McAfee®

VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

Guida dell'utente

Sommario

CAPITOLO 1

Introduzione

McAfee VirusScan Plus offre protezione proattiva al PC per bloccare attacchi dannosi e consentire all'utente di proteggere ciò a cui tiene, nonché di navigare, effettuare ricerche ed eseguire il download di file in tutta sicurezza. Le classificazioni di sicurezza Web di McAfee SiteAdvisor aiutano ad evitare siti Web pericolosi. Questo servizio fornisce inoltre protezione dagli attacchi su più fronti integrando le tecnologie antivirus, antispyware e firewall. Il servizio di protezione di McAfee distribuisce il software più recente in modo continuativo, affinché la protezione sia sempre aggiornata. Ora è possibile aggiungere protezione e gestirla senza difficoltà su più PC in ambiente domestico, senza contare che il miglioramento delle prestazioni consente di offrire una protezione non invadente, riducendo al minimo l'interferenza con le attività dell'utente.

In questo capitolo

CAPITOLO 2

McAfee SecurityCenter

McAfee SecurityCenter consente di monitorare lo stato della protezione del computer, stabilire immediatamente se i servizi di protezione del computer relativi a virus, spyware, posta elettronica e firewall sono aggiornati e intervenire sulle eventuali vulnerabilità dei sistemi di protezione utilizzati. Fornisce inoltre gli strumenti e i controlli di navigazione necessari per coordinare e gestire tutte le aree di protezione del computer.

Prima di iniziare a configurare e gestire la protezione del computer, è opportuno esaminare l'interfaccia di SecurityCenter e assicurarsi di comprendere la differenza tra stato della protezione, categorie di protezione e servizi di protezione. Quindi, per assicurarsi di avere a disposizione la protezione McAfee più recente, è necessario aggiornare SecurityCenter.

Dopo aver completato le attività iniziali di configurazione, utilizzare SecurityCenter per monitorare lo stato della protezione del computer. Nel caso in cui rilevi un problema di protezione, SecurityCenter lo segnala per consentire all'utente di risolverlo o ignorarlo, in base alla gravità. È anche disponibile un registro eventi in cui è possibile esaminare gli eventi di SecurityCenter, ad esempio eventuali modifiche di configurazione della scansione antivirus.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di SecurityCenter

SecurityCenter offre le funzioni riportate di seguito:

Stato della protezione semplificato

Consente un controllo semplificato dello stato della protezione del computer, la verifica della disponibilità di aggiornamenti e la risoluzione dei potenziali problemi di protezione.

Aggiornamenti automatici

Consente di eseguire automaticamente il download e l'installazione degli aggiornamenti dei programmi registrati. Le nuove versioni dei programmi McAfee registrati possono essere ottenute gratuitamente non appena risultano disponibili, purché l'abbonamento sia ancora valido, in modo tale da garantire una protezione sempre aggiornata.

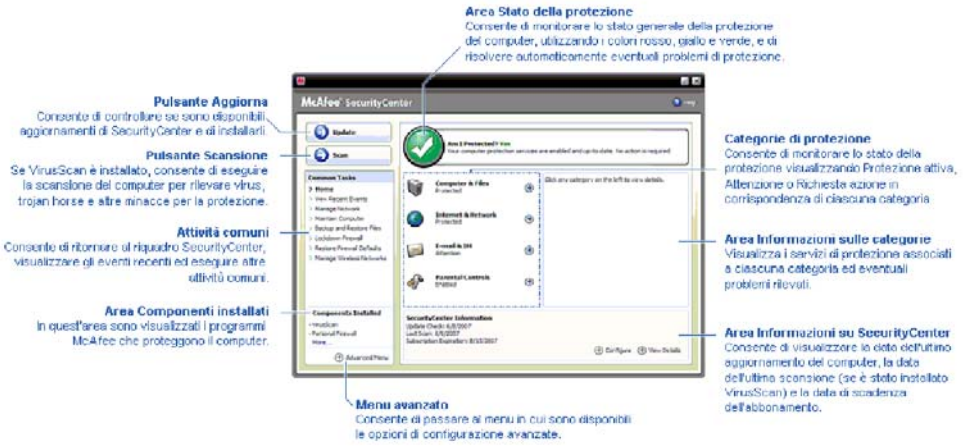
Avvisi in tempo reale

Gli avvisi di protezione notificano all'utente la diffusione di virus e di minacce per la protezione e forniscono opzioni che consentono di rimuovere e neutralizzare la minaccia o di ottenere ulteriori informazioni su di essa.

CAPITOLO 3

Utilizzo di SecurityCenter

Prima di iniziare a utilizzare SecurityCenter, esaminare i componenti e le aree di configurazione da utilizzare per gestire lo stato della protezione del computer. Per ulteriori informazioni sulla terminologia utilizzata nell'immagine, vedere le sezioni Informazioni sullo stato della protezione (pagina 8) e Informazioni sulle categorie di protezione (pagina 9). Esaminare quindi le informazioni relative al proprio account McAfee e verificare la validità del proprio abbonamento.



In questo capitolo

Informazioni sullo stato della protezione

Lo stato della protezione del computer in uso è riportato in un'apposita area del riquadro SecurityCenter. Lo stato indica se il computer è completamente protetto contro le minacce per la protezione più recenti e se può subire gli effetti causati, ad esempio, da un attacco informatico esterno, da un altro programma di protezione o da un programma che accede a Internet.

Lo stato della protezione del computer può essere rosso, giallo o verde.

Stato della protezione	Descrizione
Rosso	Il computer non è protetto. L'area dello stato della protezione del riquadro SecurityCenter è rossa e indica che il computer non è protetto. SecurityCenter segnala la presenza di almeno un problema critico di protezione. Per ottenere una protezione completa, è necessario risolvere tutti i problemi critici in ciascuna categoria di protezione. Lo stato della categoria del problema, anch'esso visualizzato in rosso, è impostato su **Necessaria azione**. Per informazioni su come risolvere i problemi di protezione, consultare la sezione Risoluzione dei problemi di protezione (pagina 18).
Giallo	Il computer è parzialmente protetto. L'area dello stato della protezione del riquadro SecurityCenter è gialla e indica che il computer non è protetto. SecurityCenter segnala la presenza di almeno un problema non critico di protezione. Per ottenere una protezione completa, è necessario risolvere o ignorare i problemi non critici associati a ogni categoria di protezione. Per informazioni su come risolvere o ignorare i problemi di protezione, vedere Risoluzione o esclusione dei problemi di protezione (pagina 17).
Verde	Il computer è completamente protetto. L'area dello stato della protezione del riquadro SecurityCenter è verde e indica che il computer è protetto. SecurityCenter non segnala alcun problema di protezione critico o non critico. In ogni categoria di protezione sono elencati i servizi che proteggono il computer.

Informazioni sulle categorie di protezione

I servizi di protezione di SecurityCenter sono suddivisi in quattro categorie: Computer e file, Internet e rete, Posta elettronica e MI e Controllo genitori. Queste categorie consentono di identificare e configurare i servizi di protezione del computer.

Per configurare i servizi di protezione di una determinata categoria e visualizzare i problemi di protezione rilevati per tali servizi, è sufficiente fare clic sulla categoria. Se lo stato di protezione del computer è rosso o giallo, per una o più categorie viene visualizzato il messaggio *Necessaria azione* o *Attenzione*, che indica che SecurityCenter ha rilevato un problema all'interno della categoria. Per ulteriori informazioni sullo stato della protezione, consultare la sezione Informazioni sullo stato della protezione (pagina 8).

Categoria di protezione	Descrizione
Computer e file	La categoria Computer e file consente di configurare i seguenti servizi di protezione: ▪ Protezione da virus ▪ Protezione da PUP ▪ Monitor di sistema ▪ Protezione di Windows
Internet e rete	La categoria Internet e rete consente di configurare i seguenti servizi di protezione: ▪ Protezione firewall ▪ Protezione dell'identità
Posta elettronica e MI	La categoria Posta elettronica e MI consente di configurare i seguenti servizi di protezione: ▪ Protezione della posta elettronica ▪ Protezione da posta indesiderata
Controllo genitori	La categoria Controllo genitori consente di configurare i seguenti servizi di protezione: ▪ Blocco contenuti

Informazioni sui servizi di protezione

I servizi di protezione rappresentano i componenti fondamentali di SecurityCenter da configurare per proteggere il proprio computer. Ogni servizio di protezione corrisponde direttamente a un programma McAfee. Quando si installa il programma VirusScan, ad esempio, nel sistema vengono attivati i seguenti servizi di protezione: protezione da virus, protezione da PUP, monitor di sistema e protezione di Windows. Per ottenere informazioni dettagliate su questi servizi di protezione, consultare la Guida di VirusScan.

Quando si installa un programma, tutti i servizi di protezione ad esso associati vengono attivati per impostazione predefinita. I servizi di protezione possono tuttavia essere disattivati in qualsiasi momento. Se ad esempio si installa Privacy Service, i servizi Blocco contenuti e Protezione dell'identità vengono entrambi attivati. Se non si desidera utilizzare il servizio di protezione Blocco contenuti, è possibile disattivarlo completamente. È anche possibile disattivare temporaneamente un servizio di protezione durante l'esecuzione di attività di configurazione o di manutenzione.

Gestione dell'account McAfee

Il proprio account McAfee può essere gestito direttamente tramite SecurityCenter, che consente di accedere facilmente alle informazioni relative all'account e di verificare lo stato corrente del proprio abbonamento.

Nota: i programmi McAfee installati da CD devono essere registrati sul sito Web di McAfee per configurare o aggiornare il proprio account McAfee. Solo dopo aver completato questa operazione si ha diritto agli aggiornamenti automatici e periodici dei programmi.

Come gestire l'account McAfee

SecurityCenter consente di accedere facilmente alle informazioni relative al proprio account McAfee.

1. Nella sezione **Attività comuni**, fare clic su **Account**.
2. Accedere al proprio account McAfee.

Come verificare l'abbonamento

È necessario verificare il proprio abbonamento per accertarsi che non sia scaduto.

- Fare clic con il pulsante destro del mouse sull'icona di SecurityCenter nell'area di notifica, all'estremità destra della barra delle applicazioni, quindi scegliere **Verifica abbonamento**.

CAPITOLO 4

Aggiornamento di SecurityCenter

Per garantire che i programmi McAfee registrati in uso siano sempre aggiornati, SecurityCenter verifica ogni quattro ore la disponibilità di aggiornamenti in linea ed eventualmente li installa. In base ai programmi installati e registrati, gli aggiornamenti in linea possono includere le definizioni più recenti dei virus nonché gli aggiornamenti della protezione della privacy o da hacker, posta indesiderata e spyware. È possibile verificare la disponibilità di aggiornamenti in qualsiasi momento durante l'intervallo predefinito di quattro ore. Mentre SecurityCenter verifica la disponibilità di aggiornamenti, è possibile proseguire con altre attività.

Benché non sia consigliato, è possibile modificare la modalità con cui SecurityCenter verifica e installa gli aggiornamenti. Ad esempio, è possibile configurare SecurityCenter in modo tale da scaricare ma non installare gli aggiornamenti o per ricevere una notifica prima di eseguire il download o l'installazione degli aggiornamenti. È inoltre possibile disattivare l'aggiornamento automatico.

Nota: per avere accesso agli aggiornamenti automatici e periodici, i programmi McAfee installati da CD devono essere registrati sul sito Web di McAfee.

In questo capitolo

Come verificare la disponibilità di aggiornamenti

Per impostazione predefinita, quando si è connessi a Internet, SecurityCenter verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore, tuttavia è possibile effettuare manualmente la verifica durante l'intervallo di quattro ore. Se gli aggiornamenti automatici sono stati disattivati, è responsabilità dell'utente verificare periodicamente la disponibilità di aggiornamenti.

- Nel riquadro SecurityCenter, fare clic su **Aggiorna**.

Suggerimento: per verificare la disponibilità di aggiornamenti senza avviare SecurityCenter, è possibile fare clic con il pulsante destro del mouse sull'icona di SecurityCenter nell'area di notifica all'estremità destra della barra delle applicazioni e quindi fare clic su **Aggiornamenti**.

Come configurare gli aggiornamenti automatici

Per impostazione predefinita, quando si è connessi a Internet, SecurityCenter esegue automaticamente la ricerca e l'installazione degli aggiornamenti ogni quattro ore. Se si desidera modificare il funzionamento predefinito, è possibile configurare SecurityCenter in modo tale che esegua automaticamente il download degli aggiornamenti e quindi visualizzi un avviso quando gli aggiornamenti sono pronti per l'installazione o per ricevere una notifica prima di scaricare gli aggiornamenti.

Nota: SecurityCenter indica che gli aggiornamenti sono pronti per essere scaricati o installati mediante un avviso. In base all'avviso è possibile scaricare, installare o posticipare gli aggiornamenti. Quando si aggiorna un programma a partire da un avviso, è possibile che venga richiesto di verificare l'abbonamento prima di procedere al download e all'installazione. Per ulteriori informazioni, vedere Utilizzo degli avvisi (pagina 23).

1. Aprire il riquadro di configurazione di SecurityCenter.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, in **Informazioni su SecurityCenter**, fare clic su **Configura**.

2. Nel riquadro di configurazione di SecurityCenter, in **Gli aggiornamenti automatici non sono attivi**, fare clic su **Attiva** e quindi su **Avanzate**.
3. Fare clic su uno dei seguenti pulsanti:
   - **Installa automaticamente gli aggiornamenti e avvisa quando i servizi vengono aggiornati (consigliato)**

- **Scarica automaticamente gli aggiornamenti e avvisa quando sono pronti per l'installazione**
- **Avvisa prima di scaricare aggiornamenti**

4 Fare clic su **OK**.

Come disattivare gli aggiornamenti automatici

Se si disattivano gli aggiornamenti automatici, l'utente dovrà verificare periodicamente la disponibilità di aggiornamenti per assicurarsi che il computer disponga della protezione più aggiornata. Per informazioni sulla verifica manuale della disponibilità di aggiornamenti, vedere Come verificare la disponibilità di aggiornamenti (pagina 14).

1 Aprire il riquadro di configurazione di SecurityCenter.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, in **Informazioni su SecurityCenter**, fare clic su **Configura**.

2 Nel riquadro di configurazione di SecurityCenter, in **Gli aggiornamenti automatici sono attivi**, fare clic su **Disattiva**.

Suggerimento: per attivare gli aggiornamenti automatici, fare clic sul pulsante **Attiva** o deselezionare l'opzione **Disattiva l'aggiornamento automatico e consenti la ricerca manuale di aggiornamenti** nel riquadro Opzioni di aggiornamento.

CAPITOLO 5

Risoluzione o esclusione dei problemi di protezione

SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. I problemi critici di protezione richiedono un intervento immediato e comportano il passaggio dello stato della protezione a rosso. I problemi non critici di protezione non richiedono un intervento immediato e, a seconda del tipo di problema, possono influire sullo stato della protezione. Per raggiungere uno stato della protezione verde, è necessario risolvere tutti i problemi critici e risolvere oppure ignorare tutti i problemi non critici. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee. Per ulteriori informazioni sul tecnico virtuale di McAfee, consultare la relativa Guida.

In questo capitolo

Risoluzione dei problemi di protezione

Nella maggior parte dei casi, i problemi di protezione possono essere risolti automaticamente, tuttavia alcuni problemi richiedono un intervento manuale. Se ad esempio la funzione Protezione firewall è disattivata, SecurityCenter può attivarla automaticamente, ma se la funzione non è installata, sarà necessario installarla. Nella tabella seguente sono riportate alcune altre azioni che è possibile intraprendere per risolvere manualmente i problemi di protezione:

Problema	Azione
Non è stata eseguita alcuna scansione completa negli ultimi 30 giorni.	Eseguire una scansione manuale del computer. Per ulteriori informazioni, consultare la Guida di VirusScan.
I file delle firme per i rilevamenti (DAT) non sono aggiornati.	Aggiornare manualmente la protezione. Per ulteriori informazioni, consultare la Guida di VirusScan.
Un programma non è stato installato.	Installare il programma dal sito Web di McAfee o da CD.
Un programma non presenta tutti i componenti necessari.	Reinstallare il programma dal sito Web di McAfee o da CD.
Un programma non è stato registrato e non può ricevere tutti i servizi di protezione.	Registrare il programma sul sito Web di McAfee.
Un programma è scaduto.	Verificare lo stato del proprio account sul sito Web di McAfee.

Nota: spesso un unico problema di protezione influisce su più categorie di protezione. In questo caso, se il problema viene risolto per una categoria, verrà risolto anche per tutte le altre categorie di protezione.

Risoluzione automatica dei problemi di protezione

SecurityCenter è in grado di risolvere automaticamente la maggior parte dei problemi di protezione. Le modifiche apportate da SecurityCenter alla configurazione durante la risoluzione automatica dei problemi di protezione non vengono aggiunte nel registro eventi. Per ulteriori informazioni sugli eventi, consultare la sezione Visualizzazione degli eventi (pagina 29).

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, nell'area dello stato della protezione, fare clic su **Correggi**.

Come risolvere manualmente i problemi di protezione

Se uno o più problemi di protezione non vengono risolti tramite la procedura automatica, è possibile intervenire manualmente.

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic sulla categoria di protezione per cui SecurityCenter ha rilevato il problema.
3. Fare clic sul collegamento accanto alla descrizione del problema.

Esclusione dei problemi di protezione

Se SecurityCenter rileva un problema non critico è possibile risolverlo o ignorarlo. Alcuni problemi non critici, ad esempio se Anti-Spam o Privacy Service non è installato, vengono automaticamente ignorati. I problemi ignorati vengono riportati nell'area delle informazioni sulle categorie di protezione del riquadro SecurityCenter solo se lo stato della protezione del computer è verde. Se un problema viene ignorato e successivamente si decide di visualizzarlo nell'area delle informazioni sulle categorie di protezione anche se lo stato della protezione non è verde, sarà possibile visualizzarlo.

Come ignorare un problema di protezione

Se SecurityCenter rileva un problema non critico che non si desidera risolvere, è possibile ignorarlo. I problemi ignorati vengono rimossi dall'area delle informazioni sulle categorie di protezione di SecurityCenter.

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic sulla categoria di protezione per cui il problema è stato rilevato.
3. Fare clic sul collegamento **Ignora** accanto al problema di protezione.

Come visualizzare o nascondere i problemi ignorati

In base alla gravità, i problemi di protezione possono essere visualizzati o nascosti.

1. Aprire il riquadro Opzioni di avviso.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
   3. In **Avvisi**, fare clic su **Avanzate**.
2. Nel riquadro Configurazione di SecurityCenter, fare clic su **Problemi ignorati**.
3. Nel riquadro Problemi ignorati, effettuare le seguenti operazioni:
   - Per ignorare un problema, selezionare la relativa casella di controllo.
   - Per visualizzare un problema nell'area delle informazioni sulle categorie di protezione, deselezionare la relativa casella di controllo.

4 Fare clic su **OK**.

Suggerimento: per ignorare un problema è anche possibile fare clic sul collegamento **Ignora** accanto al problema rilevato nell'area delle informazioni sulle categorie di protezione.

CAPITOLO 6

Utilizzo degli avvisi

Gli avvisi sono piccole finestre popup che vengono visualizzate nell'angolo inferiore destro dello schermo quando si verificano determinati eventi di SecurityCenter. Un avviso fornisce informazioni dettagliate su un evento, oltre a consigli e opzioni per la risoluzione dei problemi che possono essere associati a tale evento. Alcuni avvisi contengono inoltre dei collegamenti a informazioni aggiuntive sull'evento. Tali collegamenti reindirizzano l'utente al sito Web globale di McAfee oppure consentono di inviare informazioni a McAfee per la risoluzione dei problemi.

Esistono tre tipi di avvisi: rosso, giallo e verde.

Tipo di avviso	Descrizione
Rosso	Un avviso rosso è una notifica critica che richiede una risposta da parte dell'utente. Gli avvisi rossi vengono visualizzati quando SecurityCenter non è in grado di individuare automaticamente la risoluzione di un problema di protezione.
Giallo	Un avviso giallo è una notifica non critica che di solito richiede una risposta da parte dell'utente.
Verde	Un avviso verde è una notifica non critica che non richiede una risposta da parte dell'utente. Gli avvisi verdi forniscono informazioni di base su un evento.

Non è possibile disabilitare gli avvisi, poiché hanno un ruolo chiave nel monitoraggio e nella gestione dello stato di protezione. Tuttavia, è possibile impostare la visualizzazione di determinati tipi di avvisi informativi e configurare altre opzioni di avviso (ad esempio, se SecurityCenter deve riprodurre un suono quando viene visualizzato un avviso oppure se visualizzare la schermata iniziale di McAfee all'avvio).

In questo capitolo

Mostrare e nascondere gli avvisi informativi

Gli avvisi informativi avvisano l'utente quando si verificano degli eventi che non rappresentano una minaccia per la protezione del computer. Ad esempio, se è stata impostata la Protezione firewall, per impostazione predefinita verrà visualizzato un avviso informativo ogni volta che un programma installato sul computer viene autorizzato all'accesso a Internet. Qualora non si desideri che venga visualizzato un tipo specifico di avviso informativo, è possibile nasconderlo. Se non si desidera che venga visualizzato alcun avviso, è possibile nasconderli tutti. È inoltre possibile nascondere tutti gli avvisi informativi quando si esegue un gioco in modalità a schermo intero sul computer. Al termine del gioco, quando si esce dalla modalità a schermo intero, SecurityCenter riprende la visualizzazione degli avvisi informativi.

Se si nasconde per errore un avviso informativo, sarà possibile visualizzarlo di nuovo in qualsiasi momento. Per impostazione predefinita, SecurityCenter mostra tutti gli avvisi informativi.

Come mostrare o nascondere gli avvisi informativi

È possibile configurare SecurityCenter in modo da mostrare alcuni avvisi informativi e nasconderne altri, oppure nascondere tutti gli avvisi informativi.

1 Aprire il riquadro Opzioni di avviso.

   In che modo?

   1. Nella sezione **Attività comuni**, fare clic su **Home**.
   2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
   3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi informativi**.

3 Nel riquadro Avvisi informativi, effettuare le seguenti operazioni:

   - Per visualizzare un avviso informativo, deselezionare la relativa casella di controllo.
   - Per nascondere un avviso informativo, selezionare la relativa casella di controllo.
   - Per nascondere tutti gli avvisi informativi, selezionare la casella di controllo **Non visualizzare avvisi informativi**.

4 Fare clic su **OK**.

Suggerimento: è inoltre possibile nascondere un avviso informativo selezionando la casella di controllo **Non visualizzare questo messaggio in futuro** nella finestra dell'avviso stesso. In tal modo, sarà possibile visualizzare nuovamente l'avviso informativo deselezionando la casella di controllo appropriata nel riquadro Avvisi informativi.

Come mostrare o nascondere gli avvisi informativi durante una sessione di gioco

È possibile nascondere gli avvisi informativi quando si esegue un gioco in modalità a schermo intero sul computer. Al termine del gioco, quando si esce dalla modalità a schermo intero, SecurityCenter riprende la visualizzazione degli avvisi informativi.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Opzioni di avviso, selezionare o deselezionare la casella di controllo **Visualizza avvisi informativi quando viene rilevata la modalità di gioco**.

3 Fare clic su **OK**.

Configurazione delle opzioni di avviso

L'aspetto e la frequenza degli avvisi vengono configurati da SecurityCenter; tuttavia, l'utente può modificare alcune opzioni di avviso di base. Ad esempio, è possibile riprodurre un suono quando vengono visualizzati gli avvisi oppure nascondere l'avviso della schermata iniziale all'avvio di Windows. È inoltre possibile nascondere gli avvisi che avvertono gli utenti di epidemie di virus e altre minacce per la protezione nella community online.

Come riprodurre un suono con gli avvisi

Se si desidera ricevere un segnale acustico quando si verifica un avviso, è possibile configurare SecurityCenter in modo da riprodurre un suono al verificarsi di ciascun avviso.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel pannello Opzioni di avviso, nella sezione **Audio**, selezionare la casella di controllo **Riproduci un suono quando si verifica un avviso**.

Come nascondere la schermata iniziale all'avvio

Per impostazione predefinita, la schermata iniziale di McAfee viene visualizzata brevemente all'avvio di Windows per avvisare l'utente che sul computer è attiva la protezione offerta da SecurityCenter. È tuttavia possibile nascondere la schermata iniziale qualora non si desideri che venga visualizzata.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel pannello Opzioni di avviso, nella sezione **Schermata iniziale**, deselezionare la casella di controllo **Mostra la schermata iniziale di McAfee all'avvio di Windows**.

Suggerimento: è possibile mostrare nuovamente la schermata iniziale in qualsiasi momento selezionando la casella di controllo **Mostra la schermata iniziale di McAfee all'avvio di Windows**.

Come nascondere gli avvisi sulle epidemie di virus

È possibile nascondere gli avvisi che avvertono gli utenti di epidemie di virus e altre minacce per la protezione nella community online.

1 Aprire il riquadro Opzioni di avviso.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro a destra, nella sezione **Informazioni su SecurityCenter**, fare clic su **Configura**.
3. In **Avvisi**, fare clic su **Avanzate**.

2 Nel riquadro Opzioni di avviso, deselezionare la casella di controllo **Avvisa quando viene rilevato un virus o una minaccia per la protezione**.

Suggerimento: è possibile mostrare gli avvisi sulle epidemie di virus in qualsiasi momento selezionando la casella di controllo **Avvisa quando viene rilevato un virus o una minaccia per la protezione**.

CAPITOLO 7

Visualizzazione di eventi

Un evento è un'azione o una modifica della configurazione che si verifica nell'ambito di una categoria di protezione e i relativi servizi di protezione. Diversi servizi di protezione registrano tipi di eventi differenti. Ad esempio, SecurityCenter registra un evento se si attiva o disattiva un servizio di protezione; Virus Protection registra un evento ogni volta che un virus viene rilevato e rimosso; Firewall Protection registra un evento ogni volta che viene bloccato un tentativo di connessione a Internet. Per ulteriori informazioni sulle categorie di protezione, vedere Informazioni sulle categorie di protezione (pagina 9).

È possibile visualizzare eventi durante la risoluzione dei problemi di configurazione e la revisione delle operazioni eseguite da altri utenti. Molti genitori utilizzano il registro eventi per monitorare il comportamento dei propri figli su Internet. È possibile visualizzare gli eventi recenti se si desidera esaminare solo gli ultimi 30 eventi verificatisi, tutti gli eventi se si desidera esaminare un elenco completo di tutti gli eventi verificatisi. Quando si visualizzano tutti gli eventi, SecurityCenter avvia il registro eventi, in cui gli eventi sono ordinati in base alla categoria di protezione nell'ambito della quale si sono verificati.

In questo capitolo

Visualizzazione degli eventi recenti

È possibile visualizzare gli eventi recenti se si desidera esaminare solo gli ultimi 30 eventi verificatisi.

- Nella sezione **Attività comuni**, fare clic su **Visualizza eventi recenti**.

Come visualizzare tutti gli eventi

È possibile visualizzare tutti gli eventi se si desidera esaminare un elenco completo di tutti gli eventi verificatisi.

1. Nella sezione **Attività comuni**, fare clic su **Visualizza eventi recenti**.
2. Nel riquadro Eventi recenti, fare clic su **Visualizza registro**.
3. Nel riquadro a sinistra del registro eventi, fare clic sul tipo di eventi che si desidera visualizzare.

CAPITOLO 8

McAfee VirusScan

I servizi di rilevamento e protezione avanzati di VirusScan difendono i dati e il computer dell'utente dalle minacce più recenti per la protezione, da virus, trojan horse, cookie che registrano le informazioni, spyware, adware e altri programmi potenzialmente indesiderati. La protezione si estende oltre i file e le cartelle sul desktop, puntando alle minacce provenienti da diversi punti d'accesso, tra cui messaggi di posta elettronica, messaggi immediati e il Web.

