Quick Heal
Security Simplified

Manuale Utente

Quick Heal Total Security
Quick Heal Internet Security
Quick Heal AntiVirus Pro
Quick Heal AntiVirus Server Edition
Quick Heal Internet Security Essentials
Quick Heal Total Shield
Quick Heal AntiVirus Pro Advanced

Copyright & Informazioni sulla Licenza

Informazioni sul Copyright

I marchi

Condizioni di Licenza

L'installazione e l'utilizzo di Quick Heal Antivirus è soggetto all'accettazione incondizionata da parte dell'utente dei termini e delle condizioni della licenza dell'utente finale Quick Heal.

Per leggere i termini di licenza, visitare www.quickheal.com/eula e consultare il Contratto di licenza (EULA) per l'utente finale per il proprio prodotto.

Contatti Sede legale

Quick Heal Technologies Limited

(Propriamente riconosciuta come Quick Heal Technologies Pvt. Ltd.)

Sede legale: Marvel Edge, Office No. 7010 C & D, 7th Floor,

Viman Nagar, Pune 411014.

Telefono: +91 20 66813232

Sito ufficiale: www.quickheal.com

Email: info@quickheal.com

Data di rilascio:

October 14, 2020

Su questo Documento

La seguente tabella elenca le convenzioni che abbiamo utilizzato per redigere questo manuale.

Convenzione	Significato
Carattere in Grassetto	Qualsiasi cosa evidenziata in grassetto indica che essa può essere un titolo di menu,un titolo di finestra, una casella di controllo, un menù a tendina, un dialog, il nome dell'opzione, un collegamento ipertestuale, ecc ecc.
	Questo simbolo è utilizzato per le note. Le note integrano importanti aspetti o evidenziano informazioni riguardanti l'argomento trattato.
	Questo simbolo è utilizzato per i suggerimenti. I suggerimenti aiutano l'utente ad applicare le tecniche e le procedure al fine di raggiungere l'obiettivo desiderato in maniera più semplice.
	Questo simbolo indica la presenza di un pericolo o la necessità di fare attenzione. È da intendere anche come suggerimento per evitare perdite di dati o possibili danni all'hardware.
<Step 1> <Step 2>	Le istruzioni elencate nelle liste numerate indicano e azioni che devi eseguire.
Asterischi (*)	Gli asterischi (*) segnalano che una funzione può o non può essere disponibile in determinate versioni del prodotto.
Nome del Prodotto	Il termine Quick Heal antivirus è usato come termine generico in questo documento. Il termine può infatti riferirsi a ciascuno dei seguenti prodotti (se non specificato): Quick Heal Total Security, Quick Heal Internet Security, Quick Heal AntiVirus Pro, Quick Heal AntiVirus Server Edition, Quick Heal Internet Security Essentials, Quick Heal Total Shield, Quick Heal AntiVirus Pro Advanced.

Tabella di confronto dei prodotti Quick Heal

Caratteristiche	Quick Heal		
	AntiVirus Pro	Internet Security	Total Security
Core Protection (Antivirus, AntiSpyware, AntiMalware, Anti-Rootkit, Firewall, Rilevamento Intrusioni, Prevenzione intrusioni)	√	√	√
DNAScan Avanzato	√	√	√
Protezione Navigazione	√	√	√
Protezione Ransomware	√	√	√
Browser Sandbox	√	√	√
Safe Banking		√	√
Protezione Phishing		√	√
Protezione Spam		√	√
Scan Vulnerabilità		√	√
Protezione Furto Dati			√
Tastiera Virtuale		√	√
Parental Control		√	√
PCTuner			√
Scanner Wi-Fi		√	√
Game Booster			√
Anti-Tracker			√
PC2Mobile Scan			√
Protezione Webcam			√
File Vault			√

1. Introduzione

Per installare Quick Heal antivirus assicurarsi di ottemperare i seguenti requisiti.

Prerequisiti

Prima di installare Quick Heal antivirus è consigliabile seguire queste linee guida:

- Rimuovere eventuali altri programmi antivirus dal computer se ne avete. Più prodotti software antivirus installati su un singolo computer possono causare malfunzionamenti del sistema.
- Assicurarsi di disporre dei diritti amministrativi per l'installazione di Quick Heal Antivirus.
- Chiudere tutte le applicazioni, i browser, i programmi e i documenti aperti per un'installazione senza interruzioni.

Requisiti di Sistema

Per utilizzare l'antivirus Quick Heal, il sistema deve soddisfare i seguenti requisiti minimi.

Requisiti Generali

- 2 GB di spazio sul disco.
- Internet Explorer 6 o più recenti.
- Connessione Internet per ricevere aggiornamenti.
- Risoluzione schermo minima 1024 * 768.

Requisiti di Sistema

La seguente tabella descrive i requisiti di Sistema per i vari Sistemi Operativi.

Sistema Operativo (OS)	**Requisiti minimi di Sistema**
Sistema Operativo del desktop	
Windows 10	Processore: 1 gigahertz (GHz) o più veloce RAM: 1 gigabyte (GB) a 32-bit o 2 GB a 64-bit
Windows 8.1 / Windows 8	Processore: 1 GHz o più veloce RAM: 1 GB a 32-bit o 2 GB a 64-bit

Windows 7	Processore: 1 GHz o più veloce RAM: 1 GB a 32-bit o 2 GB a64-bit
Windows Vista	Processore: 1 GHz o più veloce RAM: 1 GB
Windows XP (pacchetto Service e più recenti)	Processore: 300 Megahertz (MHz) Pentium o più veloce RAM: 512 MB
Sistema Operativo del server	
Windows Server 2019	Processore: 1.4 GHz Pentium o più veloce RAM: 2 GB
Windows Server 2016	Processore: 1.4 GHz Pentium o più veloce RAM: 2 GB
Windows Server 2012 R2/ Windows Server 2012	Processore: 1.4 GHz Pentium o più veloce RAM: 2 GB
Windows Server 2008 R2/ Windows Server 2008	Processore: 1 GHz a 32-bit o 1.4 GHz a 64-bit RAM: Minima 512 MB (si consigliano 2 GB)
Windows Server 2003	Processore: 550 MHz a 32-bit o 1.4 GHz a 64-bit RAM: 256 MB a 32-bit o 512 MB a 64-bit

Note:

- I requisiti sono applicabili ad ogni tipo di Sistema Operativo.
- I requisiti sono applicabili ai Sistemi Operativi a 32-bit e 64-bit, se non specificato.
- Quick Heal AntiVirus Server Edition è compatibile con i Sistemi Operativi Microsoft Windows Server, mentre gli altri prodotti sono compatibili con i Sistemi Operativi del desktop.
- I requisiti di Sistema possono cambiare di volta in volta. Si consiglia di controllare gli ultimi requisiti di Sistema richiesti sul sito www.quickheal.com.

Supported POP3 email clients

Quick Heal antivirus supporta i seguenti client di posta elettronica.

- Microsoft Outlook Express 5.5 e più recenti
- Microsoft Outlook 2000 e più recenti
- Netscape Messenger 4 e più recenti

- Eudora
- Mozilla Thunderbird
- IncrediMail
- Windows Mail

Note:

La funzionalità di protezione della mail di Quick Heal antivirus non è supportata su connessioni di posta elettronica crittografate che usano Secure Sockets Layer (SSL).

Compatibilità specifica delle funzioni

La seguente tabella descrive la compatibilità specifica

Caratteristiche	Condizioni
Controllo Applicazione	• Per Microsoft Windows XP, questa applicazione è supportata solo se è installato Service Pack 1 o versioni successive.
Anti-Keylogger	• Non è supportato su Microsoft Windows XP 32-bit con Service Pack 1 o precedenti con Windows XP 64-bit. • Non è supportato su Windows 2003 Server 32-bit Service Pack 0 e Service Pack 1 e Windows 2003 Server 64 bit.
Anti-Rootkit	• É supportato su Sistemi Operativi a 32-bit .
Anti-Tracker	• L'Anti-Tracker non è supportato per Google Chrome su Windows XP e su Windows Vista.
Browser Sandbox	• Non è supportato su Microsoft Windows XP a 64-bit. • Questa funziona supporta solo i browser di Internet Explorer, Google Chrome e Mozilla Firefox. • Questa funzione non supporta il browser Microsoft Edge del Sistema Operativo Windows 10.
Disco di Emergenza	• Non è possibile creare Dischi di Emergenza usando CD/DVD su Microsoft Windows 2003 e su versioni precedenti. Tuttavia si può creare un Disco di Emergenza su unità USB.
Firewall	• La funzione Monitor Wi-Fi Networks non è supportata su Microsoft Windows XP 64-bit.
Game Booster	• Se la Protezione Virus è disabilitata non sarà possibile utilizzare l'applicazione Game Booster. • Game Booster funziona sui quattro processori logici (della

	CPU) o più elevati.
Safe Banking	● La funzione non è supportata per Windows XP a 64-bit. ● Questa funzione supporta Internet Explorer, Google Chrome, and Mozilla Firefox browsers only. ● Questa funzione non supporta il browser Microsoft Edge del Sistema Operativo Windows 10.
Auto-Protezione	● Per il Sistema Operativo Microsoft Windows XP questa funzione è supportata solo se Service Pack 2, o più recente, è installato. ● Per il Sistema Operativo Microsoft Windows Server 2003, questa funzione è supportata solo se Service Pack 1, o più recente, è installato . ● La funzionalità di Protezione dei Processi dell'Auto-Protezione è supportata su Microsoft Windows Vista Service Pack 1 e successivi.
Mobile Scan (PC2Mobile Scan)	● per i dispositivi Windows Mobile, ○ Microsoft Active Sync 4.0, o successivi, deve essere installata su Windows XP o Sistemi Operativi precedenti. ○ Windows Mobile Device Center deve essere installato su Windows Vista o Sistemi Operativi successivi.
Controllo di Quick Heal da remoto	● Supporta Internet Explorer 9 e successivi.

Installazione di Quick Heal antivirus

Per installare Quick Heal antivirus, seguire questi passi:

1. Inserire il CD/DVD di Quick Heal antivirus nel lettore DVD.

   La funzione autorun del CD/DVD è attivata e si aprirà automaticamente una schermata con un elenco di opzioni.Se il lettore DVD non apre automaticamente il CD/DVD, seguire i seguenti passi:

   (i) Andare alla cartella dove è possibile accedere al CD/DVD. (ii) Premere il tasto destro sull'unità DVD e selezionare **esplora**. (iii) Fare doppio click su **Autorun.exe**.

   In alternativa è possibile scaricare l'installer per Quick Heal antivirus dal seguente link: https://www.quickheal.co.in/quick-heal-product-installer. Per scaricare il prodotto è necessario inserire la chiave di prodotto.

2. Se si usa il CD del prodotto cliccare Install per avviare l'installazione. Se si possiede il file di installazione del processo fare doppio click su di esso.

   Completato il download, il procedura guidata di installazione esegue uno scanner dei virus pre-installazione del computer. Se viene rilevato un virus sul computer l'installer imposta

automaticamente lo scanner nella fase di avvio per scannerizzare e disinfettare il computer nella fase successiva. Dopo la disinfezione il computer si riavvia ed è necessario ricominciare con l'installazione. Se nessun virus viene rilevato sul computer l'installazione procede.

La schermata del Contratto di Licenza dell'Utente Finale appare.

Leggere attentamente il Contratto di Licenza. PEr una lettura completa usare la barra di scorrimento.Al termine del Contratto di Licenza si trovano due opzioni predefinite: **Invia file sospetti** e **Invia statistiche**. Se non si desidera inviare le statistiche o i file sospetti o entrambe, deselezionare le opzioni.

3. Accettare i **termini di licenza** e la **policy sulla privacy** e cliccare **Avanti.** In seguito, appare la schermata di posizione di installazione. Viene mostrata la locazione predefinita dove Quick Heal antivirus sta per essere installato. Appare sullo schermo anche la quantità di spazio sul disco necessaria.

   Se la posizione predefinita non ha spazio sufficiente o se si desidera installare Quick Heal antivirus in un'altra locazione, cliccare **Sfoglia** per cambiare la posizione o cliccare **Avanti** per continuare.

   L'installazione è avviata. Quando l'installazione è completata, appare un messaggio.

4. Clicca su **Registrati ora** per iniziare il processo di attivazione o clicca **Registrato dopo** per effettuare l'attivazione successivamente.

Registrazione Quick Heal antivirus

È possibile registrare/attivare l'antivirus Quick Heal online oppure offline, o mediante SMS in base alle vostre esigenze. Selezionare l'opzione fra le seguenti che più è conforme alle necessità dell'utente.

Registrazione online: Preferire questa tipologia se il computer in cui è stato installato Quick Heal antivirus ha una connessione internet.

Registrazione offline: Preferire questa tipologia se il computer in cui è stato installato Quick Heal antivirus non possiede una connessione internet. Sarà necessario generare una chiave di attivazione in seguito sarà possibile registrare l'antivirus.

Registrazione attraverso SMS: Possono usufruire di questa funzione solo gli utenti localizzati in India.

Registrazione online

Per registrare online l'antivirus Quick Heal, seguire questi passaggi:

1. Se ci si trova nella schermata di installazione, cliccare sul pulsante **Registrati Ora**.

   Se ci si registra successivamente, aprire **Quick Heal antivirus**. Nel pannello sinistro, cliccare su **Stato** e poi cliccare sul pulsante **Registrati Ora**.

   Verrà mostrata la schermata della procedura guidata di registrazione.

2. Nella Procedura Guidata di Registrazione, inserire la chiave prodotto da 20 caratteri e poi cliccare su **Avanti**.

   Verranno mostrate le Informazioni di Registrazione.

3. Inserire le informazioni rilevanti nelle caselle di testo di **Acquistato da**, **Codice rivenditore**, e **Registrati**, poi cliccare su **Avanti**.

   Verrà mostrata la schermata **Registrazione Utente**.

4. Fornire il proprio **Nome**, **Indirizzo Email**, e **Numero Telefonico**. Selezionare la propria **Regione**, **Stato**, e **Città**.

   Se il vostro Stato/Regione e Città non sono disponibili nell'elenco, è possibile digitare le vostro località nella rispettive caselle.

5. Cliccare su **Avanti**.

   Verrà mostrata una schermata di conferma con i dettagli inseriti.

   Se si rende necessario apportare una modifica, cliccare su **Indietro** per tornare alla schermata precedente ed effettuare le modifiche richieste.

6. Cliccare su **Avanti**.

   Il vostro prodotto è stato attivato con successo. Verrà mostrata la data di scadenza della licenza.

7. Cliccare su **Fine**.

Note:

Al completamento della registrazione di Quick Heal antivirus, verrà chiesto all'utente di creare un account tramite Quick Heal RDM. Questa funzione permette di gestire da remoto il dispositivo. Per sapere come creare un account tramite Quick Heal RDM, vedere Gestione Remota Quick Heal

Registrazione offline

Prima di effettuare la registrazione offline di Quick Heal antivirus, assicurarsi di avere a disposizione chiave prodotto, numero di installazione, e chiave attivazione licenza.

Trovare la Chiave Prodotto

E' possibile trovare la propria Chiave Prodotto nella scatola dello stesso. Se si è acquistato il prodotto online, la Chiave Prodotto verrà inviata al proprio indirizzo email confermando l'ordine di acquisto.

Trovare il Numero di Installazione

Per trovare il Numero di Installazione, seguire questi passaggi.

1. Se ci si trova nella schermata di installazione, cliccare sul pulsante **Registrati Ora**.

   Se si effettua la registrazione successivamente, aprire **Quick Heal antivirus**. Nel pannello sinistro, cliccare su **Stato** e poi cliccare sul pulsante **Registrati Ora**.

   The registration procedura guidata appears.

2. Nella registrazione procedura guidata, cliccare **Registrazione Offline**.

   Verrà mostrata la schermata di attivazione offline con l'URL di attivazione offline e il Numero di Installazione da 12 caratteri. Annotare questi dettagli oppure cliccare su **Salva file** per salvarli nel file di testo.

Generazione chiave di licenza obbligatoria

Per generare una chiave di attivazione licenza, seguire questi passaggi:

1. Visitare la pagina di attivazione offline su www.quickheal.com/actinfo.htm.

   Verrà mostrata una pagina di Registrazione Offline.

2. In versione prodotto, cliccare sul link **Clicca qui**.

   Assicurarsi di avere a disposizione la Chiave Prodotto e il Numero di Installazione (come descritto nella sezioni precedenti).

3. Inserire la **Chiave Prodotto** e il **Numero di Installazione** nei campi rilevanti e poi cliccare su **Invia**.

4. Nel form di registrazione, inserire le informazioni rilevanti e poi cliccare su **Invia**.

   Tutti i campi contrassegnati con l'asterisco (*) sono da compilare obbligatoriamente.

   Viene generata una nuova chiave di licenza di attivazione offline. Questa chiave è unica e può essere utilizzata una sola volta. Salva questa chiave per attivare l'antivirus Quick Heal offline. Questa chiave viene inviata anche al tuo indirizzo e-mail che hai fornito durante la registrazione del prodotto.

Attivazione di Quick Heal antivirus con chiave di attivazione della licenza

Dopo aver generato la chiave di licenza di attivazione offline, è possibile procedere con l'attivazione di Quick Heal antivirus sul computer.

1. Apri **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare **Stato** e dopo cliccare il pulsante **Registrati Ora**.
3. Nella Registrazione Procedura Guidata, cliccare **Registrazione Offline**.

Appare la schermata dell'attivazione offline

4. Fare clic su **Sfoglia** per individuare il percorso in cui è memorizzata la **<licenza>.chiave** e fare clic su **Avanti**.

La licenza viene attivata correttamente e viene visualizzata la data di scadenza.

5. Fare clic su **Fine**.

Registrazione Pacchetto Multi-Utente

Per attivare un pacchetto multiutente, si prega di prendere nota di quanto segue:

· Quando si registra un codice prodotto nel pacchetto multiutente, tutte le restanti chiavi del prodotto nel pacchetto vengono registrate contemporaneamente.

· Le informazioni di registrazione del primo codice prodotto attivato si applicano a tutti i codici prodotto rimanenti.

· La stessa validità della licenza si applica a tutti i codici Chiave Prodotto presenti nel pacchetto.

2. Riattivazione e rinnovo

Questo capitolo include le seguenti sezioni:.

Riattivazione Quick Heal antivirus

La riattivazione è una funzione che garantisce l'utilizzo del prodotto per l'intero periodo fino alla scadenza della licenza. La riattivazione è utile nel caso in cui si formatta il sistema quando vengono rimossi tutti i prodotti software o si desidera installare Quick Heal antivirus su un altro computer.

Ogni volta che viene installato l'antivirus, è necessaria la riattivazione. Il processo di riattivazione è simile al processo di attivazione, con l'eccezione che non è necessario inserire nuovamente i dettagli personali completi. Si consiglia di selezionare l'opzione Rimuovi Quick Heal e si mantiene l'aggiornamento dei file delle definizioni durante la disinstallazione. Ciò sarà utile a mantenere file di definizione dell'aggiornamento del prodotto

Rinnovo Quick Heal antivirus

Si consiglia di rinnovare la licenza prima della data di scadenza di quella precedente, di modo che il dispositivo rimanga protetto ininterrottamente. Puoi comprare il codice di rinnovo sul sito Quick Heal o dal distributore o rivenditore più vicino.

È possibile rinnovare la licenza Quick Heal antivirus in ciascuna delle seguenti opzioni.

Rinnovo online: Preferire questo metodo se il computer in cui è stato installato l'antivirus ha una connessione Internet.

Rinnovo offline: Preferire questo metodo se il computer in cui è stato installato l'antivirus non ha connessione internet. È necessario generare una chiave di attivazione e, in seguito, sarà possibile rinnovare l'antivirus.

Rinnovo online

Per rinnovare la licenza Quick Heal antivirus online è necessario seguire questi passi,.

1. Aprire **Quick Heal antivirus**.
2. Cliccare sul menu **Aiuto** in alto a destra e in seguito selezionare l'opzione **Informazioni Su**.
3. Se la licenza prodotto è scaduta, verrà mostrato il pulsante **Rinnova Ora.** Per rinnovare la propria licenza, cliccare su **Rinnovo Ora**.

La procedura guidata di Registrazione verrà visualizzata.

4. Selezionare **Ho il codice di rinnovo o una nuova chiave prodotto con me** se si è già comprato il codice di rinnovo e cliccare su **Avanti**.

   Verranno mostrate le Informazioni di Registrazione.

   Nota: Se non si dispone di una chiave di rinnovo e si desidera rinnovare la licenza, selezionare **Non ho un codice di rinnovo con me** e poi effettuare l'acquisto*.

5. Le informazioni rilevanti **Acquistato da**, **Indirizzo Email**, e il **Contatto Telefonico** verranno mostrate pre-compilate nelle caselle di testo. Tuttavia, è possibile modificare i dettagli dei dati di contatto se richiesto e poi cliccare su **Avanti**.

   Le informazioni di licenza come la **Data di scadenza attuale** e la Nuova data di scadenza verranno visualizzate ai fini della vostra conferma.

6. Cliccare su **Avanti**.

   La licenza di Quick Heal antivirus verrà rinnovata con successo.

7. Cliccare **Fine**.

Note:

* Se è stato acquistato un codice di rinnovo in più, il rinnovo della chiave aggiuntiva può essere effettuato solamente dopo 10 giorni rispetto all rinnovo corrente.

Rinnovo offline

Prima di rinnovare Quick Heal antivirus offline, assicurarsi di avere a disposizione la chiave prodotto, numero di installazione, codice di rinnovo, e chiave di attivazione licenza.

Trovare la Chiave Prodotto e il Numero di Installazione

Per trovare la Chiave Prodotto e il Numero di Installazione, seguire questi passaggi.

1. Aprire **Quick Heal antivirus**.

   Se la copia di Quick Heal antivirus è scaduta, un pulsante **Rinnova Ora** verrà mostrato in **Stato**. E' possibile rinnovare la propria licenza utilizzando questo pulsante. Se la copia di Quick Heal antivirus non è ancora scaduta, andare nel menu Aiuto, e selezionare **Informazioni su > Rinnova Ora**.

2. Cliccare su **Rinnova Offline**.

Verrà mostrata la schermata di rinnovo offline. Annotare l'URL per il rinnovo offline, la Chiave Prodotto, e il numero di installazione a 12 cifre. E' possibile cliccare **Salva su file** per salvare anche i dettagli nel file di testo.

Generare la Chiave di Attivazione di licenza

Per generare la Chiave di Attivazione di licenza, seguire i seguenti passaggi:

1. Visitare la pagina di Rinnovo Offline http://www.quickheal.com/offline_renewal.

   La schermata della pagina Rinnovo Offline appare.

2. Cliccare sul link **Clicca Qui**, sotto la versione del proprio prodotto.

   Assicurarsi di essere in possesso della Chiave del Prodotto e del Numero di Installazione (come descritto nella sezione precedente) e del Codice di Rinnovo.

3. Immettere il **codice prodotto**, **il numero di installazione**, **il codice di rinnovo acquistato**, e i dettagli inseriti in **acquistato da** e quindi fare clic su **Invia**.

   Dopo aver verificato i dati forniti, la schermata successiva visualizza il nome utente, l'indirizzo email registrato e il numero di contatto. Se il tuo indirizzo email e il numero di contatto sono cambiati, puoi aggiornarli oppure fare clic su **Invia**.

   Viene generata una nuova chiave di licenza per l'attivazione offline. Salva questa chiave per attivare Quick Heal offline. Questa chiave viene anche inviata all'indirizzo e-mail che hai fornito durante la registrazione del prodotto.

   Note:

   Questa chiave è unica e può essere utilizzata solo una volta.

Rinnovo di Quick Heal con la chiave di licenza di attivazione

Dopo aver generato la chiave di rinnovo offline, è possibile procedere con il rinnovo di Quick Heal antivirus sul computer.

1. Aprire **Quick Heal antivirus**.

   Se la propria copia di Quick Heal antivirus è scaduta, viene visualizzato il pulsante **Rinnova ora** nella dashboard di Quick Heal. È possibile rinnovare la licenza utilizzando questo pulsante. Se la copia di Quick Heal antivirus non è ancora scaduta, andare al menu Aiuto e selezionare **Informazioni > Rinnova ora**.

2. Cliccare **Rinnovo Offline**.

   Viene visualizzata la schermata dei dettagli del rinnovo offline.

3. Fare clic su **Sfoglia** per individuare il percorso in cui è memorizzata la **<chiave di licenza>** e fare clic su **Avanti**.

   La licenza viene rinnovata correttamente e viene visualizzata la validità della licenza.

4. Fare clic su **Fine**.

Rinnovo del Pacchetto

Per rinnovare un Pacchetto Multiutente, prendere nota delle seguenti condizioni:

- È possibile rinnovare una singola chiave prodotto del Pacchetto Multiutente acquistando una chiave per una licenza singola, oppure rinnovare il Pacchetto Multiutente acquistando una chiave di rinnovo multiutente per tutti gli utenti. È inoltre possibile acquistare le chiavi di rinnovo per le altre licenze in modo separato.

- Se si rinnova un Pacchetto Multiutente utilizzando una chiave di rinnovo multiutente, tutte le licenze saranno rinnovate in maniera simultanea e lo stesso periodo di validità si applicherà a tutte le chiavi di licenza presenti nel pacchetto.

3. Stato

É possibile aprire Quick Heal antivirus in ciascuna delle seguenti opzioni:

- Nella barra delle applicazioni, fare doppio click sull'icona di **Quick Heal antivirus** o premere il tasto destro sull'icona di **Quick Heal antivirus** e selezionare **Open Quick Heal antivirus**.
- Selezionare **Start > Programmi > Quick Heal antivirus > Quick Heal antivirus**.
- Selezionare **Start > Esegui**, digitare la parola `scanner` e premere INVIO.

Quando si apre Quick Heal antivirus appare la schermata dello Stato. Lo Stato include i seguenti temi.

Menu/Sezioni	Descrizione
Guida del Prodotto	É possibile avere accesso al nostro Manuale Utente al quale si può riferirsi per saperne di più su come un'opzione può essere d'aiuto all'utente e come configurarla.
Menu	Il menu include le seguenti sezioni: Guida per il Supporto: include una guida per il Supporto alla quale è possibile riferirsi per sapere come un'opzione può essere d'aiuto all'utente e come configurarla. Report:Aiuta l'utente a vedere i report degli incidenti. Invia Informazioni di Sistema:Aiuta l'utente ad inviare problemi tecnici che il computer fronteggia per i quali non riesce a trovare una soluzione. Quick Heal analizzerà il problema e condividerà la soluzione con l'utente. Supporto: Includes all sources of support that Quick Heal provides. Informazioni sulla Licenza: Include informazioni relative alla Licenza di Prodotto dell'antivirus.
Validità della Licenza	Mostra quanti giorni mancano alla scadenza della Licenza. Per saperne di più sulla licenza è possibile cliccare sul link **Licenza**.
Stato	Mostra lo stato di protezione del sistema del computer . Se il computer è sicuro, lo Stato verrà visualizzato in verde (). Se il computer ha bisogno dell'attenzione dell'utente al più presto ma non immediatamente, viene visualizzato in arancione Se il computer non è configurato con impostazioni ottimali ed è necessaria l'attenzione immediata dell'utente, viene visualizzato in rosso (). L'azione corrispondente al messaggio deve essere effettuata immediatamente per mantenere il computer protetto.
Minacce	Mostra le minacce rilevate fino a quel momento.

rilevate	
Totale dei Tracciamenti Bloccati	Mostra i tracciamenti bloccati fino a quel momento.
Notizie	Mostra le ultime notizie su Quick Heal. É possibile vedere tutte le notizie cliccando su ***Vedi tutte***.
PCTuner	Aiuta a migliorare le prestazioni del computer pulendo le voci di registro indesiderate che ingombrano lo spazio del disco rigido del computer.
Opzioni di Scansione	Fornisce varie opzioni di scansione come scansione completa del sistema, scansione personalizzata, scansione della memoria e così via.
Scansione Istantanea	Permette di eseguire uno scan del computer istantaneo.
Il mio Account	Con questo link si può visitare il portale Quick Heal Remote Device Management (Quick Heal RDM). È possibile aggiungere il prodotto a Quick Heal RDM per monitorare il prodotto in remoto attraverso il portale.
Feedback	L'utente può condividere l'esperienza di utilizzo del nostro prodotto.
Tastiera Virtuale*	La tastiera virtuale consente di inserire le informazioni richieste senza premere alcun tasto sulla tastiera fisica. Vengono così ridotti i rischi di registrazione delle informazioni dell'utente da parte di un malware di tipo keystroke logger.
Like di Facebook	Il link ai like di Facebook reindirizza l'utente alla pagina di Quick Heal su Facebook. Può così seguirci al fine di leggere post su cybersecurity, minacce e pericoli di virus cliccando solo il link dei **Like**.

Opzioni di Scansione

Opzioni di scansione fornisce varie opzioni di scansione del sistema in base alle vostre esigenze. È possibile avviare la scansione dell'intero sistema, unità, unità di rete, unità USB, cartelle o file, determinate posizioni e unità, scansione della memoria e scansione del tempo di avvio. Anche se le impostazioni predefinite per la scansione manuale sono di solito adeguate, è possibile regolare le opzioni per la scansione manuale come si preferisce.

Scansione Rapida

Questa funzione completa la scansione del sistema a ritmo più veloce. Con la Scansione Rapida, vengono scansionate solo le posizioni predefinite che possono essere vulnerabili ad attacchi dannosi.

Per avviare una scansione rapida, procedere come segue:

1. Aprire **Quick Heal antivirus**.

Nel riquadro di sinistra, fare clic su **Stato** e quindi selezionare **Opzioni di scansione** > **Scansione** rapida.

Lo scan sta per iniziare.

Al termine della scansione, è possibile visualizzare il report di scansione in **Report**.

Scansione Completa del Sistema

Questa funzione consente di avviare una scansione completa di tutti i record di avvio, unità, cartelle, file e vulnerabilità sul computer (escluse le unità di rete mappate).

