Bitdefender®
INTERNET SECURITY

Manuale

Bitdefender Internet Security
Manuale

Data di pubblicazione 20/08/2013

Avvertenze legali


Bitdefender

Indice

Installazione

1. Prepararsi all'installazione

Prima di installare Bitdefender Internet Security, completa questi passaggi preliminari per assicurarti che l'installazione funzioni senza problemi:

- Assicurati che il computer su cui desideri installare Bitdefender soddisfi i requisiti minimi di sistema.Se il computer non soddisfa i requisiti minimi di sistema, Bitdefender non sarà installato, o se installato, non funzionerà correttamente e potrà causare rallentamenti e instabilità del sistema.Per un elenco completo dei requisiti di sistema, consultare la sezione «*Requisiti di sistema*» (p. 3).
- Accedere al computer utilizzando un account Amministratore.
- Rimuovi qualsiasi altro programma simile dal computer.L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema.Durante l'installazione Windows Defender sarà disattivato.
- Disabilita o rimuovi qualsiasi programma firewall che possa essere in esecuzione sul computer.L'esecuzione simultanea di due programmi firewall può influenzarne il funzionamento e causare problemi seri al sistema.Durante l'installazione il firewall di Windows sarà disattivato.
- Assicurati che il computer sia connesso a Internet durante l'installazione, anche se l'hai avviata da un CD/DVD.Se sono disponibili versioni più recenti dei file dell'applicazione inclusi nel pacchetto d'installazione, Bitdefender può scaricarli e installarli.

2. Requisiti di sistema

Puoi installare Bitdefender Internet Security solo su computer con i seguenti sistemi operativi:

- Windows XP con Service Pack 3 (32 bit)
- Windows Vista con Service Pack 2
- Windows 7 con Service Pack 1
- Windows 8

Prima dell'installazione, assicurati che il computer soddisfi i requisiti minimi di sistema.

Nota

Per scoprire quale versione di Windows è attiva sul computer e maggiori informazioni sull'hardware, segui questi passaggi:

- In **Windows XP**, **Windows Vista** e **Windows 7**, clicca con il pulsante destro su **Computer** nel desktop e seleziona **Proprietà** nel menu.
- In **Windows 8**: dal menu Start di Windows, localizza l'opzione Computer (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona con il pulsante destro. Seleziona Proprietà nel menu inferiore. Controlla in Sistema per verificare il tipo di sistema.

2.1. Requisiti minimi di sistema

- 1 GB di spazio disponibile su disco rigido (almeno 800 MB sull'unità di sistema)
- Processore da 1.6 GHz
- 1 GB di memoria (RAM) per Windows XP, Windows Vista, Windows 7 e Windows 8

2.2. Requisiti di sistema consigliati

- 2 GB di spazio disponibile su disco rigido (almeno 800 MB sull'unità di sistema)
- Intel CORE Duo (2 GHz) o processore equivalente
- Memoria (RAM):
  - 1 GB per Windows XP
  - 1,5 GB per Windows Vista, Windows 7 e Windows 8

2.3. Requisiti software

Per poter usare Bitdefender e tutte le sue funzioni, il computer deve soddisfare i seguenti requisiti software:

- Internet Explorer 8 o superiore
- Mozilla Firefox 3.6 o superiore

- Chrome 20 o superiore
- Yahoo! Messenger 9 o superiore
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express e Windows Mail (su sistemi a 32 bit)
- Mozilla Thunderbird 3.0.4
- .NET Framework 3.5 (se assente, viene installato automaticamente con Bitdefender)

3. Installare il tuo prodotto Bitdefender

Puoi installare Bitdefender dal disco di installazione di Bitdefender oppure utilizzando un programma di installazione web scaricato sul computer dal sito di Bitdefender o da altri siti web autorizzati (ad esempio il sito web di un partner di Bitdefender o un negozio online).Il file di installazione può essere scaricato dal sito web di Bitdefender al seguente indirizzo: http://www.bitdefender.it/Downloads/.

Se il tuo acquisto vale per più di un computer (per esempio hai acquistato Bitdefender Internet Security per 3 PC), ripeti il processo d'installazione e registra il prodotto con il codice di licenza su ogni computer.

- Per installare Bitdefender dal disco di installazione, inserisci il disco nel lettore.Dopo alcuni istanti verrà visualizzata una finestra di benvenuto. Segui le indicazioni per avviare l'installazione.

  Nota

  La schermata di benvenuto fornisce un'opzione per copiare il pacchetto d'installazione dal disco a un dispositivo USB.Ciò è utile se devi installare Bitdefender su un computer che non ha un'unità disco (per esempio, su un netbook).Inserisci il dispositivo USB nella porta USB e clicca su **Copia su USB**.In seguito, spostati sul computer senza unità CD, inserisci il dispositivo USB nella porta USB e clicca due volte su `runsetup.exe` dalla cartella nella quale hai salvato il pacchetto di installazione.

  Se la schermata di benvenuto non compare, utilizza Esplora risorse per sfogliare la cartella principale del disco e clicca due volte sul file `autorun.exe`.

- Per installare Bitdefender utilizzando il programma di installazione web scaricato sul computer, individua il file e cliccaci sopra due volte.

Convalidare l'installazione

Per prima cosa, Bitdefender controllerà il sistema per convalidare l'installazione.

Se il tuo sistema non soddisfa i requisiti minimi per installare Bitdefender, sarai informato delle aree da migliorare prima di poter procedere.

Se viene rilevato un programma antivirus incompatibile o una versione precedente di Bitdefender, ti sarà chiesto di rimuoverla dal sistema.Segui le istruzioni per rimuovere il programma dal sistema, per evitare eventuali problemi in seguito.Potrebbe essere necessario riavviare il computer per completare la rimozione dei programmi antivirus rilevati.

Il pacchetto d'installazione di Bitdefender Internet Security è aggiornato costantemente. Se stai eseguendo l'installazione da un CD/DVD, Bitdefender può scaricare le versioni più aggiornate dei file durante l'installazione. Quando ti viene

richiesto, clicca su **Sì**, per consentire a Bitdefender di scaricare i file, assicurandoti così di installare la versione più aggiornata del software.

Nota
Scaricare i file d'installazione può richiedere un po' di tempo, soprattutto con le connessioni a Internet più lente.

Una volta convalidata l'installazione, comparirà la procedura guidata della configurazione. Segui tutti i passaggi per installare Bitdefender Internet Security.

Fase 1 - Benvenuto

La schermata di benvenuto ti consente di scegliere il tipo di installazione che desideri eseguire.

Per un'installazione senza problemi, basta cliccare sul pulsante **Installa**. Bitdefender sarà installato nel percorso predefinito con le impostazioni standard, passando direttamente alla Fase 3 della procedura guidata.

Se desideri configurare le impostazioni dell'installazione, seleziona **Voglio personalizzare la mia installazione** e poi clicca su **Installa** per passare alla prossima fase.

Durante questa fase possono essere eseguite due attività aggiuntive:

- Prima di procedere con l'installazione, leggi l'Accordo di licenza con l'utente finale. L'Accordo di licenza contiene i termini e le condizioni per poter utilizzare Bitdefender Internet Security.

  Se non accetti questi termini, chiudi la finestra. Il processo di installazione sarà abbandonato e uscirai dalla configurazione.

- Attivare l'invio di **rapporti anonimi sull'utilizzo**. Abilitando questa opzione, i rapporti contenenti informazioni su come il prodotto viene utilizzato sono inviati ai server Bitdefender. Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a offrire una migliore esperienza in futuro. I rapporti non conterranno dati confidenziali, come nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.

Fase 2 - Personalizzare le impostazioni dell'installazione

Nota
Questa fase appare solo se hai selezionato di personalizzare l'installazione durante la fase precedente.

Sono disponibili le seguenti opzioni:

Percorso di installazione

Di norma, Bitdefender Internet Security sarà installato in `C:\Programmi\Bitdefender\Bitdefender Internet Security`.Se desideri modificare il percorso di installazione, clicca su **Modifica** e seleziona la cartella dove vuoi installare Bitdefender.

Configura le impostazioni proxy

Bitdefender Internet Security richiede l'accesso a Internet per la registrazione del prodotto, il download di aggiornamenti per la sicurezza e il prodotto, la rilevazione in-the-cloud di componenti, ecc.Se usi una connessione proxy invece di una connessione a Internet diretta, devi selezionare questa opzione e configurare le impostazioni del proxy.

Le impostazioni possono essere importate dal browser predefinito o inserite manualmente.

Clicca su **Installa con impostazioni personalizzate** per confermare le tue preferenze e iniziare l'installazione. Se cambiassi idea, clicca sul pulsante **Non importa, usa le impostazioni standard** corrispondente.

Fase 3 - Installazione in corso

Attendi il completamento dell'installazione.Nel frattempo vengono mostrate alcune informazioni dettagliate sui progressi.

Una scansione controlla le aree critiche del sistema alla ricerca di virus, vengono scaricate ed eventualmente installate le ultime versioni dei file dell'applicazione e i servizi di Bitdefender vengono avviati.Questa fase può richiedere alcuni minuti.

Fase 4 - Fine dell'installazione

Viene mostrato un resoconto dell'installazione. Se durante l'installazione viene rilevato e rimosso qualche malware attivo, è necessario riavviare il sistema.

Puoi chiudere la finestra o passare alla configurazione iniziale del programma, cliccando su **Inizia**.

Fase 5 - Registrare il prodotto

Nota

Questa fase appare solo se hai selezionato l'opzione Inizia durante la fase precedente.

Per completare la registrazione del prodotto devi inserire un codice di licenza.È richiesta una connessione a Internet attiva.

Procedi secondo la tua situazione:

- **Ho acquistato il prodotto**

In questo caso, registra il prodotto seguendo questi passaggi:

1. Seleziona **Ho acquistato Bitdefender e voglio registrarlo subito**.
2. Digita il codice di licenza nel campo corrispondente.

Nota

Puoi trovare il tuo codice di licenza:

- Sull'etichetta del CD/DVD.
- Sulla scheda di registrazione del prodotto.
- Nella e-mail di acquisto online.

3. Clicca su **Registra ora**.

- **Non ho un codice, voglio provare gratuitamente il prodotto.**

  In questo caso, puoi usare il prodotto per un periodo di 30 giorni.Per avviare il periodo di prova, seleziona l'opzione **Non ho un codice, voglio provare gratuitamente il prodotto.**

- Clicca su **Avanti**.

Fase 6 - Configurare il comportamento del prodotto

Bitdefender può essere configurato per gestire automaticamente la tua sicurezza in modo permanente o in determinate situazioni. Usa gli interruttori per attivare o disattivare l'**Autopilot** e la **Modalità giochi automatica**.

Attiva l'Autopilot per una sicurezza silenziosa e totale. Quando l'Autopilot è attivo, Bitdefender prende tutte le decisioni in fatto di sicurezza per te e non dovrai configurare alcuna impostazione. Per ulteriori informazioni, fare riferimento a «*Autopilot*» (p. 15).

Se utilizzi spesso i videogiochi, attiva la Modalità giochi automatica e Bitdefender rileverà l'esecuzione di un gioco, entrando in Modalità giochi e modificando le sue impostazioni in modo da ridurre al minimo il suo impatto sulle prestazioni del sistema. Per ulteriori informazioni, fare riferimento a «*Modalità giochi*» (p. 16).

Clicca su **Avanti**.

Fase 7 - Accedere a MyBitdefender

Per utilizzare le funzioni online del prodotto, occorre un account MyBitdefender. Per ulteriori informazioni, fare riferimento a «*Account MyBitdefender*» (p. 35).

Procedi in base alla tua situazione.

Voglio creare un account MyBitdefender

Per creare con successo un account di MyBitdefender, segui questi passaggi:

1. Seleziona **Crea un nuovo account**.

Comparirà una nuova finestra.

2. Digita le informazioni richieste nei campi corrispondenti.I dati forniti resteranno riservati.
   - **E-mail** - Inserisci il tuo indirizzo e-mail.
   - **Nome utente** - Inserisci un nome utente per il tuo account.
   - **Password** - Inserisci una password per il tuo account. La password deve avere almeno 6 caratteri.
   - **Conferma password** - Ridigita la password.

   Nota
   Una volta che l'account è stato creato, puoi utilizzare l'indirizzo e-mail e la password forniti per accedere all'account all'indirizzo https://my.bitdefender.com.

3. Clicca su **Crea**.
4. Prima di poter usare il tuo account, devi completare la registrazione.Controlla la tua posta elettronica e segui le istruzioni nell'e-mail di conferma inviata da Bitdefender.

Voglio accedere usando il mio account Microsoft, Facebook o Google

Per accedere con il tuo account Microsoft, Facebook o Google, segui questi passaggi:

1. Seleziona il servizio che vuoi utilizzare.Sarai reindirizzato alla pagina di accesso del servizio.
2. Segui le istruzioni fornite dal servizio selezionato per collegare il tuo account a Bitdefender.

Nota
Bitdefender non accede ad alcuna informazione confidenziale, come la password dell'account con cui accedi o le informazioni personali dei tuoi amici e contatti.

Ho già un account MyBitdefender

Se in precedenza ti sei connesso a un account dal tuo prodotto, Bitdefender lo rileverà, chiedendoti di inserire la password per accedere a quell'account.

Se hai già un account attivo, ma Bitdefender non lo rileva, o semplicemente vuoi accedere a un altro account, inserisci l'indirizzo e-mail e la password e clicca su **Accedi a MyBitdefender**.

Posticipa

Se vuoi eseguire questa attività in un altro momento, clicca su **Chiedimelo più tardi**. Ricordati che per utilizzare le funzioni online del prodotto devi accedere a un account.

Iniziare

4. Le basi

Una volta installato Bitdefender Internet Security, il tuo computer sarà protetto da ogni tipo di malware (come virus, spyware e Trojan) e minaccia web (come hacker, phishing e spam).

Puoi attivare l'Autopilot per usufruire di una sicurezza assolutamente silenziosa, che non richiede alcuna impostazione da configurare. Tuttavia, potresti volere sfruttare le impostazioni di Bitdefender per ottimizzare e migliorare la tua protezione.

Bitdefender prenderà la maggior parte delle decisioni in materia di sicurezza per conto tuo, mostrandoti raramente delle finestre pop-up di avviso. Nella finestra Eventi sono disponibili maggiori dettagli sulle azioni intraprese e sulle operazioni dei programmi. Per ulteriori informazioni, fare riferimento a «*Eventi*» (p. 14).

Di tanto in tanto, dovresti aprire Bitdefender e risolvere i problemi esistenti. Devi configurare le componenti di Bitdefender o prendere azioni preventive per proteggere i tuoi computer e i tuoi dati.

Se non hai registrato il prodotto, ricordati di farlo prima che il periodo di prova finisca. Per ulteriori informazioni, fare riferimento a «*Registrare Bitdefender*» (p. 33).

Per utilizzare le funzioni online di Bitdefender Internet Security, assicurati di collegare il tuo computer a un account di MyBitdefender. Per ulteriori informazioni, fare riferimento a «*Account MyBitdefender*» (p. 35).

Nella sezione «Come fare» (p. 42) troverai una serie di istruzioni passo passo per eseguire le attività più comuni. Se dovessi riscontrare problemi nell'utilizzare Bitdefender, controlla la sezione «*Risolvere i problemi più comuni*» (p. 150) per alcune possibili soluzioni ai problemi più comuni.

4.1. Aprire la finestra di Bitdefender

Per accedere all'interfaccia principale di Bitdefender Internet Security, segui questi passaggi:

- Per **Windows XP**, **Windows Vista** e **Windows 7**:
  1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
  2. Clicca su **Bitdefender**.
  3. Clicca su **Bitdefender Internet Security** o più rapidamente, clicca due volte sull'icona di Bitdefender nell'area di stato.
- Per **Windows 8**:

  Dal menu Start di Windows, localizza Bitdefender Internet Security (puoi anche digitare direttamente "Bitdefender" nella finestra di ricerca del menu Start) e poi

clicca sulla sua icona. In alternativa, apri l'applicazione sul desktop e poi clicca due volte sull'icona di Bitdefender nell'area di stato.

Per maggiori informazioni sulla finestra di Bitdefender e l'icona nell'area di stato, fai riferimento a «*Interfaccia di Bitdefender*» (p. 21).