Con VirusScan, la protezione del computer è immediata e costante e non richiede tediose procedure amministrative. Mentre l'utente lavora, gioca, naviga sul Web o controlla la posta elettronica, VirusScan viene eseguito in background, controllando, analizzando e rilevando i danni potenziali in tempo reale. Il software pianifica scansioni complete periodiche del computer, utilizzando una gamma più complessa di opzioni. Grazie alla sua flessibilità, VirusScan offre all'utente la possibilità di personalizzare questo funzionamento, se lo desidera; in caso contrario, il computer resta comunque protetto.

Con il normale utilizzo, virus, worm e altre minacce potenziali possono infiltrarsi nel computer. In questo caso, VirusScan avvisa l'utente della minaccia, ma la gestisce in sua vece, pulendo o mettendo in quarantena gli elementi infetti prima che si verifichi qualsiasi danno. In rari casi, potrebbero essere necessarie alcune ulteriori operazioni. In questa eventualità, VirusScan consente all'utente di decidere sul da farsi: eseguire una nuova scansione al successivo avvio del computer, mantenere l'elemento rilevato oppure rimuoverlo.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di VirusScan

VirusScan fornisce le funzioni riportate di seguito.

Protezione antivirus completa

I servizi di rilevamento e protezione avanzati di VirusScan difendono i dati e il computer dell'utente dalle minacce più recenti per la protezione, da virus, trojan horse, cookie che registrano le informazioni, spyware, adware e altri programmi potenzialmente indesiderati. La protezione si estende oltre i file e le cartelle sul desktop, puntando alle minacce provenienti da diversi punti d'accesso, tra cui messaggi di posta elettronica, messaggi immediati e il Web. Non sono necessarie tediose procedure amministrative.

Opzioni di scansione con riconoscimento delle risorse

Se si riscontrano problemi di lentezza della scansione, è possibile disattivare l'opzione che richiede il minimo utilizzo delle risorse del computer, tenendo in mente che sarà assegnata maggiore priorità alla protezione antivirus rispetto alle altre attività. Grazie alla sua flessibilità, VirusScan offre all'utente la possibilità di personalizzare le opzioni di scansione manuale e in tempo reale, se lo desidera; in caso contrario, il computer resta comunque protetto.

Riparazioni automatiche

Se VirusScan rileva una minaccia per la protezione durante l'esecuzione di una scansione in tempo reale o manuale, tenterà di gestirla automaticamente in base al tipo di minaccia. In tal modo, è possibile rilevare e neutralizzare gran parte delle minacce senza l'interazione dell'utente. In rari casi, VirusScan può non essere in grado di neutralizzare autonomamente una minaccia. In questa eventualità, VirusScan consente all'utente di decidere sul da farsi: eseguire una nuova scansione al successivo avvio del computer, mantenere l'elemento rilevato oppure rimuoverlo.

Sospensione delle attività in modalità a schermo intero

Quando sul computer si riproducono film, videogiochi o si eseguono altre divertenti attività che occupano l'intero schermo, VirusScan sospende alcune attività, tra cui gli aggiornamenti automatici e le scansioni manuali.

Avvio della protezione antivirus in tempo reale

VirusScan prevede due tipi di protezione antivirus: in tempo reale e manuale. La protezione antivirus in tempo reale controlla costantemente il computer per rilevare la presenza di eventuali attività di virus, analizzando i file ogni volta che vengono aperti dall'utente o dal computer. La protezione antivirus manuale consente di eseguire la scansione dei file su richiesta. Per accertarsi che il computer resti protetto contro le minacce più recenti, attivare la protezione antivirus in tempo reale e pianificare scansioni manuali periodiche più complete. Per impostazione predefinita, VirusScan esegue una scansione pianificata una volta alla settimana. Per ulteriori informazioni sulla scansione in tempo reale e manuale, consultare Scansione del computer (pagina 57).

In rari casi, potrebbe essere opportuno sospendere temporaneamente la scansione in tempo reale (ad esempio, per modificare alcune opzioni di scansione oppure per risolvere problemi legati alle prestazioni). Se la protezione antivirus in tempo reale è disattivata, il computer non è protetto e lo stato di protezione di SecurityCenter è rosso. Per ulteriori informazioni sullo stato di protezione, vedere "Informazioni sullo stato della protezione" nella guida di SecurityCenter.

Come avviare la protezione antivirus in tempo reale

Per impostazione predefinita, la protezione da virus in tempo reale è attiva e in funzione sul computer contro virus, trojan e altre minacce per la protezione. Se si disattiva la protezione da virus in tempo reale, è necessario riattivarla per mantenere il computer protetto.

1 Aprire il riquadro di configurazione File e computer.

In che modo?

1. Nel riquadro di sinistra, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione da virus**, fare clic su **Attiva**.

Disattivare la protezione antivirus in tempo reale

È possibile disattivare temporaneamente la protezione da virus in tempo reale, quindi specificare l'orario di ripristino. È possibile ripristinare automaticamente la protezione dopo un intervallo di 15, 30, 45 o 60 minuti, al riavvio del computer oppure mai.

1. Aprire il riquadro di configurazione File e computer.

   In che modo?

   1. Nel riquadro di sinistra, fare clic su **Menu avanzato**.
   2. Fare clic su **Configura**.
   3. Nel riquadro Configura, fare clic su **Computer e file**.

2. In **Protezione da virus**, fare clic su **Disattiva**.
3. Nella finestra di dialogo, scegliere quando ripristinare la scansione in tempo reale.
4. Fare clic su **OK**.

CAPITOLO 9

Avvio della protezione aggiuntiva

In aggiunta alla protezione da virus in tempo reale, VirusScan offre la protezione avanzata da script, spyware e allegati di posta elettronica e di messaggistica immediata potenzialmente dannosi. Per impostazione predefinita, la protezione con scansione script, spyware, posta elettronica e messaggistica immediata è attiva e in funzione.

Protezione con scansione script

La scansione script rileva gli script potenzialmente dannosi e ne impedisce l'esecuzione sul computer. La scansione script controlla eventuali attività sospette del computer, ad esempio uno script che crea, copia o elimina dei file oppure apre il registro di sistema di Windows, avvisando l'utente prima che si verifichi qualsiasi danno.

Protezione da spyware

La protezione da spyware rileva eventuale spyware, adware e altri programmi potenzialmente indesiderati. Lo spyware è un software che può essere segretamente installato sul computer per controllare il comportamento dell'utente, raccogliere dati personali e interferire persino con il controllo del computer da parte dell'utente, installando software aggiuntivo oppure reindirizzando l'attività del browser.

Protezione della posta elettronica

La protezione della posta elettronica rileva le attività sospette nei messaggi e negli allegati di posta elettronica inviati e ricevuti.

Protezione della messaggistica immediata

La protezione della messaggistica immediata consente di rilevare le potenziali minacce per la sicurezza contenute negli allegati ai messaggi immediati ricevuti. Impedisce inoltre la condivisione di dati personali nei programmi di messaggistica immediata.

In questo capitolo

Avviare la protezione con scansione script

Attivare la scansione script per rilevare gli script potenzialmente dannosi e impedirne l'esecuzione sul computer. La scansione script avvisa quando uno script tenta di creare, copiare o eliminare dei file sul computer oppure di apportare modifiche al registro di sistema di Windows.

1 Aprire il riquadro di configurazione File e computer.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione con scansione script**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione con scansione script in qualsiasi momento, in tal modo si renderà il computer vulnerabile agli script dannosi.

Come avviare la protezione antispyware

Attivare la protezione da spyware per rilevare e rimuovere spyware, adware e altri programmi potenzialmente indesiderati che raccolgono e trasmettono informazioni senza l'autorizzazione dell'utente o a sua insaputa.

1 Aprire il riquadro di configurazione File e computer.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione con scansione script**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione da spyware in qualsiasi momento, in tal modo si renderà il computer vulnerabile ai programmi potenzialmente indesiderati.

Come avviare la protezione della posta elettronica

Attivare la protezione della posta elettronica per rilevare worm e le potenziali minacce contenute nei messaggi di posta elettronica in uscita (SMTP) e in arrivo (POP3), nonché negli allegati.

1 Aprire il riquadro di configurazione Posta elettronica e MI.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.

2 In **Protezione della posta elettronica**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione della posta elettronica in qualsiasi momento, in tal modo si renderà il computer vulnerabile alle minacce della posta elettronica.

Come avviare la protezione della messaggistica immediata

Attivare la protezione della messaggistica immediata per rilevare le minacce per la sicurezza che possono essere contenute negli allegati ai messaggi immediati in arrivo.

1 Aprire il riquadro di configurazione Posta elettronica e MI.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Posta elettronica e MI**.

2 In **Protezione messaggistica immediata**, fare clic su **Attiva**.

Nota: sebbene sia possibile disattivare la protezione della messaggistica immediata in qualsiasi momento, in tal modo si renderà il computer vulnerabile agli allegati dei messaggi immediati.

CAPITOLO 10

Impostazione della protezione antivirus

VirusScan prevede due tipi di protezione antivirus: in tempo reale e manuale. La protezione antivirus in tempo reale analizza i file ogni volta che vengono aperti dall'utente o dal computer. La protezione antivirus manuale consente di eseguire la scansione dei file su richiesta. È possibile impostare opzioni diverse per ogni tipo di protezione. Ad esempio, poiché la protezione in tempo reale controlla ininterrottamente il computer, è possibile selezionare una determinata serie di opzioni di scansione di base, riservando una serie di opzioni di scansione più completa alla protezione manuale su richiesta.

In questo capitolo

Impostazione delle opzioni di scansione in tempo reale

Quando l'utente avvia la protezione antivirus in tempo reale, VirusScan utilizza una serie predefinita di opzioni per la scansione dei file. È tuttavia possibile modificare le opzioni predefinite in base alle proprie esigenze.

Per modificare le opzioni di scansione in tempo reale, è necessario decidere quali elementi saranno controllati da VirusScan durante una scansione, nonché i percorsi e i tipi di file sottoposti a scansione. Ad esempio, è possibile determinare se VirusScan deve controllare virus o cookie sconosciuti, che i siti Web possono utilizzare per tenere traccia del comportamento dell'utente, e se deve sottoporre a scansione le unità di rete mappate al computer in uso o semplicemente le unità locali. L'utente può inoltre determinare quali tipi di file vengono sottoposti a scansione (tutti i file oppure solo i file di programma e i documenti, in cui viene rilevata la maggior parte dei virus).

Quando si modificano le opzioni di scansione in tempo reale è inoltre necessario stabilire l'importanza della protezione dal sovraccarico del buffer sul computer in uso. Un buffer è una parte di memoria utilizzata per contenere temporaneamente informazioni sul computer. I sovraccarichi del buffer possono verificarsi quando la quantità di informazioni memorizzate nel buffer da programmi o processi sospetti supera la capacità dello stesso. In questo caso, il computer diviene vulnerabile agli attacchi.

Come impostare le opzioni di scansione in tempo reale

L'utente può impostare le opzioni di scansione in tempo reale in modo da personalizzare gli elementi controllati da VirusScan durante una scansione in tempo reale, nonché i percorsi e i tipi di file sottoposti a scansione. Tra le opzioni disponibili è inclusa la scansione di virus sconosciuti e cookie che registrano le informazioni, nonché la protezione dal sovraccarico del buffer. È inoltre possibile configurare la scansione in tempo reale per controllare le unità di rete mappate al computer in uso.

1 Aprire il riquadro Scansione in tempo reale.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.

2 Specificare le opzioni di scansione in tempo reale desiderate, quindi fare clic su **OK**.

Per...	Procedere come segue...
Rilevare virus sconosciuti e nuove varianti di virus noti	Selezionare la casella di controllo **Ricerca di virus sconosciuti con tecnologia euristica**.
Rilevare i cookie	Selezionare la casella di controllo **Cerca e rimuovi cookie**.
Rilevare virus e altre minacce potenziali sulle unità connesse alla rete	Selezionare la casella di controllo **Esegui scansione su unità di rete**.
Proteggere il computer contro i sovraccarichi del buffer	Selezionare la casella di controllo **Attiva protezione dal sovraccarico del buffer**.
Specificare i tipi di file da analizzare	Fare clic su **Tutti i file (consigliato)** o **Solo file di programma e documenti**.

Impostazione delle opzioni di scansione manuale

La protezione antivirus manuale consente di eseguire la scansione dei file su richiesta. Quando si avvia una scansione manuale, VirusScan rileva l'eventuale presenza di virus e di altri elementi potenzialmente dannosi sul computer, utilizzando una gamma più completa di opzioni di scansione. Per modificare le opzioni di scansione manuale, è necessario decidere quali elementi saranno controllati da VirusScan durante una scansione. Ad esempio, è possibile configurare la ricerca e l'analisi di virus sconosciuti, di programmi potenzialmente indesiderati, come spyware o adware, di programmi di mascheramento, come i rootkit che possono concedere l'accesso non autorizzato al computer e dei cookie, che vengono utilizzati dai siti Web per tenere traccia del comportamento dell'utente. L'utente può inoltre stabilire il tipo di file su cui eseguire il controllo. Ad esempio, è possibile determinare se VirusScan deve controllare tutti i file oppure solo i file di programma e i documenti, in cui viene rilevata la maggior parte dei virus. È inoltre possibile stabilire se includere i file di archivio (ad esempio, i file .zip) nella scansione.

Per impostazione predefinita, VirusScan controlla tutte le unità e le cartelle sul computer in uso ogni volta che viene eseguita una scansione manuale. Tuttavia, è possibile modificare i percorsi predefiniti in base alle proprie esigenze. Ad esempio, è possibile eseguire la scansione solo di file di sistema di importanza critica, degli elementi presenti sul desktop oppure di quelli contenuti nella cartella Programmi. Se l'utente non desidera essere responsabile dell'avvio di ogni scansione manuale, è possibile impostare una pianificazione periodica delle scansioni. Le scansioni pianificate consentono di controllare l'intero computer utilizzando le opzioni di scansione predefinite. Per impostazione predefinita, VirusScan esegue una scansione pianificata una volta alla settimana.

Se si riscontrano problemi di lentezza della scansione, si consideri la disattivazione dell'opzione che richiede il minimo utilizzo delle risorse del computer, tenendo in mente che sarà assegnata maggiore priorità alla protezione antivirus rispetto alle altre attività.

Nota: quando sul computer si riproducono film, videogiochi o si eseguono altre applicazioni che occupano l'intero schermo, VirusScan sospende alcune attività, tra cui gli aggiornamenti automatici e le scansioni manuali.

Come impostare le opzioni di scansione manuale

L'utente può impostare le opzioni di scansione manuale in modo da personalizzare gli elementi controllati da VirusScan durante una scansione manuale, nonché i percorsi e i tipi di file sottoposti a scansione. Tra le opzioni disponibili è inclusa la scansione di virus sconosciuti, archivi di file, spyware e programmi potenzialmente indesiderati, cookie che registrano le informazioni, rootkit e programmi di mascheramento.

1 Aprire il riquadro Scansione manuale.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.
5. Fare clic su **Scansione manuale** nel riquadro Protezione da virus.

2 Specificare le opzioni di scansione manuale desiderate, quindi fare clic su **OK**.

Per...	Procedere come segue...
Rilevare virus sconosciuti e nuove varianti di virus noti	Selezionare la casella di controllo **Ricerca di virus sconosciuti con tecnologia euristica**.
Rilevare e rimuovere i virus nei file .zip e in altri file di archivio	Selezionare la casella di controllo **Scansione di file .zip e altri file di archivio**.
Rilevare spyware, adware e altri programmi potenzialmente indesiderati	Selezionare la casella di controllo **Ricerca di programmi spyware e programmi potenzialmente indesiderati**.
Rilevare i cookie	Selezionare la casella di controllo **Cerca e rimuovi cookie**.
Rilevare rootkit e programmi di mascheramento che possono modificare e sfruttare i file di sistema di Windows esistenti	Selezionare la casella di controllo **Ricerca di rootkit e altri programmi di mascheramento**.

Utilizzare una quantità minore di risorse del processore per le scansioni, assegnando maggiore priorità ad altre attività (quali la navigazione su Internet o l'apertura di documenti)	Selezionare la casella di controllo **Esegui scansione utilizzando risorse del computer minime**.
Specificare i tipi di file da analizzare	Fare clic su **Tutti i file (consigliato)** o **Solo file di programma e documenti**.

Come impostare il percorso di scansione manuale

È possibile impostare il percorso di scansione manuale in cui VirusScan dovrà rilevare l'eventuale presenza di virus e altri elementi dannosi. È possibile analizzare tutti i file, le cartelle e le unità del computer oppure limitare la scansione a cartelle e unità specifiche.

1 Aprire il riquadro Scansione manuale.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.
5. Fare clic su **Scansione manuale** nel riquadro Protezione da virus.

2 Fare clic su **Percorso predefinito da sottoporre a scansione**.

3 Specificare il percorso di scansione manuale desiderato, quindi fare clic su **OK**.

Per...	Procedere come segue...
Analizzare tutti i file e le cartelle sul computer	Selezionare la casella di controllo **Risorse del computer**.
Analizzare file, cartelle e unità specifiche sul computer	Deselezionare la casella di controllo **Risorse del computer** e selezionare una o più cartelle o unità.

Analizzare i file di sistema critici	Deselezionare la casella di controllo **Risorse del computer**, quindi selezionare la casella di controllo **File di sistema importanti**.

Come pianificare la scansione

È possibile pianificare le scansioni per una ricerca accurata dei virus e di altre minacce nel computer in qualsiasi giorno e ora della settimana. Le scansioni pianificate consentono di controllare l'intero computer utilizzando le opzioni di scansione predefinite. Per impostazione predefinita, VirusScan esegue una scansione pianificata una volta alla settimana. Se si riscontrano problemi di lentezza della scansione, si consideri la disattivazione dell'opzione che richiede il minimo utilizzo delle risorse del computer, tenendo in mente che sarà assegnata maggiore priorità alla protezione antivirus rispetto alle altre attività.

1 Aprire il riquadro Scansione pianificata.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.
5. Fare clic su **Scansione pianificata** nel riquadro Protezione da virus.

2 Selezionare **Attiva scansione pianificata**.

3 Per ridurre la quantità di risorse del processore normalmente utilizzata per la scansione, selezionare **Esegui scansione utilizzando risorse del computer minime**.

4 Selezionare uno o più giorni.

5 Specificare un orario di inizio.

6 Fare clic su **OK**.

Suggerimento: è possibile ripristinare la pianificazione predefinita facendo clic su **Ripristina**.

Utilizzo delle opzioni SystemGuard

I moduli SystemGuard controllano, registrano, segnalano e gestiscono le modifiche potenzialmente non autorizzate apportate al registro di sistema di Windows oppure ai file di sistema importanti sul computer. Le modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

Le modifiche del registro di sistema e dei file sono comuni e si verificano periodicamente sul computer. Poiché molte di esse sono innocue, le impostazioni predefinite dei moduli SystemGuard sono configurate in modo da offrire una protezione affidabile, intelligente e reale contro le modifiche non autorizzate e potenzialmente dannose. Ad esempio, quando i moduli SystemGuard rilevano modifiche non comuni che rappresentano una minaccia potenzialmente significativa, tali attività vengono immediatamente segnalate e registrate. Le modifiche comuni, ma comunque potenzialmente dannose, vengono solamente registrate. Il controllo delle modifiche standard o a basso rischio è comunque disattivato per impostazione predefinita. È possibile configurare la tecnologia SystemGuard in modo da estenderne la protezione a qualsiasi ambiente desiderato.

Esistono tre tipi di SystemGuard: SystemGuard programmi, SystemGuard Windows e SystemGuard browser.

SystemGuard programmi

Il modulo SystemGuard programmi rileva le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. Tra questi importanti elementi del registro di sistema e file sono incluse le installazioni di ActiveX, gli elementi del menu di avvio, gli hook di esecuzione della shell di Windows e le chiavi ShellServiceObjectDelayLoad. Monitorando tali file, la tecnologia SystemGuard programmi arresta i programmi ActiveX (scaricati da Internet) nonché i programmi spyware e potenzialmente indesiderati che possono essere automaticamente eseguiti all'avvio di Windows.

SystemGuard Windows

Anche il modulo SystemGuard Windows rileva le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. Tra questi importanti elementi del registro di sistema e file sono inclusi i gestori dei menu, i file DLL appInit e i file host di Windows. Monitorando questi file, la tecnologia SystemGuard Windows contribuisce a prevenire l'invio e la ricezione di informazioni non autorizzate o personali dal computer a Internet. Consente inoltre di arrestare programmi sospetti che possono apportare modifiche non desiderate all'aspetto e al funzionamento di programmi importanti per l'utente e i suoi familiari.

SystemGuard browser

Come i moduli SystemGuard programmi e SystemGuard Windows, anche il modulo SystemGuard browser rileva le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. SystemGuard browser, tuttavia, controlla le modifiche apportate a elementi del registro di sistema e file, come i componenti aggiuntivi, gli URL e le aree di protezione di Internet Explorer. Monitorando questi file, la tecnologia SystemGuard browser contribuisce a prevenire le attività del browser non autorizzate, come il reindirizzamento a siti Web sospetti, le modifiche apportate alle impostazioni e alle opzioni del browser all'insaputa dell'utente e l'impostazione non desiderata di siti Web sospetti come affidabili.

Come attivare la protezione SystemGuard

Attivare la protezione SystemGuards per rilevare e avvisare l'utente delle modifiche potenzialmente non autorizzate apportate al registro di sistema di Windows e ai file sul computer in uso. Le modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

1 Aprire il riquadro di configurazione File e computer.

In che modo?

1. Nel riquadro sinistro, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configura, fare clic su **Computer e file**.

2 In **Protezione SystemGuard**, fare clic su **Attiva**.

Nota: è possibile disattivare la protezione SystemGuard facendo clic su **Disattiva**.

Come configurare le opzioni SystemGuard

Utilizzare il riquadro SystemGuard per configurare le opzioni di protezione, registrazione e avviso contro modifiche non autorizzate del registro di sistema e dei file, associate a file e programmi di Windows nonché a Internet Explorer. Le modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

1 Aprire il riquadro SystemGuard.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione SystemGuard sia attivata, quindi fare clic su **Avanzate**.

2 Selezionare un tipo di SystemGuard dall'elenco.

- **SystemGuard programmi**
- **SystemGuard Windows**
- **SystemGuard browser**

3 In **Desidero**, effettuare una delle seguenti operazioni:

- Per rilevare, registrare e segnalare modifiche non autorizzate apportate al registro di sistema e ai file associate ai moduli SystemGuard programmi, Windows e browser, fare clic su **Mostra avvisi**.
- Per rilevare e registrare modifiche non autorizzate apportate al registro di sistema e ai file associate ai moduli SystemGuard programmi, Windows e browser, fare clic su **Registra solo le modifiche**.
- Per disattivare il rilevamento delle modifiche non autorizzate apportate al registro di sistema e ai file associate ai moduli SystemGuard programmi, Windows e browser, fare clic su **Disattiva SystemGuard**.

Nota: per ulteriori informazioni sui tipi di SystemGuard, vedere Informazioni sui tipi di SystemGuard (pagina 49).

Informazioni sui tipi di SystemGuard

I moduli SystemGuard rilevano le modifiche potenzialmente non autorizzate apportate al registro di sistema del computer e ad altri file di importanza fondamentale per Windows. Esistono tre tipi di SystemGuard: SystemGuard programmi, SystemGuard Windows e SystemGuard browser.

SystemGuard programmi

La tecnologia SystemGuard programmi blocca i programmi ActiveX sospetti (scaricati da Internet), nonché i programmi spyware e potenzialmente indesiderati in grado di avviarsi automaticamente all'avvio di Windows.

SystemGuard	Rileva...
Installazioni di ActiveX	Modifiche non autorizzate al registro di sistema per le installazioni di ActiveX che possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.
Elementi di avvio	Programmi spyware, adware o potenzialmente indesiderati che possono apportare modifiche ai file per gli elementi di avvio, consentendo l'esecuzione di programmi sospetti all'avvio del computer.
Hook di esecuzione della shell di Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di installare gli hook di esecuzione della shell di Windows per impedire la corretta esecuzione dei programmi di protezione.
Chiave ShellServiceObjectDelayLoad	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche alla chiave ShellServiceObjectDelayLoad del registro di sistema, consentendo l'esecuzione di file pericolosi all'avvio del computer.

SystemGuard Windows

La tecnologia SystemGuard Windows consente di impedire al computer l'invio e la ricezione di informazioni non autorizzate o personali su Internet. Consente inoltre di bloccare programmi sospetti che possono apportare modifiche non desiderate all'aspetto e al funzionamento di programmi importanti per l'utente e i suoi familiari.

SystemGuard	Rileva...
Gestori dei menu di scelta rapida	Modifiche non autorizzate al registro di sistema per i gestori dei menu di scelta rapida di Windows che possono incidere sull'aspetto e sul comportamento dei menu di Windows. I menu di scelta rapida consentono di eseguire azioni sul computer, ad esempio fare clic sui file con il pulsante destro del mouse.
DLL AppInit	Modifiche non autorizzate alle DDL appInit del registro di sistema di Windows in grado di consentire l'esecuzione di file potenzialmente pericolosi all'avvio del computer.
File hosts di Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche non autorizzate al file hosts di Windows, consentendo il reindirizzamento del browser a siti Web sospetti e il blocco degli aggiornamenti del software.
Shell di Winlogon	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per la shell di Winlogon, consentendo la sostituzione di Esplora risorse di Windows con altri programmi.
Chiave UserInit di Winlogon	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche alla chiave UserInit di Winlogon del registro di sistema, consentendo l'esecuzione di programmi sospetti quando l'utente esegue l'accesso a Windows.
Protocolli Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per i protocolli Windows che si riflettono sulle modalità di invio e ricezione di informazioni su Internet del computer.
Layered Service Provider di Winsock	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per gli LSP (Layered Service Provider) di Winsock, al fine di intercettare e modificare le informazioni inviate e ricevute su Internet.
Comandi Apri della shell di Windows	Modifiche non autorizzate ai comandi Apri della shell di Windows che possono determinare l'esecuzione di worm e di altri programmi potenzialmente pericolosi sul computer.

Utilità di pianificazione condivisa	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema e ai file per l'Utilità di pianificazione condivisa, consentendo l'esecuzione di file potenzialmente pericolosi all'avvio del computer.
Windows Messenger Service	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per Windows Messenger Service, consentendo la visualizzazione di pubblicità non richiesta e l'esecuzione in modalità remota di programmi sul computer.
File Win.ini di Windows	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al file Win.ini, consentendo l'esecuzione di programmi sospetti all'avvio del computer.

SystemGuard browser

La tecnologia SystemGuard browser consente di impedire attività del browser non autorizzate, come il reindirizzamento a siti Web sospetti, le modifiche apportate a impostazioni e opzioni del browser all'insaputa dell'utente e l'impostazione indesiderata di siti Web sospetti come affidabili.

SystemGuard	Rileva...
Oggetti helper browser	Programmi spyware, adware o potenzialmente indesiderati in grado di utilizzare gli oggetti helper del browser per tenere traccia delle abitudini di navigazione sul Web dell'utente e visualizzare pubblicità non richiesta.
Barre di Internet Explorer	Modifiche non autorizzate al registro di sistema per le barre di Internet Explorer, ad esempio Cerca e Preferiti, che possono incidere sull'aspetto e sul comportamento di Internet Explorer.
Componenti aggiuntivi di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di installare componenti aggiuntivi di Internet Explorer per tenere traccia delle abitudini di navigazione sul Web dell'utente e visualizzare pubblicità non richiesta.
ShellBrowser di Internet Explorer	Modifiche non autorizzate al registro di sistema per il componente ShellBrowser di Internet Explorer che possono incidere sull'aspetto e sul comportamento del browser Web in uso.
WebBrowser di Internet Explorer	Modifiche non autorizzate al registro di sistema per il componente WebBrowser di Internet Explorer che possono incidere sull'aspetto e sul comportamento del browser in uso.