La Scansione Completa del Sistema è consigliabile dopo la prima installazione. La nostra Scansione Completa del Sistema è capace di eseguire la scansione completa per la prima volta. La volta successiva scansionerà solo i file che sono stati modificati. Questa scansione differenziata ottimizza le tempistiche di scansione.

Per avviare una scansione completa del sistema, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, fare clic su Stato e quindi selezionare **Opzioni di scansione > Scansione** completa del sistema.

   Lo scan sta per iniziare**.**

   Al termine della scansione, è possibile visualizzare il report di scansione in **Report**.

Scansione Personalizzata

Questa funzione consente di eseguire la scansione di unità e cartelle specifiche sul sistema. Questo è utile quando si desidera eseguire la scansione solo alcuni elementi e non l'intero sistema.

Per scannerizzare specifiche cartelle, è necessario seguire i seguenti passi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare su **Stato** e in seguito selezionare **Opzioni di scansione> Scansione Personalizzata**.
3. Nella schermata Scansione personalizzata, un elenco di elementi viene visualizzato nell'elenco Oggetto di scansione se sono stati aggiunti elementi da scansionare. Se non è stato aggiunto alcun elemento prima o si desidera eseguire la scansione di alcuni nuovi elementi, fare clic su **Aggiungi** per aggiungere gli elementi di scansione.
   - Nell'elenco **Sfoglia cartella**, selezionare le cartelle da scansionare.

     È possibile aggiungere più cartelle per la scansione. Verranno scansionate anche tutte le sottocartelle nella cartella selezionata. È possibile escludere la sottocartella dalla scansione se necessario. Per escludere la sottocartella, selezionare l'opzione **Escludi sottocartella** e fare clic su **OK.**

4. Selezionare un elemento dall'elenco Scan Item e quindi fare clic su **Inizia scansione**.

   La scansione ha inizio.

   Al termine della scansione, è possibile visualizzare il Report di scansione nel menu **Report**.

Scansione Memoria

Questa opzione scansiona la memoria del sistema del computer dell'utente.

Per eseguire una scansione della memoria, seguire i seguenti passi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello di sinistra, cliccare **Stato** e in seguito selezionare **Opzioni di Scansione> Scansione Memoria**.

   La scansione inizia.

   Al termine della scansione, è possibile visualizzare il report di scansione in **Report**.

I seguenti campi vengono visualizzati durante la scansione.

Campo	Descrizione
File scansionati	Mostra il numero totale di file scansionati.
Archiviati/Compressi	Mostra il numero di file archiviati o compressi file scansionati.
Minacce rilevate	Mostra il numero di minacce individuate che sono state scansionate.
Pericoli di DNAScan	Mostra il numero di file scansionati dal DNAScan.
Boot/Virus di Partizioni	Mostra il numero di virus di Boot/Partizione.
File riparati	Mostra il numero di file malevoli che sono stati riparati.
File in quarantena	Mostra il numero di file malevoli che sono stati messi in quarantena.
File eliminati	Mostra il numero di file malevoli che sono stati eliminati.
Stato di scansione	Mostra lo stato della scansione che è stata eseguita.

Scansione in Fase di Avvio

Questa funzione aiuta a pulire anche i sistemi altamente infetti. Alcuni virus tendono ad essere attivi se il sistema è in esecuzione e non possono essere puliti. Tuttavia, utilizzando la Scansione in fase è possibile pulire tali virus. Questa scansione verrà eseguita al prossimo avvio utilizzando Windows NT Boot Shell.

Per impostare la Scansione in Fase, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Stato** e poi selezionare **Opzioni Scansione > Scansione in Fase di Avvio.**

La Scansione in Fase di Avvio ha le seguenti opzioni:

- Scansione Rapida: Scansiona solo le posizioni predefinite del sistema che presentano un alto rischio di virus.
- Scansione Completa Sistema: Scansiona l'intero sistema. Potrebbe richiedere molto tempo.

3. Cliccare su **Sì**.
4. Per riavviare il sistema ai fini della scansione immediata, cliccare su **Sì**. Per scansionare il sistema successivamente, cliccare su **No**.

Nota:

Nel caso in cui la Scansione in Fase di Avvio richieda tempo oppure sia stata avviata per errore, è possibile interromperla premendo sul pulsante **ESC**.

Scansione Vulnerabilità

Le vulnerabilità sono i difetti presenti nelle impostazioni del sistema operativo e nelle applicazioni che possono essere utilizzati in modo improprio dagli hacker. Se vengono identificate queste vulnerabilità per tempo, è possibile correggerle o patcharle per rendere il proprio sistema sicuro.

Scansione Vulnerabilità* nella nuova versione di Quick Heal antivirus viene fornito un metodo di rilevamento preventivo completo. Identifica le vulnerabilità nelle impostazioni del sistema operativo e nelle applicazioni in modo che tu possa correggere o patchare le vulnerabilità prima che il tuo sistema venga compromesso.

Per eseguire la Scansione Vulnerabilità, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Stato** e poi selezionare **Opzioni Scansione > Scansione Vulnerabilità.**

   La Scansione Vulnerabilità ricerca le vulnerabilità delle seguenti tipologie:

   Impostazioni Vulnerabilità Sistema: Rileva le impostazioni vulnerabili del sistema operativo che potrebbero causare minacce alla sicurezza.

   Vulnerabilità nella Applicazioni: Individua le vulnerabilità presenti nelle applicazioni che sono installate sul proprio computer.

   Quando la scansione è completata, verrà mostrato un riepilogo di scansione. Se si desidera vedere un report dettagliato delle vulnerabilità, cliccare una categoria da **Impostazioni Vulnerabilità Sistema** e **Vulnerabilità nelle Applicazioni**.

Report tipologie	Descrizione
Impostazioni di sistema vulnerabili	Visualizza le vulnerabilità rilevate nelle impostazioni del sistema operativo. Per visualizzare il Report in dettaglio, fare clic su Impostazioni di sistema vulnerabili nella schermata Scansione vulnerabilità. Tutte le vulnerabilità rilevate nelle impostazioni di sistema sono elencati insieme con le loro correzioni. È possibile applicare correzioni alle vulnerabilità facendo clic su Correggi in azione.
Vulnerabilità trovate nelle Applicazioni	Visualizza le vulnerabilità rilevate nelle applicazioni installate sul computer. Per visualizzare il Report in dettaglio, fare clic su Vulnerabilità presenti in Applicazioni nella schermata Scansione vulnerabilità. Tutte le vulnerabilità sono elencate con i loro link alle patch. Per applicare le patch, fare clic su Sì sotto Patch Disponibile. Sarete reindirizzati ai siti web pertinenti da dove è possibile scaricare le patch e applicarle. Se non è disponibile alcuna patch, puoi considerare di aggiornare l'applicazione o contattare il supporto del fornitore dell'applicazione.

Mobile Scan

Con PC2Mobile Scan*, l'utente può scansionare una vasta gamma di Android, iOS, e cellulari Windows. Prima di scansionare il cellulare, l'utente deve seguire i seguenti passi.

- L'opzione Mobile Scan è supportata dai sistemi operativi Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, e Windows 10.
  (Note: Mobile Scan non è supportata da Windows XP per i dispositivi iOS)
- Per dispositivi con Sistema Operativo Windows Mobile(Windows Mobile versione 3.0 e precedenti e versione 7.0), è necessario che l'utente abbia Microsoft Active Sync 4.5 o successivi per Windows XP (32-bit); e Windows Mobile Device Center per Windows Vista, Windows 7, Windows 8, Windows 8.1, o Windows 10.
- Installare PCSuite e l'unità di dispositivo sul computer. Una volta che il dispositivo è connesso a PCSuite, uscire da PCSuite.
- Per scansionare dispositivi Android, assicurarsi che il dispositivo sia connesso tramite cavo USB, e che le opzioni **USB debugging** e **Stay awake** siano abilitate.
- Per dispositivi iPhone (Mac), iTunes deve essere installato nel sistema.

Scansionare dispositivi mobili attraverso PC2Mobile Scan

Con PC2Mobile Scan, è possibile scansionare dispositivi mobili nel seguente modo :

1. Aprire **Quick Heal antivirus**.

2. Nel riquadro di sinistra, cliccare su **Stato** e in seguito selezionare **Opzioni di scansione > Mobile Scan**.
3. Connettere un cellulare al PC usando un cavo USB.
4. Cliccare sul pulsante **Cerca Cellulare**.
5. Cliccare su **Inizia Ricerca**.

   Viene effettuata una ricerca del modello del telefono cellulare collegato.
6. Selezionare il cellulare dalla lista di dispositivi mobili connessi. Cliccare **Inizio Scansione**.

   Al termine della scansione, è possibile visualizzare il Report di scansione nel menu **Report**.

4. Protezione

Mentre si lavora sul sistema del computer, si può essere connessi a Internet, unità esterne, e può inviare e ricevere comunicazioni e-mail. Il sistema può essere esposto a virus o malware che cercano di infiltrarsi nel sistema.

La sezione Protezione include quelle funzionalità che consentono di proteggere i sistemi, le cartelle, i file e i dati da eventuali minacce di malware, virus, worm e furto di dati.

La protezione include le seguenti caratteristiche:

Ransomware Protection

Virus Protection

Scan Settings

Browsing Protection

Phishing Protection

Safe Banking

Firewall Protection

IDS/IPS

Email Protection

USB Drive Protection

External Drive Protection

Browser Sandbox

Malware Protection

Anti Malware

Anti Rootkit

Protezione Ransomware

Gli attaccanti di ransomware scaricano ransomware sul computer che lo bloccano. Lasciano inoltre un messaggio all'utente per ricattarlo, chiedendogli somme di denaro per poter accedere nuovamente al computer.

La Protezione Ransomware rileva questo tipo di attacchi ransomware. Questa opzione permette all'utente di eseguire un backup dei dati sul tuo computer che l'utente può ripristinare quando necessario. La maggior parte dei documenti popolarmente noti, compresi i tally data, sono protetti.

Il computer può essere infettato da ransomware in diversi modi, come:

- Navigazione siti infetti o falsi.
- Apertura di email o allegati e-mail da attaccanti phishing.
- Apertura link dannosi da siti web o siti di social networking.
- Installazione di applicazioni e strumenti falsi.
- Giocare giochi online da siti non attendibili.

Configurazione Protezione Ransomware

Per configurare Protezione Ransomware, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, fare clic su **Protezione** e quindi su **Protezione Ransomware**.
3. Nella schermata Protezione Ransomware, attivare Protezione Ransomware.

Escludere File e Cartelle

Con questa funzione, è possibile specificare quali file e cartelle non devono essere inclusi durante la scansione per ransomware e altri attacchi dannosi. L'esclusione di file consente di evitare la scansione non necessaria di file che sono già stati sottoposti a scansione o si è sicuri che alcuni file non devono essere sottoposti a scansione.

- È possibile escludere la scansione dei file dai seguenti moduli di scansione.
- Rilevamento di virus noto
- DNAScan
- Scansione di file imballati sospetti
- Rilevamento del comportamento
- Rilevamento ransomware

Configurare ed Escludere File & Cartelle

Per Configurare ed Escludere file e cartelle, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Protezione** e in seguito cliccare **Protezione Ransomware**.

   Nella schermata Protezione ransomware, fare clic su Escludi file e cartelle.

Viene visualizzata la schermata Escludi file e cartelle. Qui vedi l'elenco dei file e delle cartelle esclusi che sono stati aggiunti.

3. Per aggiungere un nuovo file o una nuova cartella, cliccare **Aggiungi**.

   La schermata del Nuovo Oggetto da Escludere appare.

4. Nella casella di testo dell'**Oggetto**, fornire il percorso del file o della cartella. Per selezionare il percorso, l'utente può anche cliccare sull'icona del file o della cartella.

   Assicurarsi di fornire il percorso per il file o la cartella corretta, altrimenti appare un messaggio.

5. In Escludi da, l'utente può selezionare i moduli da cui vuole escludere il file o la cartella selezionati.

   È possibile selezionare il rilevamento di Virus Noto o uno qualsiasi da Dnascan, File Sospetti Compressi di scansione, e il comportamento di rilevamento e ransomware opzioni di rilevamento.

6. Cliccare **OK**.
7. Per salvare le modifiche, cliccare su **Salvare Modifiche**.

Note:

- Se stai ricevendo un avviso per un virus noto in un file pulito, puoi escluderlo per la scansione di Known Virus Detection.
- Se stai ricevendo un avviso DNAscan in un file pulito, puoi escluderlo dall'essere scansionato per DNAscan.

Protezione Virus

I virus provenienti da varie fonti come allegati e-mail, download da Internet, trasferimento di file ed esecuzione di file tentano di infiltrarsi nel sistema. Questa funzione permette di monitorare continuamente il sistema alla ricerca di virus. È importante sottolineare che questa funzione non esegue nuovamente la scansione dei file che non sono cambiati dalla scansione precedente, riducendo così l'utilizzo delle risorse.

Si consiglia di mantenere sempre abilitata la protezione antivirus per mantenere il sistema pulito e protetto da potenziali minacce. Tuttavia, la Protezione antivirus è attivata per impostazione predefinita.

Configurazione Protezione Virus

Per configurare la Protezione Virus, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Protezione Virus**. Abilitare **Protezione Virus**.
3. Per la configurazione, cliccare sull'icona delle impostazioni per la **Protezione Virus**.

   Verrà mostrata la schermata con i dettagli della Protezione Virus.
4. Impostare le opzioni seguenti come da requisito:
   - **Mostra messaggio di avviso** – Selezionare questa opzione se si desidera ricevere gli avvisi sui vari eventi. Per esempio, quando viene individuato un malware. Tale opzione è selezionata per impostazione predefinita.
   - **Seleziona azione da eseguire quando viene rilevato un virus** – Selezionare l'azione appropriata da eseguire quando viene individuato un virus durante la scansione.
   - **Backup prima di un'azione** – Selezionare questa opzione se si desidera effettuare un backup di un file prima di eseguire un'azione. I files che sono archiviati ne backup possono essere ripristinati dalla Quarantena.
   - **Abilita suono quando viene rilevata una minaccia** – Selezionare questa opzione se si desidera essere avvisati con un suono ogni volta che un virus viene individuato.
5. Per salvare le impostazioni, cliccare su **Salva Modifiche**.

Azione da intraprendere quando viene rilevato un virus

La seguente tabella descrive varie azioni e la loro relativa descrizione.

Azione	Descrizione
Ripara	Se un virus viene rilevato durante una scansione, il file viene pulito e riparato. Se il file non può essere riparato, viene messo in quarantena automaticamente.
Cancella	Elimina un file infetto da virus senza avvisare l'utente.
Nega Accesso	Limita l'accesso a un file infetto da virus dall'uso.

Disattivare la Protezione Virus

Si consiglia di mantenere sempre Virus Protection acceso per mantenere il sistema pulito e sicuro da eventuali minacce potenziali. Tuttavia, è possibile disattivare Virus Protection quando richiesto. Mentre si disattiva Protezione virus, si dispone di una serie di opzioni per disattivare temporaneamente la funzione, in modo che si accende automaticamente dopo l'intervallo di tempo di selezione passa**.**

Per disattivare la protezione dai virus, segui questi passaggi.

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccando **Protezione** e in seguito cliccare **Protezione Virus**. Disattivare **Protezione Virus**.
3. Per disattivare Protezione virus, selezionare una delle seguenti opzioni:
   - Accendere dopo 15 minuti
   - Accendere dopo 30 minuti
   - Accendere dopo 1 ora
   - Attiva dopo il riavvio successivo
   - Disabilitare permanentemente
4. Per salvare le impostazioni, fare clic su OK.

   Dopo aver disattivato Protezione virus, viene visualizzato il colore dell'icona dell'opzione Opzioni di scansione su Cambiamenti di stato da verde a rosso e un messaggio "Il sistema non è sicuro".

5.

Opzioni di Scansione

Con questa funzione, è possibile configurare le impostazioni di protezione per i file e le cartelle nel sistema.

Opzioni di Scansione include le seguenti impostazioni di protezione.

- Impostazioni di Scansione
- DNAScan Avanzata
- Bloccare File Sospetti Compressi
- Scansione Rogueware Automatica
- Programma Scansioni
- Escludere File & Cartelle
- Quarantine & Backup

Opzioni di Scanner

Questa funzione consente di definire come avviare la scansione del sistema e quali azioni devono essere adottate quando un virus viene rilevato. Tuttavia, le impostazioni predefinite sono ottimali al fine di garantire la protezione necessaria per il sistema.

Opzioni Modalità Scansione

Per configurare le impostazioni di scansione, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Protezione** e, in seguito, cliccare **Opzioni di scansione**.
3. Nella schermata delle Opzioni di Scansione, cliccare **Opzioni di Scansione**.
4. Sotto **Seleziona modalità Scansione**, selezionare **Automatico (Consigliato)** per avviare la scansione automaticamente, o selezionare **Avanzato** per un avanzato livello di scansione.
5. Sotto **Seleziona azioni da eseguire quando viene rilevato un virus**, selezionare l'azione opportuna.
6. Se si desidera eseguire un backup dei file prima di compiere un'azione su di essi, selezionare **Effettua il backup prima di intraprendere qualunque azione**.
7. Per salvare le nuove impostazioni, cliccare **Salva Modifiche**.

Modalità Scansione

Automatica (Consigliato): È il tipo di scansione predefinito ed è consigliato in quanto garantisce la protezione ottimale per il sistema. Questa impostazione è un'opzione ideale per gli utenti inesperti.

Avanzata: Questo ti aiuta a personalizzare l'opzione di scansione. Questo è ideale per utenti esperti. Quando si seleziona l'opzione Avanzate, viene attivato il pulsante Configura e si possono configurare le impostazioni avanzate per la scansione.

Azione da effettuare quando viene rilevato un virus

È possibile configurare le seguenti azioni da intraprendere quando viene rilevato un virus sul computer.

Azione	Descrizione
Riparare	Selezionare questa opzione se si desidera riparare un file infetto. Se un virus viene trovato durante una scansione in un file, ripara il file. Se il file non può essere riparato, viene messo in quarantena automaticamente. Se il file infettivo ha una Backdoor, Worm, Trojan o Malware, Quick Heal antivirus elimina automaticamente il file.
Eliminare	Selezionare questa opzione se si vuole eliminare un file infetto. Il file infetto viene eliminato senza avvisarti. Una volta che i file vengono eliminati, non possono essere recuperati.
Salta	Selezionare questa opzione se si desidera non intraprendere alcuna azione su un file infetto.
Effettua il backup prima di intraprendere qualunque azione	Lo scanner mantiene un backup dei file infetti prima di disinfettarli. I file memorizzati nel backup possono essere ripristinati dalla quarantena.

Configurare la Modalità di Scansione Avanzata

Per configurare la modalità di scansione avanzata, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Protezione** e dopo cliccare **Opzioni di Scansione**.
3. Nella schermata delle Opzioni di Scansione, cliccare **Opzioni di Scansione**.
4. Sotto Seleziona Modalità di Scansione, selezionare **Avanzate**.

   Il pulsante Configura è attivato.
5. Cliccare **Configurare**.

   Viene visualizzata la schermata dei dettagli delle impostazioni avanzate di scansione.

6. Sotto **Seleziona l'oggetto da scansionare**, selezionare **Scansiona File Eseguibili** se si desidera scansionare solo i file eseguibili. Selezionare **Scansiona tutti i file** se si desidera scansionare tutti i file.

   Tuttavia, l'opzione Scansione file eseguibili è selezionata come impostazione predefinita.

   Ci vuole tempo per eseguire la scansione di tutti i file e il processo può rallentare il sistema.

7. Selezionare uno dei seguenti oggetti per la scansione:
   - **Scansiona file archiviati**: Selezionare questa opzione se si desidera scansionare file archiviati come file zip e file RAR.
   - **Scansione file compressi**: Selezionare questa opzione se si desidera scansionare file compressi.
   - **Scansione caselle di posta**: Selezionare **Scansione rapida delle caselle di posta** per una veloce scansione della posta, mentre selezionare **Scansione completa delle caselle di posta** per una scansione più approfondita.
8. Cliccare **OK**.
9. Per salvare le proprie modifiche, è necessario che l'utente clicchi su **Salva Modifiche**.

Scansione di file archiviati

Questa funzione consente di configurare le regole di scansione per i file di archivio come file ZIP, file RAR e file CHM.

Per configurare le regole di scansione dei file archiviati, seguire questi passaggi :

1. Nella schermata delle Opzioni di Scansione Avanzata, selezionare **Scansione dei file archiviati**.

   Il pulsante Configura è attivato.

2. Cliccare il pulsante **Configura**.

   Viene visualizzata la schermata dei dettagli degli archivi di scansione.

3. In **Seleziona azione da eseguire quando viene trovato il virus**, selezionare una delle seguenti opzioni: Elimina, Quarantena e Salta.
4. In **Livello di scansione archivio**, selezionare il livello a cui si desidera eseguire la scansione dei file e delle cartelle.

   Il livello di scansione predefinito è impostato al livello 2. Tuttavia, aumentare il livello di scansione predefinito può influenzare la velocità di scansione.

5. Sotto **Seleziona il tipo di archivio da scansionare**, selezionare il tipo di file archiviati da scansionare.
6. Per salvare le nuove impostazioni, è necessario cliccare **OK**.

Azione da eseguire quando viene rilevato un virus

La seguente tabella descrive le potenziali azioni e la loro descrizione.

Azionie	Descrizione
Elimina	Selezionare questa opzione se si desidera eliminare un file infetto. Il file infetto viene eliminato senza notifica.
Quarantena	Selezionare questa opzione se si desidera mettere in quarantena un archivio infetto se si trova un virus in esso.
Salta	Selezionare questa opzione se non si desidera agire su un file infetto.

Selezionare il tipo di archivio da scansionare

Un elenco di archivi che possono essere inclusi per la scansione durante il processo di scansione è disponibile in questa sezione. Pochi degli archivi comuni sono selezionati di default che è possibile personalizzare in base alle vostre esigenze.

La seguente tabella descrive i tipi di archivio.

Pulsante	Descrizione
Seleziona Tutto	Aiuta a selezionare tutti gli archivi nella lista
Deseleziona Tutto	Aiuta a deselezionare tutti gli archivi nella lista.

Scansione file compressi

Questa funzione consente di eseguire la scansione di packer o file compressi. I packers sono i file che raggruppano molti file o li comprimono in un singolo file per ridurre la dimensione del file. Inoltre, questi file non hanno bisogno di un'applicazione di terze parti per essere estratti. Hanno una funzionalità integrata per la compressione e la decompressione.
I Packers possono anche essere usati come strumenti per diffondere malware impacchettando un file dannoso insieme ad un insieme di file. Quando tali packers sono disimballati possono causare danni al sistema del computer. Se si desidera eseguire la scansione packers, selezionare l'opzione **Scansione di file compressi**.

Scansione delle caselle di posta

Questa funzione consente di eseguire la scansione della casella di posta di Outlook Express 5.0 e versioni successive (all'interno dei file DBX). Virus come KAK e JS.Flea. B, possono rimanere all'interno dei file **DBX** e possono riapparire se le patch non vengono applicate per Outlook Express. La funzione scansiona anche gli allegati email codificati con UUENCODE/MIME/Binhex (Base 64). **Scansione delle caselle di posta** è selezionata per impostazione predefinita che attiva le seguenti due opzioni.

Opzione	Descrizione
Scansione rapida delle caselle di posta	Aiuta a saltare tutte le conversazioni scansionate in precedenza e a scansionare solo i nuovi messaggi. Questa opzione è selezionata come impostazione predefinita.
Scansione completa delle caselle di posta	Aiuta a scansionare tutte le mail nella casella di posta per tutto il tempo. Tuttavia, questo può influenzare la velocità come le dimensioni della casella di posta aumenta.

DNAScan Avanzato

Dnascan è una tecnologia indigena in prodotti Quick Heal che rileva ed elimina nuove e sconosciute minacce dannose sul sistema. La tecnologia Dnascan Avanzato intrappola con successo i file sospetti con molti meno falsi allarmi. Inoltre, mette in quarantena il file sospetto in modo che il malware non danneggi il sistema.

I file sospetti in quarantena possono essere inviati ai laboratori di ricerca Quick Heal per ulteriori analisi che aiutano a monitorare le nuove minacce e frenarli in tempo. Dopo l'analisi, la minaccia viene aggiunta nel database delle minacce dalla firma nota e la soluzione viene fornita negli aggiornamenti successivi agli utenti.

Configurare DNAScan Avanzato

Per configurare DNAScan Avanzato, è necessario seguire questi passi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Protezione** e quindi su **Impostazioni di scansione**.
3. Nella schermata Impostazioni di scansione, cliccare **DNAScan Avanzato**.

   Viene visualizzata la schermata Dettagli di Dnascan Avanzato.
4. Selezionare una delle seguenti opzioni secondo l'esigenza:
   - **Attivare DNAScan**: Select this option to enable DNAScan.
   - **Attivare il Sistema di Rilevamento dei Comportamenti**: Selezionare questa opzione se si desidera attivare il sistema di rilevamento dei comportamenti. Le applicazioni in esecuzione saranno monitorate per il loro comportamento. È inoltre possibile impostare un livello di allarme di sicurezza dall'elenco di livelli di rilevamento Seleziona comportamento o come Alto, Moderato o Basso.
   - Alto: Se si seleziona questo livello di sicurezza, Quick Heal antivirus monitorerà da vicino il comportamento di un'applicazione in esecuzione e vi avviserà se qualsiasi comportamento applicazione insolita viene notato. È possibile ricevere più avvisi e, talvolta, anche per i file autentici.

- Moderato: Se si seleziona questo livello di sicurezza, Quick Heal antivirus invierà un avviso se qualsiasi attività sospetta di un'applicazione in esecuzione viene notato.
- Basso: Se si seleziona questo livello di sicurezza, antivirus Quick Heal invierà avviso solo se qualche attività sospetta di un'applicazione in esecuzione viene notata.

  Note: Se è stato selezionato un livello di sicurezza moderato o basso, il sistema di rilevamento del comportamento* bloccherà anche molte minacce sconosciute in background senza richiedere alcuna azione se si sospetta il comportamento dell'applicazione.

  - **Non inviare file**: Selezionare questa opzione se non si desidera inviare file sospetti al laboratorio di ricerca di Quick Heal.
  - **Invia i file**: Selezionare questa opzione se si desidera inviare i file ai laboratori di ricerca per analisi più approfondite. Si può anche selezionare **mostra notifiche quando viene inviato il file** per avere la richiesta di permesso prima dell'invio.

⚠ Consiglio:

Se l'opzione **Mostra notifiche prima di inviare i file** non è selezionato, Quick Heal invierà i file sospetti senza avvisare l'utente.

DNAScan Avanzato rileva i file studiando le loro caratteristiche e i loro comportamenti.

Rilevazione in base alle Caratteristiche

Migliaia di minacce nuove e polimorfiche (che cambiano il loro codice/ informazioni del file) nascono ogni giorno. Rilevarli con la loro firma richiede tempo. La nostra tecnologia Dnascan Avanzato rileva tali minacce in tempo reale, con intervalli di tempo zero.
Ogni volta che Dnascan rileva una nuova minaccia dannosa nel sistema, mette in quarantena il file sospetto e visualizza un messaggio con il nome del file. Tuttavia, se si scopre che il file è autentico, è anche possibile ripristinare il file dalla quarantena utilizzando l'opzione fornita nella casella di messaggio.

Rilevazione in base al Comportamento

Se l'opzione **Sistema di rilevamento del comportamento** è abilitato, Dnascan monitora continuamente le attività svolte da un'applicazione nel sistema. Se l'applicazione si discosta dal suo comportamento normale o svolge qualsiasi attività sospetta, **sistema di rilevamento del comportamento** sospende tale applicazione dall'esecuzione di ulteriori attività che possono causare danni potenziali al sistema.
Al momento di rilevare tale applicazione, si richiede di prendere un'azione appropriata tra le seguenti opzioni:

- Consenti: Esegui questa azione se vuoi permettere all'applicazione di funzionare. Seleziona questa azione se sei sicuro che le applicazioni siano autentiche.

- Blocco: Eseguire questa azione se si desidera bloccare l'esecuzione dell'applicazione.

Inviare File sospetti

È possibile inviare i file sospetti automaticamente o manualmente. L'invio avviene automaticamente ogni volta che Quick Heal antivirus si aggiorna e trova nuovi file sospetti Dnascan in quarantena. Questo file viene inviato in un formato di file crittografato ai laboratori di ricerca Quick Heal.

Puoi anche inviare i file in quarantena manualmente se pensi che debbano essere inviati immediatamente. Puoi inviare i file nel modo seguente:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Impostazione** e in seguito cliccare su **Mostra File in Quarantena**.

   Appare il dialog in quarantena.

   Viene visualizzato un elenco dei file che sono stati messi in quarantena.
3. Selezionare i file che si desidera inviare ai laboratori Quick Heal e quindi fare clic su **Invia**.
4. Per chiudere il dialogo Quarantena, fare clic su **Chiudi**.

Bloccare file sospetti compressi

I file compressi sospetti sono programmi dannosi compressi o impacchettati e crittografati utilizzando una varietà di metodi. Questi file quando scompattati possono causare gravi danni ai sistemi informatici. Questa funzione consente di identificare e bloccare tali file imballati sospetti.
Si consiglia di mantenere sempre questa opzione abilitata per garantire che i file sospetti non siano accessibili e quindi prevenire l'infezione.

Configurazione Blocca File Compressi Sospetti

Per configurare **Blocca file compressi sospetti**, procedere come segue:

1. Aprire **Quick Heal antivirus**.

Nel riquadro di sinistra, fare clic su **Protezione** e quindi su **Impostazioni di scansione.**

2. Nella schermata **Impostazioni di scansione**, attivare **Blocca file imballati sospetti.**

Tuttavia, **Blocca file imballati sospetti** è attivato come impostazione predefinita.

Scansione Automatica Rogueware

Questa funzione esegue automaticamente la scansione, rimuove rogueware e falsi software di anti-virus. Se questa funzione è abilitata, tutti i file vengono scansionati per cercare possibili rogueware presenti in un file.

