusviestiä, niin pääset käyttämään tiedostoa.

Tiedoston vastaanottaminen toisesta tietokoneesta:

- Napsauta **Vastaanotettu**-painiketta ja vedä tiedosto EasyNetworkin Saapuneet-kansiosta Windowsin Resurssienhallinnan kansioon.

Vihje: Voit vastaanottaa tiedoston toisesta tietokoneesta myös valitsemalla tiedoston EasyNetworkin Saapuneet-kansiosta ja valitsemalla sitten **Työkalut**-valikosta **Hyväksy**. Siirry Hyväksy kansioon -valintaikkunassa siihen kansioon, johon haluat tallentaa vastaanottamasi tiedostot, valitse se ja napsauta **Tallenna**-painiketta.

Ilmoituksen saaminen tiedoston lähettämisestä

Voit saada ilmoituksen, kun toinen hallitun verkon tietokone lähettää sinulle tiedoston. Jos EasyNetwork ei ole auki tai se ei ole näkyvässä, ilmoitusviesti näkyy tehtäväpalkin oikeassa reunassa sijaitsevalla Windowsin ilmaisinalueella.

Ilmoituksen saaminen tiedoston lähettämisestä:

- 1 Valitse **Valinnat**-valikosta **Määritä**.
- 2 Valitse Määritä-valintaruudusta **Ilmoita, kun joku toinen tietokone lähettää tiedostoja** -valintaruutu.
- 3 Valitse **OK**.

LUKU 22

Tulostinten jakaminen

Kun olet liittynyt hallittuun verkkoon, EasyNetwork jakaa automaattisesti tietokoneeseesi liitetyt paikalliset tulostimet. Lisäksi se havaitsee toisten verkon tietokoneiden tulostimet ja sallii kyseisten tulostimien määrittämisen ja käyttämisen.

Tässä luvussa

Jaettujen tulostinten käyttäminen 164

Jaettujen tulostinten käyttäminen

Kun olet liittynyt hallittuun verkkoon, EasyNetwork jakaa automaattisesti tietokoneeseesi liitetyt paikalliset tulostimet ja käyttää jaetun tulostimen nimenä tulostimen nykyistä nimeä. Lisäksi se havaitsee toisten verkon tietokoneiden tulostimet ja sallii kyseisten tulostimien määrittämisen ja käyttämisen. Jos olet määrittänyt tulostinohjaimen tulostamaan verkon tulostuspalvelimen kautta (esimerkiksi langaton USB-tulostuspalvelin), EasyNetwork tulkitsee tulostimen paikalliseksi tulostimeksi ja jakaa sen verkossa. Voit lopettaa tulostimen jakamisen milloin tahansa.

EasyNetwork havaitsee myös kaikkien muiden verkon tietokoneiden jakamat tulostimet. Jos se havaitsee etätulostimen, jota ei ole vielä kytketty tietokoneeseesi, Jaetut tiedostot -ikkunassa näkyy **Saatavilla olevat verkkotulostimet** -linkki, kun avaat EasyNetworkin ensimmäisen kerran. Sen avulla voit asentaa saatavilla olevia tulostimia tai poistaa tietokoneeseen jo kytkettyjen tulostimien asennuksia. Voit myös päivittää verkossa havaittujen tulostimien luettelon.

Jos et ole vielä liittynyt hallittuun verkkoon, mutta olet kytkeytynyt siihen, voit käyttää jaettuja tulostimia Windowsin Ohjauspaneelin kautta.

Tulostimen jakamisen lopettaminen

Voit lopettaa tulostimen jakamisen milloin tahansa. Jäsenet, jotka ovat asentaneet tulostimen, eivät voi enää tulostaa sillä.

Tulostimen jakamisen lopettaminen:

- 1 Valitse **Työkalut**-valikosta **Tulostimet**.
- 2 Valitse Hallitse tulostimia -valintaikkunasta sen tulostimen nimi, jonka jakamisen haluat lopettaa.
- 3 Napsauta **Älä jaa** -painiketta.

Saatavilla olevan verkkotulostimen asentaminen

Hallitun verkon jäsenenä voit käyttää verkon jaettuja tulostimia. Ennen käyttöä on asennettava kyseisen tulostimen käyttämä tulostinohjain. Jos tulostimen omistaja lopettaa tulostimen jakamisen sen jälkeen kun olet asentanut sen, et voi enää tulostaa kyseisellä tulostimella.

Saatavilla olevan verkkotulostimen asentaminen:

- 1** Valitse **Työkalut**-valikosta **Tulostimet**.
- 2** Valitse tulostimen nimi Saatavilla olevat verkkotulostimet -valintaikkunasta.
- 3** Napsauta **Asenna**-painiketta.

L U K U 23

Liitteet

Termisanasto luettelee ja määrittää McAfee-tuotteissa useimmin käytetyt tietoturvatерmit.

Tietoja McAfeesta -sivu sisältää lakeihin liittyvää tietoa McAfee Corporationista.

Sanasto

8

802.11

Kokoelma langattoman lähiverkkotekniikan IEEE-standardeja. 802.11 määrittää langattoman asiakkaan ja tukiaseman tai kahden langattoman asiakkaan välisen maanpäällisen jakeluliittymän. 802.11 sisältää useita eri määrittämiä, kuten 802.11a-standardin, jonka avulla voidaan käyttää jopa 54 Mbps verkkoyhteyksiä 5 Ghz kaistassa, 802.11b-standardin, jonka avulla voidaan käyttää jopa 11 Mbps verkkoyhteyksiä 2,4 Ghz kaistassa, 802.11g-standardin, jonka avulla voidaan käyttää jopa 54 Mbps verkkoyhteyksiä 2,4 Ghz kaistassa sekä 802.11i:n, joka on kokoelma erilaisia Ethernet-verkkojen suojausstandardeja.

802.11a

802.11-standardin laajennus, jota käytetään langattomissa lähiverkoissa ja jonka avulla tietoa voidaan siirtää jopa 54 Mbps nopeudella 5 Ghz kaistassa. Vaikka tiedonsiirron nopeus on suurempi kuin 802.11b-standardissa, laajennuksen kantoalue on paljon pienempi.

802.11b

802.11-standardin laajennus, jota käytetään langattomissa lähiverkoissa ja jonka avulla tietoa voidaan siirtää jopa 11 Mbps nopeudella 2,4 Ghz kaistassa. 802.11b on tällä hetkellä yleisimmin käytetty langattoman tiedonsiirron standardi.

802.11g

802.11-standardin laajennus, jota käytetään langattomissa lähiverkoissa ja jonka avulla tietoa voidaan siirtää jopa 54 Mbps nopeudella 2,4 Ghz kaistassa.

802.1x

Wireless Home Network Security ei tue tätä standardia. Tavallisten ja langattomien verkkojen IEEE-todennusstandardi, jota käytetään useimmiten 802.11-standardin langattomien verkkoyhteyksien yhteydessä. Tämä standardi tarjoaa vahvan, molemminpuolisen todennuksen asiakkaan ja todennuspalvelimen välillä. Lisäksi 802.1x tarjoaa dynaamisen käyttäjä- ja istuntokohtaisen WEP-avaimen, joka poistaa staattisia WEP-avaimia käyttävien verkkojen hallintavaatimukset ja turvallisuusriskit.

A

arkistointi

Tarkkailtavien tiedostojen varmuuskopiointi paikallisesti CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevyasemalle tai verkkoasemalle.

arkistointi

Tarkkailtavien tiedostojen varmuuskopiointi paikallisesti CD- tai DVD-levylle, USB-asemalle, ulkoiselle kiintolevyasemalle tai verkkoasemalle.

asiakas

Sovellus, joka toimii henkilökohtaisessa tietokoneessa tai työasemassa ja käyttää palvelinta tiettyjen toimintojen suorittamiseen. Esimerkiksi sähköpostiasiakas on sovellus, jonka avulla voit lähettää ja vastaanottaa sähköpostia.

avain

Kirjaimista ja/tai numeroista muodostuva sarja, jota kaksi laitetta käyttävät niiden välisen viestinnän todentamiseen. Molemmilla laitteilla täytyy olla sama avain. Katso myös kohdat WEP, WPA, WPA2, WPA-PSK ja WPA2-PSK.

avainsana

Sana, jonka avulla voidaan määrittää varmuuskopioidun tiedoston suhde tai yhteys muihin tiedostoihin, joille on määritetty sama avainsana. Avainsanojen määrittäminen tiedostoille tekee Internetissä julkaistujen tiedostojen etsimisestä helpompaa.

D

DNS

Akronyymi, joka tulee sanoista Domain Name System (toimialueen nimijärjestelmä). Hierarkkinen järjestelmä, jossa Internetin isännillä on sekä toimialueen nimiosoite (kuten bluestem.prairienet.org) että IP-osoite (kuten 192.17.3.4). Käyttäjät käyttävät toimialueen nimiosoitetta ja se käännetään automaattisesti numeeriseksi IP-osoitteeksi, jota käyttävät pakettien reititysohjelmistot. DNS-nimet muodostuvat päätason toimialueesta (kuten .com, .org ja .net), alemman tason toimialueesta (yrityksen, yhteisön tai henkilön sivuston nimi) ja mahdollisesti yhdestä tai useammasta alitoimialueesta (alemman tason toimialueen palvelimet). Katso myös kohdat DNS-palvelin ja IP-osoite.

DNS-palvelin

Toimialueen nimijärjestelmäpalvelimen lyhenne. Tietokone, joka vastaa toimialueen nimi (DNS) -pyyntöihin. DNS-palvelin ylläpitää tietokantaa isäntätietokoneista ja niiden IP-osoitteista. Jos DNS-palvelimeen lähetetään pyyntö esimerkiksi nimellä apex.com, palvelin palauttaa Apex-yhtiön IP-osoitteen. DNS-palvelin tunnetaan myös nimellä nimipalvelin. Katso myös kohdat DNS ja IP-osoite.

