McAfee®

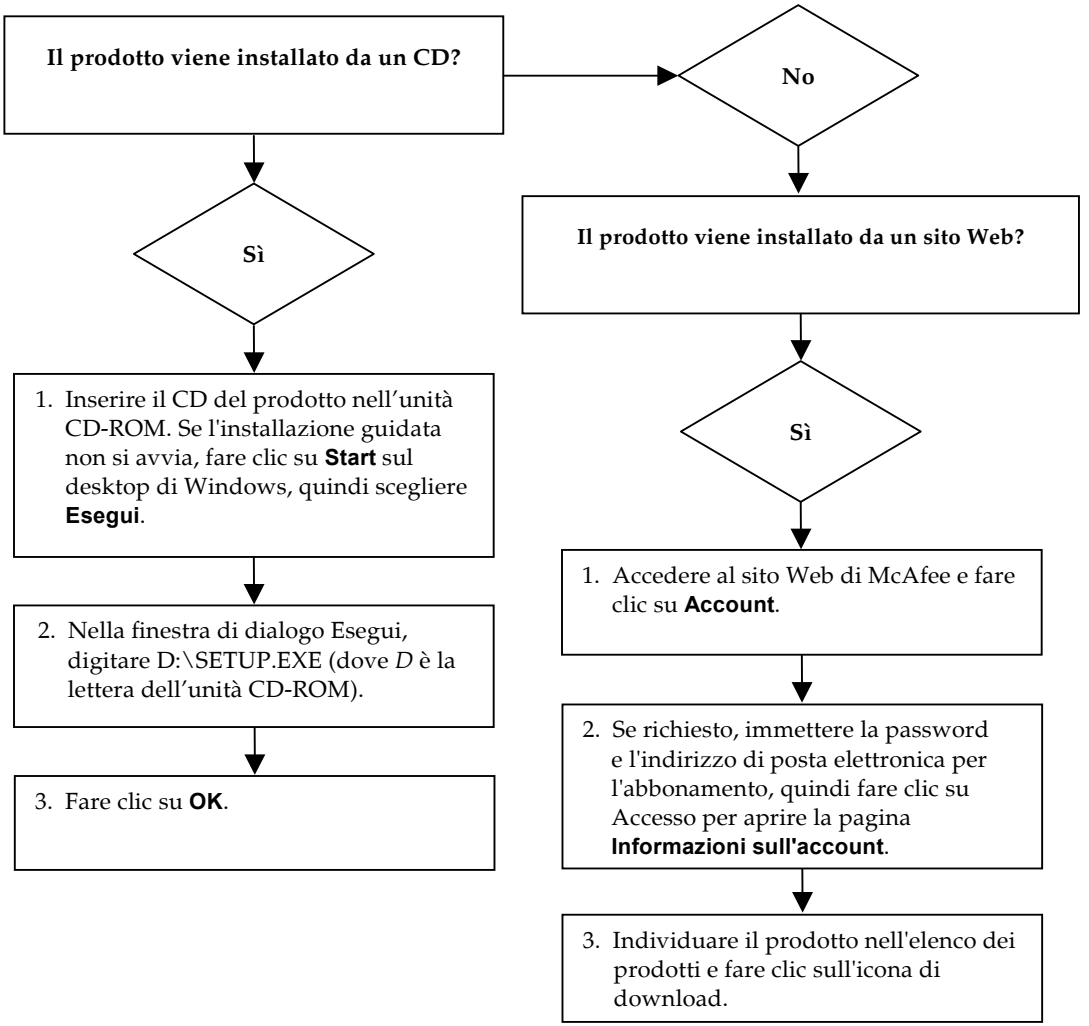
personalfirewallplus

Guida dell'utente

McAfee®

Scheda di avvio rapido

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



Per ulteriori informazioni

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

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

Vantaggi della registrazione

Per inviare la registrazione direttamente a McAfee, si consiglia di attenersi alla facile procedura contenuta nel prodotto acquistato. La registrazione, oltre a garantire l'assistenza tecnica puntuale e competente, offre i seguenti vantaggi:

- Supporto elettronico GRATUITO
- Aggiornamenti dei file di definizione dei virus (.DAT) per un anno dall'installazione quando si acquista il software VirusScan

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

  Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti dei filtri (acquisto online), visitare il sito http://it.mcafee.com.
- Aggiornamenti del pacchetto McAfee Internet Security per un anno dall'installazione quando si acquista il software MIS

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

Supporto tecnico

Per il supporto tecnico, visitare il sito http://www.mcafeeaiuto.com/.

Il sito dell'assistenza consente di accedere 24 ore su 24 alla semplice procedura di risposta guidata alle domande più comuni.

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

Sommario

Informazioni preliminari 1

Benvenuti in McAfee Personal Firewall Plus.

Il software McAfee Personal Firewall Plus 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.

Grazie a questo software, è possibile usufruire delle seguenti funzioni:

- Difende dagli attacchi degli hacker
- Completa la difesa antivirus
- Controlla Internet e le attività della rete
- Segnala eventi potenzialmente dannosi
- Fornisce informazioni dettagliate sul traffico Internet sospetto
- Integra la funzionalità Hackerwatch.org, che include la creazione di rapporti sugli eventi, gli strumenti di test e la possibilità di inviare tramite e-mail gli eventi rilevati ad altre autorità in linea
- Fornisce funzioni dettagliate di ricerca e rintracciamento degli eventi

Nuove funzioni

- **Supporto per i giochi migliorato**
  McAfee Personal Firewall Plus protegge il computer dai tentativi di intrusione e dalle attività sospette durante l'esecuzione di giochi a schermo intero, ma può nascondere gli avvisi se rileva tentativi di intrusione o attività sospette. Gli avvisi vengono visualizzati dopo aver chiuso il gioco.

- **Gestione dell'accesso a Internet migliorata**
  McAfee Personal Firewall Plus consente agli utenti di concedere in modo dinamico alle applicazioni l'accesso temporaneo a Internet. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa. Se Personal Firewall rileva un programma sconosciuto, che sta tentando di comunicare con Internet, un avviso rosso offre l'opzione di concedere all'applicazione l'accesso temporaneo a Internet.

- **Controllo della protezione potenziato**
  Se si esegue la funzione di blocco, McAfee Personal Firewall Plus consente di bloccare immediatamente tutto il traffico Internet in ingresso e in uscita tra il computer e Internet. Gli utenti possono attivare e disattivare il blocco direttamente da queste tre posizioni in Personal Firewall.

- **Opzioni di recupero migliorate**
  È possibile eseguire le Opzioni di ripristino per ripristinare automaticamente le impostazioni predefinite in Personal Firewall. Se Personal Firewall mostra un comportamento diverso da quello previsto, che non è possibile correggere, è possibile annullare le impostazioni correnti e tornare alle impostazioni predefinite del programma.

- **Protezione della connettività Internet**
  Per evitare che un utente disattivi inavvertitamente la connessione Internet, se Personal Firewall rileva che una connessione Internet viene originata da un server DHCP o DNS, l'opzione di escludere un indirizzo Internet non viene inclusa negli avvisi blu. Se il traffico in ingresso non viene originato da un server DHCP o DNS, viene visualizzata l'opzione.

- **Integrazione con HackerWatch.org potenziata**
  La segnalazione di potenziali hacker è più facile che mai. McAfee Personal Firewall Plus migliora la funzionalità di HackerWatch.org, che comprende l'invio di eventi potenzialmente dannosi al database.

- **Gestione intelligente delle applicazioni estesa**
  Quando un'applicazione tenta di accedere a Internet, Personal Firewall verifica se è affidabile o dannosa. Se viene riconosciuta come affidabile, Personal Firewall ne consente automaticamente l'accesso a Internet, senza che sia necessario l'intervento dell'utente.