4.2. Risolvere i problemi

Bitdefender utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni relative ai problemi che potrebbero avere effetto sulla sicurezza del computer e dei dati. Di norma, il sistema controlla solo una serie di problemi considerati molto importanti. Tuttavia è possibile configurare il sistema in base alle proprie necessità, scegliendo di quali problemi specifici si desidera essere avvisati.

I problemi rilevati includono importanti impostazioni di protezione che sono disattivate e altre condizioni che possono rappresentare un rischio per la sicurezza. Sono suddivisi in due categorie:

- **Problemi critici** - Impediscono a Bitdefender di proteggerti dai malware o rappresentano un grosso rischio alla sicurezza.
- **Problemi minori (non critici)** - Possono influenzare la tua protezione nel prossimo futuro.

L'icona di Bitdefender nell'area di stato indica problemi in sospeso cambiando il suo colore come segue:

Rosso: Alcuni problemi critici influenzano la sicurezza del tuo sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

Giallo: Alcuni problemi non critici influenzano la sicurezza del tuo sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli.

Inoltre muovendo il cursore sull'icona, una finestra pop-up confermerà l'esistenza di problemi in sospeso.

Quando apri la finestra di Bitdefender, l'area Stato di sicurezza sulla barra degli strumenti superiore indicherà il numero e la natura dei problemi che influenzano il sistema.

4.2.1. Procedura guidata Risolvi ogni problema

Per risolvere i problemi rilevati segui la procedura guidata **Risolvi ogni problema**.

1. Per aprire la procedura guidata, fai una delle seguenti operazioni:
   - Clicca con il pulsante destro sull'icona di Bitdefender nell'area di stato e seleziona **Visualizza i problemi di sicurezza**.In base ai problemi rilevati, l'icona è rossa (a indicare problemi critici) o gialla (a indicare problemi non critici).

- Apri la finestra di Bitdefender e clicca in qualsiasi punto nell'area Stato di sicurezza sulla barra degli strumenti superiore (per esempio, puoi cliccare sul pulsante **Risolvi ogni problema**).

2. Puoi visualizzare i problemi che influenzano la sicurezza del computer e dei dati.Tutti i problemi attuali sono stati selezionati per essere risolti.

   Se non desideri risolvere subito un particolare problema, deseleziona la casella corrispondente.Ti sarà chiesto di indicare per quanto tempo posticipare la risoluzione del problema.Scegli l'opzione che desideri nel menu e clicca su **OK**.Per non monitorare più la rispettiva categoria di problemi, seleziona **Permanentemente**.

   Lo stato del problema diventerà **Posticipa** e non sarà intrapresa alcuna azione per risolverlo.

3. Per risolvere i problemi selezionati, clicca su **Avvia**. Alcuni problemi vengono risolti immediatamente. Per altri problemi verrà eseguito un assistente per poterli risolvere.

I problemi che la procedura guidata permette di risolvere possono essere raggruppati nelle seguenti categorie principali:

- **Impostazioni di sicurezza disabilitate.** Tali problemi vengono risolti immediatamente abilitando le rispettive impostazioni di sicurezza.
- **Attività di sicurezza preventiva che devi eseguire.** Nel risolvere tali problemi, una procedura guidata permette di completare con successo l'attività.

4.2.2. Configurare gli avvisi di stato

Bitdefender ti avvisa in caso venissero rilevati problemi durante l'esecuzione delle seguenti funzioni:

- Firewall
- Antispam
- Antivirus
- Aggiornamento
- Sicurezza browser

Puoi configurare il sistema di avvisi per rispondere al meglio alle tue esigenze di sicurezza, selezionando di quali problemi specifici desideri essere informato. Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Avanzate**.

5. Clicca sul link **Configura avvisi di stato**.
6. Clicca sugli interruttori per attivare o disattivare gli avvisi di stato in base alle tue preferenze.

4.3. Eventi

Bitdefender conserva un registro dettagliato di eventi riguardanti la sua attività sul computer. Ogni volta che si verifica un evento rilevante per la sicurezza del sistema o dei dati, viene aggiunto un nuovo messaggio negli eventi di Bitdefender, in modo simile a quando ricevi un nuovo messaggio nella casella di posta.

Gli Eventi sono uno strumento molto importante per monitorare e gestire la protezione di Bitdefender.Per esempio, puoi controllare facilmente se l'aggiornamento è stato eseguito con successo, se sono stati rilevati malware sul tuo computer, ecc.In aggiunta, se necessario, puoi intraprendere ulteriori azioni o modificare le azioni intraprese da Bitdefender.

Per accedere al registro degli Eventi, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca su **Eventi** nella barra degli strumenti superiore per aprire la finestra **Panoramica eventi**.

I messaggi sono raggruppati in base alle diverse attività dei vari moduli di Bitdefender:

- **Antivirus**
- **Firewall**
- **Aggiornamento**
- **Controllo privacy**
- **Antispam**
- **Safego**

Gli **indicatori degli eventi** sono mostrati nell'interfaccia di Bitdefender per consentire una semplice identificazione delle aree con eventi rilevanti. Si tratta di icone che appaiono su specifici moduli che indicano il numero di eventi critici non analizzati, relativi alle attività di un modulo.

Per esempio, se ci fosse un evento critico non analizzato relativo alle attività del modulo Aggiornamento, nel pannello Aggiornamento compare l'icona  .

Sul pulsante Eventi nella finestra principale compare un indicatore che mostra il numero totale di messaggi non letti da tutti i moduli.

È disponibile un elenco di eventi per ogni categoria.Per avere maggiori informazioni su un particolare evento nell'elenco, cliccaci sopra. I dettagli degli eventi sono indicati nella parte inferiore della finestra.Ogni evento è fornito delle seguenti informazioni: una breve descrizione, l'azione intrapresa da Bitdefender quando si

è verificato e la data e l'ora in cui è avvenuto.Se necessario, possono essere fornite opzioni per intraprendere ulteriori azioni.

Puoi filtrare gli eventi per la loro importanza e nell'ordine in cui sono accaduti.Ci sono tre tipi di eventi filtrati dalla loro importanza, ognuno indicato da un'icona specifica:

Gli eventi **informazione** indicano operazioni avvenute con successo.

Gli **avvisi** indicano problemi non critici. Quando hai un po' di tempo, dovresti controllarli e risolverli.

Gli eventi **critici** indicato problemi importanti. Dovresti controllarli subito.

Per visualizzare gli eventi che si sono verificati in un determinato intervallo, seleziona il periodo desiderato dal campo corrispondente.

Per aiutarti a gestire facilmente gli eventi registrati, ogni sezione della finestra Eventi fornisce opzioni per eliminare o segnare come letti tutti gli eventi in quella sezione.

4.4. Autopilot

Per tutti gli utenti che vogliono essere protetti dalla propria soluzione di sicurezza senza tanti problemi, Bitdefender Internet Security include una modalità Autopilot.

Con l'Autopilot attivo, Bitdefender applica una configurazione di sicurezza ottimale e prende tutte le relative decisioni per te.Questo significa che non vedrai né finestre di pop-up né avvisi e non dovrai configurare alcuna impostazione.

In modalità Autopilot, Bitdefender risolve automaticamente i problemi critici, oltre ad attivare e gestire in modo silenzioso:

- Protezione antivirus, fornita da scansioni all'accesso e continue.
- Protezione firewall.
- Protezione della privacy, fornita dal filtro antiphishing e antimalware per la tua navigazione web.
- Aggiornamenti automatici.

Per attivare o disattivare l'Autopilot, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sull'interruttore **Mod. utente** / **Autopilot** nella barra degli strumenti superiore. Quando l'interruttore si trova in posizione Mod. utente, l'Autopilot è disattivato.

Finché l'Autopilot è attivo, l'icona di Bitdefender nell'area di stato cambia in .

Importante
Se si modifica un'impostazione gestita dall'Autopilot mentre è attivo, sarà disattivato automaticamente.

Per vedere una cronologia delle azioni eseguite da Bitdefender mentre l'Autopilot era attivo, apri la finestra Eventi.

4.5. Modalità giochi e Modalità portatile

Alcune attività del computer, ad esempio giochi o presentazioni, richiedono una maggiore risposta e performance dal sistema e nessuna interruzione.Quando il laptop funziona a batterie, si consiglia che operazioni superflue, che consumano energia aggiuntiva, siano rimandate fino a quando il laptop è connesso all'alimentazione C/A.

Per adattarsi a queste situazioni particolari, Bitdefender Internet Security include due modalità operative speciali:

- Modalità giochi
- Modalità portatile

4.5.1. Modalità giochi

La modalità giochi modifica temporaneamente le impostazioni di protezione in modo di minimizzare l'impatto sulle prestazioni del sistema.Le seguenti impostazioni sono applicate quando la Modalità giochi è attiva:

- Tutti gli allarmi e pop-up Bitdefender sono disabilitati.
- La Scansione all'accesso è impostata sul livello di protezione **Tollerante**.
- Scansione automatica disattivata.La Scansione automatica trova e utilizza gli intervalli di tempo in cui l'uso delle risorse di sistema scende sotto a una certa soglia per eseguire scansioni ricorrenti dell'intero sistema.
- Il firewall di Bitdefender è impostato in modalità standard (La Modalità Paranoid è disattivata).Questo significa che tutte le nuove connessioni (sia in entrata che in uscita) vengono consentite, indipendentemente della porta o protocollo utilizzati.
- Auto aggiornamento disattivato.
- La barra degli strumenti di Bitdefender nel tuo browser è disattivata mentre esegui giochi web.

In Modalità giochi, l'icona di Bitdefender nell'area di stato cambia in .

Utilizzare la Modalità giochi

Di norma, Bitdefender entra automaticamente in modalità giochi quando esegui un gioco incluso nell'elenco di Bitdefender dei giochi conosciuti o quando un'applicazione

passa a schermo intero.Bitdefender tornerà automaticamente alla modalità normale quando si chiude il gioco o quando l'applicazione rilevata esce dallo schermo intero.

Se si vuole attivare manualmente la Modalità giochi, utilizzare uno dei metodi seguenti:

- Clicca con il pulsante destro sull'icona di Bitdefender nell'area di stato e seleziona **Attiva Modalità giochi**.
- Attiva i tasti di scelta rapida per la Modalità giochi. Premi `Ctrl+Alt+Shift+G` (la combinazione predefinita).

Importante
Non dimenticare di disattivare la Modalità giochi quando hai finito. Per farlo, utilizzare gli stessi metodi usati per attivarla.

Attivare o disattivare la Modalità giochi automatica

Per attivare o disattivare la Modalità giochi automatica, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
5. Attiva o disattiva la Modalità giochi automatica, cliccando sull'interruttore corrispondente.

Aggiungere manualmente giochi all'Elenco dei giochi

Se lanciando una determinata applicazione o un videogioco, Bitdefender non entra automaticamente in Modalità giochi, puoi aggiungere manualmente l'applicazione nell'**Elenco dei giochi**. Una volta che un'applicazione viene aggiunta all'elenco, Bitdefender funzionerà in Modalità giochi finché l'applicazione sarà attiva.

Per visualizzare e gestire l'elenco dei giochi, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
5. Clicca sul collegamento **Elenco dei giochi**.

In fondo all'elenco sono disponibili due pulsanti:

- Clicca su **Aggiungi gioco** per aggiungere un nuovo gioco o una nuova applicazione all'elenco dei giochi.

Comparirà una nuova finestra. Cerca il file eseguibile dell'applicazione, selezionalo e clicca su **OK** per aggiungerlo all'elenco.

- **Rimuovi gioco** - Rimuovi un gioco o un'applicazione selezionata dall'elenco.

Tasti scelta rapida Modalità giochi

Per impostare e utilizzare i tasti di scelta rapida per attivare / disattivare la Modalità giochi, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
5. Assicurati che l'interruttore Tasti di scelta rapida Modalità giochi sia attivato.
6. Imposta la combinazione desiderata:
   a. La combinazione standard è `Ctrl+Alt+Shift+G`.

      Scegliere i tasti di modifica che si vogliono usare selezionando uno dei seguenti: tasto Control (`Ctrl`), tasto Maiuscola (`Shift`) o tasto Alternate (`Alt`).

   b. Nel campo editabile, inserisci la lettera corrispondente al tasto regolare che vuoi usare.

   Ad esempio, se vuoi usare la combinazione `Ctrl+Alt+D`, devi solo controllare i tasti `Ctrl` e `Alt` e digitare la `D`.

> **Nota**
> Per disattivare la combinazione di tasti, disattiva l'interruttore **Tasti di scelta rapida Modalità giochi**.

4.5.2. Modalità portatile

La Modalità portatile è stata sviluppata appositamente per chi utilizza computer portatili. Il suo proposito è minimizzare l'impatto di Bitdefender sul consumo di energia mentre questi apparecchi funzionino con la batteria.Quando Bitdefender è in Modalità portatile, le funzioni Scansione automatica e Auto aggiornamento sono disattivate, poiché richiedono più risorse di sistema e, implicitamente, aumentano il consumo di energia.

Bitdefender rileva quando il tuo portatile sta funzionando con la batteria e automaticamente va in Modalità portatile.Nello stesso modo, Bitdefender uscirà automaticamente dalla Modalità portatile quando rileverà che il portatile non sta più lavorando con la batteria.

Per attivare o disattivare la Modalità portatile, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
5. Attiva o disattiva la Modalità portatile automatica, cliccando sull'interruttore corrispondente.

Se Bitdefender non è installato su un portatile, disattiva la Modalità portatile automatica.

4.6. Impostazioni protette da password di Bitdefender

Se non sei l'unica persona a utilizzare questo computer, ti consigliamo di proteggere le tue impostazioni di Bitdefender con una password.

Per configurare la protezione tramite password per le impostazioni di Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
5. Attiva la protezione della password cliccando sull'interruttore.
6. Inserisci la password nei due campi e poi clicca su **OK**.La password deve essere composta da almeno 8 caratteri.

Una volta impostata una password, chiunque cerchi di cambiare le impostazioni di Bitdefender dovrà prima inserirla.

Importante

Assicurati di non dimenticare la tua password o conservane una copia in un luogo sicuro.Se hai dimenticato la password, dovrai reinstallare il programma o contattare il supporto di Bitdefender.

Per rimuovere la protezione tramite password, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
5. Disattiva la protezione tramite password cliccando sull'interruttore. Digita la password e clicca su **OK**.

Nota
Per modificare la password del tuo prodotto, clicca sul link **Cambia password**.

4.7. Rapporti anonimi sull'utilizzo

Di norma, Bitdefender invia rapporti contenenti informazioni su come utilizzi il programma ai server di Bitdefender.Queste informazioni sono essenziali per migliorare il prodotto e possono aiutarci a offrire una migliore esperienza in futuro.I rapporti non conterranno dati confidenziali, come nome o indirizzo IP, e non saranno utilizzati per scopi commerciali.

Se vuoi fermare l'invio dei Rapporti anonimi sull'utilizzo, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Avanzate**.
5. Clicca sull'interruttore per disattivare i rapporti anonimi sull'utilizzo.

5. Interfaccia di Bitdefender

Bitdefender Internet Security soddisfa le necessità di persone esperte e di principianti. L'interfaccia grafica dell'utente è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.

Per visualizzare lo stato del prodotto ed eseguire le attività essenziali, l'icona di Bitdefender nell'area di stato è disponibile in qualsiasi momento.

La finestra principale ti consente di accedere a informazioni importanti sul prodotto e ai moduli del programma, consentendoti di eseguire le attività più comuni. Dalla finestra principale puoi accedere alla finestra delle impostazioni per la configurazione dettagliata e le attività di gestione avanzate, oltre alla finestra degli Eventi per un registro approfondito delle attività di Bitdefender.

Se vuoi tenere sotto controllo le informazioni più importanti sulla sicurezza e accedere rapidamente alle impostazioni principali, aggiungi il Widget sicurezza al tuo desktop.

5.1. Icona area di stato

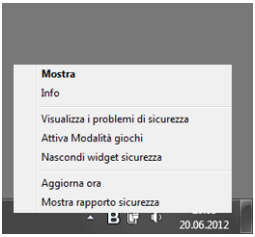
Per gestire tutto il prodotto più velocemente, puoi utilizzare l'icona di Bitdefender nell'area di stato.

Nota
Se stai utilizzando Windows Vista, Windows 7 o Windows 8, l'icona di Bitdefender potrebbe non essere sempre visibile. Per rendere l'icona sempre visibile, segui questi passaggi:

1. Clicca sulla freccia nell'angolo in basso a destra dello schermo.
2. Clicca su **Personalizza...** per aprire la finestra delle icone dell'area di Notifica.
3. Seleziona l'opzione **Mostra icone e notifiche** per l'**icona dell'agente di Bitdefender**.

