

McAfee®

wireless homenetworksecurity

Guida dell'utente

McAfee®

COPYRIGHT

Copyright © 2005 McAfee, Inc. Tutti i diritti riservati. È vietato riprodurre, trasmettere, trascrivere, archiviare in un sistema di recupero dei dati o tradurre in altra lingua completamente o in parte questo documento con qualsiasi mezzo senza previa autorizzazione scritta di McAfee, Inc., o di un suo fornitore o di una sua consociata.

ATTRIBUZIONI DEI MARCHI DI FABBRICA

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (E IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE E DESIGN, CLEAN-UP, DESIGN (E STILIZZATA), DESIGN (N STILIZZATA), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (E IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (E IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M E DESIGN, MCAFEE, MCAFEE (E IN KATAKANA), MCAFEE E DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (E IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, QUICKCLEAN, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN (E IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (E IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. Sono marchi registrati di McAfee, Inc. e/o delle relative società affiliate negli USA e/o in altri paesi. Il rosso utilizzato con riferimento alla protezione è una caratteristica distintiva dei prodotti con marchio McAfee. Tutti i marchi registrati e non registrati citati nel presente documento sono di proprietà esclusiva dei rispettivi titolari.

INFORMAZIONI SULLA LICENZA

Contratto di licenza

AVVISO AGLI UTENTI: LEGGERE ATTENTAMENTE IL TESTO DEL CONTRATTO RELATIVO ALLA LICENZA ACQUISTATO, CHE STABILISCE LE CONDIZIONI GENERALI DI FORNITURA PER L'UTILIZZO DEL SOFTWARE CONCESSO IN LICENZA. NEL CASO IN CUI NON SI SAPPIA CON ESATTEZZA CHE TIPO DI LICENZA È STATA ACQUISTATO, CONSULTARE I DOCUMENTI DI VENDITA E ALTRE AUTORIZZAZIONI CONNESSE O LA DOCUMENTAZIONE RELATIVA ALL'ORDINE DI ACQUISTO CHE ACCOMPAGNA LA CONFEZIONE DEL SOFTWARE O CHE È STATA RICEVUTA SEPARATAMENTE IN RELAZIONE ALL'ACQUISTO MEDESIMO (SOTTO FORMA DI OPUSCOLO, FILE CONTENUTO NEL CD DEL PRODOTTO O FILE DISPONIBILE SUL SITO WEB DAL QUALE È STATO ESEGUITO IL DOWNLOAD DEL SOFTWARE). SE NON SI ACCETTANO ALCUNI O TUTTI I TERMINI DEL CONTRATTO, ASTENERSI DALL'INSTALLARE IL SOFTWARE. SE PREVISTO DAL CONTRATTO, L'UTENTE POTRÀ RESTITUIRE IL PRODOTTO A MCAFEE O AL PUNTO VENDITA IN CUI È STATO ACQUISTATO ED ESSERE INTERAMENTE RIMBORSATO.

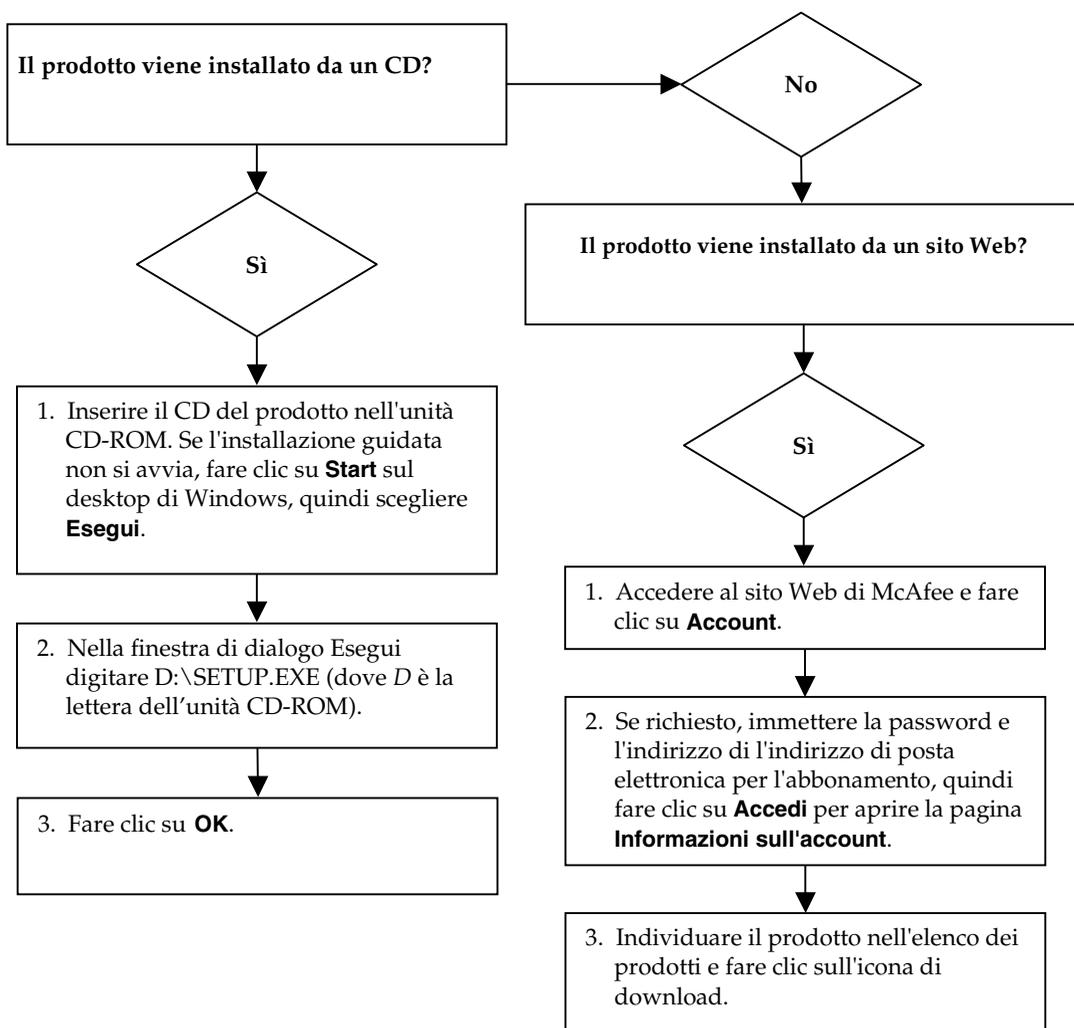
Attribuzioni

Questo prodotto include o potrebbe includere:

♦ Software sviluppato da OpenSSL Project per l'utilizzo nell'OpenSSL Toolkit (<http://www.openssl.org/>). ♦ Software crittografico scritto da Eric A. Young e software scritto da Tim J. Hudson. ♦ Software concesso in licenza o in sublicenza all'utente in base a licenze GNU GPL (General Public License) o a licenze Free Software analoghe che autorizzano l'utente, tra l'altro, a copiare, modificare e ridistribuire alcuni programmi o parte di essi e ad accedere al codice sorgente. La convenzione GPL prevede che, per qualsiasi software coperto da licenza GPL e distribuito ad altri utenti in formato binario eseguibile, debba essere reso disponibile anche il relativo codice sorgente. Per qualsiasi software coperto da licenza GPL, è reso disponibile sul presente CD il relativo codice sorgente. Qualora, in base a licenze Free Software, i diritti di utilizzo, copia o modifica di un programma che McAfee è tenuta a concedere siano più ampi dei diritti concessi in base al presente contratto, i suddetti diritti avranno la precedenza sui diritti e le restrizioni qui previste. ♦ Software originariamente scritto da Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software originariamente scritto da Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software scritto da Douglas W. Sauder. ♦ Software sviluppato da Apache Software Foundation (<http://www.apache.org/>). Per ottenere una copia del contratto di licenza di questo software, visitare il sito www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation e altri. ♦ Software sviluppato da CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ Tecnologia FEAD[®] Optimizer[®], Copyright Netopsystems AG, Berlino, Germania. ♦ Outside In[®] Viewer Technology © 1992-2001 Stellant Chicago, Inc. e/o Outside In[®] HTML Export, © 2001 Stellant Chicago, Inc. ♦ Software protetto da copyright di Thai Open Source Software Center Ltd. e Clark Cooper, © 1998, 1999, 2000. ♦ Software protetto da copyright dei manufattori di software Expat. ♦ Software protetto da copyright di The Regents of the University of California, © 1989. ♦ Software protetto da copyright di Gunnar Ritter. ♦ Software protetto da copyright di Sun Microsystems[®], Inc. © 2003. ♦ Software protetto da copyright di Gisle Aas. © 1995-2003. ♦ Software protetto da copyright di Michael A. Chase, © 1999-2000. ♦ Software protetto da copyright di Neil Winton, © 1995-1996. ♦ Software protetto da copyright di RSA Data Security, Inc., © 1990-1992. ♦ Software protetto da copyright di Sean M. Burke, © 1999, 2000. ♦ Software protetto da copyright di Martijn Koster, © 1995. ♦ Software protetto da copyright di Brad Appleton, © 1996-1999. ♦ Software protetto da copyright di Michael G. Schwern, © 2001. ♦ Software protetto da copyright di Graham Barr, © 1998. ♦ Software protetto da copyright di Larry Wall e Clark Cooper, © 1998-2000. ♦ Software protetto da copyright di Frodo Looijgaard, © 1997. ♦ Software protetto da copyright di Python Software Foundation, Copyright © 2001, 2002, 2003. Per ottenere una copia del contratto di licenza di questo software, visitare il sito www.python.org. ♦ Software protetto da copyright di Beman Dawes, © 1994-1999, 2002. ♦ Software scritto da Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software protetto da copyright di Simone Bordet e Marco Cravero, © 2002. ♦ Software protetto da copyright di Stephen Purcell, © 2001. ♦ Software sviluppato da Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). ♦ Software protetto da copyright di International Business Machines Corporation e altri, © 1995-2003. ♦ Software sviluppato da University of California, Berkeley e suoi contribuenti. ♦ Software sviluppato da Ralf S. Engelschall <rse@engelschall.com> per l'utilizzo nel mod_ssl project (<http://www.modssl.org/>). ♦ Software protetto da copyright di Kevlin Henney, © 2000-2002. ♦ Software protetto da copyright di Peter Dimov e Multi Media Ltd. © 2001, 2002. ♦ Software protetto da copyright di David Abrahams, © 2001, 2002. Per la documentazione, vedere <http://www.boost.org/libs/bind/bind.html>. ♦ Software protetto da copyright di Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software protetto da copyright di Boost.org, © 1999-2002. ♦ Software protetto da copyright di Nicolai M. Josuttis, © 1999. ♦ Software protetto da copyright di Jeremy Siek, © 1999-2001. ♦ Software protetto da copyright di Daryle Walker, © 2001. ♦ Software protetto da copyright di Chuck Allison e Jeremy Siek, © 2001, 2002. ♦ Software protetto da copyright di Samuel Krempp, © 2001. Per aggiornamenti, documentazione e riepilogo delle revisioni, vedere <http://www.boost.org>. ♦ Software protetto da copyright di Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software protetto da copyright di Cadenza New Zealand Ltd., © 2000. ♦ Software protetto da copyright di Jens Maurer, © 2000, 2001. ♦ Software protetto da copyright di Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software protetto da copyright di Ronald Garcia, © 2002. ♦ Software protetto da copyright di David Abrahams, Jeremy Siek e Daryle Walker, © 1999-2001. ♦ Software protetto da copyright di Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software protetto da copyright di Housemarque Oy <<http://www.housemarque.com>>, © 2001. ♦ Software protetto da copyright di Paul Moore, © 1999. ♦ Software protetto da copyright di Dr. John Maddock, © 1998-2002. ♦ Software protetto da copyright di Greg Colvin e Beman Dawes, © 1998, 1999. ♦ Software protetto da copyright di Peter Dimov, © 2001, 2002. ♦ Software protetto da copyright di Jeremy Siek e John R. Bandela, © 2001. ♦ Software protetto da copyright di Joerg Walter e Mathias Koch, © 2000-2002.