Configurazione della scansione automatica di Rogueware

Per configurare Scansione Rogueware Automatica, seguire questi passaggi:

1. Aprire Quick Heal antivirus.
2. Nel riquadro di sinistra, fare clic su Protezione e quindi su Impostazioni di scansione.
3. Nella schermata Impostazioni di scansione, attivare Scansione automatica Rogueware.

Tuttavia, Scansione Rogueware Automatica è attivata per impostazione predefinita.

Pianificazione di Scansione

Scansionare regolarmente aiuta l'utente a mantenere il sistema libero da virus e altri tipi di infezioni. Questa funzione consente di definire una pianificazione di quando iniziare automaticamente la scansione del sistema. È possibile definire più numeri di piani di scansione per avviare la scansione a proprio piacimento.

Configurare la Scansione Pianificata

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro a sinistra, cliccare su **Protezione** e in seguito cliccare **Opzioni di Scansione**.
3. Nella schermata Impostazioni di scansione, fare clic su **Pianificazione scansione**.

   Viene visualizzata la schermata Pianificazione scansione dettagli.
4. Per definire una nuova pianificazione di scansione, fare clic su **Nuovo**.
5. In **Nome di Scansione**, denominare la scansione.
6. Sotto frequenza di Scansione, l'utente può selezionare l'opzione che più si addice alle sue preferenze fra le seguenti:

   - Frequenza di scansione:

   - Giornaliera: selezionare questa opzione se si desidera avviare la scansione del sistema ogni giorno. Questa opzione è selezionata per impostazione predefinita.
   - Settimanale: selezionare questa opzione se si desidera avviare la scansione del sistema in un determinato giorno della settimana. Quando si seleziona l'opzione Settimanale, l'elenco a discesa Giorni feriali viene attivato in modo da poter selezionare un giorno della settimana.

- Tempo di Scansione:

  - Inizia al primo avvio: questo aiuta a pianificare lo scanner per iniziare al primo avvio della giornata. Se si seleziona questa opzione, non è necessario specificare l'ora del giorno per avviare la scansione. La scansione avviene solo durante il primo avvio indipendentemente dal momento in cui si avvia il sistema.
  - Inizia a: selezionare questa opzione per avviare la scansione del sistema in un determinato momento. Se si seleziona questa opzione, l'elenco a discesa temporale viene attivato dove è possibile impostare il tempo per la scansione. Tuttavia, questa opzione è selezionata come predefinita.

    È possibile definire ulteriormente quanto spesso la scansione dovrebbe iniziare nell'opzione scansione **Tutti i Giorni** o **Ripeti dopo ogni**.

- Priorità di Scansione.

  - Alta: è necessario per impostare un'alta priorità alla scansione.
  - Bassa:è necessaria per impostare una bassa priorità alla scansione. Tuttavia questa impostazione è selezionata come predefinita.

7. Sotto **Opzioni di scansione** è possibile specificare la modalità di scansione, definire le opzioni avanzate per la scansione, l'azione da eseguire quando viene trovato il virus e se si desidera un backup dei file prima di intraprendere qualsiasi azione su di essi. Tuttavia, l'impostazione predefinita è adeguata per una scansione che mantiene il sistema pulito.
8. Nella casella di testo **Nome utente**, immettere il nome utente e la password nella casella di testo **Password**.
9. **Eseguire l'attività il più presto possibile se mancato**: Selezionare questa opzione se si desidera avviare la scansione quando la scansione pianificata è mancato. Questo è utile nel caso in cui il sistema è stato spento e il programma di scansione passato. Più tardi quando verrà acceso il sistema, il programma di scansione si avvierà automaticamente il più presto possibile.

   Questa opzione è disponibile solo su Microsoft Windows Vista e sistemi operativi successivi.
10. Cliccare **Avanti**.

    Viene visualizzata la schermata Configura pianificazione scansione per l'aggiunta di cartelle da scansionare.
11. Cliccare **Aggiungi cartella**.
12. Nella finestra Sfoglia cartella, selezionare le unità e le cartelle da analizzare. È possibile aggiungere più numeri di unità e cartelle secondo il vostro requisito.

    Se si desidera escludere la scansione delle sottocartelle, è anche possibile selezionare **Escludi sottocartella**. Fare clic su **OK**.
13. Nella schermata Configura pianificazione scansione, fare clic su **Avanti**.

14. Viene visualizzato un riepilogo della pianificazione di scansione. Verificare e fare clic su **Fine** per salvare e chiudere la finestra di dialogo Pianificazione scansione.
15. Fare clic su **Chiudi** per chiudere la schermata Pianificazione scansione.

Modificare una pianificazione di scansione

Questa funzione consente di modificare la pianificazione della scansione se richiesto. Per modificare una pianificazione della scansione, attenersi alla seguente procedura:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare su **Protezione** e in seguito cliccare su **Impostazioni Scansione**.
3. Nella schermata delle opzioni di Scansione, cliccare **Pianificazione di Scansione**.
4. Viene visualizzata la schermata Pianificazione scansione dettagli.
5. Selezionare la pianificazione di scansione che si desidera modificare e quindi fare clic su **Modifica**.
6. Apportare le modifiche richieste nella pianificazione di scansione e quindi fare clic su **Avanti**.
7. Nella schermata Configura pianificazione scansione, è possibile aggiungere o rimuovere le unità e le cartelle secondo le preferenze e quindi fare clic su **Avanti**.
8. Controlla il riepilogo della modifica nella pianificazione della scansione.
9. Fare clic su **Fine** per chiudere la finestra di dialogo Pianificazione scansione.
10. Fare clic su **Chiudi** per chiudere la schermata Pianificazione scansione.

Rimozione Scansione Pianificata

E’ possibile rimuovere la scansione pianificata quando è richiesto. Per rimuovere la scansione pianificata, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Impostazioni Scansione**.
3. Nella schermata Opzioni Scansione, cliccare su **Scansione Pianificata**.

   Verrà mostrata la schermata con i dettagli della Scansione Pianificata.
4. Selezionare la Scansione Pianificata che si desidera rimuovere e poi cliccare su **Rimuovi**.

   Verrà mostrata la schermata di conferma.
5. Cliccare **Sì** per rimuovere la Scansione Pianificata selezionata.
6. Per chiudere la schermata di Scansione Pianificata, cliccare su **Chiudi**.

Per maggiori informazioni sulla configurazione di Impostazioni Scansione, vedere Impostazioni Scansione.

Escludi File & Cartelle

Grazie a questa funzione è possibile specificare quali file e cartelle non devono essere inclusi nella scansione per la ricerca di ransomware e altri attacchi dannosi. L'esclusione dei file consente di evitare la scansione non necessaria di file che sono già stati scansionati o per i quali si è sicuri che alcuni di essi non debbano essere scansionati.

E' possibile escludere i file dalla scansione effettuata tramite i moduli:

- Rilevazione virus noti
- DNAScan
- Scansione archivi file sospetti
- Rilevazione Comportamentale
- Rilevazione Ransomware

Configurazione Escludi File & Cartelle

Per configurare Escludi File & Cartelle, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Impostazioni Scansione**.
3. Nella schermata Impostazioni Scansione, cliccare **Escludi File & Cartelle**.

   Verrà mostrata la schermata con i dettagli di Escludi File & Cartelle. Qui è possibile visionare l'elenco dei file esclusi e delle cartelle che sono state aggiunte.
4. Per aggiungere un nuovo file o cartella, cliccare su **Aggiungi**.

   Verrà mostrata la schermata Escludi Nuovo Elemento.
5. Nella casella di testo **Elemento**, fornire il percorso del file o della cartella. E' inoltre possibile cliccare sull'icona del file o cartella per selezionare il percorso.

   Assicurarsi di fornire il percorso al file o cartella corretta, altrimenti viene mostrato un messaggio.
6. In Escludi da, selezionare i moduli di scansione dai quali si desidera escludere i file e le cartelle selezionate.

   E' possibile selezionare Rilevazione virus noti o qualunque opzione tra DNAScan, scansione archivi file sospetti, Rilevazione Comportamentale e Rilevazione Ransomware.
7. Cliccare **OK**.
8. Per salvare le impostazioni, cliccare su **Salva Modifiche**.

Nota:

- Se si riceve un avviso per un virus noto in un file pulito, è possibile escluderlo dalla Scansione di Rilevazione virus noti.
- Se si riceve un avviso da DNAScan in un file pulito, è possibile escluderlo dalla Scansione di DNAScan.

Quarantena & Backup

Questa funzione consente di isolare in modo sicuro i file infetti o sospetti. I file sospetti vengono messi in quarantena in un formato crittografato per impedirne l'esecuzione. Questo consente di prevenire l'infezione.

Se si desidera ricevere una copia dei file infetti prima della loro riparazione, selezionare l'opzione **Backup prima di eseguire un'azione** in Impostazioni Scansione.

È inoltre possibile impostare quando i file in quarantena devono essere rimossi dalla stessa e avere un loro backup se si rende necessario.

Configurazione Quarantena & Backup

Per configurare Quarantena & Backup, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Impostazioni Scansione**.
3. Nella schermata Impostazioni Scansione, cliccare su **Quarantena & Backup**.

   Verrà mostrata la schermata con i dettagli di Quarantena & Backup.
4. Selezionare **Cancella quarantena/backup file successivamente** ed impostare il numero di giorni dopo i quali i file dovrebbe essere rimossi automaticamente dalla Quarantena. Tuttavia, 30 giorni sono impostati per impostazione predefinita.
5. Per vedere quali file sono stati inseriti in quarantena, cliccare su **Vedi File**. Verrà mostrato un elenco di file in quarantena. E' possibile intraprendere una delle seguenti azioni sui file messi in quarantena:
   - Aggiungi: Permette di aggiungere nuovi file dalle cartelle e unità da inserire in quarantena manualmente.
   - Rimuovi: Permette di rimuovere qualsiasi file di quarantena dall'elenco Quarantena. Per rimuovere un file, selezionare il file e poi cliccare sul pulsante **Rimuovi**.
   - Ripristina : Permette di ripristinare un file di quarantena nella sua posizione originale. Quando si trova un file affidabile in quarantena e si prova a ripristinarlo, viene visualizzata un'opzione per aggiungere il file all'elenco di

esclusione. È possibile aggiungere il file all'elenco di esclusione in modo che lo stesso file non venga trattato come sospetto e messo di nuovo in quarantena. Per ripristinare un file, selezionare il file e quindi fare clic sul pulsante **Ripristina**.

- Rimuovi tutto: Consente di rimuovere tutti i file in quarantena dall'elenco Quarantena. Per rimuovere tutti i file, fare clic sul pulsante **Rimuovi tutto**. Nel messaggio di conferma, fare clic su **Sì** per rimuovere tutti i file.
- Invia: Consente di inviare i file in quarantena ai nostri laboratori di ricerca. Per inviare un file, selezionare il file e quindi fare clic sul pulsante **Invia**.

6. Per chiudere il dialog Quarantena, cliccare sul pulsante **Chiudi**.

Escludi Estensioni File

È possibile creare un elenco di estensioni dei file che si desidera escludere dalla Protezione Virus. È consigliabile escludere solo le estensioni dei file attendibili. Protezione Virus non analizza le estensioni dei file elencati e si concentrerà solo su quei file che sono inclini a comportamenti dannosi.

Creazione Elenco Esclusioni

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Protezione** ed in seguito cliccare **Opzioni di Scansione**.
3. Nella schermata delle Opzioni di Scansione, cliccare **Escludi le estensioni di file**.
4. Nella casella di testo Aggiungi, inserire l'estensione del file e quindi fare clic su **Aggiungi**.

   Se l'estensione aggiunta è incorretta, selezionare l'estensione nell'elenco e fare clic su **Rimuovi** per rimuoverlo.
5. Per salvare l'elenco, cliccare **OK**.

Protezione Navigazione

Quando gli utenti visitano siti Web dannosi, alcuni file possono essere installati sui loro sistemi. Questi file possono diffondere malware, rallentare il sistema, o danneggiare altri file. Questi attacchi possono causare danni sostanziali al sistema.

La Protezione di Navigazione assicura che i siti web dannosi siano bloccati mentre gli utenti accedono a Internet. Una volta che la funzione è abilitata, qualsiasi sito web che si accede viene scansionato e bloccato se trovato per essere dannoso.

Configurazione Protezione Navigazione

Per configurare la Protezione di Navigazione, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Protezione** ed in seguito cliccare **Protezione Navigazione**.
3. Accendi la **Protezione di Navigazione**.

   La Protezione di Navigazione è attivata.

Protezione Phishing

Il phishing è un tentativo fraudolento, di solito effettuato tramite e-mail, di rubare le informazioni personali. Queste e-mail di solito sembrano essere state inviate da organizzazioni e siti web apparentemente ben noti come banche, aziende e servizi che cercano le informazioni personali come il numero di carta di credito, numero di previdenza sociale, numero di conto o password.

Protezione Phishing* impedisce agli utenti di accedere a phishing e siti web fraudolenti. Non appena si accede a un sito web, viene scansionato per qualsiasi comportamento di phishing. Se trovato così, è bloccato per evitare qualsiasi tentativo di phishing.

Configurare la Protezione Phishing

Per configurare Phishing Protection, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare su **Protezione** e in seguito cliccare **su Protezione Phishing**.
3. Accendere **Phishing Protection**.

   La Protezione Phishing è attiva.

Safe Banking

Con il banking online, l'utente può controllare i suoi conti, pagare le bollette, comprare e vendere azioni e trasferire denaro tra diversi conti. Per fare queste attività, si visita un sito bancario, inserire le credenziali di identità, e di effettuare le transazioni necessarie.

Durante la visita di un sito web bancario, si può diventare una preda di un sito web bancario falso o quando si digita le credenziali, le informazioni possono essere oggetto di phishing per un truffatore. Di conseguenza, potresti perdere i tuoi soldi.

Safe Banking* protegge da tutte le possibili situazioni in cui l'identità o le credenziali dell'utente possono essere compromesse. Safe Banking lancia l'intera sessione bancaria in un ambiente sicuro che protegge i dati vitali.

Safe Banking ha le seguenti caratteristiche:

- La navigazione viene lanciata in un ambiente isolato per evitare malware zero-day da infettare il computer.
- La tua attività bancaria è isolata dalle minacce di Internet.

- Tutti i tipi di strumenti di registrazione dei tasti sono bloccati per evitare key logging di dati riservati.
- Utilizza DNS sicuro per prevenire gli attacchi di hacking.
- Assicura che l'utente visiti solo siti web verificati e protetti.

Per lavorare nell'ambiente del Safe Banking, procedere come segue:

- Impostare Safe Banking
- Avviare Safe Banking

Impostare Safe Banking

È possibile utilizzare la funzione Safe Banking con le impostazioni predefinite. Puoi anche configurare la funzione Safe Banking per una maggiore sicurezza in base alle tue esigenze.

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare su **Protezione** ed in seguito su **Safe Banking**.
3. Su Safe Banking, fare clic sull'icona **Impostazioni**. Selezionare le seguenti opzioni come richiesto:
    - **Protezione dagli attacchi basati su DNS**: Selezionare questa opzione per proteggere il sistema dalla visita di siti web fraudolenti. È possibile selezionare una rete DNS dall'elenco DNS specificato o fornire un ID alternativo. La connessione di rete sarà stabilita solo attraverso la rete configurata.
    - **Condivisione appunti:** selezionare questa opzione per consentire la condivisione degli appunti. È possibile consentire la condivisione sia o entrambi dal desktop di default per isolato ambiente sicuro bancario o in altro modo rotondo.
    - **Impostazioni scorciatoie di tastiera**: Selezionare questa opzione per creare un tasto di scelta rapida per passare dal desktop Safe Banking al desktop Windows. Safe Banking viene lanciato in un ambiente isolato e quindi non è possibile accedere a qualsiasi sistema o cartella da questa finestra. La creazione di un tasto di scelta rapida aiuta a passare tra Safe Banking e desktop di Windows.
4. Per salvare le nuove impostazioni, cliccare **Salva Modifiche**.

Avvio di Safe Banking

È possibile accedere alla funzione Safe Banking separatamente. Quando si installa Quick Heal antivirus sul desktop, è installato anche Safe Banking. Un'icona di collegamento a Safe Banking è creata sul desktop.

Per lanciare un sito web con la protezione Safe Banking, seguire questi passaggi:

1. Fare clic sull'icona di scelta rapida per **Safe Banking**. O fare clic destro sull'icona Quick Heal nel vassoio di sistema e fare clic su **Safe Banking**.

   Safe Banking viene avviato. È possibile navigare i siti web che si desidera utilizzando i browser supportati disponibili sulla barra delle applicazioni.

   È inoltre possibile segnalibro un sito web in modo da poter navigare in un tale sito web facilmente in futuro.

2. Fai clic su Aggiungi segnalibro e digita l'URL del sito web nella finestra di dialogo **Aggiungi segnalibro**. Fai clic su **Aggiungi**.

   Si può anche aggiungere un sito web per una categoria in modo che sia facile per cercare il sito preferito dall'utente in seguito.

3. Fare clic su **Visualizza segnalibro** e fare clic sull'URL che si desidera eseguire nel browser sicuro.

   Note:

   Questa funzione è supportata solo sui browser Internet Explorer, Google Chrome e Mozilla Firefox. Questa funzione non è supportata sul browser Microsoft Edge del sistema operativo Windows 10.

Protezione Firewall

Firewall protegge il sistema da intrusi e hacker monitorando e filtrando il traffico di rete in entrata e in uscita. Qualsiasi programma sospetto che può essere dannoso per i computer o sistemi è bloccato. Firewall protegge i computer da programmi dannosi sia da connessione Internet esterna o da reti in entrata nel sistema.

Configurare la Protezione Firewall

Per configurare la Protezione Firewall, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare su **Protezione** ed in seguito su **Protezione Firewall** .
3. Accendere e spegnere la **Protezione Firewall** usando il pulsante toggle.

   Tuttavia, la protezione del firewall è attivata per impostazione predefinita.

4. Per impostare la protezione firewall, fare clic in qualsiasi punto dell'area di protezione firewall.

   Per abilitare il monitoraggio delle reti Wi-Fi non sicure, attivare Monitor Wi-Fi Networks.

   Se hai abilitato questa opzione e provi a connetterti alle connessioni Wi-Fi non garantite, verrà visualizzato un avviso. Puoi decidere se vuoi connetterti a tali connessioni non garantite.

5. Per configurare le regole per accedere a Internet e controllare il traffico di rete, impostare le seguenti politiche:

   - Regole di Programma: Creare regole per i programmi che hanno accesso alla rete Internet.
   - Impostazioni Avanzate: Creare regole per traffici di rete in entrata e in uscita

Regole di Programma

Con Regole di programma, è possibile consentire o bloccare i programmi di accesso a Internet.

Per creare regole per i programmi, segui questi passaggi:

1. Nella schermata della Protezione Firewall, cliccare il pulsante **Configura** Regole di Programma.
2. Nella schermata Configura Regole di Programma, cliccare il pulsante **Aggiungi** per aggiungere un programma.

   Solo un programma eseguibile può essere aggiunto.
3. Il programma aggiunto viene inserito nell'elenco dei programmi. Nella colonna Accesso, selezionare **Consenti** o **Nega** per accedere alla rete come richiesto.
4. Per salvare le impostazioni, cliccare **OK**.

Autorizzare solo programmi affidabili

I programmi affidabili sono quei programmi che sono verificati e la cui identità è conosciuta, mentre i programmi inaffidabili sono quelli che non sono verificati o sono sospetti. Programmi dannosi mascherano la loro identità per eseguire un'operazione segreta. Tali programmi possono essere dannosi per la rete e computer.

È possibile bloccare tutti i programmi inaffidabili dall'accesso a Internet selezionando la casella **Consenti solo programmi affidabili**.

Livello di Sicurezza

Il livello di sicurezza del firewall include quanto segue:

- Basso: consente tutte le connessioni in entrata e in uscita.

- Media: monitora il traffico in entrata e visualizza il messaggio secondo il comportamento sospetto di un'applicazione.
- Alto: Monitora i traffici in entrata e in uscita e visualizza il messaggio secondo il comportamento sospetto di un'applicazione.
- Blocca tutto: blocca tutte le connessioni in entrata e in uscita. Se si imposta questo livello di sicurezza, la connessione a Internet per tutte le applicazioni, tra cui Quick Heal antivirus, verrà bloccata. Ad esempio, l'aggiornamento e l'invio delle informazioni di sistema di Quick Heal tra le altre caratteristiche potrebbe non funzionare.

Impostazioni Avanzate

1. Per creare regole per i traffici di rete in entrata e in uscita, segui questi passaggi:
2. Nella schermata Protezione firewall, fare clic sul pulsante Configura accanto a Impostazioni avanzate.
3. Nella pagina Impostazioni avanzate, selezionare quanto segue come richiesto:
    - **Visualizza messaggio di avviso**: selezionare questa opzione se si desidera ottenere messaggi di avviso se le connessioni corrispondenti alla regola eccezioni sono fatte per le connessioni in uscita bloccate. Questo vale solo per le connessioni esterne.
    - **Crea report**: selezionare questa opzione se si desidera creare un report. Si può anche configurare un percorso diverso per salvare il report.
    - **Connessioni di rete**: Con questa opzione, impostare un profilo di rete per le connessioni di rete.
    - **Regole di traffico**: Usando questa opzione, impostare le regole per il traffico di rete.
4. Per salvare le modifiche, cliccare **OK**.

Connessioni Network

Tramite Connessioni Network, è possibile impostare un profilo Firewall per le connessioni di rete. In Impostazioni del profilo di rete, è possibile visualizzare le seguenti impostazioni.

Impostazione	Descrizione
Profilo Network	Home: Tutte le connessioni in entrata e in uscita sono ammesse tranne eccezioni. Lavoro: Tutte le connessioni in entrata e in uscita sono ammesse tranne eccezioni. Pubblico: Tutte le connessioni in entrata e in uscita sono ammesse tranne eccezioni. Limitato: Tutte le connessioni in entrata e in uscita sono bloccate tranne eccezioni. Nota: La logica del profilo di rete può essere modificata in base alle proprie

	esigenze. Ad esempio, se un ambiente di rete è considerato meno rischioso, è possibile attivare o disattivare la modalità stealth. Allo stesso modo, è possibile consentire o bloccare la condivisione di file e stampante. Tuttavia, l'impostazione predefinita è ideale per la sicurezza richiesta.
Modalità Nascosta	L'attivazione della modalità Nascosta nasconde il sistema nella rete rendendolo invisibile agli altri evitando così gli attacchi.
Condivisione di stampanti e file	Abilitare questa opzione permetterà all'utente di condividere file e stampanti con altri utenti. Tuttavia, con la condivisione di file e stampante, i file possono essere accessibili da entità non autorizzate.

Regole di Traffico

Tramite Regole di Traffico, è possibile consentire o bloccare il traffico di rete. È possibile aggiungere un'eccezione per consentire o negare le comunicazioni in entrata e in uscita attraverso indirizzi IP e porte.

Per configurare una policy, procedere come segue:

1. Nella schermata Impostazioni avanzate, fare clic sulla scheda **Regole di traffico**.
2. Fare clic sul pulsante **Aggiungi**.
3. Nella casella di testo **Nome eccezione**, scrivere un nome di regola e quindi selezionare un protocollo. Fare clic su Avanti.

   Il protocollo include: TCP, UDP e ICMP.
4. Cliccare il pulsante **Aggiungi**.
5. Nella sezione **Sotto indirizzo IP locale**, selezionare un **qualsiasi indirizzo IP, indirizzo IP o intervallo di indirizzi IP**. Digitare l'indirizzo IP di conseguenza e quindi fare clic su **Avanti.**
6. In **Porte TCP/UDP** locali, seleziona **Tutte le porte, Porta specifica**(e), o **Intervallo di porte**. Digita le porte di conseguenza e quindi fai clic su **Avanti**.
7. In **Indirizzo IP remoto**, selezionare **Qualsiasi indirizzo IP**, **indirizzo IP** o **intervallo di indirizzi IP**. Digitare l'indirizzo IP di conseguenza e quindi fare clic su **Avanti**.
8. In **Porte TCP/UDP remote**, seleziona **Tutte le porte, Porta specifica(e), o Intervallo di porte**. Digita le porte di conseguenza e quindi fai clic su **Avanti**.
9. In Seleziona azione, selezionare **Consenti o Nega**.
10. In **Profilo di rete**, selezionare o una combinazione delle opzioni del profilo come **Domestico, Pubblico, Lavoro o Ristretto**.
11. Fare clic su **Fine.**

La tabella seguente descrive i pulsanti e le loro funzioni.

Pulsante	Descrizione
Aggiungi	Aiuta a creare una regola di eccezione.
Elimina	Aiuta a eliminare una regola di eccezione dall'elenco. Selezionare la regola e poi fare clic su **Elimina.**
Su	Aiuta a spostare una regola verso l'alto per organizzare secondo le preferenze dell'utente.
Giù	Aiuta a spostare una regola verso il basso per organizzare secondo le preferenze dell'utente.
Predefinite	Consente di impostare le regole per le impostazioni predefinite.
OK	Serve per salvare le nuove preferenze.
Cancella	Aiuta a cancellare le preferenze impostate e a chiudere il dialog delle Impostazioni Avanzate.

IDS/IPS

Con IDS/IPS, il computer dell'utente rimane sicuro da tentativi di intrusioni indesiderate o attacchi hacker.

Abilitare IDS/IPS

Per attivare il IDS/IPS, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Protezione** e in seguito cliccare su **IDS/IPS**.
3. Attivare **IDS/IPS**.

Protezione Email

Con questa funzione, è possibile configurare le regole di protezione per tutte le email in arrivo. Queste regole includono il blocco degli allegati/i infetti (malware, spam e virus) nelle email. È inoltre possibile impostare un'azione che deve essere presa quando viene rilevato malware nelle e-mail.
Email Security include le seguenti funzionalità.

- Protezione Email
- Protezione delle email dei client attendibili
- Protezione Spam

Protezione Email

Questa funzione è attivata per impostazione predefinita che fornisce una protezione ottimale per la posta in arrivo da e-mail dannose. Si consiglia di mantenere sempre la protezione e-mail attivata per garantire la protezione e-mail.

Configurare la Protezione Email

Per configurare la Protezione Email, segui questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, fare clic su **Protezione** e quindi su **Protezione e-mail.**
3. Nella schermata **Protezione email**, attiva **Protezione email.**

   Tuttavia, Email Protection è attivata per impostazione predefinita.
4. Viene attivata la protezione contro il malware proveniente dalle email.
5. Per impostare ulteriori regole di protezione per le e-mail, fare clic su **Protezione e-mail**.
6. Selezionare **Visualizza messaggio di avviso** se si desidera un messaggio quando un virus viene rilevato in un'e-mail o allegato.

   Note:

   Il messaggio sui virus include le seguenti informazioni: Nome del virus, indirizzo email del mittente, oggetto dell'e-mail, nome dell'allegato e azione intrapresa.
7. In **Seleziona azione da eseguire quando viene trovato il virus,** selezionare **Ripara** per riparare le email dell'utente o l'allegato quando viene trovato un virus, oppure selezionare **Elimina** per eliminare le email e gli allegati infetti.

   Note:

   Se l'allegato è impossibile da riparare verrà eliminato.
8. Selezionare **Backup prima di agire** se si desidera avere un backup delle e-mail prima di intraprendere un'azione su di loro.
9. In **Impostazioni di controllo allegati,** selezionare un'opzione per bloccare alcuni tipi di email e allegati.
10. Per salvare le impostazioni, fare clic su **Salva modifiche**.

Impostazioni Controllo Allegati

Opzione	Descrizione
Blocca allegati con estensioni multiple	Aiuta a bloccare gli allegati nelle email con estensioni multiple. I Worm usano comunemente estensioni multiple che possono essere bloccate usando questa funzione**.**
Blocca email confezionate per esplicitare le vulnerabilità	Aiuta a bloccare email cui scopo è quello di trovare ed identificare le vulnerabilità delle mail dei client.
Attiva controllo allegati	Aiuta a bloccare gli allegati email con estensioni specifiche o tutte le estensioni. Se questa opzione viene selezionata, vengono attivate le seguenti opzioni: **Blocca tutti gli allegati**: Aiuta a bloccare tutti i tipi di allegati nelle email. **Blocca gli allegati specificati dall'utente**: Aiuta a bloccare gli allegati email con alcune estensioni. Se selezioni questa opzione, il pulsante **Configura** viene attivato. Per ulteriori impostazioni, fare clic su **Configura** e impostare le seguenti opzioni: ● In **estensioni specificate dall'utente**, selezionare le estensioni che si desidera mantenere in modo che gli allegati e-mail con tali estensioni sono bloccati e tutte le estensioni rimanenti vengono eliminati. ● Se alcune estensioni non sono nell'elenco che si desidera bloccare, digitare tali estensioni nella casella di testo estensione e quindi fare clic su **Aggiungi** per aggiungerle nell'elenco. ● Fare clic su **OK** per salvare le modifiche.

Configurazione degli allegati specificati dall'utente

Per configurare gli allegati specificati dall'utente, procedere come segue:

1. Nella schermata Protezione email, selezionare Abilita controllo allegati.
2. Selezionare Blocca gli allegati specificati dall'utente.
3. Il pulsante Configura è attivato.
4. Fare clic su Configura.
5. Nell'elenco delle estensioni specificate dall'utente, ci sono un certo numero di estensioni che sono bloccate per impostazione predefinita. È possibile aggiungere più estensioni, se necessario.

6. Per aggiungere un'estensione, digitare l'estensione nell'elenco di testo e fare clic su **Aggiungi.**
7. Per rimuovere un'estensione, selezionare l'estensione e fare clic su **Elimina**.
8. Per salvare le impostazioni, fare clic su **OK**.

Protezione affidabile dei client di posta elettronica

Poiché l'email è il mezzo di comunicazione più diffuso, viene utilizzato come una modalità conveniente per fornire malware e altre minacce. Gli autori di virus cercano sempre nuovi metodi per eseguire automaticamente i loro codici virali utilizzando le vulnerabilità dei client di posta elettronica più diffusi. I vermi usano anche la propria routine del motore SMTP per diffondere la loro infezione.