Hook di ricerca URL di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per gli hook di ricerca degli URL di Internet Explorer, consentendo il reindirizzamento del browser a siti Web sospetti durante le ricerche su Internet.
URL di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per gli URL di Internet Explorer che si riflettono sulle impostazioni del browser.
Restrizioni di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per le restrizioni di Internet Explorer che si riflettono sulle impostazioni e sulle opzioni del browser.
Aree di protezione di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per le aree di protezione di Internet Explorer, consentendo l'esecuzione di file potenzialmente pericolosi all'avvio del computer.
Siti attendibili di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per i siti attendibili di Internet Explorer, consentendo al browser di considerare affidabili siti Web sospetti.
Criterio di Internet Explorer	Programmi spyware, adware o potenzialmente indesiderati in grado di apportare modifiche al registro di sistema per i criteri di Internet Explorer che si riflettono sulle impostazioni e sul comportamento del browser.

Utilizzo degli elenchi di elementi affidabili

Se VirusScan rileva una modifica al registro di sistema o ai file (SystemGuard), un programma o un sovraccarico del buffer, avvisa l'utente di impostarlo come affidabile o rimuoverlo. Se l'utente imposta l'elemento come affidabile e richiede di non ricevere notifiche future sulla relativa attività, l'elemento viene aggiunto a un elenco di elementi affidabili e VirusScan non rileva più o non invia più notifiche all'utente in merito all'attività di tale elemento. Se un elemento è stato aggiunto a un elenco di elementi affidabili, l'utente può comunque decidere di bloccarne l'attività. Il blocco impedisce all'elemento di essere eseguito o di apportare modifiche al computer senza informare l'utente ogni volta che viene fatto un tentativo. L'elemento può anche essere rimosso dall'elenco di elementi affidabili. Quando si rimuove l'elemento, VirusScan è in grado di rilevarne nuovamente l'attività.

Come gestire gli elenchi di elementi affidabili

Utilizzare il riquadro Elementi affidabili per impostare come affidabili o bloccare gli elementi precedentemente rilevati e considerati affidabili. È inoltre possibile rimuovere un elemento dall'elenco di elementi affidabili in modo da consentirne il rilevamento da parte di VirusScan.

1 Aprire il riquadro Elementi affidabili.

In che modo?

1. Nella sezione **Attività comuni**, fare clic su **Home**.
2. Nel riquadro SecurityCenter, fare clic su **Computer e file**.
3. Nell'area Computer e file, fare clic su **Configura**.
4. Nel riquadro di configurazione Computer e file, verificare che la protezione antivirus sia attivata, quindi fare clic su **Avanzate**.
5. Nel riquadro Protezione da virus, fare clic su **Elementi affidabili**.

2 Selezionare uno dei seguenti tipi di elementi affidabili:

- **SystemGuard programmi**
- **SystemGuard Windows**
- **SystemGuard browser**
- **Programmi affidabili**
- **Sovraccarichi del buffer affidabili**

3 In **Desidero**, effettuare una delle seguenti operazioni:

- Per consentire all'elemento rilevato di apportare modifiche al registro di sistema di Windows o a file di sistema critici sul computer senza informare l'utente, fare clic su **Affidabile**.
- Per impedire all'elemento rilevato di apportare modifiche al registro di sistema di Windows o a file di sistema critici sul computer senza informare l'utente, fare clic su **Blocca**.
- Per rimuovere l'elemento rilevato dall'elenco di elementi affidabili, fare clic su **Rimuovi**.

4 Fare clic su **OK**.

Nota: per ulteriori informazioni sui tipi di elementi affidabili, vedere Informazioni sui tipi di elementi affidabili (pagina 54).

Informazioni sui tipi di elementi affidabili

I SystemGuard del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. Vi sono cinque tipi di elementi affidabili che è possibile gestire dal riquadro Elementi affidabili: SystemGuard programmi, SystemGuard Windows, SystemGuard browser, programmi affidabili e sovraccarichi del buffer affidabili.

Opzione	Descrizione
SystemGuard programmi	I SystemGuard programmi del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. I SystemGuard programmi rilevano le modifiche non autorizzate al registro di sistema e ai file associate alle installazioni ActiveX, agli elementi di avvio, agli hook di esecuzione della shell di Windows e all'attività ShellServiceObjectDelayLoad. Tali tipi di modifiche non autorizzate al registro di sistema e ai file possono nuocere al computer, comprometterne la protezione e danneggiare file di sistema importanti.

SystemGuard Windows	I SystemGuard Windows del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. I SystemGuard Window rilevano modifiche non autorizzate al registro di sistema e ai file associate ai gestori dei menu di scelta rapida, ai DLL appInit, al file hosts di Windows, alla shell di Winlogon, agli LSP (Layered Service Provider) di Winsock e così via. Tali tipi di modifiche non autorizzate al registro di sistema e ai file possono ripercuotersi sulle modalità di invio e ricezione delle informazioni su Internet da parte del computer, modificare l'aspetto e il comportamento dei programmi e consentire l'esecuzione di programmi sospetti sul computer.
SystemGuard browser	I SystemGuard browser del riquadro Elementi affidabili rappresentano le modifiche precedentemente non autorizzate al registro di sistema e ai file rilevate da VirusScan che l'utente ha scelto di consentire da un avviso o dal riquadro Risultati della scansione. I SystemGuard browser rilevano modifiche non autorizzate al registro di sistema o altro comportamento indesiderato associato agli oggetti helper del browser, ai componenti aggiuntivi di Internet Explorer, agli URL di Internet Explorer, alle aree di protezione di Internet Explorer e così via. Tali tipi di modifiche non autorizzate al registro possono indurre attività del browser indesiderate come il reindirizzamento a siti Web sospetti, la modifica di impostazioni e opzioni del browser e l'impostazione involontaria di siti Web sospetti come siti affidabili.
Programmi affidabili	I programmi affidabili sono programmi potenzialmente indesiderati rilevati da VirusScan che l'utente ha deciso di considerare come affidabili da un avviso o dal riquadro Risultati della scansione.
Sovraccarichi del buffer affidabili	I sovraccarichi del buffer affidabili rappresentano attività precedentemente indesiderate rilevate da VirusScan ma che l'utente ha deciso di considerare come affidabili da un avviso o dal riquadro Risultati della scansione. I sovraccarichi del buffer possono nuocere al computer e danneggiare i file. I sovraccarichi del buffer si verificano quando la quantità di informazioni memorizzate nel buffer da programmi o processi sospetti supera la capacità dello stesso.

CAPITOLO 11

Scansione del computer

Quando si avvia SecurityCenter per la prima volta, la protezione da virus in tempo reale di VirusScan inizia a proteggere il computer da virus potenzialmente dannosi, trojan horse e altre minacce per la protezione. A meno che non si disattivi la protezione da virus in tempo reale, VirusScan monitora costantemente il computer per rilevare la presenza di eventuali attività di virus, eseguendo la scansione dei file a ogni accesso da parte dell'utente o del computer e utilizzando le opzioni di scansione in tempo reale impostate. Per garantire la protezione del computer dalle minacce per la protezione più recenti, lasciare attivata la protezione da virus in tempo reale e impostare una pianificazione per l'esecuzione di scansioni manuali periodiche più approfondite. Per ulteriori informazioni sull'impostazione delle opzioni di scansione manuale e in tempo reale, consultare Impostazione della protezione da virus (pagina 39).

VirusScan offre una serie di opzioni di scansione più dettagliate per la protezione antivirus manuale, consentendo all'utente di eseguire periodicamente scansioni più approfondite. È possibile eseguire scansioni manuali da SecurityCenter su percorsi specifici in base a una pianificazione prestabilita. Tuttavia, è anche possibile eseguire scansioni manuali direttamente in Esplora risorse senza interrompere le altre attività. La scansione in SecurityCenter offre il vantaggio di modificare immediatamente le opzioni di scansione. Tuttavia, la scansione da Esplora risorse offre un approccio comodo alla protezione del computer.

Se si esegue una scansione manuale da SecurityCenter o da Esplora risorse, al termine è comunque possibile visualizzare i risultati della scansione. La visualizzazione dei risultati di una scansione consente di determinare se VirusScan ha rilevato, riparato o messo in quarantena virus, trojan, spyware, adware, cookie e altri programmi potenzialmente indesiderati. I risultati di una scansione possono essere visualizzati in modo differente. Ad esempio è possibile visualizzare un riepilogo di base dei risultati della scansione o informazioni dettagliate quali lo stato e il tipo di infezione nonché statistiche generali sulla scansione e sul rilevamento.

In questo capitolo

Come eseguire la scansione del computer

È possibile eseguire una scansione manuale dal Menu avanzato o dal Menu standard in SecurityCenter. Se si esegue una scansione dal Menu avanzato, è possibile confermare le opzioni di scansione manuale prima della scansione. Se si esegue una scansione dal Menu standard, la scansione viene avviata immediatamente utilizzando le opzioni di scansione esistenti. È inoltre possibile eseguire una scansione in Esplora risorse utilizzando le opzioni di scansione esistenti.

- Eseguire una delle seguenti operazioni:

  Scansione in SecurityCenter

Per...	Procedere come segue...
Eseguire la scansione utilizzando le impostazioni esistenti	Nel Menu standard, fare clic su **Esegui scansione**.
Eseguire la scansione utilizzando le impostazioni modificate	Nel Menu avanzato, fare clic su **Esegui scansione**, selezionare i percorsi da sottoporre a scansione, scegliere le opzioni di scansione, quindi fare clic su **Esegui scansione**.

  Scansione in Esplora risorse

  1. Aprire Esplora risorse.
  2. Fare clic con il pulsante destro del mouse sul file, la cartella o l'unità, quindi scegliere **Esegui scansione**.

Nota: i risultati della scansione sono visualizzati nell'avviso di completamento della scansione. Nei risultati è incluso il numero di elementi sottoposti a scansione, rilevati, riparati, messi in quarantena e rimossi. Per ulteriori informazioni sui risultati della scansione o l'utilizzo degli elementi infetti, fare clic su **Visualizza dettagli scansione**.

Visualizzare i risultati della scansione

Al termine di una scansione manuale, è possibile visualizzare i risultati per determinare gli elementi rilevati durante la scansione e analizzare lo stato attuale di protezione del computer. Nei risultati della scansione è possibile visualizzare se VirusScan ha rilevato, riparato o messo in quarantena virus, Trojan Horse, spyware, adware, cookie e altri programmi potenzialmente indesiderati.

- Nel Menu standard o nel Menu avanzato, fare clic su **Esegui scansione**, quindi eseguire una delle seguenti operazioni.

Per...	Procedere come segue...
Visualizzare i risultati della scansione nell'avviso	Visualizzare i risultati della scansione nell'avviso di completamento della scansione.
Visualizzare maggiori informazioni sui risultati della scansione	Fare clic su **Visualizza dettagli scansione** nell'avviso di completamento della scansione.
Visualizzare un riepilogo rapido dei risultati della scansione	Scegliere l'icona **Scansione completata** nell'area di notifica della barra delle applicazioni.
Visualizzare le statistiche di scansione e rilevamento	Fare doppio clic sull'icona **Scansione completata** nell'area di notifica della barra delle applicazioni.
Visualizzare i dettagli sugli elementi rilevati, lo stato e il tipo di infezione.	Fare doppio clic sull'icona **Scansione completata** nell'area di notifica della barra delle applicazioni, quindi fare clic su **Visualizza risultati** nel riquadro Stato della scansione: Scansione manuale.

CAPITOLO 12

Utilizzo dei risultati della scansione

Se VirusScan rileva una minaccia per la protezione quando esegue una scansione manuale o in tempo reale, cerca di gestire la minaccia in modo automatico in base al tipo di minaccia. Se, ad esempio, VirusScan rileva un virus, Trojan Horse o cookie tracciante sul computer, tenta di pulire il file infetto. Se l'operazione di pulizia non riesce, il file viene messo in quarantena.

Per alcune minacce alla protezione, VirusScan non riesce a pulire o mettere in quarantena un file. In questo caso, viene richiesto all'utente di gestire la minaccia. In base al tipo di minaccia è possibile adottare diverse azioni correttive. Se, ad esempio, viene rilevato un virus in un file, ma VirusScan non riesce a pulire o mettere in quarantena il file, l'accesso al file viene negato. Se vengono rilevati cookie traccianti, ma VirusScan non è in grado di pulirli o metterli in quarantena, l'utente può decidere se rimuoverli o considerarli affidabili. Se vengono rilevati programmi potenzialmente indesiderati, VirusScan non adotta alcuna azione automatica e l'utente può decidere di mettere in quarantena il programma o considerarlo affidabile.

Quando gli elementi vengono messi in quarantena, sono crittografati e quindi isolati in una cartella per impedire ai file, programmi o cookie di danneggiare il computer. Gli elementi in quarantena possono essere ripristinati o rimossi. Nella maggior parte dei casi, è possibile eliminare un cookie in quarantena senza alcuna ripercussione sul sistema. Tuttavia, se VirusScan ha messo in quarantena un programma riconosciuto e utilizzato dall'utente, è possibile ripristinarlo.

In questo capitolo

Come utilizzare virus e Trojan Horse

Se VirusScan rileva un virus o Trojan Horse in un file sul computer durante una scansione manuale o in tempo reale, tenta di pulire il file. Se l'operazione di pulizia non riesce, cerca di metterlo in quarantena. Se anche questa operazione non riesce, l'accesso al file viene negato (solo scansioni in tempo reale).

1 Aprire il riquadro Risultati della scansione.

In che modo?

1. Fare doppio clic sull'icona **Scansione completata** nell'area di notifica a destra della barra delle applicazioni.
2. Nel riquadro Stato della scansione: Scansione manuale, fare clic su **Visualizza risultati**.

2 Nell'elenco dei risultati della scansione, fare clic su **Virus e Trojan**.

Nota: per utilizzare i file messi in quarantena da VirusScan, vedere Come utilizzare i file messi in quarantena (pagina 63).

Come utilizzare programmi potenzialmente indesiderati

Se VirusScan rileva un programma potenzialmente indesiderato sul computer durante una scansione manuale o in tempo reale, è possibile rimuovere il programma o considerarlo affidabile. La rimozione del programma potenzialmente indesiderato non implica l'eliminazione effettiva dal sistema bensì la messa in quarantena, per impedire al programma di causare danni al computer o ai file.

1 Aprire il riquadro Risultati della scansione.

In che modo?

1. Fare doppio clic sull'icona **Scansione completata** nell'area di notifica a destra della barra delle applicazioni.
2. Nel riquadro Stato della scansione: Scansione manuale, fare clic su **Visualizza risultati**.

2 Nell'elenco dei risultati della scansione, fare clic su **Programmi potenzialmente indesiderati**.

3 Selezionare un programma potenzialmente indesiderato.

4 In **Desidero**, fare clic su **Rimuovi** oppure **Affidabile**.

5 Confermare l'opzione selezionata.

Come utilizzare i file messi in quarantena

Quando i file infetti vengono messi in quarantena, sono crittografati e quindi spostati in una cartella per impedire ai file di danneggiare il computer. I file in quarantena possono quindi essere ripristinati o rimossi.

1 Aprire il riquadro File in quarantena.

   In che modo?

   1. Nel riquadro di sinistra, fare clic su **Menu avanzato**.
   2. Fare clic su **Ripristina**.
   3. Fare clic su **File**.

2 Selezionare un file in quarantena

3 Eseguire una delle seguenti operazioni:

   - Per riparare il file infetto e ripristinarlo nel percorso originale sul computer, fare clic su **Ripristina**.
   - Per rimuovere il file infetto dal computer, fare clic su **Rimuovi**.

4 Fare clic su **Sì** per confermare l'opzione selezionata.

Suggerimento: è possibile ripristinare o rimuovere più file contemporaneamente.

Come utilizzare i programmi e i cookie in quarantena

Quando i programmi potenzialmente indesiderati o i cookie traccianti vengono messi in quarantena, sono crittografati e quindi spostati in una cartella per impedire loro di danneggiare il computer. Gli elementi in quarantena possono quindi essere ripristinati o rimossi. Nella maggior parte dei casi, è possibile eliminare un elemento in quarantena senza alcuna ripercussione sul sistema.

1 Aprire il riquadro Programmi e cookie in quarantena.

   In che modo?

   1. Nel riquadro di sinistra, fare clic su **Menu avanzato**.
   2. Fare clic su **Ripristina**.
   3. Fare clic su **Programmi e cookie**.

2 Selezionare un programma o cookie in quarantena.

3 Eseguire una delle seguenti operazioni:

   - Per riparare il file infetto e ripristinarlo nel percorso originale sul computer, fare clic su **Ripristina**.

- Per rimuovere il file infetto dal computer, fare clic su **Rimuovi**.

4 Fare clic su **Sì** per confermare l'operazione.

Suggerimento: è possibile ripristinare o rimuovere più programmi e cookie contemporaneamente.

CAPITOLO 13

McAfee Personal Firewall

Personal Firewall offre una protezione avanzata per il computer e per i dati personali. Personal Firewall consente di stabilire una barriera tra il computer in uso e Internet, monitorando il traffico Internet alla ricerca di attività sospette, senza richiedere interazione da parte dell'utente.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Personal Firewall

Personal Firewall fornisce le funzioni illustrate di seguito.

Livelli di protezione standard e personalizzati

Protezione contro le intrusioni e le attività sospette mediante le impostazioni di protezione predefinite o personalizzabili del firewall.

Consigli in tempo reale

Il firewall offre l'opportunità di ricevere in maniera dinamica alcuni consigli che contribuiscono a determinare a quali programmi consentire l'accesso a Internet e se ritenere affidabile il traffico di rete.

Gestione intelligente dell'accesso per i programmi

Gestione dell'accesso a Internet per i programmi, mediante avvisi e registri degli eventi, e configurazione delle autorizzazioni di accesso per programmi specifici.

Protezione durante l'esecuzione di giochi

È possibile impedire la visualizzazione di avvisi relativi a tentativi di intrusione e attività sospette che possono distrarre l'utente durante l'esecuzione di giochi a schermo intero.

Protezione all'avvio del computer

All'avvio di Windows®, il firewall protegge il computer dai tentativi di intrusione, dai programmi indesiderati e dal traffico di rete.

Controllo delle porte dei servizi di sistema

Gestione delle porte dei servizi di sistema aperte e chiuse necessarie per alcuni programmi.

Gestione delle connessioni del computer

È possibile consentire e bloccare le connessioni tra il proprio computer e altri computer.

Integrazione delle informazioni di HackerWatch

Rilevamento di sequenze generali di attività di hacker e intrusioni attraverso il sito Web di HackerWatch, che inoltre fornisce dati aggiornati sulla protezione in relazione ai programmi presenti sul computer, nonché statistiche globali sugli eventi di protezione e sulle porte Internet.

Blocca firewall

Consente di bloccare immediatamente tutto il traffico in ingresso e in uscita tra il computer e Internet.

Ripristina firewall

Ripristina immediatamente le impostazioni di protezione originali del firewall.

Rilevamento avanzato di trojan

Consente di rilevare e bloccare applicazioni potenzialmente dannose, come i trojan, che potrebbero diffondere i dati personali dell'utente su Internet.

Registrazione eventi

Tiene traccia degli eventi in ingresso, in uscita e di intrusione più recenti.

Monitoraggio del traffico Internet

Analisi delle mappe che illustrano l'origine degli attacchi dannosi e del traffico a livello mondiale. Inoltre, è possibile individuare informazioni dettagliate sui proprietari e dati geografici relativi agli indirizzi IP di origine. Il firewall permette inoltre di analizzare il traffico in ingresso e in uscita, monitorare l'utilizzo della larghezza di banda dei programmi e le attività dei programmi.

Prevenzione delle intrusioni

Protezione della privacy da possibili minacce su Internet. Mediante una funzionalità di tipo euristico, McAfee offre un terzo livello di protezione bloccando gli elementi che presentano i sintomi di un attacco o le caratteristiche di un tentativo di intrusione.

Analisi complessa del traffico

Consente di analizzare il traffico Internet in ingresso e in uscita, nonché le connessioni dei programmi, compresi quelli attivamente in ascolto di connessioni aperte. In questo modo è possibile rilevare i programmi vulnerabili a un'eventuale intrusione e intervenire di conseguenza.

CAPITOLO 14

Avvio del firewall

Una volta installato il firewall, il computer è protetto da intrusioni e da traffico di rete indesiderato. Inoltre l'utente è pronto a gestire gli avvisi e l'accesso Internet in ingresso e in uscita di programmi noti e sconosciuti. Sono automaticamente selezionati i suggerimenti intelligenti e il livello di protezione Basato sull'affidabilità (con l'opzione che consente per i programmi l'accesso a Internet solo in uscita).

È possibile disattivare il firewall dal riquadro Configurazione di Internet e rete ma, in questo caso, il computer non sarà più protetto da intrusioni e da traffico di rete indesiderato e l'utente non potrà gestire in maniera efficace le connessioni Internet in ingresso e in uscita. Pertanto, la protezione firewall deve essere disattivata solo temporaneamente e in caso di necessità. Il firewall può essere anche attivato dal pannello Configurazione di Internet e rete.

Personal Firewall disattiva automaticamente Windows® Firewall e imposta se stesso come firewall predefinito.

Nota: per configurare Personal Firewall, aprire il riquadro Configurazione di Internet e rete.

In questo capitolo

Avvio della protezione firewall

È possibile attivare il firewall per proteggere il computer dalle intrusioni e dal traffico di rete indesiderato, nonché per gestire le connessioni Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è disattivata**, fare clic su **Attiva**.

Come arrestare la protezione firewall

È possibile disattivare il firewall se non si desidera proteggere il computer dalle intrusioni e dal traffico di rete indesiderato. Se il firewall è disattivato, non è possibile gestire le connessioni Internet in ingresso o in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Disattiva**.

CAPITOLO 15

Utilizzo degli avvisi

Il firewall utilizza una serie di avvisi che facilitano la gestione della protezione da parte dell'utente. Questi avvisi possono essere raggruppati in tre tipi principali:

- Avviso rosso
- Avviso giallo
- Avviso verde

Gli avvisi possono anche contenere informazioni utili per decidere come gestire gli avvisi o ottenere informazioni sui programmi in esecuzione sul computer.

In questo capitolo

Informazioni sugli avvisi

Il firewall prevede tre tipi principali di avvisi. Alcuni avvisi, inoltre, includono informazioni utili all'apprendimento o al reperimento di informazioni relative ai programmi in esecuzione sul computer.

Avviso rosso

L'avviso rosso viene visualizzato quando il firewall rileva, e quindi blocca, un trojan sul computer e suggerisce una scansione per la ricerca di altre minacce. Un trojan ha l'aspetto di un programma legittimo, ma può consentire l'accesso non autorizzato al computer, provocarne malfunzionamenti e danneggiarlo. Questo tipo di avviso può verificarsi su tutti i livelli di protezione, ad esclusione del livello "Aperto".

Avviso giallo

Il tipo più comune di avviso è quello giallo, che informa l'utente quando il firewall rileva un'attività di programma o un evento di rete. In questi casi, l'avviso descrive l'attività di programma o evento di rete e fornisce una o più opzioni che richiedono una risposta da parte dell'utente. Ad esempio, l'avviso **Rilevata nuova rete** viene visualizzato quando un computer su cui è installato il firewall è connesso a una nuova rete. È possibile scegliere se impostare o non impostare come affidabile la rete. Nel primo caso, il firewall consente il traffico da qualsiasi altro computer in rete e viene aggiunto agli indirizzi IP affidabili. Quando Suggerimenti intelligenti è attivato, i programmi vengono aggiunti al riquadro Autorizzazioni programmi.

Avviso verde

Nella maggioranza dei casi, un avviso verde fornisce informazioni di base su un evento, senza richiedere la risposta da parte dell'utente. Gli avvisi verdi sono disattivati per impostazione predefinita e in genere si verificano quando sono impostati i livelli di protezione Standard, Basato sull'affidabilità, Elevato e Mascheramento.

Assistenza per l'utente

Molti avvisi firewall contengono ulteriori informazioni che consentono di gestire con facilità la protezione del computer, tra cui:

- **Ulteriori informazioni su questo programma**: avviare il sito Web di protezione globale di McAfee per ottenere informazioni su un programma che il firewall ha rilevato sul computer.

- **Informa McAfee di questo programma**: inviare informazioni a McAfee su un file sconosciuto rilevato sul computer dal firewall.
- **McAfee suggerisce**: vengono forniti suggerimenti per la gestione degli avvisi. Ad esempio, un avviso può suggerire di concedere l'accesso a un programma.

CAPITOLO 16

Gestione degli avvisi informativi

Il firewall consente di visualizzare o nascondere gli avvisi informativi quando rileva un tentativo di intrusione o un'attività sospetta nel corso di determinati eventi, ad esempio durante l'esecuzione di giochi a schermo intero.

In questo capitolo

Visualizzazione degli avvisi durante l'esecuzione di giochi

È possibile consentire la visualizzazione degli avvisi informativi del firewall quando vengono rilevati tentativi di intrusione o attività sospette durante l'esecuzione di giochi a schermo intero.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avanzate** nella sezione **Avvisi**.
4. Nel riquadro Opzioni di avviso, selezionare **Visualizza avvisi informativi quando viene rilevata la modalità di gioco**.
5. Fare clic su **OK**.

Nascondi avvisi informativi

È possibile impedire la visualizzazione degli avvisi informativi del firewall quando vengono rilevati tentativi di intrusione o attività sospette.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Configura**.
3. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avanzate** nella sezione **Avvisi**.
4. Nel riquadro Configurazione di SecurityCenter, fare clic su **Avvisi informativi**.
5. Nel riquadro Avvisi informativi, effettuare una delle seguenti operazioni:
   - Selezionare **Non visualizzare avvisi informativi** per nascondere tutti gli avvisi informativi.
   - Cancellare un avviso da nascondere.
6. Fare clic su **OK**.

CAPITOLO 17

Configurazione della protezione del firewall

Il firewall prevede alcuni metodi per gestire la protezione e personalizzare la modalità di risposta agli eventi e agli avvisi relativi alla protezione.

Dopo avere installato il firewall per la prima volta, il livello di protezione del computer viene impostato su Basato sull'affidabilità e per i programmi in uso è consentito l'accesso a Internet solo in uscita. Il firewall comunque fornisce altri livelli, a partire da quelli maggiormente restrittivi per arrivare a quelli più permissivi.

Offre inoltre l'opportunità di ricevere suggerimenti concernenti gli avvisi e l'accesso Internet dei programmi.

In questo capitolo

Gestione dei livelli di protezione del firewall

I livelli di protezione del firewall controllano in che misura l'utente desidera gestire gli avvisi e rispondere agli stessi. Gli avvisi vengono visualizzati quando il firewall rileva traffico di rete indesiderato e connessioni a Internet in ingresso e in uscita. Per impostazione predefinita, il livello di protezione del firewall è impostato su Basato sull'affidabilità, con accesso solo in uscita.

Se è impostato il livello di protezione Basato sull'affidabilità e sono attivati i suggerimenti intelligenti, gli avvisi gialli offrono la possibilità di consentire o bloccare l'accesso per i programmi sconosciuti che richiedono l'accesso in ingresso. Al rilevamento di programmi noti, viene visualizzato un avviso informativo di colore verde e l'accesso è automaticamente consentito. Ottenuto l'accesso, un programma sarà in grado di creare connessioni in uscita e di ascoltare connessioni in ingresso non richieste.

In genere, più il livello di protezione è restrittivo (Mascheramento ed Elevato), maggiore sarà il numero di opzioni e avvisi visualizzati che, a loro volta, dovranno essere gestiti dall'utente.