- **Rilevamento avanzato dei cavalli di Troia**
  McAfee Personal Firewall Plus combina la gestione delle connessioni delle applicazioni con un database potenziato per rilevare e bloccare l'accesso a Internet e la possibile ritrasmissione di dati personali da parte di più applicazioni potenzialmente dannose, ad esempio i cavalli di Troia.

- **Miglioramento di Visual Trace**
  Visual Trace comprende mappe grafiche intuitive che illustrano l'origine degli attacchi ostili e il traffico a livello mondiale, incluse informazioni dettagliate sul contatto/proprietario, a partire dagli indirizzi IP di origine.

- **Maggiore facilità d'uso**
  McAfee Personal Firewall Plus comprende un Assistente di installazione e un'Esercitazione per gli utenti che facilitano l'installazione e l'uso del firewall. Il prodotto è stato progettato per essere utilizzato senza alcun intervento, tuttavia McAfee offre una vasta gamma di risorse che permettono di capire e apprezzare le capacità del firewall.

- **Rilevamento intrusioni migliorato**
  Il Sistema di rilevamento intrusioni (IDS) di Personal Firewall rileva i più comuni tipi di attacco e altre attività sospette. Il rilevamento intrusioni controlla la presenza di trasferimenti di dati o metodi di trasferimento sospetti in ogni pacchetto di dati e li inserisce nel registro degli eventi.

- **Analisi del traffico potenziata**
  McAfee Personal Firewall Plus offre agli utenti una visualizzazione dei dati in ingresso e in uscita dei computer, nonché una visualizzazione delle connessioni delle applicazioni comprese quelle attivamente "in ascolto" di connessioni aperte. In questo modo gli utenti possono vedere quali sono le applicazioni aperte a un'eventuale intrusione e intervenire di conseguenza.

Requisiti di sistema

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

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

Disinstallazione di altri firewall

Prima di installare il software McAfee Personal Firewall Plus, è necessario disinstallare eventuali altri programmi firewall presenti sul computer. Seguire le istruzioni di disinstallazione del programma firewall.

NOTA
Se si utilizza Windows XP, non è necessario disattivare il firewall incorporato prima di installare McAfee Personal Firewall Plus. Tuttavia, si consiglia di farlo. In caso contrario, non si riceveranno gli eventi nel registro eventi in ingresso di McAfee Personal Firewall Plus.

Impostazione del firewall predefinito

McAfee Personal Firewall è in grado di gestire le autorizzazioni e il traffico per le applicazioni Internet presenti sul computer anche se Windows Firewall è in esecuzione.

Una volta installato, McAfee Personal Firewall disattiva automaticamente Windows Firewall e viene impostato come firewall predefinito. È quindi possibile utilizzare solo le funzionalità e i messaggi di McAfee Personal Firewall. Se in seguito si attiva Windows Firewall mediante Windows Security Center o il Pannello di controllo di Windows, l'esecuzione di entrambi i firewall sul computer potrebbe causare una parziale perdita di registrazione in McAfee Firewall, nonché la duplicazione di messaggi di stato e di avviso.

NOTA

Se entrambi i firewall sono attivati, McAfee Personal Firewall non visualizza tutti gli indirizzi IP bloccati nella scheda Eventi in ingresso. Windows Firewall intercetta e blocca la maggior parte di questi eventi, impedendo a McAfee Personal Firewall di rilevarli o registrarli. McAfee Personal Firewall potrebbe tuttavia bloccare e registrare ulteriore traffico in base ad altri fattori di sicurezza.

In Windows Firewall la registrazione è disattivata per impostazione predefinita, ma se si attivano entrambi i firewall è possibile attivare tale registrazione. Il percorso del registro di Windows Firewall predefinito è C:\Windows\pfirewall.log.

Per garantire che il computer sia protetto da almeno un firewall, Windows Firewall viene automaticamente riattivato quando si disinstalla McAfee Personal Firewall.

Se si disattiva McAfee Personal Firewall o si imposta il livello di protezione su **Aperto** senza attivare manualmente Windows Firewall, l'intera protezione del firewall viene rimossa a eccezione delle applicazioni bloccate in precedenza.

Impostazione del livello di protezione

È possibile configurare le opzioni di protezione per indicare la modalità di risposta di Personal Firewall quando rileva traffico indesiderato. Per impostazione predefinita, è attivato il livello di protezione **Standard**. Con il livello di protezione **Standard**, quando si consente a un'applicazione l'accesso a Internet, si tratta dell'accesso completo. L'accesso completo consente all'applicazione di inviare e ricevere dati non richiesti su porte non di sistema.

Per configurare le impostazioni di protezione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Opzioni**.

2. Fare clic sull'icona **Impostazioni protezione**.

3. Impostare il livello di protezione desiderato utilizzando il dispositivo di scorrimento.

   La gamma di livelli di protezione va da Blocco ad Aperto:

   - **Blocco:** tutte le connessioni a Internet sul computer vengono chiuse. È possibile utilizzare questa impostazione per bloccare porte configurate per essere aperte nella pagina Servizi di sistema.

   - **Protezione elevata:** se un'applicazione richiede solo un tipo di accesso a Internet specifico (ad esempio Solo accesso in uscita), è possibile concedere o meno una connessione Internet all'applicazione. Se in seguito l'applicazione richiede l'accesso completo, è possibile concederlo o mantenere solo l'accesso in uscita.

   - **Protezione standard (impostazione consigliata):** se un'applicazione richiede l'accesso a Internet e questo le viene concesso, si tratta dell'accesso completo per gestire il traffico in ingresso e in uscita.

   - **Protezione su affidabilità:** tutte le applicazioni vengono automaticamente ritenute affidabili al primo tentativo di accesso a Internet. È tuttavia possibile configurare Personal Firewall in modo da poter utilizzare gli avvisi per la notifica di nuove applicazioni sul computer. Utilizzare questa impostazione in caso di non funzionamento di alcuni giochi o streaming audio o video.

   - **Aperto:** il firewall è disattivato. Questa impostazione consente il passaggio di tutto il traffico attraverso Personal Firewall senza alcun filtro.

     NOTA
     Quando il livello di protezione del firewall è impostato su **Aperto** o **Blocco**, le applicazioni bloccate in precedenza continuano a essere bloccate. Per impedire che ciò si verifichi, è possibile impostare le autorizzazioni dell'applicazione su **Consenti Accesso completo** oppure eliminare la regola di autorizzazione **Blocco** nell'elenco **Applicazioni Internet**.

4. Selezionare ulteriori impostazioni di protezione:

   NOTA
   se si utilizza Windows XP e sono stati aggiunti più utenti di XP, le opzioni riportate di seguito sono disponibili solo se si accede al computer in qualità di amministratore.

- **Registra eventi di Sistema di rilevamento intrusioni (IDS) nel registro eventi in ingresso:** se si seleziona questa opzione, gli eventi rilevati da IDS vengono visualizzati nel registro eventi in ingresso. Il Sistema di rilevamento delle intrusioni rileva i tipi di attacco comuni e altre attività sospette. Il rilevamento intrusioni verifica tutti i pacchetti di dati in ingresso e in uscita alla ricerca di trasferimenti di dati o metodi di trasferimento sospetti, li confronta con un database di firme ed esclude automaticamente quelli provenienti dal computer che genera l'attacco.

  IDS cerca specifici modelli di traffico utilizzati dagli hacker. IDS verifica tutti i pacchetti ricevuti dal computer alla ricerca di traffico sospetto o attacchi noti. Ad esempio, se Personal Firewall visualizza i pacchetti ICMP, li analizza alla ricerca di modelli di traffico sospetti confrontando il traffico ICMP con modelli di attacco noti.