Scheda di avvio rapido

Se si installa il prodotto dal CD o dal sito Web, stampare questa pratica pagina di riferimento.



McAfee si riserva il diritto di modificare i Piani di aggiornamento e assistenza e i criteri in qualsiasi momento senza preavviso. McAfee e i relativi nomi di prodotti sono marchi o marchi registrati di McAfee, Inc. e/o delle relative società affiliate negli USA e/o in altri paesi.
© 2005 McAfee, Inc. Tutti i diritti riservati.

Per ulteriori informazioni

Per visualizzare le Guide dell'utente sul CD del prodotto, controllare che Acrobat Reader sia installato; in caso contrario, installarlo dal CD del prodotto McAfee.

- 1 Inserire il CD del prodotto nell'unità CD-ROM.
- 2 Aprire Esplora risorse: Fare clic su **Start** sul desktop di Windows, quindi su **Cerca**.
- 3 Individuare la cartella Manuali e fare doppio clic sul file .PDF della Guida dell'utente che si desidera aprire.

Vantaggi della registrazione

Per inviare la registrazione direttamente a McAfee, si consiglia di attenersi alla facile procedura contenuta nel prodotto acquistato. Oltre a garantire supporto tecnico puntuale e competente, la registrazione offre i seguenti vantaggi:

- Supporto elettronico GRATUITO
- Aggiornamenti dei file di definizione dei virus (.DAT) per un anno dall'installazione quando si acquista il software VirusScan
Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti delle definizioni dei virus, visitare il sito <http://it.mcafee.com>
- 60 giorni di garanzia per l'eventuale sostituzione del CD del software nel caso in cui sia difettoso o danneggiato

- Aggiornamenti dei filtri di SpamKiller per un anno dall'installazione quando si acquista il software SpamKiller

Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti dei filtri, visitare il sito <http://it.mcafee.com>

- Aggiornamenti di McAfee Internet Security Suite per un anno dall'installazione quando si acquista il software MIS

Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti dei contenuti, visitare il sito <http://it.mcafee.com>

Supporto tecnico

Per il supporto tecnico, visitare il sito

<http://www.mcafeeaiuto.com/>.

Il sito del supporto tecnico consente di accedere 24 ore su 24 alla semplice procedura di risposta guidata alle domande più comuni.

Gli utenti più esperti possono anche provare le opzioni avanzate, tra cui una ricerca basata su parole chiave e un sistema di Guida in linea. Se non si trova una soluzione, si può inoltre accedere alle opzioni GRATUITE di chat e posta elettronica. Le opzioni di chat e posta elettronica consentono di entrare rapidamente in contatto tramite Internet con i tecnici qualificati del servizio di supporto, senza costi aggiuntivi. In alternativa, le informazioni sull'assistenza telefonica sono reperibili presso il sito

<http://www.mcafeeaiuto.com/>.

Sommario

Scheda di avvio rapido	iii
1 Guida introduttiva	9
Utilizzo di McAfee Wireless Home Network Security	9
Protezione della rete	9
Informazioni su Wireless Home Network Security	10
Wireless Home Network Security facilita l'utilizzo	10
Funzioni	11
Requisiti di sistema	12
Utilizzo di McAfee SecurityCenter	13
2 Installazione di Wireless Home Network Security	15
Installazione dal CD	15
Installazione dal sito Web	15
Installazione dal file di installazione	16
Utilizzo della configurazione guidata	16
3 Utilizzo della pagina Riepilogo	17
Visualizzazione della connessione	17
Visualizzazione della rete senza fili protetta	18
4 Gestione delle reti senza fili	19
Connessione a una rete	20
Disconnessione da una rete	20
Utilizzo delle opzioni avanzate	20
5 Configurazione delle opzioni	21
Visualizzazione di eventi	21
Configurazione delle impostazioni avanzate	22
Configurazione delle impostazioni di protezione	22
Configurazione delle impostazioni di avviso	22
Configurazione di altre impostazioni	23

Revoca dell'accesso alla rete	23
Ripristino delle impostazioni di protezione	24
Protezione di altri computer	24
Rotazione delle chiavi	25
Protezione delle reti senza fili	25
Rimozione della protezione dalle reti senza fili	25
6 Aggiornamento di Wireless Home Network Security	27
Verifica automatica della disponibilità di aggiornamenti	27
Verifica manuale della disponibilità di aggiornamenti	27
7 Indicazioni sugli avvisi	29
Accesso revocato	29
Chiave di protezione rotata	29
Computer connesso	29
Computer protetto	29
Computer sconnesso	29
Configurazione di rete modificata	29
Frequenza della rotazione della chiave di protezione modificata	30
Impostazioni di rete modificate	30
Password modificata	30
Rete ridenominata	30
Rete ripristinata	30
Rotazione della chiave non riuscita	30
Rotazione della chiave ripresa	31
Rotazione della chiave sospesa	31
Router o access point senza fili non protetto	31
Router o access point senza fili protetto	31
8 Risoluzione dei problemi	33
Installazione	33
Su quali computer installare questo software	33
Adattatore senza fili non rilevato	33
Più adattatori senza fili	33
Impossibile effettuare il download sui computer senza fili perché la rete è già protetta	34

Protezione o configurazione della rete	34
Router o access point non supportato	34
Aggiornamento del firmware del router o dell'access point	35
Errore di amministratore duplicato	35
La rete risulta non sicura	35
Impossibile ripristinare	35
Connessione di computer a una rete	36
In attesa di autorizzazione	36
Autorizzazione dell'accesso a un computer sconosciuto	36
Connessione a una rete o a Internet	37
Connessione a Internet non valida	37
Interruzione momentanea della connessione	37
Perdita della connessione sui dispositivi (diversi dal computer)	37
Richiesta di immissione della chiave WEP o WPA	37
Impossibile connettersi	38
Aggiornamento dell'adattatore senza fili	38
Livello del segnale debole	39
Windows non è in grado di configurare la connessione senza fili	39
Windows non visualizza alcuna connessione	40
Altri problemi	40
Nome di rete differente durante l'utilizzo di altri programmi	40
Problemi di configurazione dei router o degli access point senza fili	40
Sostituzione di computer	41
Software non funzionante in seguito all'aggiornamento dei sistemi operativi	41
9 Glossario	43
Indice	53

Benvenuti in McAfee Wireless Home Network Security, che offre protezione avanzata per la rete senza fili, i dati personali e il computer.

Questo prodotto è progettato per computer con connessioni senza fili. Quando si installa questo prodotto su computer che si connettono a una rete mediante cavo, non si dispone delle funzionalità complete sui computer cablati.

McAfee Wireless Home Network Security migliora la privacy durante l'utilizzo del computer crittografando i dati personali e privati mentre vengono inviati sulla rete senza fili protetta e impedisce agli hacker di accedere alle informazioni.

Utilizzo di McAfee Wireless Home Network Security

Prima di proteggere la rete, considerare quanto segue.

- Connessioni tramite cavo: i computer connessi al router mediante un cavo non necessitano di protezione, dato che i segnali trasmessi su un cavo non possono essere intercettati.
- Connessioni senza fili: i computer che dispongono di connessioni senza fili vanno protetti perché i dati possono essere intercettati. È necessario utilizzare un computer senza fili per proteggere una rete, perché soltanto un computer senza fili può concedere l'accesso a un altro computer senza fili.

Protezione della rete

Non è necessario proteggere la rete se si effettua la connessione tramite cavo.

- 1 Sul computer senza fili, installare l'adattatore senza fili e verificare che sia abilitato. L'adattatore senza fili può essere una scheda inserita a lato del computer oppure una porta USB. Molti computer di nuova generazione sono dotati di un adattatore senza fili incorporato, pertanto, non è necessario installarlo.
- 2 Installare il router o l'access point senza fili (gli access point vengono utilizzati per estendere il raggio d'azione della rete senza fili) e verificare che sia acceso e abilitato. Per una definizione più completa di router e access point, vedere il [Glossario a pagina 43](#).

- 3 Installare McAfee Wireless Home Network Security su ciascun computer senza fili nella rete. Non è necessario installare questo software sui computer connessi tramite cavo. Vedere [Installazione di Wireless Home Network Security a pagina 15](#).
- 4 Da uno dei computer senza fili, proteggere la rete. Vedere [Protezione delle reti senza fili a pagina 25](#).
- 5 Aggiungersi alla rete da altri computer senza fili. Vedere [Protezione di altri computer a pagina 24](#).

Informazioni su Wireless Home Network Security

Spesso si utilizza la rete senza fili a casa perché è semplice e conveniente. La tecnologia senza fili consente di accedere a Internet da qualsiasi stanza della casa o addirittura dal cortile, senza il costo e il fastidio dei cavi. Le reti senza fili facilitano l'accesso alla rete da parte di parenti e amici.

Tuttavia, questa convenienza comporta una certa vulnerabilità della protezione. Le reti senza fili utilizzano onde radio per trasmettere i dati e queste onde sono in grado di attraversare le pareti casa. Con l'ausilio di antenne specializzate, è possibile che degli intrusi accedano alla rete senza fili o intercettino i dati a chilometri di distanza.

Per proteggere la rete senza fili e i dati, è necessario restringere l'accesso alla rete senza fili e crittografare i dati. Il router o l'access point senza fili è dotato di standard di protezione incorporati ma la difficoltà è rappresentata dall'attivazione e dalla gestione corretta delle impostazioni di protezione. Oltre il 60% delle reti senza fili non utilizza un livello di protezione elevato come la crittografia.

Wireless Home Network Security facilita l'utilizzo

McAfee Wireless Home Network Security attiva la protezione sulla rete senza fili e protegge le informazioni inviate con una semplice procedura che, con un solo clic, consente di generare automaticamente una chiave di crittografia. La maggior parte delle chiavi facili da ricordare possono essere decifrate velocemente dagli hacker. Consentendo al computer di memorizzare la chiave, Wireless Home Network Security può utilizzare chiavi impossibili da decifrare.

Questo software, eseguito continuamente in background, consente inoltre di creare e distribuire una nuova chiave di crittografia ogni pochi minuti, dimostrandosi efficace anche contro gli hacker più determinati. I computer autorizzati, come quelli di parenti e amici che desiderano avere accesso alla rete senza fili, ricevono una chiave di crittografia e tutte le distribuzioni delle chiavi.

Questa procedura garantisce una protezione efficace e al contempo può essere implementata facilmente a casa dal proprietario di una rete senza fili. Con un solo clic, è possibile impedire agli hacker di rubare i dati trasmessi senza fili. Gli hacker non potranno inserire cavalli di Troia o altro malware sulla rete. È inoltre non potranno utilizzare la rete senza fili come piattaforma per il lancio di attacchi di spam o di virus. Anche eventuali freeloader occasionali che potrebbero utilizzare la rete per il download illegale di film e canzoni verranno bloccati, evitando il fastidio di errati carichi di responsabilità per azioni illegali.