E

eristäminen

Kun epäilyttävä tiedosto tunnistetaan, se asetetaan eristykseen. Voit sitten suorittaa asianmukaisen toiminnon.

ESS (laajennettu palvelukokoelma)

Kahden tai useamman verkon kokoelma, joka muodostaa yhtenäisen aliverkon.

eväste

Webissä käytettävä tietolohko, jonka Web-palvelin tallentaa asiakasjärjestelmään. Kun käyttäjä palaa samaan Web-sivustoon, selain lähettää evästeen kopion takaisin palvelimeen. Evästeitä käytetään käyttäjien tunnistamiseen, palvelimen ohjaamiseen, jotta se lähettää mukautetun version pyydetystä Web-sivusta, käyttäjän tilitietojen lähettämiseen ja muihin hallinnollisiin käyttötarkoituksiin.

Evästeiden avulla Web-sivustot muistavat kuka sinä olet ja pitävät kirjaa siitä, kuinka paljon vierailijoita Web-sivustossa on käynyt, milloin he ovat vierailleet ja mitä sivuja he ovat näyttäneet. Evästeet auttavat myös yrityksiä mukauttamaan Web-sivustonsa sinua varten. Useat Web-sivustot vaativat käyttäjänimeä ja salasanaa tiettyjen sivujen käyttämiseen, ja lähettävät evästeen tietokoneeseesi, jotta sinun ei tarvitse kirjautua sisään jokaisella vierailukerralla. Evästeitä voidaan kuitenkin käyttää myös haitallisiin käyttötarkoituksiin. Internetin mainosyritykset käyttävät usein evästeitä päätelläkseen mitä sivustoja sinä käytät useimmiten ja julkaisevat sitten mainoksia suosikki-Web-sivustoissasi. Ennen kuin hyväksyt sivuston evästeet, varmista, että sivusto on luotettava.

Vaikka evästeet ovat monen laillisen yrityksen tietolähde, ne voivat olla myös hakkereiden tietolähde. Useat verkkokauppoja sisältävät Web-sivustot laittavat luottokortti- ja muita henkilökohtaisia tietoja evästeisiin, jotta asiakkaiden on helpompi tehdä ostoksia. Valitettavasti evästeet saattavat sisältää tietoturva-aukkoja, joiden avulla hakkerit voivat päästä käsiksi asiakkaiden tietokoneisiin tallennettujen evästeiden sisältämiin tietoihin.

H

hallittu verkko

Kotiverkko, jossa on kahdentyypisiä jäseniä: hallittuja jäseniä ja hallinnan piiriin kuulumattomia jäseniä. Hallitut jäsenet sallivat muiden verkon tietokoneiden valvoa McAfee-suojastasoan, hallinnan piiriin kuulumattomat eivät.

I

Internet

Internet sisältää valtavan määrän toisiinsa liitettyjä verkkoja, jotka käyttävät TCP/IP-protokollaa tiedonsiirtoon ja etsimiseen. Internet perustuu Yhdysvaltojen puolustusministeriön 1960-luvun lopulla ja 1970-luvun alussa rahoittamaan yliopistojen ja korkeakoulujen tietokoneiden muodostamaan verkkoon, jota kutsuttiin ARPANET:ksi. Tänä päivänä Internet on maailmanlaajuinen verkko, joka sisältää lähes 100 000 itsenäistä verkkoa.

Intranet

Yleensä organisaation sisäinen yksityinen verkko, joka toimii samalla tavoin kuin Internet. Nykyinen käytäntö on, että opiskelijat ja työntekijät voivat muodostaa Intranet-yhteyden kampusten ja yritysten tilojen ulkopuolelta. Palomuurit, sisäänkirjautumistoiminnot ja salasanat ovat suunniteltu järjestelmien suojaamiseksi.

IP-huijausyritys

IP-paketin IP-osoitteiden väärentäminen. Tätä huijauskeinoa käytetään useissa erilaisissa hyökkäyksissä, kuten istunnon kaappauksissa. Sitä käytetään usein myös roskapostiviestien otsikoiden väärentämiseen, jotta viestejä ei voida jäljittää.

IP-osoite

Internet-protokollaosoite tai IP-osoite on ainutkertainen numerosarja, joka koostuu neljästä pistein eritellystä osasta (esim. 63.227.89.66). Jokaisella Internetin tietokoneella aina suurimmasta palvelimesta matkapuhelimen kautta verkkoyhteyttä käyttävään kannettavaan tietokoneeseen on oma yksilöivä IP-osoitteensa. Kaikilla tietokoneilla ei ole toimialueen nimeä, mutta jokaisella tietokoneella on IP-osoite.

Seuraava luettelo sisältää muutamia epätavallisia IP-osoitetyyppejä:

- **Reitittämättömät IP-osoitteet:** Näitä IP-osoitteita kutsutaan myös henkilökohtaiseksi IP-tilaksi. Näitä osoitteita ei voi käyttää Internetissä. Yksityiset IP-osoitelohkot ovat 10.x.x.x, 172.16.x.x - 172.31.x.x ja 192.168.x.x.
- **Silmukka-IP-osoitteet:** Silmukkaosoitteita käytetään testitarkoituksiin. Tähän IP-osoitelohkoon lähetetty tietoliikenne palautuu suoraan takaisin paketin luoneeseen laitteeseen. Se ei koskaan poistu laitteesta ja sitä käytetään pääasiassa laitteistojen ja ohjelmistojen testaamiseen. Silmukka-IP-osoitelohko on 127.x.x.x.

Tyhjä IP-osoite: Tämä on virheellinen osoite. Kun tämä osoite näkyy, se viittaa siihen, että tietoliikenteellä on tyhjä IP-osoite. On itsestään selvää, että tämä ei ole tavallista, ja se useimmiten viittaa siihen, että liikenteen lähettäjä yrittää tahallaan salata tietoliikenteen lähdeosoitetta. Lähettäjä ei voi vastaanottaa vastauksia tietoliikenteeseen, ellei pakettia vastaanota sovellus, joka pystyy ymmärtämään paketin sisällön ja tulkitsemaan kyseistä sovellusta koskevia yksityiskohtaisia ohjeita. Mikä tahansa IP-osoite, joka alkaa nolllalla (0.x.x.x) on tyhjä IP-osoite. Esimerkiksi 0.0.0.0 on tyhjä IP-osoite.

J

jaettu salaisuus

Katso myös kohta RADIUS. Suojaa RADIUS-viestien arkaluontoisia osia. Jaettu salaisuus on salasana, jonka todentaja ja todennuspalvelun jakavat jollakin suojatulla keinolla.

jakaminen

Toiminto, jonka avulla sähköpostiviestin vastaanottajat voivat ladata varmuuskopioituja tiedostoja rajoitetun ajanjakson aikana. Kun tiedosto jaetaan, lähetetään tiedoston varmuuskopioitu versio sähköpostiviestin vastaanottajille. Viestin vastaanottajat saavat sähköpostiviestin McAfee Data Backupilta, jossa heille kerrotaan jaettavista tiedostoista. Sähköpostiviesti sisältää linkin, josta jaettavat tiedostot voidaan ladata.

julkaiseminen

Varmuuskopioidun tiedoston julkaiseminen Internetissä.

K

kaistanleveys

Tiedon määrä, joka voidaan siirtää tietyssä ajassa. Digitaalisten laitteiden kaistanleveys ilmoitetaan useimmiten bitteinä per sekunti (bps) tai tavuina per sekunti. Analogisten laitteiden kaistanleveys ilmoitetaan värähdyksinä sekunnissa tai hertseinä (Hz).

kieltoluettelo

Haitallisten Web-sivustojen luettelo. Web-sivusto voidaan sijoittaa kieltoluetteloon, jos se sisältää petollisia toimintoja tai yrittää käyttää hyväkseen selaimen tietoturva-aukkoja lähettääkseen mahdollisia haittaohjelmia käyttäjän tietokoneeseen.

kirjasto

Data Backup -käyttäjien julkaisemien tiedostojen online-talennealue. Kirjasto on Internetin Web-sivusto, jota voi käyttää kuka tahansa Internet-käyttäjä.

komentosarja

Komentosarjat voivat luoda, kopioida tai poistaa tiedostoja. Ne voivat avata myös Windowsin rekisterin.

kuva-analyysi

Estää mahdollisesti sopimattomia kuvia tulemasta näkyville. Kuvat estetään kaikilta muilta käyttäjiltä, paitsi aikuisikäryhmän jäseniltä.

Käyttöpiste

Verkkolaite, jonka avulla 802.11-standardia käyttävät asiakkaat voivat muodostaa yhteyden lähiverkkoon. Käyttöpisteet laajentavat langattoman verkon käyttöaluetta. Käyttöpisteitä kutsutaan joskus myös langattomiksi reitittimiksi.

käytönvalvonta-asetukset

Käytönvalvonta-asetuksilla voit määrittää sisältöluokitukset Web-sivustoille ja sisällöille, joita käyttäjä voi katsella, sekä rajoittaa Internet-käytön ajankohtaa ja kestoja. Käytönvalvonta-asetuksilla voit myös rajoittaa käyttäjien pääsyä Web-sivustoihin ja sallia tai estää käytön ikäryhmien käyttöoikeuksien tai salasanojen perusteella.