Nella tabella che segue sono riportati i sei livelli di protezione del firewall, a partire dal più restrittivo:

Livello	Descrizione
Blocco	Blocca tutte le connessioni di rete, sia in ingresso che in uscita. L'accesso a siti Web, posta elettronica e aggiornamenti della protezione è bloccato. Il risultato offerto da questo livello di protezione equivale a quello che si otterrebbe rimuovendo la connessione a Internet. È possibile utilizzare questa impostazione per bloccare porte configurate come aperte nel riquadro Servizi di sistema.
Mascheramento	Blocca tutte le connessioni a Internet in ingresso, escluse le porte aperte, nascondendo la presenza del computer su Internet. Il firewall avvisa quando un nuovo programma tenta di stabilire una connessione a Internet in uscita oppure riceve una richiesta di connessione in ingresso. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi.
Elevato	Avvisa quando un nuovo programma tenta di stabilire una connessione a Internet in uscita oppure riceve una richiesta di connessione in ingresso. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi. Quando il livello di protezione è impostato su Elevato, un programma richiede solo il tipo di accesso necessario in quel momento, ad esempio l'accesso solo in uscita, che l'utente può consentire o bloccare. In seguito, qualora il programma richieda una connessione sia in ingresso che in uscita, è possibile consentire l'accesso completo al programma dal riquadro Autorizzazioni programmi.

Standard	Esegue il monitoraggio delle connessioni in ingresso e in uscita e visualizza un avviso quando un nuovo programma tenta di accedere a Internet. I programmi bloccati e aggiunti sono visualizzati nel riquadro Autorizzazioni programmi.
Basato sull'affidabilità	Consente ai programmi di accedere a Internet in ingresso e in uscita (accesso completo) oppure solo in uscita. Il livello di protezione predefinito è Basato sull'affidabilità e ai programmi è consentito solo l'accesso in uscita. Se a un programma viene consentito l'accesso completo, il firewall lo considera automaticamente affidabile e lo aggiunge all'elenco dei programmi consentiti nel riquadro Autorizzazioni dei programmi. Se un programma dispone solo dell'accesso in uscita, il firewall lo considera automaticamente affidabile solo quando effettua una connessione a Internet in uscita. Una connessione in ingresso non viene automaticamente considerata affidabile.
Aperto	Consente tutte le connessioni Internet, sia in ingresso che in uscita.

Il firewall offre inoltre la possibilità di reimpostare immediatamente il livello di protezione su Basato sull'affidabilità, consentendo l'accesso solo in uscita, dal riquadro Ripristina le impostazioni predefinite della protezione firewall.

Impostazione del livello di protezione su Blocco

È possibile impostare il livello di protezione su Blocco per bloccare tutte le connessioni di rete in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Blocco** venga visualizzato come livello corrente.
4. Fare clic su **OK**.

Impostazione del livello di protezione su Mascheramento

Il livello di protezione del firewall può essere impostato su Mascheramento per bloccare tutte le connessioni di rete in ingresso, fatta eccezione per le porte aperte, e nascondere la presenza del computer su Internet.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Mascheramento** venga visualizzato come livello corrente.
4. Fare clic su **OK**.

Nota: in modalità Mascheramento, il firewall avvisa l'utente quando nuovi programmi richiedono la connessione a Internet in uscita o ricevono richieste di connessione in ingresso.

Impostazione del livello di protezione su Elevato

È possibile impostare il livello di protezione del firewall su Elevato per ricevere un avviso se un nuovo programma tenta di stabilire una connessione in uscita a Internet oppure riceve una richiesta di connessione in ingresso.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Elevato** venga visualizzato come livello corrente.
4. Fare clic su **OK**.

Nota: in modalità Elevato, un programma richiede solo il tipo di accesso necessario in un dato momento, ad esempio l'accesso solo in uscita, che può essere consentito o bloccato. Se, in seguito, il programma richiede una connessione sia in ingresso che in uscita, è possibile consentire l'accesso completo al programma dal riquadro Autorizzazioni programmi.

Impostazione del livello di protezione su Standard

È possibile impostare il livello di protezione su Standard per monitorare le connessioni in ingresso e in uscita e per ricevere un avviso quando nuovi programmi tentano di effettuare l'accesso a Internet.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Standard** venga visualizzato come livello corrente.
4. Fare clic su **OK**.

Impostazione del livello di protezione su Basato sull'affidabilità

Il livello di protezione del firewall può essere impostato su Basato sull'affidabilità per consentire l'accesso completo o l'accesso alla rete solo in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **La protezione firewall è attivata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Basato sull'affidabilità** venga visualizzato come livello corrente.
4. Eseguire una delle seguenti operazioni:
   - Per consentire l'accesso completo alla rete in ingresso e in uscita, selezionare **Accesso completo**.
   - Per consentire l'accesso alla rete solo in uscita, selezionare **Autorizza solo accesso in uscita**.
5. Fare clic su **OK**.

Nota: Autorizza solo accesso in uscita è l'opzione predefinita.

Impostazione del livello di protezione su Aperto

È possibile impostare il livello di protezione su Aperto per consentire tutte le connessioni di rete in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, spostare il dispositivo di scorrimento in modo tale che **Aperto** venga visualizzato come livello corrente.
4. Fare clic su **OK**.

Configurazione dei suggerimenti intelligenti per gli avvisi

È possibile configurare il firewall in modo tale da includere, escludere o visualizzare suggerimenti negli avvisi quando i programmi tentano di accedere a Internet. L'attivazione dei suggerimenti intelligenti aiuta a decidere la modalità di gestione degli avvisi.

Con i suggerimenti intelligenti attivati, e il livello di protezione impostato su Basato sull'affidabilità con accesso consentito solo in uscita, il firewall consente o blocca automaticamente i programmi conosciuti e visualizza un suggerimento nell'avviso se rileva la presenza di programmi potenzialmente pericolosi.

Se i suggerimenti intelligenti sono disattivati, il firewall non consente né blocca l'accesso a Internet e non fornisce indicazioni sul piano di azione nell'avviso.

Se per i suggerimenti intelligenti è impostata l'opzione Solo visualizzazione, un avviso chiede di consentire o bloccare l'accesso ma indica un piano di azione.

Attiva suggerimenti intelligenti

È possibile attivare i suggerimenti intelligenti per fare in modo che il firewall consenta o blocchi automaticamente programmi e avvisi nel caso in cui rilevi programmi non riconosciuti e potenzialmente pericolosi.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Attiva suggerimenti intelligenti**.
4. Fare clic su **OK**.

Disattiva suggerimenti intelligenti

È possibile disattivare i suggerimenti intelligenti per fare in modo che il firewall consenta o blocchi i programmi e avvisi nel caso in cui rilevi programmi non riconosciuti e potenzialmente pericolosi. Tuttavia, gli avvisi non includono suggerimenti sulla gestione dell'accesso per i programmi. Se rileva un nuovo programma sospetto o noto come potenziale minaccia, il firewall impedisce automaticamente al programma di accedere a Internet.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Disattiva suggerimenti intelligenti**.
4. Fare clic su **OK**.

Impostazione dei suggerimenti intelligenti per la sola visualizzazione

È possibile visualizzare i suggerimenti intelligenti in modo tale che gli avvisi contengano indicazioni utili per decidere se consentire o bloccare programmi non riconosciuti o potenzialmente pericolosi.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Suggerimenti intelligenti**, selezionare **Solo visualizzazione**.
4. Fare clic su **OK**.

Ottimizzazione della protezione firewall

La protezione di un computer può risultare compromessa per diverse ragioni. Ad esempio, alcuni programmi potrebbero tentare di connettersi a Internet prima dell'avvio di Windows®. Inoltre, utenti particolarmente esperti potrebbero rintracciare il computer, inviando un ping, per stabilire se è connesso a una rete. Grazie al firewall è possibile difendersi contro questi due tipi di intrusione, consentendo l'attivazione della protezione all'avvio e il blocco delle richieste ping. La prima impostazione impedisce ai programmi di accedere a Internet all'avvio di Windows, mentre la seconda blocca le richieste ping che consentono ad altri utenti di individuare il computer su una rete.

Le impostazioni di installazione standard includono il rilevamento automatico dei tentativi di intrusione più comuni, ad esempio attacchi o vulnerabilità che causano negazioni del servizio (DoS, Denial of Service). L'utilizzo di tali impostazioni garantisce la protezione dell'utente contro attacchi e scansioni, tuttavia è possibile disattivare il rilevamento automatico per uno o più attacchi o scansioni nel riquadro Rilevamento delle intrusioni.

Protezione del computer durante l'avvio

È possibile proteggere il computer all'avvio di Windows per bloccare nuovi programmi che non avevano accesso a Internet durante l'avvio e che adesso lo richiedono. Il firewall visualizza gli avvisi rilevanti per i programmi che avevano richiesto l'accesso a Internet, che è possibile consentire o bloccare. Per utilizzare questa opzione, è necessario che il livello di protezione non sia impostato su Aperto o su Blocco.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Impostazioni protezione**, selezionare **Attiva protezione all'avvio**.
4. Fare clic su **OK**.

Nota: finché è abilitata la protezione all'avvio le connessioni risultano bloccate e non viene registrata alcuna intrusione.

Come configurare le impostazioni di richieste ping

È possibile consentire o impedire ad altri utenti del computer di rilevare il computer sulla rete.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Livello di protezione, in **Impostazioni protezione**, effettuare una delle seguenti operazioni:
   - Selezionare **Consenti richieste ping ICMP** per consentire il rilevamento del computer sulla rete mediante richieste ping.
   - Deselezionare **Consenti richieste ping ICMP** per impedire il rilevamento del computer sulla rete mediante richieste ping.
4. Fare clic su **OK**.

Come configurare il rilevamento intrusioni

È possibile rilevare i tentativi di intrusione per proteggere il computer da attacchi e scansioni non autorizzate. Le impostazioni standard del firewall includono il rilevamento automatico dei tentativi di intrusione più comuni, quali gli attacchi di negazione di servizio (DoS, Denial of Service) o lo sfruttamento dei punti deboli, tuttavia è possibile disattivare il rilevamento automatico per uno o più attacchi o scansioni.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Rilevamento delle intrusioni**.
4. In **Rileva tentativi di intrusione**, effettuare una delle seguenti operazioni:
   - Selezionare un nome per rilevare automaticamente l'attacco o la scansione.
   - Deselezionare un nome per disattivare il rilevamento automatico dell'attacco o della scansione.
5. Fare clic su **OK**.

Come configurare le impostazioni relative allo stato della protezione firewall

È possibile configurare il firewall in modo che ignori la mancata segnalazione di problemi specifici del computer a SecurityCenter.

1. Nella sezione **Informazioni su SecurityCenter** del riquadro McAfee SecurityCenter, fare clic su **Configura**.
2. Nel riquadro Configurazione di SecurityCenter, nella sezione **Stato protezione**, fare clic su **Avanzate**.
3. Nel riquadro Problemi ignorati, selezionare una o più delle seguenti opzioni:
   - **La protezione firewall è disattivata.**
   - **Il firewall è impostato sul livello di protezione Aperto.**
   - **Il servizio firewall non è in esecuzione.**
   - **La protezione firewall non è installata nel computer.**
   - **Windows Firewall non è attivo.**
   - **Il firewall in uscita non è installato nel computer.**
4. Fare clic su **OK**.

Blocco e ripristino del firewall

La funzione di blocco arresta immediatamente tutto il traffico di rete in ingresso e in uscita per consentire di isolare e risolvere il problema nel computer.

Come bloccare immediatamente il firewall

È possibile bloccare il firewall per bloccare immediatamente tutto il traffico di rete tra il computer e Internet.

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Blocca firewall**.
2. Nel riquadro Blocca firewall, fare clic su **Blocco**.
3. Fare clic su **Sì** per confermare.

Suggerimento: è anche possibile bloccare il firewall facendo clic con il pulsante destro del mouse sull'icona di SecurityCenter nell'area di notifica all'estrema destra della barra delle applicazioni, quindi fare clic su **Collegamenti rapidi** e infine su **Blocca firewall**.

Come sbloccare immediatamente il firewall

È possibile sbloccare il firewall per consentire immediatamente tutto il traffico di rete tra il computer e Internet.

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Blocca firewall**.
2. Nel riquadro Blocco attivato, fare clic su **Sblocca**.
3. Fare clic su **Sì** per confermare.

Come ripristinare le impostazioni del firewall

È possibile ripristinare rapidamente le impostazioni di protezione originali del firewall. La funzione di ripristino reimposta il livello di protezione su Basato sull'affidabilità e consente l'accesso alla rete solo in uscita, attiva i suggerimenti intelligenti, ripristina l'elenco dei programmi predefiniti e le relative autorizzazioni nel riquadro Autorizzazioni programmi, rimuove gli indirizzi IP affidabili ed esclusi e ripristina i servizi di sistema, le impostazioni del registro eventi e il rilevamento intrusioni.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Ripristina le impostazioni predefinite del firewall**.
2. Nel riquadro Ripristina le impostazioni predefinite della protezione firewall, fare clic su **Ripristina impostazioni predefinite**.
3. Fare clic su **Sì** per confermare.

Suggerimento: è anche possibile ripristinare le impostazioni predefinite del firewall facendo clic con il pulsante destro del mouse sull'icona di SecurityCenter nell'area di notifica all'estrema destra della barra delle applicazioni, quindi fare clic su **Collegamenti rapidi** e infine su **Ripristina le impostazioni predefinite del firewall**.

CAPITOLO 18

Gestione dei programmi e delle autorizzazioni

Personal Firewall consente di gestire e di creare autorizzazioni di accesso per programmi già esistenti e nuovi che richiedono accesso a Internet in ingresso e in uscita. Il firewall consente di controllare l'accesso completo o solo in uscita per i programmi, ma anche di bloccare qualsiasi tipo di accesso.

In questo capitolo

Autorizzazione di accesso a Internet per i programmi

Alcuni programmi, quali i browser Internet, devono necessariamente accedere a Internet per funzionare in modo corretto.

Personal Firewall consente di utilizzare la pagina Autorizzazioni programmi per:

- Consentire l'accesso per i programmi
- Consentire solo l'accesso in uscita per i programmi
- Bloccare l'accesso per i programmi

È inoltre possibile consentire l'accesso completo e solo in uscita a Internet per un programma dal registro Eventi in uscita ed Eventi recenti.

Come autorizzare l'accesso completo per un programma

È possibile consentire a un programma bloccato esistente nel computer di avere accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Bloccato** o **Solo accesso in uscita**.
5. In **Azione**, fare clic su **Autorizza accesso**.
6. Fare clic su **OK**.

Come autorizzare l'accesso completo per un nuovo programma

È possibile consentire a un nuovo programma del computer di avere accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, fare clic su **Aggiungi programma autorizzato**.
5. Nella finestra di dialogo **Aggiungi programma**, cercare e selezionare il programma che si desidera aggiungere, quindi fare clic su **Apri**.

Nota: è possibile modificare le autorizzazioni di un programma appena aggiunto in modo analogo a quello di un programma esistente, selezionandolo e quindi facendo clic su **Autorizza solo accesso in uscita** o su **Blocca accesso** in **Azione**.

Come autorizzare l'accesso completo dal registro Eventi recenti

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi recenti, in modo che abbia accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, selezionare la descrizione dell'evento, quindi fare clic su **Autorizza accesso**.
4. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Argomenti correlati

- Come visualizzare gli eventi in uscita (pagina 117)

Come autorizzare l'accesso completo dal registro Eventi in uscita

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi in uscita in modo che abbia accesso completo a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.
5. Selezionare un programma, quindi in **Desidero**, fare clic su **Autorizza accesso**.
6. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Autorizzazione per l'accesso solo in uscita ai programmi

Alcuni programmi del computer richiedono l'accesso a Internet in uscita. Il firewall consente di configurare le autorizzazioni dei programmi per consentire l'accesso a Internet solo in uscita.

Come autorizzare l'accesso solo in uscita per un programma

È possibile autorizzare un programma per l'accesso a Internet solo in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Bloccato** o **Accesso completo**.
5. In **Azione**, fare clic su **Autorizza solo accesso in uscita**.
6. Fare clic su **OK**.

Come autorizzare l'accesso solo in uscita dal registro Eventi recenti

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi recenti in modo che abbia accesso a Internet solo in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, selezionare la descrizione dell'evento, quindi fare clic su **Autorizza solo accesso in uscita**.
4. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Come autorizzare l'accesso solo in uscita dal registro Eventi in uscita

È possibile autorizzare un programma esistente bloccato, visualizzato nel registro Eventi in uscita in modo che abbia accesso a Internet solo in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.
5. Selezionare un programma, quindi in **Desidero**, fare clic su **Autorizza solo accesso in uscita**.
6. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Blocco dell'accesso a Internet per i programmi

Personal Firewall consente di impedire ai programmi l'accesso a Internet. Accertarsi che il blocco di un programma non interrompa la connessione di rete o non impedisca a un altro programma che richiede l'accesso a Internet di funzionare in modo corretto.

Come bloccare l'accesso per un programma

È possibile bloccare un programma in modo che non abbia accesso a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, selezionare un programma contrassegnato con **Accesso completo** o **Solo accesso in uscita**.
5. In **Azione**, fare clic su **Blocca accesso**.
6. Fare clic su **OK**.

Come bloccare l'accesso per un nuovo programma

È possibile bloccare un nuovo programma in modo che non abbia accesso a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. In **Autorizzazioni programmi**, fare clic su **Aggiungi programma bloccato**.
5. Nella finestra di dialogo Aggiungi programma, cercare e selezionare il programma che si desidera aggiungere, quindi fare clic su **Apri**.

Nota: per modificare le autorizzazioni di un programma appena aggiunto, selezionare il programma e fare clic su **Autorizza solo accesso in uscita** o su **Autorizza accesso** in **Azione**.

Come bloccare l'accesso dal registro Eventi recenti

È possibile bloccare un programma visualizzato nel registro Eventi recenti in modo che non abbia accesso a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, selezionare la descrizione dell'evento, quindi fare clic su **Blocca accesso**.
4. Nella finestra di dialogo Autorizzazioni programmi, fare clic su **Sì** per confermare.

Rimozione delle autorizzazioni di accesso per i programmi

Prima di rimuovere un'autorizzazione per un programma, accertarsi che l'eliminazione non influisca sulla funzionalità del computer o della connessione di rete.

Come rimuovere un'autorizzazione per un programma

È possibile rimuovere un programma in modo che non abbia accesso a Internet in ingresso e in uscita.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. Selezionare un programma in **Autorizzazioni programmi**.
5. In **Azione**, fare clic su **Rimuovi autorizzazione programma**.
6. Fare clic su **OK**.

Nota: Personal Firewall impedisce all'utente di modificare alcuni programmi visualizzando in grigio e disattivando determinate azioni.

Informazioni sui programmi

Se non si è certi dell'autorizzazione da applicare per un programma, è possibile reperire informazioni relative al programma sul sito Web HackerWatch di McAfee.

Come reperire informazioni sui programmi

È possibile reperire informazioni sui programmi sul sito Web HackerWatch di McAfee per decidere se consentire o bloccare l'accesso a Internet in ingresso e in uscita.

Nota: accertarsi di essere connessi a Internet affinché il browser possa avviare il sito Web HackerWatch di McAfee, che fornisce informazioni aggiornate su programmi, requisiti di accesso a Internet e minacce per la protezione.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Autorizzazioni programmi**.
4. Selezionare un programma in **Autorizzazioni programmi**.
5. In **Azione**, fare clic su **Ulteriori informazioni**.

Come reperire informazioni sui programma dal registro Eventi in uscita

Mediante il registro Eventi in uscita, è possibile ottenere le informazioni sui programmi presenti sul sito Web HackerWatch di McAfee e decidere per quali programmi consentire o bloccare l'accesso a Internet in ingresso e in uscita.

Nota: accertarsi di essere connessi a Internet affinché il browser possa avviare il sito Web HackerWatch di McAfee, che fornisce informazioni aggiornate su programmi, requisiti di accesso a Internet e minacce per la protezione.

1. Nel riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In Eventi recenti selezionare un evento, quindi fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.
5. Selezionare un indirizzo IP, quindi fare clic su **Ulteriori informazioni**.

CAPITOLO 19

Gestione dei servizi di sistema

Per funzionare correttamente, alcuni programmi, tra cui i server Web o i programmi server di condivisione dei file, devono accettare connessioni non richieste da altri computer attraverso porte progettate per i servizi di sistema. In genere il firewall chiude le porte dei servizi di sistema poiché rappresentano l'origine più probabile dei problemi di protezione del sistema. Per accettare le connessioni dai computer remoti è comunque necessario aprire tali porte.

In questo capitolo

Configurazione delle porte dei servizi di sistema

È possibile configurare le porte dei servizi di sistema in modo da consentire o bloccare l'accesso remoto alla rete a un servizio presente sul computer.

Nell'elenco che segue sono riportati i servizi di sistema comuni e le porte ad essi associate:

- Porte 20-21 di File Transfer Protocol (FTP)
- Porta 143 del server di posta (IMAP)
- Porta 110 del server di posta (POP3)
- Porta 25 del server di posta (SMTP)
- Porta 445 di Microsoft Directory Server (MSFT DS)
- Porta 1433 di Microsoft SQL Server (MSFT SQL)
- Porta 123 di Network Time Protocol
- Porta 3389 di Desktop remoto/ Assistenza remota / Terminal Server (RDP)
- Porta 135 per chiamate di procedura remota (RPC)
- Porta 443 del server Web protetto (HTTPS)
- Porta 5000 di Universal Plug and Play (UPNP)
- Porta 80 del server Web (HTTP)
- Porte 137-139 per la condivisione file in Windows (NETBIOS)

È inoltre possibile configurare le porte dei servizi di sistema in modo da consentire a un computer di condividere la connessione Internet con altri computer a cui è collegato tramite la stessa rete. Tale connessione, nota come Condivisione connessione Internet (ICS, Internet Connection Sharing), fa sì che il computer che condivide la connessione svolga la funzione di gateway per Internet per gli altri computer collegati in rete.

Nota: se nel computer è presente un'applicazione che accetta le connessioni al server Web o FTP, è possibile che il computer che condivide la connessione debba aprire la porta dei servizi di sistema associata e consentire le connessioni in arrivo e di inoltro per tali porte.

Come consentire l'accesso alla porta di un servizio di sistema esistente

È possibile aprire una porta esistente per consentire l'accesso remoto a un servizio di rete del computer in uso.

Nota: le porte dei servizi di sistema aperte possono rendere il computer vulnerabile a minacce per la protezione, pertanto devono essere aperte solo in caso di necessità.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. In **Apri porta del servizio di sistema** selezionare un servizio di sistema per aprire la porta associata.
5. Fare clic su **OK**.

Come bloccare l'accesso a una porta dei servizi di sistema esistente

È possibile chiudere una porta esistente per bloccare l'accesso remoto alla rete di un servizio del computer in uso.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. In **Apri porta del servizio di sistema**, deselezionare un servizio di sistema per chiudere la porta associata.
5. Fare clic su **OK**.

Come configurare una nuova porta dei servizi di sistema

È possibile configurare nel computer una nuova porta dei servizi di rete da aprire o chiudere per consentire o bloccare l'accesso remoto al computer in uso.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. Fare clic su **Aggiungi**.
5. Nel riquadro Servizi di sistema, in **Porte e servizi di sistema**, immettere quanto segue:
   - Nome programma
   - Porte TCP/IP in ingresso
   - Porte TCP/IP in uscita
   - Porte UDP in ingresso
   - Porte UDP in uscita
6. Se si desidera inviare le informazioni relative all'attività di tale porta a un altro computer Windows collegato in rete, che condivide la connessione a Internet, selezionare **Inoltrare l'attività di questa porta agli utenti di rete che utilizzano Condivisione connessione Internet (ICS, Internet Connection Sharing)**.
7. Se lo si desidera, descrivere la nuova configurazione.
8. Fare clic su **OK**.

Nota: se nel computer è presente un'applicazione che accetta le connessioni al server Web o FTP, è possibile che il computer che condivide la connessione debba aprire la porta dei servizi di sistema associata e consentire le connessioni in arrivo e di inoltro per tali porte. Se si utilizza Condivisione connessione Internet (ICS, Internet Connection Sharing), occorre inoltre aggiungere una connessione a computer affidabile all'elenco Indirizzi IP affidabili. Per ulteriori informazioni, vedere Come aggiungere una connessione a computer affidabile.

Come modificare una porta dei servizi di sistema

È possibile modificare le informazioni di accesso alla rete in ingresso e in uscita relative a una porta dei servizi di sistema esistente.

Nota: se le informazioni sulla porta non vengono inserite in modo corretto, il servizio di sistema non funziona.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. Selezionare un servizio di sistema e fare clic su **Modifica**.
5. Nel riquadro Servizi di sistema, in **Porte e servizi di sistema**, immettere quanto segue:
   - Nome programma
   - Porte TCP/IP in ingresso
   - Porte TCP/IP in uscita
   - Porte UDP in ingresso
   - Porte UDP in uscita
6. Se si desidera inviare le informazioni relative all'attività di tale porta a un altro computer Windows collegato in rete, che condivide la connessione a Internet, selezionare **Inoltrare l'attività di questa porta agli utenti di rete che utilizzano Condivisione connessione Internet (ICS, Internet Connection Sharing)**.
7. Se lo si desidera, descrivere la configurazione modificata.
8. Fare clic su **OK**.

Come rimuovere una porta dei servizi di sistema

È possibile rimuovere dal computer una porta dei servizi di sistema. Dopo la rimozione i computer remoti non saranno più in grado di accedere al servizio di rete sul computer in uso.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **Servizi di sistema**.
4. Selezionare un servizio di sistema e fare clic su **Rimuovi**.
5. Alla richiesta di conferma, fare clic su **Sì**.

CAPITOLO 20

Gestione delle connessioni al computer

È possibile configurare il firewall in modo tale da gestire connessioni remote specifiche al computer mediante la creazione di regole, basate sugli indirizzi IP, associate ai computer remoti. I computer associati a indirizzi IP affidabili si possono considerare idonei alla connessione al computer in uso mentre gli indirizzi IP sconosciuti, sospetti o inattendibili, possono essere esclusi dalla connessione al computer.

Quando si consente una connessione, accertarsi che il computer considerato affidabile sia protetto. Se infatti tale computer fosse infetto per la presenza di un worm o di un altro meccanismo, il computer in uso potrebbe essere vulnerabile all'infezione. McAfee consiglia inoltre di proteggere con un firewall e un programma antivirus aggiornato anche i computer considerati affidabili. Il firewall non registra il traffico né genera avvisi relativi a eventi provenienti da indirizzi IP inclusi nell'elenco Indirizzi IP affidabili.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

In questo capitolo

Impostazione di una connessione come affidabile

È possibile aggiungere, modificare e rimuovere indirizzi IP affidabili nel riquadro IP affidabili ed esclusi nella sezione **Indirizzi IP affidabili**.

L'elenco **Indirizzi IP affidabili** nel riquadro IP affidabili ed esclusi consente a tutto il traffico proveniente da un determinato computer di raggiungere il computer in uso. Personal Firewall non registra il traffico né genera avvisi relativi a eventi provenienti da indirizzi IP inclusi nell'elenco **Indirizzi IP affidabili**.

Il firewall imposta come affidabili tutti gli indirizzi IP selezionati in elenco e consente sempre il traffico proveniente dagli stessi attraverso il firewall su qualsiasi porta. L'attività intercorrente tra il computer associato a un indirizzo IP affidabile e quello in uso non viene filtrata o analizzata dal firewall. Per impostazione predefinita, Indirizzi IP affidabili elenca la prima rete privata rilevata dal firewall.

Quando si consente una connessione, accertarsi che il computer considerato affidabile sia protetto. Se infatti tale computer fosse infetto per la presenza di un worm o di un altro meccanismo, il computer in uso potrebbe essere vulnerabile all'infezione. McAfee consiglia inoltre di proteggere con un firewall e un programma antivirus aggiornato anche i computer considerati affidabili.