Altre soluzioni non offrono la semplicità o l'efficacia della protezione offerta da Wireless Home Network Security. L'applicazione di filtri agli indirizzi MAC o la disattivazione della trasmissione SSID offre solo una protezione superficiale. Anche gli hacker più inesperti sono in grado di forzare questi meccanismi, utilizzando strumenti scaricabili gratuitamente da Internet. Altre utilità, quali le reti VPN non proteggono la rete senza fili, lasciando gli utenti vulnerabili a numerosi attacchi.

McAfee Wireless Home Network Security è il primo prodotto che rende inattaccabili le reti domestiche senza fili.

Funzioni

Questa versione di Wireless Home Network Security offre le seguenti funzioni:

- Protezione sempre attiva: rileva e protegge automaticamente qualsiasi rete senza fili vulnerabile a cui ci si è connessi.
- Interfaccia intuitiva: è possibile proteggere la rete senza dover prendere decisioni difficili o conoscere termini tecnici complessi.
- Crittografia automatica potente: consente l'accesso alla rete solo a parenti e amici e protegge la trasmissione e la ricezione dei dati.
- Soluzione solo software: Wireless Home Network Security funziona con router o access point senza fili standard e il software per la protezione. Non è necessario acquistare hardware addizionale.
- Rotazione automatica della chiave: persino gli hacker più determinati non possono acquisire le informazioni, poiché la chiave è in continua rotazione.
- Aggiunta di utenti di rete: è possibile autorizzare parenti e amici ad accedere alla rete.
- Strumento di connessione intuitivo: strumento di connessione senza fili intuitivo e informativo, con dettagli sulla potenza del segnale e sullo stato della protezione.
- Registrazione di eventi e avvisi: segnalazioni e avvisi di facile comprensione offrono agli utenti più esperti ulteriori informazioni sulla rete senza fili.

- Modalità sospensione: è possibile sospendere temporaneamente la rotazione della chiave in modo che particolari applicazioni possano funzionare senza interruzione.
- Compatibilità con altri dispositivi: Wireless Home Network Security si aggiorna automaticamente con i moduli di router o access point senza fili più recenti delle marche più diffuse, inclusi: Linksys®, NETGEAR®, D-Link®, Belkin® e altri.

Requisiti di sistema

- Microsoft® Windows 98SE, Windows Me, Windows 2000 o Windows XP
- PC con processore compatibile Pentium
Windows 98 o 2000: 133 MHz o superiore
Windows Me: 150 MHz o superiore
Windows XP (Home e Pro): 300 MHz o superiore
- RAM
Windows 98SE, Me o 2000: 64 MB
Windows XP (Home e Pro): 128 MB
- 50 MB di spazio su disco
- Microsoft Internet Explorer 5.5 o versione successiva

NOTA

Per eseguire l'aggiornamento all'ultima versione di Internet Explorer, visitare il sito Web di Microsoft, all'indirizzo <http://www.microsoft.com/>.

Rete senza fili

- Adattatore di rete senza fili standard
- Router o access point senza fili standard, inclusi gran parte dei modelli Linksys®, NETGEAR®, D-Link® e Belkin®

Utilizzo di McAfee SecurityCenter

McAfee SecurityCenter è un punto di riferimento unico per la protezione. È possibile eseguire SecurityCenter dall'icona McAfee nella barra delle applicazioni di Windows oppure dal desktop di Windows.

NOTA

Per ulteriori informazioni su queste funzioni, fare clic su ? nella finestra di dialogo di **SecurityCenter**.

Per aprire McAfee SecurityCenter:

- 1 Fare clic con il pulsante destro del mouse sull'icona McAfee .
- 2 Fare clic su **Apri SecurityCenter**.

Per accedere alla funzione Wireless Home Network Security:

- 1 Fare clic con il pulsante destro del mouse sull'icona McAfee .
- 2 Selezionare **Wireless Network Security** e fare clic sulla funzione che si desidera utilizzare.

Installazione di Wireless Home Network Security

2

Questa sezione spiega come installare Wireless Home Network Security e fornisce una guida introduttiva su come proteggere la rete.

Quando si installa McAfee Wireless Home Network Security, considerare quanto segue.

- Installare questo software su tutti i computer senza fili.
- Non è necessario installare questo software sui computer connessi tramite cavo.

Installazione dal CD

- 1 Inserire il CD del prodotto nell'unità CD-ROM. Se l'installazione non viene avviata automaticamente, fare clic su **Start** sul desktop di Windows, quindi su **Esegui**.
- 2 Nella finestra di dialogo **Esegui**, digitare D:\SETUP.EXE (dove D è la lettera corrispondente all'unità CD-ROM).
- 3 Fare clic su **OK**.
- 4 Andare a [Utilizzo della configurazione guidata a pagina 16](#).

Installazione dal sito Web

Quando si installa Wireless Home Network Security dal sito Web, è necessario salvare il file di installazione. Questo file viene utilizzato per installare Wireless Home Network Security su altri computer.

- 1 Visitare il sito Web McAfee e fare clic su **Account**.
- 2 Se richiesto, immettere la password e l'indirizzo di posta elettronica di sottoscrizione, quindi fare clic su **Accesso** per aprire la pagina **Informazioni sull'account**.
- 3 Individuare il prodotto nell'elenco dei prodotti e fare clic su **Salva oggetto con nome...** Il file di installazione è salvato sul computer.

Installazione dal file di installazione

Se è stato scaricato il pacchetto di installazione (anziché disporre di un CD), è necessario installare il software su tutti i computer senza fili. Dopo che la rete è protetta, i computer senza fili non possono connettersi alla rete senza immettere la chiave. Effettuare una delle seguenti operazioni:

- Prima di proteggere la rete, scaricare il pacchetto di installazione su ogni computer senza fili.
- Copiare il file di installazione su un supporto di memorizzazione USB o un CD scrivibile e installare il software su altri computer senza fili.
- Se la rete è già protetta, collegare un cavo al router per scaricare il file. È inoltre possibile fare clic su **Visualizza chiave di rete** per visualizzare la chiave corrente e connettersi alla rete senza fili mediante tale chiave.

Dopo aver installato Wireless Home Network Security su tutti i computer senza fili, attenersi alle istruzioni sullo schermo. Fare clic su **Fine** per visualizzare la Configurazione guidata. Andare a [Utilizzo della configurazione guidata a pagina 16](#).

Utilizzo della configurazione guidata

La configurazione guidata consente di:

- Proteggere la rete da uno dei computer senza fili. Per ulteriori informazioni, vedere [Protezione delle reti senza fili a pagina 25](#).

Se Wireless Home Network Security non può determinare il corretto router o access point da proteggere, viene chiesto di riprovare o annullare. Provare ad avvicinarsi al router o all'access point che si sta proteggendo e fare clic su **Riprova**.

- Aggiungersi a una rete protetta (questo passaggio non è necessario se è presente soltanto un computer senza fili). Per ulteriori informazioni, vedere [Gestione delle reti senza fili a pagina 19](#).
- Connettersi a una rete. Per ulteriori informazioni, vedere [Connessione a una rete a pagina 20](#).

Se l'adattatore senza fili non viene rilevato oppure il router o l'access point senza fili non è acceso, si riceverà un avviso.

Utilizzo della pagina Riepilogo

3

Per visualizzare lo stato della connessione, fare clic con il pulsante destro sull'icona McAfee (), scegliere **Wireless Network Security**, quindi selezionare **Riepilogo**. Verrà visualizzata la pagina **Riepilogo** (Figura 3-1).



Figura 3-1. Pagina Riepilogo

Visualizzazione della connessione

Il riquadro Connessione visualizza lo stato della connessione. Se si desidera eseguire una ricerca della connessione senza fili, fare clic su **Ricerca protezione**.

- **Stato:** indica se la connessione è attiva o meno. Se la connessione è attiva, verrà visualizzato il nome della rete.
- **Protezione:** indica la modalità di protezione della rete.
- **Velocità:** indica la velocità della connessione dalla scheda d'interfaccia di rete (NIC o Network Interface Card).
- **Durata:** indica la durata della connessione alla rete specifica.
- **Potenza del segnale:** indica la potenza della connessione senza fili.

Visualizzazione della rete senza fili protetta

Il riquadro Rete senza fili protetta fornisce informazioni sulla rete.

- Connessioni di oggi: indica quante volte gli utenti si sono connessi alla rete nella giornata corrente.
- Rotazioni chiave di oggi: indica quante volte la chiave è stata rotata nella giornata corrente, includendo il tempo trascorso da quando la chiave è stata rotata l'ultima volta.
- Rotazione della chiave sospesa: indica che la rotazione della chiave sulla rete è sospesa. Per riprendere la rotazione della chiave e garantire che tutta la rete sia completamente protetta dagli hacker, fare clic su **Riprendi rotazione chiave**.
- Computer protetti questo mese corrente: indica il numero dei computer protetti nel mese corrente.
- Computer: se si è connessi a una rete protetta, indica tutti i computer sulla rete e l'ultima connessione di ciascun computer.

 : indica che il computer è connesso.

 : indica che il computer può riconnettersi senza aggiungersi alla rete.

 : indica che il computer non è connesso. È necessario aggiungere nuovamente il computer alla rete perché la chiave è stata aggiornata.

Fare clic su **Visualizza eventi di rete** per visualizzare gli eventi della rete. Vedere [Visualizzazione di eventi a pagina 21](#).

Fare clic su **Visualizza chiave corrente** per visualizzare la chiave.

Se si sta effettuando la connessione di dispositivi senza fili non supportati da Wireless Home Network Security (ad esempio, la connessione alla rete di un palmare senza fili), attenersi alla seguente procedura.

- 1 Nella schermata Riepilogo, fare clic su **Visualizza chiave corrente**.
- 2 Annotare la chiave.
- 3 Fare clic su **Sospendi rotazione chiave**. La sospensione della rotazione della chiave impedisce che i dispositivi connessi manualmente alla rete vengano disconnessi.
- 4 Immettere la chiave nel dispositivo.

Dopo aver utilizzato questi dispositivi, fare clic su **Riprendi rotazione chiave**. Per accertarsi che la rete sia completamente protetta contro gli hacker, McAfee raccomanda di riprendere la rotazione della chiave.

Per selezionare le reti senza fili a cui connettersi o aggiungersi, fare clic con il pulsante destro del mouse sull'icona McAfee (), scegliere **Wireless Network Security** e selezionare **Reti senza fili disponibili**. Verrà visualizzata la pagina **Reti senza fili disponibili** (Figura 4-1).



Figura 4-1. Pagina Reti senza fili disponibili

Quando si è connessi a una rete senza fili protetta, le informazioni inviate e ricevute vengono crittografate. Gli hacker non possono intercettare i dati che vengono trasmessi sulla rete protetta e non possono connettersi alla rete.

 : la rete è protetta.

 : la rete è protetta utilizzando la protezione WEP o WPA-PSK.

 : la rete non è protetta ma è ancora possibile connettersi (non consigliato).

Connessione a una rete

Per connettersi a una rete, selezionare quella a cui si desidera connettersi e fare clic su **Connetti**. Se è stata configurata manualmente una chiave già condivisa per il router o l'access point, sarà necessario immettere anche la chiave.