L

Langaton lähiverkko (WLAN)

Katso myös kohta Lähiverkko. Lähiverkko, johon voidaan muodostaa langaton yhteys. Lähiverkko käyttää korkeataajuuksisia radioaaltoja johtojen sijaan solmujen väliseen viestintään.

langaton verkkopiste

Tietty maantieteellinen sijainti, jossa mobiileja yhteyksiä käyttävät vierailijat voivat käyttää julkisia langattomia laajakaistaverkkopalveluja langattoman käyttöpisteen avulla. Langattomat verkkopisteet (hotspots) sijaitsevat usein suuria ihmismääriä sisältävissä paikoissa kuten lentokentillä, rautatieasemilla, kirjastoissa, satamissa, messukeskuksissa ja hotelleissa. Langattomat verkkopisteet toimivat tavallisesti hyvin rajoitetulla käyttöalueella.

langaton verkkosovitin

Sisältää vaadittavat virtapiirit, joiden avulla tietokone tai muu laite voi keskustella langattoman reitittimen kanssa (eli luoda yhteyden langattomaan verkkoon). Langattomat verkkosovittimet voidaan rakentaa laitteiston päävirtapiirien yhteyteen tai ne voivat olla erillisiä lisälaitteita, jotka lisätään laitteeseen liittämällä ne sopivaan porttiin.

Langattomat PCI-verkkosovitinkortit

Liittää työaseman verkkoon. Kortti asetetaan tietokoneen PCI-korttipaikkaan.

Langattomat USB-verkkosovitinkortit

Langattomat USB-verkkosovitinkortit tarjoavat laajennettavan Plug-and-Play-sarjakäyttöliittymän. Tämä liittymä tarjoaa standardinmukaisen, halvan langattoman yhteyden oheislaitteille, kuten näppäimistöille, hiirille, peliohjaimille, tulostimille, skannereille, tallennuslaitteille ja videokonferenssikameroille.

Luvattomat käyttöpisteet

Käyttöpiste, jonka toiminnalle yritys ei ole myöntänyt lupaa. Ongelma on siinä, että luvattomat käyttöpisteet eivät usein noudata langattomien lähiverkkojen suojauskäytäntöjä. Luvaton käyttöpiste mahdollistaa avoimen suojaamattoman käyttöliittymän yrityksen verkkoon fyysisesti kontrolloidun tilan ulkopuolelta.

Oikein suojatussa langattomassa lähiverkossa luvattomat käyttöpisteet aiheuttavat enemmän vahinkoa kuin luvattomat käyttäjät. Jos yritys käyttää toimivia todennusmekanismeja, luvattomat langattoman lähiverkon käyttäjät eivät todennäköisesti pysty käyttämään yrityksen arvokkaita liiketoimintaresursseja. Ongelmia syntyy kuitenkin silloin, kun yrityksen työntekijä tai hakkeri liittyy verkkoon luvattoman käyttöpisteen. Lähes kuka tahansa käyttäjä, jolla on käytössään 802.11-laite pystyy käyttämään yrityksen lähiverkkoa luvattoman käyttöpisteen avulla. Tällä tavoin he pääsevät hyvin lähelle yrityksen tärkeitä resursseja.

Lähiverkko

Tietokoneverkko, joka kattaa suhteellisen pienen alueen. Useimmat lähiverkot ovat rajoitettu yksittäiseen rakennukseen tai rakennusten muodostamaan ryhmään. Kuitenkin yksi lähiverkko voidaan liittää muihin lähiverkkoihin minkä tahansa välimatkan päästä puhelin- ja radioaaltojen avulla. Tällä tavalla yhdistettyjen lähiverkkojen järjestelmää kutsutaan suuralueverkoksi. Useimmat lähiverkot liittävät työasemat ja henkilökohtaiset tietokoneet toisiinsa yksinkertaisten keskittimien tai valitsimien avulla. Jokaisella lähiverkon solmulla (yksittäisellä tietokoneella) on oma suorittimensa, jonka avulla se suorittaa ohjelmia, mutta se voi myös käyttää tietoja ja laitteita (esim. tulostimia) missä tahansa lähiverkon sisällä. Tämä tarkoittaa sitä, että useat käyttäjät voivat jakaa kalliita laitteita, kuten laser-tulostimia, sekä tietoja. Käyttäjät voivat myös käyttää lähiverkkoa viestiäkseen toistensa kanssa, esimerkiksi lähettämällä sähköpostia tai käyttämällä keskusteluohjelmia.

M

MAC (MAC-osoite tai viestin todennuskoodi)

Jos haluat lisätietoja ensimmäisestä termistä, katso kohta MAC-osoite. Viestin todennuskoodi on koodi, jota käytetään määritetyn viestin tunnistamiseen (esim. RADIUS- viestin tunnistamiseen). Koodi on yleensä kryptograafisesti vahva hajautuskokoelma viestin sisältämistä tiedoista, joka sisältää ainutlaatuisen arvon, jonka avulla koodin suojaus voidaan varmistaa.

MAC-osoite

Alemman tason osoite, joka on määritetty verkkoa käyttävälle fyysiselle laitteelle.

mahdollinen haittaohjelma

Vakoilu- ja mainosohjelmat ja muut ohjelmat, jotka keräävät ja lähettävät tietoja ilman käyttäjän myöntämää lupaa ovat mahdollisia haittaohjelmia.

MAPI-tili

Akronyymi, joka tulee sanoista Messaging Application Programming Interface. Microsoftin käyttöliittymämäärittäjä, jonka avulla eri viestintä- ja työryhmäsovellukset (kuten sähköposti, ääniviesti ja faksi) toimivat yhden asiakkaan kautta, kuten esimerkiksi Exchange-asiakkaan kautta. Tästä syystä MAPI:a käytetään usein yritysympäristöissä, jos yritys käyttää Microsoft Exchange Serveriä. Kuitenkin monet ihmiset käyttävät myös Microsoft Outlookia henkilökohtaisen sähköpostinsa lukemiseen.

mato

Mato on itseään kopioiva virus, joka piileskelee tietokoneen aktiivisessa muistissa ja voi lähettää itsensä kopioita sähköpostiviesteissä. Madot kopioituvat ja kuluttavat järjestelmäresursseja, hidastaen tietokoneen suorituskykyä tai keskeyttäen tehtäviä.

melko tärkeät tarkkailukohteet

Tietokoneellasi sijaitseva kansio, jonka muutoksia McAfee Data Backup tarkkailee. Jos määrität melko tärkeän tarkkailukohteen, McAfee Data Backup varmuuskopioi ainoastaan kyseisen kansion tarkkailtavien tiedostotyyppien mukaiset tiedostot, ilman alihakemistoja.

MITM-hyökkäys

Hyökkääjä salakuuntelee julkisen avaimenvaihdon viestejä ja lähettää ne sitten uudelleen, vaihtaen oman julkisen avaimensa pyydetyllä tilalla siten, että alkuperäiset viestien lähettäjät näytävät yhä keskustelevan suoraan toistensa kanssa. Hyökkääjä käyttää ohjelmaa, joka näyttää olevan asiakkaan palvelin ja palvelimen asiakas. Hyökkäystä saatetaan käyttää yksinkertaisesti siksi, että hyökkääjä pääsee näkemään viestejä tai että hän voi muokata viestejä ennen niiden uudelleenlähettämistä. Termi MITM (Man-in-the-middle) on peräisin pallopelistä, jossa pelaajat yrittävät heittää pallon suoraan toisilleen ja välissä oleva pelaaja yrittää siepata pallon.

MSN-tili

Akronyymi, joka tulee sanoista Microsoft Network. Online-palvelu ja Internet-portaali. Tämä on Web-pohjainen tili.

O

online-varmuuskopiovarasto

Online-palvelimen sijainti, jonne tarkkailtavat tiedostot tallennetaan varmuuskopioinnin jälkeen.

otsikko

Otsikko on viestiin lisättävää tietoa, joka säilyy viestissä sen koko elinajan. Otsikko kertoo Internet-ohjelmistolle kuinka viesti tulee toimittua, mihin osoitteeseen viestin vastaukset tulee lähettää, mikä on kyseisen sähköpostiviestin yksilöivä tunniste sekä muita viestiä koskevia hallinnollisia tietoja. Otsikkokenttien esimerkkejä ovat: Vastaanottaja, lähettäjä, CC, päivämäärä, aihe, viestin tunniste ja vastaanotettu.

P

pakkaus

Toiminto, jonka avulla tietoja (tiedostoja) pakataan muotoon, joka minimoi niiden tallentamiseen tai siirtämiseen vaadittavan levytilan määrän.

palauttaminen

Tiedoston kopion noutaminen online-varmuuskopiovarastosta tai arkistosta.

palomuuuri

Järjestelmä, joka on kehitetty estämään luvattomia saapuvia ja lähteviä yhteyksiä yksityisessä verkossa. Palomuuureja on sekä laitteistoina että ohjelmistoina, sekä niiden yhdistelminä. Palomuuureja käytetään usein luvattomien Internet-käyttäjien estämiseen, jotta he eivät pysty muodostamaan yhteyttä Internetiin liitettyihin yksityisiin verkkoihin, kuten Intranet-verkkoihin. Kaikki Intranetin saapuvat ja lähtevät viestit kulkevat palomuurin läpi. Palomuuuri tutkii jokaisen viestin ja estää ne viestit, jotka eivät vastaa määritettyä suojausehtoja. Palomuuria pidetään henkilökohtaisten tietojen ensisijaisena suojauskeinona. Tietoturvallisuuden lisäämiseksi tietoja voidaan myös salata.

palvelin

Tietokone tai ohjelmisto, joka tarjoaa tiettyjä palveluja muissa tietokoneissa suoritettaville ohjelmille. Internet-palveluntarjoajasi postipalvelin on ohjelmisto, joka käsittelee kaikkia palveluntarjoajan käyttäjien saapuvia ja lähteviä sähköpostiviestejä. Lähiverkon palvelin on laitteisto, joka muodostaa verkon pääsolmun. Siinä voi olla myös ohjelmisto, joka tarjoaa tiettyjä palveluja, tietoja tai muita toimintoja kaikille siihen liitetuille asiakastietokoneille.