- **Accetta richieste ping ICMP**: il traffico ICMP viene utilizzato principalmente per l'esecuzione di tracce e ping. Il ping viene spesso utilizzato per eseguire una rapida verifica prima di tentare di stabilire le comunicazioni. Se si utilizza o si è utilizzato un programma di condivisione di file peer-to-peer, è possibile essere spesso oggetto di ping. Se si seleziona questa opzione, Personal Firewall consente tutte le richieste di ping senza registrare i ping nel registro eventi in ingresso. Se l'opzione non è selezionata, Personal Firewall blocca tutte le richieste di ping e registra i ping nel registro eventi in ingresso.

- **Consenti a utenti con restrizioni di modificare impostazioni di Personal Firewall**: se si utilizza Windows XP o Windows 2000 Professional con più utenti, selezionare questa opzione per consentire agli utenti di XP con restrizioni di modificare le impostazioni di Personal Firewall.

5 Dopo aver apportato le modifiche desiderate, fare clic su **OK**.

Verifica di McAfee® Personal Firewall Plus

È possibile verificare l'installazione di Personal Firewall per controllarne la possibile vulnerabilità a intrusioni e attività sospette.

Per verificare l'installazione di Personal Firewall dall'icona McAfee visualizzata nella barra delle applicazioni:

- Fare clic con il pulsante destro del mouse sull'icona McAfee  nella barra delle applicazioni di Windows, e selezionare **Prova firewall**.

Personal Firewall apre Internet Explorer e all'indirizzo http://www.hackerwatch.org/ viene visualizzato il sito Web di HackerWatch gestito da McAfee. Per verificare Personal Firewall, seguire le istruzioni visualizzate nella pagina Test di Hackerwatch.org.

Utilizzo di McAfee SecurityCenter

McAfee SecurityCenter è un punto di riferimento singolo per la protezione, accessibile dalla relativa icona nella barra delle applicazioni di Windows oppure dal desktop di Windows. McAfee SecurityCenter consente di eseguire le seguenti operazioni utili:

- Ottenere l'analisi gratuita del grado di protezione del computer.
- Avviare, gestire e configurare tutti gli abbonamenti a McAfee utilizzando un'unica icona.
- Vedere avvisi sui virus costantemente aggiornati e le ultimissime informazioni sui prodotti.
- Ottenere collegamenti rapidi alle domande frequenti e informazioni sugli account nel sito Web di McAfee.

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

Quando SecurityCenter è in esecuzione e sono attivate tutte le funzioni di McAfee installate sul computer, nella barra delle applicazioni di Windows viene visualizzata un'icona rossa con una M  . Quest'area si trova in genere nell'angolo inferiore destro del desktop di Windows e contiene l'orologio.

In caso di disattivazione di una o più applicazioni McAfee installate nel computer, l'icona McAfee risulterà di colore nero  .

Per avviare McAfee SecurityCenter:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee  , quindi selezionare **Apri SecurityCenter**.

Per avviare Personal Firewall da McAfee SecurityCenter:

1. In SecurityCenter, fare clic sulla scheda **Personal Firewall Plus**.
2. Selezionare un'attività nel menu Desidero.

Per avviare Personal Firewall da Windows:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee  nella barra delle applicazioni di Windows, quindi scegliere **Personal Firewall**.
2. Selezionare un'attività.

Utilizzo di McAfee Personal Firewall Plus

2

Per aprire Personal Firewall:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare un'attività.

Informazioni sulla pagina Riepilogo

Il riepilogo di Personal Firewall comprende quattro pagine riassuntive:

- Riepilogo principale
- Riepilogo applicazione
- Riepilogo eventi
- Riepilogo di HackerWatch

Le pagine Riepilogo contengono una grande varietà di rapporti sugli eventi recenti in ingresso, sullo stato delle applicazioni e sulle attività di intrusione in tutto il mondo segnalate da HackerWatch.org, nonché collegamenti alle operazioni più comuni eseguite in Personal Firewall.

Per aprire la pagina Riepilogo principale in Personal Firewall:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo** (Figura 2-1).

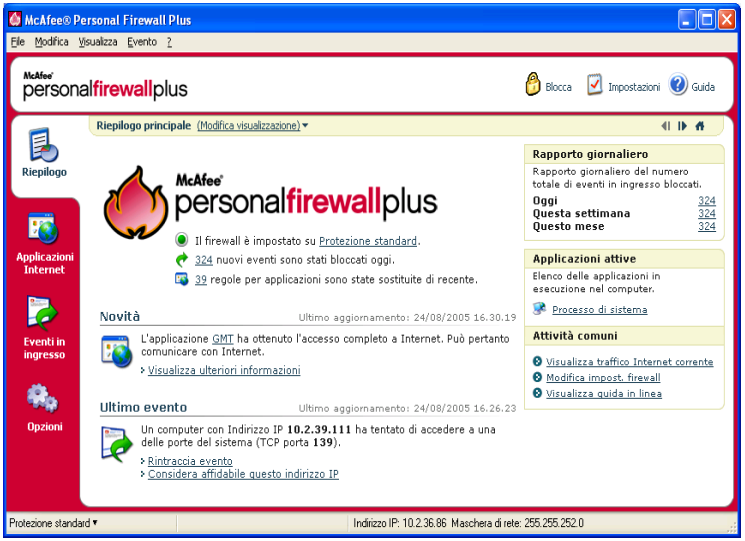


Figura 2-1. Pagina Riepilogo principale

Fare clic sulle seguenti opzioni per accedere alle varie pagine Riepilogo:

Voce	Descrizione
Modifica visualizzazione	Fare clic su **Modifica visualizzazione** per aprire un elenco di pagine Riepilogo. Nell'elenco selezionare una pagina Riepilogo da visualizzare.
Freccia destra	Fare clic sull'icona a forma di freccia rivolta verso destra per visualizzare la pagina Riepilogo successiva.
Freccia sinistra	Fare clic sull'icona a forma di freccia rivolta verso sinistra per visualizzare la pagina Riepilogo precedente.
Home Page	Fare clic sull'icona della home page per tornare alla pagina **Riepilogo principale**.

Nella pagina Riepilogo principale sono disponibili le seguenti informazioni:

Voce	Descrizione
Impostazioni protezione	Lo stato dell'impostazione di protezione indica il livello di protezione su cui è impostato il firewall. Fare clic sul collegamento per modificare il livello di protezione.
Eventi bloccati	Lo stato eventi bloccati visualizza il numero di eventi bloccati nel corso della giornata. Fare clic sul collegamento per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso.
Modifiche regole applicazioni	Lo stato della regola dell'applicazione visualizza il numero di regole applicazioni che sono state modificate di recente. Fare clic sul collegamento per visualizzare l'elenco di applicazioni consentite e bloccate nonché per modificare le autorizzazioni delle applicazioni.
Novità	**Novità** visualizza l'ultima applicazione a cui è stato consentito l'accesso completo a Internet.
Ultimo evento	**Ultimo evento** visualizza gli eventi in ingresso più recenti. È possibile fare clic su un collegamento per rintracciare l'evento o per impostare l'indirizzo IP come affidabile. Se si imposta un indirizzo IP come affidabile, si consente a tutto il traffico che ne proviene di raggiungere il computer.
Rapporto giornaliero	**Rapporto giornaliero** visualizza il numero di eventi in ingresso bloccati da Personal Firewall nel corso della giornata, nella settimana e nel mese in corso. Fare clic sul collegamento per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso.

Voce	Descrizione
Applicazioni attive	**Applicazioni attive** visualizza le applicazioni attualmente in esecuzione nel computer e connesse a Internet. Fare clic su un'applicazione per visualizzare gli indirizzi IP a cui l'applicazione è connessa.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per andare alla pagina di Personal Firewall in cui è possibile visualizzare l'attività del firewall ed eseguire le attività.

Per visualizzare la pagina Riepilogo applicazione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo applicazione**.