Se si fa doppio clic su questa icona, Bitdefender si aprirà. Inoltre, facendo clic con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto Bitdefender.

- **Mostra** - Apre la finestra principale di Bitdefender.
- **Informazioni** - Apre una finestra nella quale puoi visualizzare informazioni su Bitdefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.
- L'opzione **Visualizza i problemi di sicurezza** ti aiuta a rimuovere le vulnerabilità attuali.Se l'opzione non è disponibile, non ci sono errori da risolvere.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Risolvere i problemi*» (p. 12).



Icona della barra delle applicazioni

- **Attiva/Disattiva modalità giochi** - attiva / disattiva la modalità giochi.
- **Nascondi / Mostra widget sicurezza** - Attiva / disattiva il widget sicurezza.
- **Aggiorna ora** - Inizia un aggiornamento immediato.Puoi seguire lo stato di aggiornamento nel pannello Aggiornamento della finestra principale di Bitdefender.
- L'opzione **Mostra rapporto sicurezza** apre una finestra dove è possibile visualizzare uno stato settimanale oltre a diversi suggerimenti per il sistema.Puoi seguire i suggerimenti per migliorare la sicurezza del sistema.

L'icona di Bitdefender nell'area di stato fornisce informazioni relative ai problemi del computer o al funzionamento del prodotto, visualizzando un simbolo speciale come segue:

Alcuni problemi critici influenzano la sicurezza del tuo sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

Alcuni problemi non critici influenzano la sicurezza del tuo sistema.Quando hai un po' di tempo, dovresti controllarli e risolverli.

Il prodotto funziona inGame Mode.

L'Autopilot di Bitdefender è attivo.

Se Bitdefender non è in funzione, l'icona nell'area di stato appare su uno sfondo grigio: .Questo si verifica normalmente quando la licenza è scaduta. Può anche verificarsi quando i servizi di Bitdefender non rispondono o quando altri errori interferiscono con il normale funzionamento di Bitdefender.

5.2. Finestra principale

La finestra principale di Bitdefender ti consente di eseguire le attività più comuni, risolvere rapidamente problemi di sicurezza, visualizzare informazioni sugli eventi relativi alle attività del prodotto e configurare le impostazioni.Tutto è a pochi clic di distanza.

La finestra è organizzata in due sezioni principali:

Barra degli strumenti superiore
: Qui puoi controllare lo stato di sicurezza del tuo computer e accedere alle attività importanti.

Area pannelli
: Qui puoi gestire i moduli principali di Bitdefender.

Il menu a tendina di MyBitdefender nella parte superiore della finestra ti consente di gestire il tuo account e accedere alle funzioni online del prodotto dalla dashboard dell'account.

Puoi trovare diversi collegamenti utili nella parte inferiore della finestra Questi collegamenti sono disponibili anche nelle finestre Eventi e Impostazioni.

Accedi	Descrizione
Numero di giorni rimasti	Il tempo rimasto prima della scadenza della licenza attuale viene indicato.Clicca sul link per aprire una finestra dove potrai visualizzare maggiori informazioni sul tuo codice di licenza o registrare il prodotto con un nuovo codice di licenza.
Aiuto e supporto	Clicca su questo link se hai bisogno di aiuto con Bitdefender. Comparirà una nuova finestra, dove potrai aprire l'aiuto del prodotto, andare al Centro di supporto o contattare il servizio clienti.
	Aggiunge dei punti di domanda in diverse aree della finestra di Bitdefender per aiutarti a trovare facilmente informazioni sui diversi elementi dell'interfaccia. Sposta il cursore su un punto interrogativo per vedere alcune veloci informazioni sull'elemento accanto.

5.2.1. Barra degli strumenti superiore

La barra degli strumenti superiore contiene i seguenti elementi:

- L'**area Stato di sicurezza** sul lato sinistro della barra degli strumenti ti informa se ci sono problemi relativi alla sicurezza del tuo computer, aiutandoti a risolverli.

  Il colore dell'area Stato sicurezza cambia in base ai problemi rilevati e ai diversi messaggi che vengono mostrati:

  - **L'area è colorata di verde.** Nessun problema da risolvere.Il computer e i dati sono protetti.
  - **L'area è colorata di giallo.** Alcuni problemi non critici influenzano la sicurezza del tuo sistema.Quando hai un po' di tempo, dovresti controllarli e risolverli.

▶ **L'area è colorata di rosso.** Alcuni problemi critici influenzano la sicurezza del tuo sistema.Devi risolvere i problemi rilevati immediatamente.

Cliccando su **Visualizza problemi** nel centro della barra degli strumenti o in qualsiasi punto nell'area di stato della sicurezza alla sua sinistra, puoi accedere a una procedura guidata che ti aiuterà a rimuovere facilmente qualsiasi minaccia dal tuo computer.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Risolvere i problemi*» (p. 12).

- Il menu **Eventi** ti consente di accedere a una cronologia dettagliata degli eventi più importanti che si sono verificati durante l'attività del prodotto.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Eventi*» (p. 14).
- **Impostazioni** ti consente di accedere a una finestra dove puoi configurare le impostazioni del prodotto.Per ulteriori informazioni, ti preghiamo di far riferimento a «*Finestra panoramica impostazioni*» (p. 27).
- L'opzione **Autopilot** / **Mod. utente** ti consente di attivare l'Autopilot per usufruire di una sicurezza completamente silenziosa. Per ulteriori informazioni, ti preghiamo di far riferimento a «*Autopilot*» (p. 15).

5.2.2. Area pannelli

Nell'area dei pannelli puoi gestire direttamente i moduli di Bitdefender.

Per scorrere tra i pannelli, usa l'interruttore scorrevole sotto alla finestra dei pannelli o le frecce localizzate a destra e sinistra.

Ogni pannello, contiene i seguenti elementi:

- Il nome del modulo e un messaggio di stato.
- Nell'angolo in alto a destra della maggior parte dei pannelli è disponibile un'icona . Cliccandoci sopra, puoi raggiungere immediatamente la finestra delle impostazioni avanzate.
- L'icona del modulo.

  Se ci sono eventi legati all'attività di un modulo che non hai ancora letto, accanto all'icona del modulo stesso sarà visualizzato un contatore di eventi. Per esempio, se ci fosse un evento non analizzato relativo alle attività del modulo Aggiornamento, nel pannello Aggiornamento comparirebbe l'icona . Clicca sul contatore per andare direttamente alla finestra degli Eventi del relativo modulo.
- Un pulsante che ti consente di eseguire funzioni importanti del modulo.
- Alcuni pannelli hanno un interruttore per consentirti di attivare o disattivare una funzione importante del modulo.

Puoi organizzare i pannelli come desideri, seguendo questi passaggi:

1. Clicca su sul lato sinistro dell'interruttore scorrevole sotto i pannelli per aprire la finestra Panoramica moduli.
2. Trascina i pannelli dei singoli moduli e rilasciali in altri slot per riorganizzare l'area in base alle tue esigenze.
3. Clicca su per tornare alla finestra principale.

I pannelli disponibili in quest'area sono:

Antivirus

La protezione antivirus è la base della tua sicurezza. Bitdefender ti protegge in tempo reale e su richiesta da ogni sorta di malware, come virus, Trojan, spyware, adware, ecc.

Dal pannello Antivirus, puoi accedere facilmente a tutte le attività di scansione importanti.Clicca su **Controlla ora** e seleziona un'attività dal menu a tendina:

- Scansione veloce
- Scansione sistema
- Gestisci scansioni
- Scansione vulnerabilità
- Modalità soccorso

L'interruttore **Scansione automatica** ti consente di attivare o disattivare questa funzione.

Per maggiori informazioni sulle attività di scansione e su come configurare la protezione antivirus, fai riferimento a «*Protezione antivirus*» (p. 74).

Antispam

Il modulo antispam di Bitdefender protegge la tua casella di posta da messaggi indesiderati filtrando tutto il traffico mail POP3.

Di norma la protezione antispam è attivata.

Puoi cliccare su **Gestisci** nel pannello antispam e seleziona Amici o Spammer nel menu a tendina per modificare l'elenco corrispondente.

Per maggiori informazioni sulla configurazione della protezione antispam, fai riferimento a «*Antispam*» (p. 99).

Privacy

Il modulo Controllo privacy ti aiuta a mantenere privati i tuoi dati personali.Ti protegge mentre sei online da attacchi di phishing, tentativi di frode, sottrazione di dati personali e molto altro.

L'interruttore antiphishing ti consente di attivare o disattivare la protezione antiphishing.

Per maggiori informazioni su come configurare Bitdefender per proteggere la tua privacy, fai riferimento a «*Controllo privacy*» (p. 107).

Firewall

Il firewall ti protegge mentre sei connesso alle reti e a Internet filtrando tutti i tentativi di connessione.

Cliccando su **Gestisci adattatori** nel pannello firewall, puoi configurare le impostazioni di connessione generali per gli adattatori di rete.

L'interruttore Firewall ti consente di attivare o disattivare la protezione del firewall.

Avvertimento

Poiché espone il computer a connessioni non autorizzate, la disattivazione del firewall dovrebbe essere solo una misura temporanea.Riattiva il firewall il prima possibile.

Per maggiori informazioni sulla configurazione del firewall, fai riferimento a «*Firewall*» (p. 115).

Aggiornamento

In un mondo dove i criminali informatici cercano costantemente di trovare nuovi modi per colpire, è essenziale tenere aggiornata la tua soluzione di sicurezza per essere sempre un passo avanti a loro.

Di norma, Bitdefender controlla ogni ora la presenza di eventuali aggiornamenti. Se desideri disattivare gli aggiornamenti automatici, usa l'interruttore **Auto aggiornamento** nel pannello Aggiorna.

Avvertimento

È una questione di sicurezza piuttosto importante. Si consiglia di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se Bitdefender non verrà aggiornato regolarmente non sarà in grado di proteggerti dalle minacce più recenti.

Clicca sul pulsante **Aggiorna ora** sul pannello per eseguire un aggiornamento automatico.

Per maggiori informazioni sugli aggiornamenti di configurazione, fai riferimento a «*Mantenere aggiornato Bitdefender*» (p. 38).

Safego

Per essere sempre al sicuro sui social network, puoi accedere a Safego, la soluzione di sicurezza di Bitdefender per social network, direttamente da Bitdefender Internet Security.

Clicca sul pulsante **Gestisci** nel pannello di Safego e seleziona **Attiva per Facebook** dal menu a tendina. Se Safego è già stato attivato, potrai accedere ad alcune statistiche sulla sua attività, selezionando **Visualizza rapporto per Facebook** nel menu.

Per ulteriori informazioni, fare riferimento a «*Protezione di Safego per Facebook*» (p. 144).

Portafoglio

Il Portafoglio consente di gestire le password aiutandoti a memorizzarle, proteggendo la tua privacy e garantendoti sempre una navigazione online sicura.

Clicca sul pulsante **Gestisci** nel pannello del Portafoglio e seleziona un'attività dal menu a tendina:

- **Apri Portafoglio** - Apre il database del Portafoglio attuale.
- **Esporta Portafoglio** - Consente di salvare il dabatase attuale in un dato percorso sul proprio sistema.
- **Crea nuovo Portafoglio** - Avvia una procedura guidata che ti consentirà di creare un nuovo database del Portafoglio.

Per maggiori informazioni sulla configurazione del Portafoglio, fai riferimento a «*Massima protezione per le tue credenziali*» (p. 129).

Contr. Genitori

Il Controllo genitori di Bitdefender ti consente di limitare l'accesso a Internet e a particolari applicazioni, impedendo ai bambini di visualizzare contenuti inappropriati quando non ci sei

Clicca sul pulsante **Configura** e attiva il pannello Controllo genitori per configurare gli account Windows dei bambini e monitorare le loro attività ovunque ci si trovi.

Per maggiori informazioni sulla configurazione del Controllo Genitori, fare riferimento a «*Contr. Genitori*» (p. 134).

5.3. Finestra panoramica impostazioni

La finestra Panoramica impostazioni ti consente di accedere alle impostazioni avanzate del prodotto. Qui puoi configurare Bitdefender in ogni dettaglio.

Seleziona un modulo per configurare le sue impostazioni o eseguire le attività di sicurezza e gestione.Il seguente elenco descrive brevemente ogni modulo.

Generali

Ti consente di configurare le impostazioni generali del prodotto, come le impostazioni della password, la Modalità giochi, la Modalità portatile, le impostazioni del proxy e gli avvisi di stato.

Antivirus

Ti consente di configurare la tua protezione contro i malware, rileva e risolve le vulnerabilità del tuo sistema, imposta le eccezioni per la scansione e gestisce i file in quarantena.

Antispam
: Permette di mantenere la Posta in arrivo libera da SPAM e di configurare in dettaglio le impostazioni antispam.

Controllo privacy
: Ti consente di prevenire eventuali fughe di dati e protegge la tua privacy mentre sei online. Configura la protezione per il browser e i programmi di chat, crea regole per la protezione dei dati e molto altro.

Firewall
: Ti consente di configurare le impostazioni generali e le regole del firewall, oltre alle attività di rilevazione intrusioni e monitoraggio della rete.

Aggiornamento
: Ti consente di configurare i dettagli del processo di aggiornamento.

Portafoglio
: Ti consente di accedere alle tue credenziali con un'unica password principale.

Per tornare alla finestra principale, clicca su  nell'angolo in alto a sinistra della finestra.

5.4. Widget sicurezza

Il **widget sicurezza** è un modo semplice e veloce per monitorare e controllare Bitdefender Internet Security. Aggiungendo questo piccolo e discreto widget sul desktop, puoi visualizzare tutte le informazioni critiche ed eseguire le attività principali in qualsiasi momento:

- Monitorare le attività di scansione in tempo reale.
- Monitorare le attività del firewall in tempo reale.
- Monitorare lo stato di sicurezza del sistema e risolvere ogni eventuale problema.
- Visualizzare le notifiche e accedere agli ultimissimi eventi segnalati da Bitdefender.
- Accedere immediatamente al proprio account MyBitdefender.
- Eseguire una scansione di file o cartelle, trascinando e rilasciando uno o più elementi sul widget.

Widget sicurezza

Lo stato di sicurezza generale del computer è indicato **al centro** del widget. Lo stato è indicato dal colore e dalla forma dell'icona che compare in quest'area.

Alcuni problemi critici influenzano la sicurezza del tuo sistema.

Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile. Clicca sull'icona di stato per iniziare a risolvere i problemi segnalati.

Alcuni problemi non critici influenzano la sicurezza del tuo sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli. Clicca sull'icona di stato per iniziare a risolvere i problemi segnalati.

Il tuo sistema è protetto.

Quando è in corso una scansione su richiesta, viene mostrata questa icona.

In caso di problemi, clicca sull'icona di stato per lanciare la procedura guidata della risoluzione problemi.

Il pulsante **sul lato sinistro** del widget ti consente di accedere direttamente alla finestra delle impostazioni del firewall e rappresenta anche una sorta di visore in tempo reale delle attività del firewall. Quando su questo pulsante compare una barra blu, significa che il modulo del firewall sta filtrando le connessioni alla rete. Più la barra blu è alta e più intensa è l'attività del modulo.

Il lato superiore del widget mostra il contatore degli eventi non analizzati (il numero di eventi rilevanti segnalati da Bitdefender, in caso ve ne fossero). Clicca sul contatore degli eventi, per esempio 1 nel caso di un solo evento non analizzato, per aprire la finestra Panoramica eventi. Per ulteriori informazioni fare riferimento a «*Eventi*» (p. 14).

Il pulsante **sul lato destro** del widget ti consente di accedere direttamente alla finestra delle impostazioni dell'antivirus e rappresenta anche una sorta di visore in tempo reale delle attività di scansione. Quando su questo pulsante compare una barra blu, indica che è in corso un'attività di scansione antivirus in tempo reale. Più la barra blu è alta e più intensa è l'attività del modulo.

Il pulsante **sul lato inferiore** del widget lancia il pannello di controllo dell'account MyBitdefender in una finestra del browser. Per ulteriori informazioni fare riferimento a «*Account MyBitdefender*» (p. 35).