Palvelun esto

Internetin palvelunestohyökkäys on tapahtuma, jossa käyttäjältä tai yhteisöltä estetään jonkin resurssin palvelujen käyttö, joita he normaalisti pystyvät käyttämään. Tavallisesti palvelun menettäminen tarkoittaa kykenemättömyyttä käyttää tiettyä verkkopalvelua, kuten sähköpostia tai kaikkien verkkoyhteyksien ja palveluiden väliaikaista menettämistä. Pahimmassa tapauksessa esimerkiksi Web-sivusto, jolla on miljoonia käyttäjiä voi joutua keskeyttämään toimintansa. Palvelunestohyökkäys voi myös tuhota tietokonejärjestelmän ohjelmia ja tiedostoja. Vaikka palvelunestohyökkäykset ovat tavallisesti tarkoituksellisia ja haitallisia, niitä voi joskus tapahtua myös vahingossa. Palvelunestohyökkäys on tietokonejärjestelmien tietoturvaohjaus, joka ei tavallisesti aiheuta tietovarkauksia tai muita suojauksen menetyksiä. Kyseiset hyökkäykset voivat kuitenkin aiheuttaa kohdehenkilölle tai yritykselle huomattavia taloudellisia tappioita tai aikaavieviä korjaustoimia.

perusteksti

Mikä tahansa viesti, joka ei ole salattu.

phishing-huijaus

Phishing-huijaus on huijausyritys, jossa hakkeri pyrkii varastamaan tärkeitä tietoja, kuten luottokortti- ja sosiaaliturvanumeroita, käyttäjätunnuksia ja salasanoja. Phishing-huijausyrityksessä mahdollisille uhreille lähetetään virallisen näköinen sähköpostiviesti, jonka lähettäjä näyttää olevan uhrin Internet-palveluntarjoaja, pankki tai usein käyttämä verkkokauppa. Sähköpostiviestejä saatetaan lähettää valituissa luetteloissa oleville henkilöille tai missä tahansa luettelossa oleville henkilöille sillä oletuksella, että osa viestin vastaanottajista todella sattuu omistamaan tilin väärennetyssä organisaatiossa.

pika-arkistointi

Ainoastaan niiden tarkkailtavien tiedostojen arkistointi, jotka ovat muuttuneet viimeisimmän täydellisen tai pika-arkistoinnin jälkeen.

ponnahdusikkunat

Pieniä ikkunoita, jotka tulevat näyttöön muiden ikkunoiden päälle. Ponnahdusikkunoita käytetään useimmiten mainosten näyttämiseen Web-selaimissa. McAfee estää ponnahdusikkunat, jotka ladataan automaattisesti, kun Web-sivu ladataan selaimeesi. McAfee ei estä ponnahdusikkunoita, jotka ladataan, kun napsautat linkkiä.

POP3-tili

Akronyymi, joka tulee sanoista Post Office Protocol 3. Useimmilla kotikäyttäjillä on POP3-tili. Tämä on POP-standardin nykyversio, jota käytetään yleisesti TCP/IP-verkoissa. POP3-tili tunnetaan myös tavanomaisena sähköpostitilinä.

portti

Paikka, johon tieto kulkee tietokoneelle tai tietokoneelta, esimerkiksi tavallinen analoginen modeemi kytkettynä sarjaporttiin. TCP/IP-yhteyksien porttien numerot ovat virtuaalisia arvoja, joita käytetään tietoliikenteen erottelamiseen sovelluskohtaisiin tietovirtoihin. Portit ovat määritetty standardiprotokollille, kuten SMTP:lle ja HTTP :lle siten, että ohjelmat tietävät mihin porttiin niiden kannattaa yrittää muodostaa yhteys. TCP-pakettien kohdeportti viittaa etsittävään sovellukseen tai palvelimeen.

PPPoE

Akronyymi, joka tulee sanoista Point-to-Point Protocol Over Ethernet. Useat Internet-palveluntarjoajat käyttävät PPPoE:ta, koska protokolla tukee PPP:ssä usein käytettyjä protokollatasoja ja todennusta, ja PPPoE:n avulla voidaan muodostaa Point-to-Point-yhteys Ethernetin normaalisti monipisteisessä arkkitehtuurissa.

protokolla

Sovittu muoto, jonka avulla tietoa siirretään kahden laitteen välillä. Käyttäjän näkökulmasta protokollien ainoa kiinnostava puoli on se, että käyttäjän tietokoneen tai laitteen täytyy tukea oikeita protokollia, jos he haluavat kommunikoida muiden tietokoneiden kanssa. Protokolla voidaan ottaa käyttöön joko laitteistossa tai ohjelmistossa.

puskurin ylivuoto

Puskurin ylivuotoja esiintyy, kun epäilyttävät ohjelmat tai prosessit yrittävät tallentaa tietokoneen puskuuriin (tietojen väliaikaiselle tallennusalueelle) enemmän tietoja kuin mitä siihen mahtuu. Tämä vioittaa vierekkäisissä puskuureissa olevia kelvollisia tietoja tai korvaa ne.

R

RADIUS (Remote Access Dial-In User Service)

Protokolla, jonka avulla käyttäjät voidaan todentaa. Protokollaa käytetään useimmiten etäyhteyksien yhteydessä. Protokolla kehitettiin alunperin etäkäyttöpalvelimia varten, mutta nykyään sitä käytetään useissa erilaisissa todennusympäristöissä, kuten esimerkiksi langattoman verkon käyttäjän jaetun salaisuuden todentamisessa 802.1x-standardin yhteydessä.

reaaliaikainen tarkistus

Tiedostot tarkistetaan virusten ja muiden haitallisten mekanismien varalta, kun sinä tai tietokoneesi käytät niitä.

reititin

Verkkolaite, joka edelleenlähettää paketteja verkosta toiseen. Reitittimet perustuvat sisäisiin reititystaulukoihin ja ne lukevat jokaisen saapuvan paketin ja päättävät sitten miten paketti lähetetään eteenpäin. Lähtevien pakettien lähetysosoite reitittimessä määräytyy paketin lähde- ja kohdeosoitteen, sekä verkkoliikenteen tilatietojen, kuten verkon käytön, kustannusten ja heikkojen yhteyksien perusteella, Reittimiä kutsutaan joskus myös käyttöpisteiksi.

roaming

Toiminto, jonka avulla voidaan siirtyä yhden käyttöpisteen käyttöalueelta toiselle ilman palvelukatkoja tai yhteyden menetyksiä.

S

salasana

Useimmiten aakkosnumeerinen koodi, jonka avulla voit käyttää tietokonetta, tiettyä ohjelmaa tai Web-sivustoa.

Salasanasäilö

Henkilökohtaisten salasanojesi suojattu tallennesäilö. Sen avulla voit tallentaa salasanasi luottaen siihen, että kukaan muu käyttäjä, ei edes McAfee-valvoja tai järjestelmänvalvoja, saa niitä käyttöönsä.

salattu teksti

Tietoja, jotka ovat salattu. Salattu teksti ei ole lukukelpoista ennen kuin se on muunnettu perustekstiksi (salaamattomaksi) salausavaimen avulla.

salaus

Toiminto, jossa tietoa muunnetaan tekstistä koodiksi muuttaen tietoa siten, että henkilöt, jotka eivät tiedä kuinka salaus puretaan eivät voi lukea sitä.

sanakirjahyökkäys

Sanakirjahyökkäykset suoritetaan siten, että käyttäjän salasana yritetään päätellä kokeilemalla useita erilaisia tietyn luettelon sisältämiä sanoja. Hyökkääjät eivät yritä kaikkia mahdollisia sanayhdistelmiä manuaalisesti, vaan käyttävät työkaluja, jotka yrittävät tunnistaa käyttäjän salasanat automaattisten toimintojen avulla.

selain

Asiakasoehjelma, joka tekee pyyntöjä Web-palvelimille Internetissä HTTP-protokollan (Hypertext Transfer Protocol) avulla. Web-selain näyttää sisällön käyttäjälle graafisessa muodossa.

sisältöluokitus-ryhmät

Ikäryhmä, johon käyttäjä kuuluu. Sisältö luokitellaan (eli se on saatavissa tai estetty) käyttäjän sisältöluokitusryhmän perusteella. Sisältöluokitusryhmiä ovat: nuori lapsi, lapsi, nuorempi teini-ikäinen, vanhempi teini-ikäinen ja aikuinen.

SMTP-palvelin

Akronyymi, joka tulee sanoista Simple Mail Transfer Protocol. TCP/IP-protokolla, jonka avulla viestejä voidaan lähettää verkon tietokoneesta toiseen. Tätä protokollaa käytetään Internetissä sähköpostin reitittämiseen.

solmu

Verkkoon liitetty yksittäinen tietokone.

SSID-tunnus

Langattoman lähiverkon alijärjestelmän laitteiden verkon nimi. Perustekstinä oleva 32 merkin merkkijono, joka lisätään kaikkiin langattoman lähiverkon pakettien otsikkoihin. SSID-tunnus erottaa langattomat lähiverkot toisistaan, joten kaikkien verkon käyttäjien täytyy toimittaa sama SSID-tunnus käyttääkseen tiettyä käyttöpistettä. SSID-tunnus estää asiakaslaitteita, joilla ei ole verkon SSID-tunnusta käyttämästä verkkoa. Käyttöpisteet lähettävät kuitenkin SSID-tunnuksensa julkisesti oletusasetuksena. Vaikka SSID-tunnuksen julkaisu on pois käytöstä, hakkerit voivat silti tunnistaa verkon SSID-tunnuksen nuuskintatyökalujen avulla.

SSL-protokolla

Netscapen kehittämä protokolla henkilökohtaisten asiakirjojen lähettämiseen Internetissä. SSL-protokolla salaa SSL-yhteyden välityksellä lähetettävät tiedot julkisen avaimen avulla. Sekä Netscape Navigator että Internet Explorer käyttävät ja tukevat SSL-protokollaa ja useat Web-sivustot käyttävät protokollaa vastaanottaessaan luottamuksellisia käyttäjätietoja, kuten luottokorttien numeroita. URL-osoitteet, jotka vaativat SSL-yhteyden alkavat tekstillä https: tavanomaisen http:n sijaan.

synkronointi

Voit ratkaista varmuuskopioitujen tiedostoversioiden ja paikalliselle tietokoneelle tallennettujen tiedostoversioiden ristiriidat synkronoinnin avulla. Tiedostot kannattaa synkronoida silloin, kun online-varmuuskopiovarastossa oleva tiedostoversio on uudempi kuin muilla tietokoneilla oleva tiedostoversio. Synkronointi päivittää tietokoneillasi olevan tiedoston online-varmuuskopiovarastossa olevalla tiedostoversiolla.