Nella pagina Riepilogo applicazione sono disponibili le seguenti informazioni:

Voce	Descrizione
Controllo traffico	**Controllo traffico** visualizza le connessioni Internet in ingresso e in uscita nel corso degli ultimi quindici minuti. Fare clic sul grafico per visualizzare i dettagli di controllo del traffico.
Applicazioni attive	**Applicazioni attive** visualizza l'utilizzo della larghezza di banda delle applicazioni più attive del computer nel corso delle ultime 24 ore. **Applicazione**: l'applicazione che accede a Internet. **%**: la percentuale di larghezza di banda utilizzata dall'applicazione. **Autorizzazione**: il tipo di accesso a Internet consentito all'applicazione. **Regola creata**: data e ora di creazione della regola per l'applicazione.
Novità	**Novità** visualizza l'ultima applicazione a cui è stato consentito l'accesso completo a Internet.
Applicazioni attive	**Applicazioni attive** visualizza le applicazioni attualmente in esecuzione nel computer e connesse a Internet. Fare clic su un'applicazione per visualizzare gli indirizzi IP a cui l'applicazione è connessa.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per andare alle pagine di Personal Firewall in cui è possibile vedere lo stato dell'applicazione ed eseguire attività relative all'applicazione.

Per visualizzare la pagina Riepilogo eventi:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo eventi**.

Nella pagina Riepilogo eventi sono disponibili le seguenti informazioni:

Voce	Descrizione
Confronto porte	**Confronto porte** visualizza un grafico a torta relativo alle porte del computer in uso su cui è stato effettuato il maggior numero di tentativi nel corso degli ultimi 30 giorni. È possibile fare clic sul nome di una porta per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso. È inoltre possibile spostare il puntatore del mouse sul numero di una porta per visualizzarne una descrizione.
Principali eventi	**Principali eventi** visualizza gli indirizzi IP bloccati più di frequente, la data e l'ora in cui si è verificato l'ultimo evento in ingresso per ogni indirizzo e il numero totale di eventi in ingresso nel corso degli ultimi trenta giorni per ogni indirizzo. Fare clic su un evento per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso.
Rapporto giornaliero	**Rapporto giornaliero** visualizza il numero di eventi in ingresso bloccati da Personal Firewall nel corso della giornata, nella settimana e nel mese in corso. Fare clic su un numero per visualizzare i dettagli dell'evento provenienti dalla pagina Eventi in ingresso.
Ultimo evento	**Ultimo evento** visualizza gli eventi in ingresso più recenti. È possibile fare clic su un collegamento per rintracciare l'evento o per impostare l'indirizzo IP come affidabile. Se si imposta un indirizzo IP come affidabile, si consente a tutto il traffico che ne proviene di raggiungere il computer.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per accedere alle pagine di Personal Firewall in cui è possibile visualizzare i dettagli degli eventi ed eseguire attività relative agli eventi.

Per visualizzare la pagina Riepilogo di HackerWatch:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo di HackerWatch**.

Nella pagina Riepilogo di HackerWatch sono disponibili le informazioni seguenti.

Voce	Descrizione
Attività a livello mondiale	**Attività a livello mondiale** visualizza una mappa mondiale in cui sono identificate le attività bloccate di recente controllate da HackerWatch.org. Fare clic sulla mappa per aprire la mappa di Analisi delle minacce globali in HackerWatch.org.
Traccia degli eventi	**Traccia degli eventi** visualizza il numero di eventi in ingresso inviati a HackerWatch.org.
Attività globale delle porte	**Attività globale delle porte** visualizza le porte principali che sono state minacciate nel corso degli ultimi cinque giorni. Fare clic su una porta per visualizzarne il numero e la descrizione.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per accedere alle pagine di HackerWatch.org in cui è possibile ottenere ulteriori informazioni sulle attività degli hacker in tutto il mondo.

Informazioni sulla pagina Applicazioni Internet

Nella pagina Applicazioni Internet viene visualizzato l'elenco delle applicazioni autorizzate e bloccate.

Per avviare la pagina Applicazioni Internet:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni** (Figura 2-2).

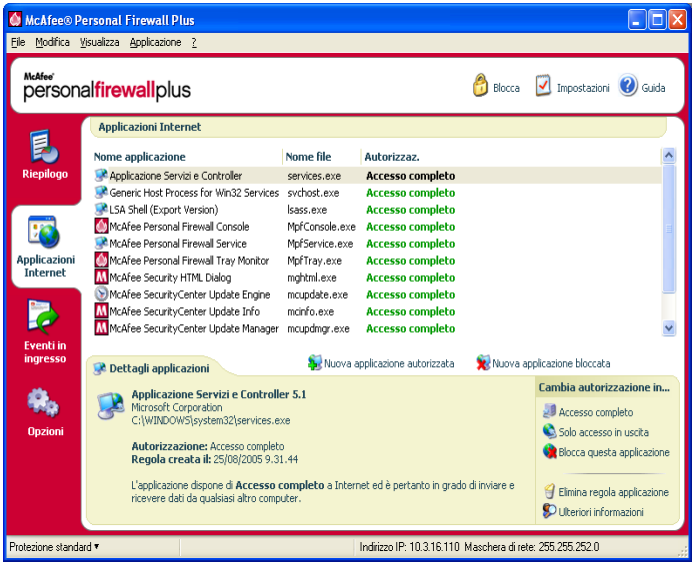


Figura 2-2. Pagina Applicazioni Internet

Nella pagina Applicazioni Internet sono disponibili le seguenti informazioni:

- Nomi delle applicazioni
- Nomi dei file
- Livelli di autorizzazione correnti
- Dettagli sulle applicazioni: nome e versione dell'applicazione, nome della società, nome del percorso, timestamp e spiegazione dei tipi di autorizzazione

Modifica delle regole delle applicazioni

Personal Firewall consente di modificare le regole di accesso per le applicazioni.

Per modificare la regola di un'applicazione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.
2. Nell'elenco **Applicazioni Internet**, fare clic con il pulsante destro del mouse sulla regola di un'applicazione e selezionare un livello diverso:
   - **Accesso completo:** consente all'applicazione di stabilire connessioni Internet in uscita e in ingresso.
   - **Solo accesso in uscita:** consente all'applicazione di stabilire solo una connessione Internet in uscita.
   - **Blocca questa applicazione:** non consente all'applicazione di accedere a Internet.

     NOTA
     Quando il livello di protezione del firewall è impostato su **Aperto** o **Blocco**, le applicazioni bloccate in precedenza continuano a essere bloccate. Per impedire che ciò si verifichi, è possibile impostare la regola di accesso dell'applicazione su **Accesso completo** oppure eliminare la regola di autorizzazione **Blocco** dall'elenco **Applicazioni Internet**.

Per eliminare la regola di un'applicazione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.
2. Nell'elenco **Applicazioni Internet**, fare clic con il pulsante destro del mouse sulla regola dell'applicazione, quindi selezionare **Elimina regola applicazione**.

Alla successiva richiesta di accesso a Internet da parte dell'applicazione, sarà possibile impostarne il livello di autorizzazione per aggiungerla nuovamente all'elenco.

Autorizzazione e blocco delle applicazioni Internet

Per modificare l'elenco delle applicazioni Internet autorizzate e bloccate:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.
2. Nella pagina Applicazioni Internet, fare clic su una delle seguenti opzioni:
   - **Nuova applicazione autorizzata**: consente all'applicazione l'accesso completo a Internet.
   - **Nuova applicazione bloccata**: non consente all'applicazione di accedere a Internet.
   - **Elimina regola applicazione**: consente di rimuovere la regola di un'applicazione.

Pagina Informazioni sugli eventi in ingresso

Utilizzare la pagina Eventi in ingresso per visualizzare il registro eventi in ingresso generato quando le connessioni Internet non richieste vengono bloccate da Personal Firewall.

Per aprire la pagina Eventi in ingresso:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso** (Figura 2-3).