5.4.1. Eseguire la scansione di file e cartelle

Puoi utilizzare il widget sicurezza per eseguire una scansione veloce di file e cartelle.Trascina un file o una cartella che desideri controllare e rilascialo sopra al **widget sicurezza**.

Comparirà la procedura guidata scansione antivirus e ti guiderà attraverso il processo di scansione.Le opzioni di scansione sono preconfigurate per ottenere i migliori risultati di rilevamento e non possono essere modificate.Quando viene rilevato un file infetto, Bitdefender cerca di pulirlo, rimuovendo il codice malware). Se la disinfezione fallisce, la procedura guidata della scansione antivirus ti consentirà di indicare altre azioni da intraprendere sui file infetti.

5.4.2. Nascondi / mostra widget sicurezza

Se non desideri più visualizzare il widget, clicca su .

Per ripristinare il widget sicurezza, usa uno dei seguenti metodi:

- Dall'area di stato:
  1. Clicca con il pulsante destro sull'icona di Bitdefender nell'area di stato.
  2. Clicca su **Mostra widget sicurezza** nel menu contestuale che apparirà.
- Dall'interfaccia di Bitdefender:
  1. Apri la finestra di Bitdefender.
  2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
  3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
  4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
  5. Attiva l'opzione **Mostra widget sicurezza** cliccando sull'interruttore corrispondente.

5.5. Rapporto sicurezza

Il Rapporto sicurezza ti fornisce uno stato settimanale del tuo prodotto, oltre a diversi suggerimenti per migliorare la protezione del sistema. Questi suggerimenti sono importanti per la gestione della protezione globale e potrai facilmente verificare le azioni che si possono intraprendere sul sistema.

Il rapporto viene generato una volta la settimana e riassume le informazioni più importanti sulle attività del tuo prodotto, in modo da verificare facilmente tutto ciò che è successo in questo periodo di tempo.

La protezione offerta dal Rapporto sicurezza è divisa in due categorie:

- La sezione **Protezione cloud** consente di visualizzare informazioni sulla protezione del sistema.
  - **Scansione file**

    Ti consente di visualizzare i file esaminati da Bitdefender durante la settimana. Puoi visualizzare diverse informazioni, come il numero di file esaminati, il numero di file infetti e il numero di file puliti da Bitdefender.

    Per maggiori informazioni sulla protezione antivirus, fai riferimento a «*Protezione antivirus*» (p. 74)
  - **Scansione applicazioni**

    Ti consente di visualizzare il numero di applicazioni bloccate. Per proteggerti da eventuali applicazioni dannose, Bitdefender utilizza Active Virus Control per monitorare le applicazioni in esecuzione sul sistema.

    Per maggiori informazioni su Active Virus Control, fai riferimento a «*Active Virus Control*» (p. 93).
  - **Scansione web**

    Ti consente di verificare il numero di pagine web esaminate e bloccate da Bitdefender. Per impedirti di rivelare informazioni personali durante la navigazione, Bitdefender protegge il tuo traffico web.
- La sezione **Protezione privacy** consente di visualizzare informazioni sulla privacy del sistema.
  - **Scansione Vulnerabilità**

    Ti consente di visualizzare il numero di vulnerabilità sul sistema.

    Per maggiori informazioni sulla Scansione vulnerabilità, fai riferimento a «*Risolvere le vulnerabilità del sistema*» (p. 95).

5.5.1. Controllare il Rapporto sicurezza

Il Rapporto sicurezza utilizza un sistema di identificazione dei problemi per rilevare e fornire informazioni sui problemi che potrebbero influenzare la sicurezza del computer e dei dati. I problemi rilevati includono importanti impostazioni di protezione che sono disattivate e altre condizioni che possono rappresentare un rischio per la sicurezza. Utilizzando il rapporto, puoi configurare alcune componenti specifiche di Bitdefender o prendere azioni preventive per proteggere il computer e i tuoi dati personali.

Per controllare il Rapporto sicurezza, segui questi passaggi:

1. Accedi al rapporto:
   - Apri la finestra di Bitdefender e clicca sull'  icona nella parte superiore.

- Clicca con il pulsante destro sull'icona di Bitdefender nell'area di stato e seleziona **Mostra rapporto sicurezza**.
- Una volta completato un rapporto, comparirà una finestra per avvisarti. Clicca su **Mostra** per accedere al rapporto sicurezza.

  Nel browser si aprirà una pagina web in cui potrai visualizzare il rapporto.

2. Puoi verificare lo stato generale della sicurezza nella parte superiore della finestra.
3. Porta il cursore del mouse sulle aree selezionate per verificare i tuoi suggerimenti.
4. In caso di problemi da risolvere, comparirà una  piccola icona.

   Sposta il cursore del mouse sull'icona per maggiori informazioni.
5. Segui le istruzioni per risolvere i relativi problemi.

Il colore dell'area Stato sicurezza cambia in base ai problemi rilevati e ai diversi messaggi che vengono mostrati:

- **L'area è di colore verde.** Non ci sono problemi da risolvere. Il computer e i dati sono protetti.
- **L'area è di colore giallo.** Alcuni problemi non critici influenzano la sicurezza del sistema. Quando hai un po' di tempo, dovresti controllarli e risolverli.
- **L'area è di colore rosso.** Alcuni problemi critici influenzano la sicurezza del sistema. Devi risolvere i problemi rilevati immediatamente.

5.5.2. Attivare o disattivare gli avvisi sullo Stato di sicurezza

Per attivare o disattivare gli avvisi del rapporto sicurezza, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Generali**.
5. Clicca sull'interruttore per attivare o disattivare gli avvisi del rapporto sicurezza.

   Di norma, gli avvisi del rapporto sicurezza sono attivati.

6. Registrare Bitdefender

Per essere protetto da Bitdefender, devi registrare il tuo prodotto con un codice di licenza.Il codice di licenza specifica per quanto tempo puoi usare il prodotto.Non appena il codice di licenza scade, Bitdefender cessa di eseguire le sue funzioni e di proteggere il computer.

Dovresti acquistare o rinnovare un codice di licenza alcuni giorni prima della scadenza di quello attuale.Per ulteriori informazioni, fare riferimento a «*Comprare o rinnovare i codici di licenza*» (p. 34).Se stai usando una versione di prova di Bitdefender, devi registrarla con un codice di licenza, per continuare a usarla dopo il periodo di prova.

6.1. Inserire il tuo codice di licenza

Se durante l'installazione, hai selezionato di valutare il prodotto, puoi usarlo per un periodo di prova di 30 giorni.Per continuare a usare Bitdefender dopo la scadenza del periodo di prova, devi registrare il prodotto con un codice di licenza.

Nella parte inferiore della finestra di Bitdefender, compare un link che indica il numero di giorni rimasti per la tua licenza. Clicca su questo link per aprire la finestra di registrazione.

Puoi vedere lo stato della registrazione di Bitdefender, il codice di licenza corrente e i giorni mancanti alla scadenza della licenza.

Per registrare Bitdefender Internet Security:

1. Digita il codice di licenza nel campo corrispondente.

Nota

Puoi trovare il tuo codice di licenza:

- Sull'etichetta del CD.
- Sulla scheda di registrazione del prodotto.
- Nella e-mail di acquisto online.

Se non hai un codice di licenza di Bitdefender, clicca sul link fornito nella finestra per aprire una pagina web da cui potrai acquistarne uno.

2. Clicca su **Registra ora**.

Dopo aver acquistato un codice di licenza, finché la registrazione del prodotto con il codice non viene completata, Bitdefender Internet Security continuerà ad apparire come versione di prova.

6.2. Comprare o rinnovare i codici di licenza

Se il periodo di prova è quasi scaduto, devi acquistare un codice di licenza e registrare il prodotto.Analogamente, se il tuo codice di licenza attuale è quasi in scadenza, devi rinnovare la licenza.

Bitdefender ti avviserà quando la data di scadenza della tua licenza attuale si sta avvicinando. Segui le istruzioni nell'avviso per acquistare una nuova licenza.

Puoi visitare una pagina web dove acquistare in qualsiasi momento un codice di licenza, seguendo questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul link che indica il numero di giorni rimasti nella tua licenza, localizzato nella parte inferiore della finestra di Bitdefender, per aprire la finestra di registrazione del prodotto.
3. Clicca su **Non disponi di un codice di licenza? Acquistane uno ora!**
4. Sul tuo browser si aprirà una pagina web, da dove poter acquistare un codice di licenza di Bitdefender.

7. Account MyBitdefender

Le funzioni online del prodotto e i servizi aggiuntivi di Bitdefendersono disponibili esclusivamente tramite MyBitdefender. Devi collegare il computer a MyBitdefender accedendo a un account da Bitdefender Internet Security per poter eseguire una delle seguenti azioni:

- Recupera il tuo codice di licenza, se dovessi perderlo.
- Configura le impostazioni del Controllo genitori per gli account Windows dei bambini e monitora le loro attività ovunque ti trovi.
- Proteggi il tuo account Facebook con Safego.
- Gestisci Bitdefender Internet Security in remoto.

Molte soluzioni di sicurezza di Bitdefender per PC, così come per molte altre piattaforme, si interfacciano con MyBitdefender. Puoi gestire la sicurezza di tutti i dispositivi collegati al tuo account da una sola dashboard centralizzata.

Puoi accedere al tuo account MyBitdefender da qualsiasi dispositivo connesso a Internet, all'indirizzo https://my.bitdefender.com.

Puoi anche accedere e gestire il tuo account direttamente dal prodotto:

1. Apri la finestra di Bitdefender.
2. Clicca su **MyBitdefender** nella parte superiore della finestra e seleziona un'opzione dal menu a tendina:
   - **Impostazioni account**

     Accedi a un account, crea un nuovo account, configura il comportamento di MyBitdefender.
   - **Dashboard**

     Lancia la dashboard di MyBitdefender nel tuo browser.

7.1. Collegare il tuo computer a MyBitdefender

Per collegare il tuo computer a un account MyBitdefender, devi accedere a un account da Bitdefender Internet Security. Fin quando non colleghi il tuo computer a MyBitdefender, ti sarà chiesto di accedere a MyBitdefender ogni volta che utilizzi una funzione che richiede un account.

Per aprire la finestra di MyBitdefender, dalla quale puoi creare o accedere a un account, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca su **MyBitdefender** nella parte superiore della finestra e seleziona **Impostazioni account** dal menu a tendina.

Sei hai già eseguito l'accesso a un account, tale account sarà visualizzato. Clicca su **Vai a MyBitdefender** per accedere alla tua dashboard. Per cambiare l'account collegato al computer, clicca su **Accedi con altro account**.

Se non hai eseguito l'accesso a un account, procedi in base alla tua situazione.

Voglio creare un account MyBitdefender

Per creare con successo un account di MyBitdefender, segui questi passaggi:

1. Seleziona **Crea un nuovo account**.

   Comparirà una nuova finestra.

2. Digita le informazioni richieste nei campi corrispondenti.I dati forniti resteranno riservati.

   - **E-mail** - Inserisci il tuo indirizzo e-mail.
   - **Nome utente** - Inserisci un nome utente per il tuo account.
   - **Password** - Inserisci una password per il tuo account.La password deve avere almeno 6 caratteri.
   - **Conferma password** - Ridigita la password.

3. Clicca su **Crea**.
4. Prima di poter usare il tuo account, devi completare la registrazione. Controlla la tua posta elettronica e segui le istruzioni nell'e-mail di conferma inviata da Bitdefender.

Voglio accedere usando il mio account Microsoft, Facebook o Google

Per accedere con il tuo account Microsoft, Facebook o Google, segui questi passaggi:

1. Clicca sull'icona del servizio che vuoi usare per accedere.Sarai reindirizzato alla pagina di accesso del servizio.
2. Segui le istruzioni fornite dal servizio selezionato per collegare il tuo account a Bitdefender.

Nota

Bitdefender non accede ad alcuna informazione confidenziale, come la password dell'account con cui accedi o le informazioni personali dei tuoi amici e contatti.

Ho già un account MyBitdefender

Se hai già un account ma non hai ancora eseguito l'accesso a tale account, segui questi passaggi per accedere:

1. Digita l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

Nota

Se hai dimenticato la tua password, clicca su **Hai dimenticato la password?** e segui le istruzioni per recuperarla.

2. Clicca su **Accedi a MyBitdefender**.

Una volta che il computer è collegato a un account, puoi utilizzare l'indirizzo e-mail e la password forniti per accedere all'indirizzo https://my.bitdefender.com.

Puoi anche accedere al tuo account direttamente da Bitdefender Internet Security utilizzando il menu a tendina nella parte superiore della finestra.

8. Mantenere aggiornato Bitdefender

Tutti giorni vengono trovati e identificati nuovi malware. È quindi molto importante mantenere aggiornato Bitdefender con le firme malware più recenti.

Se siete connessi a Internet con una linea a banda larga o ADSL, Bitdefender si prenderà cura di sé da solo. Di norma, verifica la presenza di aggiornamenti all'accensione del computer e in seguito ad ogni **ora**.Se vi è un aggiornamento disponibile, viene scaricato e installato automaticamente sul computer.

Il processo di aggiornamento viene eseguito direttamente, ciò significa che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto e, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Importante
Per essere sempre protetti contro le minacce più recenti, mantieni attivato l'Aggiornamento automatico.

In alcune situazioni particolari, è necessario il tuo intervento per mantenere aggiornata la protezione di Bitdefender:

- Se il tuo computer si collega a Internet tramite un server proxy, devi configurare le impostazioni proxy come descritto nella sezione *«Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?»* (p. 67).
- Se non hai una connessione a Internet, puoi aggiornare Bitdefender manualmente, come descritto nella sezione *«Il mio computer non è connesso a Internet. Come aggiornare Bitdefender?»* (p. 159).Il file per l'aggiornamento manuale viene rilasciato una volta alla settimana.
- Con una connessione a Internet lenta potrebbero verificarsi degli errori durante lo scaricamento degli aggiornamenti.Per scoprire come superare tali errori, fai riferimento a *«Come aggiornare Bitdefender con una connessione a Internet lenta»* (p. 158).
- Se sei connesso a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di Bitdefender su richiesta dell'utente.Per ulteriori informazioni, fare riferimento a *«Eseguire un aggiornamento»* (p. 39).

8.1. Verificare se Bitdefender è aggiornato

Per verificare se la protezione di Bitdefender è aggiornata, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nell'**area Stato sicurezza**, sul lato sinistro della barra degli strumenti, cerca la data dell'ultimo aggiornamento.

   Queste informazioni saranno mostrate solo se lo stato della sicurezza è verde.

Per maggiori informazioni sugli ultimi aggiornamenti, controlla gli eventi di aggiornamento:

1. Nella finestra principale, clicca su **Eventi** nella barra degli strumenti superiore.
2. Nella finestra **Panoramica eventi**, clicca su **Aggiorna**.

Puoi sapere quando gli aggiornamenti sono stati lanciati e avere maggiori informazioni al riguardo (se hanno avuto successo o meno, e se richiedono di riavviare il computer per completare l'installazione).Se necessario, riavvia il sistema al più presto.

8.2. Eseguire un aggiornamento

Per poter eseguire gli aggiornamenti, serve una connessione a Internet.

Per avviare un aggiornamento, esegui una delle seguenti operazioni:

- Apri la finestra di Bitdefender e clicca su **Aggiorna ora** nel pannello **Aggiorna**.
- Clicca con il pulsante destro sull'icona di Bitdefender nell'area di stato e seleziona **Aggiorna ora**.

Il modulo Aggiornamento si connetterà al server di aggiornamento di Bitdefender per cercare eventuali aggiornamenti.Se viene rilevato un aggiornamento, ti sarà chiesto di confermare l'aggiornamento oppure sarà eseguito automaticamente, secondo le impostazioni di aggiornamento.

Importante
Potrebbe essere necessario riavviare il computer, una volta completato l'aggiornamento. Si raccomanda di farlo il prima possibile.

8.3. Attivare o disattivare l'aggiornamento automatico

Per attivare o disattivare l'aggiornamento automatico, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Aggiorna**, clicca sull'interruttore **Aggiornamento**.
3. Comparirà una finestra di avviso.Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare l'aggiornamento automatico. Puoi disattivare l'aggiornamento automatico per 5, 15 o 30 minuti, per un'ora, permanentemente o fino al riavvio del sistema.

Avvertimento
È una questione di sicurezza piuttosto importante. Si consiglia di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se Bitdefender non verrà aggiornato regolarmente non sarà in grado di proteggerti dalle minacce più recenti.