Come aggiungere una connessione a computer affidabile

È possibile aggiungere una connessione a un computer affidabile con i relativi indirizzi IP.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
4. Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP affidabili**, quindi fare clic su **Aggiungi**.
5. In **Aggiungi regola indirizzi IP affidabili**, effettuare una delle seguenti operazioni:
   - Selezionare **Indirizzo IP singolo** e immettere l'indirizzo IP.
   - Selezionare **Intervallo di indirizzi IP** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**.
6. Se un servizio di sistema utilizza Condivisione connessione Internet (ICS, Internet Connection Sharing), è possibile

aggiungere il seguente intervallo di indirizzi IP: da 192.168.0.1 a 192.168.0.255.

7 Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.

8 Se lo si desidera, digitare una descrizione della regola.

9 Fare clic su **OK**.

10 Nella finestra di dialogo **IP affidabili ed esclusi**, fare clic su **Sì** per confermare.

Nota: per ulteriori informazioni su Condivisione connessione Internet (ICS, Internet Connection Sharing), vedere Come configurare un nuovo servizio di sistema.

Come aggiungere un computer affidabile dal registro Eventi in ingresso

È possibile aggiungere una connessione a computer affidabile con il relativo indirizzo IP dal registro Eventi in ingresso.

1 Nella sezione Attività comuni del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.

2 Fare clic su **Rapporti e registri**.

3 In **Eventi recenti**, fare clic su **Visualizza registro**.

4 Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.

5 Selezionare un indirizzo IP di origine quindi, nella sezione **Desidero**, fare clic su **Imposta indirizzo come affidabile**.

6 Fare clic su **Sì** per confermare.

Come modificare una connessione a computer affidabile

È possibile modificare una connessione a computer affidabile con i relativi indirizzi IP.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.

2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.

3 Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.

4 Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP affidabili**.

5 Selezionare un indirizzo IP, quindi fare clic su **Modifica**.

6 In **Modifica regola indirizzi IP affidabili**, effettuare una delle seguenti operazioni:

- Selezionare **Indirizzo IP singolo** e immettere l'indirizzo IP.

- Selezionare **Intervallo di indirizzi IP** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**.

7 Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.

8 Se lo si desidera, digitare una descrizione della regola.

9 Fare clic su **OK**.

Nota: non è possibile modificare le connessioni predefinite del computer che il firewall ha aggiunto automaticamente da una rete privata affidabile.

Come rimuovere una connessione a computer affidabile

È possibile rimuovere una connessione a computer affidabile con i relativi indirizzi IP.

1 Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.

2 Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.

3 Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.

4 Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP affidabili**.

5 Selezionare un indirizzo IP, quindi fare clic su **Rimuovi**.

6 Nella finestra di dialogo **IP affidabili ed esclusi**, fare clic su **Sì** per confermare.

Esclusione delle connessioni a computer

È possibile aggiungere, modificare e rimuovere indirizzi IP esclusi nel riquadro IP affidabili ed esclusi nella sezione **Indirizzi IP esclusi**.

I computer associati a indirizzi IP sconosciuti, sospetti o inattendibili possono essere esclusi dalla connessione al computer.

Poiché Personal Firewall blocca tutto il traffico indesiderato, di solito non è necessario escludere un indirizzo IP. È opportuno farlo solo quando si è certi che una connessione Internet comporti una specifica minaccia. Assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet. In base alle impostazioni di protezione, Personal Firewall avvisa l'utente nel momento in cui rileva un evento proveniente da un computer escluso.

Come aggiungere una connessione a computer escluso

È possibile aggiungere una connessione a computer escluso con i relativi indirizzi IP.

Nota: assicurarsi di non bloccare indirizzi IP importanti, quali il server DNS o DHCP o altri server del provider di servizi Internet.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
4. Nel riquadro IP affidabili ed esclusi selezionare **Indirizzi IP esclusi**, quindi fare clic su **Aggiungi**.
5. In **Aggiungi regola indirizzi IP esclusi**, effettuare una delle seguenti operazioni:
   - Selezionare **Indirizzo IP singolo** e immettere l'indirizzo IP.
   - Selezionare **Intervallo di indirizzi IP** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**.
6. Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.
7. Se lo si desidera, digitare una descrizione della regola.
8. Fare clic su **OK**.
9. Nella finestra di dialogo **IP affidabili ed esclusi**, fare clic su **Sì** per confermare.

Come modificare una connessione a computer escluso

È possibile modificare una connessione a computer escluso con i relativi indirizzi IP.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
4. Nel riquadro IP affidabili ed esclusi selezionare **Indirizzi IP esclusi**, quindi fare clic su **Modifica**.
5. In **Modifica indirizzo IP escluso**, effettuare una delle seguenti operazioni:
   - Selezionare **Indirizzo IP singolo** e immettere l'indirizzo IP.
   - Selezionare **Intervallo di indirizzi IP** e immettere gli indirizzi IP iniziale e finale nelle caselle **Da indirizzo IP** e **A indirizzo IP**.
6. Facoltativamente, selezionare **La regola scade tra** e immettere il numero di giorni in cui applicare la regola.
7. Se lo si desidera, digitare una descrizione della regola.
8. Fare clic su **OK**.

Come rimuovere una connessione a computer escluso

È possibile rimuovere una connessione a computer escluso con i relativi indirizzi IP.

1. Nel riquadro McAfee SecurityCenter fare clic su **Internet e rete**, quindi su **Configura**.
2. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
3. Nel riquadro Firewall, fare clic su **IP affidabili ed esclusi**.
4. Nel riquadro IP affidabili ed esclusi, selezionare **Indirizzi IP esclusi**.
5. Selezionare un indirizzo IP, quindi fare clic su **Rimuovi**.
6. Nella finestra di dialogo **IP affidabili ed esclusi**, fare clic su **Sì** per confermare.

Come escludere un computer dal registro Eventi in ingresso

È possibile escludere una connessione a computer con il relativo indirizzo IP dal registro Eventi in ingresso.

Poiché gli indirizzi IP visualizzati nel registro Eventi in ingresso sono bloccati, l'esclusione di un indirizzo non aggiunge nessuna ulteriore protezione a meno che il computer non utilizzi delle porte deliberatamente aperte o non includa un programma a cui è stato consentito l'accesso a Internet.

Aggiungere un indirizzo IP all'elenco **Indirizzi IP esclusi** solo se si dispone di una o più porte deliberatamente aperte e se si ha motivo di credere che sia necessario bloccare l'accesso di tale indirizzo alle porte aperte..

È possibile utilizzare la pagina Eventi in ingresso, che elenca gli indirizzi IP del traffico Internet in ingresso, per escludere un indirizzo IP che sembra essere l'origine di attività Internet sospette o indesiderate.

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.
5. Selezionare un indirizzo IP di origine quindi, nella sezione **Desidero**, fare clic su **Escludi questo indirizzo**.
6. Nella finestra di dialogo **Aggiungi regola indirizzi IP esclusi**, fare clic su **Sì** per confermare.

Come escludere un computer dal registro Eventi Sistema rilevamento intrusioni

È possibile escludere una connessione a computer e il relativo indirizzo IP dal registro Eventi Sistema rilevamento intrusioni.

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Fare clic su **Rapporti e registri**.
3. In **Eventi recenti**, fare clic su **Visualizza registro**.
4. Fare clic su **Internet e rete**, quindi su **Eventi Sistema rilevamento intrusioni**.
5. Selezionare un indirizzo IP di origine quindi, nella sezione **Desidero**, fare clic su **Escludi questo indirizzo**.
6. Nella finestra di dialogo **Aggiungi regola indirizzi IP esclusi**, fare clic su **Sì** per confermare.

CAPITOLO 21

Registrazione, monitoraggio e analisi

Il firewall fornisce registrazione, monitoraggio e analisi estesi e di facile lettura relativi a eventi e traffico Internet. La comprensione di tali argomenti agevola la gestione delle connessioni Internet.

In questo capitolo

Registrazione eventi

Il firewall consente di attivare o disattivare la registrazione e, nel primo caso, specificare i tipi di eventi da registrare. Grazie alla registrazione degli eventi è possibile visualizzare gli eventi recenti in ingresso, in uscita e gli eventi di intrusione.

Come configurare le impostazioni del registro eventi

È possibile specificare e configurare i tipi di eventi del firewall da registrare. Per impostazione predefinita la registrazione degli eventi è attivata per tutti gli eventi e le attività.

1. Nel riquadro Configurazione di Internet e rete, in **Protezione firewall abilitata**, fare clic su **Avanzate**.
2. Nel riquadro Firewall, fare clic su **Impostazioni registro eventi**.
3. Se non è già selezionato, selezionare **Attiva registrazione eventi**.
4. In **Attiva registrazione eventi**, selezionare o deselezionare i tipi di eventi che si desidera o non si desidera registrare. Tra i tipi di eventi sono inclusi:
   - Programmi bloccati
   - Ping ICMP
   - Traffico da indirizzi IP esclusi
   - Eventi su porte dei servizi di sistema
   - Eventi su porte sconosciute
   - Eventi del Sistema di rilevamento intrusioni (IDS, Intrusion Detection System)
5. Per impedire la registrazione su determinate porte, selezionare **Non registrare gli eventi sulle porte seguenti**, quindi immettere i singoli numeri di porta separati da virgole o intervalli separati da trattini, ad esempio: `137-139, 445, 400-5000`.
6. Fare clic su **OK**.

Come visualizzare gli eventi recenti

Quando l'accesso è attivato, è possibile visualizzare gli eventi recenti. Nel riquadro Eventi recenti sono visualizzate la data e la descrizione dell'evento. Viene visualizzata l'attività dei programmi per i quali è stato esplicitamente bloccato l'accesso a Internet.

- Nel riquadro Attività comuni del **Menu avanzato**, fare clic su **Rapporti e registri** o su **Visualizza eventi recenti**. In alternativa, fare clic su **Visualizza eventi recenti** nel riquadro Attività comuni dal menu standard.

Come visualizzare gli eventi in ingresso

Quando l'accesso è attivato, è possibile visualizzare gli eventi in ingresso. Gli eventi in ingresso comprendono la data e l'ora, l'indirizzo IP, il nome host nonché il tipo di evento e di informazioni.

1. Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.

Nota: un indirizzo IP può essere impostato come affidabile, escluso e rintracciato dal registro Eventi in ingresso.

Come visualizzare gli eventi in uscita

Quando l'accesso è attivato, è possibile visualizzare gli eventi in uscita. Gli eventi in uscita includono il nome del programma che tenta l'accesso in uscita, la data e l'ora dell'evento e il percorso del programma sul computer.

1. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Internet e rete**, quindi su **Eventi in uscita**.

Nota: è possibile consentire l'accesso completo e solo in uscita a un programma dal registro Eventi in uscita, nonché individuare ulteriori informazioni relative al programma.

Come visualizzare gli eventi di rilevamento intrusioni

Quando l'accesso è attivato, è possibile visualizzare gli eventi di intrusione in ingresso. Gli eventi di rilevamento intrusioni visualizzano la data e l'ora, l'IP di origine, il nome host dell'evento e il tipo di evento.

1. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Internet e rete**, quindi su **Eventi Sistema rilevamento intrusioni**.

Nota: un indirizzo IP può essere escluso e rintracciato dal registro Eventi Sistema rilevamento intrusioni.

Utilizzo delle statistiche

Il firewall sfrutta il sito Web della protezione HackerWatch di McAfee per fornire statistiche sugli eventi di protezione e l'attività delle porte Internet globali.

Come visualizzare le statistiche globali sugli eventi di protezione

HackerWatch tiene traccia degli eventi di protezione Internet a livello mondiale, visualizzabili da SecurityCenter. Le informazioni registrate elencano gli incidenti segnalati a HackerWatch nel corso delle ultime 24 ore, degli ultimi 7 giorni e degli ultimi 30 giorni.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **HackerWatch**.
3. In Traccia degli eventi, visualizzare le statistiche sugli eventi di protezione.

Come visualizzare l'attività globale delle porte Internet

HackerWatch tiene traccia degli eventi di protezione Internet a livello mondiale, visualizzabili da SecurityCenter. Le informazioni visualizzate includono gli eventi principali relativi alle porte segnalati in HackerWatch durante gli ultimi sette giorni. In genere vengono visualizzate le informazioni sulle porte HTTP, TCP e UDP.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **HackerWatch**.
3. Visualizzare gli eventi principali relativi alle porte in **Attività recente sulle porte**.

Rintracciamento del traffico Internet

Il firewall prevede alcune opzioni per rintracciare il traffico Internet, che consentono di rintracciare geograficamente un computer di rete, ottenere informazioni relative a dominio e rete e rintracciare i computer dai registri Eventi in ingresso ed Eventi Sistema di rilevamento intrusioni.

Come rintracciare geograficamente un computer di rete

È possibile utilizzare il tracciato visivo per individuare geograficamente un computer che è connesso o tenta di connettersi al computer in uso, tramite il nome o l'indirizzo IP, nonché per accedere alle informazioni sulla rete e ai dati per la registrazione. L'esecuzione del tracciato visivo consente di visualizzare il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer e fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione mappa**.

Nota: non è possibile registrare eventi da indirizzi IP di loopback, privati o non validi.

Come ottenere i dati per la registrazione del computer

È possibile ottenere i dati per la registrazione di un computer da SecurityCenter tramite Tracciato visivo. Le informazioni includono il nome del dominio, il nome e l'indirizzo dell'intestatario e il contatto amministrativo.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer, quindi fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione intestatario dominio**.

Come ottenere informazioni sulla rete del computer

È possibile ottenere informazioni sulla rete di un computer da SecurityCenter tramite Tracciato visivo. Tali informazioni includono dettagli sulla rete in cui risiede il dominio in questione.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Tracciato visivo**.
3. Digitare l'indirizzo IP del computer, quindi fare clic su **Rintraccia**.
4. In **Tracciato visivo**, selezionare **Visualizzazione rete**.

Come rintracciare un computer dal registro Eventi in ingresso

Dal riquadro Eventi in ingresso, è possibile rintracciare un indirizzo IP visualizzato nel registro Eventi in ingresso.

1. Assicurarsi che il menu avanzato sia attivato. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Internet e rete**, quindi su **Eventi in ingresso**.
4. Nel riquadro Eventi in ingresso, selezionare un indirizzo IP di origine, quindi fare clic su **Rintraccia questo indirizzo**.
5. Nel riquadro Tracciato visivo, fare clic su una delle seguenti opzioni:
   - **Visualizzazione mappa**: consente di individuare geograficamente un computer mediante l'indirizzo IP selezionato.
   - **Visualizzazione intestatario dominio**: consente di individuare le informazioni sul dominio mediante l'indirizzo IP selezionato.
   - **Visualizzazione rete**: consente di individuare le informazioni sulla rete mediante l'indirizzo IP selezionato.
6. Fare clic su **Fine**.

Come rintracciare un computer dal registro Eventi Sistema rilevamento intrusioni

Dal riquadro Eventi Sistema rilevamento intrusioni, è possibile rintracciare un indirizzo IP visualizzato nell'omonimo registro.

1. Nel riquadro Attività comuni, fare clic su **Rapporti e registri**.
2. In **Eventi recenti**, fare clic su **Visualizza registro**.
3. Fare clic su **Internet e rete**, quindi su **Eventi Sistema rilevamento intrusioni**. Nel riquadro Eventi Sistema rilevamento intrusioni, selezionare un indirizzo IP di origine, quindi fare clic su **Rintraccia questo indirizzo**.
4. Nel riquadro Tracciato visivo, fare clic su una delle seguenti opzioni:
   - **Visualizzazione mappa**: consente di individuare geograficamente un computer mediante l'indirizzo IP selezionato.
   - **Visualizzazione intestatario dominio**: consente di individuare le informazioni sul dominio mediante l'indirizzo IP selezionato.
   - **Visualizzazione rete**: consente di individuare le informazioni sulla rete mediante l'indirizzo IP selezionato.
5. Fare clic su **Fine**.

Come rintracciare un indirizzo IP monitorato

È possibile rintracciare un indirizzo IP monitorato per ottenere una visualizzazione geografica indicante il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione. Sono inoltre reperibili i dati per la registrazione e le informazioni sulla rete relative all'indirizzo IP.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Programmi attivi**.
4. Selezionare un programma e l'indirizzo IP visualizzato sotto il nome del programma.
5. In **Attività programmi**, fare clic su **Rintraccia questo indirizzo IP**.
6. Nella sezione **Tracciato visivo** è possibile visualizzare una mappa che indica il percorso più probabile utilizzato per il trasferimento dei dati dal computer di origine a quello di destinazione. Sono inoltre reperibili i dati per la registrazione e le informazioni sulla rete relative all'indirizzo IP.

Nota: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Tracciato visivo**.

Monitoraggio del traffico Internet

Personal Firewall prevede alcuni metodi di monitoraggio del traffico Internet, tra cui:

- **Grafico analisi traffico**: visualizza il traffico Internet recente in entrata e in uscita.
- **Grafico utilizzo traffico**: visualizza la percentuale di larghezza di banda utilizzata dalle applicazioni maggiormente attive durante le ultime 24 ore.
- **Programmi attivi**: visualizza i programmi attualmente utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

Informazioni sul grafico analisi traffico

Il grafico Analisi traffico è una rappresentazione numerica e grafica del traffico Internet, sia in ingresso che in uscita. Inoltre, la funzione Controllo traffico visualizza i programmi attualmente utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

Dal riquadro Analisi traffico è possibile visualizzare il traffico Internet, in ingresso e in uscita, con velocità di trasferimento corrente, media e massima. È inoltre possibile visualizzare il volume del traffico, compresi la quantità di traffico dall'avvio del firewall e il traffico complessivo relativo al mese in corso e ai precedenti.

Il riquadro Analisi traffico mostra l'attività Internet in tempo reale nel computer in uso, inclusi il volume e la velocità di traffico Internet recente, in ingresso e in uscita, la velocità di connessione e i byte totali trasferiti attraverso Internet.

La linea verde continua rappresenta la velocità di trasferimento corrente del traffico in ingresso. La linea verde tratteggiata rappresenta la velocità di trasferimento media del traffico in ingresso. Se la velocità di trasferimento corrente e la velocità di trasferimento media sono identiche, la linea tratteggiata non viene visualizzata sul grafico e la linea continua rappresenta entrambe le velocità.

La linea rossa continua rappresenta la velocità di trasferimento corrente del traffico in uscita. La linea rossa tratteggiata rappresenta la velocità di trasferimento media del traffico in uscita. Se la velocità di trasferimento corrente e la velocità di trasferimento media sono identiche, la linea tratteggiata non viene visualizzata sul grafico e la linea continua rappresenta entrambe le velocità.

Come analizzare il traffico in ingresso e in uscita

Il grafico Analisi traffico è una rappresentazione numerica e grafica del traffico Internet, sia in ingresso che in uscita. Inoltre, la funzione Controllo traffico visualizza i programmi attualmente utilizzati dalla maggior parte delle connessioni di rete sul computer e gli indirizzi IP per l'accesso dei programmi.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Analisi traffico**.

Suggerimento: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Analisi traffico**.

Come monitorare la larghezza di banda dei programmi

È possibile visualizzare il grafico a torta che mostra la percentuale approssimativa di larghezza di banda utilizzata dai programmi più attivi presenti nel computer durante le ultime ventiquattro ore. Il grafico a torta fornisce la rappresentazione visiva delle quantità di larghezza di banda relative utilizzate dai programmi.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Utilizzo traffico**.

Suggerimento: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Utilizzo traffico**.

Come monitorare l'attività dei programmi

È possibile visualizzare l'attività dei programmi in ingresso e in uscita in cui vengono mostrate le connessioni e le porte del computer remoto.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **Controllo traffico**.
3. In **Controllo traffico**, fare clic su **Programmi attivi**.
4. È possibile visualizzare le seguenti informazioni:
   - Grafico attività programmi: selezionare un programma per visualizzare il grafico della relativa attività.
   - Connessione in ascolto: selezionare un elemento in ascolto sotto il nome del programma.
   - Connessione al computer: selezionare un indirizzo IP sotto il nome del programma, il processo di sistema o il servizio.

Nota: per visualizzare le statistiche più aggiornate, fare clic su **Aggiorna** in **Programmi attivi**.

CAPITOLO 22

Informazioni sulla protezione Internet

Il firewall utilizza il sito Web della protezione di McAfee, HackerWatch, per fornire informazioni aggiornate sui programmi e sull'attività Internet globale. HackerWatch prevede inoltre un'esercitazione HTML relativa al firewall.

In questo capitolo

Come avviare l'esercitazione HackerWatch

Per ottenere ulteriori informazioni sul firewall, è possibile accedere all'esercitazione HackerWatch da SecurityCenter.

1. Accertarsi che sia attivato il menu avanzato e fare clic su **Strumenti**.
2. Nel riquadro Strumenti, fare clic su **HackerWatch**.
3. In **Risorse di HackerWatch**, fare clic su **Visualizza esercitazione**.

CAPITOLO 23

McAfee QuickClean

QuickClean migliora le prestazioni del computer eliminando i file superflui. Vuota il Cestino ed elimina i file temporanei, i collegamenti, i frammenti di file perduti, i file di registro, i file memorizzati nella cache, i file della cronologia del browser, la posta elettronica inviata ed eliminata, i file usati di recente, i file Active-X e i file di punto di ripristino del sistema. QuickClean protegge inoltre la privacy utilizzando il componente McAfee Shredder per eliminare in maniera sicura e definitiva gli elementi che potrebbero contenere informazioni personali sensibili, quali il nome e l'indirizzo. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

L'utilità di Deframmentazione dischi dispone i file e le cartelle nel computer in modo da assicurare che non siano sparsi, ovvero frammentati, quando vengono salvati nel disco rigido del computer. La deframmentazione periodica del disco rigido assicura che i file e le cartelle frammentate vengano consolidate per recuperarle rapidamente in un momento successivo.

Se non si desidera eseguire manualmente la manutenzione del computer è possibile pianificare l'esecuzione automatica di QuickClean e Deframmentazione dischi, come attività indipendenti, con la frequenza desiderata.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di QuickClean

QuickClean offre varie operazioni di pulitura per eliminare i file non necessari in maniera sicura ed efficiente. L'eliminazione di tali file consente di aumentare lo spazio sul disco rigido del computer e migliorarne le prestazioni.

Pulitura del computer

QuickClean elimina i file superflui dal computer. Vuota il Cestino ed elimina i file temporanei, i collegamenti, i frammenti di file perduti, i file di registro, i file memorizzati nella cache, i file della cronologia del browser, la posta elettronica inviata ed eliminata, i file usati di recente, i file Active-X e i file di punto di ripristino del sistema. QuickClean elimina questi elementi senza conseguenze sulle altre informazioni essenziali.

È possibile utilizzare le operazioni di pulitura di QuickClean per eliminare i file non necessari dal computer. La tabella seguente illustra le operazioni di pulitura di QuickClean.

Nome	Funzione
Pulitura del Cestino	Elimina i file del Cestino.
Pulitura dei file temporanei	elimina i file memorizzati in cartelle temporanee.
Pulizia dei collegamenti	Elimina i collegamenti interrotti e i collegamenti a cui non è associato un programma.
Pulitura dei frammenti di file persi	Elimina i frammenti di file persi nel computer.
Pulizia del registro di sistema	Elimina le informazioni del registro di sistema di Windows ® relative ai programmi che non sono più installati nel computer. Il registro è un database in cui Windows memorizza le informazioni di configurazione. Contiene i profili relativi a ciascun utente del computer nonché le informazioni relative all'hardware del sistema, i programmi installati e le impostazioni delle proprietà. Windows utilizza di continuo tali informazioni durante il funzionamento.
Pulitura della cache	Elimina i file memorizzati nella cache accumulati durante la navigazione sul Web. Tali file sono solitamente memorizzati come file temporanei in una cartella cache. Una cartella cache è un'area di memorizzazione temporanea nel computer. Per aumentare la velocità e l'efficienza della navigazione sul Web, la volta successiva che si desidera visualizzare una pagina, il browser può recuperarla dalla cache invece che dal server remoto.

Pulitura dei cookie	elimina i cookie. Tali file sono solitamente memorizzati come file temporanei. Un cookie è un piccolo file, che contiene informazioni che di solito comprendono il nome utente e l'ora e la data correnti, memorizzato nel computer dell'utente che naviga sul Web. I cookie vengono utilizzati principalmente dai siti Web per identificare gli utenti che si sono registrati o che hanno visitato il loro sito; tuttavia, possono anche essere una fonte di informazioni per gli hacker.
Pulitura della cronologia del browser	Elimina la cronologia del browser Web.
Pulitura posta elettronica per Outlook Express e Outlook (posta inviata ed eliminata)	Elimina la posta elettronica inviata ed eliminata da Outlook® e Outlook Express.
Pulitura dei file utilizzati di recente	Elimina i file utilizzati di recente creati con uno dei programmi seguenti: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Cronologia di Windows ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
Pulitura di ActiveX	Elimina i controlli ActiveX. ActiveX è un componente software utilizzato dai programmi o dalle pagine Web per aggiungere funzionalità che si integrano e appaiono come parte normale del programma o della pagina Web. La maggior parte dei controlli ActiveX sono innocui; tuttavia, alcuni potrebbero acquisire informazioni dal computer.
Pulitura dei punti di ripristino configurazione di sistema	Elimina dal computer i vecchi punti di ripristino configurazione di sistema (ad eccezione dei più recenti). I punti di ripristino configurazione di sistema vengono creati da Windows per contrassegnare le modifiche apportate al computer, in modo che sia possibile tornare a uno stato precedente qualora si verificassero dei problemi.

Pulitura del computer

È possibile utilizzare le operazioni di pulitura di QuickClean per eliminare i file non necessari dal computer. Al termine, in **Riepilogo di QuickClean**, sarà possibile visualizzare la quantità di spazio su disco recuperata dopo la pulitura, il numero di file eliminati nonché la data e l'ora di esecuzione dell'ultima operazione di QuickClean nel computer.

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **McAfee QuickClean**, fare clic su **Avvia**.
3. Eseguire una delle seguenti operazioni:
   - Scegliere **Avanti** per accettare le operazioni di pulitura predefinite visualizzate nell'elenco.
   - Selezionare o deselezionare le operazioni di pulitura appropriate, quindi fare clic su **Avanti**. Se si seleziona la pulitura dei file utilizzati di recente, è possibile scegliere **Proprietà** per selezionare o deselezionare i file che sono stati creati di recente con i programmi nell'elenco, quindi fare clic su **OK**.
   - Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi scegliere **Avanti**.
4. Al termine dell'analisi, fare clic su **Avanti**.
5. Fare clic su **Avanti** per confermare l'eliminazione dei file.
6. Eseguire una delle seguenti operazioni:
   - Fare clic su **Avanti** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
   - Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder**, specificare il numero di tentativi, fino a un massimo di 10, quindi fare clic su **Avanti**. L'eliminazione definitiva dei file può richiedere molto tempo se le informazioni da cancellare sono molte.

7 Se durante la pulitura sono presenti file o elementi bloccati, è possibile che venga richiesto di riavviare il computer. Fare clic su **OK** per chiudere la richiesta.

8 Fare clic su **Fine**.

Nota: non è possibile recuperare i file eliminati con Shredder. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

Deframmentazione del computer

L'utilità di Deframmentazione dischi dispone i file e le cartelle nel computer in modo che non siano sparsi, ovvero frammentati, quando vengono salvati nel disco rigido del computer. La deframmentazione periodica del disco rigido assicura che i file e le cartelle frammentate vengano consolidate per recuperarle rapidamente in un momento successivo.

Deframmentare il computer

È possibile deframmentare il computer per migliorare l'accesso a file e cartelle e il loro recupero.