SystemGuard-toiminto

SystemGuards-toiminnot tunnistavat tietokoneeseen tehdyt luvattomat muutokset ja varoittavat niistä.

sähköposti

Sähköinen posti, Internetin tai yrityksen lähiverkon tai suuralueverkon kautta lähetetyt viestit. EXE- (suoritettavat tiedostot) tai VBS-muodossa (Visual Basic -komentosarjat) olevat tiedostot ovat yhä kasvavassa määrin suosiossa virusten ja troijjalaisten levityskeinona.

sähköpostiasiakas

Sähköpostitili. Esimerkiksi Microsoft Outlook tai Eudora.

T

tapahtuma

Tapahtumat IP-osoitteesta 0.0.0.0

Jos näet tapahtumia IP-osoitteesta 0.0.0.0, siihen on kaksi todennäköistä syytä. Ensimmäinen ja tavanomaisin syy on, että jostain syystä tietokoneesi on vastaanottanut huonosti muotoutuneen paketin. Internet ei ole aina 100 % luotettava, joten huonoja paketteja saattaa esiintyä. Koska palomuuuri näkee paketit ennen kuin TCP/IP-protokolla voi vahvistaa ne, se saattaa raportoida paketit tapahtumana.

Toinen tilanne voi tapahtua, kun lähde-IP-osoite on tekaistu tai väärennetty. Huijausyrityspaketit saattavat viitata siihen, että joku yrittää tarkistaa tietokonettasi etsiessään troijalaisia. On tärkeää muistaa, että palomuuuri estää yrityksen.

Tapahtumat IP-osoitteesta 127.0.0.1

Tapahtumat luetteloivat joskus lähde-IP-osoitteeseen osoitteen 127.0.0.1. On tärkeää huomata, että tämä IP-osoite on erityistapaus, jota kutsutaan silmukkaosoitteeksi.

Huolimatta siitä, mitä tietokonetta käytät, 127.0.0.1 viittaa aina paikalliseen tietokoneeseen. Tämä osoite tunnetaan myös nimellä localhost, koska tietokoneen nimi "localhost" palauttaa aina IP-osoitteen 127.0.0.1. Tarkoittaako tämä, että tietokoneesi yrittää murtautua itse itseensä? Onko joku troijalainen tai vakoiluohjelma ottamassa tietokoneesi haltuunsa? Ei todennäköisesti. Useat lailliset ohjelmat käyttävät silmukkaosoitetta komponenttien väliseen viestintään. Esimerkiksi useat henkilökohtaiset posti- ja Web-palvelimet antavat sinun määrittää ne Web-käyttöliittymän avulla, jota voidaan useimmiten käyttää http://localhost/-osoitteen kautta.

Palomuuuri kuitenkin sallii näiden ohjelmien lähettämisen tietoliikenteen, joten jos näet tapahtumia IP-osoitteesta 127.0.0.1, se todennäköisesti tarkoittaa sitä että lähde-IP-osoite on tekaistu tai väärennetty. Huijausyrityspaketit ovat useimmiten merkkejä siitä, että joku tarkistaa järjestelmäsi etsiessään troijalaisia. On tärkeää muistaa, että palomuuuri estää tämän huijausyrityksen. On itsestään selvää, että IP-osoitteesta 127.0.0.1 tulevien tapahtumien raportoiminen ei ole tarpeellista.

Kuten sanottua, jotkut ohjelmat, kuten esimerkiksi Netscape 6.2 ja sitä uudemmat versiot vaativat, että lisäät IP-osoitteen 127.0.0.1 **Luotettavien IP-osoitteiden** luetteloon. Näiden ohjelmien komponentit keskustelevat keskenään sellaisella tavalla, että palomuuuri ei pysty päättelemään, onko tietoliikenne paikallista.

Esimerkiksi jos käytät Netscape 6.2:a ja et merkitse osoitetta 127.0.0.1 luotettavaksi, et pysty käyttämään selaimen ystäväluettoa. Tästä syystä jos näet tietoliikennetapahtumia osoitteesta 127.0.0.1 ja kaikki tietokoneesi ohjelmat toimivat normaalisti, voit turvallisesti estää kyseisen liikenteen. Jos kuitenkin jonkun ohjelman, kuten Netscapen käytössä esiintyy ongelmia, lisää IP-osoite 127.0.0.1 palomuurin **Luotettavien IP-osoitteiden** luetteloon ja selvitä, ratkeako ongelma tällä tavoin.

Jos IP-osoitteen 127.0.0.1 lisääminen **Luotettavien IP-osoitteiden** luetteloon korjaa ongelman, sitten sinun täytyy harkita seuraavia vaihtoehtoja: jos merkitset osoitteen 127.0.0.1 luotettavaksi ohjelma toimii oikein, mutta olet alttiimpi huijausyrityshyökkäyksille. Jos et merkitse osoitetta luotettavaksi, ohjelma ei toimi oikein, mutta suojauksesi kyseistä haitallista tietoliikennettä vastaan pysyy ennallaan.

Lähiverkon tietokoneista saapuvat tapahtumat

Useimmissa yritysten lähiverkkojen määrittämissä voit merkitä kaikki lähiverkkosi tietokoneet luotettaviksi.

Yksityisistä IP-osoitteista saapuvat tapahtumat

IP-osoitteita, jotka ovat muodossa 192.168.xxx.xxx, 10.xxx.xxx.xxx ja 172.16.0.0 - 172.31.255.255 kutsutaan reitittämättömiksi tai yksityisiksi IP-osoitteiksi. Nämä IP-osoitteet eivät koskaan poistu verkostasi ja ne voidaan useimmiten merkitä luotettaviksi.

192.168-lohkoa käytetään Microsoftin Internet-yhteyden jakamisen yhteydessä. Jos käytät jaettua Internet-yhteyttä ja näet tapahtumia tästä IP-lohkosta, sinun kannattaa lisätä IP-osoite 192.168.255.255 **Luotettavien IP-osoitteiden** luetteloon. Tämä merkitsee koko 192.168.xxx.xxx-lohkon luotettavaksi.

Jos et ole yksityisessä verkossa ja näet tapahtumia näistä IP-osoitealueista, lähde-IP-osoite saattaa olla tekaistu tai väärennetty. Huijausyrityspaketit ovat useimmiten merkki siitä, että joku yrittää tarkistaa järjestelmäsi etsiessään troijalaisia. On tärkeää muistaa, että palomuuuri estää tämän huijausyrityksen.

Koska yksityiset IP-osoitteet ovat erillisiä Internetissä käytettävistä IP-osoitteista, näiden tapahtumien raportoimisesta ei ole mitään hyötyä.

tarkkailtavat tiedostotyypit

Tarkkailtavat tiedostotyypit ovat tiedostotyyppisiä (esimerkiksi .doc ja .xls), jotka McAfee Data Backup varmuuskopioi tai arkistoi tarkkailukohteissa.

tarkkailukohteet

Tietokoneen kansiot, joita McAfee Data Backup tarkkailee.

tavallinen sähköpostitili

Useimmilla kotikäyttäjillä on tämän tyyppinen tili. Katso myös kohta POP3-tili.

TKIP-protokolla

Pikakorjauskeino, jolla voidaan korjata WEP-suojauksen tietoturva-aukkoja, erityisesti salausavainten uudelleenkäyttöön liittyviä aukkoja. TKIP-protokolla vaihtaa väliaikaisia avaimia 10 000 paketin välein. Tämä tarjoaa dynaamisen jakelukeinon, joka parantaa verkon suojausta huomattavasti. TKIP-suojaus aloitetaan 128-bittisellä väliaikaisella avaimella, joka jaetaan verkon asiakkaiden ja käyttöpisteiden välillä. TKIP-protokolla yhdistää väliaikaisen avaimen asiakaskoneen MAC-osoitteen kanssa ja lisää sitten huomattavan suuren 16 oktetin alustusvektorin, joka luo avaimen, jolla tiedot salataan. Tämä toiminto takaa, että jokainen asema käyttää eri avainvirtaa tietojen salaamiseen. TKIP-protokolla käyttää RC4:ää salauksen suorittamiseen. WEP käyttää myös RC4:ää.

todennus

Henkilön tunnistusmenetelmä, joka useimmiten perustuu käyttäjänimeen ja salasanaan. Todennuksen avulla voidaan varmistaa, että henkilö on kuka hän väittää olevansa, mutta menetelmässä ei määritetä todennettavan henkilön käyttöoikeuksia.

toimialue

Verkkoyhteyden osoite, joka esittää osoitteen omistajan nimen hierarkisessa muodossa: palvelin.yhteisö.tyyppi. Esimerkiksi osoite www.whitehouse.gov toimii Valkoisen talon Web-palvelimen tunnisteena, joka on Yhdysvaltojen hallintojärjestelmän osa.

Trojijan hevonen

Trojialaiset ovat ohjelmia, jotka esiintyvät vaarattomina ohjelmina. Trojialaiset eivät ole viruksia, koska ne eivät kopioi itseään, mutta ne saattavat olla aivan yhtä tuhoisia.

tärkeä tarkkailukohde

Tietokoneesi kansio (ja kaikki sen alihakemistot), jonka muutoksia McAfee Data Backup tarkkailee. Jos määrität tärkeän tarkkailukohteen, McAfee Data Backup varmuuskopioi kaikki kyseisen kansion ja sen alihakemistojen tarkkailtavien tiedostotyyppien mukaiset tiedostot.

täydellinen arkistointi

Käyttäjän määrittämien tarkkailtavien tiedostotyyppien ja sijaintien tietojen täydellinen arkistointi.

ulkoinen kiintolevyasema

Kiintolevyasema, joka sijaitsee tietokoneen kotelon ulkopuolella.