8.4. Modificare le impostazioni di aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy. Di norma, Bitdefender controllerà la disponibilità di aggiornamenti su Internet ogni ora e installerà gli aggiornamenti disponibili senza avvisarti.

Le impostazioni predefinite di aggiornamento sono adatte alla maggior parte degli utenti e normalmente non serve modificarle.

Per modificare le impostazioni di aggiornamento, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Aggiorna**.
4. Nella finestra **Impostazioni aggiornamento**, puoi modificare le impostazioni in base alle tue preferenze.

Ubicazione aggiornamento

Bitdefender è configurato per aggiornarsi dai server di aggiornamento di Bitdefender su Internet.L'ubicazione dell'aggiornamento è un indirizzo Internet generico che viene automaticamente reindirizzato al server di aggiornamento più vicino di Bitdefender nel tuo paese.

Non modificare l'ubicazione dell'aggiornamento a meno che non ti sia stato consigliato da un operatore di Bitdefender o dal tuo amministratore di rete (se sei connesso a una rete aziendale).

Puoi tornare alla generica ubicazione dell'aggiornamento Internet cliccando su **Predefinito**.

Regole di esecuzione dell'aggiornamento

Puoi scegliere fra tre modi per scaricare e installare gli aggiornamenti:

- **Aggiornamento silenzioso** - Bitdefender scarica e implementa l'aggiornamento automaticamente.
- **Chiedi prima di scaricare** - Ogni volta che un aggiornamento è disponibile, ti sarà chiesto se desideri scaricarlo.
- **Chiedi prima di installare** - Ogni volta che si scarica un aggiornamento, ti sarà chiesto se desideri installarlo.

Per completare l'installazione di alcuni aggiornamenti devi riavviare il sistema.Come impostazione predefinita, se un aggiornamento richiede un riavvio, Bitdefender continuerà a funzionare con i file precedenti finché l'utente non riavvia

volontariamente il computer. Questo per impedire che il processo di aggiornamento di Bitdefender interferisca con il lavoro dell'utente.

Se vuoi essere avvisato quando un aggiornamento richiede un riavvio del sistema, disattiva l'opzione **Posticipa riavvio** cliccando sull'interruttore corrispondente.

Come fare

9. Installazione

9.1. Come faccio a installare Bitdefender su un secondo computer?

Se hai acquistato un codice di licenza per più di un computer, puoi utilizzarlo per registrare un secondo PC.

Per installare Bitdefender correttamente su un secondo computer, segui questi passaggi:

1. Installa Bitdefender dal CD/DVD o utilizzando il programma d'installazione fornito nell'e-mail di conferma dell'acquisto online e segui le stesse fasi di installazione.

   All'inizio dell'installazione, ti sarà chiesto di scaricare i file d'installazione più recenti disponibili.

2. Quando compare la finestra di registrazione, inserisci il codice di licenza e clicca su **Registra**.

3. Nella prossima fase, avrai l'opportunità di accedere al tuo account MyBitdefender o di creare un nuovo account MyBitdefender.

   Puoi anche scegliere di creare un account MyBitdefender in un secondo momento.

4. Attendi il termine del processo di installazione e chiudi la finestra.

9.2. Quando dovrei reinstallare Bitdefender?

In alcune situazioni, potresti dover reinstallare il tuo prodotto Bitdefender.

Alcune tipiche situazioni in cui dovresti reinstallare Bitdefender sono:

- hai reinstallato il sistema operativo.
- hai acquistato un computer nuovo.
- vuoi cambiare la lingua visualizzata nell'interfaccia di Bitdefender.

Per reinstallare Bitdefender puoi usare il disco di installazione acquistato o scaricare una nuova versione dal sito web di Bitdefender.

Durante l'installazione, ti sarà chiesto di registrare il prodotto con il tuo codice di licenza.

Se hai perso il codice di licenza, puoi accedere a https://my.bitdefender.com per recuperarlo. Digita l'indirizzo e-mail e la password per l'account nei campi corrispondenti.

Per maggiori informazioni sull'installazione di Bitdefender, fai riferimento a «*Installare il tuo prodotto Bitdefender*» (p. 5).

9.3. Dove posso scaricare il mio prodotto Bitdefender?

Puoi scaricare il prodotto Bitdefender dai siti web autorizzati (per esempio, il sito web di un partner di Bitdefender o un negozio online) o direttamente dal nostro sito web, al seguente indirizzo: http://www.bitdefender.it/Downloads/.

Nota
Prima di iniziare l'installazione, si consiglia di rimuovere qualsiasi altra soluzione antivirus installata sul tuo sistema. Usando più di una soluzione di sicurezza sullo stesso computer, il sistema diventa instabile.

Per installare Bitdefender, segui questi passaggi:

1. Clicca due volte sul file di installazione che hai scaricato e segui le istruzioni che compariranno sullo schermo.
2. Quando compare la finestra di registrazione, inserisci il codice di licenza e clicca su **Registra**.
3. Nella prossima fase, avrai l'opportunità di accedere al tuo account MyBitdefender o di creare un nuovo account MyBitdefender.

   Puoi anche scegliere di creare un account MyBitdefender in un secondo momento.
4. Attendi il termine del processo di installazione e chiudi la finestra.

9.4. Come posso passare da un prodotto Bitdefender a un altro?

Puoi passare facilmente da un prodotto Bitdefender a un altro.

I tre prodotti Bitdefender che puoi installare sul sistema sono:

- Bitdefender Antivirus Plus
- Bitdefender Internet Security
- Bitdefender Total Security

Se non possiedi un codice di licenza per il prodotto che intendi utilizzare, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Per accedere alla finestra di registrazione del prodotto, clicca sul collegamento che indica il numero di giorni rimasti per la licenza, localizzato nella parte inferiore della finestra di Bitdefender.
3. Clicca su **Non disponi di un codice di licenza? Acquistane uno ora!**
4. Sul tuo browser si aprirà una pagina web, da dove poter acquistare un codice di licenza di Bitdefender.

Dopo aver acquistato il codice di licenza per il prodotto Bitdefender che intendi utilizzare, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nella parte inferiore della finestra di Bitdefender, compare un link che indica il numero di giorni rimasti per la tua licenza.

   Clicca su questo link per aprire la finestra di registrazione.
3. Inserisci il nuovo codice di licenza e clicca su **Registra ora**.
4. Ti sarà comunicato che il codice di licenza è per un altro prodotto Bitdefender.

   Clicca sul collegamento corrispondente e segui la procedura per eseguire l'installazione.

9.5. Come posso utilizzare il mio codice di licenza Bitdefender dopo aver aggiornato Windows?

Questa situazione si verifica quando dopo aver aggiornato il sistema operativo vuoi continuare a utilizzare il tuo codice di licenza Bitdefender.

Se stai utilizzando Bitdefender 2009, 2010, 2011, 2012 o 2013, puoi passare, gratuitamente, alla versione di Bitdefender più recente, secondo tale schema:

- DaBitdefender Antivirus 2009, 2010, 2011, 2012 o 2013 al più recente Bitdefender Antivirus Plus.
- Da Bitdefender Internet Security 2009, 2010, 2011, 2012 o 2013 al più recente Bitdefender Internet Security.
- Da Bitdefender Total Security 2009, 2010, 2011, 2012 o 2013 al più recente Bitdefender Total Security.

Possono verificarsi 2 situazioni:

- Dopo aver aggiornato il sistema operativo con Windows Update, scopri che Bitdefender non funziona più.

  In questo caso, devi installare nuovamente il prodotto utilizzando la versione più recente disponibile.

  Per risolvere questa situazione, segui questi passaggi:

  1. Rimuovi Bitdefender seguendo questi passaggi:

     ▶ Per **Windows XP**:

     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.

b. Attendi per qualche istante, finché non compare l'elenco del software installato.

c. Trova **Bitdefender** e seleziona **Rimuovi**.

d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

- Per **Windows Vista** e **Windows 7**:

  a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.

  b. Attendi per qualche istante, finché non compare l'elenco del software installato.

  c. Trova **Bitdefender** e seleziona **Disinstalla**.

  d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

  e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

- Per **Windows 8**:

  a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.

  b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.

  c. Attendi per qualche istante, finché non compare l'elenco del software installato.

  d. Trova **Bitdefender** e seleziona **Disinstalla**.

  e. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

  f. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

2. Scarica il file d'installazione, selezionando il prodotto di cui possiedi un codice di licenza valido.

   Il file di installazione può essere scaricato dal sito web di Bitdefender al seguente indirizzo: http://www.bitdefender.it/Downloads/.

3. Clicca due volte sul file d'installazione per iniziare l'installazione.

4. Quando compare la finestra di registrazione, inserisci il codice di licenza e clicca su **Registra**.

5. Nella prossima fase, avrai l'opportunità di accedere al tuo account **MyBitdefender** o di creare un nuovo account **MyBitdefender**.

   Puoi anche scegliere di creare un account **MyBitdefender** in un secondo momento.

   Attendi il termine del processo di installazione e chiudi la finestra.

- Hai cambiato sistema e vuoi continuare a utilizzare la protezione di Bitdefender.

  In questo caso, devi installare nuovamente il prodotto utilizzando la versione più recente.

  Per risolvere questa situazione, segui questi passaggi:

  1. Scarica il file d'installazione, selezionando il prodotto di cui possiedi un codice di licenza valido.

     Il file di installazione può essere scaricato dal sito web di Bitdefender al seguente indirizzo: http://www.bitdefender.it/Downloads/.

  2. Clicca due volte sul file d'installazione per iniziare l'installazione.
  3. Quando compare la finestra di registrazione, inserisci il codice di licenza e clicca su **Registra**.
  4. Nella prossima fase, avrai l'opportunità di accedere al tuo account **MyBitdefender** o di creare un nuovo account **MyBitdefender**.

     Puoi anche scegliere di creare un account **MyBitdefender** in un secondo momento.

     Attendi il termine del processo di installazione e chiudi la finestra.

  Per maggiori informazioni sull'installazione di Bitdefender, fai riferimento a «*Installare il tuo prodotto Bitdefender*» (p. 5).

9.6. Come posso riparare Bitdefender?

Se desideri riparare la tua copia di Bitdefender Internet Security dal menu del pulsante Start di Windows, segui questi passaggi:

- Per **Windows XP**, **Windows Vista** e **Windows 7**:
  1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
  2. Clicca su **Bitdefender Internet Security**.
  3. Seleziona **Ripara** o **Disinstalla**.

     Apparirà una finestra.
  4. Seleziona **Ripara**.

     Questa operazione richiederà alcuni minuti.
  5. Dovrai riavviare il computer per completare il processo.

- Per **Windows 8**:

  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Seleziona **Bitdefender Internet Security** e clicca su **Disinstalla**.

     Apparirà una finestra.
  4. Seleziona **Ripara**.

     Questa operazione richiederà alcuni minuti.
  5. Dovrai riavviare il computer per completare il processo.

10. Registrazione

10.1. Quale prodotto Bitdefender sto usando?

Per scoprire quale programma di Bitdefender hai installato, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nella parte superiore della finestra dovresti vedere uno dei seguenti:
   - Bitdefender Antivirus Plus
   - Bitdefender Internet Security
   - Bitdefender Total Security

10.2. Come posso registrare una versione di prova?

Se hai installato una versione di prova, puoi usarla solo per un periodo limitato. Per continuare a usare Bitdefender dopo la scadenza del periodo di prova, devi registrare il prodotto con un codice di licenza.

Per registrare Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nella parte inferiore della finestra di Bitdefender, compare un link che indica il numero di giorni rimasti per la tua licenza.

   Clicca su questo link per aprire la finestra di registrazione.
3. Inserisci il codice di licenza e clicca su **Registra ora**.

   Se non hai un codice di licenza, clicca sul link fornito nella finestra per visitare una pagina web da cui potrai acquistarne uno.
4. Attendi il termine del processo di registrazione e chiudi la finestra.

10.3. Quando scade la protezione di Bitdefender?

Per scoprire quanti giorni mancano alla scadenza del tuo codice di licenza, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nella parte inferiore della finestra di Bitdefender, compare un link che indica il numero di giorni rimasti per la tua licenza.
3. Per ulteriori informazioni, clicca sul link per aprire la finestra di registrazione.
4. Nella finestra **Registra il tuo prodotto**, puoi:
   - Guarda il codice di licenza attuale

- Registra con un altro codice di licenza
- Acquista un codice di licenza

10.4. Come posso rinnovare la protezione di Bitdefender?

Quando la protezione di Bitdefender sta per scadere, devi rinnovare il tuo codice di licenza.

- Segui questi passaggi per visitare un sito web dove rinnovare il tuo codice di licenza di Bitdefender:

  1. Apri la finestra di Bitdefender.
  2. Nella parte inferiore della finestra di Bitdefender, compare un link che indica il numero di giorni rimasti per la tua licenza. Clicca su questo link per aprire la finestra di registrazione.
  3. Clicca su **Non disponi di un codice di licenza? Acquistane uno ora!**
  4. Sul tuo browser si aprirà una pagina web, da dove poter acquistare un codice di licenza di Bitdefender.

  Nota
  In alternativa, puoi contattare il rivenditore da cui hai acquistato il tuo prodotto Bitdefender.

- Segui questi passaggi per registrare Bitdefender con il nuovo codice di licenza:

  1. Apri la finestra di Bitdefender.
  2. Nella parte inferiore della finestra di Bitdefender, compare un link che indica il numero di giorni rimasti per la tua licenza. Clicca su questo link per aprire la finestra di registrazione.
  3. Inserisci il codice di licenza e clicca su **Registra ora**.
  4. Attendi il termine del processo di registrazione e chiudi la finestra.

Per maggiori informazioni, puoi contattare Bitdefender per avere assistenza, come descritto nella sezione «*Chiedere aiuto*» (p. 181).

11. MyBitdefender

11.1. Come posso accedere a MyBitdefender utilizzando un altro account online?

Hai creato un nuovo account MyBitdefender che desideri utilizzare da qui in avanti.

Per utilizzare correttamente un altro account, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca su **MyBitdefender** nella parte superiore della finestra e seleziona **Impostazioni account** dal menu a tendina.

   Sei hai già eseguito l'accesso a un account, tale account sarà visualizzato. Clicca su **Accedi con altro account** per modificare l'account associato al computer.

   Comparirà una nuova finestra.
3. Digita l'indirizzo e-mail e la password per l'account nei campi corrispondenti.
4. Clicca su **Accedi a MyBitdefender**
5. Clicca su **Vai a MyBitdefender** per accedere alla tua dashboard.

11.2. Come posso cambiare l'indirizzo e-mail utilizzato per l'account MyBitdefender?

Hai creato un account MyBitdefender utilizzando un indirizzo e-mail che non usi più e ora vorresti cambiarlo.

L'indirizzo e-mail non può essere cambiato, ma puoi utilizzare un altro indirizzo e-mail per creare un nuovo account online.

Per creare un altro account MyBitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca su **MyBitdefender** nella parte superiore della finestra e seleziona **Impostazioni account** dal menu a tendina.

   Sei hai già eseguito l'accesso a un account, tale account sarà visualizzato. Clicca su **Accedi con altro account** per modificare l'account associato al computer.

   Comparirà una nuova finestra.
3. Seleziona **Crea un nuovo account**.
4. Digita le informazioni richieste nei campi corrispondenti. I dati forniti resteranno riservati.

   - **E-mail** - Inserisci il tuo indirizzo e-mail.

- **Nome utente** - Inserisci un nome utente per il tuo account.
- **Password** - Inserisci una password per il tuo account. La password deve avere almeno 6 caratteri.
- **Conferma password** - Ridigita la password.
- Clicca su **Crea**.

5. Prima di poter usare il tuo account, devi completare la registrazione. Controlla la tua posta elettronica e segui le istruzioni nell'e-mail di conferma inviata da Bitdefender.

Utilizza il nuovo indirizzo e-mail per accedere a MyBitdefender.

11.3. Come posso cambiare la password dell'account MyBitdefender?

Per impostare una nuova password per il tuo account MyBitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca su **MyBitdefender** nella parte superiore della finestra e seleziona **Impostazioni account** dal menu a tendina.

   Comparirà una nuova finestra.
3. Clicca sul collegamento **Ho dimenticato password**.
4. Digita l'indirizzo e-mail utilizzato per creare il tuo account MyBitdefender e clicca sul link **Recupera password**.
5. Controlla la tua casella di posta, apri il messaggio e clicca sul link fornito.