Configurazione della protezione dei client di posta elettronica affidabili

Per configurare Trusted Email Clients Protection, seguire questi passaggi:

1. Aprire Quick Heal antivirus.
2. Nel riquadro di sinistra, fare clic su Protezione e quindi su **Protezione e-mail**.
3. Nella schermata Protezione email, attivare **Protezione Clienti Email Attendibili**.
4. Per aggiungere un nuovo client di posta elettronica, fare clic su **Trusted Email Clients Protection**.

   Viene visualizzata la schermata dei dettagli della protezione dei client di posta elettronica affidabili.
5. Fare clic su **Sfoglia** e selezionare un client di posta affidabile
6. Fare clic su **Aggiungi** per aggiungere il client di posta elettronica nella lista.
7. Per salvare le impostazioni, fare clic su **Salva modifiche**.

Protezione Spam

Protezione Spam * consente di differenziare le email autentiche e filtrare le email indesiderate come spam, phishing ed email per adulti. Raccomandiamo di mantenere la protezione dello Spam permessa.

Configurazione Protezione Spam

Per configurare la protezione dello Spam, segua questi punti:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Protezione Email**.
3. Nella schermata Protezione Email, abilitare **Protezione Spam**.
4. Per impostazioni dettagliate, cliccare su **Protezione Spam**.

5. Selezionare l'**oggetto Tag subject con testo (Consigliato)**, per contrassegnare l'oggetto di un'e-mail come SPAM.
6. In **livello protezione Spam**, impostare il livello di protezione:
    - Basso – Selezionare questa opzione qualora si riceva soltanto poche e-mail di spam o qualora si desideri bloccare solo le e-mail di spam comuni. C'è una piccola possibilità che e-mail attendibili siano identificate come spam.
    - Moderato (Consigliato) – Garantisce un filtraggio ottimale. Questo è ideale se si ricevono tante e-mail spam. Tuttavia, c'è la possibilità che diverse e-mail attendibili siano identificate come spam. Si consiglia di selezionare il filtro moderato che è anche l'opzione abilitata per impostazione predefinita.
    - Alto – Applica criteri di filtraggio rigorosi, ma non è l'ideale in quanto è molto probabile che anche le e-mail attendibili vengano bloccate. Selezionare un filtro rigoroso solo quando si ricevono troppe e-mail di spam altrimenti è sempre preferibile utilizzare mezzi alternativi per bloccare le e-mail di spam.
7. Selezionare **Abilita blacklist e-mail** per creare una blacklist di indirizzi e-mail. Le regole di protezione verranno applicate sugli indirizzi e-mail che si trovano in blacklist.
8. Selezionare **Abilita whitelist e-mail** per creare una whitelist di indirizzi e-mail. Le regole di protezione verranno applicate sugli indirizzi e-mail che si trovano in whitelist.
9. Selezionare **Abilita plugin AntiSpam** per implementare le regole di protezione per il plug-in di AntiSpam.
10. Cliccare su **Salva Modifiche** per salvare le impostazioni.

Creazione blacklist di indirizzi e-mail per la Protezione Spam

La blacklist è l'elenco di indirizzi e-mail indesiderati. Il contenuto degli indirizzi e-mail nella blacklist viene filtrato e contrassegnato come "[SPAM] -".

Questa funzione è utile in particolare se il server utilizza un relay di posta aperto, utilizzato per inviare e ricevere e-mail da mittenti sconosciuti. Questo sistema di posta può essere utilizzato in modo improprio dagli spammer. Tramite la blacklist, è possibile filtrare le e-mail in arrivo indesiderate o provenienti da mittenti sconosciuti sia per gli indirizzi e-mail che per i domini.

Per aggiungere indirizzi e-mail alla blacklist, seguire questi passaggi:

1. Nella schermata delle impostazioni di Protezione Spam, selezionare **Abilita blacklist e-mail**.

   Viene abilitato il pulsante Personalizza.
2. Cliccare su **Personalizza**.
3. Inserire l'indirizzo e-mail nella casella di testo blacklist e poi cliccare su **Aggiungi**.

   Durante l'inserimento di un indirizzo e-mail, fare attenzione a non inserire nella blacklist lo stesso indirizzo e-mail che è stato inserito nella whitelist, altrimenti verrà mostrato un messaggio di avviso.

Per modificare un indirizzo e-mail, selezionare l'indirizzo e-mail nell'elenco e fare clic su Modifica. Per rimuovere un indirizzo e-mail, seleziona un indirizzo e-mail e fai clic su Rimuovi.

4. E’ possibile importare la blacklist cliccando su **Importa Lista**.

   Ciò è molto utile quando è stato esportato l'elenco delle e-mail o salvato i dati AntiSpam e si desidera utilizzare tali e-mail.

5. E’ possibile esportare la blacklist cliccando su **Esporta Lista**.

   Questo esporta tutti gli indirizzi e-mail esistenti nell'elenco. Ciò è utile quando si desidera reinstallare l'antivirus Quick Heal in un secondo momento o su un altro sistema e si desidera inserire gli stessi indirizzi e-mail successivamente.

6. Cliccare su **OK** per salvare le impostazioni.

Creazione whitelist di indirizzi e-mail per la Protezione Spam

Whitelist è l'elenco degli indirizzi e-mail attendibili. Il contenuto degli indirizzi e-mail inseriti nella whitelist può ignorare il criterio di filtraggio della protezione antispam e non viene contrassegnato come SPAM.

Ciò è utile se si rileva che alcuni indirizzi e-mail autentici vengono contrassegnati come SPAM. Se si inserisce un dominio nella blacklist ma si desidera comunque ricevere e-mail da determinati indirizzi con quel dato dominio.

Per aggiungere gli indirizzi e-mail alla whitelist, seguire questi passaggi:

1. Nella schermata delle impostazioni di Protezione Spam, selezionare **Abilita whitelist e-mai**.

   Il pulsante Personalizza verrà così attivato.

2. Cliccare su **Personalizza**.

3. Inserire un indirizzo e-mail nella casella di testo whitelist e poi cliccare su **Aggiungi**.

   Durante l'inserimento di un indirizzo e-mail, fare attenzione a non inserire nella whitelist lo stesso indirizzo e-mail che è stato inserito nella blacklist, altrimenti viene mostrato un messaggio di avviso.

   Per modificare un indirizzo e-mail, selezionare l'indirizzo e-mail nell'elenco e fare clic su **Modifica**. Per rimuovere un indirizzo e-mail, selezionare un indirizzo e-mail e fare clic su **Rimuovi**.

4. E’ possibile importare la whitelist cliccando su **Importa Lista.**

   Ciò è molto utile se si è esportato l'elenco di e-mail o salvato dati AntiSpam e si desidera utilizzare tali e-mail.

5. E’ possibile esportare la whitelist cliccando su **Esporta Lista**.

Questo esporta tutti gli indirizzi e-mail esistenti nell'elenco. Ciò è utile quando si desidera reinstallare l'antivirus Quick Heal in un secondo momento o su un altro sistema e si desidera che gli stessi indirizzi e-mail vengano inseriti successivamente.

6. Cliccare su **OK** per salvare le impostazioni.

Aggiungi Domini alla whitelist oppure blacklist

Per aggiungere indirizzi di dominio alla whitelist o blacklist, seguire questi passaggi:

1. Selezionare tra le opzioni **Abilita whitelist e-mail** oppure **Abilita blacklist e-mail** e poi cliccare su **Personalizza**.
2. Digitare il dominio e poi cliccare su **Aggiungi**.

   Il dominio dovrebbe essere nel formato: `*@mytest.com`.
3. Per salvare le modifiche effettuate, cliccare su **OK**.

Protezione Unità USB

Ogni volta che qualsiasi unità esterna è collegata al sistema, la funzione di esecuzione automatica si avvia automaticamente e potrebbero essere avviati anche tutti i programmi nell'unità. Il malware ad esecuzione automatica può anche essere scritto nelle unità in modo che si avvii non appena l'unità viene collegata e diffonda il malware nel sistema. Questa funzione ti permette di proteggere i dispositivi USB dai malware con esecuzione automatica.

Per configurare Protezione Unità USB, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Protezione Unità USB**.

   Viene visualizzata la schermata dei dettagli degli Strumenti.
3. Nell’elenco Seleziona unità removibile, sono elencate tutte le unità removibili collegate al sistema. Selezionare l’unità e fare clic sul pulsante **Unità Removibile Sicura**.

   L’unità sarà messa in sicurezza contro i malware con esecuzione automatica quando vengono utilizzati in altri sistemi.

Consiglio:

Quick Heal consiglia di mantenere sempre disabilitata la funzione di autorun della propria unità USB.

Protezione Unità Esterne

Ogni volta che qualsiasi dispositivo esterno come unità USB o CD/DVD viene utilizzato con il computer, il sistema è a rischio virus e malware che possono infiltrarsi attraverso i dispositivi esterni. Questa funzione consente di impostare regole di protezione per dispositivi esterni come CD, DVD e unità USB.

Protezione Unità Esterne include le seguenti funzionalità.

- Protezione di Autorun
- Scansione Unità Esterne
- Scansione Windows Mobile

Protezione di Autorun

La funzione di Autorun dei dispositivi USB o dei CD/DVD tende a funzionare non appena tali dispositivi vengono collegati al computer. Il malware di esecuzione automatica può anche avviarsi con i dispositivi e diffondere malware che possono causare danni sostanziali al computer. Questa funzione permette di proteggere il computer dal malware ad esecuzione automatica.

Configurazione Protezione di Autorun

Per configurare la Protezione di Autorun, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Protezione Unità Esterne**.
3. Nella schermata di Protezione Unità Esterne, abilitare la **Protezione di Autorun**.

   La Protezione di Autorun viene abilitata.

Scansione Unità Esterne

Le unità basate su USB sono dispositivi esterni in grado di trasferire malware al sistema. Con questa funzione, è possibile scansionare le unità basate su USB non appena vengono collegate al computer.

Configurazione Scansione Unità Esterne

Per configurare Scansione Unità Esterne, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Protezione Unità Esterne**.
3. Nella schermata Protezione Unità Esterne, abilitare **Scansione Unità Esterne**.

   Scansione Unità Esterne viene abilitata.
4. Per impostazioni dettagliate, cliccare su **Scansione Unità Esterne**.
5. Selezionare una delle seguenti opzioni:
   - **Scansiona solo i file nella directory principale dell'unità**: Selezionare questa opzione se si desidera eseguire la scansione dei file solo nella directory principale dell'unità. I file all'interno delle cartelle sull'unità principale vengono ignorati. Questa scansione richiede poco tempo ma è meno sicura. Tuttavia, questa opzione è selezionata per impostazione predefinita.
   - **Scansiona intera unità**: Selezionare questa opzione se si desidera eseguire la scansione di tutti i file sull'unità USB. Questa scansione richiede tempo ma è più sicura.
6. Cliccare su **Salva Modifiche** per salvare le impostazioni.

Suggerimento:

Scansione Unità Esterne non funziona se la Protezione Furto Dati è abilitata, ed è selezionata la sua option **Blocco completo degli accessi alle unità esterne**.

Scansione Windows Mobile

Questa funzione permette di impostare le regole per ricevere una notifica ogni volta che un telefono Windows Mobile che utilizza un cavo USB viene collegato per la scansione.

Configurazione Scansione Windows Mobile

Per configurare Scansione Windows Mobile*, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Protezione Unità Esterne**.
3. Nella schermata di Protezione Unità Esterne, abilitare **Scansione Windows Mobile**.

   Scansione Windows Mobile viene abilitata.

Browser Sandbox

Quando si naviga in Internet, non si è a conoscenza di quali siano i siti affidabili e verificati. I siti attendibili sono quelli che pubblicano la propria identità in modo che vengano stabiliti come

entità conosciute. Tuttavia, tutti i siti non attendibili non sono siti falsi o siti di phishing. I siti Web non attendibili possono essere siti Web commerciali, di fornitori, venditori, terze parti, pubblicità e siti Web di intrattenimento.

I siti dannosi mascherano la propria identità per eseguire un'operazione nascosta. Questi siti possono violare le credenziali riservate, infettare il computer e diffondere messaggi di spam.

Browser Sandbox* protegge da qualsiasi tipo di attacco dannoso. Browser Sandbox applica una rigorosa policy di sicurezza per tutti i siti Web non attendibili e non verificati. Se si apre qualsiasi file scaricato con Browser Sandbox attivo, tale file viene aperto in Browser Sandbox per isolare qualsiasi possibile infezione.

Configurazione Browser Sandbox

Per configurare Browser Sandbox, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Browser Sandbox**. Abilitare **Browser Sandbox**.
3. Dall'elenco a discesa con il livello di sicurezza di **Browser Sandbox**, selezionare il livello di sicurezza.

   L'impostazione predefinita è ottimale e ideale per gli utenti inesperti.
4. Selezionare **Mostra bordo intorno alla finestra del browser** per indicare che il browser è in esecuzione all'interno della Browser Sandbox.

   Nota: Questa non è una funzione obbligatoria per la sicurezza e può essere disabilitata, se si preferisce.
5. Selezionare **Aprire i documenti scaricati in ambiente sandbox*** per aprire qualsiasi documento scaricato in un ambiente isolato per prevenire la diffusione dell'infezione da virus.
6. In **Controlla l'accesso del browser ai dati personali**, è necessario impostare queste opzioni:
   - Per proteggere i dati riservati (come estratti conto, immagini, documenti importanti) durante la navigazione, selezionare **Impedisci al browser di accedere alle cartelle riservate**, quindi selezionare la cartella che si desidera proteggere.

     I dati nella cartella riservata non saranno accessibili dal browser e da altre applicazioni in esecuzione in Browser Sandbox. Pertanto, i dati sono al sicuro e non verranno sottratti.
   - Per proteggere i dati da manipolazioni, selezionare **Impedisci al browser di modificare i dati protetti**, quindi selezionare la cartella che si desidera proteggere.

I dati nella cartella protetta saranno accessibili ma non possono essere manipolati o modificati.

- Per scaricare il contenuto in una determinata cartella durante la navigazione, selezionare **Consenti al browser di memorizzare tutti i download nella cartella specificata** e quindi fornire il percorso alla cartella.

  Questo permette di scaricare il contenuto di cui si ha necessità per un utilizzo futuro in una determinata cartella durante la navigazione.

7. Per pulire la cache della Sandbox, cliccare sul pulsante **Cancella**.

   Questo consente di pulire i file temporanei.

8. Per salvare le impostazioni, cliccare su **Salva Modifiche**.

Nota:

- Questa funzione è supportata solo sui browser Internet Explorer, Google Chrome e Mozilla Firefox. Questa funzionalità non è supportata nel browser Microsoft Edge su sistema operativo Windows 10.
- (*) Questa funzione è supportata sui sistemi operativi Windows 7 e versioni successive.

Protezione Malware

Questa funzione permette di proteggere il sistema da minacce quali spyware, adware, keylogger e riskware mentre si è connessi ad Internet.

Configurazione Protezione Malware

Per configurare la Protezione Malware, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **Protezione Malware**. Abilitare la **Protezione Malware**.

   Protezione Malware viene abilitata.

3. Per impostare misure di sicurezza approfondite per la protezione malware, cliccare su Protezione Malware e poi impostare le seguenti opzioni.

   - **Abilita rilevazione adware:** se si desidera rilevare qualsiasi adware, selezionare questa opzione. Se viene abilitata questa opzione, vengono visualizzate ulteriori azioni da eseguire.

- **Selezionare l’azione da intraprendere quando viene rilevato un adware**: Selezionare una delle seguenti azioni da eseguire quando viene rilevato un adware: Richiedi, Ripara, Salta.

Azione	Descrizione
Richiedi	Se si seleziona questa opzione, verrà visualizzato un messaggio quando viene rilevato un adware. Il messaggio mostrerà le seguenti opzioni: ● **Permetti**: Cliccare questo pulsante per consentire all’adware di eseguirsi. ● **Rimuovi**: Cliccare su questo pulsante per rimuovere l'adware. Nel caso in cui l'adware non venga rimosso correttamente, l'adware viene messo in quarantena e verrà pulito nella successiva Scansione al Tempo di Avvio. ● **Chiudi**: Cliccare su questo pulsante per chiudere il messaggio. Tuttavia, lo stesso messaggio continuerà a essere visualizzato finché non si eseguirà un'azione.
Ripara	Selezionare questa opzione se si desidera riparare un file. Se un adware viene rilevato in un file durante la scansione, il file viene riparato. Se il file non può essere riparato, viene messo in quarantena e verrà pulito alla successiva Scansione al Tempo di Avvio.
Salta	Selezionare questa opzione se non si desidera eseguire alcuna azione sul file.

Anti Malware

Quick Heal AntiMalware, grazie al suo motore di scansione malware avanzato, esegue la scansione del registro, dei file e delle cartelle ad altissima velocità per rilevare e pulire a fondo spyware, adware, rogueware, dialer, riskware e molte altre potenziali minacce del sistema.

Eseguire Quick Heal AntiMalware

E’ possibile eseguire Quick Heal AntiMalware in una qualsiasi delle seguenti modalità:

- Nel pannello sinistro, cliccare su **Protezione** e poi cliccare su **AntiMalware**.
- Cliccare col tasto destro sull’icona del prodotto antivirus Quick Heal antivirus nel registro del sistema Windows e selezionare Eseguire Antimalware.

Utilizzo Quick Heal Antimalware

Nella schermata Quick Heal Antimalware, fare clic su **Scansiona Adesso** per avviare il processo di scansione del malware. Durante la scansione, Quick Heal Antimalware visualizza i file, cartelle

e voci di registro infettati da malware. Una volta completata la scansione, verrà visualizzato un elenco con tutti i malware rilevati contenuti in file dannosi, cartelle e voci di registro.

È possibile cancellare specifiche voci di file, cartelle o registri dall'elenco visualizzato, ma assicurarsi che tutti gli elementi eliminati siano applicazioni autentiche e non dannose.

Nel caso in cui venga rilevato un malware, è possibile eseguire una delle seguenti azioni:

Opzione	Descrizione
Pulizia	Aiuta a pulire i malware e i suoi resti dal sistema. Se il file viene eliminato, o una cartella o una voce del registro di sistema, viene chiesto se si vuole escludere tali elementi nella scansione futura. Se si desidera escludere definitivamente tali elementi, fare clic su **Sì**, altrimenti fare clic su **No** per l'esclusione temporanea.
Salta	Aiuta a saltare qualsiasi azione contro i malware nel sistema.
Stop Scansione	Aiuta a fermare la scansione.
Imposta il punto di ripristino del Sistema prima della pulizia	Ti aiuta a creare il punto di ripristino del sistema prima che il processo di pulizia inizi nel tuo sistema. Questo ti aiuta a tornare alla pulizia effettuata da Quick Heal Anti Malware utilizzando Ripristino configurazione di sistema di Windows. Nota: La funzione **Imposta il punto di ripristino del Sistema prima della pulizia** non è disponibile nel sistema operativo Windows 2000.
Dettagli	Collega direttamente al sito Quick Heal.

Anti Rootkit

Questa funzione consente di rilevare e pulire in modo proattivo i rootkit attivi nel sistema. Questo programma esegue la scansione di oggetti come processi in esecuzione, Registro di sistema di Windows, e file e cartelle per qualsiasi attività sospetta e rileva i rootkit senza firme. Anti-rootkit rileva la maggior parte dei rootkit esistenti ed è progettato per rilevare i rootkit imminenti e anche per fornire la possibilità di pulirli.

Tuttavia, si raccomanda che Quick Heal Anti-rootkit dovrebbe essere utilizzato da una persona che ha una buona conoscenza del sistema operativo o con l'aiuto di Quick Heal tecnico di supporto ingegnere. L'uso improprio di questo programma potrebbe causare sistema instabile.

Usare l'Anti-Rootkit di Quick Heal

Per usare l'Anti-Rootkit, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro a sinistra, cliccare **Protezione** e in seguito cliccare su **Anti-Rootkit**.

Apparirà un messaggio che inviterà l'utente a chiudere tutte le altre applicazioni prima di lanciare l'Anti-Rootkit.

3. Nel pannello di sinistra della schermata dell'Anti-Rootkit, cliccare il pulsante di **Inizio Scansione**.

   Quick Heal Anti-rootkit inizia la scansione del sistema per attività rootkit sospette nei processi in esecuzione, Registro di sistema di Windows e file e cartelle.

   Dopo il completamento della scansione, il risultato viene visualizzato in tre schede.

4. Selezionare l'azione appropriata contro ogni minaccia visualizzata. Ad esempio, è possibile terminare il processo rootkit, rinominare la voce/File e cartelle del Registro di sistema rootkit.

   Dopo aver preso l'azione, si dovrebbe riavviare il sistema in modo che rootkit pulizia avviene.

Pulsante	Descrizione
Stop Scansionamento	Aiuta a fermare la scansione mentre la scansione è in corso.
Chiudi	Aiuta a chiudere la finestra dell'Anti-rootkit. Se si sceglie di chiudere la finestra Anti-rootkit mentre la scansione è in corso, verrà chiesto di interrompere la scansione prima.
Inoltro dei Report degli errori	A causa di infezione o di alcune condizioni impreviste nel sistema, la scansione di Quick Heal Anti-rootkit può fallire. In caso di guasto, verrà chiesto di ri-scansionare il sistema e inviare la relazione di errore a Quick Heal Team per ulteriori analisi.

Con l'aiuto della funzione Impostazioni disponibile nella schermata Anti-rootkit, è possibile configurare quali elementi eseguire la scansione.

Configurare le impostazioni di Quick Heal Anti-Rootkit

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare su **Protezione** ed in seguito su **Anti-Rootkit**.

   Quick Heal Anti-rootkit è configurato con la Scansione Automatica come impostazione predefinita, dove esegue la scansione delle aree di sistema richieste.

Opzione di Scansione	**Descrizione**
Scansione Automatica	Scansione Automatica è l'impostazione di scansione predefinita per Anti-rootkit. In Scansione Automatica, il Quick Heal Anti-rootkit analizza le aree di sistema predefinite come: ● Processi nascosti. ● Registro delle entrate nascoste. ● Hidden Files and Folders. ● Executable ADS.
Scansione Personalizzata	Consente di personalizzare l'impostazione di scansione per Anti-rootkit per le seguenti opzioni:
	Rileva processo nascosto - analizza i processi nascosti in esecuzione nel sistema.
	Rileva elementi di registro nascosti - analizza gli elementi nascosti nel registro di Windows.
	Rileva file e cartelle nascosti - analizza i file e le cartelle nascosti nel sistema ed eseguibili ADS (flussi di dati alternativi). È inoltre possibile scegliere tra le seguenti opzioni: ● Unità di scansione su cui è installato il sistema operativo ● Analizza tutte le unità fisse ● ADS (flussi di dati alternativi) per la scansione di ADS eseguibile.
Percorso dei Report dei file	Quick Heal Anti-rootkit crea un file di report di scansione nella posizione da cui viene eseguito. Tuttavia, è possibile specificare una posizione diversa.

Panoramica dei flussi di dati alternativi - ADS

Flussi di dati alternativi o ADS consente di memorizzare i dati in formati nascosti collegati a un normale file visibile. I flussi non sono di dimensioni limitate e ci possono essere più di un flusso collegato a un file normale. ADS è un rischio per la sicurezza perché i flussi sono quasi completamente nascosti.

Trojan o autore di virus può approfittare di flussi di diffondere malware in modo da nascondere la fonte di virus.

Scansione Risultati e Rootkit di Pulizia

1. Aprire **Quick Heal Anti-Rootkit**.
2. Nel pannello di sinistra della schermata di Quick Heal Anti-Rootkit, cliccare su **Inizio Scansione.**
3. Quick Heal Anti-rootkit inizia la scansione del sistema per attività rootkit sospette nei processi in esecuzione, Registro di sistema di Windows e file e cartelle.

Dopo il completamento della scansione, il risultato viene visualizzato in tre schede diverse. Prendere la decisione appropriata. È necessario riavviare il sistema in modo che rootkit pulizia avviene.

Tabelle che appaiono nella schermata dei Risultati di Scansione

Opzioni	Descrizione
Processo	Al termine della scansione, Quick Heal Anti-rootkit rileva e visualizza un elenco di processi nascosti. È possibile selezionare la scheda Processo per la risoluzione, ma assicurarsi che l'elenco dei processi non includa alcun processo di fiducia noto. Quick Heal Anti-rootkit visualizza anche un riepilogo del numero totale di processi scansionati e processi nascosti rilevati.
Termine del processo nascosto	Dopo aver selezionato l'elenco dei processi da chiudere, fare clic sul pulsante Termina. Se un processo viene terminato con successo, il suo campo PID (Process Identifier) mostrerà n/a e il nome del processo sarà aggiunto da Terminato. Tutti i processi terminati saranno rinominati dopo un riavvio.
Registro	Simile alla scansione di processo, Quick Heal Anti-rootkit visualizza un elenco di chiavi di registro nascoste. È possibile selezionare le chiavi per rinominare, ma assicurarsi che l'elenco delle chiavi non includa alcuna chiave di registro di fiducia nota. Quick Heal Anti-rootkit visualizza anche un riepilogo del numero totale di elementi scansionati e il numero di oggetti nascosti rilevati.
Rinominare la chiave del Registro Nascosto	Dopo aver selezionato l'elenco dei tasti da rinominare, fare clic sul pulsante Rinomina. Rinominare l'operazione richiede il riavvio quindi il nome della chiave sarà preceduto da Rinomina in coda.
File e Cartelle	Allo stesso modo, Quick Heal Anti-rootkit visualizza un elenco di file e cartelle nascosti. È possibile selezionare la scheda File e cartelle per rinominare, ma assicurarsi che l'elenco di file e cartelle non includa alcun file di fiducia conosciuto. Quick Heal Anti-rootkit visualizza anche un elenco di flussi di dati alternativi

	eseguibili. Quick Heal Anti-rootkit visualizza anche un riepilogo del numero totale di file scansionati e il numero di file nascosti rilevati.
Rinominare File e Cartelle nascoste	Dopo aver selezionato l'elenco dei file e delle cartelle da rinominare, fare clic sul pulsante Rinomina. La ridenominazione dell'operazione richiede il riavvio, quindi il nome File e Cartelle sarà preceduto da Rinomina in coda.

Pulire i Rootkit tramite Disco di Emergenza Quick Heal

A volte i rootkit non vengono puliti correttamente e riappaiono anche dopo la scansione Quick Heal Anti-rootkit. In questi casi, è anche possibile utilizzare il Disco di Emergenza Quick Heal per una pulizia completa. Per la pulizia in questo modalità, creare un Disco di Emergenza Quick Heal e avviare il sistema attraverso di esso.

Per creare un Disco di Emergenza Quick Heal e pulire il sistema attraverso di esso, seguire questi passaggi:

Fase 1

Per creare il Disco di Emergenza Quick Heal, seguire il link **Crea Disco di Emergenza**, p - .

Fase 2

1. Aprire **Quick Heal Anti-Rootkit**.
2. Nel riquadro di sinistra nella schermata Quick Heal Anti-rootkit, fare clic sul pulsante **Inizio Scansione**.
3. Quick Heal Anti-rootkit inizia la scansione del sistema per attività rootkit sospette nei processi in esecuzione, Registro di sistema di Windows, e file e cartelle.
4. Al termine della scansione, il risultato della scansione viene visualizzato in tre schede diverse.
5. Prendere le misure appropriate contro ogni minaccia visualizzata. Ad esempio, è possibile terminare il processo rootkit o rinominare la voce o i file del registro di rootkit.

Fase 3

1. Avviare il sistema utilizzando **Disco di Emergenza Quick Heal**.
2. Il Disco di Emergenza Quick Heal eseguirà automaticamente la scansione e la pulizia dei rootkit dal sistema.

5. Privacy

La sezione Privacy include quelle funzionalità che consentono di proteggere i dati, le informazioni personali e la privacy.

La privacy include le seguenti funzionalità.

Data Backup

Manage Backup

Restore Backup

File Vault

Parental Control

Webcam Protection

Anti-Tracker

Registry Restore

Data Theft Protection

Wi-Fi Scanner

Blocco Schermo Protection

Anti-Keylogger

Data Backup

Utilizzando Data Backup, è possibile modificare la posizione per eseguire il backup dei dati. È possibile eseguire il backup dei dati che si preferisce. Il backup dei dati è necessario per la protezione contro attacchi ransomware. Se si verificano attacchi ransomware, è possibile ripristinare i dati di backup.

È possibile modificare la posizione di backup se non si dispone di spazio sufficiente sulla posizione predefinita.

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare su **Privacy** ed in seguito su **Backup dei Dati**. Attiva **Backup dei Dati**.
3. Per configurare quali dati salvare e dove, fare clic su **Backup dei Dati**. Specificare la posizione in cui salvare i dati e selezionare i tipi di file da salvare in **Seleziona i tipi di file per i quali eseguire il backup.**

4. Cliccare **Cambia Locazione** per cambiare la locazione del Backup.

   Appare quindi un messaggio che avverte che il backup corrente verrà spostato nella nuova posizione selezionata e il backup dei nuovi dati verrà salvato nella nuova posizione selezionata.

5. Cliccare **Seleziona Locazione** e dopo sfoglia le locazioni. Cliccare **OK**.

6. Cliccare **Sposta**.

   I dati vengono spostati con successo.

   In **Seleziona i tipi di file per i quali eseguire il Backup**, è possibile elencare le estensioni di file per cui si desidera eseguire il backup o anche aggiungere le estensioni di file nella lista di esclusione di cui non eseguire il backup.

Selezionare i tipi di file per cui eseguire il Backup

L'elenco dei file di backup include tre categorie di file: predefinito, personalizzato e utente specificato. I dati della categoria di file predefinito vengono salvati senza errore. Tuttavia, al fine di eseguire il backup dei dati dalla categoria personalizzata, è necessario mantenere le categorie di file selezionate.