Se la rete è protetta, prima di connettersi sarà necessario aggiungersi. Per aggiungersi alla rete, un utente già connesso alla rete dovrà fornire l'autorizzazione.

Quando ci si aggiunge a una rete, è possibile riconnettersi senza aggiungersi di nuovo. Inoltre è possibile autorizzare altri utenti ad aggiungersi alla rete.

Disconnessione da una rete

Per disconnettersi dalla rete alla quale si è connessi, fare clic su **Disconnetti**.

Utilizzo delle opzioni avanzate

Se si desidera utilizzare le opzioni di connessione avanzate, fare clic su **Avanzate**. Verrà visualizzata la finestra di dialogo **Impostazioni avanzate rete senza fili**. Dalla finestra di dialogo, è possibile eseguire le seguenti operazioni.

- Modificare l'ordine delle reti alle quali si ci connette automaticamente: la rete al primo posto nell'elenco è quella alla quale si è effettuato il collegamento l'ultima volta ed è quella alla quale Wireless Home Network Security tenta di connettersi per prima. Per spostare una rete, selezionarla e fare clic su **Sposta in alto** o **Sposta in basso**. Ad esempio, se ci si è allontanati dalla rete alla quale si è effettuato il collegamento l'ultima volta e la rete è ora troppo lontana e il segnale troppo debole, è possibile modificare la posizione delle reti nell'elenco in modo tale che la rete con il segnale più potente figuri al primo posto.
- Rimuovere le reti preferite: rimuovere le reti dall'elenco. Ad esempio, se ci si è connessi a una rete esterna per errore, questa viene inclusa nell'elenco. Per rimuoverla, selezionarla, quindi fare clic su **Rimuovi**.
- Modificare le proprietà di rete: se si verificano dei problemi di connessione a una rete non protetta, è possibile modificare le proprietà della rete. Notare che questa opzione è valida solo per le reti non protette. Per modificare le proprietà, selezionare una rete, quindi fare clic su **Proprietà**.
- Aggiungere reti che non trasmettono SSID: ad esempio se si prova a connettersi alla rete senza fili di un amico, ma questa non viene visualizzata nell'elenco, fare clic su **Aggiungi** e immettere le informazioni corrette. Notare che la rete aggiunta non può essere protetta da Wireless Home Network Security.

Configurazione delle opzioni

5

Per configurare le opzioni, fare clic con il pulsante destro del mouse sull'icona McAfee (), scegliere **Wireless Network Security**, quindi selezionare **Opzioni**. Viene visualizzata la pagina **Opzioni** (Figura 5-1).

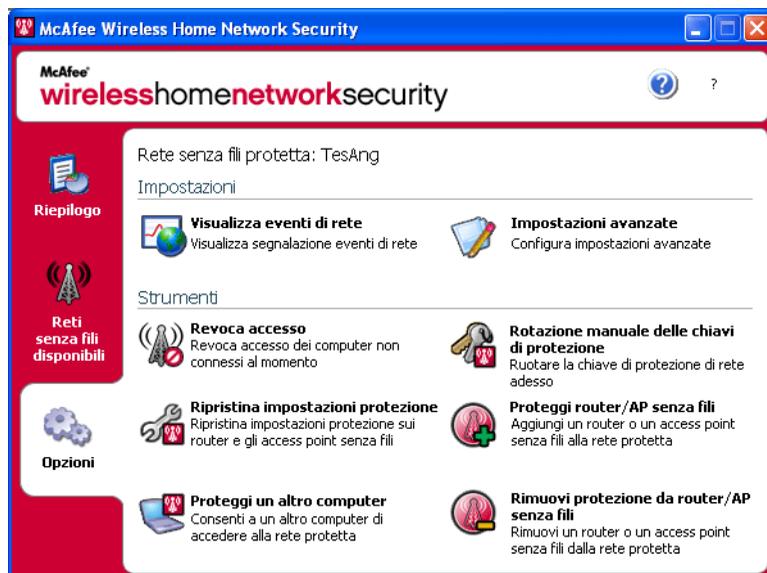


Figura 5-1. Pagina Opzioni

Visualizzazione di eventi

Le azioni eseguite da Wireless Home Network Security vengono memorizzate nei registri eventi. Per visualizzare tali registri, fare clic su **Visualizza eventi di rete**. Le informazioni vengono visualizzate in ordine cronologico per impostazione predefinita.

Nella casella **Eventi sulla rete**, è possibile selezionare il tipo di eventi visualizzati (tutti gli eventi vengono comunque registrati) nonché gli eventi per ciascuna rete di cui si fa parte (se si fa parte di più reti).

Quando si verifica un evento, viene visualizzato un avviso con una breve descrizione. Per ulteriori informazioni sugli avvisi, vedere [Indicazioni sugli avvisi a pagina 29](#).

Configurazione delle impostazioni avanzate

Questa sezione è per gli utenti più esperti. Per configurare protezione, avvisi e altre impostazioni, fare clic su **Impostazioni avanzate**.

Quando si modifica un'impostazione, affinché le modifiche vengano applicate, fare clic su **OK**. Si noti che dopo aver fatto clic su **OK**, tutti i computer connessi temporaneamente perdono la connettività per alcuni minuti.

Configurazione delle impostazioni di protezione

Per modificare le impostazioni di protezione, utilizzare la scheda **Impostazioni protezione**.

- Nome rete senza fili protetta: nome della rete corrente protetta. Quando si modifica il nome di una rete, viene visualizzato nell'elenco **Reti senza fili disponibili** ed è necessario riconnettersi alla rete. Vedere [Gestione delle reti senza fili a pagina 19](#).
- Modalità protezione: modalità di protezione corrente. Per modificare la protezione predefinita (WEP), selezionare WPA-PSK TKIP per una crittografia più efficace. Accertarsi che i router, gli access point e gli adattatori senza fili che si connettono alla rete supportino questa modalità, altrimenti non saranno in grado di connettersi. Per ulteriori informazioni sull'aggiornamento dell'adattatore, vedere [Aggiornamento dell'adattatore senza fili a pagina 38](#).
- Attiva rotazione automatica chiave: per sospendere la rotazione della chiave, deselezionare questa opzione. Per modificare la frequenza della rotazione della chiave, spostare il dispositivo di scorrimento. Per ulteriori informazioni sulla rotazione della chiave, vedere [Visualizzazione della rete senza fili protetta a pagina 18](#).
- Cambia nome utente o password: per motivi di sicurezza, è possibile modificare la password o il nome utente predefinito per il router o l'access point senza fili, selezionandolo e facendo clic su **Cambia nome utente o password**. Il nome utente o la password predefiniti sono quelli utilizzati quando si è effettuato l'accesso e la configurazione del router o dell'access point.

Configurazione delle impostazioni di avviso

Per modificare le impostazioni di avviso, utilizzare la scheda **Impostazioni avviso**.

Selezionare il tipo di eventi di cui si desidera essere avvisati e fare clic su **OK**. Se non si desidera essere avvisati riguardo alcuni tipi di eventi, deselezionare la casella appropriata.

Configurazione di altre impostazioni

Per modificare le altre impostazioni, utilizzare la scheda **Altre impostazioni**.

- **Visualizza chiavi in testo normale:** per le reti non protette da Wireless Home Network Security. Le chiavi per le reti non protette visualizzate nell'elenco **Reti senza fili disponibili** possono essere visualizzate in testo normale anziché in asterischi. Se si visualizzano le chiavi in testo normale, queste vengono eliminate per motivi di sicurezza.
- **Ignora tutte le chiavi salvate:** per le reti non protette da Wireless Home Network Security. Eliminare tutte le chiavi salvate. Si noti che se si eliminano queste chiavi, quando ci si connette alle reti WEP e WPA-PSK è necessario immettere di nuovo una chiave.
- **Abbandona rete:** per le reti protette da Wireless Home Network Security. È possibile rifiutare i diritti di accesso a una rete senza fili protetta. Ad esempio, se si desidera abbandonare una rete e si prevede di non connettersi di nuovo, selezionarla dall'elenco e fare clic su **Abbandona rete**.
- **Visualizza messaggio di notifica quando si è connessi a una rete senza fili:** quando viene effettuata una connessione, viene visualizzato un messaggio di notifica.

Revoca dell'accesso alla rete

Per impedire l'accesso alla rete da parte di computer che si sono aggiunti alla rete, ma che non sono correntemente connessi, attenersi alla seguente procedura:

- 1 Fare clic su **Revoca accesso**. Verrà visualizzata la finestra di dialogo **Revoca accesso**.
- 2 Fare clic su **Revoca**.

La rotazione della chiave viene ripristinata, i computer connessi al momento ricevono la nuova chiave e non vengono disconnessi. I computer non connessi al momento non ricevono la chiave aggiornata e devono nuovamente aggiungersi alla rete prima di potersi connettere.

Quando si revoca l'accesso a un computer, il computer deve riaggiungersi alla rete protetta prima che possa connettersi di nuovo. Per effettuare tale operazione è necessario che sul computer sia installato Wireless Home Network Security (vedere [Installazione di Wireless Home Network Security a pagina 15](#)), quindi connettersi alla rete protetta e aggiungersi di nuovo (vedere [Connessione a una rete a pagina 20](#)).

Ripristino delle impostazioni di protezione

Ripristinare le impostazioni di protezione solo se si riscontrano problemi con la rete senza fili. Per ulteriori informazioni, vedere [Impossibile connettersi a pagina 38](#).

Per correggere le impostazioni di un router o un access point sulla rete corrente, attenersi alla seguente procedura.

- 1 Fare clic su **Ripristina impostazioni protezione**. Verrà visualizzata la finestra di dialogo **Ripristina**.
- 2 Fare clic su **Ripristina**.
- 3 Al termine, fare clic su **Chiudi**.

Se non è possibile stabilire una connessione con i router o gli access point della rete, verrà visualizzato un messaggio di errore. Connettersi alla rete utilizzando un cavo, quindi tentare nuovamente il ripristino. Se la password per il router o l'access point è stata modificata, verrà richiesta la nuova password.

Protezione di altri computer

Per ottenere ulteriori informazioni su come proteggere altri computer e farli accedere alla rete protetta, fare clic su **Proteggi un altro computer**.

Per proteggere un altro computer, attenersi alla seguente procedura.

- 1 Installare McAfee Wireless Home Network Security sul computer che si desidera proteggere.
- 2 Dal computer che si sta proteggendo, fare clic con il pulsante destro del mouse sull'icona McAfee () , scegliere **Wireless Network Security**, quindi selezionare **Reti senza fili disponibili**. Verrà visualizzata la pagina **Reti senza fili disponibili**.
- 3 Selezionare una rete protetta a cui aggiungersi, quindi fare clic su **Connetti**. Per aggiungersi alla rete, è necessario ricevere l'autorizzazione da un utente già connesso alla rete.

Quando ci si aggiunge a una rete, è possibile riconnettersi senza aggiungersi di nuovo. Inoltre è possibile autorizzare altri utenti ad aggiungersi alla rete.

- 4 Fare clic su **OK** nella finestra di dialogo di conferma.

Se si sta effettuando la connessione di dispositivi senza fili non supportati da Wireless Home Network Security (ad esempio, la connessione alla rete di un palmare senza fili), attenersi alla seguente procedura.