   Comparirà una nuova finestra.
6. Digita la nuova password. La password deve avere almeno 6 caratteri.
7. Ridigita la password nel campo **Conferma password**.
8. Clicca su **Invia** e poi su **Applica le modifiche**.

Ora per accedere al tuo account MyBitdefender, digita il tuo indirizzo e-mail e la nuova password che hai appena impostato.

12. Scansione con Bitdefender

12.1. Come posso controllare un file o una cartella?

Il modo più semplice di controllare un file o una cartella è cliccare con il pulsante destro sull'oggetto che desideri controllare, selezionare Bitdefender e poi **Controlla con Bitdefender** dal menu.

Per completare la scansione, segui la procedura guidata della Scansione antivirus. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

Tipiche situazioni in cui si userebbe questo metodo includono:

- Si sospetta che un file o una cartella specifica sia infetta.
- Ogni volta che scarichi file da Internet che potrebbero essere pericolosi.
- Controlla una rete condivisa prima di copiare i file sul computer.

12.2. Come posso eseguire una scansione del mio sistema?

Per eseguire una scansione completa del sistema, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Scansione sistema** dal menu a tendina.
3. Segui la procedura guidata della scansione antivirus per completare la scansione. Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.

   Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per ulteriori informazioni, fare riferimento a *«Procedura guidata scansione antivirus»* (p. 85).

12.3. Come posso creare un'attività di scansione personale?

Se desideri controllare percorsi particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personalizzata.

Per creare un'attività di scansione personale, procedi così:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Gestisci scansioni** dal menu a tendina.
3. Clicca su **Nuova attività personalizzata** per inserire un nome per la scansione e selezionare i percorsi da controllare.

4. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**.

   Puoi configurare facilmente le opzioni di scansione, impostando il livello della scansione. Trascina il pulsante scorrevole lungo la barra per impostare il livello di scansione desiderato.

   Puoi anche scegliere di spegnere il computer al termine della scansione, se non venisse rilevata alcuna minaccia. Ricordati che questo sarà il comportamento predefinito ogni volta che esegui questa attività.

5. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
6. Clicca su **Elenco** se desideri impostare un elenco per la tua scansione.
7. Clicca su **Inizia la scansione** e segui la procedura guidata della scansione antivirus per completare la scansione. Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.
8. Se lo desideri, puoi eseguire nuovamente una scansione personale precedente cliccando sulla rispettiva voce nell'elenco disponibile.

12.4. Come posso escludere una cartella dalla scansione?

Bitdefender consente di escludere determinati file, cartelle o estensioni di file dalla scansione.

Le eccezioni devono essere utilizzate da utenti con una conoscenza avanzata del computer e solo nelle seguenti situazioni:

- Hai una cartella di grandi dimensioni sul tuo sistema, dove tieni film e musica.
- Hai una cartella di grandi dimensioni sul tuo sistema, dove tieni diversi dati.
- Tieni una cartella dove installare diversi tipi di programmi e applicazioni a scopo di prova.La scansione della cartella può causare la perdita di alcuni dati.

Per aggiungere la cartella all'elenco delle eccezioni, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Eccezioni**.
5. Assicurati che l'opzione **Eccezioni per i file** sia attivata cliccando sull'interruttore.
6. Clicca sul collegamento **File e cartelle escluse**.
7. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.

8. Clicca su **Sfoglia**, seleziona la cartella che desideri escludere dalla scansione e quindi clicca su **OK**.
9. Clicca su **Aggiungi** e poi su **OK** per salvare le modifiche e chiudere la finestra.

12.5. Cosa fare quando Bitdefender rileva un file pulito come infetto?

In alcuni casi Bitdefender marca per errore un file legittimo come una minaccia (un falso positivo). Per correggere questo errore, aggiungi il file all'area Eccezioni di Bitdefender:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
   d. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
   e. Clicca sull'interruttore per disattivare la **scansione all'accesso**.

      Comparirà una finestra di avviso. Devi confermare la tua scelta selezionando dal menu per quanto tempo desideri disattivare la protezione in tempo reale. Puoi disattivarla durante 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a «*Come posso visualizzare gli elementi nascosti in Windows?*» (p. 69).
3. Ripristina il file dalla quarantena:
   a. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
   d. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Quarantena**.
   e. Seleziona il file e clicca su **Ripristina**.
4. Aggiungi il file all'elenco delle eccezioni. Per scoprire come fare, fai riferimento a «*Come posso escludere una cartella dalla scansione?*» (p. 54).
5. Attiva la protezione antivirus in tempo reale di Bitdefender.
6. Contatta gli operatori del nostro supporto in modo da poter rimuovere la firma di rilevazione. Per scoprire come fare, fai riferimento a «*Chiedere aiuto*» (p. 181).

12.6. Come posso verificare quali virus sono stati rilevati da Bitdefender?

Ogni volta che viene eseguita una scansione, viene creato un registro di scansione dove Bitdefender registra i problemi rilevati.

Il registro di scansione contiene informazioni dettagliate sul processo di scansione registrato, sull'obiettivo della scansione, le minacce individuate e le azioni intraprese su queste minacce.

Puoi aprire il registro della scansione direttamente dalla procedura guidata di scansione, una volta completata, cliccando su **Registro**.

Per controllare un registro di scansione o qualsiasi infezione rilevata in un secondo momento, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Eventi antivirus**, seleziona la scheda **Scansione Virus**.

   Qui puoi trovare tutti gli eventi della scansione antimalware, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.
5. Nell'elenco degli eventi, puoi controllare quali scansioni sono state eseguite di recente. Clicca su un evento per visualizzare maggiori dettagli al riguardo.
6. Per aprire un registro di scansione, clicca su **Guarda registro**. Il registro di scansione si aprirà in una nuova finestra.

13. Contr. Genitori

13.1. Come posso proteggere i bambini dalle minacce online?

Il Controllo genitori di Bitdefender ti consente di limitare l'accesso a Internet e a particolari applicazioni, impedendo ai bambini di visualizzare contenuti inappropriati quando non ci sei.

Per configurare il Controllo genitori, segui questi passaggi:

1. Creare degli account di Windows limitati (standard) per i bambini. Per ulteriori informazioni, fare riferimento a «*Come posso creare gli account utente di Windows?*» (p. 59).
2. Assicurati di aver avviato il computer con un account amministratore. Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo genitori.
3. Configura il Controllo genitori per gli account di Windows che saranno usati dai bambini.
   a. Apri la finestra di Bitdefender.
   b. Vai al pannello **Controllo genitori** e clicca sull'interruttore per attivarlo.
   c. Clicca sul pulsante **Configura**.
   d. La dashboard del Controllo genitori si aprirà in una nuova finestra. Qui è dove puoi verificare e configurare le impostazioni del Controllo genitori.
   e. Clicca su **Aggiungi bambino** nel menu di sinistra.
   f. Inserisci il nome e l'età del bambino nella scheda **Profilo**. Impostando l'età del bambino caricherai automaticamente le impostazioni considerate appropriate per quella categoria d'età, in base agli standard di sviluppo del bambino.

Controlla le attività dei bambini e modifica le impostazioni del Controllo genitori utilizzando MyBitdefender da qualsiasi computer o dispositivo mobile connesso a Internet.

Per maggiori informazioni sull'utilizzo del Controllo Genitori, fare riferimento a «*Contr. Genitori*» (p. 134).

13.2. Come posso limitare l'accesso a Internet per i bambini?

Una volta configurato il Controllo genitori, puoi bloccare facilmente l'accesso a Internet in determinati momenti.

Il Controllo genitori di Bitdefender ti consente di controllare l'utilizzo di Internet da parte dei bambini anche quando non sei a casa.

Per limitare l'accesso a Internet in determinati momenti della giornata, segui questi passaggi:

1. Accedi a un browser web da qualsiasi dispositivo con accesso a Internet.
2. Vai a:https://my.bitdefender.com
3. Accedi al tuo account usando il tuo nome utente e la password.
4. Clicca su **Controllo genitori** per accedere alla dashboard.
5. Seleziona il profilo del bambino sul lato sinistro del menu.
6. Clicca su  nel pannello **Web** per accedere alla finestra **Attività web**.
7. Clicca su **Programmazione**.
8. Seleziona dalla griglia gli intervalli di tempo durante i quali bloccare l'accesso a Internet.Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi.Per avviare una nuova selezione, clicca su **Azzera**.
9. Clicca sul pulsante **Salva**.

Nota

Bitdefender eseguirà gli aggiornamenti ogni ora anche se l'accesso web fosse bloccato.

13.3. Come posso impedire che i bambini accedano a un sito web?

Il Controllo genitori di Bitdefender ti consente di controllare i contenuti a cui i bambini accedono tramite il computer e di bloccare l'accesso a un sito web anche quando non sei a casa.

Per bloccare l'accesso a un sito web, segui questi passaggi:

1. Accedi a un browser web da qualsiasi dispositivo con accesso a Internet.
2. Vai a:https://my.bitdefender.com
3. Accedi al tuo account usando il tuo nome utente e la password.
4. Clicca su **Controllo genitori** per accedere alla dashboard.
5. Seleziona il profilo del bambino sul lato sinistro del menu.
6. Clicca su  nel pannello **Web** per accedere alla finestra **Attività web**.
7. Clicca su **Blacklist**.
8. Inserisci il sito web nel campo corrispondente.
9. Clicca su **Aggiungi** per aggiungere il sito web all'elenco.

10. Seleziona dalla griglia gli intervalli di tempo durante i quali è consentito l'accesso. Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi.

    Clicca sul pulsante **Salva**.

11. Se cambiassi idea, seleziona il sito web e clicca sul pulsante **Rimuovi** corrispondente.

13.4. Come posso impedire ai bambini di usare un gioco?

Il Controllo genitori di Bitdefender ti consente di controllare i contenuti a cui i bambini accedono tramite il computer.

Se devi limitare l'accesso a un gioco o a un'applicazione, puoi utilizzare il Controllo genitori di Bitdefender anche quando non sei a casa.

Per bloccare l'accesso a un gioco, segui questi passaggi:

1. Accedi a un browser web da qualsiasi dispositivo con accesso a Internet.
2. Vai a:https://my.bitdefender.com
3. Accedi al tuo account usando il tuo nome utente e la password.
4. Clicca su **Controllo genitori** per accedere alla dashboard.
5. Seleziona il profilo del bambino sul lato sinistro del menu.
6. Clicca su  nel pannello **Applicazioni** per accedere alla finestra **Attività applicazioni**.
7. Clicca su **Blacklist**.
8. Digita (o copia e incolla) il percorso del file eseguibile nel campo corrispondente.
9. Clicca su **Blocca** per aggiungere l'applicazione alle **app bloccate**.
10. Se cambiassi idea, clicca sul pulsante corrispondente **Consenti**.

13.5. Come posso creare gli account utente di Windows?

Un account utente di Windows è un profilo unico che include tutte le impostazioni, i privilegi e i file personali per ogni utente. Gli account Windows consentono all'amministratore del PC domestico di controllare l'accesso di ogni utente.

Impostare gli account utente è utile quando il PC è utilizzato sia da genitori sia da bambini. Un genitore può impostare account per ogni bambino.

Scegli il sistema operativo che possiedi per scoprire come creare degli account Windows.

- **Windows XP:**

  1. Accedi al tuo computer come amministratore.

2. Clicca su Start, clicca su Pannello di controllo e poi su Account utente.
3. Clicca su Crea un nuovo account.
4. Inserisci il nome per l'utente. Puoi usare nome e cognome, il nome di battesimo o un soprannome. Poi clicca su Avanti.
5. Per il tipo di account, scegli limitato e poi Crea account. Gli account limitati sono adatti ai bambini perché non consentono di effettuare cambiamenti importanti a livello di sistema o installare determinate applicazioni.
6. Sarà creato il tuo nuovo account e potrai vederlo elencato nella schermata di Gestione account.

- **Windows Vista o Windows 7:**

1. Accedi al tuo computer come amministratore.
2. Clicca su Start, clicca su Pannello di controllo e poi su Account utente.
3. Clicca su Crea un nuovo account.
4. Inserisci il nome per l'utente. Puoi usare nome e cognome, il nome di battesimo o un soprannome. Poi clicca su Avanti.
5. Per il tipo di account, clicca su standard e poi su Crea account. Gli account limitati sono adatti ai bambini perché non consentono di effettuare cambiamenti importanti a livello di sistema o installare determinate applicazioni.
6. Sarà creato il tuo nuovo account e potrai vederlo elencato nella schermata di Gestione account.

- **Windows 8:**

1. Accedi al tuo computer come amministratore.
2. Punta il cursore del mouse nell'angolo in alto a destra dello schermo, clicca su Impostazioni e poi su Modifica impostazioni PC.
3. Clicca su Utenti nel menu a sinistra e poi clicca su Aggiungi nuovo utente.

   Puoi creare un account Microsoft o un account locale. Leggi la descrizione di ciascun account e segui le istruzioni sullo schermo per creare un nuovo account.

Nota
Ora che hai aggiunto nuovi account utente, puoi creare le password per gli account.

13.6. Come rimuovere un profilo di un bambino

Se desideri rimuovere un profilo di un bambino, segui questi passaggi:

1. Accedi a un browser web da qualsiasi dispositivo con accesso a Internet.
2. Vai a: https://my.bitdefender.com.
3. Accedi al tuo account usando il tuo nome utente e la password.

4. Clicca su **Controllo genitori** per accedere alla dashboard.
5. Seleziona il profilo del bambino che vuoi rimuovere dal menu a sinistra.
6. Clicca su **Impostazioni account**.
7. Cliccare su **Rimuovere profilo**.
8. Clicca su **OK**.

14. Controllo privacy

14.1. Come posso essere certo che le mie transazioni online sono sicure?

Per assicurarti che le tue operazioni online restino private, puoi utilizzare il browser fornito da Bitdefender per proteggere le transazioni e le applicazioni di home banking.

Bitdefender Safepay è un browser sicuro progettato per proteggere i dati della tua carta di credito, il numero del tuo conto bancario e altre informazioni personali che potresti inserire nei più diversi siti web.

Per garantire la massima sicurezza e privacy alle tue attività online, segui questi passaggi:

1. Clicca due volte sull'icona di Bitdefender Safepay sul desktop.

   Si aprirà il browser di Bitdefender Safepay.

2. Clicca sul pulsante  per accedere alla **tastiera virtuale**.
3. Usa la **tastiera virtuale** ogni volta che devi digitare informazioni personali, come le password.

14.2. Come posso proteggere il mio account Facebook?

Safego è un'applicazione Facebook sviluppata da Bitdefender per tenere al sicuro il tuo account di social network.

Il suo compito è controllare i link che ricevi dai tuoi amici Facebook e monitorare le impostazioni sulla privacy del tuo account.

Per accedere a Safego dal tuo prodotto di Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Safego**, clicca su **Gestisci** e seleziona **Attiva per Facebook** dal menu a tendina.

   Sarai indirizzato al tuo account.

3. Usa le tue informazioni di accesso a Facebook per connetterti all'applicazione Safego.
4. Consenti a Safego di accedere al tuo account Facebook.

14.3. Come posso eliminare un file in modo permanente con Bitdefender?

Se desideri eliminare un file in modo permanente dal sistema, devi cancellare i dati fisicamente dal tuo disco rigido.

Il Distruttore di file di Bitdefender ti aiuterà a distruggere rapidamente file o cartelle dal computer, utilizzando il menu contestuale di Windows, seguendo questi passaggi:

1. Clicca con il pulsante destro sul file o la cartella che vuoi eliminare in maniera definitiva, seleziona Bitdefender e poi **Distruttore di file**.
2. Apparirà una finestra di conferma. Clicca su **Sì** per avviare la procedura guidata del Distruttore di file.
3. Attendi che Bitdefender termini la distruzione dei file.
4. I risultati sono mostrati. Clicca su **Chiudi** per uscire dalla procedura guidata.

15. Informazioni utili

15.1. Come faccio a testare la mia soluzione antivirus?

Per assicurarti che il tuo prodotto Bitdefender stia funzionando correttamente, ti consigliamo di utilizzare il test Eicar.

Il test Eicar ti consente di verificare l'efficacia della tua protezione antivirus, utilizzando un file sicuro appositamente sviluppato a tale scopo.