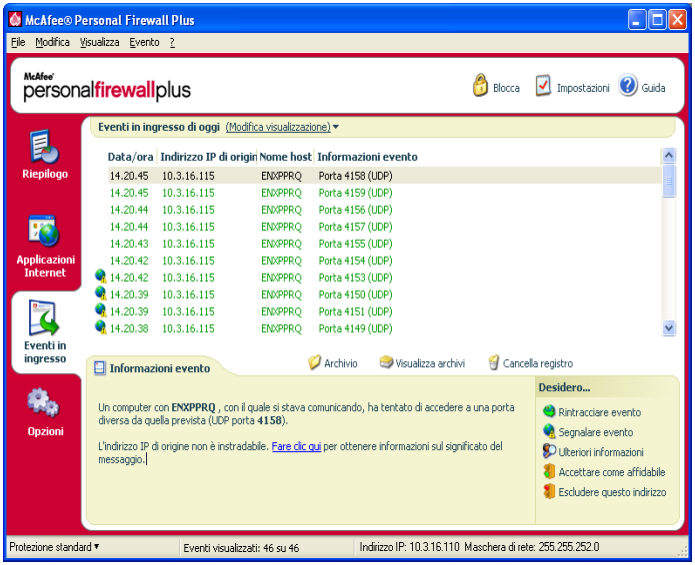


Figura 2-3. Eventi in ingresso di oggi

Nella pagina Eventi in ingresso di oggi sono disponibili le seguenti informazioni:

- Data/ora
- Indirizzo IP di origine
- Nome host
- Nomi dei servizi o delle applicazioni
- Informazioni evento: tipi di connessione, porte di connessione, nome host o IP e spiegazione del significato degli eventi relativi alle varie porte

Il significato degli eventi

Informazioni sugli indirizzi IP

Gli indirizzi IP sono numeri. Per la precisione, sono costituiti da quattro numeri compresi tra 0 e 255. Tali numeri indicano una destinazione precisa a cui può essere indirizzato il traffico su Internet.

Tipi indirizzo IP

Numerosi indirizzi IP sono considerati speciali per varie ragioni:

Non istradabili: detti anche “spazi IP privati”. Questi indirizzi IP non possono essere utilizzati in Internet. I blocchi privati sono 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.

Indirizzi IP di loop-back: gli indirizzi di loop-back vengono utilizzati a scopo di test. Il traffico inviato a questo blocco di indirizzi IP torna subito al dispositivo che genera il pacchetto, non lascia mai il dispositivo e viene utilizzato principalmente per test di hardware e software. Il blocco di indirizzi IP di loop-back è 127.x.x.x.

Indirizzo IP nullo: si tratta di un indirizzo non valido. Una volta rilevato, Personal Firewall indica che il traffico utilizzava un indirizzo IP vuoto. Spesso questa situazione indica che l'origine del traffico viene deliberatamente nascosta dal mittente. Il mittente non sarà in grado di ricevere risposte al traffico, a meno che il pacchetto non venga ricevuto da un'applicazione in grado di comprendere i contenuti del pacchetto in cui sono incluse istruzioni specifiche per tale applicazione. Qualsiasi indirizzo che inizi per 0 (0.x.x.x) è un indirizzo nullo. Ad esempio, 0.0.0.0 è un indirizzo IP nullo.

Eventi da 0.0.0.0

Due sono le cause più probabili per il rilevamento di eventi dall'indirizzo IP 0.0.0.0. La prima causa, più comune, è che il computer abbia ricevuto un pacchetto non corretto. Internet non è sempre affidabile al 100% ed è possibile che vengano inoltrati pacchetti non validi. Poiché i pacchetti vengono esaminati da Personal Firewall prima della convalida da parte di TCP/IP, è possibile che vengano segnalati come evento.

Nel secondo caso, l'indirizzo IP di origine ha subito un attacco di tipo spoofing, ovvero è stato contraffatto. I pacchetti contraffatti possono indicare la scansione in corso del computer alla ricerca di cavalli di Troia. Personal Firewall blocca questo tipo di attività, quindi il computer in uso è sicuro.

Eventi da 127.0.0.1

Alcuni eventi vengono generati dall'indirizzo IP 127.0.0.1. Questo viene chiamato indirizzo di loopback o localhost.

Molti programmi legittimi utilizzano infatti l'indirizzo di loopback per la comunicazione fra i componenti. Ad esempio, è possibile configurare molti server e-mail o Web tramite un'interfaccia Web. Per accedere all'interfaccia, digitare “http://localhost/” nel browser Web.

Il traffico proveniente da tali programmi viene autorizzato da Personal Firewall. Quindi se si rilevano eventi da 127.0.0.1, è probabile che l'indirizzo IP di origine sia stato sottoposto a spoofing, ossia che sia contraffatto. I pacchetti contraffatti indicano in genere che un altro computer sta eseguendo la scansione del proprio computer alla ricerca di cavalli di Troia. Personal Firewall blocca questi tentativi di intrusione, quindi il computer in uso è sicuro.

Esistono programmi, come Netscape 6.2 e versioni successive, che richiedono l'aggiunta di 127.0.0.1 all'elenco degli indirizzi IP affidabili. La modalità di comunicazione tra i componenti di tali programmi non consente a Personal Firewall di determinare se si tratti o meno di traffico locale.

Nel caso di Netscape 6.2, se non si imposta 127.0.0.1 come affidabile, non sarà possibile utilizzare l'elenco degli amici. Se si rileva quindi traffico proveniente da 127.0.0.1 e tutte le applicazioni del computer funzionano normalmente, è possibile bloccare tale traffico senza che si verifichino problemi. Se tuttavia in un programma, ad esempio Netscape, si verificano problemi, aggiungere 127.0.0.1 all'elenco Indirizzi IP affidabili di Personal Firewall, quindi verificare se i problemi sono stati risolti.

Se l'inserimento di 127.0.0.1 nell'elenco degli indirizzi IP affidabili consente di risolvere il problema, è necessario valutare attentamente le opzioni disponibili. Se si imposta 127.0.0.1 come affidabile, il programma funzionerà correttamente, ma si sarà più vulnerabili ad attacchi di spoofing. Se non si ritiene affidabile l'indirizzo, il programma non funzionerà correttamente, ma si sarà protetti dal traffico dannoso.

Eventi dai computer nella LAN

Gli eventi possono essere generati dai computer presenti nella LAN. Per mostrare che questi eventi provengono dalla rete, Personal Firewall li visualizza in verde.

Nella maggior parte delle configurazioni LAN aziendali si consiglia di selezionare la casella di controllo **Considera affidabili tutti i computer della LAN** nella finestra di dialogo Indirizzi IP affidabili.

In determinate situazioni, la rete "locale" può essere tanto pericolosa quanto Internet, soprattutto se si utilizza una rete DSL o con modem via cavo a larghezza di banda elevata. In questo caso, non selezionare **Considera affidabili tutti i computer della LAN**. Aggiungere invece gli indirizzi IP dei computer locali all'elenco degli indirizzi IP affidabili.

Eventi dagli indirizzi IP privati

Gli indirizzi IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx, e 172.16.0.0 - 172.31.255.255 sono detti non instradabili o privati. Tali indirizzi IP non dovrebbero mai lasciare la rete e possono essere considerati quasi sempre affidabili.

Il blocco 192.168 xxx.xxx viene utilizzato con Condivisione connessione Internet di Microsoft. Se si utilizza Condivisione connessione Internet e si rilevano eventi provenienti da tale blocco IP, è possibile aggiungere l'indirizzo IP 192.168.255.255 all'elenco degli indirizzi IP affidabili. In tal modo verrà impostato come affidabile l'intero blocco 192.168.xxx.xxx.

Se non si è connessi a una rete privata e si rilevano eventi provenienti da tali intervalli IP, è possibile che gli indirizzi IP di origine siano stati sottoposti a spoofing, ossia che siano contraffatti. I pacchetti contraffatti indicano in genere una scansione per la ricerca di cavalli di Troia. È importante ricordare che tale tentativo è stato bloccato da Personal Firewall, quindi il computer in uso è sicuro.