- 1 Nella schermata Riepilogo, fare clic su **Visualizza chiave corrente**.
- 2 Annotare la chiave.
- 3 Fare clic su **Sospendi rotazione chiave**. La sospensione della rotazione della chiave impedisce che i dispositivi connessi manualmente alla rete vengano disconnessi.
- 4 Immettere la chiave nel dispositivo.

Dopo aver utilizzato questi dispositivi, fare clic su **Riprendi rotazione chiave**. Per accertarsi che la rete sia completamente protetta contro gli hacker, McAfee raccomanda di riprendere la rotazione della chiave.

Rotazione delle chiavi

Per effettuare la rotazione della chiave di protezione per la rete, fare clic su **Ruota manualmente la chiave di protezione**.

Protezione delle reti senza fili

Per proteggere un router o un access point, attenersi alla seguente procedura.

- 1 Fare clic su **Proteggi router/AP senza fili**. Verrà visualizzata la finestra di dialogo **Proteggi rete senza fili**. Se il router o l'access point non viene visualizzato nell'elenco, fare clic su **Aggiorna**.
- 2 Selezionare il router o l'access point che si desidera proteggere, quindi fare clic su **Proteggi**.

Rimozione della protezione dalle reti senza fili

È necessario essere connessi al router o all'access point senza fili dal quale si desidera rimuovere la protezione.

Per rimuovere la protezione di un router o un access point, attenersi alla seguente procedura.

- 1 Fare clic su **Rimuovi protezione router/AP senza fili**. Verrà visualizzata la finestra di dialogo **Rimuovi protezione rete senza fili**. Se il router o l'access point non viene visualizzato nell'elenco, fare clic su **Aggiorna**.
- 2 Selezionare il router o l'access point dal quale si desidera rimuovere la protezione, quindi fare clic su **Rimuovi protezione**.

Aggiornamento di Wireless Home Network Security

6

Quando si è connessi a Internet, Wireless Home Network Security verifica la disponibilità di aggiornamenti ogni quattro ore, quindi scarica e installa automaticamente gli aggiornamenti settimanali senza interrompere le operazioni in corso. Questi aggiornamenti hanno un impatto minimo sulle prestazioni del sistema durante il download.

In caso di aggiornamento di un prodotto, viene visualizzato un avviso. Quando si riceve l'avviso, è possibile aggiornare Wireless Home Network Security.

Verifica automatica della disponibilità di aggiornamenti

McAfee SecurityCenter è configurato automaticamente per verificare gli aggiornamenti di tutti i servizi McAfee ogni quattro ore quando si è connessi a Internet e per notificare tali aggiornamenti con avvisi e segnali acustici. Per impostazione predefinita, SecurityCenter scarica e installa automaticamente tutti gli aggiornamenti disponibili.

NOTA

In alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutte le applicazioni in esecuzione prima di riavviare.

Verifica manuale della disponibilità di aggiornamenti

Oltre alla verifica automatica durante la connessione a Internet, è possibile verificare manualmente la disponibilità di aggiornamenti in qualsiasi momento.

Per verificare manualmente la disponibilità di aggiornamenti di Wireless Home Network Security, attenersi alla seguente procedura:

- 1 Assicurarsi che il computer sia connesso a Internet.
- 2 Fare clic con il pulsante destro del mouse sull'icona McAfee, quindi scegliere **Aggiornamenti**. Verrà visualizzata la finestra di dialogo **Aggiornamenti di SecurityCenter**.

- 3 Fare clic su **Controlla**.

Se è disponibile un aggiornamento, verrà visualizzata la finestra di dialogo **McAfee SecurityCenter**. Fare clic su **Aggiorna** per continuare.

Se non è disponibile alcun aggiornamento, verrà visualizzata una finestra di dialogo per segnalare che Wireless Home Network Security è aggiornato. Fare clic su **OK** per chiudere la finestra di dialogo.

- 4 Se richiesto, accedere al sito Web. La **procedura guidata di aggiornamento** consente di installare automaticamente l'aggiornamento.
- 5 Al termine dell'installazione dell'aggiornamento fare clic su **Fine**.

NOTA

In alcuni casi, viene richiesto di riavviare il computer per completare l'aggiornamento. Salvare le modifiche effettuate e chiudere tutte le applicazioni in esecuzione prima di riavviare.

Gli avvisi vengono visualizzati quando si verifica un evento e notificano le modifiche apportate alla rete.

Accesso revocato

Un utente ha aggiornato la chiave di rete. Per ulteriori informazioni, vedere [Revoca dell'accesso alla rete a pagina 23](#).

Chiave di protezione rotata

La chiave di protezione per la rete è stata rotata. McAfee Wireless Home Network Security effettua la rotazione automatica della chiave di crittografia della rete, rendendo più difficile agli hacker l'intercettazione dei dati o la connessione alla rete.

Computer connesso

Un utente si è connesso alla rete. Per ulteriori informazioni, vedere [Connessione a una rete a pagina 20](#).

Computer protetto

Un utente che dispone dell'accesso alla rete protetta ha autorizzato un altro utente all'accesso. Esempio: 'Lance' ha autorizzato l'accesso a 'Mercks' e ora possono utilizzare entrambi la rete senza fili 'CoppiWAP'.

Computer sconnesso

Un utente si è sconnesso dalla rete. Per ulteriori informazioni, vedere [Disconnessione da una rete a pagina 20](#).

Configurazione di rete modificata

Un utente ha modificato la modalità di protezione per la rete. Per ulteriori informazioni, vedere [Configurazione delle impostazioni di protezione a pagina 22](#).

Frequenza della rotazione della chiave di protezione modificata

La frequenza della rotazione della chiave di protezione per la rete è stata modificata. McAfee Wireless Home Network Security effettua la rotazione automatica della chiave di crittografia della rete, rendendo più difficile agli hacker l'intercettazione dei dati o la connessione alla rete.

Impostazioni di rete modificate

Un utente sta per modificare le impostazioni di protezione della rete. La connessione verrà interrotta temporaneamente durante tale operazione. La modifica potrebbe interessare una o più delle seguenti impostazioni:

- Nome di rete
- Modalità protezione
- Frequenza della chiave sospesa
- Stato della rotazione automatica della chiave

Password modificata

Un utente ha modificato il nome utente o la password su un router o access point sulla rete. Per ulteriori informazioni, vedere [Configurazione delle impostazioni di protezione a pagina 22](#).

Rete ridenominata

Un utente ha ridenominato la rete ed è necessario connettersi di nuovo. Per ulteriori informazioni, vedere [Connessione a una rete a pagina 20](#).

Rete ripristinata

Un utente ha tentato di ripristinare la rete perché si riscontravano problemi di connessione.

Rotazione della chiave non riuscita

La rotazione della chiave non è riuscita perché:

- Le informazioni di accesso per il router o l'access point sono state modificate. Se si dispone delle informazioni di accesso, vedere [Ripristino delle impostazioni di protezione a pagina 24](#).
- La versione firmware del router o dell'access point è stata modificata con una versione che non è supportata. Per ulteriori informazioni, vedere [Impossibile connettersi a pagina 38](#).

-
- Il router o l'access point non è disponibile. Accertarsi che il router o l'access point sia attivato e che sia connesso alla rete.
 - Errore di duplicazione amministratore. Per ulteriori informazioni, vedere [Errore di amministratore duplicato a pagina 35](#).

Se si riscontrano problemi di connessione con questa rete, vedere [Ripristino delle impostazioni di protezione a pagina 24](#).

Rotazione della chiave ripresa

Un utente ha ripreso la rotazione della chiave. La rotazione della chiave impedisce agli hacker di accedere alla rete.

Rotazione della chiave sospesa

Un utente ha sospeso la rotazione della chiave. Per accertarsi che la rete sia completamente protetta contro gli hacker, McAfee raccomanda di riprendere la rotazione della chiave.

Router o access point senza fili non protetto

Un router o access point senza fili è stato rimosso dalla rete. Per ulteriori informazioni, vedere [Rimozione della protezione dalle reti senza fili a pagina 25](#).

Router o access point senza fili protetto

Un router o access point senza fili è stato protetto sulla rete. Per ulteriori informazioni, vedere [Protezione delle reti senza fili a pagina 25](#).

Questo capitolo descrive le procedure per la risoluzione dei problemi di McAfee Wireless Home Network Security e dispositivi di terzi.

Installazione

Questa sezione spiega come risolvere problemi di installazione.

Su quali computer installare questo software

Installare McAfee Wireless Home Network Security su ciascun computer senza fili nella rete (a differenza di altre applicazioni McAfee, è possibile installare questo software su diversi computer).

È possibile (ma non necessario) installarlo su computer che non dispongono di adattatori senza fili, ma il software non sarà attivo su tali computer perché non necessitano di protezione senza fili. Per proteggere la rete è necessario proteggere il router o l'access point (vedere [Protezione delle reti senza fili a pagina 25](#)) da uno dei computer senza fili.

Adattatore senza fili non rilevato

Se l'adattatore senza fili non viene rilevato al momento dell'installazione e dell'attivazione, riavviare il computer. Se l'adattatore continua a non essere rilevato dopo aver riavviato il computer, attenersi alla seguente procedura.

- 1 Aprire la finestra di dialogo **Proprietà connessione senza fili**.
- 2 Deselezionare la casella **Filtro MWL**, quindi selezionarla.
- 3 Fare clic su **OK**.

Se questo non funziona, l'adattatore senza fili potrebbe non essere supportato. Aggiornare l'adattatore o acquistarne uno nuovo. Per visualizzare un elenco di adattatori supportati, passare a <http://www.mcafee.com/it/router>. Per aggiornare l'adattatore, vedere [Aggiornamento dell'adattatore senza fili a pagina 38](#).

Più adattatori senza fili

Se un messaggio di errore conferma che sono stati installati più adattatori senza fili, è necessario disattivarne o scollegarne uno. Wireless Home Network Security funziona esclusivamente con un solo adattatore senza fili.

Impossibile effettuare il download sui computer senza fili perché la rete è già protetta

Se si dispone di un CD, installare McAfee Wireless Home Network Security dal CD su tutti i computer senza fili.

Se è stato installato il software su uno dei computer senza fili e la rete è stata protetta prima di installare il software su tutti gli altri computer senza fili, sono disponibili le seguenti opzioni.

- Rimuovere la protezione dalla rete (vedere [Rimozione della protezione dalle reti senza fili a pagina 25](#)). Quindi, scaricare il software e installarlo su tutti i computer senza fili. Proteggere di nuovo la rete (vedere [Protezione delle reti senza fili a pagina 25](#)).
- Visualizzare la chiave di rete (vedere [Visualizzazione della rete senza fili protetta a pagina 18](#)). Quindi, immettere la chiave sul computer senza fili per connettersi alla rete. Scaricare e installare il software, quindi aggiungersi alla rete dal computer senza fili (vedere [Protezione di altri computer a pagina 24](#)).
- Scaricare l'eseguibile sul computer già connesso alla rete e salvarlo su un dispositivo di memorizzazione USB o masterizzarlo su un CD in modo da poterlo installare su altri computer.

Protezione o configurazione della rete

Questa sezione spiega come risolvere i problemi di protezione e configurazione di una rete.

Router o access point non supportato

Se un errore informa che il router o l'access point senza fili non è supportato, McAfee Wireless Home Network Security non sarà stato in grado di configurare il dispositivo perché non l'ha rilevato o trovato.