Per testare la tua soluzione antivirus, segui questi passaggi:

1. Scarica il test dalla pagina web ufficiale dell'organizzazione EICAR http://www.eicar.org/.
2. Clicca sull'opzione **Anti-Malware Testfile**.
3. Clicca su **Download** nel menu a sinistra.
4. Ora dalla tabella **Download area using the standard protocol http**, clicca sul file di test **eicar.com**.
5. Sarai avvisato che la pagina a cui stai cercando di accedere contiene il file sospetto EICAR-Test-File (in realtà NON è un virus).

   Cliccando sull'opzione **Conosco i rischi, quindi prosegui**, il test sarà scaricato e comparirà una finestra di Bitdefender per informarti che ha rilevato un virus.

   Clicca su **Maggiori dettagli** per scoprire altre informazioni su questa azione.

Se non ricevi alcun avviso da parte di Bitdefender, ti consigliamo di contattare il supporto tecnico di Bitdefender come descritto nella sezione *«Chiedere aiuto»* (p. 181).

15.2. Come posso rimuovere Bitdefender?

Se desideri rimuovere Bitdefender Internet Security, segui questi passaggi:

- Per **Windows XP**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova **Bitdefender** e seleziona **Rimuovi**.
  4. Clicca su **Rimuovi** e poi su **disinstalla COMPLETAMENTE Bitdefender**.
  5. Hai le seguenti opzioni:
     - L'opzione **Disinstalla e resta protetto** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi sarà installato sul sistema per proteggerti dai malware.

- L'opzione **Disinstalla senza la app** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi non sarà installato.

Seleziona l'opzione desiderata e clicca su **Avanti**.

6. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

- Per **Windows Vista** e **Windows 7**:

1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
2. Attendi per qualche istante, finché non compare l'elenco del software installato.
3. Trova **Bitdefender** e seleziona **Disinstalla**.
4. Clicca su **Disinstalla** e poi su **disinstalla COMPLETAMENTE Bitdefender**.
5. Hai le seguenti opzioni:
   - L'opzione **Disinstalla e resta protetto** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi sarà installato sul sistema per proteggerti dai malware.
   - L'opzione **Disinstalla senza la app** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi non sarà installato.

   Seleziona l'opzione desiderata e clicca su **Avanti**.
6. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

- Per **Windows 8**:

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Seleziona **Bitdefender Internet Security** e clicca su **Disinstalla**.
4. Clicca su **Disinstalla** e poi su **disinstalla COMPLETAMENTE Bitdefender**.
5. Hai le seguenti opzioni:
   - L'opzione **Disinstalla e resta protetto** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi sarà installato sul sistema per proteggerti dai malware.
   - L'opzione **Disinstalla senza la app** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi non sarà installato.

   Seleziona l'opzione desiderata e clicca su **Avanti**.
6. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

Nota
Bitdefender Virus Scanner 60 secondi è un'applicazione gratuita che utilizza una tecnologia di scansione in-the-cloud per rilevare programmi dannosi ed eventuali minacce in meno di 60 secondi.

15.3. Come posso mantenere protetto il sistema dopo aver disinstallato Bitdefender?

Durante il processo di rimozione di Bitdefender Internet Security, puoi utilizzare l'opzione **disinstalla e resta protetto**. Selezionando questa opzione, Bitdefender Virus Scanner 60 secondi sarà installato sul tuo sistema.

Bitdefender Virus Scanner 60 secondi è un'applicazione gratuita che utilizza una tecnologia di scansione in-the-cloud per rilevare programmi dannosi ed eventuali minacce in meno di 60 secondi.

Puoi continuare a utilizzare l'applicazione anche se reinstalli Bitdefender o se installi qualsiasi altro programma antivirus sul sistema.

Se desideri rimuovere Bitdefender Virus Scanner 60 secondi, segui questi passaggi:

- Per **Windows XP**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova **Bitdefender Virus Scanner 60 secondi** e seleziona **Rimuovi**.
  4. Seleziona **Disinstalla** al passaggio successivo e attendi la fine del processo.
- Per **Windows Vista** e **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova **Bitdefender Virus Scanner 60 secondi** e seleziona **Disinstalla**.
  4. Seleziona **Disinstalla** al passaggio successivo e attendi la fine del processo.
- Per **Windows 8**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Seleziona **Bitdefender Virus Scanner 60 secondi** e clicca su **Disinstalla**.
  4. Seleziona **Disinstalla** al passaggio successivo e attendi la fine del processo.

15.4. Come posso spegnere automaticamente il computer al termine della scansione?

Bitdefender offre diverse attività di scansione che puoi utilizzare per assicurarti che il tuo sistema sia privo di malware. Eseguire una scansione dell'intero sistema potrebbe richiedere molto tempo in base alla propria configurazione hardware e software.

Per questo motivo, Bitdefender ti consente di configurare Bitdefender per spegnere il sistema al termine della scansione.

Considera questo esempio: hai finito di lavorare al computer e vuoi andare a riposare. Ti piacerebbe che Bitdefender eseguisse una scansione antimalware sull'intero sistema.

Ecco come impostare Bitdefender per spegnere il sistema al termine della scansione:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Gestisci scansioni** dal menu a tendina.
3. Clicca su **Nuova attività personalizzata** per inserire un nome per la scansione e selezionare i percorsi da controllare.
4. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**.
5. Clicca su **OK** per salvare le modifiche e chiudere la finestra.
6. Scegli di spegnere il computer al termine della scansione, se non venisse rilevata alcuna minaccia.
7. Clicca su **Avvia Scansione**.

Se non vengono rilevate minacce, il computer si spegnerà.

Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo. Per ulteriori informazioni, fare riferimento a «*Procedura guidata scansione antivirus*» (p. 85).

15.5. Come posso configurare Bitdefender per usare una connessione a Internet tramite proxy?

Se il tuo computer si collega a Internet tramite un server proxy, devi configurare Bitdefender con le impostazioni del proxy. Normalmente Bitdefender rileva automaticamente e importa le impostazioni proxy dal sistema.

Importante

Le connessioni Internet domestiche normalmente non usano un server proxy. Come regola empirica, quando gli aggiornamenti non funzionano, controlla e configura le

impostazioni di connessione proxy del tuo programma di Bitdefender. Se Bitdefender può essere aggiornato, allora è configurato correttamente per connettersi a Internet.

Per gestire le impostazioni del proxy, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Generali**.
4. Nella finestra **Impostazioni generali**, seleziona la scheda **Avanzate**.
5. Attiva l'uso del proxy cliccando sull'interruttore.
6. Clicca sul collegamento **Gestione proxy**.
7. Ci sono due opzioni per determinare le impostazioni proxy:
   - **Importa le impostazioni del proxy dal browser predefinito** - le impostazioni del proxy dell'utente attuale, estratte dal browser predefinito. Se il server proxy richiede un nome utente e una password, devi indicarli nei rispettivi campi.

     Nota
     Bitdefender può importare le impostazioni del proxy dai browser più diffusi, incluso le ultime versioni di Internet Explorer, Mozilla Firefox e Opera.

   - **Impostazioni proxy personalizzate** - le impostazioni proxy che puoi configurare direttamente. Le seguenti impostazioni devono essere specificate:
     - **Indirizzo** - inserisci l'indirizzo IP del server proxy.
     - **Porta** - inserisci la porta che Bitdefender utilizza per connettersi al server proxy.
     - **Nome utente** - inserisci un nome utente riconosciuto dal proxy.
     - **Password** - inserisci la password dell'utente già specificato in precedenza.
8. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Bitdefender userà le impostazioni del proxy disponibili finché non riesce a connettersi a Internet.

15.6. Sto usando una versione di Windows a 32 o 64 bit?

Per scoprire se hai un sistema operativo a 32 o 64 bit, segui questi passaggi:

- Per **Windows XP**:
  1. Clicca su **Start**.
  2. Individua **Risorse del computer** nel menu **Start**.
  3. Clicca con il pulsante destro su **Risorse del computer** e seleziona **Proprietà**.

4. Se vedi l'opzione **x64 Edition** indicata sotto la voce **Sistema**, stai usando una versione a 64 bit di Windows XP.

   Se non vedi l'opzione **x64 Edition**, stai usando una versione di XP a 32 bit.

- Per **Windows Vista** e **Windows 7**:

  1. Clicca su **Start**.
  2. Individua **Risorse del computer** nel menu **Start**.
  3. Clicca con il pulsante destro su **Computer** e seleziona **Proprietà**.
  4. Vai in **Sistema** per verificare le informazioni sul tuo sistema.

- Per **Windows 8**:

  1. Dal menu Start di Windows, localizza l'opzione **Computer** (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona con il pulsante destro.
  2. Seleziona **Proprietà** nel menu inferiore.
  3. Controlla in **Sistema** per verificare il tipo di sistema.

15.7. Come posso visualizzare gli elementi nascosti in Windows?

Questi passaggi sono utili nel caso in cui tu debba occuparti di un malware per trovare e rimuovere i file infetti, che potrebbero essere nascosti.

Segui questi passaggi per mostrare gli elementi nascosti in Windows:

1. Clicca su **Start** e poi seleziona **Pannello di controllo**.

   In **Windows 8**: dal menu Start, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nel menu Start) e clicca sulla sua icona.
2. Seleziona **Opzioni cartella**.
3. Vai alla scheda **Visualizza**.
4. Seleziona **Mostra contenuto delle cartelle di sistema** (solo per Windows XP).
5. Seleziona **Mostra file e cartelle nascoste**.
6. Deseleziona **Nascondi estensioni per i file conosciuti**.
7. Deseleziona **Nascondi file protetti del sistema operativo**.
8. Clicca su **Applica** e poi su **OK**.

15.8. Come posso rimuovere le altre soluzioni di sicurezza?

La ragione principale per usare una soluzione di sicurezza è garantire la protezione e la sicurezza dei tuoi dati. Ma cosa succede quando si ha più di un prodotto di sicurezza sullo stesso sistema?

Usando più di una soluzione di sicurezza sullo stesso computer, il sistema diventa instabile. Il programma d'installazione di Bitdefender Internet Security rileva automaticamente altri programmi di sicurezza e ti offre la possibilità di disinstallarli.

Se non hai rimosso le altre soluzioni di sicurezza durante l'installazione iniziale, segui questi passaggi:

- Per **Windows XP**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Rimuovi**.
  4. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
- Per **Windows Vista** e **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  4. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
- Per **Windows 8**:
  1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
  3. Attendi per qualche istante, finché non compare l'elenco del software installato.
  4. Trova il nome del programma che desideri rimuovere e seleziona **Disinstalla**.
  5. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

Se non dovessi riuscire a rimuovere le altre soluzioni di sicurezza dal tuo sistema, cerca uno strumento di disinstallazione nel sito web del venditore o contattalo direttamente per ricevere le istruzioni di disinstallazione.

15.9. Come posso usare il Ripristino di sistema in Windows?

Se non riesci ad avviare il computer in modalità normale, puoi avviarlo in modalità provvisoria e usare il Ripristino configurazione di sistema per ripristinare il computer a una configurazione precedente avviabile senza errori.

Per eseguire il Ripristino configurazione di sistema, devi accedere a Windows come amministratore.

Per usare il Ripristino configurazione di sistema, segui questi passaggi:

- Per **Windows XP**:
  1. Avvia Windows in modalità provvisoria.
  2. Segui questo percorso dal menu Start di Windows: **Start → Tutti i programmi → Utilità di sistema → Ripristino configurazione di sistema**.
  3. Nella pagina del **Ripristino di configurazione di sistema**, seleziona **Ripristina uno stato precedente del computer** e poi clicca su Avanti.
  4. Segui i passaggi della procedura guidata e dovresti poter riavviare il sistema in modalità normale.
- Per **Windows Vista** e **Windows 7**:
  1. Avvia Windows in modalità provvisoria.
  2. Segui questo percorso dal menu Start di Windows: **Tutti i programmi → Accessori → Utilità di sistema → Ripristino configurazione di sistema**.
  3. Segui i passaggi della procedura guidata e dovresti poter riavviare il sistema in modalità normale.
- Per **Windows 8**:
  1. Avvia Windows in modalità provvisoria.
  2. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
  3. Seleziona **Ripristino** e poi **Apri Ripristino configurazione di sistema**.
  4. Segui i passaggi della procedura guidata e dovresti poter riavviare il sistema in modalità normale.

15.10. Come posso riavviare in modalità provvisoria?

La modalità provvisoria è una modalità operativa diagnostica, usata principalmente per risolvere problemi che affliggono il normale uso di Windows. Problemi quali conflitti di driver o virus, impediscono a Windows di avviarsi regolarmente. In modalità provvisoria solo poche applicazioni funzionano e Windows carica soltanto i driver e le componenti di base del sistema operativo. Ecco perché la maggior parte

dei virus sono inattivi usando Windows in modalità provvisoria e possono essere rimossi facilmente.

Per avviare Windows in modalità provvisoria:

1. Riavvia il computer.
2. Premi più volte il tasto **F8** prima del lancio di Windows per accedere al menu di avvio.
3. Seleziona **Modalità provvisoria** nel menu di avvio o **Modalità provvisoria con supporto di rete** se desideri avere l'accesso a Internet.
4. Premi **Invio** e attendi il caricamento di Windows in modalità provvisoria.
5. Questo processo termina con un messaggio di conferma. Clicca su **OK** per confermare.
6. Per avviare Windows normalmente, riavvia semplicemente il sistema.

Gestire la propria sicurezza

16. Protezione antivirus

Bitdefender protegge il tuo computer da ogni tipo di minaccia malware (virus, Trojan, spyware, rootkit e altro).La protezione offerta da Bitdefender è divisa in due categorie:

- Scansione all'accesso - Impedisce che nuove minacce malware entrino nel tuo sistema.Ad esempio, Bitdefender esaminerà un documento Word, quando sarà aperto, e un'e-mail, quando verrà ricevuta.

  La scansione all'accesso garantisce una protezione in tempo reale contro i malware, essendo una componente essenziale di ogni programma di sicurezza informatica.

  Importante
  Per impedire ai virus di infettare il tuo computer, tieni attivata la **Scansione all'accesso**.

- Scansione su richiesta - Permette di rilevare e di rimuovere malware già residenti nel tuo sistema.Si tratta della classica scansione antivirus avviata dall'utente. Si sceglie quale unità, cartella o file Bitdefender deve controllare e Bitdefender li esamina, su richiesta.

  Con la Scansione automatica attivata, non vi è alcun bisogno di eseguire manualmente le scansioni alla ricerca di malware.La Scansione automatica controllerà il tuo computer più volte, prendendo tutte le azioni opportune se dovesse rilevare malware.La Scansione automatica si avvia solo quando ci sono abbastanza risorse di sistema disponibili per non rallentare il computer.

Bitdefender controlla automaticamente ogni supporto rimovibile che è collegato al computer per assicurarti di accedervi in sicurezza.Per ulteriori informazioni, fare riferimento a «*Scansione automatica di supporti rimovibili*» (p. 88).

Gli utenti più esperti possono configurare le eccezioni della scansione, se non desiderano controllare determinati file o estensioni.Per ulteriori informazioni, fare riferimento a «*Configurare le eccezioni della scansione*» (p. 90).

Quando rileva un virus o un malware, Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto, ricostruendo il file originale.Questa operazione si riferisce alla disinfezione.I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione.Per ulteriori informazioni, fare riferimento a «*Gestire i file in quarantena*» (p. 92).

Se il tuo computer è stato infettato da un malware, fai riferimento a «*Rimuovere malware dal sistema*» (p. 171).Per aiutarti a ripulire il tuo computer dai malware che non possono essere rimossi dal sistema operativo Windows, Bitdefender ti offre una Modalità soccorso.Si tratta di un ambiente sicuro, realizzato specificatamente per la rimozione dei malware, che ti consente di avviare il tuo computer in modo

indipendente da Windows.Quando il computer parte in Modalità soccorso, i malware di Windows non sono attivi, semplificando così la loro rimozione.

Per proteggerti da applicazioni sconosciute e pericolose, Bitdefender utilizza Active Virus Control, una tecnologia euristica avanzata, che monitora continuamente le applicazioni in esecuzione sul sistema.Active Virus Control blocca automaticamente le applicazioni che mostrano un comportamento simile ai malware per impedirgli di danneggiare il computer.Occasionalmente, applicazioni legittime potrebbero essere bloccate. In questo caso, puoi configurare Active Virus Control per non bloccare queste applicazioni di nuovo creando delle regole di eccezione.Per altre informazioni, fai riferimento a «*Active Virus Control*» (p. 93).