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Deframmentazione dischi**, fare clic su **Analizza**.
3. Seguire le istruzioni riportate sullo schermo.

Nota: per ulteriori informazioni su Deframmentazione dischi, vedere la Guida di Windows.

Pianificazione di un'attività

L'utilità di Pianificazione attività automatizza la frequenza con cui QuickClean o Deframmentazione dischi sono eseguiti nel computer. Ad esempio, è possibile pianificare un'attività di QuickClean per vuotare il Cestino ogni domenica alle 21:00, oppure un'attività di Deframmentazione dischi per deframmentare il disco rigido del computer l'ultimo giorno di ogni mese. È possibile creare, modificare o eliminare un'attività in qualsiasi momento. Perché l'attività pianificata venga eseguita, è necessario aver effettuato l'accesso al computer. Se per qualche motivo l'attività non viene eseguita, questa verrà ripianificata cinque minuti dopo l'accesso successivo.

Pianificare un'attività di QuickClean

È possibile pianificare un'attività di QuickClean per pulire automaticamente il computer utilizzando una o più operazioni di pulitura. Al termine, nella sezione **Riepilogo di QuickClean** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1. Aprire il riquadro Pianificazione attività.

   In che modo?

   1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
   2. In **Pianificazione attività**, fare clic su **Avvia**.

2. Nell'elenco **Selezionare operazione da pianificare**, fare clic su **McAfee QuickClean**.
3. Immettere un nome per l'attività nella casella **Nome attività**, quindi fare clic su **Crea**.
4. Eseguire una delle seguenti operazioni:
   - Scegliere **Avanti** per accettare le operazioni di pulitura visualizzate nell'elenco.
   - Selezionare o deselezionare le operazioni di pulitura appropriate, quindi fare clic su **Avanti**. Se si seleziona la pulitura dei file utilizzati di recente, è possibile scegliere **Proprietà** per selezionare o deselezionare i file che sono stati creati di recente con i programmi nell'elenco, quindi fare clic su **OK**.
   - Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi scegliere **Avanti**.

5 Eseguire una delle seguenti operazioni:
   - Fare clic su **Pianifica** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
   - Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder**, specificare il numero di tentativi, fino a un massimo di 10, quindi scegliere **Pianifica**.
6 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.
7 Se sono state apportate modifiche alle proprietà della pulitura dei file utilizzati di recente, è possibile che venga richiesto di riavviare il computer. Fare clic su **OK** per chiudere la richiesta.
8 Fare clic su **Fine**.

Nota: non è possibile recuperare i file eliminati con Shredder. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

Modificare un'attività di QuickClean

È possibile modificare un'attività pianificata di QuickClean per modificare le attività di pulitura utilizzate o la frequenza con cui un'attività viene eseguita automaticamente nel computer. Al termine, nella sezione **Riepilogo di QuickClean** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1 Aprire il riquadro Pianificazione attività.

   In che modo?

   1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
   2. In **Pianificazione attività**, fare clic su **Avvia**.
2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **McAfee QuickClean**.
3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**, quindi fare clic su **Modifica**.
4 Eseguire una delle seguenti operazioni:
   - Fare clic su **Avanti** per accettare le operazioni di pulitura selezionate per l'attività.
   - Selezionare o deselezionare le operazioni di pulitura appropriate, quindi fare clic su **Avanti**. Se si seleziona la pulitura dei file utilizzati di recente, è possibile scegliere **Proprietà** per selezionare o deselezionare i file che sono stati creati di recente con i programmi nell'elenco, quindi fare clic su **OK**.

- Fare clic su **Ripristina impostazioni predefinite** per ripristinare le operazioni di pulitura predefinite, quindi scegliere **Avanti**.

5 Eseguire una delle seguenti operazioni:

- Fare clic su **Pianifica** per accettare l'opzione predefinita **Eliminare i file usando l'eliminazione standard di Windows**.
- Fare clic su **Eliminare i file in modalità protetta utilizzando Shredder**, specificare il numero di tentativi, fino a un massimo di 10, quindi scegliere **Pianifica**.

6 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.

7 Se sono state apportate modifiche alle proprietà della pulitura dei file utilizzati di recente, è possibile che venga richiesto di riavviare il computer. Fare clic su **OK** per chiudere la richiesta.

8 Fare clic su **Fine**.

Nota: non è possibile recuperare i file eliminati con Shredder. Per informazioni sull'eliminazione definitiva dei file, vedere McAfee Shredder.

Eliminare un'attività di QuickClean

È possibile eliminare un'attività QuickClean pianificata se non si desidera più che sia eseguita automaticamente.

1 Aprire il riquadro Pianificazione attività.

In che modo?

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **McAfee QuickClean**.

3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**.

4 Fare clic su **Elimina**, quindi scegliere **Sì** per confermare l'eliminazione.

5 Fare clic su **Fine**.

Pianificare un'attività di deframmentazione dischi

È possibile pianificare un'attività di deframmentazione dischi per pianificare la frequenza con cui il disco rigido del computer viene deframmentato automaticamente. Al termine, nella sezione **Deframmentazione dischi** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1 Aprire il riquadro Pianificazione attività.

   In che modo?

   1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
   2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **Deframmentazione dischi**.

3 Immettere un nome per l'attività nella casella **Nome attività**, quindi fare clic su **Crea**.

4 Eseguire una delle seguenti operazioni:

   - Fare clic su **Pianifica** per accettare l'opzione predefinita **Esegui deframmentazione anche se lo spazio disco è insufficiente**.
   - Deselezionare l'opzione **Esegui deframmentazione anche se lo spazio disco è insufficiente**, quindi fare clic su **Pianifica**.

5 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.

6 Fare clic su **Fine**.

Modificare un'attività di deframmentazione dischi

È possibile modificare un'attività di deframmentazione dischi per cambiare la frequenza con cui viene eseguita automaticamente sul computer. Al termine, nella sezione **Deframmentazione dischi** è possibile visualizzare la data e l'ora della pianificazione per la successiva esecuzione dell'attività.

1 Aprire il riquadro Pianificazione attività.

   In che modo?

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **Deframmentazione dischi**.

3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**, quindi fare clic su **Modifica**.

4 Eseguire una delle seguenti operazioni:

- Fare clic su **Pianifica** per accettare l'opzione predefinita **Esegui deframmentazione anche se lo spazio disco è insufficiente**.
- Deselezionare l'opzione **Esegui deframmentazione anche se lo spazio disco è insufficiente**, quindi fare clic su **Pianifica**.

5 Nella finestra di dialogo **Pianifica**, selezionare la frequenza con cui si desidera eseguire l'attività, quindi fare clic su **OK**.

6 Fare clic su **Fine**.

Eliminare un'attività di deframmentazione dischi

È possibile eliminare un'attività di deframmentazione dischi se non si desidera più che sia eseguita automaticamente.

1 Aprire il riquadro Pianificazione attività.

In che modo?

1. Nella sezione **Attività comuni** della finestra di dialogo McAfee SecurityCenter, fare clic su **Manutenzione computer**.
2. In **Pianificazione attività**, fare clic su **Avvia**.

2 Nell'elenco **Selezionare operazione da pianificare**, fare clic su **Deframmentazione dischi**.

3 Selezionare l'attività dall'elenco **Selezionare un'attività esistente**.

4 Fare clic su **Elimina**, quindi scegliere **Sì** per confermare l'eliminazione.

5 Fare clic su **Fine**.

CAPITOLO 24

McAfee Shredder

McAfee Shredder cancella gli elementi, ovvero li elimina definitivamente dal disco rigido del computer. Esistono appositi strumenti informatici che consentono di recuperare le informazioni anche dopo che i file e le cartelle sono stati eliminati manualmente, il Cestino è stato svuotato oppure è stata eliminata la cartella dei file temporanei di Internet. Inoltre, è possibile recuperare un file eliminato in virtù del fatto che alcuni programmi eseguono copie temporanee e nascoste dei file aperti. Shredder protegge la privacy dell'utente eliminando in modo sicuro e definitivo i file indesiderati. È importante ricordare che i file eliminati non possono essere ripristinati.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Shredder

Shredder elimina gli elementi dal disco rigido in modo da rendere impossibile il recupero delle informazioni ad essi associate. Protegge la privacy dell'utente eliminando in maniera sicura e definitiva i file, le cartelle, gli elementi del Cestino e della cartella dei file temporanei Internet, nonché l'intero contenuto dei dischi del computer, quali CD riscrivibili, dischi rigidi esterni e floppy.

Eliminazione definitiva di file, cartelle e dischi

Shredder rende impossibile il recupero delle informazioni contenute nei file e nelle cartelle eliminate dal Cestino e dalla cartella dei file temporanei Internet, nemmeno con l'ausilio di strumenti specifici. Con Shredder è possibile specificare quante volte (fino a dieci) si desidera eliminare definitivamente un elemento. Un numero più elevato di tentativi di eliminazione definitiva rende più sicura l'eliminazione dei file.

Eliminare definitivamente file e cartelle

È possibile eliminare definitivamente file e cartelle dal disco rigido del computer, compresi gli elementi del Cestino e della cartella dei file temporanei Internet.

1 Aprire **Shredder**.

In che modo?

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Nel riquadro di sinistra, fare clic su **Strumenti**.
3. Fare clic su **Shredder**.

2 Nel riquadro Elimina definitivamente file e cartelle, fare clic su **Cancellare file e cartelle** nella sezione **Desidero**.

3 Nella sezione **Livello di eliminazione**, fare clic su uno dei seguenti livelli di eliminazione:

- **Rapido**: elimina definitivamente con un passaggio gli elementi selezionati.
- **Completo**: elimina definitivamente con sette passaggi gli elementi selezionati.
- **Personalizzato**: elimina definitivamente con dieci passaggi gli elementi selezionati.

4 Fare clic su **Avanti**.

5 Eseguire una delle seguenti operazioni:

- Nell'elenco **Selezionare i file da distruggere**, fare clic su **Contenuto del Cestino** o **File temporanei Internet**.
- Fare clic su **Sfoglia**, cercare i file da eliminare definitivamente, selezionarli, quindi fare clic su **Apri**.

6 Fare clic su **Avanti**.

7 Fare clic su **Avvia**.

8 Al termine dell'operazione di eliminazione definitiva, fare clic su **Fine**.

Nota: non utilizzare alcun file fino al termine dell'operazione.

Eliminare definitivamente un intero disco

È possibile eliminare definitivamente e in modo rapido l'intero contenuto di un disco. È possibile eliminare definitivamente solo il contenuto di unità rimovibili, quali dischi rigidi esterni, CD riscrivibili e floppy.

1 Aprire **Shredder**.

In che modo?

1. Nella sezione **Attività comuni** del riquadro McAfee SecurityCenter, fare clic su **Menu avanzato**.
2. Nel riquadro di sinistra, fare clic su **Strumenti**.
3. Fare clic su **Shredder**.

2 Nella sezione **Desidero** del riquadro Elimina definitivamente file e cartelle, fare clic su **Cancellare un intero disco**.

3 Nella sezione **Livello di eliminazione**, fare clic su uno dei seguenti livelli di eliminazione:

- **Rapido**: elimina definitivamente con un solo passaggio l'unità selezionata.
- **Completo**: elimina definitivamente con sette passaggi l'unità selezionata.
- **Personalizzato**: elimina definitivamente con dieci passaggi l'unità selezionata.

4 Fare clic su **Avanti**.

5 Nell'elenco **Selezionare il disco**, fare clic sull'unità che si desidera eliminare definitivamente.

6 Fare clic su **Avanti**, quindi su **Sì** per confermare.

7 Fare clic su **Avvia**.

8 Al termine dell'operazione di eliminazione definitiva, fare clic su **Fine**.

Nota: non utilizzare alcun file fino al termine dell'operazione.

CAPITOLO 25

McAfee Network Manager

Network Manager rappresenta graficamente i computer e i componenti che costituiscono la rete domestica. Consente di eseguire il monitoraggio remoto dello stato di protezione di tutti i computer gestiti in rete e quindi di risolvere le vulnerabilità della protezione segnalate sugli stessi.

Prima di utilizzare Network Manager, è possibile acquisire dimestichezza con alcune delle sue funzioni. La guida di Network Manager contiene dettagli sulla configurazione e sull'utilizzo di tali funzioni.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di Network Manager

Network Manager offre le seguenti funzioni.

Mappa grafica della rete

La mappa della rete di Network Manager fornisce una panoramica grafica dello stato di protezione dei computer e dei componenti che costituiscono la rete domestica. Quando vengono apportate modifiche alla rete, ad esempio con l'aggiunta di un computer, la mappa della rete è in grado di riconoscerle. È possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere i componenti della mappa per personalizzare la visualizzazione. Possono inoltre essere visualizzati i dettagli di uno qualsiasi dei componenti sulla mappa della rete.

Gestione remota

Utilizzare la mappa della rete di Network Manager per gestire lo stato di protezione dei computer che costituiscono la rete domestica. È possibile invitare un computer a diventare membro della rete gestita, monitorare lo stato di protezione del computer gestito e risolvere le vulnerabilità conosciute della protezione da un computer remoto della rete.

Informazioni sulle icone di Network Manager

Nella seguente tabella sono descritte le icone di uso comune nella mappa della rete di Network Manager.

Icona	Descrizione
	Rappresenta un computer gestito in linea
	Rappresenta un computer gestito non in linea
	Rappresenta un computer non gestito in cui è installato SecurityCenter
	Rappresenta un computer non gestito e non in linea
	Rappresenta un computer in linea in cui non è installato SecurityCenter oppure un dispositivo di rete sconosciuto
	Rappresenta un computer non in linea in cui non è installato SecurityCenter oppure un dispositivo di rete sconosciuto non in linea
	Indica che l'elemento corrispondente è protetto e connesso
	Indica che l'elemento corrispondente potrebbe richiedere l'attenzione dell'utente
	Indica che l'elemento corrispondente richiede l'attenzione immediata dell'utente
	Rappresenta un router domestico senza fili
	Rappresenta un router domestico standard
	Rappresenta Internet, quando è stata effettuata la connessione
	Rappresenta Internet, quando non è stata effettuata la connessione

CAPITOLO 26

Impostazione di una rete gestita

Per impostare una rete gestita occorre organizzare gli elementi della mappa della rete e aggiungere membri (computer) alla rete. Affinché un computer possa essere gestito in modalità remota oppure sia autorizzato a gestire in modalità remota altri computer della rete, è necessario che diventi un membro affidabile della rete. I nuovi computer vengono aggiunti alla rete dai membri della rete (computer) esistenti, dotati di autorizzazioni amministrative.

È possibile visualizzare i dettagli associati a uno qualsiasi dei componenti visualizzati nella mappa della rete, anche dopo aver apportato modifiche alla rete, ad esempio con l'aggiunta di un computer.

In questo capitolo

Utilizzo della mappa della rete

Quando un computer si connette alla rete, Network Manager analizza lo stato della rete al fine di determinare se sono presenti eventuali membri gestiti o non gestiti, quali sono gli attributi del router e lo stato di Internet. Se non viene rilevato alcun membro, Network Manager presume che il computer attualmente connesso sia il primo della rete, rendendolo membro gestito con autorizzazioni amministrative. Per impostazione predefinita, il nome della rete include il gruppo di lavoro o nome di dominio del primo computer che si connette alla rete e su cui è installato SecurityCenter. Tuttavia, è possibile rinominare la rete in qualsiasi momento.

Quando si apportano modifiche alla propria rete, se ad esempio si aggiunge un computer, è possibile personalizzare la mappa della rete. Ad esempio, è possibile aggiornare la mappa della rete, rinominare la rete e mostrare o nascondere i componenti della mappa della rete per personalizzare la visualizzazione. Possono inoltre essere visualizzati i dettagli associati a uno qualsiasi dei componenti visualizzati sulla mappa della rete.

Come accedere alla mappa della rete

La mappa della rete rappresenta graficamente i computer e i componenti che costituiscono la rete domestica.

- Nel menu standard o avanzato, fare clic su **Gestione rete**.

Nota: al primo accesso alla mappa della rete, viene richiesto di impostare come affidabili gli altri computer della rete.

Come aggiornare la mappa della rete

È possibile aggiornare la mappa della rete in qualsiasi momento; ad esempio, dopo che un nuovo computer è diventato membro della rete gestita.

1. Nel menu standard o avanzato, fare clic su **Gestione rete**.
2. Fare clic su **Aggiornare la mappa della rete** nella sezione **Desidero**.

Nota: il collegamento **Aggiornare la mappa della rete** è disponibile solo se non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Come rinominare la rete

Per impostazione predefinita, il nome della rete include il gruppo di lavoro o nome di dominio del primo computer che si connette alla rete e su cui è installato SecurityCenter. Se si preferisce utilizzare un nome diverso, è possibile modificarlo.

1. Nel menu standard o avanzato, fare clic su **Gestione rete**.
2. Fare clic su **Rinominare la rete** nella sezione **Desidero**.
3. Digitare il nome della rete nella casella **Nome di rete**.
4. Fare clic su **OK**.

Nota: il collegamento **Rinominare la rete** è disponibile solo se non è stato selezionato alcun elemento nella mappa della rete. Per deselezionare un elemento, fare clic sull'elemento selezionato oppure in un'area vuota della mappa della rete.

Come visualizzare o nascondere un elemento nella mappa della rete

Per impostazione predefinita, nella mappa della rete sono visualizzati tutti i computer e i componenti della rete domestica. Tuttavia, se vi sono elementi nascosti, è possibile visualizzarli in qualsiasi momento. È possibile nascondere solo gli elementi non gestiti, ma non i computer gestiti.

Per...	Nel Menu standard o nel Menu avanzato, fare clic su **Gestione rete**, quindi eseguire una delle seguenti operazioni.
Nascondere un elemento nella mappa della rete	Fare clic su un elemento nella mappa della rete, quindi su **Nascondere l'elemento** nella sezione **Desidero**. Nella finestra di dialogo di conferma, fare clic su **Sì**.
Mostrare elementi nascosti nella mappa della rete	Nella sezione **Desidero**, fare clic su **Visualizzare gli elementi nascosti**.

Come visualizzare i dettagli di un elemento

Per visualizzare informazioni dettagliate su qualsiasi componente in rete, selezionarne uno nella mappa della rete. Tra le informazioni disponibili sono inclusi il nome del componente, il relativo stato di protezione nonché altri dettagli richiesti per la gestione del componente.

1. Fare clic sull'icona di un elemento nella mappa della rete.
2. Nella sezione **Dettagli** è possibile visualizzare le informazioni sull'elemento.

Aggiunta alla rete gestita

Affinché un computer sia gestito in modalità remota oppure ottenga l'autorizzazione per la gestione remota di altri computer in rete, è necessario che diventi membro affidabile della rete. I nuovi computer vengono aggiunti alla rete dai membri della rete (computer) esistenti, dotati di autorizzazioni amministrative. Per garantire che vengano aggiunti alla rete solo i computer affidabili, gli utenti dei computer che concedono l'autorizzazione e quelli che la ricevono devono autenticarsi reciprocamente.

Quando un computer viene aggiunto alla rete, viene richiesto di esporne lo stato di protezione McAfee agli altri computer in rete. Se un computer accetta di esporre il proprio stato di protezione, esso diventerà un membro gestito della rete. Se un computer rifiuta di esporre il proprio stato di protezione, esso diventerà un membro non gestito della rete. I membri non gestiti della rete sono di solito computer guest che desiderano accedere ad altre funzioni della rete (ad esempio, l'invio di file o la condivisione stampanti).

Nota: se sono stati installati altri programmi di rete McAfee (ad esempio, EasyNetwork), dopo l'aggiunta il computer verrà riconosciuto come computer gestito anche in tali programmi. Il livello di autorizzazione assegnato a un computer in Network Manager si applica a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Aggiunta a una rete gestita

Quando si riceve un invito a diventare membro di una rete gestita, è possibile accettarlo o rifiutarlo. È anche possibile determinare se si desidera che il computer in uso e altri computer in rete eseguano il monitoraggio reciproco delle rispettive impostazioni di protezione (ad esempio, se i servizi di protezione da virus di un computer sono aggiornati).

1. Nella finestra di dialogo Rete gestita, assicurarsi che la casella di controllo **Consenti a tutti i computer della rete di monitorare le impostazioni di protezione** sia selezionata.
2. Fare clic su **Aggiungi**.
   Quando si accetta l'invito vengono visualizzate due carte da gioco.
3. Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer che ha inviato l'invito a diventare membro della rete gestita.
4. Fare clic su **OK**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Annulla** nella finestra di dialogo Rete gestita.

Invio a un computer di un invito a diventare membro della rete gestita

Se un computer viene aggiunto alla rete gestita oppure un altro computer non gestito è presente in rete, è possibile invitare tale computer a diventare membro della rete gestita. Solo i computer con autorizzazioni amministrative in rete possono invitare altri computer a diventare membri. Quando si invia l'invito, occorre inoltre specificare il livello di autorizzazione che si desidera assegnare al computer aggiunto.

1. Fare clic sull'icona del computer non gestito nella mappa della rete.
2. Fare clic su **Monitorare il computer** nella sezione **Desidero**.
3. Nella finestra di dialogo Invita un computer a diventare membro della rete gestita, effettuare una delle seguenti operazioni:
   - Fare clic su **Consenti accesso Guest a programmi della rete gestita** per consentire l'accesso al computer di accedere alla rete (è possibile utilizzare questa opzione per gli utenti temporanei della rete domestica).
   - Fare clic su **Consenti accesso completo a programmi della rete gestita** che consente al computer di accedere alla rete.

- Fare clic su **Consenti accesso con privilegi di amministratore a programmi della rete gestita** che consente al computer di accedere alla rete con autorizzazioni amministrative. Consente inoltre al computer di concedere l'accesso ad altri computer che desiderano diventare membri della rete gestita.

4 Fare clic su **OK**.
Al computer viene inviato un invito a diventare membro della rete gestita. Quando il computer accetta l'invito vengono visualizzate due carte da gioco.

5 Verificare che le carte da gioco siano uguali a quelle visualizzate sul computer invitato a diventare membro della rete gestita.

6 Fare clic su **Consenti accesso**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Consentire al computer di diventare membro della rete può mettere a rischio altri computer; pertanto, fare clic su **Rifiuta accesso** nella finestra di dialogo di conferma.

Impostazione di computer in rete come non affidabili

Se per errore i computer sulla rete sono stati considerati affidabili, è possibile considerarli come non affidabili.

- Fare clic su **Non considerare affidabili i computer su questa rete** nella sezione **Desidero**.

Nota: il collegamento **Non considerare affidabili i computer su questa rete** non è disponibile se si dispone delle autorizzazioni amministrative e sono presenti altri computer gestiti in rete.

CAPITOLO 27

Gestione remota della rete

Dopo aver impostato la rete gestita, è possibile eseguire la gestione remota dei computer e dei componenti che costituiscono la rete. È possibile eseguire il monitoraggio dello stato e dei livelli di autorizzazione dei computer e dei componenti, nonché risolvere la maggior parte delle vulnerabilità della protezione in modalità remota.

In questo capitolo

Monitoraggio dello stato e delle autorizzazioni

Una rete gestita prevede membri gestiti e non gestiti. I membri gestiti, diversamente da quelli non gestiti, consentono agli altri computer in rete di monitorare lo stato delle protezione McAfee. I membri non gestiti sono di solito computer guest che desiderano accedere ad altre funzioni della rete (ad esempio, l'invio di file o la condivisione di stampanti). Un computer gestito in rete può invitare un computer non gestito a diventare un computer gestito in qualsiasi momento. In maniera simile, un computer gestito può diventare non gestito in qualsiasi momento.

Ai computer gestiti sono associate autorizzazioni amministrative, complete o Guest. Le autorizzazioni amministrative consentono al computer gestito di amministrare lo stato di protezione di tutti gli altri computer gestiti in rete, nonché di concedere agli altri computer di diventare membri della rete. Le autorizzazioni complete e Guest consentono a un computer solo di accedere alla rete. È possibile modificare il livello di autorizzazione di un computer in qualsiasi momento.

Poiché una rete gestita può comprendere anche dei dispositivi (ad esempio i router), è possibile gestire anche questi ultimi mediante Network Manager. È inoltre possibile configurare e modificare le proprietà di visualizzazione di un dispositivo sulla mappa della rete.

Monitoraggio dello stato della protezione di un computer

Se lo stato della protezione del computer non è monitorato sulla rete (il computer non è membro oppure è un membro non gestito), è possibile inviare una richiesta di monitoraggio.

1. Fare clic sull'icona del computer non gestito nella mappa della rete.
2. Fare clic su **Monitorare il computer** nella sezione **Desidero**.

Interruzione del monitoraggio dello stato della protezione di un computer

È possibile interrompere il monitoraggio dello stato della protezione di un computer gestito nella rete privata; tuttavia, il computer diventa un membro non gestito e non sarà possibile monitorarne lo stato di protezione in modalità remota.

1. Fare clic sull'icona del computer gestito nella mappa della rete.
2. Fare clic su **Interrompere il monitoraggio del computer** nella sezione **Desidero**.
3. Nella finestra di dialogo di conferma, fare clic su **Sì**.

Modifica delle autorizzazioni di un computer gestito

È possibile modificare le autorizzazioni di un computer gestito in qualsiasi momento. Ciò consente di modificare i computer che possono monitorare lo stato della protezione di altri computer della rete.

1. Fare clic sull'icona del computer gestito nella mappa della rete.
2. Fare clic su **Modificare i permessi per il computer** nella sezione **Desidero**.
3. Nella finestra di dialogo di modifica dei permessi, selezionare o deselezionare la casella di controllo per determinare se il computer selezionato e altri computer sulla rete gestita possono monitorare reciprocamente il rispettivo stato della protezione.
4. Fare clic su **OK**.

Gestione di una periferica

È possibile gestire una periferica eseguendo l'accesso alla relativa pagina Web di amministrazione da Network Manager.

1. Fare clic sull'icona di una periferica nella mappa della rete.
2. Fare clic su **Gestire la periferica** nella sezione **Desidero**. Il browser Web verrà aperto e verrà visualizzata la pagina Web di amministrazione della periferica.
3. Nel browser Web, fornire i dati di accesso e configurare le impostazioni di protezione della periferica.

Nota: se la periferica è un router o un punto di accesso senza fili protetto con Wireless Network Security, per configurare le impostazioni di protezione della periferica è necessario utilizzare Wireless Network Security.

Modifica delle proprietà di visualizzazione di una periferica

Quando si modificano le proprietà di visualizzazione di una periferica è possibile modificare il nome della periferica visualizzato e specificare se si tratta di un router senza fili.

1. Fare clic sull'icona di una periferica nella mappa della rete.
2. Fare clic su **Modificare le proprietà della periferica** nella sezione **Desidero**.
3. Per specificare il nome della periferica visualizzato, digitare un nome nella casella **Nome**.
4. Per specificare il tipo di periferica, fare clic su **Router** se si tratta di un router standard oppure **Router wireless** se si tratta di un router senza fili.
5. Fare clic su **OK**.

Risoluzione delle vulnerabilità della protezione

I computer gestiti con autorizzazioni amministrative possono monitorare lo stato della protezione McAfee di altri computer gestiti sulla rete e risolvere le vulnerabilità segnalate in modalità remota. Ad esempio, se lo stato della protezione McAfee di un computer gestito indica che VirusScan è disattivato, un altro computer gestito con autorizzazioni amministrative può attivare VirusScan in modalità remota.

Quando si risolvono le vulnerabilità della protezione in modalità remota, Network Manager è in grado di risolvere gran parte dei problemi segnalati. Tuttavia, alcune vulnerabilità della protezione possono richiedere un intervento manuale sul computer locale. In tal caso, Network Manager risolve i problemi che è possibile su cui è possibile intervenire in modalità remota, quindi richiede all'utente di risolvere i restanti problemi effettuando l'accesso a SecurityCenter sul computer vulnerabile e attenendosi ai suggerimenti forniti. In alcuni casi, per correggere il problema si suggerisce di installare la versione più recente di SecurityCenter sul computer remoto o sui computer in rete.