Verificare di disporre della versione più recente di Wireless Home Network Security richiedendo un aggiornamento (McAfee aggiunge costantemente supporto per i nuovi router e access point). Se il router o l'access point viene visualizzato nell'elenco all'indirizzo <http://www.mcafee.com/it/router> e si riceve comunque questo errore, si stanno verificando errori di comunicazione tra il computer e il router o l'access point. Vedere [Impossibile connettersi a pagina 38](#) prima di proteggere di nuovo la rete.

Aggiornamento del firmware del router o dell'access point

Se un errore informa che il firmware del router o dell'access point senza fili non è supportato, il dispositivo in uso è supportato ma la revisione firmware del dispositivo non lo è. Verificare di disporre della versione più recente di Wireless Home Network Security richiedendo un aggiornamento (McAfee aggiunge costantemente supporto per le nuove revisioni firmware).

Se si dispone della versione più recente di Wireless Home Network Security, fare riferimento al sito Web del produttore o all'azienda di supporto per il router o l'access point e installare una nuova versione del firmware elencata in <http://www.mcafee.com/it/router>.

Errore di amministratore duplicato

Dopo aver configurato il router o l'access point, è necessario disconnettersi dall'interfaccia di amministrazione. A volte, in caso di mancata disconnessione, il router o l'access point si comporta come se fosse in fase di configurazione tramite un altro computer. In tal caso viene visualizzato un messaggio di errore.

Se non è possibile disconnettersi, scollegare l'alimentazione dal router o dall'access point, quindi ricollegarla.

La rete risulta non sicura

Se la rete risulta non sicura, non è protetta. È necessario proteggerla (vedere [Protezione delle reti senza fili a pagina 25](#)) per renderla sicura. È opportuno considerare che McAfee Wireless Home Network Security funziona soltanto con router e access point compatibili (vedere <http://www.mcafee.com/it/router>).

Impossibile ripristinare

Se non è possibile eseguire il ripristino, provare quanto riportato di seguito. Ciascuna delle seguenti procedure è indipendente.

- Connettersi alla rete utilizzando un cavo, quindi tentare nuovamente il ripristino.
- Scollegare l'alimentazione dal router o dall'access point, ricollegarlo di nuovo, quindi tentare la connessione.
- Ripristinare le impostazioni predefinite del router o dell'access point, quindi eseguire il ripristino.
- Utilizzare le opzioni avanzate, disconnettere tutti i computer dalla rete e ripristinare le impostazioni predefinite del router o dell'access point senza fili, quindi attivare la protezione.

Connessione di computer a una rete

Questa sezione spiega come risolvere i problemi di connessione dei computer a una rete.

In attesa di autorizzazione

Se si tenta di aggiungersi a una rete protetta e il computer resta nella modalità di attesa dell'autorizzazione, verificare quanto segue.

- Un computer senza fili che dispone già dell'accesso alla rete è acceso e connesso alla rete.
- È presente qualcuno per concedere l'accesso al computer quando viene visualizzato.
- I computer si trovano nel raggio di azione senza fili reciproco.

Se **Consenti accesso** non viene visualizzato sul computer che già dispone dell'accesso alla rete, provare a concedere l'accesso da un altro computer.

Se non sono disponibili altri computer, rimuovere la protezione della rete dal computer che già dispone dell'accesso e proteggere la rete dal computer che non disponeva dell'accesso. Quindi, aggiungersi alla rete dal computer che inizialmente proteggeva la rete.

Autorizzazione dell'accesso a un computer sconosciuto

Quando si riceve una richiesta di autorizzazione di accesso da un computer sconosciuto, verificarne l'identità. Potrebbe trattarsi di un tentativo di accesso illegittimo alla rete.

Connessione a una rete o a Internet

Questa sezione spiega come risolvere i problemi di connessione a una rete o a Internet.

Connessione a Internet non valida

Se non è possibile connettersi, tentare di accedere alla rete utilizzando un cavo, quindi connettersi a Internet. Se ancora non è possibile connettersi, verificare quanto segue:

- Il modem è acceso
- Le impostazioni PPPoE (vedere il [Glossario a pagina 43](#)) sono corrette
- La linea DSL o via cavo è attiva

I problemi di connettività, quali la velocità e la potenza del segnale, possono essere causati anche da interferenze di altri dispositivi senza fili. Provare a modificare il canale del telefono cordless, eliminare le possibili fonti di interferenza o cambiare la posizione del router, access point o computer senza fili.

Interruzione momentanea della connessione

Quando la connessione si interrompe temporaneamente (ad esempio, durante un gioco online), la rotazione della chiave potrebbe provocare brevi ritardi della rete. Sospendere momentaneamente la rotazione della chiave. Si consiglia di riprendere la rotazione della chiave appena si è in grado di garantire la completa protezione della rete dagli hacker.

Perdita della connessione sui dispositivi (diversi dal computer)

Se la connessione di alcuni dispositivi viene interrotta durante l'utilizzo di McAfee Wireless Home Network Security, sospendere la rotazione della chiave.

Richiesta di immissione della chiave WEP o WPA

Se è necessario immettere una chiave WEP o WPA per collegarsi alla rete, probabilmente il software non è stato installato sul computer. Per il corretto funzionamento, è necessario che Wireless Home Network Security sia installato su ciascun computer senza fili nella rete. Vedere [Protezione o configurazione della rete a pagina 34](#).

Impossibile connettersi

Se ancora non è possibile connettersi, provare quanto riportato di seguito. Ciascuna delle seguenti procedure è indipendente.

- Se non si è collegati a una rete protetta, verificare di disporre della chiave corretta e immetterla nuovamente.
- Disconnettere l'adattatore senza fili, quindi connetterlo nuovamente oppure disattivarlo e riattivarlo nuovamente.
- Spegner il router o l'access point, accenderlo nuovamente, quindi tentare la connessione.
- Verificare che il router o l'access point senza fili sia connesso e ripristinare le impostazioni di protezione (vedere [Ripristino delle impostazioni di protezione a pagina 24](#)).

Se non è possibile eseguire il ripristino, vedere [Impossibile ripristinare a pagina 35](#).

- Riavviare il computer.
- Aggiornare l'adattatore senza fili o acquistarne uno nuovo. Per aggiornare l'adattatore, vedere [Aggiornamento dell'adattatore senza fili a pagina 38](#). Ad esempio, la rete potrebbe utilizzare la protezione WPA-PSK TKIP e l'adattatore senza fili potrebbe non supportare la modalità di protezione della rete (le reti visualizzano WEP, anche se sono state impostate su WPA).
- Se non è possibile connettersi dopo aver aggiornato il router o l'access point senza fili, potrebbe essere stato eseguito l'aggiornamento a una versione non supportata. Verificare che il router o l'access point sia supportato. Se non fosse supportato, effettuare il downgrade a una versione supportata oppure attendere la disponibilità di un aggiornamento di Wireless Home Network Security.

Aggiornamento dell'adattatore senza fili

Per aggiornare l'adattatore, attenersi alla seguente procedura.

- 1 Sul desktop, fare clic su **Start**, scegliere **Impostazioni**, quindi **Pannello di controllo**.
- 2 Fare doppio clic sull'icona **Sistema**. Verrà visualizzata la finestra di dialogo **Proprietà di sistema**.
- 3 Selezionare la scheda **Hardware**, quindi fare clic su **Gestione periferiche**.
- 4 Nell'elenco **Gestione periferiche**, fare doppio clic sull'adattatore.
- 5 Selezionare la scheda **Driver** e verificare il driver a disposizione.

- 6 Visitare il sito Web del produttore dell'adattatore e verificare la disponibilità di un aggiornamento. I driver si trovano solitamente nella sezione Supporto o Download.
- 7 Se è disponibile l'aggiornamento di un driver, seguire le istruzioni riportate sul sito Web per effettuarne il download.
- 8 Tornare alla scheda **Driver**, quindi fare clic su **Aggiorna driver**. Verrà visualizzata una procedura guidata di Windows.
- 9 Seguire le istruzioni riportate sullo schermo.

Livello del segnale debole

Se la connessione si interrompe o è lenta, il livello del segnale potrebbe non essere abbastanza potente. Per migliorare il segnale, provare quanto riportato di seguito.

- Verificare che i dispositivi senza fili non siano bloccati da oggetti metallici quali bruciatori, condutture o apparecchi di grandi dimensioni. I segnali senza fili non passano attraverso questi oggetti.
- Se il segnale deve attraversare delle pareti, accertarsi che non debba essere trasmesso attraverso un angolo vuoto, più tempo il segnale impiega all'interno della parete, più si indebolisce.
- Se il router o l'access point senza fili dispone di più antenne, provare ad orientare le due antenne perpendicolarmente l'una all'altra (ad esempio, una verticale e l'altra orizzontale ad angolo di 90°).
- Alcuni produttori dispongono di antenne ad alta ricezione. Le antenne direzionali offrono un raggio d'azione più lungo, mentre le antenne omnidirezionali offrono maggiore versatilità. Consultare le istruzioni di installazione del produttore per effettuare l'installazione dell'antenna.

Se questa procedura non riesce, aggiungere un access point alla rete più vicino al computer al quale si sta tentando di connettersi. Se si configura il secondo AP con lo stesso nome di rete (SSID) e con un canale differente, l'adattatore individuerà automaticamente il segnale più potente e si collegherà attraverso l'AP appropriato.

Windows non è in grado di configurare la connessione senza fili

Ignorare eventuali messaggi che informano che Windows non è in grado di configurare la connessione senza fili. Utilizzare Wireless Home Network Security per connettersi a reti senza fili e per configurarle. Nella finestra di dialogo di Windows **Proprietà connessione senza fili**, nella scheda **Reti senza fili**, verificare che la casella **Usa Windows per configurare le impostazioni della rete senza fili** non sia selezionata.

Windows non visualizza alcuna connessione

Se si stabilisce una connessione, ignorare l'icona di rete di Windows in caso presenti una X (nessuna connessione). Si è stabilita una buona connessione.

Altri problemi

Questa sezione spiega come risolvere altri tipi di problemi.

Nome di rete differente durante l'utilizzo di altri programmi

Se il nome della rete è diverso quando viene visualizzato tramite altri programmi (ad esempio, _SafeAaf è parte del nome) non c'è da preoccuparsi. Wireless Home Network Security contrassegna le reti con un codice quando sono protette.

Problemi di configurazione dei router o degli access point senza fili

Se si verifica un errore durante la configurazione del router o dell'access point o durante l'aggiunta di più router sulla rete, verificare che tutti i router o gli access point presentino un indirizzo IP distinto.

Se il nome del router o dell'access point senza fili viene visualizzato nella finestra di dialogo **Proteggi router o access point**, ma si verifica un errore durante la configurazione, verificare che il router o l'access point sia supportato. Per visualizzare un elenco di router o access point supportati, passare a <http://www.mcafee.com/it/router>.

Se il router o l'access point è configurato, ma non sembra essere sulla rete corretta (ad esempio, non vengono visualizzati altri computer collegati alla LAN), verificare di aver configurato il router o l'access point appropriato. Scollegare l'alimentazione dal router o dall'access point e verificare che la connessione venga interrotta. Se viene configurato il router o l'access point errato, rimuovere la protezione e applicarla al router o all'access point corretto.