URL

URL tulee sanoista Uniform Resource Locator. URL on Internet-osoitteiden standardimuoto.

valkoinen lista

Sallittujen Web-sivustojen luettelo. Luettelon Web-sivustojen käyttö on sallittua, koska ne eivät sisällä haitallisia toimintoja.

wardriver-verkkovarkaat

Tunkeutujia, jotka käyttävät kannettavia tietokoneita, erityisohjelmistoja ja laitteita ja ajelevat ympäri kaupunkia, esikaupunkialueita ja liikealueita etsiessään salakuunneltavia langattomia tietoliikennesyhteyksiä.

varmuuskopiointi

Tarkkailtavien tiedostojen varmuuskopioiminen suojattuun online-palvelimeen.

Web-bugit

Pieniä grafiikkatiedostoja, jotka voivat upottaa itsensä HTML-sivuihisi ja sallia luvattoman lähteen asettaa evästeitä tietokoneeseesi. Nämä evästeet voivat sitten lähettää tietoja luvattomalle lähteelle. Web-bugeja kutsutaan myös pikselitunnisteiksi, läpinäkyviksi GIF-tiedostoiksi ja näkymättömiksi GIF-tiedostoiksi.

WEP

Salaus- ja todennusprotokolla, joka kehitettiin osana 802.11-standardia. Protokollan ensimmäiset versiot perustuivat RC4-salaustekstiin ja sisälsivät merkittäviä tietoturva-aukkoja. WEP yrittää suojata tiedot salaamalla radioaaltojen välityksellä siirrettäviä tietoja siten, että ne ovat suojattuja, kun niitä siirretään verkon yhdestä päätepestestä toiseen. Viime aikoina on kuitenkin huomattu, että WEP-salaus ei ole aivan niin turvallinen kuin aiemmin on uskottu.

verkkoasema

Levy- tai nauha-asema, joka on liitetty useiden käyttäjien jakaman verkon palvelimeen. Verkkoasemia kutsutaan joskus etäasemiksi.

verkkokartta

Network Managerin graafinen esitys kotiverkon tietokoneista ja osista.

Verkkokortti

Kortti, joka liitetään kannettavaan tietokoneeseen tai muuhun laitteeseen ja jonka avulla laite voidaan liittää lähiverkkoon.

verkkoon

Kun liität kaksi tai useampia tietokoneita toisiinsa, luot verkon.

Wi-Fi (Wireless Fidelity)

Termi, jota käytetään yleisesti kaikista 802.11-standardin verkoista, oli kysessä sitten 802.11b-, 802.11a-, dual-band-verkko tai joku muu verkko. Termiä käyttää Wi-Fi Alliance -yhteistyöjärjestö.

Wi-Fi Alliance

Organisaatio, jonka muodostavat johtavat langattomien laitteistojen ja ohjelmistojen valmistajat, tavoitteenaan 1) kaikkien 802.11-standardiin perustuvien tuotteiden yhteentoimivuuden varmistaminen ja 2) Wi-Fi-termin promotointi kaikkien 802.11-standardiin perustuvien langattomien lähiverkkotuotteiden kansainvälisenä brändin nimenä kaikilla markkinoilla. Organisaatio toimii yhteistyöjärjestönä, testauslaboratoriona ja selvitystoimistona toimittajille, jotka haluavat promotoida tuotteiden yhteentoimivuutta ja toimialan kasvua.

Vaikka kaikkia 802.11a/b/g-tuotteita kutsutaan nimellä Wi-Fi, vain tuotteet, jotka ovat läpäisseet Wi-Fi Alliancen testit saavat käyttää tuotteistaan nimitystä Wi-Fi Certified (Wi-Fi-varmennettu). Wi-Fi Certified on rekisteröity tavaramerkki. Tuotteissa, jotka ovat läpäisseet testit tulee olla paketoinnissaan tunnistava leima, jossa lukee, että tuote on Wi-Fi-varmennettu. Tuotteen leimassa täytyy näkyä myös tuotteen käyttämä radiotaajuus. Järjestö tunnettiin aiemmin nimellä Wireless Ethernet Compatibility Alliance (WECA), mutta se muutti nimeään lokakuussa 2002, jotta nimi vastaisi paremmin Wi-Fi-brändiä, jonka järjestö haluaa luoda.

Wi-Fi Certified (Wi-Fi-varmennettu)

Mitkä tahansa tuotteet, jotka ovat testattu ja hyväksytty Wi-Fi Certified -tuotteiksi (rekisteröity tavaramerkki) Wi-Fi Alliancen toimesta, ovat yhteensopivia toistensa kanssa, vaikka ne olisivat eri valmistajien tuotteita. Wi-Fi Certified -tuotteen käyttäjä voi käyttää minkä tahansa valmistajan käyttöpistettä minkä tahansa valmistajan asiakasohjelmistolla, edellyttäen, että asiakasohjelmisto on myös Wi-Fi Certified -tuote. On kuitenkin tyypillistä, että mitkä tahansa langattomat tuotteet, jotka käyttävät samaa radiotaajuutta (esim. 2,4 GHz / 802.11b tai 11g, 5 GHz / 802.11a) toimivat toistensa kanssa, vaikka ne eivät ole Wi-Fi Certified -tuotteita.

WPA

Määritysstandardi, joka lisää nykyisten ja tulevien langattomien lähiverkkojärjestelmien tietosuojaa ja käyttöoikeuksien hallintaa erittäin paljon. Standardi on suunniteltu toimimaan olemassaolevissa laitteistoissa ohjelmistopäivityksenä, koska WPA on kehitetty IEEE 802.11i-standardin pohjalta ja on yhteensopiva sen kanssa. Kun WPA on asennettu oikein, se tarjoaa langattomien lähiverkkojen käyttäjille korkeatasoisen suojauksen ja varmistuksen siitä, että vain luvalliset verkkokäyttäjät voivat muodostaa yhteyden verkkoon.

WPA-PSK

Erikoislaatuinen WPA-tila, joka on suunniteltu kotikäyttäjille, jotka eivät vaadi vahvaa yritystason tietosuojaa ja eivät käytä todennuspalvelimia. Tässä tilassa kotikäyttäjä antaa aloitussalanan manuaalisesti aktivoitakseen suojatun langattoman verkkoyhteyden esijaetun avaintilan, ja vaihtaa sitten verkon jokaisen langattoman tietokoneen ja käyttöpiesteen salasanaa säännöllisesti. Katso myös kohdat WPA2-PSK ja TKIP.

WPA2

Katso myös kohta WPA. WPA2 on WPA-tietosuojastandardin päivitys, joka perustuu 802.11i IEEE -standardiin.

WPA2-PSK

Katso myös kohdat WPA-PSK ja WPA2. WPA2-PSK on samankaltainen kuin WPA-PSK ja se perustuu WPA2-standardiin. WPA2-PSK:n yleinen ominaisuus on se, että laitteet tukevat usein monia erilaisia salaustoimintoja (esim. AES, TKIP) samanaikaisesti, kun vanhemmat laitteet useimmiten tukivat vain yhtä salaustoimintoa kerralla (eli kaikkien laitteiden täytyi käyttää samaa salaustoimintoa).

VPN (Virtual Private Network)

Verkko, joka muodostuu julkisten linjojen avulla yhdistettävistä solmuista. On olemassa lukuisia järjestelmiä, joiden avulla voidaan luoda verkkoja käyttämällä Internetiä tiedonsiirtokeinona. Nämä järjestelmät käyttävät salausta ja muita suojausmekanismeja varmistakseen, että ainoastaan luvalliset käyttäjät voivat käyttää verkkoa ja että verkon tietoja ei voida salakuunnella.

välimuistipalvelin

Palomuurin osa, joka hallitsee lähiverkon saapuvaa ja lähtevää Internet-tietoliikennettä. Välimuistipalvelin voi parantaa verkon suorituskykyä toimittamalla usein pyydettyjä tietoja, kuten suosittuja Web-sivuja, ja suodattamalla ja hylkäämällä pyyntöjä, joita verkon omistaja ei pidä asianmukaisina, kuten yksityistiedostojen luvatonta käyttöä koskevia pyyntöjä.

välityspalvelin

Tietokone tai tietokoneessa suoritettava ohjelmisto, joka toimii verkon ja Internetin välisenä suojamuurina ja näyttää ainoastaan yhden verkko-osoitteen ulkopuolisille sivustoille. Koska välityspalvelin toimii kaikkien verkon sisäisten tietokoneiden suojamuurina, se suojaa käyttäjien verkkoidentiteettiä, silti kuitenkin mahdollistaen Internet-yhteyksien muodostamisen. Katso myös kohta Välimuistipalvelin.

väsytyksen menetelmähyökkäys

Tunnetaan myös nimellä väsytyksen menetelmämurtautuminen. Sovellusohjelmien käyttämä yritys ja erehdys -menetelmä, jonka avulla yritetään purkaa salattua tietoa, kuten salasanoja sinnikkäällä yrittämisellä älykkäiden strategioiden sijaan. Samalla tavalla kuin rikollinen saattaa murtautua kassakaappiin yrittämällä mahdollisimman monia erilaisia yhdistelmiä, väsytyksen menetelmämurtautuminen yrittää murtaa salauksen kokeilemalla kaikkia mahdollisia sallittujen merkkien yhdistelmiä. Väsytyksen menetelmää pidetään erehtymättömänä, joskin aikaa vievänä murtautumiskeinona.

yhdistetty yhdyskäytävä

Laite, joka yhdistää langattoman käyttöpiirteen, reitittimen ja palomuurin toiminnot. Jotkut laitteet saattavat sisältää myös suojausparannuksia ja siltausominaisuuksia.