Risolvere vulnerabilità della protezione

È possibile utilizzare Network Manager per risolvere gran parte delle vulnerabilità della protezione sui computer gestiti remoti. Ad esempio, se VirusScan è disattivato su un computer remoto, è possibile attivarlo.

1. Fare clic sull'icona di un elemento sulla mappa della rete.
2. Visualizzare lo stato della protezione dell'elemento nella sezione **Dettagli**.
3. Fare clic su **Risolvere vulnerabilità della protezione** nella sezione **Desidero**.
4. Dopo aver risolto i problemi di protezione, fare clic su **OK**.

Nota: benché Network Manager risolva automaticamente gran parte delle vulnerabilità della protezione, per l'esecuzione di alcune operazioni potrebbe essere necessario avviare SecurityCenter sul computer vulnerabile e attenersi ai suggerimenti forniti.

Installazione del software di protezione McAfee sui computer remoti

Se su uno o più computer in rete non viene utilizzata la versione più recente di SecurityCenter, non è possibile monitorare in modalità remota il rispettivo stato della protezione. Se si desidera monitorare questi computer in modalità remota, è necessario installare la versione più recente di SecurityCenter su ciascuno di essi.

1. Aprire SecurityCenter sui computer su cui si desidera installare il software di protezione.
2. Nella sezione **Attività comuni,** fare clic su **Il mio account**.
3. Effettuare il log in utilizzando l'indirizzo di posta elettronica e la password usati per registrare il software di protezione in fase di installazione.
4. Selezionare il prodotto appropriato, fare clic sull'icona **Download/Installa** e seguire le istruzione riportate sullo schermo.

CAPITOLO 28

McAfee EasyNetwork

EasyNetwork consente la condivisione protetta di file, semplifica i trasferimenti di file e permette la condivisione delle stampanti tra computer della rete domestica. Tuttavia, per accedere alle relative funzioni è necessario aver installato EasyNetwork sui computer in rete.

Prima di utilizzare EasyNetwork, è opportuno acquisire dimestichezza con alcune delle funzioni. I dettagli relativi alla configurazione e all'utilizzo di queste funzioni sono reperibili nella Guida in linea di EasyNetwork.

Nota: SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee.

In questo capitolo

Funzioni di EasyNetwork

EasyNetwork fornisce le funzioni riportate di seguito.

Condivisione di file

EasyNetwork semplifica la condivisione dei file tra i computer in rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer che dispongono di accesso completo o con privilegi di amministratore alla rete gestita (membri) possono condividere file o accedere a file condivisi da altri membri.

Trasferimento di file

È possibile inviare file ad altri computer che dispongono di accesso completo o con privilegi di amministratore alla rete gestita (membri). Nel momento in cui si riceve un file, esso viene visualizzato nella casella dei file in arrivo di EasyNetwork, che rappresenta il percorso di archiviazione temporaneo per tutti i file inviati da altri computer della rete.

Condivisione automatica di stampanti

Dopo che l'utente è diventato membro di una rete gestita, è possibile condividere tutte le stampanti locali collegate al computer con altri membri, utilizzando il nome corrente della stampante come nome della stampante condivisa, rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

CAPITOLO 29

Impostazione di EasyNetwork

Per utilizzare EasyNetwork è necessario avviarlo e diventare membro di una rete gestita. Solo in seguito sarà possibile condividere, cercare e inviare file ad altri computer in rete. È anche possibile condividere le stampanti. Sarà possibile decidere di abbandonare la rete in qualsiasi momento.

In questo capitolo

Come avviare EasyNetwork

Per impostazione predefinita viene richiesto di avviare EasyNetwork dopo l'installazione, per quanto sia anche possibile avviarlo in un secondo momento.

- Nel menu **Start**, scegliere **Programmi**, quindi **McAfee** e fare clic su **McAfee EasyNetwork**.

Suggerimento: se sono state create icone sul desktop e icone di avvio rapido durante l'installazione, è anche possibile avviare EasyNetwork facendo doppio clic sull'omonima icona del desktop oppure nell'area di notifica all'estremità destra della barra delle applicazioni.

Aggiunta di un membro alla rete gestita

Se SecurityCenter non è disponibile su nessun computer in rete a cui è connesso l'utente, quest'ultimo diventerà membro della rete e gli verrà chiesto di stabilire se si tratta di rete affidabile. Poiché è il primo computer a diventare membro della rete, il nome del computer in uso viene incluso nel nome della rete, che potrà tuttavia essere rinominata in qualsiasi momento.

Quando un computer stabilisce una connessione alla rete, richiede agli altri computer in rete l'autorizzazione a diventarne membro. Alla richiesta è possibile acconsentire da qualsiasi computer con autorizzazioni amministrative in rete. La persona che concede le autorizzazioni può inoltre determinare il livello di autorizzazione del computer che diventa membro della rete, ad esempio, Guest (solo trasferimento file) oppure completo/con privilegi di amministratore (trasferimento e condivisione file). In EasyNetwork, i computer che dispongono di accesso con privilegi di amministratore possono consentire l'accesso ad altri computer e gestire autorizzazioni (alzare o abbassare il livello dei computer) mentre i computer con accesso completo non sono in grado di eseguire attività amministrative di questo tipo.

Nota: se sono stati installati altri programmi di rete McAfee (ad esempio, Network Manager), dopo l'aggiunta il computer verrà riconosciuto come computer gestito anche in tali programmi. Il livello di autorizzazione assegnato al computer in EasyNetwork viene applicato a tutti i programmi di rete McAfee. Per ulteriori informazioni sul significato di autorizzazione guest, completa o con autorizzazioni amministrative in altri programmi di rete McAfee, consultare la relativa documentazione.

Aggiunta di un membro alla rete

Quando un computer si connette a una rete affidabile per la prima volta dopo l'installazione di EasyNetwork, viene visualizzato un messaggio che chiede al computer se intende diventare membro di una rete gestita. Se il computer accetta di diventarlo, verrà inviata una richiesta a tutti gli altri computer in rete che dispongono di accesso con privilegi di amministratore. Tale richiesta deve essere accettata prima che il computer possa condividere stampanti o file oppure inviare e copiare file in rete. Al primo computer in rete vengono automaticamente concesse le autorizzazioni amministrative.

1. Nella finestra File condivisi, fare clic su **Aggiungi il computer alla rete**.
   Quando un computer con privilegi di amministratore in rete acconsente alla richiesta, viene visualizzato un messaggio in cui viene chiesto se si intende consentire al computer in uso e agli altri della rete di gestire le impostazioni di protezione reciproche.
2. Per consentire al computer in uso e agli altri computer di rete di gestire le reciproche impostazioni di protezione, fare clic su **OK**, altrimenti fare clic su **Annulla**.
3. Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer a partire dal quale sono state concesse le autorizzazioni, quindi fare clic su **OK**.

Nota: se sul computer che ha inviato l'invito a diventare membro della rete gestita non sono visualizzate le stesse carte da gioco mostrate nella finestra di dialogo di conferma, si è verificata una violazione della protezione sulla rete gestita. Diventare membro della rete può mettere a rischio il proprio computer; pertanto, fare clic su **Annulla** nella finestra di dialogo di conferma.

Autorizzazione di accesso alla rete

Quando un computer chiede di diventare membro di una rete gestita, viene inviato un messaggio agli altri computer in rete che dispongono di accesso con privilegi di amministratore. Il primo computer a rispondere diventa quello dell'utente che concede le autorizzazioni e, come tale, l'utente di questo computer sarà responsabile della scelta del tipo di accesso: Guest, completo o con privilegi di amministratore.

1. Nell'avviso, fare clic sul livello di accesso appropriato.
2. Nella finestra di dialogo Invita un computer a diventare membro della rete gestita, effettuare una delle seguenti operazioni:
   - Fare clic su **Consenti accesso Guest a programmi della rete gestita** per consentire l'accesso al computer di accedere alla rete (è possibile utilizzare questa opzione per gli utenti temporanei della rete domestica).
   - Fare clic su **Consenti accesso completo a programmi della rete gestita** che consente al computer di accedere alla rete.
   - Fare clic su **Consenti accesso con privilegi di amministratore a programmi della rete gestita** che consente al computer di accedere alla rete con autorizzazioni amministrative. Consente inoltre al computer di concedere l'accesso ad altri computer che desiderano diventare membri della rete gestita.
3. Fare clic su **OK**.
4. Verificare che le carte da gioco visualizzate nella finestra di dialogo di conferma della protezione siano visualizzate anche sul computer, quindi fare clic su **Concedi accesso**.

Nota: se le stesse carte da gioco visualizzate nella finestra di dialogo di conferma della protezione non vengono visualizzate anche sul computer, significa che si è verificata una violazione della protezione sulla rete gestita. Poiché concedere a questo computer l'accesso alla rete può mettere a rischio il computer in uso, fare clic su **Rifiuta accesso** nella finestra di dialogo di conferma della protezione.

Rinominare la rete

Per impostazione predefinita, il nome della rete include il nome del primo computer diventato membro della rete; tuttavia, è possibile modificarlo in qualsiasi momento. Quando si rinomina la rete, è possibile modificare la relativa descrizione visualizzata in EasyNetwork.

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, digitare il nome della rete nella casella **Nome di rete**.
3. Fare clic su **OK**.

Abbandono della rete gestita

Se l'utente diventato membro di una rete non intende più essere tale, può abbandonare la rete. Dopo aver abbandonato una rete, è sempre possibile chiedere nuovamente di essere aggiunti; tuttavia, sarà necessario ottenere di nuovo l'autorizzazione. Per ulteriori informazioni sull'adesione, vedere Aggiunta di un membro alla rete gestita (pagina 166).

Abbandono della rete gestita

È possibile abbandonare una rete gestita di cui si era precedentemente diventati membro.

1. Nel menu **Strumenti**, scegliere **Abbandona rete**.
2. Nella finestra di dialogo Abbandona rete, selezionare il nome della rete che si desidera abbandonare.
3. Fare clic su **Abbandona rete**.

CAPITOLO 30

Condivisione e invio di file

EasyNetwork semplifica la condivisione e l'invio di file tra gli altri computer presenti in rete. Quando i file vengono condivisi, è possibile autorizzarne l'accesso in sola lettura ad altri computer. Solo i computer membri della rete gestita (che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri.

Nota: l'eventuale condivisione di un numero elevato di file può incidere sulle risorse del computer.

In questo capitolo

Condivisione di file

Solo i computer membri della rete gestita (che dispongono di accesso completo o con privilegi di amministratore) possono condividere file o accedere a file condivisi da altri computer membri. Se si condivide una cartella, vengono condivisi tutti i file in essa contenuti e le relative sottocartelle, tuttavia la condivisione delle cartelle aggiunte successivamente non avviene automaticamente. Una volta eliminati, file e cartelle condivisi vengono rimossi dalla finestra File condivisi. È possibile interrompere la condivisione di un file in qualsiasi momento.

Per accedere a un file condiviso, aprirlo direttamente da EasyNetwork oppure copiarlo sul computer e quindi aprirlo. Se l'elenco dei file condivisi è troppo lungo per individuare il file desiderato, è possibile effettuare la ricerca dei file.

Nota: i file condivisi con EasyNetwork non sono accessibili da altri computer mediante Esplora risorse, in quanto la condivisione dei file EasyNetwork viene eseguita mediante connessioni protette.

Condivisione di un file

Quando si condivide un file, questo viene reso disponibile a tutti i membri che dispongono di accesso alla rete gestita, sia esso completo o con privilegi di amministratore.

1. In Esplora risorse, individuare il file che si desidera condividere.
2. Trascinare il file dal percorso in Esplora risorse nella finestra File condivisi in EasyNetwork.

Suggerimento: è anche possibile condividere un file facendo clic su **Condividi file** nel menu **Strumenti**. Nella finestra di dialogo Condividi, passare alla cartella in cui è memorizzato il file che si desidera condividere, selezionarlo e fare clic su **Condividi**.

Interruzione della condivisione di un file

Se un file viene condiviso sulla rete gestita, è possibile interrompere la condivisione in qualsiasi momento. Quando si interrompe la condivisione di un file, gli altri membri della rete gestita non possono accedervi.

1. Nel menu **Strumenti**, scegliere **Interrompi condivisione file**.
2. Nella finestra di dialogo Interrompi condivisione file, selezionare il file che non si desidera più condividere.
3. Fare clic su **OK**.

Copia di un file condiviso

Un utente copia un file condiviso in modo da poterne disporre anche quando non è più condiviso. È possibile copiare un file condiviso proveniente da un qualsiasi computer della rete gestita.

- Trascinare un file dalla finestra File condivisi in EasyNetwork in un percorso di Esplora risorse o sul desktop di Windows.

Suggerimento: è anche possibile copiare un file condiviso selezionandolo in EasyNetwork, quindi facendo clic su **Copia in** nel menu **Strumenti**. Nella finestra di dialogo Copia in, passare alla cartella in cui si desidera copiare il file, selezionarlo e fare clic su **Salva**.

Ricerca di un file condiviso

È possibile ricercare un file di cui si è eseguita la condivisione oppure che è stato condiviso da qualsiasi altro membro della rete. Nel momento in cui vengono digitati i criteri di ricerca, EasyNetwork visualizza i risultati corrispondenti nella finestra File condivisi.

1. Nella finestra File condivisi, fare clic su **Cerca**.
2. Fare clic sull'opzione appropriata (pagina 173) nell'elenco **Contiene**.
3. Digitare, tutto o in parte, il nome del file o del percorso nell'elenco **Nome file o percorso**.
4. Fare clic sul tipo di file (pagina 173) nell'elenco **Tipo**.
5. Negli elenchi **Da** e **A** , fare clic sulle date che rappresentano l'intervallo temporale in cui è stato creato il file.

Criteri di ricerca

Nelle tabelle seguenti sono descritti i criteri che è possibile specificare quando si esegue la ricerca di file condivisi.

Nome o percorso del file

Contiene	Descrizione
Contiene tutte le parole	Consente di cercare il nome di un file o di un percorso contenente tutte le parole specificate nell'elenco **Nome file o percorso**, in qualsiasi ordine.
Contiene una qualsiasi delle parole	Consente di cercare il nome di un file o di un percorso contenente una qualsiasi delle parole specificate nell'elenco **Nome file o percorso**.

Contiene la stringa esatta	Consente di cercare il nome di un file o di un percorso contenente esattamente la stringa specificata nell'elenco **Nome file o percorso**.

Tipo di file

Tipo	Descrizione
Qualsiasi	Consente di cercare tutti i tipi di file condivisi.
Documento	Consente di cercare tutti i documenti condivisi.
Immagine	Consente di cercare tutti i file immagine condivisi.
Video	Consente di cercare tutti i file video condivisi.
Audio	Consente di cercare tutti i file audio condivisi.
Compressi	Consente di cercare tutti i file compressi (ad esempio, i file .zip)

Invio di file ad altri computer

È possibile inviare file ad altri computer purché siano membri della rete gestita. Prima di inviare un file, EasyNetwork verifica che il computer che lo riceve abbia sufficiente spazio su disco.

Nel momento in cui si riceve un file, esso viene visualizzato nella casella dei file in arrivo di EasyNetwork, un percorso di archiviazione temporaneo per i file inviati da altri computer della rete. Se durante la ricezione EasyNetwork è aperto, il file viene immediatamente visualizzato nella casella dei file in arrivo; in caso contrario viene visualizzato un messaggio nell'area di notifica all'estremità destra della barra delle applicazioni. Se non si desidera ricevere messaggi di notifica (se interrompono le proprie attività, ad esempio) è possibile disattivare questa funzione. Qualora nella casella dei file in arrivo esista già un file con lo stesso nome, il nuovo file viene rinominato con un suffisso numerico. I file restano nella casella finché l'utente li accetta, cioè finché vengono copiati sul computer in uso.

Invio di un file a un altro computer

È possibile inviare un file a un altro computer nella rete gestita senza condividerlo. Prima che un utente del computer destinatario possa visualizzare il file, sarà necessario salvarlo in un percorso locale. Per ulteriori informazioni, vedere Accettazione di un file da un altro computer (pagina 176).

1. In Esplora risorse, individuare il file che si desidera inviare.
2. Trascinare il file dal percorso in Esplora risorse in un'icona attiva del computer in EasyNetwork.

Suggerimento: per inviare più file a un computer premere CTRL mentre li si seleziona. Per inviare i file è inoltre possibile fare clic su **Invia** nel menu **Strumenti**, selezionare i file e fare clic su **Invia**.

Accettazione di un file proveniente da un altro computer

Se un altro computer della rete gestita invia un file all'utente, è necessario accettarlo salvandolo sul computer. Se EasyNetwork non è in esecuzione durante l'invio del file al computer in uso, l'utente riceverà un messaggio nell'area di notifica all'estremità destra della barra delle applicazioni. Fare clic sul messaggio di notifica per aprire EasyNetwork e accedere al file.

- Fare clic su **Ricevuto**, quindi trascinare il file dalla casella dei file in arrivo di EasyNetwork in una cartella di Esplora risorse.

Suggerimento: è anche possibile ricevere un file da un altro computer selezionandolo nella casella dei file in arrivo di EasyNetwork e facendo clic su **Accetta** nel menu **Strumenti**. Nella finestra di dialogo Accetta nella cartella, passare alla cartella in cui si desidera salvare i file in ricezione, effettuare la selezione e fare clic su **Salva**.

Ricezione di una notifica all'invio di un file

È possibile ricevere un messaggio di notifica quando un altro computer della rete gestita invia un file. Se EasyNetwork non è in esecuzione, il messaggio di notifica viene visualizzato nell'area di notifica all'estremità destra della barra delle applicazioni.

1. Nel menu **Opzioni**, scegliere **Configura**.
2. Nella finestra di dialogo Configura, selezionare la casella di controllo **Avvisa quando è in corso l'invio di file da un altro computer**.
3. Fare clic su **OK**.

CAPITOLO 31

Condivisione di stampanti

Dopo che l'utente è diventato membro di una rete gestita, EasyNetwork condivide le stampanti locali collegate al computer in uso, utilizzando il nome della stampante come nome della stampante condivisa, EasyNetwork rileva le stampanti condivise da altri computer in rete e ne consente la configurazione e l'uso.

Se è stato configurato un driver per stampare mediante un server di stampa di rete (ad esempio, un server di stampa USB senza fili), EasyNetwork considera la stampante come locale e la condivide in rete. È anche possibile interrompere la condivisione di una stampante in qualsiasi momento.

In questo capitolo

Uso delle stampanti condivise

EasyNetwork rileva le stampanti condivise dagli altri computer della rete. In caso di rilevamento di una stampante remota non connessa al computer, quando EasyNetwork viene aperto per la prima volta, nella finestra File condivisi viene visualizzato il collegamento **Stampanti di rete disponibili**. In questo modo l'utente potrà installare le stampanti disponibili o disinstallare quelle già connesse al computer nonché aggiornare l'elenco delle stampanti per assicurarsi di visualizzare informazioni aggiornate.

Se invece è connesso alla rete gestita ma non ne è diventato membro, l'utente potrà accedere alle stampanti condivise mediante il pannello di controllo delle stampanti di Windows.

Interruzione della condivisione di una stampante

Se si interrompe la condivisione di una stampante, i membri non potranno utilizzarla.

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Gestione stampanti di rete, fare clic sul nome della stampante che non si desidera più condividere.
3. Fare clic su **Non condividere**.

Installazione di una stampante di rete disponibile

Se l'utente è membro della rete gestita, può accedere alle stampanti condivise in rete; tuttavia, sarà necessario installare il driver utilizzato dalla stampante. Se il proprietario della stampante ne interrompe la condivisione, gli utenti non saranno in grado di utilizzarla.

1. Nel menu **Strumenti**, scegliere **Stampanti**.
2. Nella finestra di dialogo Stampanti di rete disponibili, fare clic sul nome di una stampante.
3. Fare clic su **Installa**.

Riferimento

Nel Glossario dei termini sono elencati e illustrati i termini relativi alla protezione più comunemente utilizzati nei prodotti McAfee.

Glossario

8

802.11

Insieme di standard IEEE per la trasmissione di dati su una rete senza fili. 802.11 è comunemente noto come Wi-Fi.

802.11a

Estensione di 802.11 che consente la trasmissione di dati fino a 54 Mbps nella banda dei 5 GHz. Nonostante la velocità di trasmissione sia superiore rispetto a 802.11b, la distanza coperta è di gran lunga inferiore.

802.11b

Estensione di 802.11 che consente la trasmissione di dati fino a 11 Mbps nella banda dei 2,4 GHz. Nonostante la velocità di trasmissione sia inferiore rispetto a 802.11b, la distanza coperta è superiore.

802.1x

Standard IEEE per l'autenticazione sulle reti cablate e senza fili. 802.1x è comunemente utilizzato con la rete senza fili 802.11.

A

Access Point

Dispositivo di rete, noto comunemente come router senza fili, che si collega a un hub o switch Ethernet per ampliare la gamma fisica di servizi a un utente senza fili. Quando gli utenti senza fili si collegano con i dispositivi portatili, la trasmissione passa da un Access Point (AP) all'altro per mantenere la connettività.

account di posta elettronica standard

Vedere POP3.

archiviazione

Creazione di una copia dei file importanti su CD, DVD, unità USB, disco rigido esterno o unità di rete.

archiviazione completa

Archiviazione completa di un set di dati in base ai tipi di file e ai percorsi impostati. Vedere anche archiviazione rapida.

archiviazione rapida

Archiviazione solo dei file che sono cambiati dopo l'ultima archiviazione completa o rapida. Vedere anche archiviazione completa.

archivio del backup in linea

Percorso del server online dove sono memorizzati i file dopo che ne è stato eseguito il backup.

Archivio protetto password

Area di memorizzazione protetta per le password personali che consente di memorizzare le password in modo tale che nessun altro utente, compreso un amministratore, possa accedervi.

attacco brute force

Metodo di codifica dei dati crittografati come le password, mediante uno sforzo notevole (la forza bruta) piuttosto che impiegando strategie intellettuali. L'uso della forza bruta è considerato un metodo di attacco infallibile anche se richiede tempi piuttosto lunghi. L'attacco di forza bruta è noto anche come brute-force cracking.

attacco di tipo dictionary

Tipo di attacco di forza bruta che utilizza parole comuni per provare a scoprire una password.

attacco di tipo man-in-the-middle

Metodo di intercettazione ed eventuale modifica dei messaggi tra due parti senza che una delle parti venga a conoscenza della violazione del collegamento della comunicazione.

autenticazione

Processo di identificazione di un individuo, di solito basato su un nome utente univoco e una password.

B

backup

Creazione di una copia dei file importanti su un server online protetto.

browser

Programma utilizzato per visualizzare le pagine Web su Internet. Tra i browser Web più conosciuti si annoverano Microsoft Internet Explorer e Mozilla Firefox.

C

cache

Area di memorizzazione temporanea sul computer. Ad esempio, per aumentare la velocità e l'efficienza della navigazione sul Web, la volta successiva che si desidera visualizzare una pagina, il browser può recuperarla dalla cache invece che dal server remoto.

Cestino

Cestino della spazzatura fittizio per i file e le cartelle eliminati in Windows.

chiave

Serie di lettere e numeri utilizzata da due dispositivi per autenticarne la comunicazione. Entrambi i dispositivi devono disporre della chiave. Vedere anche WEP, WPA, WPA2, WPA-PSK e WPA2- PSK.

client

Applicazione eseguita su PC o workstation che richiede un 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.

client di posta elettronica

Programma eseguito sul computer per l'invio e la ricezione di e-mail, ad esempio Microsoft Outlook.

collegamento

File che contiene solo il percorso di un altro file sul computer.

compressione

Processo mediante il quale i file vengono compressi in un formato tale da ridurre al minimo lo spazio richiesto per memorizzarli o trasmetterli.

condivisione

Operazione che consente ai destinatari di un messaggio di posta elettronica di accedere ai file di backup selezionati per un periodo limitato di tempo. Quando si condivide un file, la copia di backup del file viene inviata ai destinatari del messaggio di posta elettronica specificati. I destinatari ricevono un messaggio di posta elettronica da Data Backup in cui viene segnalato che i file sono stati condivisi. Nel messaggio di posta elettronica è riportato anche un collegamento ai file condivisi.

Controllo ActiveX

Componente software utilizzato dai programmi o dalle pagine Web per aggiungere funzionalità che appaiono come parte normale del programma o della pagina Web. La maggior parte dei controlli ActiveX sono innocui; tuttavia, alcuni potrebbero acquisire informazioni dal computer.

Controllo genitori

Impostazioni che consentono di controllare i contenuti visualizzati dai minori e le operazioni consentite durante la navigazione in Internet. Per impostare il Controllo genitori, è possibile attivare o disattivare il filtraggio immagini, scegliere un gruppo di classificazione del contenuto e impostare le limitazioni degli orari di navigazione sul Web.

cookie

Piccolo file contenente informazioni che di solito comprendono il nome utente e l'ora e la data correnti, memorizzato nel computer dell'utente che naviga sul Web. I cookie vengono utilizzati principalmente dai siti Web per identificare gli utenti che si sono registrati o che hanno visitato il loro sito; tuttavia, possono anche essere una fonte di informazioni per gli hacker.

crittografia

Processo mediante il quale i dati vengono trasformati da testo in codice, oscurando le informazioni per renderle illeggibili agli utenti che non sanno come decifrarle. I dati crittografati sono noti anche come testo crittografato.

D

DAT

(File delle firme elettroniche dei dati) File contenenti le definizioni utilizzate durante il rilevamento di virus, trojan horse, spyware, adware e altri programmi potenzialmente indesiderati sul computer o sull'unità USB.

denial of Service (Negazione del servizio)

Tipo di attacco che rallenta o arresta il traffico su una rete. Un attacco DoS (denial of service) si verifica quando una rete è inondata da una quantità di ulteriori richieste talmente elevata che il normale traffico viene rallentato o completamente interrotto. In genere non comporta il furto di informazioni o altre vulnerabilità della protezione.

dialer

Software che aiuta a stabilire una connessione Internet. Se utilizzati in maniera dannosa, i dialer sono in grado di reindirizzare le connessioni Internet a provider diversi dall'ISP (Internet Service Provider) predefinito, senza informare l'utente dei costi aggiuntivi.

disco rigido esterno

Disco rigido collegato all'esterno del computer.

DNS

(Domain Name System) Sistema che converte i nomi host o di dominio in indirizzi IP. Sul Web, il DNS viene utilizzato per convertire facilmente un indirizzo Web leggibile, ad esempio www.nomehost.com, in indirizzi IP quali 111.2.3.44 in modo da recuperare il sito Web. Senza il DNS, sarebbe necessario immettere l'indirizzo IP nel browser Web.

dominio

Sottorete locale o descrizione dei siti su Internet.

Su una rete locale (LAN), un dominio è una sottorete costituita da computer client e server controllati da un database di protezione. In questo contesto, le prestazioni dei domini possono essere migliori. Su Internet, un dominio è parte di ogni indirizzo Web; ad esempio, in www.abc.com il dominio è: abc.

E

e-mail

(Posta elettronica) Messaggi inviati e ricevuti a livello elettronico su una rete di computer. Vedere anche Web mail.

elenco degli elementi affidabili

Contiene gli elementi considerati affidabili e non rilevati. Elementi quali, ad esempio, programmi potenzialmente indesiderati o modifiche del registro, dovranno essere rimossi dall'elenco se considerati erroneamente affidabili o se si desidera verificarne di nuovo la presenza.

elenco indirizzi autorizzati

Elenco di siti Web a cui è consentito l'accesso perché non considerati dannosi.

elenco indirizzi bloccati

Nell'anti-phishing, elenco di siti Web considerati dannosi.