Se è impossibile configurare o aggiungere il router o l'access point, ma si è sicuri che sia supportato, alcune modifiche apportate potrebbero impedirne la corretta configurazione.

- Seguire le indicazioni del produttore per configurare il router o l'access point senza fili per il DHCP o per configurare il corretto indirizzo IP. In alcuni casi, il produttore fornisce uno strumento di configurazione.

- Ripristinare le impostazioni di fabbrica del router o dell'access point e provare nuovamente a ripristinare la rete. La porta di amministrazione potrebbe essere stata modificata oppure l'amministrazione senza fili potrebbe essere stata disattivata. Verificare che venga utilizzata la configurazione predefinita e che la configurazione senza fili sia attivata. Un'altra possibilità è che l'amministrazione http sia disattivata. In questo caso, verificare che l'amministrazione http sia attivata.
- Se il router o l'access point senza fili non viene visualizzato nell'elenco dei router o degli access point senza fili che è possibile proteggere o ai quali è possibile connettersi, attivare la trasmissione SSID e verificare che il router o l'access point sia attivato.
- In caso si venga disconnessi o sia impossibile stabilire una connessione, i filtri MAC potrebbero essere attivati. Disattivare i filtri MAC.
- Se non è possibile eseguire operazioni di rete (ad esempio, condividere file o eseguire la stampa su stampanti condivise) tra due computer connessi alla rete senza fili, verificare di non aver attivato l'isolamento dell'access point. L'isolamento dell'access point impedisce che i computer senza fili vengano connessi tra di loro tramite la rete.

Sostituzione di computer

Se il computer che gestisce la protezione della rete viene sostituito e non esistono altri computer che dispongono dell'accesso (è impossibile accedere alla rete), ripristinare le impostazioni di fabbrica del router o dell'access point senza fili e applicare di nuovo la protezione sulla rete.

Software non funzionante in seguito all'aggiornamento dei sistemi operativi

Se Wireless Home Network Security non funziona dopo aver aggiornato i sistemi operativi, disinstallare e installare nuovamente il programma.

802.11

Insieme di standard IEEE per la tecnologia LAN senza fili. 802.11 specifica un'interfaccia over-the-air tra un client senza fili e una stazione di base o tra due client senza fili. Diverse specifiche di 802.11 includono 802.11a, uno standard per una connessione di rete fino a 54 Mbps nella banda da 5 GHz, 802.11b, uno standard per una connessione di rete fino a 11 Mbps nella banda da 2,4 GHz, 802.11g, uno standard per una connessione di rete fino a 54 Mbps nella banda da 2,4 GHz e 802.11i, una suite di standard di protezione per tutte le Ethernet senza fili.

802.11a

Estensione di 802.11 che si applica alle LAN senza fili e invia dati fino a 54 Mbps nella banda da 5 GHz. Nonostante la velocità di trasmissione sia superiore che in 802.11 b, la distanza coperta è di gran lunga inferiore.

802.11b

Estensione di 802.11 che si applica alle LAN senza fili e fornisce la trasmissione da 11 Mbps nella banda da 2,4 GHz. 802.11b è attualmente considerato lo standard senza fili.

802.11g

Estensione di 802.11 che si applica alle LAN senza fili e fornisce fino a 54 Mbps nella banda da 2,4 GHz.

802.1x

Non supportato da Wireless Home Network Security. Si tratta di uno standard IEEE per l'autenticazione su reti cablate e senza fili, ma viene utilizzato soprattutto insieme alla connessione di rete senza fili 802.11. Questo standard fornisce un'autenticazione reciproca e potente tra un client e un server di autenticazione. Inoltre, 802.1x può fornire chiavi WEP dinamiche utente per utente e per sessione, diminuendo il carico amministrativo e i rischi per la protezione legati alle chiavi WEP statiche.

A

Access Point (AP)

Dispositivo di rete che consente ai client 802.11 di connettersi a una rete locale (LAN). Gli AP estendono la gamma fisica di servizi per un utente senza fili. Talvolta sono denominati router senza fili.

Access point pericoloso

Access point di cui un'azienda non autorizza il funzionamento. Questo tipo di access point spesso non è conforme ai criteri di protezione della LAN senza fili (WLAN). Un access point pericoloso attiva un'interfaccia non protetta e aperta alla rete aziendale dall'esterno della struttura fisicamente controllata.

All'interno di una WLAN correttamente protetta, gli access point pericolosi sono più dannosi degli utenti pericolosi. Se sono attivi dei meccanismi di autenticazione efficaci, è probabile che gli utenti non autorizzati che tentano l'accesso a una WLAN non riescano a raggiungere le preziose risorse aziendali. Maggiori problemi sorgono, tuttavia, quando un impiegato o un hacker si collega a un access point pericoloso. Questo, infatti, consente l'accesso alla rete aziendale a chiunque disponga di un dispositivo dotato di 802.11, consentendogli di avvicinarsi a importanti risorse.

Adattatore senza fili

Contiene i circuiti che consentono a un computer o altri dispositivi di comunicare con un router senza fili (collegamento a una rete senza fili). Gli adattatori senza fili possono essere incorporati nei circuiti principali di un dispositivo hardware oppure essere costituiti da un componente aggiuntivo a parte da inserire nel dispositivo mediante un'apposita porta.

Attacco di forza bruta

Noto anche come brute force cracking, si tratta di un metodo di prova ed errore utilizzato da applicazioni per decodificare dati crittografati come le password, mediante uno sforzo notevole (mediante la forza bruta) piuttosto che impiegando strategie intellettuali. Proprio come un criminale potrebbe forzare una cassaforte o aprirla tentando diverse combinazioni possibili, un'applicazione che utilizza la forza bruta procede attraverso tutte le possibili combinazioni dei caratteri consentiti in sequenza. L'uso della forza bruta è considerato un approccio infallibile anche se piuttosto lungo.

Attacco di tipo Dictionary

Tipo di attacco che consiste nei tentativi di individuare le password utilizzando una gran quantità di parole contenute in un elenco. Gli hacker non tentano manualmente tutte le combinazioni, ma dispongono di strumenti che tentano automaticamente di identificare una determinata password.

Attacco di tipo Man-in-the-Middle

L'hacker intercetta i messaggi in uno scambio di chiavi pubbliche e li ritrasmette sostituendone la chiave pubblica con quella richiesta, in modo che le due parti originarie risultino ancora in comunicazione diretta tra loro. L'hacker utilizza un programma che al client sembra il server e al server sembra il client. L'attacco può essere utilizzato semplicemente per ottenere accesso ai messaggi o per consentire all'hacker di modificarli prima di trasmetterli di nuovo. Il termine deriva da un gioco in cui i partecipanti tentano di lanciarsi una palla mentre un altro giocatore nel mezzo tenta di afferrarla.

Autenticazione

Processo di identificazione di un individuo, di solito basato su un nome utente e una password. L'autenticazione verifica l'autenticità dell'identità dichiarata dall'utente, ma non fornisce alcun dato sui suoi diritti di accesso.

B

C

Chiave

Serie di lettere e/o numeri utilizzata da due dispositivi per autenticarne la comunicazione. Entrambi i dispositivi devono disporre di una chiave. Vedere anche WEP e WPA-PSK.

Client

Applicazione eseguita su PC o workstation e risiedente su un server per l'esecuzione di alcune operazioni. Ad esempio, un client di posta elettronica è un'applicazione che consente l'invio e la ricezione di messaggi di posta elettronica.

Crittografia

Conversione dei dati in un codice segreto. La crittografia è il modo più efficace per ottenere una protezione dei dati. Per leggere un file crittografato, è necessario disporre di una chiave o una password segreta che ne consenti la codifica. I dati non crittografati sono detti testo normale; i dati crittografati sono detti testo in codice.

D

E

ESS (Extended Service Set)

Insieme di una o più reti che formano un'unica sottorete.

F

Firewall

Sistema progettato per impedire l'accesso non autorizzato a o da una rete privata. I firewall possono essere implementati sia nell'hardware che nel software o con una combinazione di entrambi. I firewall vengono utilizzati di frequente per impedire a utenti Internet non autorizzati di accedere a reti private connesse a Internet, specialmente a una intranet. Tutti i messaggi in entrata o in uscita da una intranet passano attraverso il firewall. Il firewall esamina tutti i messaggi e blocca quelli non conformi ai criteri di protezione specificati. È considerato la prima linea di difesa nella protezione delle informazioni private. Per una maggiore protezione, è possibile crittografare i dati.

G

Gateway integrato

Dispositivo che combina le funzioni di access point (AP), router e firewall. Alcuni dispositivi possono persino includere funzionalità avanzate di protezione e bridging.

H

Hotspot

Specifico luogo geografico in cui un access point (AP) fornisce servizi pubblici di rete a banda larga senza fili a visitatori mobili attraverso una rete senza fili. Gli hotspot si trovano spesso in luoghi particolarmente affollati come gli aeroporti, le stazioni ferroviarie, le librerie, i porti marittimi, i centri congressuali e gli alberghi. Di solito dispongono di una portata di accesso limitata.

I

Indirizzo IP

Identificativo di un computer o un dispositivo su una rete TCP/IP. Le reti che utilizzano il protocollo TCP/IP instradano i messaggi in base all'indirizzo IP della destinazione. L'indirizzo IP presenta il formato di un indirizzo dinamico a 32 bit espresso con quattro numeri separati da punti. Ogni numero può essere compreso tra zero e 255. Ad esempio, 192.168.1.100 può essere un indirizzo IP.

Indirizzo MAC (Media Access Control Address)

Indirizzo di livello basso assegnato al dispositivo fisico che accede alla rete.

J

K

L

LAN (Local Area Network)

Rete di computer che si estende in un'area relativamente ridotta. Molte LAN sono ristrette a un solo edificio o gruppo di edifici. Tuttavia, una LAN può essere connessa ad altre LAN a qualunque distanza tramite telefono e onde radio. Un sistema di LAN connesse in questo modo è detto WAN (Wide-Area Network).

Molte LAN si connettono a workstation e PC di solito mediante semplici hub o switch. Ciascun nodo (singolo computer) in una LAN dispone della propria CPU con cui esegue programmi, ma è anche in grado di accedere ai dati e ai dispositivi (ad esempio le stampanti) presenti in qualsiasi punto della LAN. In tal modo, molti utenti possono condividere dispositivi costosi, come le stampanti laser, nonché i dati. Gli utenti, inoltre, possono utilizzare la LAN per comunicare tra di loro, ad esempio inviando messaggi di posta elettronica o avviando sessioni di chat.

Larghezza di banda

Quantità di dati trasmettibili in un lasso di tempo fisso. Per i dispositivi digitali, la larghezza di banda di solito viene espressa in bit per secondo (bps) o byte per secondo. Per i dispositivi analogici, la larghezza di banda viene espressa in cicli per secondo o Hertz (Hz).

M

MAC (Media Access Control o Message Authenticator Code)

Per il primo significato, vedere Indirizzo MAC. Il secondo è un codice utilizzato per identificare un determinato messaggio (ad esempio, un messaggio RADIUS). Il codice generalmente è un hash dei contenuti del messaggio sottoposto a potente crittografica, che include un valore univoco per garantire una protezione contro la riproduzione.