Nella categoria specificata dall'utente, è possibile aggiungere le estensioni di file per le quali si desidera eseguire il backup o escludere alcune estensioni di file di cui non è necessario il backup. Fare attenzione mentre si esclude qualsiasi estensione di file in quanto questi dati non saranno sottoposti a backup.

Per aggiungere o escludere le estensioni di file, segui questi passaggi:

1. Nella schermata del Backup dei Dati, selezionare **Selezionare i tipi di file per cui eseguire il Backup > Avanzato**.

2. Cliccare **Configura**.

   Appare l'elenco delle categorie di file. Questa lista include le seguenti categorie di file.

   Tipo di file predefinito: Non è possibile modificare i tipi di file predefiniti. I dati di questi file sono sottoposti a backup senza errore.

   Tipo di file personalizzato: Per eseguire il backup dei dati, è necessario mantenere selezionate le categorie di file. Se non si selezionano le categorie di file, i dati non verranno salvati.

   Le voci verranno visualizzate in **tipo di file specificato dall'utente**. Dopo aver selezionato le voci, è necessario selezionare i file esclusi dall'utente per escludere il salvataggio del backup delle estensioni elencate.

   Tipo di file specificato dall'utente: Visualizza le estensioni di file che sono state aggiunte o escluse.

3. Per escludere le estensioni dei file, selezionare File esclusi dall'utente e fare clic su Escludi estensione. Inserisci le estensioni dei file e fai clic su OK per salvare le voci.
4. Per includere le estensioni dei file, selezionare **File specificati dall'utente** e fare clic su **Aggiungi estensione**. Inserire le estensioni dei file e fare clic su **OK** per salvare le voci.

   Le voci verranno visualizzate in **Tipo di file specificato dall'utente**. Dopo aver inserito le voci, è necessario selezionare i File specificati dall'utente per eseguire il backup dei dati delle estensioni elencate.

Gestisci Backup

Usando Gestisci Backup, puoi cancellare i dati backuppati o copiare i dati di backup dalla posizione di backup corrente in una posizione diversa. È possibile modificare la posizione di backup se non si dispone di spazio sufficiente sulla posizione corrente.

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Privacy** ed in seguito **Data Backup**. Per configurare il backup, cliccare **Manage Backup**.

   Se non avete bisogno dei dati di backup, è possibile eliminare il backup per liberare lo spazio su disco.
3. Per cancellare, cliccare **Delete**. Appare un messaggio di avviso. Leggi attentamente il messaggio. Per confermare l'eliminazione, fai clic su **Sì**.
4. Per copiare i dati di backup, fare clic su Seleziona posizione e quindi sfogliare una posizione.

   Fare clic su OK.
5. Appare un messaggio. I dati che vengono copiati da una posizione protetta ad un'altra posizione non saranno protetti. Tuttavia, i nuovi dati continueranno ad essere sottoposti a backup nella posizione protetta.
6. Cliccare **Copia**.

   I dati sono copiati con successo.

Ripristino Backup

Usando Ripristina Backup è possibile ripristinare il backup dei dati in caso di attacchi ransomware. TUttavia è importare cliccare su esegui il backup dei tuoi dati per evitare attacchi ransomware

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro a sinistra, cliccare **Privacy** ed in seguito **Ripristina Backup**.

3. Per ripristinare il backup, cliccare su **Ripristina Backup**.

Appaiono due opzioni **Dal sistema** e **Da altre fonti**. Con **Dal Sistema** è possibile ripristinare i dati dalla posizione di backup corrente sul computer mentre con **Da altre Fonti**, è possibile ripristinare i dati da qualsiasi altra posizione in cui il backup è disponibile.

4. Selezionare **Dal sistema**, se si desidera ripristinare i dati dalla posizione di backup corrente e quindi selezionare una versione. Fare clic su **Avanti**.
5. Fare clic su **Seleziona** posizione e sfoglia una posizione sul computer. Fare clic su **OK** e quindi su **Avanti**.
6. Selezionare **da altre fonti**, se si desidera ripristinare i dati da qualsiasi altra posizione in cui il backup è disponibile. Fare clic su **Seleziona posizione** e quindi sfogliare una posizione sul computer. Fare clic su **OK** e quindi su **Avanti**.

   I dati vengono ripristinati con successo.

File Vault

File Vault*è un'unità virtuale che è possibile creare sul computer. È possibile salvare dati riservati e importanti come documenti, file, foto, video e qualsiasi altro dato in un formato crittografato per impedire l'accesso non autorizzato.

Creare un Vault

Per creare un file vault, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Privacy** ed in seguito su **File Vault**.

   Nella schermata File Vault, è possibile visualizzare un elenco di volte, se ne è stata aggiunta una.
3. Per creare un nuovo vault, fare clic su **Crea vault**.
4. Nel campo **Nome dei File Vault**, scrivere un nome del vault.
5. Nel campo **Posizione del File Vault**, fare clic su Sfoglia per sfogliare una posizione e fare clic su **OK**.
6. Nel campo **Dimensione dei file vault**, assegnare la capacità di spazio.

   Assicurarsi di possedere 15 Mb di spazio minimo sul disco.
7. Cliccare su **Avanti**.
8. Impostare una password al Vault.

Impostare una password forte e ricordarlo. Sarà necessario inserire questa password per sbloccare il vault per accedere ai dati.

Sotto **Indirizzo email**, fornire un indirizzo email. Questo indirizzo email può essere il tuo indirizzo email esistente o uno nuovo.

9. Nota attentamente questo indirizzo email. Se dimentichi la password, puoi resettarla usando questo indirizzo email.
10. Fare clic su **Fine**.

    Il vault viene creato con successo.

Mettere in sicurezza il Vault

Dopo che il vault è stato creato, è pronto per l'uso.

1. Fare clic su **Apri file vault**.
2. Spostare e/o creare file o cartelle che si desidera proteggere nel vault.
3. Dopo aver lavorato nel caveau, devi chiuderlo a chiave.

   Fare clic destro sul vault e quindi selezionare **Blocca Vault**, o aprire **File Vault** da Quick Heal antivirus e impostare l'accesso del vault come Lock.

Importare il Vault

Se l'utente ha creato un vault sicuro sul tuo computer, può importarlo se necessario. Potrebbe essere necessario importare il vault se ha spostato il vault sicuro in una qualsiasi altra posizione o reinstallato Quick Heal antivirus. Senza importare il vault, non è possibile accedere ai dati nel vault.

Per importare un file vault, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Privacy** ed in seguito **File Vault**.

   Nella schermata di **File Vault**,è possibile visualizzare una lista di vault, se l'utente ne ha inseriti alcuni.
3. Per importare un vault, cliccare **Importare Vault**.
4. Nel campo del **Percorso File Vault**, sfogliare il percorso fino al vault che vuoi importare.

   Assicurarsi di aver scelto un file dal formato valido (con un'estensione **.qhe**).
5. Cliccare **Aggiungi alla Lista** per importare il vault.

   Il vault è elencato nella **lista dei vault**.

   Assicurarsi di fornire la politica di accesso richiesta (**Lock/Unlock**). È possibile accedere al vault da File Vault o anche dall'unità in cui è disponibile il vault.

Eliminare un Vault

Per eliminare un vault di file, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Privacy** ed in seguito **File Vault**.

   Nella schermata del File Vault, è possibile visualizzare la lista dei vault aggiunti.
3. Selezionare il vault che si desidera eliminare e quindi fare clic su **Elimina Vault**.

   Assicurarsi che l'accesso al vault sia bloccato e che sia disponibile per la cancellazione.
4. Immettere la password nel vault e quindi fare clic su **Avanti**.
5. Quando viene richiesta la conferma, fare clic su **Sì.**

Parental Control

Parental Control* è un metodo molto efficace per controllare l'accesso a Internet, l'accesso alle applicazioni e l'accesso al computer da parte di bambini e altri utenti. Questa funzione assicura che i bambini e gli altri utenti non visitano tipi inappropriati di siti Web, e può accedere solo alle applicazioni consentite in modo che siano al sicuro da eventuali minacce di virus e non sono esposti a contenuti offensivi o inappropriati. I genitori possono anche limitare l'accesso al computer e a Internet in base al giorno e all'ora.

Assicurarsi di configurare le seguenti opzioni prima di configurare Parental Control.

Primo Step

Verificare se si è loggati come utente amministrativo nel computer su cui è stato installato Quick Heal antivirus. Nel caso in cui non si è un utente amministrativo, si consiglia di creare un account da Amministratore e configurarlo. L'utente non deve condividere le credenziali amministrative con gli altri utenti per i quali stai creando account riservati.

Secondo step

Creare account Standard separati (utente Ristretto) per figli o altri utenti. In questo modo, avranno un accesso limitato al computer. Questo aiuta anche ad applicare diverse politiche di protezione a diversi utenti. Le politiche di protezione potrebbero includere le preferenze del sito web per ogni utente con limitazioni e un programma per l'accesso a Internet.

Terzo step

Impostare una password per impedire agli utenti non autorizzati di modificare le impostazioni o rimuovere Quick Heal antivirus dal computer. Per vedere come impostare la password di Quick Heal antivirus, vedere Protezione password di Quick Heal.

Configurare il Parental Control

Per configurare il Parental Control, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Privacy** ed in seguito **Parental Control**.

   La schermata di Parental Control appare.
3. Selezionare **Visualizza messaggio di allerta**, se si vuole ricevere una notifica quando un utente visita un sito bloccato.
4. In **Seleziona a chi applicare le regole**, selezionare una delle seguenti opzioni:
   - **Applica a tutti gli utenti**: Seleziona questa opzione se vuoi applicare la stessa impostazione a tutti gli utenti. Se selezioni questa opzione, l'opzione **Tutti gli utenti** viene visualizzata sotto.
   - **Applicare a utenti specifici**: Selezionare questa opzione se si desidera applicare impostazioni diverse a utenti diversi. Se si seleziona l'opzione **Applica a utenti specifici**, sotto viene visualizzato un elenco di tutti gli utenti.
5. Per configurare ulteriori impostazioni, fare clic su un utente disponibile in **Seleziona a chi applicare le impostazioni**. Gli utenti vengono visualizzati in base alle opzioni selezionate **Applica a tutti gli utenti** o **Applica a utenti specifici**.

   Verrà mostrata la schermata delle regole di protezione. You can configure any or all of the following options based on your requirement.
   - Controllo Navigazione Internet
   - Controllo delle Applicazioni
   - Controllo Accesso PC
6. Dopo la configurazione, cliccare su **Salva Modifiche** per salvare le vostre impostazioni.

Controllo Navigazione Internet

Il Controllo Navigazione Internet include le seguenti opzioni.

Limita accesso a categorie particolari di siti web

TRamite questa funzione, è possibile limitare l'accesso ai siti web per categorie. Se si limita una categoria di sito Web, tutti i siti Web di quella categoria verranno bloccati.

Se si desidera limitare la maggior parte dei siti Web in una categoria ma consentire determinati siti Web in quella categoria, è possibile farlo restringendo quella categoria e inserendo tali siti Web nell'elenco di esclusione.

Per limitare l'accesso alle categorie del sito web, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Privacy** e poi cliccare su **Parental Control**.

   Verrà mostrata la schermata con i dettagli delle impostazioni di Parental Control.
3. Cliccare un utente disponibile in **Selezionare a chi applicare le impostazioni.** Gli utenti verranno mostrati in base alle opzioni se si è selezionato **Applica a tutti gli utenti** oppure **Applica a utenti specifici**.
4. Nella schermata delle regole di protezione, selezionare **Controllo Navigazione Internet**.
5. Selezionare **Limita accesso a categorie particolari di siti web**. Verrà mostrata una lista di categorie di siti web.
6. Nella schermata Categoria Web, seleziona un gruppo di età in **Blocca le categorie di siti Web in base al gruppo di età** per limitare l'accesso a determinati tipi di siti Web per i propri figli o altri utenti. Se è possibile selezionare un determinato gruppo di età, verranno applicate le impostazioni ottimali. È possibile personalizzare le impostazioni predefinite per un gruppo di età, se necessario. Per ripristinare le impostazioni personalizzate di un gruppo di età, aggiornare lo stesso gruppo di età. È possibile ripristinare le impostazioni predefinite in qualsiasi momento selezionando l'opzione Predefinito.
7. In **Seleziona i diritti di accesso per le seguenti categorie di siti Web**, attivare una categoria di siti Web per consentire l'accesso ai siti Web o disattivarli per negare l'accesso. Inoltre, le impostazioni predefinite sono ottimali e ideali per gli utenti inesperti.

   Se si desidera escludere un determinato sito Web dalla categoria bloccata, inserire tale sito Web nell'elenco di esclusione. Ad esempio, se si è bloccato la categoria **Streaming media e download**, ma si desidera comunque consentire l'accesso a **YouTube**, è possibile farlo inserendo YouTube nell'elenco di esclusione.
   - Nel dialog Categoria Web, cliccare sul pulsante **Escludi**.
   - Nella casella testuale **Inserisci URL**, inserire l'URL del sito web per il quale si desidera che gli utenti possano accedere e poi cliccare sul pulsante **Aggiungi.** Cliccare su **OK**.

   Parimenti, se si desidera rimuovere un sito web dall'elenco di esclusione, selezionare un URL e poi cliccare su **Rimuovi**. Cliccare su **Rimuovi Tutto** per cancellare tutti gli URL dall'elenco di esclusione.
8. Cliccare su **OK** e poi confermare le proprie preferenze. Cliccare su **OK**.
9. Per salvare le impostazioni, cliccare su **Salva Modifiche**.

Limita accesso a particolari siti web

Con questa funzione è possibile bloccare l'accesso a siti web specifici. Ciò è utile quando si desidera limitare l'accesso a determinati siti Web o se si dispone di un elenco più breve di siti Web da limitare.

Questa opzione è utile anche quando un sito Web non rientra in una categoria selezionata o è stata limitata una categoria di sito Web, ma un determinato sito Web è ancora accessibile.

Per limitare l'accesso a un determinato sito Web, segui questi passaggi:

1. Aprire **Quick Heal antivirus**.

Nel pannello sinistro, cliccare su **Privacy** e poi cliccare su **Parental Control**.

Verrà mostrata la schermata con le impostazioni di Parental Control.

Cliccare un utente disponibile in **Selezionare a chi applicare le impostazioni.** Gli utenti verranno mostrati in base alle opzioni se si è selezionato **Applica a tutti gli utenti** oppure **Applica a utenti specifici**.

Nella schermata delle regole di protezione, selezionare **Controllo Navigazione Internet**.

Selezionare **Limita accesso a particolari siti web** e poi cliccare sul pulsante **Elenco Blocchi**.

Cliccare sul pulsante **Aggiungi**.

Nella casella testuale **Inserire Sito Web**, inserire l'URL del sito web e poi cliccare su **OK**. Qualora si desideri bloccare tutti i sottodomini del sito web, selezionare **Blocca anche sottodomini**.

Per esempio, se si blocca **www.abc.com** e i relativi sottodomini, i sottodomini come **mail.abc.com** e **news.abc.com** verranno anch'essi bloccati.

Cliccare su **OK** e poi cliccare su **OK**.

Per salvare le impostazioni, cliccare su **Salva Modifiche**.

Accesso Internet Pianificato

Tramite questa funzione, è possibile limitare l'accesso a Internet da parte dei propri figli solo nella fascia oraria configurata. Non appena la fascia oraria configurata è terminata, l'accesso a Internet viene bloccato.

Per impostare l'accesso Internet pianificato, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.

Nel pannello sinistro, cliccare su **Privacy** e poi cliccare su **Parental Control**.

Verrà mostrata la schermata con le impostazioni di Parental Control.

Cliccare un utente disponibile in **Selezionare a chi applicare le impostazioni.** Gli utenti verranno mostrati in base alle opzioni se si è selezionato **Applica a tutti gli utenti** oppure **Applica a utenti specifici**.

Nella schermata delle regole di protezione, selezionare **Controllo Navigazione Internet**.

Selezionare **Accesso Internet Pianificato** e poi cliccare sul pulsante **Configura.**

Viene visualizzato il grafico Accesso Internet Pianificato.

In **Specifica quando l'utente può accedere ad Internet**, selezionare una delle seguenti opzioni:

- **Consenti sempre l'accesso a Internet:** selezionare questa opzione se si desidera consentire ad altri utenti l'accesso a Internet senza alcuna restrizione.
- **Consenti l'accesso a Internet secondo la pianificazione:** selezionare questa opzione se si desidera impostare una restrizione per l'accesso a Internet.

Il grafico del programma giornaliero e orario viene attivato.

- Selezionare le celle per i giorni e gli orari durante i quali si desidera consentire l'accesso a Internet.

  Le celle selezionate sono evidenziate per indicare la pianificazione consentita.

Cliccare su **OK** e poi cliccare su **OK**.

Per salvare le impostazioni, cliccare su **Salva Modifiche**.

Controllo Applicazioni

Controllo Applicazioni include le seguenti opzioni.

Limita accesso a particolari categorie di applicazioni

Tramite questa funzione, è possibile limitare l'accesso alle applicazioni per categorie. Se si limita una categoria di applicazioni, tutte le applicazioni in quella categoria verranno bloccate.

Se si desidera limitare la maggior parte delle applicazioni in una categoria ma consentire determinate applicazioni in quella categoria, è possibile farlo restringendo quella categoria e inserendo tali applicazioni nell'elenco di esclusione.

Per limitare l'accesso alle categorie di applicazioni, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Privacy** e poi cliccare su **Parental Control**.

   Verrà mostrata la schermata con le impostazioni di Parental Control.

Cliccare un utente disponibile in **Selezionare a chi applicare le impostazioni.** Gli utenti verranno mostrati in base alle opzioni se si è selezionato **Applica a tutti gli utenti** oppure **Applica a utenti specifici**.

Nella schermata delle regole di protezione , selezionare **Controllo Applicazioni.**

Seleziona **Limita accesso a particolari categorie di Applicazioni** e poi cliccare il pulsante **Categorie**. Verrà mostrato un elenco delle categorie delle applicazioni.

Abilitare una categoria di applicazioni per consentire l'accesso alle applicazioni in quella categoria o disattivarla per negare l'accesso.

Se si desidera escludere determinate applicazioni dall'elenco dei blocchi, includere tale applicazione nell'elenco di esclusione.

- Nel dialog Categoria Applicazioni, cliccare sul pulsante **Escludi**.

- Cliccare il pulsante **Aggiungi** e sfogliare un'applicazione da aggiungere all'elenco di esclusione. Cliccare su **OK**.

Parimenti, se si desidera rimuovere un'applicazione dall'elenco di esclusione, selezionare l'applicazione e fare clic su **Rimuovi**. Fare clic su **Rimuovi tutto** per eliminare tutte le applicazioni dall'elenco di esclusione.

Cliccare su **OK** e poi cliccare su **OK**.

Per salvare le impostazioni, cliccare su **Salva Modifiche**.

La seguente tabella descrive le categorie.

Categoria	Descrizione
Applicazioni CD/DVD	Include applicazioni quali AC3 Filter, Alcohol, Alcohol 120%, AnyDVD, BlindWrite, e così via.
Applicazioni Chat	Include applicazioni come Camfrog Video Chat, ManyCam, Skype, ecc. ecc.
Download Manager	Include applicazioni come Akamai Netsession, aTube Catcher, DamnVid, Download Manager Plus DownloadStudio, ecc. ecc.
Email dei Client	Include applicazioni come FlashMail, Foxmail, Idea!, Lotus Notes Client, Novell Groupwise, The Bat!, Thunderbird, Windows Mail, ecc. ecc..
Applicazioni di Condivisione File	Include applicazioni come Ares, BearShare, BitComet, BitTorrent, ecc. ecc.
Giochi	Include applicazioni come 3D Sniper, 4st Attack, Adrenaline Rush, Agent Combat, Air Hawk, ecc. ecc.
Media Player	Include applicazioni come AIMP3, ALLPlayer, Audacity, Avidemux, BS Player, ecc. ecc.
Altre	Include applicazioni come 2X Client, Advanced SystemCare, AquaSnap, Autoruns, Checksum Control,ecc. ecc.
Proxy di Rete	Include 602LAN SUITE, Anon Proxy Server, CCProxy, Gateway Veloce e Sicuro per applicazioni come Internet Freedom, ecc. ecc.
Modem USB	Include applicazioni come Huawei , ecc. ecc
Browser di Rete	Include applicazioni come America Online, Avant Browser, Comodo Dragon, Firefox, Google Chrome, ecc. ecc

Limitare l'accesso a particolari applicazioni

Con questa funzione, è possibile bloccare l'accesso degli utenti a applicazioni specifiche. Questo è utile quando si desidera limitare l'accesso degli utenti a determinate applicazioni o se si dispone di un elenco più breve di applicazioni da limitare.

Questa opzione è utile anche quando un'applicazione non rientra in una categoria selezionata o hai limitato una categoria di applicazione ma una certa applicazione è ancora accessibile.

Per limitare l'accesso a una particolare applicazione, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare **Privacy** ed in seguito cliccare **Parental Control**.

   La schermata della funzione Dettagli Parental Control appare.
3. Cliccare un utente disponibile sotto **Selezionare a chi applicare le misure.** Gli utenti vengono visualizzati in base alle opzioni selezionate **Applica a tutti gli utenti** o **Applica a utenti specifici.**
4. Nella schermata delle Regole di Protezione, selezionare **Controllo Applicazioni**.
5. Selezionare **Restringere accesso a determinate applicazioni** ed i seguito cliccare il pulsante **Bloccare Elenco**.
6. Cliccare Il pulsante **Aggiungi** e sfoglia le applicazioni per bloccarne una.

   Allo stesso modo, se si desidera rimuovere un'applicazione dalla lista dei bloccati, selezionare l'applicazione ed in seguito cliccare **Rimuovi**. Cliccare **Rimuovi Tutto** per rimuovere tutte le applicazioni dalla lista dei bloccati.
7. Cliccare **OK** ed in seguito cliccare **OK**.
8. Per salvare le nuove impostazioni cliccare **Salvare Modifiche**.

   Note: Il Controllo Applicazioni funzionerà solo se la Protezione Virus è attivata.

Controllo accessi PC

Con questa funzione, è possibile permettere ai figli l'accesso al computer o laptop solo secondo la fascia oraria configurata. Non appena la fascia oraria configurata è terminata, il computer verrà bloccato. Tuttavia, possono accedere con le loro credenziali dopo che il tempo assegnato è finito, ma solo per quarantacinque secondi. Possono accedere quante volte preferiscono, tuttavia il computer verrà bloccato ogni quarantacinque secondi.
Per configurare Controllo accessi PC, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello di sinistra cliccare **Privacy** ed in seguito cliccare **Parental Control**.

   La schermata della funzione dei dettagli di Parental Control appare.
3. Cliccare un utente disponibile sotto **Selezionare a chi applicare le misure.** Gli utenti vengono visualizzati in base alle opzioni selezionate **Applica a tutti gli utenti** o **Applica a utenti specifici.**
4. Nella schermata delle Regole di protezione, selezionare **Controllo Accesso PC** ed in seguito cliccare il pulsante **Configura**. Viene visualizzato il grafico di accesso al PC Schedule.

Sotto **Specificare quando l'utente può accedere al PC**,è possibile selezionare le seguenti opzioni:

- **Permetti sempre l’accesso al PC**: Selezionare questa opzione se si desidera consentire agli utenti di accedere al computer senza alcuna restrizione.
- **Permetti accesso al PC come pianificato:** Selezionare questa opzione se si desidera impostare uno slot temporale per l'accesso al computer.

- Tempo di accesso giornaliero: Consente di assegnare il tempo su base oraria. Gli utenti possono accedere al computer per la durata del tempo consentito in qualsiasi momento durante un giorno.
- Orari di accesso giornaliero (ora dell'orologio): selezionare le celle per i giorni e gli orari durante i quali si desidera consentire l'accesso al computer. Gli utenti possono accedere al computer solo durante la finestra di tempo consentito.

  Le celle selezionate sono evidenziate che indicano la pianificazione consentita.

Cliccare **OK** ed in seguito **OK**.

Per salvare le nuove impostazioni cliccare su **Salva Modifiche**.

Creazione Account Amministratore

Questa funzione consente di installare e rimuovere un'applicazione dal sistema o di modificare le impostazioni, incluso il Parental Control. Ciò garantisce che solo i genitori abbiano il pieno controllo del sistema.

Per creare un Account Amministratore, seguire questi passaggi:

1. Cliccare su **Start > Pannello di controllo**.
2. Cliccare su **Account Utente.**
3. Il tipo di account viene mostrato sotto il nome utente. Controllare se il proprio tipo di account è Amministratore. Se il proprio tipo di account non è Amministratore, si deve cambiarlo in account Amministratore.

Impostazione Protezione tramite password sulle Impostazioni Quick Heal

È possibile proteggere le impostazioni dell'antivirus Quick Heal attivando la protezione tramite password. La protezione con password garantisce che le vostre impostazioni siano protette da modifiche da parte di utenti non autorizzati.

Per sapere come abilitare la protezione tramite password dell'antivirus Quick Heal, vedere Protezione Password.

Creazione account utente limitati

Gli account utente limitati delimitano gli utenti solo al proprio account e impediscono loro di assumere il pieno controllo del computer. Ciò consente di proteggere il computer impedendo all’utente di apportare modifiche che potrebbero influire sui privilegi di sicurezza.

Per impostare degli account ristretti, seguire questi passaggi:

Per il Sistema Operativo Microsoft Windows XP:

1. Cliccare **Start > Pannello di Controllo > Account Utente**.
2. Sotto **Account Utente**, cliccare **Creare un nuovo Account Utente**.
3. Riempire **Nome Account** e cliccare **Successivo**.
4. Selezionare **Limitato**.
5. Cliccare **Crea Account**.

Per il Sistema Operativo Microsoft Windows Vista/Windows 7:

1. Cliccare **Start > Pannello di Controllo> Account Utente**.
2. Sotto **Account Utente**, cliccare **Gestisci altri Account**.
3. Cliccare **Crea un Nuovo Account Utente**.
4. Riempi in **Nome Account** e seleziona **Utente Standard**.
5. Cliccare **Crea Account**.

Protezione Webcam

Ci sono diverse applicazioni e malware che cercano di accedere alla webcam del tuo computer senza il tuo consenso per catturare le tue foto, invadendo così la tua privacy. Gli aggressori di malware possono quindi ricattare per queste foto. Protezione Webcam * rileva tali malware e aiuta a prendere le misure appropriate per prevenire tali tentativi non autorizzati di invadere la privacy dell'utente.

Configurare la Protezione Webcam

Per configurare Webcam Protection, segui questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare **Privacy** ed in seguito cliccare **Protezione Webcam**.

   Attivare la **Protezione Webcam**.

   Note: La Protezione Webcam è impostata come predefinita.

Se la Protezione Webcam è attivata e qualsiasi nuova applicazione o browser tenta di accedere alla webcam del computer, viene visualizzato un messaggio di avviso. L'utente può negare l'autorizzazione se non ti fidi dell'applicazione.

3. Per configurare ulteriormente, fare clic su **Protezione Webcam**.

Appare un elenco di applicazioni. È possibile aggiungere un'applicazione e impostare la politica di accesso per essa. È inoltre possibile modificare la politica di accesso per un'applicazione o rimuovere un'applicazione secondo il requisito.
Per aggiungere un'applicazione, fare clic sul pulsante **Aggiungi**. Sfogliare un file dell'applicazione, aggiungerlo all'elenco e imposta la politica di accesso.
Se si permette ad un'applicazione di accedere alla webcam, è possibile selezionare **Avvisami sull'uso della webcam**. Ogni volta che l'applicazione con politica di accesso consentita accede alla webcam, viene visualizzato un messaggio di avviso. Se non si seleziona **Avvisami isull'uso della webcam**, nessun messaggio di avviso verrà visualizzato.

Tuttavia, se si nega l'accesso per un'applicazione, non è necessario selezionare **Notificami su webcam** utilizzare per tale applicazione.

4. Per salvare le nuove impostazioni, cliccare **Salva Modifiche**.

Anti-Tracker

Anti-Tracker* protegge la privacy bloccando i tracker che raccolgono le impronte ogni volta che si naviga online.

Ci sono tracker che raccolgono dati quando si naviga online. Tali dati vengono utilizzati per comprendere le preferenze di navigazione e il comportamento degli utenti per promuovere il marketing, visualizzare annunci, condividere o vendere informazioni personali alle aziende.

Configurazione Anti-Tracker

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Privacy** e poi cliccare su **Anti-Tracker**.

   Viene visualizzato un riepilogo di tutti i tracker bloccati. E' possibile configurare una qualsiasi delle seguenti funzionalità: Gestisci Estensioni, Gestisci Esclusioni, Pulizia Cache del Browser, e Impostazioni Anti-Tracker.

Gestisci Estensioni

1. Nella schermata di Anti-Tracker, cliccare **Gestisci Estensioni**.

   Verrà mostrato un elenco dei browser.

2. Abilita estensioni per bloccare i tracker dei browser elencati. Per salvare le impostazioni, cliccare su **Chiudi**.

Gestisci Esclusioni

1. Nella schermata di Anti-Tracker, cliccare su **Gestisci Esclusioni**.
2. Inserire i siti web sui quali si desidera che i tracker non siano bloccati da Anti-Tracker e poi cliccare su **Aggiungi**.

   Assicurarsi di spuntare i siti web affidabili. E' possibile rimuovere qualsiasi sito web, in base alle preferenze.
3. Cliccare **Salva**.

Pulizia Cache del Browser

1. Nella schermata di Anti-Tracker, cliccare su **Pulizia Cache del Browser**.

   Verrà mostrato il dialog Pulizia Cache del Browser.
   E' possibile pulire la cache di un sito web manualmente in base alle proprie preferenze.
2. Per pulire le cache istantaneamente, selezionare un browser e cliccare su **Pulisci Cache**.

   E' possibile impostare una pianificazione per pulire le cache anche automaticamente.
3. Cliccare sull'icona **Impostazioni** di uno qualunque dei browser elencati.
4. Impostare una pianificazione e cliccare su **Salva**.