Tietoja McAfeesta

McAfee, Inc.:n pääkonttori sijaitsee Santa Clarassa, Kaliforniassa. McAfee on yksi maailman johtavista tietomurtojen esto- ja tietoturvariskien hallintasovellusten valmistajista. McAfee toimittaa luotettavia ratkaisuja ja palveluita, jotka suojaavat järjestelmiä ja verkkoja ympäri maailman. McAfeen kokemus tietoturvakysymyksissä ja tehokas tuotekehitys tuottavat sovelluksia, joiden avulla kotikäyttäjät, yritykset, julkisen sektorin laitokset ja palveluntarjoajat pystyvät torjumaan hyökkäyksiä, estämään haittayrityksiä ja kehittämään ja parantamaan tietoturvaansa jatkuvasti.

Copyright

Copyright © 2006 McAfee, Inc. Kaikki oikeudet pidätetään. Mitään tämän julkaisun osaa ei saa jäljentää, lähettää, kopioida, tallentaa tallenusjärjestelmään tai kääntää millekään kielelle missään muodossa tai millään tavalla ilman McAfee, Inc.:n myöntämää kirjallista lupaa. McAfee ja muut tässä julkaisussa olevat tavaramerkit ovat McAfee, Inc.:n ja/tai sen yhteistyökumppaneiden rekisteröityjä tavaramerkkejä Yhdysvalloissa ja/tai muissa maissa. McAfee käyttää mainonnassaan tuotteilleen ominaista punaista väriä, jonka avulla McAfee-tuotteet voidaan erottaa muista tietoturvatuotteista. Kaikki muut tässä julkaisussa olevat rekisteröidyt ja rekisteröimättömät tavaramerkit ja tekijänoikeuden suojaamat materiaalit ovat yksinomaan vastaavien omistajiensa omaisuutta.

TAVARAMERKIT

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (AND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SITEADVISOR, SITEADVISOR, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS.

Hakemisto

8

| | |
|---------------|-----|
| 802.11 | 168 |
| 802.11a..... | 168 |
| 802.11b | 168 |
| 802.11g..... | 168 |
| 802.1x..... | 168 |

A

| | |
|---|-----|
| arkistointi | 168 |
| asiakas | 169 |
| Avaa Internet ja verkko -asetusikkuna ... | 16 |
| Avaa | |
| Käytönvalvonta-asetukset-asetusikkuna | 18 |
| Avaa SecurityCenter ja käytä | |
| lisäominaisuuksia | 11 |
| Avaa SecurityCenter-asetusikkuna | 20 |
| Avaa Sähköposti ja pikaviesti | |
| -asetusikkuna | 17 |
| Avaa Tietokone ja tiedostot -asetusikkuna | 15 |
| avain | 169 |
| avainsana | 169 |
| Avainten kierrätys epäonnistui..... | 136 |

C

| | |
|-----------------|-----|
| Copyright | 186 |
|-----------------|-----|

D

| | |
|-------------------|-----|
| DNS..... | 169 |
| DNS-palvelin..... | 169 |

E

| | |
|---|-----|
| EasyNetworkin asentaminen..... | 149 |
| EasyNetworkin käynnistäminen | 150 |
| Eheyttä tiedostoja ja kansioita | 37 |
| Ei-toivottujen tiedostojen poistaminen | |
| Shredder-ohjelmalla | 47 |
| eristäminen | 169 |
| ESS (laajennettu palvelukokoelma) | 169 |
| eväste..... | 170 |
| Evää oikeudet verkon käyttöön . 75, 83, 98, | |
| 100, 101, 102 | |

H

| | |
|---------------------------------------|----|
| Hae päivityksiä automaattisesti | 27 |
|---------------------------------------|----|

| | |
|---------------------------------------|---------|
| Hae päivityksiä manuaalisesti..... | 29, 30 |
| Hallitse verkkoa | 38 |
| hallittu verkko..... | 170 |
| Hallittuun verkkoon liittyminen | 57, 58, |
| 151, 155 | |
| Hallitun tietokoneen oikeuksien | |
| muokkaaminen | 63 |
| Hallitun verkon määrittäminen | 53 |
| Hallitusta verkosta poistuminen | 155 |
| Hanki lisätietoja viruksista | 38 |
| Heikko signaalitaso | 143 |
| Hälytysasetusten määrittäminen..... | 31 |

I

| | |
|--|-----|
| Ilmoita ennen päivitysten lataamista ... | 27, |
| 28 | |
| Ilmoituksen saaminen tiedoston | |
| lähettämisestä | 162 |
| Internet | 170 |
| Internet ja verkko -suojausten toiminta | 16 |
| Internetiin ei voi muodostaa yhteyttä . | 139 |
| Intranet | 170 |
| IP-huijausyritys | 170 |
| IP-osoite..... | 171 |

J

| | |
|---|-----|
| jaettu salaisuus | 171 |
| Jaettujen tulostinten käyttäminen | 164 |
| Jaetun tiedoston hakeminen | 159 |
| Jaetun tiedoston kopioiminen | 159 |
| jakaminen | 171 |
| Jatka avainten kierrätystä ... 110, 111, 113, | |
| 140 | |
| julkaiseminen | 171 |

K

| | |
|--|-------------------|
| Kahden järjestelmänvalvojan virhe | 135 |
| kaistanleveys..... | 171 |
| Katkaise yhteys suojattuihin langattomiin | |
| verkkoihin..... | 98, 100, 101, 102 |
| Kehotus antaa WEP-, WPA- tai | |
| WPA2-avain..... | 140 |
| Keskeytä avainten automaattinen | |
| kierrätys | 98, 111, 113, 140 |
| kieltoluettelo..... | 171 |
| Kierrätä avaimia automaattisesti .. 98, 110, | |
| 111, 112, 113, 114, 126, 136, 140 | |

Kierrätä verkkoavaimia manuaalisesti 114, 126, 140
kirjasto172
Kohteen tietojen tarkasteleminen56
komentosarja172
Korjaa suojausongelmat automaattisesti19
Korjaa suojausongelmat manuaalisesti .19
Korjaa tietoturvan puutteet65
Korjaa verkon suojausasetukset98, 106, 108, 136, 141
kuva-analyysi172
Käyttäjäasetusten määrittäminen23
Käyttöoikeuksien myöntäminen tuntemattomalle tietokoneelle.....138
Käyttöpiste172
käytönvalvonta-asetukset172
Käytönvalvonta-asetukset-suojauksen toiminta18

L

Laitteen hallitseminen63
Laitteen näytön ominaisuuksien muokkaaminen64
Laitteet menettävät yhteyden.....140
Lakkaa luottamasta verkon tietokoneisiin60
Langaton lähiverkko (WLAN)172
langaton verkkopiste172
langaton verkkosovitin.....172
Langattomaan verkkoon ei voi muodostaa yhteyttä141
Langattoman verkon suojauksen hallinta103
Langattomat PCI-verkkosovitinkortit ..172
Langattomat USB-verkkosovitinkortit .173
Langattomien reititinten tai yhteispisteiden määrittäminen145
Langattomien verkkojen hallinnointi91
Langattomien verkkojen hallinta92
Langattomien verkkojen suojaaminen ..73
Langattomien verkkojen valvonta.....119
Langattomien verkkoyhteyksien valvonta 120, 121, 122, 123, 124
Lataa ja päivitä päivitykset automaattisesti.....27
Lataa päivitykset automaattisesti.....27, 28
Lataus epäonnistuu suojattua verkkoa käytettäessä134
Liitteet167
Liity suojattuihin langattomiin verkkoihin 75, 78, 98, 138
Lisävalikon käyttäminen20

Lisää tietokoneita käyttämällä siirrettävää laitetta 86, 89, 134
Lisää tietokoneita käyttämällä Windows Connect Now -tekniikkaa..... 87, 88, 113, 134
Lisää tietokoneita suojattuun langattomaan verkkoon . 77, 82, 86, 138, 140
Luettele suositut verkot 94, 95
Luo järjestelmänvalvojan tili23
Luo suojattuja langattomia verkkoja76, 100, 137
luvattomat käyttöpisteet.....173
Lähiverkko173

M

MAC (MAC-osoite tai viestin todennuskoodi)173
MAC-osoite173
mahdollinen haittaohjelma.....173
MAPI-tili.....174
mato174
McAfee EasyNetwork147
McAfee Network Manager49
McAfee QuickClean.....39
McAfee SecurityCenter7
McAfee Shredder45
McAfee Wireless Network Security67
McAfee Wireless Protection.....5
McAfee-tietoturvaohjelmiston asentaminen etätietokoneisiin66
melko tärkeät tarkkailukohteet174
Mihin tietokoneeseen ohjelmisto on asennettava132
MITM-hyökkäys174
MSN-tili.....174
Muita ohjelmia käytettäessä verkolla on toinen nimi.....144
Muodosta yhteys suojattuihin langattomiin verkkoihin 82, 98, 99
Muut ongelmat.....144
Muuta järjestelmänvalvojan salasanaa .25
Muuta langattomien laitteiden käyttöoikeustietoja 98, 107, 136
Myönnä tietokoneille järjestelmänvalvojan käyttöoikeudet 75, 83
Määritä hälytysasetukset 31, 96
Määritä käyttäjäasetukset24
Määritä ohitettujen ongelmien asetukset22
Määritä tiedottavien hälytysten asetukset32
Määritä verkon suojausasetukset.....106