Poiché gli indirizzi IP privati fanno riferimento a computer diversi a seconda della rete a cui si è connessi, la segnalazione di tali eventi risulta inutile, quindi non viene effettuata.

Visualizzazione degli eventi nel registro eventi in ingresso

Nel registro eventi in ingresso, gli eventi vengono visualizzati in numerosi modi diversi. La visualizzazione predefinita mostra solo gli eventi che si verificano nel corso della giornata. È possibile visualizzare anche gli eventi che si sono verificati durante la settimana scorsa oppure il registro completo.

Grazie a Personal Firewall è inoltre possibile visualizzare eventi in ingresso relativi a giorni specifici, provenienti da specifici indirizzi Internet (indirizzi IP) o contenenti le stesse informazioni sull'evento.

Per informazioni su un evento, fare clic sull'evento. Le informazioni verranno visualizzate nel riquadro **Informazioni evento**.

Visualizzazione degli eventi del giorno

Utilizzare questa opzione per rivedere gli eventi del giorno.

Per visualizzare gli eventi del giorno:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra eventi di oggi**.

Visualizzazione degli eventi della settimana

Utilizzare questa opzione per rivedere gli eventi settimanali.

Per visualizzare gli eventi della settimana:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra eventi di questa settimana**.

Visualizzazione del registro eventi in ingresso completo

Utilizzare questa opzione per rivedere tutti gli eventi.

Per mostrare tutti gli eventi nel registro eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra registro completo**.

   Il registro degli eventi in ingresso visualizza tutti gli eventi del registro.

Visualizzazione degli eventi di un giorno specifico

Utilizzare questa opzione per rivedere gli eventi di un giorno specifico.

Per visualizzare gli eventi di un giorno specifico:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi del giorno selezionato**.

Visualizzazione degli eventi di un indirizzo Internet specifico

Utilizzare questa opzione per rivedere gli eventi che vengono originati da un particolare indirizzo Internet.

Per mostrare gli eventi di un indirizzo Internet:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, e fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi dell'indirizzo Internet selezionato**.

Visualizzazione di eventi con le stesse informazioni sull'evento

Utilizzare questa opzione per rivedere gli eventi nel registro degli eventi in ingresso per i quali nella colonna Informazioni evento sono riportate le stesse informazioni dell'evento selezionato. È possibile verificare quante volte si è verificato l'evento e se proviene dalla stessa origine. La colonna Informazioni evento contiene una descrizione dell'evento e, se noto, il programma o il servizio comune che utilizza la porta interessata.

Per visualizzare gli eventi con le stesse informazioni sull'evento:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, e fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi con le stesse informazioni sull'evento**.

Risposta agli eventi in ingresso

Oltre a rivedere informazioni dettagliate sugli eventi visualizzati nel registro eventi in ingresso, è possibile creare con Visual Trace una traccia degli indirizzi IP di un evento del registro eventi in ingresso oppure ottenere informazioni sull'evento visitando HackerWatch.org, il sito Web della comunità on-line per la protezione dagli attacchi degli hacker.

Rintracciamento dell'evento selezionato

È possibile tentare di creare con Visual Trace una traccia visuale degli indirizzi IP relativi a un evento riportato nel registro eventi in ingresso.

Per creare la traccia di un evento selezionato:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, e selezionare **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse sull'evento per il quale si desidera creare una traccia, quindi fare clic su **Rintraccia evento selezionato**. Per creare la traccia di un evento, è possibile anche fare doppio clic sull'evento.

Per impostazione predefinita, la traccia visuale viene avviata in Personal Firewall mediante il programma Visual Trace di Personal Firewall.

Suggerimenti da HackerWatch.org

Per ottenere suggerimenti da HackerWatch.org:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, e selezionare **Eventi in ingresso**.
2. Selezionare l'evento nella pagina Eventi in ingresso, quindi fare clic su **Ulteriori informazioni** nel riquadro **Desidero**.

Il browser Web predefinito verrà aperto e verrà visualizzato il sito Web HackerWatch.org in cui sono disponibili informazioni relative al tipo di evento e suggerimenti relativi all'opportunità di segnalare l'evento.

Segnalazione di un evento

Per segnalare un evento che si ritiene essere un attacco al computer in uso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, e selezionare **Eventi in ingresso**.
2. Fare clic sull'evento che si desidera segnalare, quindi fare clic su **Segnalare evento** nel riquadro **Desidero**.

Personal Firewall segnala l'evento al sito Web HackerWatch.org, utilizzando l'ID univoco del computer in uso.

Registrazione a HackerWatch.org

Alla prima apertura della pagina Riepilogo, HackerWatch.org verrà contattato da Personal Firewall per generare un ID utente univoco. Se si è già utenti registrati, la richiesta di accesso verrà convalidata automaticamente. Ai nuovi utenti viene richiesta l'immissione di uno pseudonimo e di un indirizzo di e-mail. Per utilizzare le funzionalità di filtro e di invio tramite e-mail degli eventi disponibili nel sito Web sarà quindi necessario fare clic sul collegamento di convalida disponibile nel messaggio di e-mail di conferma di HackerWatch.org.

È possibile segnalare l'evento al sito Web HackerWatch.org senza convalidare l'ID utente. Tuttavia, per filtrare gli eventi e inviare un messaggio di e-mail a un amico, è necessario abbonarsi al servizio.

L'abbonamento a tale servizio consente di tenere traccia delle segnalazioni inviate e di ricevere avvisi, nel caso in cui a HackerWatch.org siano necessarie più informazioni o ulteriori azioni da parte dell'utente. L'abbonamento consente inoltre di verificare tutte le informazioni ricevute, in modo da poterle utilizzare.

Tutti gli indirizzi di e-mail forniti a HackerWatch.org rimangono riservati. Se una richiesta di ulteriori informazioni viene inviata da un ISP, tale richiesta viene reindirizzata tramite HackerWatch.org, in modo da non esporre mai l'indirizzo di e-mail degli utenti.

Considerare affidabile un indirizzo

È possibile utilizzare la pagina Eventi in ingresso per aggiungere un indirizzo IP all'elenco degli indirizzi IP affidabili e consentire una connessione permanente.

Se nella pagina Eventi in ingresso viene individuato un evento contenente un indirizzo IP che si desidera autorizzare, è possibile impostare Personal Firewall in modo che le connessioni da tale indirizzo siano consentite in qualunque momento.

Per aggiungere un indirizzo IP all'elenco degli indirizzi IP affidabili:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, e selezionare **Eventi in ingresso**.
2. Fare clic con il pulsante destro del mouse sull'evento contenente l'indirizzo IP da impostare come affidabile e scegliere **Considera affidabile l'indirizzo IP di origine**.

Verificare che l'indirizzo IP visualizzato nel messaggio di conferma Accettare come affidabile sia corretto, quindi fare clic su **OK**. L'indirizzo IP viene aggiunto all'elenco.

Per assicurarsi che l'indirizzo IP sia stato aggiunto:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, e selezionare **Opzioni**.
2. Fare clic sull'icona **IP affidabili ed esclusi**, quindi sulla scheda **Indirizzi IP affidabili**.

L'indirizzo IP verrà visualizzato come attivato nell'elenco degli indirizzi IP affidabili.

Esclusione di un indirizzo

Se nel registro eventi in ingresso viene visualizzato un indirizzo IP, questo significa che il traffico proveniente da tale indirizzo è stato bloccato. Pertanto, l'esclusione di un indirizzo non aggiunge ulteriore protezione a meno che il computer non abbia porte deliberatamente aperte dalla funzione Servizi di sistema o un'applicazione autorizzata a ricevere dati.

Aggiungere un indirizzo IP all'elenco di esclusione solo se si dispone di una o più porte deliberatamente aperte e se si ha motivo di credere che sia necessario bloccarle.