   La cache del browser sarà rimossa automaticamente. Questo consente di eseguire velocemente il browser.
5. Per chiudere il dialog Pulisci Cache del Browser, cliccare su **Chiudi**.

Impostazioni Anti-Tracker

1. Nella schermata di Anti-Tracker, cliccare su **Impostazioni Anti-Tracker**.

   Verrà mostrato un elenco delle categorie di tracker.
2. Selezionare un tracker in base alle proprie preferenze. Per salvare le impostazioni, cliccare su **Salva**.

   Assicurarsi delle motivazioni per le quali si consentono o si bloccano i tracker.

 Nota:

Anti-Tracker non è supportato da Google Chrome su Windows XP e Windows Vista.

Ripristino Registro

Il Registro è un database utilizzato per memorizzare le impostazioni e le opzioni dei sistemi operativi Microsoft Windows. Contiene informazioni e impostazioni per tutto l'hardware, il software, gli utenti e le preferenze del sistema.

Ogni volta che un utente apporta le modifiche alle impostazioni del Pannello di Controllo, o alle associazioni di file, alle policy di sistema o installazioni di nuovi software, le modifiche vengono replicate e memorizzate nel Registro di sistema. Il malware attacca il Registro di sistema per limitare le caratteristiche specifiche dei sistemi operativi o di altre applicazioni. Si può modificare il registro di sistema in modo tale che limiti l'azione del malware che crea problemi al sistema.

La funzione Quick Heal Registry Restore ripristina l'area del registro di sistema critica e altre aree dalle modifiche apportate dal malware. Ripara anche il registro di sistema.

Configurare il Ripristino del Registro

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare **Privacy** ed in seguito **Ripristino del Registro**.
3. Seleziona **Ripristina aree critiche del registro di sistema** per ripristinare il registro di sistema critico durante la scansione. Le aree del Registro di sistema critiche sono generalmente modificate da malware per eseguire determinate attività automaticamente o per evitare il rilevamento o la modifica da applicazioni di sistema come Disabilitazione del Task Manager e Disattivazione dell'Editor del Registro di sistema.
4. Selezionare **Ripara voci del registro di sistema dannose** per la scansione del registro di sistema per le voci relative a malware. Il malware e i suoi resti vengono riparati automaticamente durante la scansione.

Protezione contro il Furto di Dati

Con Protezione contro il Furto di Dati, è possibile bloccare il trasferimento dei dati tra il sistema e le unità USB e dispositivi CD/ DVD. Data Theft Protection assicura che nessun file o dati possono essere copiati dal sistema a qualsiasi unità o dispositivi esterni. Allo stesso modo nessun file o dati possono essere trasferiti dalle unità USB e dai dispositivi CD/DVD al sistema. Quindi né le informazioni possono essere furto né possono essere impiantati file dannosi nel sistema.

Questa funzione consente di bloccare il trasferimento dei dati tra il sistema e dispositivi esterni come unità USB e dispositivi CD/DVD. Data Theft Protection garantisce che nessun file o dati possono essere copiati dal sistema a qualsiasi dispositivo esterno o viceversa. Garantisce la sicurezza dei dati ed elimina anche la possibilità di trasferimento di eventuali file dannosi.

Configurare la Protezione contro il Furto di Dati

Per configurare la protezione contro il Furti di Dati, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare su **Privacy** ed in seguito cliccare su **Protezione contro il furto di Dati.**
3. Attivare **Protezione contro il Furto di Dati.**

   Protezione contro il Furto di Dati è attivata.
4. Fare clic su **Protezione furto di dati** e fare una qualsiasi delle seguenti opzioni:
   - **Solo lettura e nessun accesso in scrittura a unità esterne**: Consente il trasferimento dei dati dalle unità USB e dispositivi CD/ DVD al sistema, ma non viceversa. Tuttavia, questa opzione è selezionata come impostazione predefinita.
   - **Blocca l'accesso completo alle unità esterne:** Blocca il trasferimento dei dati tra il sistema e tutti i dispositivi esterni.
   - **Autorizza unità USB e dispositivi mobili:** selezionare questa opzione se si desidera consentire l'accesso solo alle unità USB e ai dispositivi mobili autorizzati. Se questa opzione è selezionata e si collega un'unità USB o un dispositivo mobile al sistema, viene richiesta una password per accedervi. Quindi l'accesso è concesso solo ai dispositivi autorizzati.

     Questa opzione funzionerà solo se la Protezione contro il furto di dati e Protezione Password sono attive.
   - **Blocca Dispositivi Mobili**: Blocca completamente l'accesso ai dispositivi mobili.
5. per salvare le nuove impostazioni cliccare **Salva Modifiche**.

Wi-Fi Scanner

Wi-Fi Scanner* scansiona il router Wi-Fi e aiuta l'utente a sapere se è sicura per la connessione. Se ci sono vulnerabilità, consiglia modi per risolverle.

Scansionare il router Wi-Fi

Per scansionare il router Wi-Fi, seguire questi passaggi

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Privacy** ed in seguito cliccare **Wi-Fi Scanner**.

   una finestra di dialogo appare.
3. Per scansionare la propria connessione Wi-fi selezionare **Inizio Scansione**.

Una richiesta di consenso appare. Leggere attentamente il consenso.

4. Per procedere cliccare **Acconsento**.

   Inizia la scansione. Al termine della scansione, viene visualizzato un Report. Il Report visualizza il nome della rete Wi-Fi e le eventuali vulnerabilità.

   C'è un link Linee guida che offre possibili soluzioni per risolvere le vulnerabilità.

Protezione Blocco Schermo

I programmi dannosi che bloccano lo schermo impedendo l'accesso al computer sono noti come Blocco Schermo. Con Protezione Blocco Schermo*, è possibile creare una combinazione di tasti scorciatoia per avviare una pulizia del computer e rimuovere tali programmi dannosi. Premendo il tasto corto, è possibile avviare la pulizia del computer e rimuovere il programma dannoso.

Configurare la Protezione Blocco Schermo

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare su **Privacy** ed in seguito **Protezione Blocco Schermo** .
3. Per attivare la Protezione Blocco Schermo, selezionare **Proteggi dai Blocchi Schermo**. Tuttavia questa opzione è selezionata come predefinita.
4. Selezionare un alfabeto dall'elenco a discesa per creare una combinazione di scorciatoie con **Ctrl+Alt+Shift**. Qui A è selezionato per impostazione predefinita.
5. Cliccare **Salva Modifiche**.

Note:

- É necessario riavviare il computer almeno una volta dopo l'installazione per attivare questa opzione

Anti-Keylogger

I Keyloggers sono programmi dannosi che registrano tutte le informazioni digitate dall'utente sulla tastiera del computer o laptop e condividere tali informazioni con gli hacker. È possibile perdere informazioni riservate come nomi utente, password o PIN per gli hacker. Anti-keylogger ti aiuta a evitare che le informazioni vengano registrate dal malware del registratore di tasti.

Configurare Anti-Keylogger

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Privacy** ed in seguito **Anti-Keylogger**.
3. Attivare o disattivare **Anti-Keylogger** a seconda della preferenza.

6. Prestazioni

La sezione Prestazioni include quelle funzionalità che ti aiutano a migliorare le prestazioni del tuo computer, pulire la cronologia di navigazione e migliorare l'esperienza di gioco.

Le prestazioni includono le seguenti caratteristiche.

Auto Silent Mode

Track Cleaner

Hijack Restore

System Explorer

Game Booster

Modalità di silenzioso automatico

Con la modalità di silenzioso automatico, è possibile mantenere l'antivirus in esecuzione in background, ma non vengono visualizzate notifiche o pop-up. Qualsiasi scansione pianificata viene anche rinviata alla pianificazione successiva fino a quando la modalità Auto Silent non viene disattivata, se qualsiasi applicazione è in esecuzione in modalità a schermo intero.

Avviare la Modalità di Silenzioso automatico

Per accendere la modalità di Silenzioso automatico:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare **Performance** ed in seguito **Modalità di SIlenzioso Automatico**. Attivare la Modalità di Silenzioso automatico.

   Tuttavia, la Modalità di Silenzioso Automatico è accesa come impostazione predefinita.

Track Cleaner

La maggior parte dei programmi memorizzano l'elenco dei file aperti di recente nel loro formato interno per aiutarti ad aprirli di nuovo per un accesso rapido. Tuttavia, se un sistema è utilizzato da più di un utente, la privacy dell'utente potrebbe essere compromessa. Track Cleaner ti aiuta a rimuovere tutte le tracce di tali programmi (MRU) più recenti e prevenire la violazione della privacy.

Usare Track Cleaner

Per utilizzare Track Cleaner, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Performance** ed in seguito **Track Cleaner**.

   La schermata di Track Cleaner appare.Vengono visualizzati tutti i programmi aperti di recente.
3. Selezionare i programmi le cui tracce si desidera rimuovere o selezionare **Check All** per selezionare tutti i programmi nell'elenco.
4. Per iniziare la pulizia, cliccare **Inizia Pulizia**.
5. Per chiudere la finestra Track Cleaner, fare clic su **Chiudi**.

Ripristina Hijack

Se hai modificato le impostazioni predefinite di Internet Explorer o se le impostazioni sono state modificate da malware, spyware e, talvolta, applicazioni autentiche, è possibile ripristinare le impostazioni predefinite. Questa funzione consente di ripristinare le impostazioni del browser Internet Explorer, e anche di impostazioni critiche del sistema operativo come l'editor del Registro e Task Manager.

Usare il Ripristino Hijack

Per avviare il ripristino Hijack, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Performance** ed in seguito cliccare su **Ripristino Hijack**.
3. Nella schermata di Ripristino Hijack, selezionare **Spunta Tutto** per selezionare tutte le impostazioni del browser nella lista.
4. Selezionare **Ripristina host file predefinito** per ripristinare l’host file.
5. Selezionare **Ripristina importanti impostazioni di sistema** per ripristinare importanti impostazioni di sistema.
6. Per iniziare a ripristinare le nuove impostazioni, cliccare **Ripristina adesso**.

Ripristinare l’Host File Predefinito

L’host file predefinito include i seguenti campi:

Campo	Descrizione
Indirizzo IP	Immettere l’indirizzo IP dell’host.
Nome Host	Immettere il nome dell’host.
Aggiungi	Cliccare **Aggiungi** per aggiungere dettagli dell’host nella lista.
Modifica	Selezionare l'host nell'elenco e fare clic su **Modifica** per apportare le modifiche.

Elimina	Selezionare l' host nella lista e cliccare **Cancella** per rimuoverlo.
OK	Cliccare **OK** per salvare le impostazioni dell'host e uscire dalla finestra di Specificazioni Host.
Chiudi	Cliccare **Chiudi** per uscire senza salvare dalla finestra di Specificazioni Host.

Ripristinare importanti impostazioni di sistema

La funzione di ripristino di importanti impostazioni del Sistema include le seguenti opzioni:

Opzione	Descrizione
Spunta Tutto	Aiuta a ripristinare tutte le impostazioni di sistema nell'elenco.
OK	Consente di salvare tutte le impostazioni modificate ed uscire dalla finestra Impostazioni di sistema importanti.
Chiudi	Consente di uscire senza salvare le impostazioni dalla finestra Impostazioni di sistema importanti.

I pulsanti nella schermata Ripristina Hijack sono i seguenti.

Pulsante	Descrizione
Ripristina Adesso	Aiuta ad avviare il ripristino delle impostazioni selezionate.
Annulla	Consente di annullare le impostazioni effettuate nella schermata corrente. Se si fa clic sul pulsante **Annulla**, si apre una finestra Annulla operazioni. Verranno elencate le impostazioni che sono state ripristinate alle impostazioni predefinite. Selezionare le impostazioni o **Seleziona tutto** per selezionare tutte le impostazioni. Fare clic su **OK** per tornare alle impostazioni esistenti.
Chiudi	Ti aiuta a uscire dalla finestra di Hijack Restore senza salvare le tue impostazioni.

System Explorer

Questo strumento fornisce tutte le informazioni importanti relative al computer come il processo in esecuzione, BHO installati, barre degli strumenti installate in Internet Explorer, installato Activex, Host, LSP, Programmi di avvio, Impostazioni di Internet Explorer e connessione di rete attiva. Questo aiuta a diagnosticare il sistema per qualsiasi nuovo malware o riskware.

Usare System Explorer

Per utilizzare System Explorer, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare su **Performance** ed in seguito su **System Explorer**.

   Nella schermata di System Explorer, è possibile selezionare un processo, uno strumento, un programma o qualsiasi altro processo che si desidera analizzare. In base alla selezione, è possibile selezionare un processo e visualizzare la sua descrizione. È possibile terminare qualsiasi processo che si pensa così.

Game Booster

Game Booster* aiuta a divertirsi giocando su PC senza intoppi. Non appena lanci qualsiasi gioco, Game Booster dà priorità al gioco rispetto ad altri processi e applicazioni per migliorare l'esperienza di gioco. In questo modo si può giocare più velocemente senza alcuna interruzione.

Configurare Game Booster

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare su **Performance** ed in seguito su **Game Booster.** Attivare **Game Booster**.

Note:

- Se Virus Protection è disattivato, Game Booster non funzionerà.
- Game Booster funzionerà su quattro processori logici (CPU) o più.

7. Impostazioni

La sezione Impostazioni include quelle funzionalità che consentono di configurare la connessione a Internet, creare dischi di emergenza e altre impostazioni.
Le impostazioni includono le seguenti funzionalità.

Aggiornamento Automatico

Questa funzione ti aiuta a prendere automaticamente gli aggiornamenti delle ultime firme di virus. Si consiglia di mantenere il vostro antivirus Quick Heal aggiornato per la protezione contro nuovi e sconosciuti malware e virus.

Per prendere gli aggiornamenti regolarmente, garantire le seguenti condizioni.

1. Devi sempre tenere acceso l'**Aggiornamento Automatico.**
2. È necessario impostare una modalità di aggiornamento per prendere gli aggiornamenti.

Configurare l'Aggiornamento Automatico

Per configurare l'aggiornamento automatico, segui questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra cliccare su **Impostazioni** ed in seguito su **Aggiornamento Automatico**. Attivare l'**Aggiornamento Automatico**.

   Tuttavia, l'Aggiornamento Automatico è selezionato come impostazione predefinita.

3. Per configurare come eseguire gli aggiornamenti, fare clic sull'icona di impostazione di **Aggiornamento Automatico**.
4. Selezionare **Mostra finestra di notifica di aggiornamento**, se si desidera ottenere una notifica circa l'aggiornamento di Quick Heal antivirus. Tuttavia, questa opzione è attivata come impostazione predefinita.
5. Selezionare la modalità di aggiornamento tra le seguenti opzioni:
    - **Scarica da Internet** – Ti aiuta a scaricare gli aggiornamenti sul tuo computer da Internet.
    - **Recupera i File di Aggiornamento da uno specifico percorso**– Consente di scegliere gli aggiornamenti da una cartella locale o da una cartella di rete.
6. Seleziona altre opzioni.
    - **Copia i File di Aggiornamento in una locazione specifica**– Consente di salvare una copia degli aggiornamenti su un'unità locale del computer.
    - Controllare l'ultima versione di antivirus Quick Heal:
    - **Avvisami quando è disponibile l'aggiornamento:** Seleziona questa opzione se vuoi essere avvisato quando è disponibile un nuovo aggiornamento.
    - **Scarica automaticamente l'aggiornamento**: Selezionare questa opzione se si desidera scaricare automaticamente un nuovo aggiornamento quando disponibile sul sistema. Quindi è necessario installarlo per aggiornare la versione corrente.
7. Per salvare le nuove impostazioni, cliccare **Salvare Modifiche**.

Selezionare la Modalità di Aggiornamento

Quick Heal antivirus fornisce più modalità di aggiornamento che è possibile selezionare in base alla vostra convenienza.

- Preleva i file di aggiornamento dal percorso specificato
- Scegliere gli aggiornamenti è utile in due modi.
    a. **Computer singolo**: Se il computer in cui è installato Quick Heal antivirus non è connesso a Internet.
    b. **Computer multipli**: è possibile scaricare gli aggiornamenti su un singolo computer per salvare la larghezza di banda di Internet e raccogliere gli aggiornamenti per tutti i computer della rete.

Per scegliere gli aggiornamenti automaticamente, assicurarsi le seguenti cose.

1. Seleziona **Recupera File aggiornati fra quelli specificati**.
2. Sfoglia un percorso per l'unità sul computer o qualsiasi altro computer nella rete.
3. Per salvare le impostazioni, fare clic su **Salva modifiche.**

Copia i file di aggiornamento nella posizione specificata

Ogni volta che l'antivirus Quick Heal viene aggiornato con le nuove firme del database dei virus, una versione dell'aggiornamento viene salvata nella posizione specificata qui. Questo è utile nel caso in cui ci sia qualche problema tecnico o l'antivirus si blocca a causa di un nuovo aggiornamento. È possibile tornare alla versione precedente facilmente.

Note:

- Per salvare l'aggiornamento in questa posizione, è necessario mantenere questa opzione selezionata.

Vedi i File in Quarantena

Questa funzione consente di isolare in modo sicuro i file infetti o sospetti. Quando un file viene messo in quarantena, Quick Heal antivirus crittografa il file e lo mantiene all'interno della directory di quarantena. Essendo tenuti in un formato crittografato, questi file non possono essere eseguiti e quindi sono sicuri. Quarantena mantiene anche una copia del file infetto prima di riparare. Tuttavia, è possibile eseguire un backup dei file anche prima di intraprendere un'azione.

Avviare i File in Quarantena

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, cliccare **Impostazione** ed in seguito cliccare **Vedere Quarantena**.

Viene visualizzato un elenco di tutti i file in quarantena e sottoposti a backup.

È possibile eseguire le seguenti operazioni nella finestra di dialogo Quarantena:

Pulsante	Descrizione
Aggiungi	Permette di mettere i file in Quarantena manualmente.
Rimuovi	Permette di rimuovere un file dalla Quarantena e dal backup.
Ripristina	Permette di ripristinare un file in Quarantena nella sua posizione originale. Quando si trova un file affidabile in Quarantena e si prova a ripristinarlo, viene visualizzata un'opzione per aggiungere il file all'elenco di esclusione. È possibile aggiungere il file all'elenco di esclusione in modo che lo stesso file non venga trattato come sospetto e messo di nuovo in Quarantena.
Rimuovi Tutto	Permette di rimuovere tutti i file dalla Quarantena.
Invia	Permette di inviare i file di Quarantena ai nostri laboratori di ricerca per analisi dettagliate. Selezionare i file che si desidera inviare e poi

	cliccare su **Invia**.

Quando si invia un file in Quarantena ai laboratori di ricerca Quick Heal, vi verrà chiesto di fornire il vostro indirizzo e-mail e un motivo per l'invio dei file. I motivi includono quanto segue:

Pulsante	Descrizione
File sospetti	Selezionare questo motivo qualora si ritenga che un particolare file nel proprio sistema sia stato la causa di attività sospette nel sistema stesso.
File irreparabile	Selezionare questo motivo se Quick Heal è stato in grado di rilevare il file dannoso nel sistema durante le scansioni, ma non è stato in grado di riparare l'infezione del file.
Falso positivo	Selezionare questo motivo se un file di dati non dannoso che è già stato utilizzato e per il quale si è già consapevoli della sua funzione, è stato rilevato dall'antivirus Quick Heal come file dannoso.

Impostazioni Report

Vengono generati report su tutte le attività del prodotto antivirus Quick Heal. È possibile utilizzare questi report per verificare lo svolgimento di tutte le attività, ad esempio se il computer è stato scansionato, se è stato rilevato un malware o se è stato visitato un sito Web bloccato.

Tali report continuano ad essere aggiunti all'elenco dei report. È possibile impostare una regola che definisca quando tali report devono essere rimossi in modo automatico. L'impostazione predefinita per l'eliminazione dei report è di 30 giorni. E' inoltre possibile conservare i report qualora ve ne sia necessità.

Configurazione Impostazioni Report

Per configurare le Impostazioni Report, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello sinistro, cliccare su **Impostazioni** e poi su **Impostazioni Report**.

   Verrà mostrata la schermata con le Impostazioni Report.
3. Selezionare **Cancella report successivamente**, e poi selezionare il numero dei giorni dopo i quali tali report devono essere rimossi in modo automatico.

   Pulendo **Cancella report successivamente**, nessun report verrà rimosso.
4. Per applicare le impostazioni, cliccare su **Salva Modifiche**.

Report Statistiche di Virus

Questa funzione consente di inviare automaticamente al Centro di ricerca di Quick Heal il Report sulle statistiche di rilevamento dei virus generato durante le scansioni.

Configurare i Report Statistiche di Virus

Per configurare Report Statistiche di Virus, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, fare clic su **Impostazioni** e quindi su **Report Statistiche di Virus**. Attivare **Report Statistiche di Virus**.
3. Il Report Statistiche di Virus è attivato.

Ripristinare le Impostazioni Predefinite

Questa funzione consente di ripristinare le impostazioni personalizzate dalle impostazioni predefinite. Questo è molto utile quando si cambia le impostazioni predefinite, ma non si è soddisfatti con la protezione o si sente la vostra protezione viene compromessa. È possibile ripristinare le impostazioni di sistema predefinite.

Ripristinare le Impostazioni Predefinite

Per ripristinare le impostazioni predefinite, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello di sinistra, fare clic su **Impostazioni** e quindi su **Ripristina impostazioni predefinite**.
3. Nelle Impostazioni predefinite di ripristino, fare clic sul pulsante **Tutto predefinito**.

Il tuo antivirus Quick Heal viene ripristinato alle impostazioni predefinite.

Protezione Password

Questa funzione consente di limitare le persone non autorizzate dalla modifica delle impostazioni antivirus Quick Heal in modo che la sicurezza non sia compromessa. Si consiglia di mantenere sempre attiva la protezione con password.

Protezione di Safe Mode

Se si esegue Windows in modalità provvisoria, il computer inizia con solo i file e driver di base e le funzionalità di sicurezza di Quick Heal antivirus sono disabilitate per impostazione predefinita. In tale situazione, gli utenti non autorizzati possono sfruttare e rubare i dati o modificare le impostazioni delle funzionalità antivirus di Quick Heal.

Per impedire l'accesso al sistema da parte di utenti non autorizzati, è possibile configurare Protezione Modalità Sicura. Una volta configurato, è necessario fornire una password per lavorare in modalità provvisoria.

Configurare la Protezione Password

Per configurare la Protezione Password, procedere come segue:

1. Aprire Quick Heal antivirus.
2. Nel riquadro di sinistra, fare clic su Impostazioni e quindi su Protezione password. Attivare Protezione password.
3. La funzione Protezione password è disattivata per impostazione predefinita.
4. In Inserisci password, immettere una nuova password se si sta impostando la password per la prima volta, e quindi inserire la stessa password in Conferma password.
5. Se stai impostando la password per la prima volta, Inserisci la vecchia password non sarà disponibile.
6. Per abilitare la protezione in modalità sicura, selezionare **Abilita Protezione modalità sicura**.
7. Cliccare **Salvare Modifiche**.

Notifica novità

Con questa funzione, si ottengono le ultime notizie sulla sicurezza informatica, minacce di virus e avvisi e altre informazioni importanti relative alla protezione del computer. Le ultime notizie sono disponibili anche sotto Stato. Se non si desidera ottenere l'avviso di notizie, disattivare Notifica Novità.

Disattivare Notifica Novità

Per disattivare Notifica Novità, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel riquadro di sinistra, fare clic su Impostazioni e quindi su Notifica Novità. Disattiva Notifica Novità.

Impostazioni Internet

Questa funzione consente di attivare il supporto proxy, impostare il tipo di proxy, configurare l'indirizzo IP e la porta del proxy per l'utilizzo della connessione Internet. Se si utilizza un server proxy sulla rete, o Socks Version 4 & 5 rete, è necessario inserire l'indirizzo IP (o il nome di dominio) e la porta del proxy, SOCKS V4 & SOCKS V5 server nelle impostazioni Internet. Tuttavia, se configuri Impostazioni Internet, devi inserire il tuo nome utente e le credenziali della password.

- I seguenti moduli antivirus Quick Heal richiedono l'accesso a Internet e possono dipendere dalle impostazioni configurate.

- Procedura di registrazione guidata
- Aggiornamento rapido
- Messenger

Configurare le Impostazioni Internet

1. Aprire **Quick Heal antivirus**.
2. Nel pannello di sinistra, fare clic su **Impostazioni** e quindi su **Impostazioni Internet**.
3. Fare clic su **Impostazioni Internet** e selezionare **Abilita impostazioni proxy**.

   Vengono attivate le caselle di testo tipo proxy, server, porta e credenziali utente.
4. In **Elenco tipologie**, seleziona il tipo di proxy da HTTP, SOCKS V4, SOCKS V5 in base alle tue preferenze.
5. Nella casella di testo **Server**, inserire l'indirizzo IP del server proxy o del dominio.
6. Nella casella di testo **Porta**, immettere il numero di porta del server proxy.

   Il numero di porta è impostato come 80 per HTTP e 1080 per SOCKS V4, SOCKS V5 per impostazione predefinita.
7. Inserisci il tuo nome utente e le credenziali della password.
8. Per salvare le impostazioni, fare clic su **Salva modifiche.**

Auto-Protezione

Questa funzione consente di proteggere Quick Heal antivirus in modo che i suoi file, cartelle, configurazioni e voci di registro configurate contro il malware non vengono alterati o manomessi in alcun modo. Protegge anche i processi e i servizi di Quick Heal antivirus. Si consiglia di mantenere sempre Self Protection su. Tuttavia, questa opzione è attivata per impostazione predefinita.

Configurare Auto-Protezione

Aprire Quick Heal antivirus.

1. Nel riquadro di sinistra, fare clic su Impostazioni e quindi Auto Protezione.
2. Accendi il sistema di autodifesa.

Tuttavia, Self Protection è attivata per impostazione predefinita.

Controllo Remoto di Quick Heal

Per gestire l'antivirus Quick Heal sul tuo dispositivo tramite Quick Heal RDM, è importante mantenere sempre attiva l'opzione Gestisci in remoto Quick Heal. Tuttavia, è possibile disabilitare questa opzione se non si desidera controllare il dispositivo attraverso il portale web.

Per abilitare la gestione remota di Quick Heal, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello di sinistra, fare clic su Impostazioni e quindi su **Controllo Remoto di Quick Heal**.
3. Attivare **Controllo Remoto di Quick Heal**.

   Se non hai ancora aggiunto alcun dispositivo, viene visualizzata la pagina del prodotto Add your Quick Heal. Questa pagina visualizza la descrizione su come aggiungere un dispositivo con il link al Quick Heal portale RDM .

Controllo Remoto di Dispositivo Quick Heal

Quick Heal Remote Device Management o Quick Heal RDM è un portale web basato su cloud che offre una struttura di monitoraggio completa per gestire e controllare computer e laptop da remoto.

Con Quick Heal RDM, è possibile visualizzare alcuni stato di sicurezza dei dispositivi, cronologia delle licenze e dettagli di licenza, e rinnovare le licenze.

Per usufruire di Quick Heal RDM, seguire questi passaggi:

- Creare un account con il portale web Quick Heal RDM
- Aggiungere dispositivi al portale Quick Heal RDM

Creare un account con il portale web Quick Heal RDM

Prima di creare un account con il portale Quick Heal RDM, è necessario attivare Quick Heal antivirus sul dispositivo con una chiave di prodotto valida. Per sapere come attivare Quick Heal antivirus, consultare Registrazione di Quick Heal.

1. Una volta che l'**antivirus Quick Heal** è registrato sul tuo dispositivo, viene visualizzata la schermata di registrazione di Quick Heal RDM. Per ottenere l'invito di iscrizione, inserisci il tuo indirizzo email e quindi fai clic su Avanti.

   Un'e-mail su come attivare l'account Quick Heal RDM viene inviata al tuo indirizzo email.
2. Controlla la tua email e fai clic sul pulsante **Attiva** o copia il link indicato nel tuo browser.

   Si viene reindirizzati alla pagina Imposta password del portale Quick Heal RDM.
3. Impostare la password e quindi fare clic su **Salva**.

4. Il tuo account con il portale Quick Heal RDM viene creato con successo. Per gestire un dispositivo, è necessario aggiungere il dispositivo nel portale Quick Heal RDM prima.

Registrarsi sul portale web Quick Heal RDM

È possibile creare un account con Quick Heal RDM direttamente dal portale web anche.

Per iscriversi a Quick Heal RDM, seguire questi passaggi:

1. Visita Quick Heal RDM sul seguente sito web: https://mydevice.quickheal.com.
2. Nell'area in alto a destra, fare clic sul pulsante **Iscriviti**.

   Inserisci il nome utente o indirizzo e-mail, numero di cellulare valido e codice prodotto.
3. Inserire il codice di verifica corretto.
4. Leggere attentamente il **Contratto di Licenza** e la **Privacy Policy**.
5. Selezionare l'opzione **Accetto l'accordo di licenza Quick Heal** e l'opzione **Informativa sulla privacy.**
6. Fare clic su **Iscriviti**.

   Un'e-mail su come attivare l'account Quick Heal RDM viene inviata al tuo indirizzo email.
7. Controllare l'email e cliccare sul pulsante **Attiva** o **copia il link nel tuo browser**.

   Si viene reindirizzati alla pagina della password impostata di Quick Heal RDM.
8. Impostare la password e quindi fare clic su **Salva.**

   L'account con il portale Quick Heal RDM viene creato con successo. Per gestire un dispositivo, è necessario aggiungere il dispositivo nel portale Quick Heal RDM prima.

Registrarsi sul portale web Quick Heal RDM con l'account Google

È possibile creare un account con il portale Quick Heal RDM con il tuo account Google esistente anche.

Per iscriversi al tuo account Google, seguire questi passaggi:

1. Fare clic sul pulsante **Accedi con Google**.
2. Inserire il nome utente e la password del tuo account Google esistente.

   Leggi attentamente il **Contratto di Licenza** e le **Policy sulla privacy.**
3. Fare clic su **Accetta**.
4. Nella pagina Crea nuovo account, inserire il numero di cellulare valido e la chiave del prodotto.