ESS

(Extended Service Set) Insieme di una o più reti che formano un'unica sottorete.

evento

Azione avviata dall'utente, da un dispositivo o dal computer che attiva una risposta. Nei prodotti McAfee, gli eventi sono registrati nel registro eventi.

F

file temporanei

File creati in memoria o sul disco dal sistema operativo o da un altro programma e che vengono utilizzati durante una sessione per essere quindi eliminati.

filtraggio immagini

Opzione Controllo genitori che blocca la visualizzazione di immagini Web potenzialmente inadeguate.

firewall

Sistema progettato (hardware, software o entrambi) per impedire l'accesso non autorizzato a o da una rete privata. I firewall vengono utilizzati di frequente per impedire a utenti di Internet non autorizzati di accedere a reti private connesse a Internet, specialmente a una rete Intranet. Tutti i messaggi in entrata o in uscita su Internet passano attraverso il firewall, il quale esamina tutti i messaggi e blocca quelli non conformi ai criteri di protezione specificati.

frammenti di file

Porzioni di un file sparsi su un disco. La frammentazione dei file si verifica quando si aggiungono o eliminano file e può inoltre rallentare le prestazioni del computer.

G

gateway integrato

Dispositivo che combina le funzioni di punto di accesso, router e firewall. Alcuni dispositivi possono persino includere funzionalità avanzate di protezione e bridging.

gruppo di classificazione del contenuto

Nel Controllo genitori, gruppo di età a cui appartiene un utente. Il contenuto viene reso disponibile o bloccato in base al gruppo di classificazione del contenuto al quale appartiene l'utente. I gruppi di classificazione del contenuto comprendono: minori di 6 anni, 6-9 anni, 10-13 anni, 14-18 anni, maggiori di 18 anni.

H

hotspot

Limite geografico coperto da un Access Point (AP) Wi-Fi (802.11). Gli utenti che entrano in un hotspot con un laptop senza fili possono connettersi a Internet, a condizione che l'hotspot sia un Web beacon, ovvero che pubblicizzi la propria presenza, e non sia richiesta l'autenticazione. Gli hotspot sono spesso situati in zone molto popolate, quali ad esempio gli aeroporti.

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 0 e 255, ad esempio 192.168.1.100.

Indirizzo MAC

(Indirizzo Media Access Control) Numero di serie univoco assegnato al dispositivo fisico che accede alla rete.

Internet

Internet è un sistema costituito da un numero elevatissimo di reti interconnesse che utilizzano i protocolli TCP/IP per individuare e trasferire dati. Internet è l'evoluzione di una rete di computer di università e college creata tra la fine degli anni '60 e l'inizio degli anni '70 dal Dipartimento della difesa degli Stati Uniti e denominata ARPANET. Internet è oggi una rete globale costituita da circa 100.000 reti indipendenti.

intranet

Rete privata di computer, generalmente all'interno di un'organizzazione, alla quale possono accedere solo gli utenti autorizzati.

L

LAN

(Local Area Network) Rete di computer che si estende in un'area relativamente ridotta, ad esempio un singolo edificio. I computer su una rete LAN possono comunicare tra loro e condividere le risorse quali stampanti e file.

larghezza di banda

Quantità di dati trasmettibili in un determinato lasso di tempo.

Launchpad

Componente dell'interfaccia U3 che funge da punto di partenza per l'avvio e la gestione dei programmi USB U3.

libreria

Area di memorizzazione online per i file pubblicati e di cui è stato eseguito il backup. La libreria di Data Backup è un sito Web su Internet, accessibile a chiunque disponga di un accesso a Internet.

M

MAC (message authentication code)

Codice di protezione utilizzato per crittografare i messaggi trasmessi tra i computer. Il messaggio viene accettato se il computer riconosce il codice decrittografato come valido.

MAPI

(Messaging Application Programming Interface) Specifica di interfaccia di Microsoft che consente a differenti applicazioni di workgroup e messaggistica (tra cui posta elettronica, casella vocale e fax) di collaborare attraverso un singolo client, ad esempio il client di Exchange.

mappa di rete

Rappresentazione grafica dei computer e dei componenti che costituiscono la rete domestica.

MSN

(Microsoft Network) Gruppo di servizi basati sul Web offerti da Microsoft Corporation, tra cui motore di ricerca, messaggistica immediata e portale.

N

NIC

(Network Interface Card) Scheda che si inserisce in un laptop o in altro dispositivo e connette il dispositivo alla LAN.

nodo

Singolo computer connesso a una rete.

P

parola chiave

Parola che è possibile assegnare a un file di backup per stabilire un rapporto o una connessione con altri file a cui è stata assegnata la stessa parola chiave. L'assegnazione di parole chiave ai file agevola la ricerca dei file che sono stati pubblicati su Internet.

password

Codice, in genere costituito da lettere e numeri, utilizzato per ottenere l'accesso a un computer, a un programma o a un sito Web.

percorsi di monitoraggio rapido

Cartella sul computer sottoposta al monitoraggio delle modifiche da parte di Data Backup. Se si imposta un percorso di monitoraggio rapido, Data Backup esegue il backup dei tipi di file monitorati all'interno della cartella, ignorando il contenuto delle sottocartelle.

percorsi monitorati

Cartelle sul computer monitorate da Data Backup.

percorso di monitoraggio approfondito

Cartella sul computer sottoposta al monitoraggio delle modifiche da parte di Data Backup. Se si imposta un percorso di monitoraggio approfondito, Data Backup esegue il backup dei tipi di file monitorati in tale cartella e nelle relative sottocartelle.

phishing

Sistemi ingannevoli utilizzati per il furto di dati riservati quali il numero della carta di credito e del codice fiscale, l'ID utente e le password da parte di individui sconosciuti per uso fraudolento.

plug-in

Piccolo programma software che utilizza un programma di maggiori dimensioni per fornire ulteriori funzionalità. Ad esempio, i plug-in consentono al browser Web di accedere ai file incorporati nei documenti HTML il cui formato non verrebbe normalmente riconosciuto (ad esempio, file di animazione, audio e video) e, quindi, di eseguirli.

POP3

(Post Office Protocol 3) Interfaccia tra un programma client di posta elettronica e il server di posta elettronica. La maggior parte degli utenti domestici utilizza account e-mail POP3, noti anche come account e-mail standard.

popup

Piccole finestre che vengono visualizzate davanti ad altre finestre sullo schermo del computer. Le finestre popup sono spesso utilizzate nei browser Web per visualizzare annunci pubblicitari.

porta

Punto in cui le informazioni entrano e/o escono dal computer. Ad esempio, il tradizionale modem analogico viene connesso alla porta seriale.

PPPoE

(Point-to-Point Protocol Over Ethernet) Metodo di utilizzo del protocollo punto a punto su Ethernet come mezzo di trasporto.

Programma potenzialmente indesiderato (PUP)

Programma che raccoglie e trasmette informazioni personali senza il consenso della persona interessata (ad esempio, spyware e adware).

protocollo

Formato hardware o software per la trasmissione di dati tra due dispositivi. Per comunicare con altri computer, il computer o dispositivo in uso deve utilizzare il protocollo corretto.

proxy

Computer o software che separa una rete da Internet, presentando un solo indirizzo di rete ai siti esterni. Rappresentando tutti i computer interni, il proxy protegge le identità di rete pur continuando a fornire l'accesso a Internet. Vedere anche server proxy.

pubblicazione

Operazione il cui scopo è rendere un file di backup disponibile a tutti su Internet. È possibile accedere ai file pubblicati eseguendo una ricerca nella libreria di Data Backup.

punto di accesso pericoloso

Access Point non autorizzato. I punti di accesso pericolosi possono essere installati su una rete aziendale protetta per concedere l'accesso alla rete a utenti non autorizzati. Possono inoltre essere creati per consentire all'autore dell'attacco di condurre un attacco di tipo man-in-the-middle.

punto di ripristino configurazione di sistema

Istantanea (immagine) del contenuto della memoria del computer o di un database. Windows crea dei punti di ripristino periodicamente e in caso di eventi significativi del sistema (ad esempio se si installa un programma o un driver). È inoltre possibile creare e denominare i propri punti di ripristino in qualsiasi momento.

Q

quarantena

Isolamento. In VirusScan, ad esempio, i file sospetti sono rilevati e messi in quarantena in modo da non poter danneggiare il computer o i file.

R

RADIUS

(Remote Access Dial-In User Service) Protocollo che consente 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 RADIUS viene ora utilizzato in un'ampia gamma di ambienti di autenticazione, inclusa l'autenticazione 802.1x del segreto condiviso di un utente di una WLAN.

registro di sistema

Database in cui Windows memorizza le informazioni di configurazione. Contiene i profili relativi a ciascun utente del computer nonché le informazioni relative all'hardware del sistema, i programmi installati e le impostazioni delle proprietà. Windows utilizza di continuo tali informazioni durante il funzionamento.

rete

Insieme di Access Point e dei relativi utenti, equivalente a un ESS.

rete domestica

Due o più computer connessi in un ambiente domestico per la condivisione dei file e dell'accesso a Internet. Vedere anche LAN.

rete gestita

Rete domestica con due tipi di membri: membri gestiti e membri non gestiti. I membri gestiti, diversamente da quelli non gestiti, consentono agli altri computer in rete di monitorare lo stato della protezione.

ripristino

Recupero di una copia di un file dall'archivio del backup in linea o da un archivio.

roaming

Spostamento da un'area coperta da un Access Point (AP) a un'altra senza interruzione di servizio o perdita di connettività.

rootkit

Insieme di strumenti (programmi) che concedono a un utente l'accesso a livello di amministratore a un computer o rete di computer. Possono comprendere spyware e altri programmi potenzialmente indesiderati che possono rappresentare un rischio per la protezione dei dati presenti sul computer o per la privacy.

router

Dispositivo di rete che inoltra pacchetti di dati da una rete all'altra. Sulla base di tabelle di instradamento interne, i router leggono ogni pacchetto in ingresso e decidono come inoltrarlo in base alla combinazione dell'indirizzo di origine e di destinazione, nonché delle attuali condizioni di traffico, quali il carico, i costi della linea e il cattivo stato della linea. A volte il router è denominato anche Access Point (AP).

S

Scansione in tempo reale

Verifica della presenza di virus e altre attività in file e cartelle al momento dell'accesso da parte dell'utente o del computer.

Scansione su richiesta

Scansione avviata su richiesta, ossia all'avvio dell'operazione. Diversamente dalla scansione in tempo reale, la scansione su richiesta non viene avviata automaticamente.

scheda di rete senza fili

Dispositivo che fornisce la funzionalità senza fili a un computer o PDA. È collegato mediante una porta USB, uno slot per scheda PC (CardBus), uno slot per scheda di memoria o internamente al bus PCI.

scheda senza fili USB

Scheda senza fili connessa mediante uno slot USB del computer.

schede senza fili PCI

(Peripheral Component Interconnect) Scheda senza fili che si inserisce in uno slot di espansione PCI all'interno del computer.

script

Elenco di comandi in grado di essere eseguiti in modo automatico, ovvero senza l'intervento dell'utente. Diversamente dai programmi, in genere gli script sono memorizzati nel rispettivo testo normale e vengono compilati a ogni esecuzione. Anche le macro e i file batch sono detti script.

segreto condiviso

Stringa o chiave, normalmente una password, condivisa tra due parti in comunicazione prima di avviare la comunicazione. Il segreto condiviso viene utilizzato per proteggere le porzioni più riservate dei messaggi RADIUS.

server

Computer o programma che accetta le connessioni da altri computer o programmi e restituisce le apposite risposte. Ad esempio, il programma di posta elettronica si collega a un server di posta elettronica ogni volta che l'utente invia o riceve messaggi e-mail.

server DNS

(Server Domain Name System) Computer che restituisce l'indirizzo IP associato a un host o nome del dominio. Vedere anche DNS.

server proxy

Componente del firewall che gestisce il traffico Internet da e verso una LAN (Local Area Network). Un server proxy consente di migliorare le prestazioni fornendo i dati richiesti frequentemente, ad esempio una pagina Web, e di filtrare ed eliminare le richieste non considerate appropriate, quali le richieste di accesso non autorizzato ai file proprietari.

sincronizzazione

Risoluzione di eventuali incoerenze tra i file di backup e quelli memorizzati sul computer locale. La sincronizzazione è necessaria quando la versione di un file presente nell'archivio del backup in linea è più recente rispetto a quella del file memorizzato negli altri computer.

Smart drive

Vedere Unità USB.

SMTP

(Simple Mail Transfer Protocol) Protocollo TCP/IP per l'invio di messaggi da un computer a un altro su una rete. Questo protocollo è utilizzato su Internet per instradare i messaggi di posta elettronica.

sovraccarico del buffer

Condizione che si verifica quando programmi o processi sospetti tentano di memorizzare in un buffer (area di memorizzazione temporanea dei dati) del computer una quantità di dati superiore al limite consentito. I sovraccarichi del buffer causano il danneggiamento o la sovrascrittura di dati validi presenti nei buffer adiacenti.

spoofing degli indirizzi IP

Contraffazione di indirizzi IP in un pacchetto IP. Viene utilizzato in molti tipi di attacchi, inclusa la presa di controllo della sessione. Viene inoltre impiegato per contraffare le intestazioni dei messaggi di posta indesiderati in modo da impedire la corretta individuazione dei mittenti.

SSID

(Service Set Identifier) Token, o chiave segreta, che identifica una rete Wi-Fi (802.11). Il token SSID viene impostato dall'amministratore della rete e deve essere fornito dagli utenti che desiderano accedere alla rete.

SSL

(Secure Sockets Layer) Protocollo sviluppato da Netscape per la trasmissione di documenti privati tramite Internet. Il protocollo SSL utilizza una chiave pubblica per crittografare i dati trasferiti sulla connessione SSL. Gli URL che richiedono una connessione SSL iniziano con https anziché con http.

SystemGuard

Avvisi di McAfee che rilevano e notificano la presenza di modifiche non autorizzate sul computer.

T

testo crittografato

Testo crittografato. Il testo crittografato è illeggibile finché non viene convertito in testo normale, ovvero viene decrittografato.

testo normale

Testo non crittografato. Vedere anche crittografia.

tipi di file monitorati

Tipi di file, ad esempio DOC, XLS e così via, di cui Data Backup esegue il backup o che memorizza negli archivi all'interno dei percorsi monitorati.

TKIP

(Temporal Key Integrity Protocol) Protocollo che rileva eventuali punti deboli nella protezione WEP, soprattutto in caso di riutilizzo delle chiavi di crittografia. Il protocollo 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 punti di accesso. TKIP combina la chiave temporale con l'indirizzo MAC del client e aggiunge un vettore di inizializzazione da 16 ottetti, relativamente grande, per produrre la chiave utilizzata per la crittografia dei dati. Questa procedura assicura che ogni stazione utilizzi flussi di chiavi differenti per crittografare i dati. TKIP utilizza RC4 per eseguire la crittografia.

Trojan horse

Programma che ha l'aspetto di programma legittimo ma può consentire l'accesso non autorizzato al computer, provocarne malfunzionamenti e danneggiare file importanti.

U

U3

(You: Simplified, Smarter, Mobile) Piattaforma che consente di eseguire programmi per Windows 2000 o Windows XP direttamente su un'unità USB. L'iniziativa U3 è stata fondata nel 2004 da M-Systems e SanDisk e consente agli utenti di eseguire programmi U3 su computer Windows senza installare o memorizzare dati e impostazioni sul computer stesso.

unità di rete

Unità disco o nastro collegata a un server su una rete e condivisa da più utenti. Le unità di rete sono spesso note come unità remote.

Unità USB

Piccola unità di memoria che si collega alla porta USB del computer. Un'unità USB funge da piccolo disco rigido, semplificando il trasferimento di file da un computer all'altro.

URL

(Uniform Resource Locator) Il formato standard per gli indirizzi Internet.

USB

(Universal Serial Bus) Interfaccia di computer seriale standardizzata che consente di collegare al computer dispositivi periferici quali tastiere, joystick e stampanti.

V

Virus

Programmi in grado di autoreplicarsi che possono alterare i file o i dati. Spesso hanno l'aspetto di programmi legittimi e la loro provenienza sembra affidabile.

VPN

(Virtual Private Network) Rete privata configurata all'interno di una rete pubblica in modo tale da usufruire delle strutture di gestione della rete pubblica. Le reti VPN vengono utilizzate dalle aziende per creare reti WAN in grado di coprire vaste aree geografiche, per fornire connessioni da sito a sito alle filiali o per consentire agli utenti mobili di connettersi alle LAN aziendali.

W

wardriver

Persona che tenta di intercettare le reti Wi-Fi (802.11) girando per le città con un computer Wi-Fi e alcuni componenti hardware o software speciali.

Web bug

Piccoli file grafici che si incorporano autonomamente nelle pagine HTML e consentono a un'origine non autorizzata di impostare cookie sul computer dell'utente. I cookie possono quindi trasmettere dati all'origine non autorizzata. I Web bug sono anche chiamati Web beacon, pixel tag, GIF trasparenti o GIF invisibili.

Web mail

Messaggi inviati e ricevuti elettronicamente via Internet. Vedere anche posta elettronica.

WEP

(Wired Equivalent Privacy) Protocollo di crittografia e autenticazione definito come parte dello standard Wi-Fi (802.11). Le versioni iniziali sono basate su crittografia 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 fra due punti. Tuttavia, si è scoperto che WEP non è tanto sicuro come si credeva.

Wi-Fi

(Wireless Fidelity) Termine utilizzato da Wi-Fi Alliance per fare riferimento a qualsiasi tipo di rete 802.11.

Wi-Fi Alliance

Organizzazione costituita dai principali fornitori di hardware e software senza fili. Wi-Fi Alliance si impegna a certificare tutti i prodotti basati sullo standard 802.11 per assicurare l'interoperabilità e a promuovere il termine Wi-Fi come marchio globale in tutti i mercati per tutti i prodotti LAN senza fili basati su 802.11. L'organizzazione funge da consorzio, laboratorio di collaudo e centro di raccolta e smistamento per i fornitori che desiderano promuovere lo sviluppo di questo settore.

Wi-Fi Certified

Prodotto che deve essere testato e approvato da Wi-Fi Alliance. I prodotti Wi-Fi Certified devono garantire l'interoperabilità anche se provengono da produttori diversi. Un utente che dispone di un prodotto Wi-Fi Certified può utilizzare un punto di accesso (AP) di qualunque marca con hardware client di qualsiasi altra marca, purché siano certificati.

WLAN

(Wireless Local Area Network) Rete LAN che utilizza una connessione senza fili. Una WLAN utilizza onde radio ad alta frequenza anziché fili per consentire ai computer di comunicare tra loro.

worm

Virus in grado di autoreplicarsi; esso risiede nella memoria attiva e può inviare copie di sé stesso attraverso i messaggi di posta elettronica. I worm si replicano e consumano risorse del sistema, rallentando le prestazioni o interrompendo le attività.

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 upgrade 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 l'accesso alla rete venga effettuato solo da utenti autorizzati.

WPA-PSK

Una speciale modalità WPA progettata per gli utenti privati che non richiedono una protezione avanzata a livello enterprise e non hanno accesso a server di autenticazione. Utilizzando questa modalità, l'utente privato inserisce manualmente la password iniziale per attivare l'accesso protetto Wi-Fi in modalità PSK (Pre-Shared Key, Chiave già condivisa) e deve cambiare regolarmente la passphrase su ciascun punto di accesso e computer senza fili. Vedere anche WPA2-PSK e TKIP.

WPA2

Aggiornamento dello standard di protezione WPA, basato sullo standard IEEE 802.11i.

WPA2-PSK

Modalità WPA speciale, simile a WPA-PSK e basata sullo standard WPA2. Una funzione comune di WPA2-PSK è che i dispositivi spesso supportano più modalità di crittografia (ad esempio AES, TKIP) contemporaneamente, mentre i dispositivi più obsoleti supportano generalmente solo una singola modalità di crittografia alla volta (ossia, tutti i client devono utilizzare la stessa modalità di crittografia).

Informazioni su McAfee

McAfee, Inc., con sede centrale a Santa Clara, California, leader globale nella gestione dei rischi associati alla protezione e nella prevenzione delle intrusioni, offre soluzioni e servizi dinamici e affidabili che proteggono sistemi e reti in tutto il mondo. Grazie alla sua insuperata esperienza in materia di protezione e al suo impegno in termini di innovazione, McAfee offre agli utenti privati, alle aziende, al settore pubblico e ai provider di servizi la capacità di bloccare gli attacchi, di impedire le interruzioni dei servizi e di controllare e migliorare continuamente la protezione dei loro sistemi.

Copyright

Licenza

AVVISO AGLI UTENTI: LEGGERE ATTENTAMENTE IL TESTO DEL CONTRATTO RELATIVO ALLA LICENZA ACQUISTATA, 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 ACQUISTATA, 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, INC. O AL PUNTO VENDITA IN CUI È STATO ACQUISTATO ED ESSERE INTERAMENTE RIMBORSATO.

CAPITOLO 32

Assistenza clienti e supporto tecnico

SecurityCenter notifica la presenza di problemi di protezione, critici e non critici, non appena vengono rilevati. I problemi critici di protezione richiedono un intervento immediato e comportano il passaggio dello stato della protezione a rosso. I problemi non critici di protezione non richiedono un intervento immediato e, a seconda del tipo di problema, possono influire sullo stato della protezione. Per raggiungere uno stato della protezione verde, è necessario risolvere tutti i problemi critici e risolvere oppure ignorare tutti i problemi non critici. Se occorre assistenza nel rilevare i problemi di protezione, è possibile avviare il tecnico virtuale di McAfee. Per ulteriori informazioni sul tecnico virtuale di McAfee, consultare la relativa Guida.

Se il software di protezione è stato acquistato da un partner o fornitore diverso da McAfee, aprire un browser Web e accedere a www.mcafeeaiuto.com. Quindi, da Collegamenti partner, selezionare il partner o il fornitore per accedere al tecnico virtuale di McAfee.

Nota: per installare ed eseguire il tecnico virtuale di McAfee, è necessario accedere al computer come amministratore di Windows. In caso contrario, il tecnico virtuale di McAfee potrebbe non essere in grado di risolvere i problemi. Per informazioni sull'accesso come amministratore di Windows, vedere la Guida di Windows. In Windows Vista™, viene visualizzata una richiesta all'avvio del tecnico virtuale di McAfee. In questo caso, fare clic su **Accetto**. Il tecnico virtuale non è disponibile con Mozilla® Firefox.

In questo capitolo

Utilizzo del tecnico virtuale di McAfee

Analogamente a un addetto del supporto tecnico, il tecnico virtuale raccoglie informazioni sui programmi SecurityCenter in uso al fine di fornire assistenza nella risoluzione dei problemi di protezione del computer. Il tecnico virtuale, quando attivato, verifica il corretto funzionamento dei programmi SecurityCenter in uso. Se rileva problemi, il tecnico virtuale offre la possibilità di risolverli automaticamente oppure fornisce indicazioni dettagliate su di essi. Effettuate tutte le operazioni, il tecnico virtuale comunica i risultati delle analisi e, se necessario, consente di ottenere ulteriore assistenza dal supporto tecnico di McAfee.

Per preservare la protezione e l'integrità del computer e dei file in uso, il tecnico virtuale non raccoglie dati personali che possano identificare l'utente.

Nota: per ulteriori informazioni, accedere al tecnico virtuale e fare clic sull'icona **?**.

Come avviare il tecnico virtuale

Il tecnico virtuale raccoglie informazioni sui programmi SecurityCenter in uso al fine di fornire assistenza nella risoluzione dei problemi di protezione. Per garanire la privacy, il tecnico virtuale non raccoglie alcun dato personale in grado di identificare gli utenti del computer.

1. Nella sezione **Attività comuni**, fare clic su **Tecnico virtuale di McAfee**.
2. Seguire le istruzioni visualizzate sullo schermo per scaricare e avviare il tecnico virtuale.

Supporto e download

Consultare le tabelle seguenti per informazioni sui siti di assistenza e download McAfee nel proprio Paese, comprese le Guide dell'utente.

Supporto e download

Paese	Assistenza McAfee	Download McAfee
Australia	www.mcafeeaiuto.com	au.mcafee.com/root/downloads.asp
Brasile	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (inglese)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (francese)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Cina (chn)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Cina (tw)	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Repubblica Ceca	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Danimarca	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
Finlandia	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Francia	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Germania	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Gran Bretagna	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Italia	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Giappone	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Corea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Messico	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norvegia	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polonia	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

Portogallo	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Spagna	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Svezia	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Turchia	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Stati Uniti	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

Guide dell'utente di McAfee Total Protection

Paese	Guide dell'utente McAfee
Australia	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (francese)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Cina (chn)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Cina (tw)	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Danimarca	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Germania	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Gran Bretagna	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
Olanda	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

Corea	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portogallo	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

Guide dell'utente di McAfee Internet Security

Paese	Guide dell'utente di McAfee
Australia	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (francese)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Cina (chn)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Cina (tw)	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Danimarca	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Germania	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

Gran Bretagna	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Olanda	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portogallo	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

Guide dell'utente di McAfee VirusScan Plus

Paese	Guide dell'utente di McAfee
Australia	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (francese)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Cina (chn)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Cina (tw)	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

Danimarca	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Germania	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Gran Bretagna	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Olanda	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portogallo	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

Guide dell'utente di McAfee VirusScan

Paese	Guide dell'utente di McAfee
Australia	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasile	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
Canada (inglese)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

Canada (francese)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Cina (chn)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Cina (tw)	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Repubblica Ceca	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Danimarca	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
Finlandia	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Francia	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Germania	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Gran Bretagna	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
Olanda	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italia	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Giappone	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Corea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Messico	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norvegia	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polonia	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portogallo	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Spagna	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Svezia	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Turchia	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Stati Uniti	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Consultare le tabelle seguenti per informazioni sul Centro minacce McAfee e sui siti contenenti informazioni virus nel proprio Paese.

Paese	Quartier generale della sicurezza	Informazioni sui virus
Australia	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasile	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (inglese)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (francese)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Cina (chn)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
Cina (tw)	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Repubblica Ceca	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Danimarca	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finlandia	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Francia	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Germania	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Gran Bretagna	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Olanda	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italia	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Giappone	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Corea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Messico	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norvegia	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polonia	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo

Portogallo	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Spagna	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Svezia	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Turchia	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Stati Uniti	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Consultare la seguente tabella per informazioni sui siti HackerWatch nel proprio Paese.

Paese	HackerWatch
Australia	www.hackerwatch.org
Brasile	www.hackerwatch.org/?lang=pt-br
Canada (inglese)	www.hackerwatch.org
Canada (francese)	www.hackerwatch.org/?lang=fr-ca
Cina (chn)	www.hackerwatch.org/?lang=zh-cn
Cina (tw)	www.hackerwatch.org/?lang=zh-tw
Repubblica Ceca	www.hackerwatch.org/?lang=cs
Danimarca	www.hackerwatch.org/?lang=da
Finlandia	www.hackerwatch.org/?lang=fi
Francia	www.hackerwatch.org/?lang=fr
Germania	www.hackerwatch.org/?lang=de
Gran Bretagna	www.hackerwatch.org
Olanda	www.hackerwatch.org/?lang=nl
Italia	www.hackerwatch.org/?lang=it
Giappone	www.hackerwatch.org/?lang=jp
Corea	www.hackerwatch.org/?lang=ko
Messico	www.hackerwatch.org/?lang=es-mx
Norvegia	www.hackerwatch.org/?lang=no
Polonia	www.hackerwatch.org/?lang=pl
Portogallo	www.hackerwatch.org/?lang=pt-pt
Spagna	www.hackerwatch.org/?lang=es
Svezia	www.hackerwatch.org/?lang=sv

Turchia	www.hackerwatch.org/?lang=tr
Stati Uniti	www.hackerwatch.org

Indice

D

E

F

G

V

W