Se nella pagina Eventi in ingresso viene individuato un evento contenente un indirizzo IP che si desidera escludere, è possibile configurare Personal Firewall in modo che le connessioni da tale indirizzo non siano mai consentite.

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.

Per aggiungere un indirizzo IP all'elenco degli indirizzi IP esclusi:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. La pagina Eventi in ingresso elenca gli indirizzi IP del traffico Internet in ingresso. Selezionare un indirizzo IP, quindi eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse sull'indirizzo IP, quindi selezionare **Escludi l'indirizzo IP di origine**.
   - Fare clic su **Escludere questo indirizzo** nel menu **Desidero**.

3 Nella finestra di dialogo Aggiungi regola indirizzi IP esclusi, utilizzare una o più delle seguenti impostazioni per configurare la regola dell'indirizzo IP escluso:

- **Indirizzo IP singolo**: l'indirizzo IP da escludere. L'indirizzo predefinito è quello selezionato nella pagina Eventi in ingresso.
- **Intervallo di indirizzi IP**: gli indirizzi IP tra l'indirizzo specificato in Da indirizzo IP e l'indirizzo specificato in A indirizzo IP.
- **Data scadenza regola**: data e ora in cui la regola dell'indirizzo IP escluso scade. Per selezionare la data e l'ora, selezionare i menu a discesa appropriati.
- **Descrizione**: se lo si desidera, descrivere la nuova regola.
- Fare clic su **OK**.

4 Nella finestra di dialogo, fare clic su **Sì** per confermare l'impostazione. Fare clic su **No** per tornare alla finestra di dialogo Aggiungi regola indirizzi IP esclusi.

Se Personal Firewall rileva un evento proveniente da una connessione Internet esclusa, invierà un avviso in base al metodo specificato nella pagina Impostazioni avviso.

Per assicurarsi che l'indirizzo IP sia stato aggiunto:

1 Fare clic sulla scheda **Opzioni**.

2 Fare clic sull'icona **IP affidabili ed esclusi**, quindi sulla scheda **Indirizzi IP esclusi**.

L'indirizzo IP verrà visualizzato come attivato nell'elenco degli indirizzi IP esclusi.

Gestione del registro eventi in ingresso

È possibile utilizzare la pagina Eventi in ingresso per gestire gli eventi del registro eventi in ingresso generati quando il traffico Internet non richiesto viene bloccato da Personal Firewall.

Archiviazione del registro eventi in ingresso

È possibile archiviare il registro degli eventi in ingresso corrente per salvare tutti gli eventi in ingresso registrati, incluse la data e le ore, gli IP di origine, i nomi host, le porte e le informazioni sull'evento. Il registro degli eventi in ingresso va archiviato periodicamente per evitare che diventi troppo grande.

Per archiviare il registro eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee ella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso** .
2. Nella pagina Eventi in ingresso, fare clic su **Archivio**.
3. Nella finestra di dialogo Archivia registro, fare clic su **Sì** per procedere con l'operazione.
4. Fare clic su **Salva** per salvare l'archivio nel percorso predefinito oppure scegliere un percorso in cui salvare l'archivio.

Nota: per impostazione predefinita, Personal Firewall archivia automaticamente il registro degli eventi in ingresso. Selezionare o deselezionare **Archivia automaticamente gli eventi registrati** nella pagina Impostazioni registro eventi per attivare o disattivare l'opzione.

Visualizzazione dei registri eventi in ingresso archiviati

È possibile visualizzare i registri eventi in ingresso archiviati in precedenza. L'archivio salvato include la data e le ore, gli IP di origine, i nomi host, le porte e le informazioni sugli eventi.

Per visualizzare il registro degli eventi in ingresso archiviato:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina Eventi in ingresso, fare clic su **Visualizza archivi**.
3. Selezionare o cercare il nome file dell'archivio e fare clic su **Apri**.

Cancellazione del registro eventi in ingresso

È possibile cancellare tutte le informazioni dal registro eventi in ingresso.

ATTENZIONE: una volta cancellato il registro eventi in ingresso, non sarà possibile recuperarne il contenuto. Se si ritiene di averne bisogno in futuro, si consiglia di archiviare il registro eventi anziché cancellarlo.

Per cancellare il registro eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina Eventi in ingresso, fare clic su **Cancella registro**.
3. Fare clic su **Sì** nella finestra di dialogo per cancellare il registro.

Copia di un evento negli Appunti

È possibile copiare un evento negli Appunti per incollarlo in un file di testo utilizzando il Blocco note.

Per copiare gli eventi negli appunti:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Fare clic con il pulsante destro del mouse sull'evento nel registro degli eventi in ingresso.
3. Fare clic su **Copia negli Appunti evento selezionato**.
4. Avviare Blocco note.
   - Digitare `notepad` nella riga di commando oppure fare clic su **Start**, scegliere **Programmi**, quindi **Accessori**. Selezionare **Blocco note**.
5. Fare clic su **Modifica**, quindi su Incolla. Il testo dell'evento verrà visualizzato nel Blocco note. Ripetere il passaggio fino a quando non saranno disponibili tutti gli eventi necessari.
6. Salvare il file del Blocco note in una posizione protetta.

Eliminazione dell'evento selezionato

È possibile eliminare eventi dal registro eventi in ingresso.

Per eliminare eventi dal registro eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina Eventi in ingresso, fare clic sull'evento che si desidera eliminare.
3. Nel menu Modifica, fare clic su **Elimina evento selezionato**. L'evento viene eliminato dal registro degli eventi in ingresso.

Informazioni sugli avvisi

Si consiglia di acquisire familiarità con i tipi di avviso che verranno visualizzati durante l'utilizzo di Personal Firewall. Esaminare i seguenti tipi di avviso che possono essere visualizzati e le possibili risposte, in modo da poter reagire con sicurezza.

> **NOTA**
> I suggerimenti sugli avvisi aiutano a deciderne la gestione. Per visualizzare i suggerimenti con gli avvisi, fare clic sulla scheda **Opzioni**, sull'icona **Impostazioni avviso**, quindi selezionare **Usa suggerimenti intelligenti** (opzione predefinita) o **Visualizza solo suggerimenti intelligenti** dall'elenco **Suggerimenti intelligenti**.

Avvisi rossi

Gli avvisi rossi contengono informazioni importanti che richiedono l'attenzione immediata dell'utente:

- **Applicazione Internet bloccata**: questo avviso viene visualizzato se Personal Firewall blocca l'accesso a Internet di un'applicazione. Ad esempio, se viene visualizzato un avviso relativo a un programma cavallo di Troia, a tale programma viene automaticamente impedito l'accesso a Internet e all'utente viene consigliato di cercare i virus nel computer.
- **L'applicazione richiede l'accesso a Internet:** questo avviso viene visualizzato quando Personal Firewall rileva traffico Internet o di rete per le nuove applicazioni.
- **L'applicazione è stata modificata:** questo avviso viene visualizzato quando Personal Firewall rileva una modifica a un'applicazione a cui in precedenza era stato consentito l'accesso a Internet. Se l'applicazione non è stata aggiornata di recente, si consiglia di non concedere facilmente l'accesso a Internet all'applicazione modificata.

- **L'applicazione richiede l'Accesso server:** questo avviso viene visualizzato quando Personal Firewall rileva che un'applicazione a cui in precedenza era stato consentito l'accesso a Internet ha richiesto l'accesso a Internet come server.

  NOTA
  L'impostazione predefinita Aggiornamenti automatici di Windows XP SP2 scarica e installa gli aggiornamenti per il sistema operativo Windows e per gli altri programmi Microsoft eseguiti sul computer senza segnarlo agli utenti. Quando un'applicazione viene modificata da uno degli aggiornamenti invisibili di Windows, gli avvisi di McAfee Personal Firewall vengono visualizzati al successivo avvio dell'applicazione Microsoft.