N

| | |
|---|-----------------------------------|
| Network Managerin kuvakkeiden toiminta | 51 |
| Nimeä suojatut langattomat verkot uudelleen | 95, 98 |
| Nimeä verkko uudelleen | 154 |
| Näytä avaimet tavallisena tekstinä..... | 115, 116 |
| Näytä avaimet tähtimerkkeinä | 115, 116 |
| Näytä avainten kierrätyskertojen määrä | 109, 110, 111, 112, 113, 114, 126 |
| Näytä kuukauden aikana suojattujen tietokoneiden määrä.. | 125, 126, 127, 129 |
| Näytä nykyiset avaimet | 109, 134 |
| Näytä online-tietoturvaraportti... | 120, 121, 122, 123, 124, 133 |
| Näytä päivän aikana muodostettujen yhteyksien määrä | 125, 127, 129 |
| Näytä suojatun langattoman verkon tapahtumat | 125, 126, 127, 128, 129 |
| Näytä tällä hetkellä suojatut tietokoneet | 93, 126, 127, 129 |
| Näytä verkkoyhteyden kesto | 120, 121, 122, 123, 124 |
| Näytä verkon signaalinvoimakkuus | 93, 123, 143 |
| Näytä verkon suojaustila. | 93, 106, 121, 146 |
| Näytä verkon yhteysnopeus. | 120, 121, 122, 123, 124 |
| Näytä yhteyden tila | 120, 121, 122, 123, 124 |
| Näytä yhteysilmoitukset | 99 |

O

| | |
|---|------------------------|
| Odotetaan käyttöoikeuksien todentamista | 138 |
| Ohjelmisto ei toimi käyttöjärjestelmän päivityksen jälkeen..... | 146 |
| Olenko suojattu? | 13 |
| Ominaisuudet | 8, 40, 46, 50, 68, 148 |
| online-varmuuskopiovarasto | 174 |
| Ota Wireless Network Security käyttöön | 70 |
| otsikko | 174 |

P

| | |
|---|-----|
| pakkaus | 174 |
| Palauta järjestelmänvalvojan salasana .. | 24 |
| Palauta tietokoneen aikaisemmat asetukset | 37 |
| palauttaminen | 175 |
| palomuuuri | 175 |
| palvelin..... | 175 |
| Palvelun esto..... | 175 |

| | |
|---|--------------------|
| perusteksti | 175 |
| phishing-huijaus | 175 |
| pika-arkistointi | 175 |
| Poista automaattiset päivitykset käytöstä | 27, 29, 30 |
| Poista käyttämättömiä tiedostoja ja kansioita | 36 |
| Poista langattomia reitittimiä tai yhteyspisteitä | 98, 99, 134, 138 |
| Poista suositut langattomat verkot .. | 94, 95 |
| Poista verkkoavaimet | 117 |
| Poista Wireless Network Security käytöstä | 71 |
| Poistu suojatuista langattomista verkoista | 100, 101, 102, 138 |
| ponnahdusikkunat..... | 176 |
| POP3-tili..... | 176 |
| portti..... | 176 |
| PPPoE..... | 176 |
| protokolla..... | 176 |
| puskurin ylivuoto | 176 |
| Päivitysasetusten määrittäminen | 26 |
| Päivitä langaton verkkosovitin | 141, 142 |
| Päivitä reitittimen tai yhteyspisteen laiteohjelmisto | 135 |
| Päivitä verkkokartta..... | 54 |

Q

| | |
|---------------------------------------|----|
| QuickClean-ohjelman käyttäminen | 43 |
| QuickClean-ohjelman toiminnot..... | 40 |

R

| | |
|--|-----|
| RADIUS (Remote Access Dial-In User Service) | 176 |
| reaaliaikainen tarkistus..... | 176 |
| reititin..... | 177 |
| Reititintä tai yhteyspistettä ei voi korjata | 136 |
| roaming..... | 177 |

S

| | |
|---|-----|
| Saatavilla olevan verkkotulostimen asentaminen..... | 165 |
| salasana..... | 177 |
| Salanasäilö | 177 |
| salattu teksti..... | 177 |
| salaus..... | 177 |
| sanakirjahyökkäys | 177 |
| SecurityCenterin asetusten määrittäminen | 21 |
| SecurityCenterin kuvakkeiden toiminta | 11 |
| SecurityCenterin käyttäminen | 9 |
| SecurityCenterin tietojen tarkasteleminen | 20 |

| | |
|---|--------------------|
| selain | 177 |
| Shredder-ohjelman käyttäminen | 48 |
| Shredder-ohjelman toiminnot | 46 |
| Siirry McAfee-käyttäjätileihin | 23 |
| Siirrä päivitykset | 28, 29 |
| sisältöluokitus-ryhmät | 177 |
| SMTP-palvelin | 178 |
| solmu | 178 |
| SSID-tunnus | 178 |
| SSL-protokolla | 178 |
| Suojaa muut langattomat laitteet | 77, 84 |
| Suojattujen langattomien verkkojen määrittäminen | 74 |
| Suojattujen langattomien verkkojen valvonta | 125, 126, 127, 129 |
| Suojauksen tilan asetusten määrittäminen | 22 |
| Suojauksen tilan toiminta | 13 |
| Suojausasetusten määrittäminen | 104, 146 |
| Suojausluokkien ja -tyyppien toiminta | 14 |
| Suojausongelmien korjaaminen | 19 |
| Suojaustilojen määrittäminen | 104 |
| Suorita yleisiä tehtäviä | 33 |
| synkronointi | 178 |
| SystemGuard-toiminto | 178 |
| sähköposti | 178 |
| Sähköposti ja pikaviesti -suojauksen toiminta | 17 |
| sähköpostiasiakas | 178 |
| Säädä avainten kierrätyksen tiheyttä | 110, 111, 114 |

T

| | |
|--|----------|
| tapahtuma | 179 |
| Tarkastele asennettujen tuotteiden tietoja | 20 |
| Tarkastele äskettäisiä tapahtumia | 34 |
| Tarkista päivitysten tila | 12 |
| Tarkista suojauksen tila | 11 |
| tarkkailtavat tiedostotyypit | 180 |
| tarkkailukohteet | 180 |
| tavallinen sähköpostitili | 180 |
| Tiedostojen ja kansioden poistaminen sekä levyasemien tyhjentäminen | 48 |
| Tiedostojen jakaminen | 158 |
| Tiedostojen jakaminen ja lähettäminen | 157 |
| Tiedostojen lähettäminen toisiin tietokoneisiin | 161 |
| Tiedoston hyväksyminen toiselta tietokoneelta | 161, 162 |
| Tiedoston jakaminen | 158 |
| Tiedoston jakamisen lopettaminen | 159 |

| | |
|---|---------|
| Tiedoston lähettäminen toiseen tietokoneeseen | 161 |
| Tietoa Wireless Network Securityn kuvakkeista | 92, 120 |
| Tietoja käyttöoikeustyypeistä | 75, 83 |
| Tietoja McAfeesta | 185 |
| Tietokone ja tiedostot -suojauksen toiminta | 15 |
| Tietokoneen kutsuminen hallittuun verkkoon | 58 |
| Tietokoneen puhdistaminen | 41, 43 |
| Tietokoneen suojauksen tilan valvominen | 62 |
| Tietokoneen suojauksen tilan valvomisen lopettaminen | 63 |
| Tietokoneiden liittäminen verkkoon ... | 137 |
| Tietoturvan puutteiden korjaaminen ... | 65 |
| Tilan ja oikeuksien valvonta | 62 |
| TKIP-protokolla | 180 |
| todennus | 180 |
| toimialue | 181 |
| Troijan hevonen | 181 |
| Tulostimen jakamisen lopettaminen ... | 164 |
| Tulostinten jakaminen | 163 |
| tärkeä tarkkailukohte | 181 |
| täydellinen arkistointi | 181 |

U

| | |
|---|-----|
| ulkoinen kiintolevyasema | 181 |
| URL | 181 |
| Useita langattomia verkkosovittimia ... | 134 |

V,W

| | |
|--|----------|
| Vaihda tietokoneet | 146 |
| Valitse toinen suojaustila | 146 |
| valkoinen lista | 181 |
| wardriver-verkkovarkaat | 181 |
| varmuuskopiointi | 181 |
| Web-bugit | 181 |
| WEP | 182 |
| Verkko vaikuttaa suojaamattomalta ... | 137 |
| verkkoasema | 182 |
| Verkkoavainten hallinta | 109, 126 |
| Verkkokartan kohteiden näyttäminen ja piilottaminen | 56 |
| Verkkokartan käyttäminen | 54 |
| verkkokartta | 182 |
| Verkkokortti | 182 |
| verkkoon | 182 |
| Verkkoon liittyminen | 152 |
| Verkon etähallinta | 61 |
| Verkon käyttöoikeuksien myöntäminen | 152 |
| Verkon nimeäminen uudelleen | 55 |

| | |
|--|---------|
| Verkon suojaaminen tai määrittäminen | 134 |
| Vianmäärittäminen | 131 |
| Wi-Fi (Wireless Fidelity) | 182 |
| Wi-Fi Alliance | 182 |
| Wi-Fi Certified (Wi-Fi-varmennettu) ... | 183 |
| Windows ei tue langatonta yhteyttä | 143 |
| Windows näyttää, että yhteyttä ei ole .. | 144 |
| Wireless Network Securityn asentaminen | 132 |
| Wireless Network Securityn ottaminen | |
| käyttöön | 70, 140 |
| WPA | 183 |
| WPA2 | 183 |
| WPA-PSK | 183 |
| WPA-PSK | 183 |
| VPN (Virtual Private Network) | 183 |
| välimuistipalvelin | 183 |
| välityspalvelin | 184 |
| väsytyksen menetelmähyökkäys | 184 |
| Y | |
| yhdistetty yhdyskäytävä | 184 |
| Yhteensopimaton reititin tai yhteyspiste | 135 |
| Yhteensopivaa langatonta verkkosovitinta ei havaita | 133 |
| Yhteyden muodostaminen Internetiin ja verkkoon | 139 |
| Yhteyden muodostaminen verkkoihin, joissa SSID-lähetys on poistettu käytöstä | 84 |
| Yhteys on katkennut | 140 |
| Yleisten tehtävien suorittaminen | 33 |
| Ylläpidä tietokonetta automaattisesti | 35 |
| Ylläpidä tietokonetta manuaalisesti | 36 |