N

Negazione del servizio

Su Internet un attacco di negazione del servizio (DoS - Denial of Service) è un incidente durante il quale un utente o un'organizzazione vengono privati dei servizi di una risorsa solitamente disponibile. Una tipica perdita di servizio è la mancanza di disponibilità di un particolare servizio di rete, ad esempio la posta elettronica, o la perdita temporanea di tutti i servizi e della connettività di rete. Nei casi peggiori, ad esempio, un sito Web a cui accedono milioni di persone può essere occasionalmente forzato a interrompere temporaneamente il funzionamento. Un attacco di negazione del servizio può anche distruggere i programmi e i file in un sistema informatico. Per quanto di solito sia intenzionale e pericoloso, un attacco di negazione del servizio talvolta può capitare accidentalmente. Un attacco di negazione del servizio è un tipo di violazione della protezione di un sistema informatico che di solito non comporta il furto di informazioni o altre perdite di protezione. Tuttavia, questi attacchi possono costare alla persona o all'azienda che li riceve una gran quantità di tempo e denaro.

NIC (Network Interface Card)

Scheda che si inserisce in un laptop o in altro dispositivo e connette il dispositivo alla LAN.

O

P

PPPoE

Point-to-Point Protocol Over Ethernet (Protocollo punto a punto su Ethernet). Utilizzato da molti provider DSL, PPPoE supporta i livelli di protocollo e l'autenticazione ampiamente utilizzata in PPP e consente di stabilire la connessione point-to-point nell'architettura solitamente multipunto di Ethernet.

Protocollo

Formato concordato per la trasmissione di dati tra due dispositivi. Dal punto di vista di un utente, l'unico aspetto rilevante dei protocolli è che il computer o il dispositivo deve supportare quelli appropriati, se desidera comunicare con altri computer. Il protocollo può essere implementato nell'hardware o nel software.

Q

R

RADIUS (Remote Access Dial-In User Service)

Protocollo che fornisce l'autenticazione degli utenti, di solito nel contesto dell'accesso remoto. Inizialmente definito per l'uso con i server di accesso remoto dial-in, il protocollo viene ora utilizzato in un'ampia gamma di ambienti di autenticazione, inclusa l'autenticazione 802.1x di un segreto condiviso degli utenti di una WLAN.

Rete

Insieme di access point e dei relativi utenti, equivalente a un ESS. Informazioni su questa rete vengono gestite in McAfee Wireless Home Network Security. Vedere ESS.

Roaming

Capacità di spostarsi da un'area a copertura AP a un'altra senza interruzione di servizio o perdita di connettività.

Router

Dispositivo di rete che inoltra pacchetti da una rete all'altra. Sulla base di tabelle di instradamento interne, i router leggono ogni pacchetto in ingresso e decidono come inoltrarlo. L'interfaccia sul router alla quale i pacchetti in uscita vengono inviati può essere determinata da una combinazione dell'indirizzo di origine e di destinazione, nonché dalle attuali condizioni di traffico come carico, costi della linea e linee non valide. Talvolta sono denominati access point (AP).

S

Schede senza fili PCI

Connettono un computer desktop a una rete. La scheda si inserisce in uno slot di espansione PCI all'interno del computer.

Schede senza fili USB

Forniscono un'interfaccia seriale Plug and Play espandibile. Questa interfaccia fornisce una connessione senza fili standard e a basso costo per periferiche come tastiere, mouse, joystick, stampanti, scanner, dispositivi di archiviazione e videocamere per conferenze.

Segreto condiviso

Vedere anche RADIUS. Protegge parti riservate dei messaggi RADIUS. Il segreto condiviso è una password che può essere condivisa dall'autenticatore e dal server di autenticazione in maniera protetta.

Spoofing degli indirizzi IP

Contraffazione di indirizzi IP in un pacchetto IP. Viene utilizzato in molti tipi di attacchi, incluso il dirottamento di sessione. Viene inoltre impiegato per contraffare le intestazioni dei messaggi di posta elettronica di SPAM in modo da impedirne la corretta individuazione.

SSID (Service Set Identifier)

Nome di rete per i dispositivi in un sottosistema LAN senza fili. Si tratta di una stringa di testo non crittografata, contenente 32 caratteri, aggiunta all'inizio di ogni pacchetto WLAN. L'SSID differenzia una WLAN dall'altra, per cui tutti gli utenti di una rete devono fornire lo stesso SSID per accedere a un determinato AP. L'SSID impedisce l'accesso a qualsiasi dispositivo client che non disponga dell'SSID. Tuttavia, per impostazione definita un access point (AP) trasmette il proprio SSID nella sua ricetrasmittente. Anche se la trasmissione SSID è disattivata, un hacker può rilevare l'SSID attraverso lo sniffing.

SSL (Secure Sockets Layer)

Protocollo sviluppato da Netscape per la trasmissione di documenti privati tramite Internet. L'SSL funziona utilizzando una chiave pubblica per crittografare i dati trasferiti sulla connessione SSL. Sia Netscape Navigator che Internet Explorer utilizzano e supportano SSL e molti siti Web utilizzano il protocollo per ottenere informazioni riservate dell'utente, come i numeri di carta di credito. Per convenzione, gli URL che richiedono una connessione SSL iniziano con https: invece di http:.

T

Testo in codice

Dati crittografati. Il testo in codice è illeggibile finché non viene convertito in testo normale (decriptografato) con una chiave.

Testo normale

Qualsiasi messaggio non crittografato.

TKIP (Temporal Key Integrity Protocol)

Metodo di correzione rapida per superare la debolezza inerente alla protezione WEP, in particolare il riutilizzo delle chiavi di crittografia. TKIP modifica le chiavi temporali ogni 10.000 pacchetti, fornendo un metodo di distribuzione dinamica che migliora notevolmente la protezione della rete. Il processo (di protezione) TKIP inizia con una chiave temporale da 128 bit condivisa tra client e access point (AP). TKIP combina la chiave temporale con l'indirizzo MAC (del computer client) e aggiunge un vettore di inizializzazione da 16 ottetti relativamente grande per produrre la chiave che crittografa i dati. Questa procedura assicura che ogni stazione utilizzi flussi di chiavi differenti per crittografare i dati. TKIP utilizza RC4 per eseguire la crittografia. WEP utilizza anche RC4.

U

V

VPN (Virtual Private Network)

Rete costruita utilizzando cavi pubblici per la riunione dei nodi. Ad esempio, esistono molti sistemi che consentono di creare reti utilizzando Internet come mezzo di trasmissione dei dati. Tali sistemi utilizzano la crittografia e altri meccanismi di protezione per garantire che solo gli utenti autorizzati possano accedere alla rete e che i dati non possano essere intercettati.

W

Wardriver

Intrusi armati di laptop, software speciale e qualche hardware di fortuna che girano per città, sobborghi e parchi aziendali per intercettare il traffico LAN senza fili.

WEP (Wired Equivalent Privacy)

Protocollo di crittografia e autenticazione definito come parte dello standard 802.11. Le versioni iniziali sono basate su codici RC4 e sono caratterizzate da una notevole vulnerabilità. WEP tenta di fornire la protezione crittografando i dati su onde radio, in modo che siano protetti durante la trasmissione da un'estremità all'altra. Tuttavia, si è scoperto che WEP non è tanto sicuro come si credeva.

Wi-Fi (Wireless Fidelity)

Utilizzato genericamente quando ci si riferisce a qualunque tipo di rete 802.11, che sia 802.11b, 802.11a, dual-band, ecc. Il termine è utilizzato da Wi-Fi Alliance.

Wi-Fi Alliance

Organizzazione costituita da fornitori leader nel software e nei dispositivi senza fili con la missione di (1) certificare l'interfunzionalità di tutti i prodotti basati su 802.11 e di (2) promuovere il termine Wi-Fi come nome di marchio globale in tutti i mercati per qualsiasi prodotto LAN senza fili basato su 802.11. L'organizzazione funge da consorzio, laboratorio di collaudo e centro di raccolta e smistamento per i fornitori che desiderano promuovere l'interfunzionalità e lo sviluppo di questo settore.

Mentre tutti i prodotti 802.11a/b/g sono detti Wi-Fi, solo i prodotti che hanno superato la verifica Wi-Fi Alliance possono essere definiti Wi-Fi Certified (un marchio registrato). I prodotti che superano la verifica mostrano un sigillo di identificazione sulla confezione che segnala il prodotto come Wi-Fi Certified e che indica la banda di frequenza radio utilizzata. Questo gruppo prima era noto con il nome di Wireless Ethernet Compatibility Alliance (WECA), ma ha modificato il nome nell'ottobre 2002 per rispecchiare meglio il marchio Wi-Fi che desidera costruire.

Wi-Fi Certified

Tutti i prodotti collaudati e approvati come Wi-Fi Certified (un marchio registrato) da Wi-Fi Alliance sono interfunzionanti gli uni con gli altri, anche se realizzati da produttori diversi. Un utente che dispone di un prodotto Wi-Fi Certified può utilizzare un access point (AP) di qualunque marchio con hardware client di qualsiasi altro marchio altrettanto certificato. Tuttavia, in genere, tutti i prodotti Wi-Fi che utilizzano la stessa frequenza di onde radio (ad esempio, 2,4 GHz per 802.11b o 11g, 5 GHz per 802.11a) di altri prodotti funzionano senza problemi, anche se non sono Wi-Fi Certified.

WLAN (Wireless Local Area Network)

Vedere anche LAN. Rete locale che utilizza supporto senza fili per la connessione. Per comunicare tra nodi, una WLAN utilizza onde radio ad alta frequenza anziché cavi.

WPA (Wi-Fi Protected Access)

Standard di specifiche che aumenta notevolmente il livello di protezione dei dati e il controllo dell'accesso dei sistemi LAN senza fili esistenti e futuri. Progettato per funzionare sull'hardware esistente come aggiornamento software, WPA è derivato dallo standard IEEE 802.11i ed è compatibile con esso. Se correttamente installato, garantisce agli utenti della LAN senza fili un elevato livello di protezione dei dati e che solo utenti di rete autorizzati potranno accedere alla rete.

WPA-PSK

Una speciale modalità WPA progettata per gli utenti privati che non richiedono una potente protezione di classe aziendale e non hanno accesso a server di autenticazione. In tal modo, l'utente privato inserisce manualmente la password iniziale per attivare l'accesso protetto Wi-Fi in modalità PSK (Chiave già condivisa) e deve regolarmente cambiare la passphrase su ogni access point e computer senza fili. Vedere anche TKIP.

X

Y

Z

Indice

A

aggiornamento di Wireless Home Network Security
verifica automatica degli aggiornamenti, 27
verifica manuale degli aggiornamenti, 27
avvisi, 29

C

chiavi, rotazione, 25
configurazione guidata, uso, 16
connessione, visualizzazione, 17

E

eventi, visualizzazione, 21

F

funzioni, 11

G

glossario, 43

I

impostazioni avanzate
altro, 23
avvisi, 22
protezione, 22
impostazioni, ripristino, 24

M

McAfee SecurityCenter, 13

O

opzioni
avanzate, 20
configurazione, 21
Opzioni, pagina, 21

P

protezione dei computer, 24

R

requisiti di sistema, 12
rete
connessione, 20
disconnessione, 20
protezione, 25
revoca dell'accesso, 23
rimozione della protezione, 25
visualizzazione, 18
Reti senza fili disponibili, pagina, 19
Riepilogo, pagina, 17
risoluzione dei problemi, 33

S

scheda di avvio rapido, iii

W

Wireless Home Network Security
installazione, 15
introduzione, 10
utilizzo, 9