  IMPORTANTE
  È necessario consentire l'accesso alle applicazioni che richiedono l'accesso a Internet per scaricare gli ultimi aggiornamenti del prodotto on-line, quali i servizi di McAfee.

Avviso Applicazione Internet bloccata

Se viene visualizzato un avviso relativo a un programma cavallo di Troia (Figura 2-4), a tale programma viene automaticamente impedito l'accesso a Internet e all'utente viene consigliato di cercare i virus nel computer. Se non è installato McAfee VirusScan, è possibile avviare McAfee SecurityCenter.

Figura 2-4. Avviso Applicazione Internet bloccata

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Ulteriori informazioni** per ottenere informazioni dettagliate sull'evento consultando il registro eventi in ingresso (per ulteriori informazioni vedere *Pagina Informazioni sugli eventi in ingresso* a pagina 23).
- Fare clic su **Launch McAfee VirusScan (Avvia McAfee VirusScan)** per cercare i virus nel computer.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Consenti accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).

Avviso L'applicazione richiede l'accesso a Internet

Se si seleziona **Standard** o **Elevata** nelle opzioni delle impostazioni di protezione, Personal Firewall visualizza un avviso (Figura 2-5) quando vengono rilevate connessioni Internet o di rete per le applicazioni nuove o modificate.

Figura 2-5. Avviso L'applicazione richiede l'accesso a Internet

Se viene visualizzato un avviso in cui viene raccomandata attenzione nel consentire l'accesso dell'applicazione a Internet, è possibile fare clic su **Per ulteriori informazioni, fare clic qui** per ottenere ulteriori informazioni sull'applicazione. Questa opzione viene visualizzata nell'avviso solo se Personal Firewall è configurato per utilizzare i suggerimenti intelligenti.

McAfee potrebbe non riconoscere l'applicazione durante il tentativo di accesso a Internet (Figura 2-6).

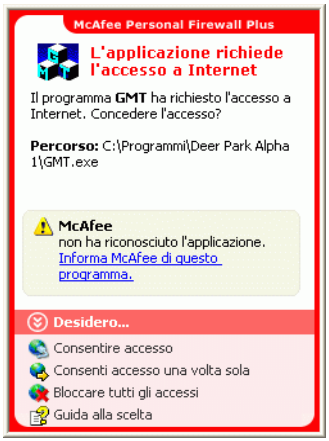


Figura 2-6. L'applicazione richiede l'accesso a Internet

Pertanto, potrebbe non fornire indicazioni su come gestirla. È possibile segnalare l'applicazione a McAfee facendo clic su **Informa McAfee di questo programma**. Viene visualizzata una pagina Web che chiede le informazioni relative all'applicazione. Inserire il maggior numero di informazioni disponibili.

Le informazioni inviate dagli utenti vengono utilizzate, in combinazione con altri strumenti di ricerca, dai nostri operatori HackerWatch per determinare se un'applicazione deve essere inserita nel nostro database di applicazioni note e, in tal caso, come deve essere gestita da Personal Firewall.

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consentire accesso** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consenti acesso una vola sola** per concedere all'applicazione una connessione Internet temporanea. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Consenti accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni.

Avviso L'applicazione è stata modificata

Se è stata selezionata la protezione **Basata sull'affidabilità**, **Standard** o **Elevata** nelle opzioni di impostazione di protezione, Personal Firewall visualizza un avviso (Figura 2-7) quando rileva una modifica in un'applicazione che in precedenza era stata autorizzata ad accedere a Internet. Se l'applicazione in questione non è stata aggiornata di recente, si consiglia di non concedere facilmente l'accesso a Internet all'applicazione modificata.

Figura 2-7. Avviso L'applicazione è stata modificata

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consentire accesso** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consenti accesso una volta sola** per concedere all'applicazione una connessione Internet temporanea. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Consenti accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni.

Avviso L'applicazione richiede l'Accesso server

Se è stata selezionata la protezione **Elevata** nelle opzioni di impostazione di protezione, Personal Firewall visualizza un avviso (Figura 2-8) quando viene rilevato che un'applicazione, che in precedenza era stata autorizzata ad accedere a Internet, ha richiesto l'accesso a Internet come server.

Figura 2-8. Avviso L'applicazione richiede l'Accesso server

Un avviso viene ad esempio visualizzato quando MSN Messenger richiede accesso al server per inviare un file durante una conversazione.

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consenti accesso una volta sola** per consentire all'applicazione un accesso a Internet temporaneo. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Consentire accesso server** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consentire solo accesso in uscita** per impedire le connessioni Internet in ingresso.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni. Avvisi verdi

Avvisi verdi

Gli avvisi verdi indicano la presenza di eventi in Personal Firewall, come le applicazioni a cui è stato automaticamente concesso l'accesso a Internet.

Programma autorizzato all'accesso a Internet: questo avviso viene visualizzato quando l'accesso a Internet viene concesso automaticamente a tutte le applicazioni nuove e viene emessa una notifica (protezione **Basata sull'affidabilità**).
Un esempio di applicazione modificata è un'applicazione con regole modificate per consentirne automaticamente l'accesso a Internet.

Avviso Applicazione autorizzata all'accesso a Internet

Se nelle opzioni di impostazione di protezione è stata selezionata la protezione **Basata sull'affidabilità**, Personal Firewall consente automaticamente l'accesso a Internet a tutte le applicazioni nuove, quindi informa l'utente con un avviso (Figura 2-9).

Figura 2-9. Programma autorizzato all'accesso a Internet

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro applicazioni** per ottenere informazioni dettagliate sull'evento mediante il registro delle applicazioni Internet (per ulteriori informazioni vedere *Informazioni sulla pagina Applicazioni Internet* a pagina 21).
- Per evitare la visualizzazione di questi tipi di avvisi, fare clic su **Disattivare tipo di avviso**.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.

Avviso L'applicazione è stata modificata

Se nelle opzioni di impostazione di protezione è stata selezionata la protezione **Basata sull'affidabilità**, Personal Firewall consente automaticamente l'accesso a Internet a tutte le applicazioni modificate. Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro applicazioni** per ottenere informazioni dettagliate sull'evento mediante il registro eventi in ingresso applicazioni Internet (per ulteriori informazioni vedere *Informazioni sulla pagina Applicazioni Internet* a pagina 21).
- Per evitare la visualizzazione di questi tipi di avvisi, fare clic su **Disattivare tipo di avviso**.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Bloccare tutti gli accessi** per impedire la connessione Internet.

Avvisi blu

Gli avvisi blu contengono informazioni, ma non richiedono una reazione da parte dell'utente.

- **Tentativo di connessione bloccato:** questo avviso viene visualizzato quando il traffico Internet o di rete indesiderato viene bloccato da Personal Firewall. (Basata su affidabilità, Standard o Elevata.)

Avviso Tentativo di connessione bloccato

Se è stata seleziona la protezione **Basata sull'affidabilità**, **Standard** o **Elevata** , Personal Firewall visualizza un avviso (Figura 2-10) in caso di blocco del traffico Internet o di rete indesiderato.

Figura 2-10. Avviso Tentativo di connessione bloccato

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro eventi** per ottenere informazioni dettagliate sull'evento mediante il registro eventi in ingresso di Personal Firewall (per ulteriori informazioni vedere *Pagina Informazioni sugli eventi in ingresso* a pagina 23).
- Fare clic su **Rintracciare questo indirizzo** per creare una traccia visuale degli indirizzi IP relativi all'evento.
- Fare clic su **Escludere questo indirizzo** per bloccare l'accesso al computer di questo indirizzo. L'indirizzo verrà aggiunto all'elenco degli indirizzi IP esclusi.
- Fare clic su **Accettare come affidabile** per consentire l'accesso di questo indirizzo IP al computer.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.

Indice

R

S

V

W