5. Inserire il codice di verifica corretto.

   Leggere attentamente il Contratto di Licenza e la Privacy Policy.

6. Selezionare l'opzione **Accetto l'accordo di licenza Quick Hea**l e l'opzione **Informativa sulla privacy.**

7. Fare clic su **Iscriviti.**

   Il tuo account con il portale Quick Heal RDM viene creato con successo. Da ora in poi, puoi accedere al tuo account Quick Heal RDM utilizzando il tuo account Google esistente e gestire il tuo dispositivo.

   Al primo accesso a Quick Heal RDM, è necessario configurare la pagina Aggiungi dispositivo. Per sapere come aggiungere un dispositivo, vedere Aggiunta di un dispositivo a Quick Heal RDM.

Aggiungere Dispositivi al portale web Quick Heal RDM

Per gestire i dispositivi da remoto, è necessario aggiungere i dispositivi in Quick Heal RDM. Al primo accesso al portale Quick Heal RDM dopo aver creato un account con esso, viene richiesto di aggiungere dispositivi.

Per aggiungere un dispositivo, procedere come segue:

1. Visitare il portale Quick Heal RDM al seguente sito web: https://mydevice.quickheal.com.
2. Accedi al portale Quick Heal RDM.

   Appare la pagina **Aggiungi dispositivo**.

3. Digitare un nome sul dispositivo e inserire la chiave del prodotto.

   Puoi dare qualsiasi nome al dispositivo che preferisci.

4. Fare clic su **Aggiungi**.

   Viene generata una One Time Password (**OTP**). Per ottenere OTP, vai alla tua applicazione desktop e fai quanto segue**:**

   i. Aprire Quick Heal antivirus sul desktop e fare clic su Impostazioni.

   ii. Attivare da remoto Gestisci Quick Heal.

   Viene effettuata una convalida e viene visualizzato OTP sulla procedura Quick Heal Remote Device guidata.

5. Inserire questo OTP sul portale web Quick Heal RDM e fare clic su **Invia**.

   Il dispositivo viene aggiunto con successo.

6. Una volta convalidato l'OTP sul portale, fare clic su **Avanti** per la procedura guidata Quick Heal Dispositivo remoto ubicata sul desktop.

7. Per chiudere la procedura guidata, fare clic su **OK**.

Creare un Disco di Emergenza

È possibile creare il proprio disco di avvio di emergenza che aiuterà ad avviare il sistema del computer Windows e scansionare e pulire tutte le unità, comprese le partizioni NTFS. Questo disco aiuta a pulire il sistema gravemente infetto dai file che infettano virus che non possono essere puliti dall'interno di Windows.

Il disco di emergenza verrà creato con l'ultimo file di pattern di firma del virus utilizzato da Quick Heal antivirus sul sistema.

Per creare un disco di emergenza, procedere come segue:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello di sinistra cliccare **Impostazioni** ed in seguito cliccare su **Crea Disco di Emergenza**.
3. Nella schermata Crea disco di emergenza, fare clic sul link e scaricare il pacchetto richiesto per lo strumento di emergenza.
4. Estrai il pacchetto scaricato dal tuo sistema. Per esempio: `c:\my documents\qhemgpkg`.
5. Fornire il percorso estratto del pacchetto e fare clic su **Avanti**.
6. Per creare Disco di Emergenza, selezionare una qualsiasi delle opzioni visualizzate sullo schermo. Ad esempio, selezionare Crea disco USB di emergenza o Crea CD/DVD di emergenza.

   Note: la creazione di Disco di Emergenza utilizzando CD/DVD non è supportata su Microsoft Windows 2003 e versioni precedenti. Tuttavia, è possibile creare disco di emergenza su unità USB.

7. Selezionare l'unità disco da convertire in un disco di emergenza e fare clic su Avanti.

   Dopo la creazione di un disco di emergenza, viene visualizzato un messaggio.

Cose da ricordare durante la creazione di un disco di emergenza

- Si raccomanda di conservare una copia del pacchetto estratto sul proprio sistema.
- Durante l'utilizzo di un dispositivo USB, riscrivibile CD/ DVD, prendere un backup come il dispositivo verrà formattato.
- Per avviare il sistema da USB o CD/DVD, è necessario impostare la sequenza di avvio nel BIOS.

- Una volta completata la scansione, è necessario rimuovere il disco di emergenza USB o CD/ DVD prima di riavviare il computer, altrimenti si riavvierà nuovamente nella shell di avvio.

Usare Disco di Emergenza

1. Inserire il disco di emergenza nell'**unità CD/DVD/USB.**
2. Riavviare il sistema.
3. Disco di Emergenza avvia automaticamente la scansione di tutte le unità. Disinfetterà l'infezione, se trovata.
4. Riavviare il sistema**.**

Importazione/Esportazione Impostazioni

Questa funzione consente di importare ed esportare le impostazioni delle funzionalità antivirus di Quick Heal. Se hai bisogno di reinstallare o hai più computer e vuoi le stesse impostazioni, puoi semplicemente esportare le impostazioni configurate sul tuo computer corrente e importarle facilmente sui computer. Possono essere esportate sia le impostazioni predefinite che quelle impostate da te.

Importazione ed Esportazione delle Impostazione di Quick Heal antivirus

Per importare o esportare le impostazioni antivirus di Quick Heal, procedere come segue:

1. Aprire **Quick Heal antivirus.**
2. Sul pannello di sinistra, fare clic su **Impostazioni** e quindi fare clic sulla scheda **Importa** o **Esporta**.
    - **Importa**: Consente di importare le impostazioni da un file . dat.

      Mentre si importano le impostazioni, appare un avvertimento Questo sovrascriverà tutte le impostazioni configurate. Per confermare l'importazione, fare clic su **Sì**.
    - **Esporta**: Consente di esportare le impostazioni correnti in un file . dat.
3. Dopo l'esportazione o l'importazione, appare un messaggio. Fare clic su **OK** per chiudere la finestra di dialogo Importa o Esporta.

- Le impostazioni possono essere importate dallo stesso sapore del prodotto e solo dalla stessa versione. Ad esempio, le impostazioni di Quick Heal Antivirus Pro versione 19.00 possono essere importati in Quick Heal Antivirus Pro versione 19.00 solo.
- Le impostazioni delle seguenti funzionalità non possono essere esportate o

importate:

- Scansione Programmata
- Protezione Password

8. PCTuner

PCTuner* permette di migliorare le prestazioni del proprio computer in molteplici modi.
Per accedere a PCTuner, seguire i seguenti passaggi:

- Selezionare **Start > Programmi > Quick Heal antivirus > Quick Heal PCTuner**.
- Aprire **Quick Heal** antivirus e in Status, cliccare su **PCTuner**.

Verrà visualizzata la schermata di Quick Heal PCTuner.

Sono disponibili le seguenti funzioni di Quick Heal PCTuner:

Menu	Funzione
Dashboard	Mostra lo stato del sistema.
Tuneup	Permette di ripulire il disordine del sistema come file spazzatura, voci di registro non valide e la cronologia di navigazione.
Strumenti	Contiene gli strumenti per cancellare in modo sicuro i file dal disco rigido.
Report	Fornisce i report per le varie attività di tune-up eseguite.
Ripristino	Ripristina gli elementi rimossi durante il tuneup.
Informazioni su	Fornisce informazioni sul software e relative al supporto.
Aiuto	Include gli Aiuti. In alternativa, è possibile premere F1 per vedere l'argomento Aiuto.

Ogni funzione contiene un elenco di elementi che sono i seguenti.

Menu	Elementi Menu
Dashboard	Stato
Tuneup	Tuneup Automatico Pulizia del Disco Pulizia del Registro Pulizia Tracce Deframmentazione Programmazione Impostazioni
Strumenti	Duplica Finder dei File

	Eliminazione Sicura Startup Booster Ottimizzazione dei Servizi
Report	Tuneup Automatico Pulizia del Disco Pulizia di Registro Pulizia delle Tracce Programmazione Eliminazione Sicura Duplica Finder dei file Startup Booster Ottimizzazione Servizi Ripristino
Ripristino	Disc/Registro Startup Booster
Informazioni su	Informazioni

Stato

Questa funzione fornisce lo stato del sistema su alcune attività di tuneup di Pctuner con l'aiuto di un misuratore di stato. Le attività di messa a punto comprendono le seguenti caratteristiche:

- Pulizia del disco
- Pulizia del Registro
- Pulizia tracce
- Deframmentazione

Il puntatore del misuratore di stato punta alla regione verde scuro solo se si eseguono tutte le attività di tune-up periodicamente. La funzione Status fornisce anche lo stato delle attività di tune-up nel formato seguente.

Stato	**Descrizione**
Attività di Tune-up	Il nome dell'attività di Tuneup (Pulizia disco, Pulizia registro, Pulizia tracce e Deframmentazione).
Eseguito per Ultimo	L'ultima data di esecuzione di ciascuna attività di Tuneup. Se l'attività di Tuneup interessata non è mai stata eseguita, allora il risultato sarà **MAI.**

	La terza colonna include un simbolo contro ogni attività di Tuneup. Se il simbolo è quindi significa che l'attività di sintonizzazione corrispondente non è mai stata eseguita, o significa che l'attività di sintonizzazione corrispondente non è stata eseguita negli ultimi 15 giorni. Se il simbolo nella terza colonna è ,significa che l'attività corrispondente è stata svolta negli ultimi 15 giorni.
Pulsante di Tuneup Ora	Selezionare la modalità avanzata se si desidera personalizzare il comportamento di scansione. Questo è ideale solo per gli utenti esperti. Se selezioni questa opzione, il pulsante Configura viene attivato.

Note:

Quando si programma una Deframmentazione,il messaggio viene visualizzato il messaggio Deframmentazione è stato impostato per essere eseguito al prossimo avvio.

Tuneup

Questa funzione pulisce disordine di sistema come i file spazzatura non validi e indesiderati, voci di registro non valide, tracce della cronologia di Internet, e così via. Tuneup include le seguenti opzioni.

Tuneup Automatico

Auto Tuneup esegue **Pulizia Disco, Pulizia Registro, Pulizia Tracce** e **Deframmentazione**. E 'ideale per gli utenti alle prime armi, e per gli utenti che non vogliono perdere tempo eseguendo attività di pulizia individuale. Solo gli elementi eliminati da Pulizia Disco e Pulizia del Registro possono essere recuperati.

Personalizzare il Tuneup Automatico

Prima di eseguire, è necessario personalizzare Tuneup Automatico per eseguirlo secondo i propri requisiti. Per personalizzare Tuneup Automatico, seguire questi passaggi:

1. Selezionare **Sintonizza > Impostazioni**.

   Appare la schermata Impostazioni di sintonia. Questa schermata ha tre schede: Impostazioni disco, Impostazioni registro e Traccia impostazioni. Ogni scheda ha una lista di elementi preceduta da una casella di controllo. Tutti gli elementi sono selezionati in ciascuna scheda per impostazione predefinita.

2. Cancella gli elementi che devono essere saltati da Tuneup Automatico. Per un utente inesperto, si consiglia di mantenere tutti gli elementi selezionati.

Esegui il backup prima di eliminare è selezionato per impostazione predefinita. Se questa opzione non è selezionata, Auto Tuneup eliminerà tutti gli elementi senza eseguire il backup. Si consiglia di tenerlo selezionato.

3. Fare clic su **Applica** per salvare le nuove impostazioni.
4. Fare clic su **Chiudi** per uscire senza salvare le impostazioni.

Eseguire il Tuneup Automatico

Per eseguire il Tuneup Automatico, procedere come segue:

1. Selezionare **Tuneup** > **Tuneup Automatico** .
2. Fare clic su **Impostazioni** se si desidera personalizzare il Tuneup Automatico come indicato nella sezione precedente.
3. Fare clic su **Start** per iniziare il Tuneup Automatico.
4. Fare clic su **Stop** se si desidera interrompere il Tuneup Automatico; altrimenti fare clic su **Chiudi** dopo il completamento del Tuneup Automatico.

Pulizia del Disco

Pulizia del Disco trova e rimuove i file spazzatura non validi e indesiderati dal disco rigido. Questi file consumano spazio sul disco rigido e anche rallentare il sistema notevolmente. Pulizia del Disco elimina questi file liberando spazio e aiuta a migliorare le prestazioni del sistema. La funzione Pulizia disco elimina anche i file temporanei, i file cache Internet, i file di scelta rapida impropri, i file di nome spazzatura e le cartelle vuote.

Eseguire la Pulizia del Disco

Per eseguire Pulizia disco, procedere come segue:

1. Selezionare **Tuneup > Pulizia disco**.
2. Fare clic su **Impostazioni** per personalizzare Pulizia disco.
3. Fare clic su **Start.**

Una lista con le posizioni del file e la sua categoria spazzatura appare.

È possibile fare clic su **Stop** per fermare le voci aggiunte alla lista.

Ogni posizione del file sarà preceduta da una casella di controllo. Tutte le posizioni dei file sono selezionate per impostazione predefinita.

4. Cancellare le posizioni che devono essere saltate da **Pulizia disco.**
5. Ci sono altri quattro campi che mostrano le seguenti informazioni:
   - **File trovati**:Il totale dei file trovati durante la Pulizia del DIsco.
   - **Dimensione Totale**: la dimensione del totale dei file trovati durante la Pulizia del Disco.
   - **Files Selezionati**: Il numero di File selezionati per l'eliminazione.

- **Dimensione File Selezionati**: la dimensione del totale dei file selezionati per l'eliminazione.

1. Cliccare **Rimuovi File** per rimuovere i file.
2. Cliccare **Chiudi** per uscire dalla Pulizia del Disco.

Pulizia del Registro

Questa funzione rimuove voci di registro non valide e obsolete dal sistema che appaiono a causa di caratteri impropri non-installati o inesistenti. A volte durante la disinstallazione, le voci del registro di sistema non vengono eliminate. Ciò si traduce in prestazioni più lente del sistema. Questa funzione rimuove tali voci di registro non valide per aumentare le prestazioni del sistema.

Eseguire la Pulizia del Registro

Per eseguire Registry Cleanup, procedere come segue:

1. Selezionare **Tuneup > Pulizia del registro**.
2. Fare clic su **Impostazioni** per personalizzare Pulizia del Registro come indicato nella sezione precedente.
3. Fare clic su **Start**.

   Viene visualizzato un elenco con le voci di registro e il loro percorso.
4. È possibile fare clic su **Stop** per fermare le voci aggiunte alla lista.

   Ogni voce del registro sarà preceduta da una casella di controllo. Tutte le voci del registro sono selezionate per impostazione predefinita.
5. Cancellare le voci di registro che devono essere saltate dalla Pulizia del Registro.
6. Ci sono altri due campi che mostrano le seguenti informazioni:
   - **Elementi trovati**: Il numero totale di voci del registro trovate per Registry Cleanup.
   - **Elementi selezionati**: Il numero totale di voci di registro selezionate per la rimozione.
7. Cliccare **Rimuovere voci** per rimuovere i file.
8. Cliccare **Chiudi** per uscire dalla Pulizia di Registro.

Pulizia Tracce

Questa funzione rimuove tracce dalla cronologia di Internet e MRU (Most Recently Used) elenco di varie applicazioni. Elimina in modo sicuro la cronologia, pulisce i cookie, la cache, i moduli auto-completi e le password. Tracce come voci auto complete e password salvate devono essere eliminati per garantire che la privacy degli utenti non venga violata. Inoltre cancella le tracce da programmi di applicazione popolari come le applicazioni di Microsoft

Office, Adobe Acrobat Reader, Media Player, Winzip, Winrar e tracce come cookie del browser e password salvate.

Eseguire la Pulizia Tracce

Per eseguire la Pulizia Tracce, procedere come segue:

1. Selezionare **Tuneup > Pulizia Tracce**.
2. Fare clic su **Impostazioni** se si desidera personalizzare la Pulizia delle tracce come indicato nella sezione precedente.
3. Fare clic su **Start**.

   Appare un elenco con applicazioni contenenti tracce.
4. È possibile fare clic su **Stop** per fermare le voci aggiunte alla lista.

   Ogni applicazione contenente tracce sarà preceduta da una casella di controllo. Tutte le applicazioni contenenti tracce sono selezionate per impostazione predefinita.
5. Cancella le applicazioni che devono essere saltate da Pulizia tracce
6. Ci sono altri due campi che mostrano le seguenti informazioni:
   - **Totale file Trovati:** Il numero totale di applicazioni contenenti tracce trovate da Traces Cleanup.
   - **Elementi selezionati**: numero totale di applicazioni contenenti tracce selezionate per la rimozione.
7. Fare clic su Pulisci elementi per rimuovere le tracce dalle applicazioni elencate.
8. Fare clic su Chiudi per uscire da Traces Cleanup.

Deframmentazione

I file sono spesso memorizzati in diverse posizioni che rallentano le prestazioni del sistema. Questa funzione deframmenta i file vitali, come file di pagina e alveari di registro per migliorare le prestazioni del sistema. Deframmentazione riduce il numero di frammenti e raggruppa tutti i frammenti in un blocco contiguo per migliorare le prestazioni del sistema.

Usare la Deframmentazione

Per deframmentare i file della pagina e gli alveari di registro, attenersi alla seguente procedura:

1. Seleziona **Sintonizza > Deframmentazione.**

Appaiono due opzioni per la deframmentazione: **Abilita deframmentazione** e **Annulla deframmentazione**. Annulla deframmentazione è selezionata per impostazione predefinita.

2. Selezionare **Deframmentazione al prossimo avvio** per eseguire la deframmentazione la prossima volta che si avvia il sistema; altrimenti selezionare **Deframmentazione ad ogni avvio** per eseguire la deframmentazione ogni volta che si avvia il sistema.
3. **Deframmentazione sistema di paging file (memoria virtuale)** e **Deframmentazione Registro di sistema di Windows** non sono selezionati come impostazioni predefinite. È possibile selezionare uno qualsiasi di questi due o entrambi per la deframmentazione da eseguire. Si consiglia di mantenere queste opzioni selezionate.
4. Fare clic sul pulsante **Applica** per salvare queste impostazioni, oppure fare clic su **Chiudi** per uscire senza salvare.

Scheduler

Questa funzione consente di pianificare periodicamente l'attività di Tuneup in base alle proprie esigenze. È possibile configurare la pianificazione di Tuneup per eseguire la Pulizia del Disco, la Pulizia del Registro, la Pulizia delle Tracce e la funzione Deframmentazione. E' possibile creare un'attività e programmarla. L'attività viene eseguita in background all'ora specificata al momento della creazione dell'attività. È possibile visualizzare i dettagli delle attività eseguite in Schedule Report.

Personalizzazione Scheduler

E' possibile effettuare la personalizzazione di Scheduler per essere eseguito in base alle proprie esigenze. Tuttavia, la Deframmentazione può essere programmata solo al successivo boot. Per la personalizzazione di Scheduler, seguire questi passaggi:

1. Selezionare **Tuneup > Scheduler**.

   Viene visualizzato un elenco di attività insieme ai dettagli quali Nome attività, Frequenza, Attività, Backup ed Elimina backup meno recente.
2. Ci sono tre opzioni selezionabili quando si pianifica l'attività di tuneup:
   i. **Nuovo** – per configurare qualunque attività
   ii. **Modifica** – per modificare un'attività esistente
   iii. **Rimuovi** – per rimuovere un'attività già pianificata
3. Per pianificare un nuova attività di Tuneup, cliccare su **Nuovo**.

   Verrà mostrata la schermata Configura Pianificazione di Tuneup.
4. Immettere i dettagli relativi a **Nome attività**, **Frequenza**, e **Avvia alle**.

   Ciascuna attività di Tuneup nella schermata è preceduta da una casella di spunta. Tutti gli elementi sono selezionati nell'elenco per impostazione predefinita.
5. Pulire gli elementi che devono essere bypassati dalla funzione Scheduler.

6. **Esegui backup prima della pulizia** è selezionato per impostazione predefinita. Se questa opzione non è selezionata, la pulizia verrà eseguita senza effettuare il backup. Si raccomanda di mantenerlo selezionato. **Elimina il backup più vecchio se viene superato il limite massimo di backup**, eliminerà il backup più vecchio quando il limite del backup viene superato.
7. Inserire **Nome Utente** e **Password**.
8. Cliccare su **Applica** per salvare le nuove impostazioni oppure altrimenti cliccare su **Chiudi** per uscire senza salvare le impostazioni.

Nota:

Mantenendo non selezionata l'opzione Elimina backup meno recente se viene superato il limite massimo di backup, quando il limite di backup viene superato Scheduler non funzionerà.

Impostazioni

Questa funzione consente di personalizzare le impostazioni del disco, le impostazioni del registro e traccia le impostazioni secondo i requisiti.

Personalizzare la Pulizia del Disco

È possibile personalizzare Pulizia disco per eseguire secondo i requisiti prima di eseguirlo. Per personalizzare Pulizia disco, seguire questi passaggi:

1. Selezionare **Sintonizza > Impostazioni**.

   Viene visualizzata la schermata Impostazioni di sintonizzazione.

2. Fare clic su **Impostazioni disco**.

   Ogni elemento della lista è preceduto da una casella di controllo. Tutti gli elementi sono selezionati nella lista per impostazione predefinita.

3. Cancella gli elementi che devono essere saltati dalla funzione Pulizia disco.
4. **Eseguire il backup prima di eliminare i file** è selezionato per impostazione predefinita. Se questa opzione non è selezionata, Pulizia disco eliminerà tutti gli elementi senza eseguire il backup. Si consiglia di tenerlo selezionato.
5. Fare clic su **Applica** per salvare le nuove impostazioni oppure fare clic su **Chiudi** per uscire senza salvare le impostazioni.

Personalizzare la Pulizia Registro

È possibile personalizzare Pulizia del Registro per eseguire secondo i requisiti prima di eseguirlo. Per personalizzare Pulizia del Registro, seguire questi passaggi:

1. Selezionare **Sintonizza > Impostazioni**.

Viene visualizzata la schermata Impostazioni di sintonizzazione.

2. Fare clic su **Impostazioni del Registro di sistema**.

   Ogni elemento della lista è preceduto da una casella di controllo. Tutti gli elementi sono selezionati nella lista per impostazione predefinita.

3. Cancella gli elementi che devono essere saltati dalla funzione Pulizia del Registro.
4. **Eseguire il backup prima di eliminare gli elementi** è selezionato per impostazione predefinita. Se questa opzione non è selezionata, Pulizia del Registro eliminerà tutti gli elementi senza prendere il backup. Si consiglia di tenerlo selezionato.
5. Fare clic su **Applica** per salvare le nuove impostazioni oppure fare clic su **Chiudi** per uscire senza salvare le impostazioni.

Personalizza la Pulizia Tracce

È possibile personalizzare la Pulizia Tracce per eseguire secondo i requisiti prima di eseguirlo. Per personalizzare la Pulizia TRacce, seguire questi passaggi:

1. Selezionare **Sintonizza > Impostazioni**.

   Viene visualizzata la schermata **Impostazioni di sintonizzazione**.

2. Fare clic su **Impostazioni tracce**.

   Ogni elemento della lista è preceduto da una casella di controllo. Tutti gli elementi sono selezionati nella lista per impostazione predefinita.

3. Cancella gli elementi che devono essere saltati dalla funzione Pulizia tracce.
4. **Eseguire il backup prima di eliminare i file** è selezionato. Se questa opzione non è selezionata, Pulizia del Registro eliminerà tutti gli elementi senza prendere il backup. Si consiglia di tenerlo selezionato.
5. Fare clic su **Applica** per salvare le nuove impostazioni oppure fare clic su **Chiudi** per uscire senza salvare le impostazioni.

Strumenti

Questa funzione consente di eliminare i file duplicati dal sistema. Offre la cancellazione sicura in cui i file vengono eliminati in modo permanente e non saranno recuperati anche se il software di recupero viene utilizzato. Il menu Strumenti include le seguenti opzioni.

Duplicate File Finder

Questa funzione rimuove i file duplicati di varie categorie di file predefinite. Cerca i file duplicati su posizioni specifiche dell'utente. L'utente può anche fornire un elenco di esclusione delle cartelle, da omettere dalla scansione dei file duplicati. I file duplicati verranno eliminati utilizzando il metodo di cancellazione One Pass, Two Pass o Dod secondo le preferenze. Il metodo di cancellazione predefinito è One Pass.

Le categorie di file predefinite che verranno scansionate durante l'esecuzione della funzione Duplicate File Finder sono le seguenti.

Categoria di File	Estensione
Immagini/ Foto	.pcx, .tiff, .wpg, .bmp, .gif, .jpg, .jpeg, .wmp, .png, .tif
File Creative Artwork	.ai, .eps, .pcx, .psd, .tiff, .wpg, .bmp, .gif, .jpg, .jpeg, .wmp, .png, .cdr, .pdf, .tif
Filmati	.avi, .rm, .vob, .mov, .qt, .mpeg, .mpg, .mpe, .mpa, .dat
File Audio	.wmv, .wma, .mp4, .mp3
File di Testo	.txt, .asci, .xml
Documenti	.pdf, .doc, .rtf, .wri, .sam, .dox, .xls, .ppt, .docx, .xlsx, .pptx, .wk3, .wk4, .vsd, .vsdx, .wg, .123, .wpd
Email	.eml

Eliminare File Duplicati

Per eliminare i file duplicati, procedere come segue:

1. Selezionare **Strumenti > Duplicate File Finder**.
2. Per modificare le impostazioni di **Duplicate File Finder**, fare clic su **Opzioni**.

   Appare la finestra Opzioni **Duplicate File Finder** di Quick Heal
3. Nell'elenco Seleziona un tipo di categoria duplicato; cancella le categorie che devono essere saltate dal Duplicate File Finder.

   Nell'elenco Escludi cartella/e, è possibile aggiungere elenchi di esclusione Duplicate File Finder per saltarle.
4. Fare clic sul pulsante **Aggiungi cartella** per aggiungere le posizioni per le esclusioni. Selezionare una posizione e fare clic su **Cancella** se la posizione aggiunta è errata. Fare clic su **Cancella tutto** per rimuovere tutte le posizioni di esclusione aggiunte.
5. L'opzione **Use Secure Delete** è attivata e il metodo One Pass Random - Quick Data Destruction è selezionato per impostazione predefinita. È possibile selezionare qualsiasi metodo di eliminazione. Vedere **Metodi di eliminazione** per conoscere i diversi metodi di eliminazione.
6. Fare clic sul pulsante **Applica** per salvare la modifica delle impostazioni oppure fare clic sul pulsante **Chiudi** per uscire senza salvare le impostazioni modificate.
7. Fare clic su **Aggiungi** percorso per aggiungere il percorso per Duplicate File Finder per cercare i file duplicati.

   Viene visualizzata la finestra **Sfoglia cartella**.

8. Cerca la cartella desiderata. Selezionare **Escludi sottocartella** se si desidera escludere le sottocartelle all'interno della cartella nella scansione. L'opzione **Escludi sottocartella** non è selezionata per impostazione predefinita.
9. Fare clic su **OK** dopo aver selezionato il percorso richiesto. Se il percorso aggiunto non è corretto, selezionare quel percorso e fare clic su Cancella per eliminare il percorso. Fare clic su **Cancella tutto** per eliminare tutti i percorsi aggiunti dall'elenco.
10. Fare clic su **Avvia ricerca**.

Viene visualizzato un elenco delle posizioni dei file con posizioni di file duplicate. Le informazioni della scansione sono fornite nei seguenti campi.

- **Avanzamento ricerca**: Visualizza lo stato di avanzamento della ricerca.
- **Cartelle scansionate: consente di visualizzare il numero di cartelle scansionate.**
- **File scansionati**: Visualizza il numero di file scansionati.
- **Duplicati trovati**: Visualizza il numero di file con duplicati trovati.
- **Spazio sprecato**: Visualizza lo spazio che è stato consumato dai file duplicati.

11. Fare clic su **Controlla tutto** per selezionare tutti i file duplicati all'interno degli originali espansi.
12. Fare clic su **Elimina** per eliminare tutti i file duplicati.
13. Fare clic su **Chiudi** per uscire dal menu **Strumenti.**

Eliminazione Sicura

Questa funzione viene utilizzata per l'eliminazione di file o cartelle indesiderati completamente dal sistema. Nel caso in cui si desidera eliminare i dati riservati, Secure Delete consente di eliminare i dati rendendo assolutamente impossibile recuperare con qualsiasi mezzo. I dati cancellati utilizzando la funzione Elimina di Windows possono essere recuperati utilizzando un software di recupero come il link a tali dati rimane nel cluster di hard disk. La funzione Secure Delete di Quick Heal Pctuner cancella il file o le cartelle direttamente dal disco rigido rendendolo irrecuperabile anche se viene utilizzato un software di recupero

Metodi di Eliminazione

Di seguito sono riportati i tre metodi di eliminazione dei file disponibili in Quick Heal Pctuner.

Metodo di Eliminazione	Descrizione
One Pass Random – Distruzione Dati	One-pass random usa lettere casuali per sovrascrivere i dati. Questo metodo di cancellazione è rapido e abbastanza sicuro. I dati una volta

veloce	cancellati non possono essere recuperati. Questa è l'opzione migliore per la maggior parte degli utenti. Questo è anche il metodo predefinito di eliminazione dei file.
Two Pass – Distruzione più sicura	Two-pass utilizza il doppio del numero di lettere casuali per sovrascrivere i dati. Questo metodo di eliminazione fornisce un ulteriore livello di sicurezza. I dati una volta eliminati non possono essere recuperati da alcun software di recupero.
DoD – Distruzione dati Standard	DoD utilizza il metodo di crittografia che si avvale di lettere casuali per sovrascrivere i dati secondo il Department of Defense Memo. I dati una volta eliminati non possono essere recuperati da alcun software di recupero.

Utilizzo Cancellazione Sicura

Per cancellare i file e le cartelle utilizzando la Cancellazione Sicura, seguire questi passaggi:

1. Selezionare **Strumenti > Cancellazione Sicura**.
2. Cliccare sul pulsante **Opzioni**.

   Viene visualizzata la finestra Seleziona metodo di cancellazione sicura.
3. Seleziona il metodo di cancellazione e poi cliccare sul pulsante **Accetta**. Selezionare **Abilita Eliminazione Sicura tramite Tasto Destro (Menu contestuale)** per qualsiasi dato semplicemente facendo clic destro su **Eliminazione sicura.**
4. Fare clic sul pulsante **Aggiungi file** per individuare il file che si desidera eliminare.
5. Fare clic sul pulsante Aggiungi cartella per individuare la cartella e le sottocartelle che si desidera eliminare.

   Se la selezione per l'eliminazione dei file non è corretta, selezionare il file e fare clic su **Cancella**. Fare clic su **Cancella tutto** per eliminare tutte le selezioni.
6. Cliccare **Continua**.
7. Una finestra appare con il messaggio che la cancellazione è irrecuperabile. Aiuta anche a cambiare il metodo di cancellazione. Se si desidera modificare il metodo di cancellazione in questa fase, fare clic su **Opzioni**. Fare clic su **Sì** per procedere con il processo di cancellazione.
8. I file selezionati vengono eliminati e viene visualizzata una schermata di riepilogo Cancellazione.
9. Fare clic sul pulsante **Visualizza Report** per visualizzare il Report del processo di eliminazione oppure fare clic su **Chiudi** per uscire dal menu **Strumenti**.

Startup Booster

Questo strumento rimuove i programmi di avvio indesiderati dal sistema. Rimuove tutte le applicazioni non necessarie dal Registro di sistema Run e Startup, e migliora la velocità di avvio del sistema.

Usare Startup Booster

Per utilizzare Startup Booster, segui questi passaggi:

1. Selezionare **Strumenti >Startup Booster**
2. Fare clic su **Avvia ricerca.**

   Le applicazioni che si caricano automaticamente durante l'avvio vengono visualizzate in un elenco. Ogni applicazione è preceduta da una casella di controllo. Nessuna applicazione è selezionata per impostazione predefinita.
3. Selezionare le applicazioni che devono essere rimosse dal caricamento ogni volta che il sistema si avvia.
4. Fare clic su **Rimuovi** per rimuovere l'applicazione dall'elenco oppure fare clic su **Chiudi** per uscire.

Ottimizzazione del Servizio

Il computer può avere molti servizi indesiderati che vengono eseguiti all'avvio, consumando CPU e memoria che possono potenzialmente rallentare le prestazioni del sistema. Service Optimizer analizza il sistema e suggerisce servizi che possono essere disattivati in modo sicuro per l'esecuzione all'avvio in base alle risposte ai servizi correlati.

Di seguito sono riportati i servizi disponibili per Service Optimizer in Quick Heal Pctuner.

- Servizi connessi alla rete
- Servizi relativi al sistema
- Servizi relativi alle prestazioni
- Servizi connessi alla sicurezza

Usare Service Optimizer

1. Per utilizzare Service Optimizer, procedere come segue:
2. Selezionare **Strumenti > Service Optimizer.**

   I servizi sono suddivisi in quattro sezioni rappresentate da quattro schede: Rete, Sistema, Prestazioni e Sicurezza.
3. Seleziona il servizio e seleziona la risposta alle domande in ogni sezione.

Ogni volta che si apre Service Optimizer, il pulsante Applica appare attenuato. Tuttavia, cambiando una qualsiasi delle risposte, come se si seleziona SÌ o NO, il pulsante Applica viene attivato.

4. Fare clic sul pulsante **Applica** per ottimizzare il servizio oppure fare clic su **Chiudi** per uscire senza salvare.
5. È possibile ottenere un riepilogo di ottimizzazione del servizio se si è ottimizzato qualsiasi servizio. Fare clic su **Visualizza Report** per visualizzare il Report dettagliato oppure fare clic su **Chiudi** per uscire.

Note:

- Se le risposte relative ai servizi non richiedono alcuna modifica, viene visualizzato un messaggio.
- Se si fa clic sul pulsante Predefinito, tutti i servizi ottimizzati vengono ripristinati allo stato originale.

Report

Questo menu contiene report per varie attività eseguite da Quick Heal PCTuner. Include diverse voci di menu. Ogni voce di menu corrisponde al report di una particolare attività.

Le voci nel menu Report sono le seguenti.

Ci sono quattro pulsanti in ogni voce di menu. Le loro azioni sono le stesse per tutte le voci di menu che sono le seguenti:

Pulsante	Azione
Dettagli	Permette di visualizzare un report dettagliato dei record selezionati nell’elenco.
Cancella tutto	Permette di cancellare tutti i report dell’elenco.
Cancella	Permette di cancellare dall’elenco i report selezionati.
Chiudi	Permette di uscire dal menu Report.

Cliccando sul pulsante Dettagli in qualsiasi voce di menu, si apre una finestra denominata Report. Ciò include altri cinque pulsanti le cui azioni sono comuni a tutte le voci di menu che sono le seguenti:

Pulsante	Azione
Precedente	Permette di visualizzare il report dettagliato del record precedente nell'elenco.
Successivo	Permette di visualizzare il report dettagliato del record successivo nell'elenco.

Stampa	Permette di produrre la stampa del report dettagliato.
Salva come	Permette di salvare sul sistema il report dettagliato in formato testo.
Chiudi	Permette di uscire dalla finestra Report.

Report Auto Tuneup

Questa funzione include un elenco di record con un report dettagliato sulla funzione di Auto Tuneup eseguita sul sistema. Per visualizzare i Report di Auto Tuneup, seguire questi passaggi:

1. Selezionare **Report > Auto Tuneup**.
2. Selezionare nell'elenco il record richiesto.
3. Cliccare sul pulsante **Dettagli**.

   Viene visualizzata la finestra Report che include il report dettagliato per il record selezionato.

Report di Cleanup Disco

Questa funzione include un elenco di record con un report dettagliato sulla funzione **Cleanup Disco** eseguita sul sistema. Per visualizzare i Report d Cleanup Discoi, seguire questi passaggi:

1. Selezionare **Report > Cleanup Disco**.
2. Selezionare nell'elenco il record richiesto.
3. Cliccare sul pulsante **Dettagli**.

   Viene visualizzata la finestra Report che include il report dettagliato per il record selezionato.

Report Cleanup di Registro

Questa funzione include un elenco di record con un report dettagliato sulla funzione **Cleanup di Registro** eseguita nel sistema. Per visualizzare i report su Cleanup di Registro, seguire questi passaggi:

1. Selezionare **Report > Cleanup di Registro**.
2. Selezionare nell'elenco i record desiderati.
3. Cliccare sul pulsante **Dettagli**.

   Viene visualizzata la finestra Report che include il report dettagliato per il record selezionato.

Report Pulizia Tracce

Questa funzione include un elenco di record con un Report dettagliato sulla funzionalità Traces Cleanup eseguita sul sistema. Per visualizzare i report di pulizia delle tracce, procedere come segue:

1. Selezionare **Report > Pulizia Tracce**.
2. Selezionare il record richiesto nell'elenco.
3. Fare clic sul pulsante **Dettagli**.

Appare la finestra **Report** che include il report dettagliato per il record selezionato.

Report di Pianificazione

Questa funzione include un elenco di record con una relazione dettagliata su tutte le attività pianificate eseguite sul sistema. Per visualizzare Scheduler Reports, procedere come segue:

1. Selezionare **Report > Pianificazione**.
2. Selezionare il record richiesto nell'elenco.
3. Fare clic sul pulsante **Dettagli**.

Appare la finestra **Report** che include il report dettagliato per il record selezionato.

Report di Eliminazione Sicura

Questa funzione include un elenco di record con un Report dettagliato sulla funzione Eliminazione Sicura eseguita sul sistema. Per visualizzare i report di eliminazione sicura, procedere come segue:

1. Selezionare **Report > Eliminazione sicura**.
2. Selezionare il record richiesto nell'elenco.
3. Fare clic sul pulsante **Dettagli**.

Appare la finestra Report che include il report dettagliato per il record selezionato.

Report Duplicate File Finder

Questa funzione include un elenco di record con un Report dettagliato sulla funzione Duplicate File Finder eseguita sul sistema. Per visualizzare i **Report Duplicate File Finder,** procedere come segue:

1. Selezionare **Report > Duplicate File Finder**.
2. Selezionare il record richiesto nell'elenco.
3. Fare clic sul pulsante **Dettagli**.

Appare la finestra **Report** che include il report dettagliato per il record selezionato.

Report di Startup Booster

Questa funzione include un elenco di record con un report dettagliato sulla funzione di Startup Booster eseguita sul sistema. Per visualizzare i Report di Startup Booster, attenersi alla seguente procedura:

1. Selezionare **Report > Startup Booster**.
2. Selezionare nell'elenco il record richiesto.
3. Cliccare il pulsante dei **Dettagli**.

   Viene visualizzata la finestra Report che include il report dettagliato per il record selezionato.

Report di Service Optimizer

Questa funzione include un elenco di record con un report dettagliato sulla funzione **Service Optimizer** eseguita sul sistema. Per visualizzare i report di Service Optimizer, seguire questi passaggi:

1. Selezionare **Report > Service Optimizer**.
2. Selezionare nell'elenco il record richiesto.
3. Cliccare il pulsante dei **Dettagli**.

   Viene visualizzata la finestra Report che include il report dettagliato per il record selezionato.

Report di Ripristino

Questa funzione include un elenco dei record (tramite un report dettagliato sulla funzione **Ripristino** eseguita sul sistema. Per visualizzare i Report di Ripristino, seguire questi passaggi:

1. Selezionare **Report > Ripristino**.
2. Selezionare nell'elenco il record richiesto.
3. Cliccare il pulsante dei **Dettagli**.

   Viene visualizzata la finestra Report che include il report dettagliato per il record selezionato.

Ripristino

Questa funzione ripristina gli elementi nelle sue posizioni originali che sono stati eliminati da una qualsiasi delle funzionalità di pulizia del disco, pulizia del registro e Startup Booster. Tuttavia, non ripristina gli elementi eliminati dalla Pulizia Tracce.

⚠ Consiglio:

Se **Elimina elementi senza eseguire il backup** non è selezionato durante **Pulizia disco o Pulizia registro**, il backup non verrà eseguito. In caso di Tuneup Automatico, **Eseguire il backup prima di eliminare i file** deve essere selezionato per eseguire il backup e ripristinare i file quando necessario.

L'area Ripristina punti elenca le attività di ottimizzazione che possono essere ripristinate. Le azioni che possono essere eseguite sui punti di ripristino sono le seguenti.

Ripristinare Report

Per ripristinare, seguire questi passaggi:

1. Selezionare il **Punto di Ripristino** richiesto.
2. Fare clic sul pulsante Ripristina.
3. Appare una finestra con il seguente messaggio: **Sei sicuro di voler ripristinare il backup?** Fare clic su **Sì** se si desidera ripristinare il backup oppure fare clic su **No** se non si desidera ripristinare il backup.
4. Se si è fatto clic su **Sì** nel passaggio precedente, il backup viene ripristinato e viene visualizzato un messaggio Il backup selezionato è stato ripristinato con successo. Fare clic su OK per completare il processo di ripristino.

Eliminare Report

Per eliminare uno qualsiasi dei punti di ripristino nell'elenco, procedere come segue:

1. Selezionare il **Punto di Ripristino** richiesto.
2. Fare clic sul pulsante **Elimina**.
3. Appare un messaggio con il seguente avviso: **Sei sicuro di volerlo eliminare?** Fare clic su **OK** se si desidera eliminare il punto di ripristino oppure fare clic su **Annulla** per uscire senza eliminare.

9. Aiuto & Altri consigli

Gli aggiornamenti per l’antivirus Quick Heal vengono rilasciati regolarmente. Questi aggiornamenti possono includere miglioramenti o funzionalità di sicurezza contro nuovi malware e virus. Per impedire al computer di ricevere nuovi virus, è necessario mantenere sempre aggiornato l'antivirus Quick Heal.

L'impostazione predefinita dell'antivirus Quick Heal è configurata per ricevere gli aggiornamenti automaticamente da Internet, senza l'intervento dell'utente. Tuttavia, il sistema deve essere connesso a Internet per ricevere regolarmente gli aggiornamenti.

Nota:

- Gli aggiornamenti possono includere miglioramenti e nuove firme del database dei virus contro nuovi malware e virus.
- Gli aggiornamenti possono aggiornare la versione corrente dell'antivirus Quick Heal alla nuova versione.

E' possibile aggiornare l'antivirus Quick Heal online e offline in base alle preferenze.

Aggiornamento online Quick Heal

Tuttavia, l'impostazione predefinita dell'antivirus Quick Heal è configurata per ricevere automaticamente gli aggiornamenti da Internet. Tramite Aggiorna Ora, è possibile aggiornare manualmente l'antivirus Quick Heal ogni volta che si preferisce.

Per aggiornare l'antivirus Quick Heal online, segui questi passaggi.

1. Cliccare col tasto destro sull'icona dell'antivirus Quick Heal dell'area di notifica e selezionare **Aggiorna Ora**.

   In alternativa, aprire **Quick Heal antivirus**. Nell'angolo in alto a destra, fai clic sul menu e quindi seleziona **Informazioni su**. Nella schermata Informazioni, fare clic sul pulsante **Aggiorna ora**.

   Quick Update avvierà l'aggiornamento.

2. Al completamento dell'aggiornamento, cliccare su **Fine**.

   Nota: Quick Update si connette al sito web di Quick Heal, scarica gli aggiornamenti appropriati, e li applica.

Aggiornare Quick Heal offline

È possibile aggiornare l'antivirus Quick Heal senza connettersi a Internet. L'aggiornamento offline è utile se il computer in cui è installato Quick Heal antivirus non è connesso a Internet o se si dispone di diversi computer. Non è necessario scaricare l'aggiornamento su tutti i computer della rete.

Per aggiornare Quick Heal antivirus offline, segui questi passaggi.

1. Visitare http://www.quickheal.com/update.

2. Sul portale Quick Heal Offline Product Updates, inserire le informazioni richieste sulla versione del prodotto, sull'architettura del sistema operativo e sul tipo di aggiornamenti.
3. Fare clic sul pulsante **Scarica**.
4. Fare doppio clic sul file scaricato.

   Appare la procedura guidata Quick Heal Updater.

5. Fare clic su **Aggiorna ora**.

   In alternativa, è possibile fare clic sul link **Estrai gli aggiornamenti** e sfogliare la cartella in cui si desidera salvare l'aggiornamento. Una volta salvato l'aggiornamento, puoi andare nella cartella e applicare l'aggiornamento manualmente.

   Tuttavia, è possibile selezionare **Installa aggiornamenti dopo l'estrazione** e quindi fare clic su **Continua** per applicare l'aggiornamento automaticamente.

   Il tuo antivirus viene aggiornato con successo.

Aggiornare le linee Guida per l'ambiente di rete

Se si utilizzano più computer con Quick Heal installato, è possibile configurare un server per fornire aggiornamenti gratuiti a tutti i computer della rete. Si consiglia di seguire queste linee guida per ottenere i migliori risultati.

1. Imposta un computer (può essere il server) come macchina di aggiornamento master. Supponiamo che il nome del server sia **SERVER.**
2. Crea una cartella denominata **QHUPD** su un'unità locale nel tuo computer. Ad esempio: **C: QHUPD.** Assegna a questa cartella il diritto di condivisione in sola lettura.
3. Aprire **Quick Heal antivirus**.
4. Nel riquadro di sinistra, fare clic su **Impostazioni** e quindi su **Aggiornamento automatico**. Attivare Aggiornamento automatico.
5. L'a**ggiornamento automatico** è attivato.
6. Fare clic sull'icona di impostazione per l'aggiornamento automatico.
7. Selezionare **Copia i file di aggiornamento** nella posizione specificata.
8. Sfoglia la cartella **QHUPD** e clicca su **OK**.
9. Per salvare le impostazioni, fare clic su **Salva modifiche**.
10. Su tutti i computer utente all'interno della rete, lanciare **Quick Heal antivirus**.

11. In Impostazioni, vai alla pagina Aggiornamento automatico.

    Selezionare **Scegli i file di aggiornamento** dal percorso specificato e fare clic su **Sfoglia**.

12. Individuare la cartella `SERVER\QHUPD` in Risorse di Rete. In alternativa si può trascrivere il percorso `\\SERVER\QHUPD`.

13. Per salvare le nuove impostazioni, cliccare **Salva Modifiche**.

Pulizia Virus

Quick Heal antivirus vi avvisa della presenza di un'infezione virus quando:

- Un virus viene individuato durante una Scansione manuale.
- Un virus viene individuato da Protezione Virus/Protezione Email Quick Heal.

Pulizia virus individuati durante la scansione

Le impostazioni predefinite dell'antivirus Quick Heal sono adeguatamente configurate e sono ottimali per proteggere il vostro sistema. Se viene rilevato un virus durante la scansione, Quick Heal antivirus cerca di riparare il virus. Tuttavia, se non riesce a riparare i file infetti, tali file vengono messi in Quarantena. Nel caso in cui siano state personalizzate le impostazioni predefinite di scanner, intraprendere un'azione appropriata quando viene rilevato un virus.

Opzioni Scansione

Durante la scansione, è possibile intraprendere una delle seguenti azioni in base alle necessità:

Pulsante	Descrizione
Scheda Azione	Mostra l'azione da eseguire sui file.
Salta Cartella	Permette di evitare la scansione della cartella corrente. La scansione si sposta in un'altra posizione. Questa opzione è utile durante la scansione di una cartella che contiene elementi non sospetti.
Salta File	Permette di evitare la scansione del file corrente. Questa opzione è utile quando si effettua la scansione di un numero rilevante di file.
Interrompi	Permette di interrompere il processo di scansione.
Chiudi	Permette di uscire dal processo di scansione.
Spegni il PC appena finito	Permette di spegnere il sistema dopo aver terminato la scansione. Questa funzione funzionerà solo quando la scansione è completa.

Pulire virus rilevati in memoria

"Virus Attivi in memoria" significa che un virus è attivo, si sta diffondendo ad altri file o computer (se collegato a una rete) e può fare attività dannosa.

Ogni volta che un virus viene rilevato durante la scansione della memoria, una Scansione nella Fase di Avvio è automaticamente programmato per l'esecuzione la prossima volta che si avvia il sistema. Scansione nella Fase di Avvio esegue la scansione e la pulizia di tutte le unità, comprese le partizioni NTFS, prima che il desktop sia completamente caricato. Rileverà e pulirà anche i più tipici Rootkit, spyware, Trojan speciali e logger.

Riavvio richiesto durante la pulizia a causa di malware

Alcuni malware cadere e iniettare le loro librerie di collegamento dinamico nei processi in esecuzione del sistema come explorer.exe, Iexplore.exe, svchost.exe, ecc. che non possono essere disabilitati o puliti. Durante la scansione della memoria quando vengono rilevati, saranno impostati per la cancellazione nel prossimo avvio automaticamente. Quick Heal antivirus scansione della memoria fornirà dettagli o raccomandazioni di azione per voi in tali casi.

Pulizia del Boot/Partizioni dai virus

Se Quick Heal antivirus scanner di memoria rileva un virus di avvio o partizione nel sistema, si consiglia di avviare il sistema utilizzando un disco di avvio pulito. Scansionerà e pulirà il virus utilizzando il disco di emergenza Quick Heal.

Risposta agli avvisi di virus trovati dalla Protezione Virus

Protezione antivirus di Quick Heal antivirus analizza continuamente il sistema alla ricerca di virus in background mentre si lavora. Per impostazione predefinita, Virus Protection ripara automaticamente i file infetti. Si otterrà anche un prompt dopo l'azione è presa da Virus Protection.

Informazioni su licenza Antivirus

La sezione Informazioni di Quick Heal antivirus include le seguenti informazioni.

- Versione Quick Heal
- Dettagli di licenza
- Validità della licenza
- Opzione Aggiorna ora

I seguenti pulsanti sono disponibili nella sezione Informazioni.

Opzione	Descrizione
Rinnova Ora	Permette di rinnovare l'abbonamento esistente.
Dettagli di Licenza	Le informazioni sulla licenza e il Contratto di licenza con l'utente finale (EULA) sono disponibili in questa sezione. **Aggiorna i dettagli della licenza**: Questa funzione è utile per sincronizzare le informazioni sulla licenza esistenti con Quick Heal Activation Server. Se si desidera rinnovare l’abbonamento esistente e non sai come rinnovarlo o affrontare il problema durante il rinnovo, è

	possibile chiamare il team di supporto Quick Heal e fornire la chiave del prodotto e il codice di rinnovo. Il team di supporto di Quick Heal rinnoverà la copia. Tuttavia, è necessario seguire questi passaggi: 1. Essere connessi a Internet. 2. Fare clic su Aggiorna dettagli della licenza. 3. Fare clic su Continua per aggiornare l'abbonamento esistente. **Dettagli di licenza di stampa**: Fare clic su Dettagli di licenza di stampa per prendere la stampa delle informazioni di abbonamento esistenti.
Aggiorna ora	Ti aiuta ad aggiornare il database dei virus di Quick Heal antivirus.

Inviare informazioni di Sistema

Informazioni di Sistema è uno strumento essenziale per raccogliere informazioni critiche di un sistema basato su Windows per i seguenti casi.

Per rilevare Malware	Questo strumento raccoglie informazioni per rilevare nuovi malware dai processi in esecuzione, Registro di sistema, file di sistema come Config.Sys, Autoexec.bat, e registro degli eventi di sistema e delle applicazioni.
Per ottenere Informazioni su Quick Heal	Raccoglie informazioni sulla versione installata di Quick Heal antivirus, le sue impostazioni di configurazione e i file in quarantena, se presenti.

Generare Informazioni di Sistema

Per generare informazioni di sistema, segui questi passaggi:

1. Aprire Quick Heal antivirus.
2. Nell'angolo in alto a destra, fare clic sull'opzione di menu e quindi selezionare l'opzione Invia informazioni di sistema.

Si apre la procedura System Information guidata.

3. Fare clic su Avanti per continuare.

Selezionare un motivo per inviare le informazioni di sistema. Se si sospetta un nuovo malware nel sistema, selezionare Sospetto che il mio sistema sia stato infettato da nuovi malware o se si verificano problemi durante l'utilizzo di Quick Heal antivirus, selezionare Sto avendo problemi durante l'utilizzo di Quick Heal.

4. Inserisci i commenti nella casella di testo Commenti e inserisci anche il tuo indirizzo email.

5. Fare clic su Fine.

Le informazioni di sistema (INFO.QHC) saranno generate e inviate al supporto tecnico Quick Heal.

Questo strumento genera un file INFO.QHC in C: e lo invia automaticamente a sysinfo@quickheal.com.

⚠ Nota:

Il file INFO.QHC contiene i dettagli critici del sistema e i dettagli della versione di Quick Heal antivirus installato sul sistema nel formato testo e binario. L'informazione contiene l'esecuzione automatica di file (attraverso Registro, Autoexec.bat, System.ini e Win.ini) e processi in esecuzione con i loro dettagli libreria supportati. Questi dettagli vengono utilizzati per analizzare il sistema per il nuovo malware e il corretto funzionamento di Quick Heal antivirus. Queste informazioni sono utilizzate per fornire servizi migliori e adeguati ai clienti.

Si prega di notare che questo strumento non raccoglie altre informazioni di identificazione personale come password, né condividiamo o divulghiamo queste informazioni con chiunque. Rispettiamo la tua privacy.

Report

Quick Heal antivirus crea e mantiene un rapporto dettagliato di tutte le attività importanti come la scansione dei virus, aggiorna i dettagli, modifiche nelle impostazioni delle caratteristiche, e così via.

Visualizzare i Report

Per visualizzare report e statistiche di diverse caratteristiche, seguire questi passaggi:

1. Aprire **Quick Heal antivirus**.
2. Nel pannello a sinistra, fare clic su Stato. Nell'angolo in alto a destra, fare clic sull'opzione menu e quindi selezionare l'opzione Rapporti.

   Una lista dei report appare.
3. Nella lista **Report di** cliccare una funzione per vedere il suo report.

   L'elenco dei dettagli del rapporto appare nel riquadro di destra. Le statistiche del rapporto su ogni caratteristica includono la data e l'ora quando il rapporto è stato generato ed il motivo per cui il rapporto è stato generato.

Pulsante	Azione
Dettagli	Consente di visualizzare un rapporto dettagliato del record selezionato nell'elenco.
Cancella Tutto	Aiuta a eliminare tutti i record nella lista.
Cancella	Aiuta a eliminare il record selezionato nell'elenco.
Chiudi	Ti aiuta a chiudere la schermata Report.

È possibile visualizzare ulteriori dettagli di una segnalazione di una funzionalità. Nel pannello di destra, fare clic sul rapporto per visualizzare i dettagli. Viene visualizzata la schermata dei dettagli del report che include le seguenti opzioni.

Pulsante	Azione
Anteprima	Consente di visualizzare il rapporto dettagliato del record precedente nell'elenco. Questo pulsante non è disponibile se il record selezionato è il primo record nell'elenco.
Avanti	Consente di visualizzare il rapporto dettagliato del record successivo nella lista. Questo pulsante non è disponibile se il record selezionato è l'ultimo record nell'elenco.
Stampa	Ti aiuta a prendere la stampa del rapporto dettagliato.
Salva come	Ti aiuta a salvare il rapporto dettagliato in . txt in una posizione del tuo sistema.
Chiudi	Ti aiuta ad uscire dalla schermata dei dettagli del rapporto.

Disinstallare il software antivirus

Rimozione antivirus Quick Heal può esporre il sistema a minacce di virus. Tuttavia, è possibile disinstallare antivirus Quick Heal nel modo seguente:

1. Selezionare **Start > Programmi > Quick Heal antivirus# > Disinstalla Quick Heal antivirus.**
   - **Rimuovere Quick Heal e mantenere le definizioni di aggiornamento file**: se si seleziona questa opzione, Quick Heal salverà le informazioni di licenza, tutte le definizioni di aggiornamento scaricate, rapporti, file in quarantena, anti-spam whitelist/ blacklist in un repository sul computer, in modo che questi possano essere utilizzati durante la reinstallazione.
   - **Rimuovere Quick Heal completamente** - Se si seleziona questa opzione, Quick Heal sarà completamente rimosso dal computer.
2. Selezionare una delle opzioni e fare clic su **Avanti** per continuare con la disinstallazione.

Se si dispone di antivirus protetto da password Quick Heal, viene visualizzata una schermata di autenticazione.

3. Inserire la password e fare clic su **OK.**

Il processo di disinstallazione viene avviato.

Quando la disinstallazione è completa, appare un messaggio.

È possibile fornire feedback e motivi per disinstallare antivirus Quick Heal facendo clic su Scrivi a noi il motivo di disinstallazione di Quick Heal antivirus. Il tuo feedback è prezioso per noi e ci aiuta a migliorare la qualità del prodotto.

Nota:

Annotare la chiave del prodotto per riferimento futuro. È possibile salvare le informazioni chiave del prodotto facendo clic su **Salva** su file. Riavviare il computer è consigliato dopo la disinstallazione antivirus Quick Heal. Per riavviare fare clic su **Riavvia ora**, o fare clic su **Riavvia più tardi** per continuare a lavorare sul sistema e riavviare dopo qualche tempo.

10. Report

Quick Heal fornisce un ampio supporto tecnico per gli utenti registrati. Si consiglia di avere tutti i dettagli necessari con voi durante l'e-mail o la chiamata per ricevere supporto efficiente dai dirigenti di supporto Quick Heal.

Supporto Tecnico

L'opzione Supporto include FAQ (Frequently Asked Questions) dove puoi trovare le risposte alle domande più frequenti, inviare le tue domande, inviare e-mail sulle tue domande o chiamarci direttamente.

Per vedere le opzioni di supporto, segui questi passaggi:

1. Aprire **Quick Heal antivirus.**
2. Nel pannello a sinistra, fare clic su **Stato**.
3. Nell'angolo in alto a destra, fare clic sull'opzione **Menu** e quindi selezionare l'opzione **Supporto**.

Il supporto include le seguenti opzioni.

Supporto Web : Include Visita FAQ (Domande frequenti) e Visita Forum - dove è possibile inviare le domande degli utenti per ottenere una risposta appropriata.

Supporto Email : Include Submit Ticket che ti reindirizza alla nostra pagina web di supporto. Qui è possibile leggere alcuni dei problemi più comuni con le risposte. Se non si trova una risposta al problema, puoi inviare un ticket.

Supporto Live Chat : Utilizzando questa opzione, è possibile chattare con i nostri dirigenti di supporto.

Supporto telefonico: Include numeri di telefono. È possibile chiamare il nostro team di supporto e ottenere i problemi risolti.

Supporto remoto: Questo modulo di supporto ci aiuta a connetterci facilmente al sistema del computer da remoto e aiutare a risolvere i problemi tecnici.

Altre fonti di Supporto

Per ottenere un'ulteriore fonte di supporto, visitare www.quickheal.com/support-center-faqs.

11. Indice compatibilità

La seguente tabella descrive la compatibilità delle funzionalità.

Opzione	Versione Prodotto
Anti-Tracker	Disponibile per Quick Heal Total Security
Protezione Perdita di Dati	Disponibile per Quick Heal Total Security
File Vault	Disponibile per Quick Heal Total Security
Game Booster	Disponibile per Quick Heal Total Security
Mobile Scan (PC2Mobile)	Disponibile per Quick Heal Total Security
Parental Control	Disponibile per Quick Heal Total Security e Quick Heal Internet Security.
PCTuner	Disponibile per Quick Heal Total Security
Protezione Phishing	Non disponibile per Quick Heal AntiVirus Pro
Safe Banking	Non disponibile per Quick Heal AntiVirus Pro
Protezione Spam	Non disponibile per Quick Heal AntiVirus Pro
Virtual Keyboard	Non disponibile per Quick Heal AntiVirus Pro
Scansione Vulnerabilità	Non disponibile per Quick Heal AntiVirus Pro
Protezione Webcam	Disponibile per Quick Heal Total Security
Wi-Fi Scanner	Non disponibile per Quick Heal AntiVirus Pro