Molte forme di malware sono realizzate per infettare sistemi sfruttando le loro vulnerabilità, come la mancanza di aggiornamenti del sistema operativo o la presenza di applicazioni datate.Bitdefender ti aiuta a identificare e risolvere facilmente le vulnerabilità del sistema per rendere il tuo computer più sicuro da malware e hacker.Per ulteriori informazioni, fare riferimento a «*Risolvere le vulnerabilità del sistema*» (p. 95).

16.1. Scansione all'accesso (protezione in tempo reale)

Bitdefender fornisce una continua protezione in tempo reale contro un ampio spettro di minacce malware mediante la scansione di tutti i file utilizzati, le e-mail e le comunicazioni tramite programmi di chat (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Le impostazioni predefinite della protezione in tempo reale assicurano una buona protezione contro i malware, con un impatto minore sulle prestazioni di sistema.Puoi modificare facilmente le impostazioni della protezione in tempo reale in base alle tue necessità passando a uno dei livelli di protezione predefiniti.O, se sei un utente avanzato, puoi configurare le impostazioni della scansione in ogni dettaglio, creando un livello di protezione personalizzato.

16.1.1. Attivare o disattivare la protezione in tempo reale

Per attivare o disattivare la protezione antimalware in tempo reale, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
5. Clicca sull'interruttore per attivare o disattivare la scansione all'accesso.
6. Se vuoi disattivare la protezione in tempo reale, comparirà una finestra di avviso.Devi confermare la tua scelta selezionando dal menu per quanto tempo

desideri disattivare la protezione in tempo reale. Puoi disattivarla durante 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.La protezione in tempo reale si attiverà automaticamente allo scadere del tempo indicato.

Avvertimento

È una questione di sicurezza piuttosto importante. Si consiglia di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale non è attiva, non si è protetti dalle minacce malware.

16.1.2. Impostare il livello di protezione in tempo reale

Il livello di protezione in tempo reale definisce le impostazioni della scansione per la protezione in tempo reale.Puoi modificare facilmente le impostazioni della protezione in tempo reale in base alle tue necessità passando a uno dei livelli di protezione predefiniti.

Per impostare il livello di protezione in tempo reale, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
5. Trascina il pulsante scorrevole lungo la barra per impostare il livello di protezione desiderato.Usa la descrizione sul lato destro della barra per selezionare il livello di protezione che si adatta meglio alle tue necessità di sicurezza.

16.1.3. Configurare le impostazioni della protezione in tempo reale

Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender.Puoi configurare le impostazioni della protezione in tempo reale in ogni dettaglio, creando un livello di protezione personalizzato.

Per configurare le impostazioni della protezione in tempo reale, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
5. Clicca su **Personalizzato**.
6. Configura le impostazioni della scansione come necessario.
7. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- Se non conosci alcuni termini, verificali nel glossario.Puoi anche trovare informazioni utili cercando su Internet.
- **Opzione di scansione per i file a cui accedi.** Puoi impostare Bitdefender per eseguire la scansione su tutti i file a cui si accede o solo sulle applicazioni (file dei programmi).Controllare tutti i file a cui si ha avuto accesso fornisce una protezione migliore, mentre controllare solo le applicazioni può essere usato per ottenere prestazioni migliori.

  Di norma, sia le cartelle locali sia quelle condivise in rete sono soggette a una scansione all'accesso.Per migliorare le prestazioni del sistema, è possibile escludere i percorsi di rete dalla scansione all'accesso.

  Le applicazioni (o programmi) sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file.Questa categoria include le seguenti estensioni dei file:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Controlla il contenuto degli archivi.** La scansione degli archivi è un processo lento e che richiede molte risorse, che quindi non è consigliato per la protezione in tempo reale.Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema.I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale.

  Se decidi di utilizzare questa opzione, puoi impostare un limite di dimensione massima degli archivi da controllare con la scansione all'accesso.Seleziona la casella corrispondente e digita la dimensione massima dell'archivio (in MB).

- **Opzioni di scansione per il traffico e-mail, web e chat.** Per impedire il download di malware sul tuo PC, Bitdefender controlla automaticamente i seguenti punti d'entrata per i malware:
  - ▶ E-mail in entrata e in uscita
  - ▶ Traffico web
  - ▶ File ricevuti via Yahoo! Messenger

  Controllare il traffico web potrebbe rallentare leggermente la navigazione web, ma impedirà l'accesso a ogni malware tramite Internet o i download.

  Sebbene non consigliabile, puoi disattivare la scansione antivirus per e-mail, web o messaggistica istantanea, in modo da migliorare le prestazioni del sistema.Disattivando le opzioni di scansione corrispondenti, le e-mail e i file ricevuti o scaricati da Internet non saranno controllati, consentendo ai file infetti di essere salvati sul computer.Questa non è una minaccia particolarmente importante, perché la protezione in tempo reale bloccherà i malware quando si accede ai file infetti (apertura, spostamento, copiatura o esecuzione).
- **Controlla i settori di avvio.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido.Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer.Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
- **Controlla solo i file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Scansione per keylogger.** Seleziona questa opzione per eseguire una scansione del sistema alla ricerca di applicazioni keylogger.I keylogger registrano ciò che digiti sulla tastiera per poi inviare queste informazioni tramite Internet a un hacker. L'hacker può trovare informazioni sensibili nei dati rubati, come numeri e password di un conto corrente, e usarle per ottenere benefici personali.

Azioni intraprese su malware rilevati

Puoi configurare le azioni intraprese dalla protezione in tempo reale.

Per configurare tali azioni, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
5. Clicca su **Personalizzato**.
6. Configura le impostazioni della scansione come necessario.
7. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

In Bitdefender, la protezione in tempo reale può intraprendere le seguenti azioni:

Esegui azioni appropriate

Bitdefender intraprenderà le azioni consigliate in base al tipo di file rilevato:

- **File infetti.** File rilevati che corrispondono a firme malware infette nel database di firme malware di Bitdefender.Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto e di ricostruire il file originale.Questa operazione si riferisce alla disinfezione.

  I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione.I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione.Per ulteriori informazioni, fare riferimento a *«Gestire i file in quarantena»* (p. 92).

  Importante

  Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente maligno. In questi casi, il file infetto è eliminato dal disco.

- **File sospetti.** I file sono stati rilevati come sospetti dall'analisi euristica.I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione. Saranno messi in quarantena per impedire una potenziale infezione.

  Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori antimalware di Bitdefender.Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

- **Archivi contenenti file infetti.**

  - Gli archivi che contengono solo file infetti sono eliminati automaticamente.
  - Se un archivio contiene sia file puliti che infetti, Bitdefender tenterà di eliminare i file infetti a condizione che possa riformare l'archivio con i file puliti.Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Sposta i file in quarantena

Sposta i file infetti nella quarantena.I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione.Per ulteriori informazioni, fare riferimento a *«Gestire i file in quarantena»* (p. 92).

Nega l'accesso

Nel caso di individuazione di un file infetto, l’accesso al file verrà negato.

16.1.4. Ripristinare le impostazioni predefinite

Le impostazioni predefinite della protezione in tempo reale assicurano una buona protezione contro i malware, con un impatto minore sulle prestazioni di sistema.

Per ripristinare le impostazioni predefinite della protezione in tempo reale, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
5. Clicca su **Predefinito**.

16.2. Scansione su richiesta

L'obiettivo principale di Bitdefender è di mantenere il proprio computer privo di virus. Ciò avviene tenendo lontani i nuovi virus dal computer ed esaminando i messaggi e-mail e qualsiasi nuovo file scaricato o copiato sul sistema.

Esiste il rischio che un virus sia già contenuto nel tuo sistema, addirittura prima dell'installazione di Bitdefender. Questo è il motivo per cui suggeriamo di effettuare una scansione sul tuo computer alla ricerca di virus residenti dopo aver installato Bitdefender. Inoltre, è una buona idea effettuare frequentemente una scansione del computer, alla ricerca di virus.

La scansione su richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scansione e gli elementi da esaminare.Puoi eseguire la scansione del computer ogni volta che vuoi, avviando le attività predefinite o una tua scansione (attività definite dall'utente).Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale.

16.2.1. Autoscan

La scansione automatica è una scansione su richiesta che controlla in background tutti i dati alla ricerca di malware e intraprende azioni appropriate per ogni infezione rilevata.La Scansione automatica trova e utilizza gli intervalli di tempo in cui l'uso delle risorse di sistema scende sotto a una certa soglia per eseguire scansioni ricorrenti dell'intero sistema.

Vantaggi della Scansione automatica:

- L'impatto sul sistema è vicino allo zero.
- Eseguendo una prescansione dell'intero disco rigido, le future attività a richiesta saranno completate molto velocemente.
- La scansione all'accesso richiederà molto meno tempo.

Per attivare o disattivare la Scansione automatica, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca sull'interruttore per attivare o disattivare la funzione **Scansione aut.**

16.2.2. Controllare un file o una cartella alla ricerca di malware

Dovresti controllare i file e le cartelle ogni volta che sospetti che possano essere stati infettati.Clicca con il pulsante destro del mouse sul file o la cartella che desideri controllare, seleziona **Bitdefender** e poi **Controlla con Bitdefender**.Comparirà la procedura guidata scansione antivirus e ti guiderà attraverso il processo di scansione.Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.

16.2.3. Eseguire una Scansione veloce

QuickScan utilizza una scansione in-the-cloud per rilevare eventuali malware in esecuzione sul tuo sistema.In genere eseguire una Scansione veloce richiede meno di un minuto e usa una frazione delle risorse di sistema necessarie per una scansione standard.

Per eseguire una Scansione veloce, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Scansione veloce** dal menu a tendina.
3. Segui la procedura guidata della scansione antivirus per completare la scansione.Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

16.2.4. Eseguire una scansione del sistema

La Scansione del sistema esamina l'intero computer per rilevare tutti i tipi di malware che minacciano la sua sicurezza, come virus, spyware, adware, rootkit e altri.Se hai disattivato la Scansione automatica, si consiglia di eseguire una Scansione del sistema almeno una volta alla settimana.

Nota

Poiché la **Scansione del sistema** esegue una scansione accurata dell'intero sistema, potrebbe richiedere un po' di tempo. Pertanto, si consiglia di eseguire questa operazione quando non si utilizza il computer.

Prima di eseguire una Scansione del sistema, si consiglia di:

- Assicurarsi che le firme malware di Bitdefender siano aggiornate. Eseguire la scansione con un database delle firme obsoleto può impedire a Bitdefender di rilevare nuovi malware, trovati dopo l'ultimo aggiornamento.Per ulteriori informazioni, fare riferimento a «*Mantenere aggiornato Bitdefender*» (p. 38).
- Chiudere tutti i programmi aperti.

Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale.Per ulteriori informazioni, fare riferimento a «*Configurare una scansione personale*» (p. 82).

Per eseguire una Scansione del sistema, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Scansione sistema** dal menu a tendina.
3. Segui la procedura guidata della scansione antivirus per completare la scansione.Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati.Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

16.2.5. Configurare una scansione personale

Per configurare una scansione antimalware in ogni dettaglio e poi eseguirla, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Gestisci scansioni** dal menu a tendina.
3. Clicca su **Nuova attività personalizzata** per inserire un nome per la scansione e selezionare i percorsi da controllare.
4. Se desideri configurare le opzioni di scansione in ogni dettaglio, seleziona la scheda **Avanzate**.Comparirà una nuova finestra.Attenersi alla seguente procedura:
   a. Puoi configurare facilmente le opzioni di scansione, impostando il livello della scansione. Trascina il pulsante scorrevole lungo la barra per impostare il livello di scansione desiderato.Usa la descrizione sul lato destro della barra per identificare il livello di scansione che si adatta meglio alle tue necessità.

      Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender.Per configurare in ogni dettaglio le opzioni della scansione, clicca su **Personalizzato**. Al termine di questa sezione trovi maggiori informazioni al riguardo.

   b. Puoi anche configurare queste opzioni generali:

- **Esegui l'attività con bassa priorità .** Diminuisce la priorità del processo di scansione. Consentirai ad altri programmi di essere più veloci, incrementando il tempo necessario per terminare il processo di scansione.
- **Minimizza la Procedura guidata di scansione nell'area di stato .** Minimizza la finestra di scansione nell'area di stato. Clicca due volte sull'icona di Bitdefender per riaprirlo.
- Specifica l'azione da intraprendere se non venisse rilevata alcuna minaccia.

c. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

5. Clicca su **Elenco** se desideri impostare un elenco per la tua scansione.Usa l'interruttore per attivare o disattivare l'**Elenco**.Seleziona una delle opzioni corrispondenti per impostare un elenco:
   - All'avvio del sistema
   - Una volta
   - Periodicamente
6. Clicca su **Inizia la scansione** e segui la procedura guidata della scansione antivirus per completare la scansione.In base ai percorsi da controllare, la scansione potrebbe richiedere un po' di tempo.Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.
7. Se lo desideri, puoi eseguire nuovamente una scansione personale precedente cliccando sulla rispettiva voce nell'elenco disponibile.

Informazioni sulle opzioni di scansione

Questa informazione potrebbe esserti utile:

- Se non conosci alcuni termini, verificali nel glossario.Puoi anche trovare informazioni utili cercando su Internet.
- **Controlla file.** Puoi impostare Bitdefender per eseguire la scansione su tutti i file o solo sulle applicazioni (file dei programmi).Controllare tutti i file ti garantisce una protezione migliore, mentre controllare solo le applicazioni può essere utile per eseguire una scansione più veloce.

  Le applicazioni (o programmi) sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file.Questa categoria include le seguenti estensioni dei file:386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg;

msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Opzioni di scansione per archivi.** Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema.I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale.Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere ogni minaccia potenziale, anche se non è immediata.

  Nota
  La scansione dei file archiviati incrementa la durata totale della scansione e richiede più risorse di sistema.

- **Controlla i settori di avvio.** È possibile impostare Bitdefender per controllare i settori di boot del disco rigido.Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer.Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.
- **Controlla la memoria.** Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.
- **Controlla il registro.** Seleziona questa opzione per controllare le chiavi del registro.Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione delle componenti del sistema operativo Windows, oltre a quelle delle applicazioni installate.
- **Controlla cookie.** Seleziona questa opzione per controllare i cookie memorizzati dai browser sul tuo computer.
- **Controlla solo i file nuovi e modificati.** Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.
- **Ignora keylogger commerciali.** Seleziona questa opzione se hai installato e utilizzi un programma keylogger commerciale sul tuo computer.I keylogger commerciali sono programmi legittimi di monitoraggio del computer la cui funzione elementare è registrare tutto ciò che viene digitato sulla tastiera.
- **Scansione per rootkit.** Seleziona questa opzione per eseguire una scansione alla ricerca di rootkit e oggetti nascosti usando tale software.

16.2.6. Procedura guidata scansione antivirus

Ogni volta che si inizia una scansione su richiesta (ad esempio, cliccando con il pulsante destro su una cartella, selezionando Bitdefender e poi **Controlla con Bitdefender**), apparirà la procedura guidata Scansione antivirus di Bitdefender.Segui la procedura guidata per completare la scansione.

Nota

Se non compare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per un'esecuzione in background.Cerca l'icona  di avanzamento della scansione nell'area di stato.Clicca sull'icona per aprire la finestra di scansione e visualizzarne l'avanzamento.

Fase 1 - Eseguire la scansione

Bitdefender inizierà la scansione degli oggetti selezionati.Puoi vedere in tempo reale informazioni sulle statistiche e sullo stato della scansione (incluso il tempo trascorso, una stima del tempo rimasto e il numero di minacce rilevate).Per visualizzare altri dettagli, clicca sul collegamento **Mostra altro**.

Attendi che Bitdefender termini la scansione.La durata del processo dipende dalla complessità della scansione.

Arrestare o mettere in pausa la scansione. Puoi fermare la scansione in qualsiasi momento, cliccando su **Ferma e Sì** Verrete portati all'ultimo passo dell'assistente.Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione, dovrai cliccare su **Riprendi**.

Archivi protetti da password. Quando viene rilevato un archivio protetto da password, in base alle impostazioni di scansione, ti potrebbe essere richiesto d'inserire la password.Gli archivi protetti da password non possono essere esaminati a meno di non fornire la password.Sono disponibili le seguenti opzioni:

- **Password.** Se desideri che Bitdefender controlli l'archivio, seleziona questa opzione e digita la password.Se non si conosce la password, scegliere un'altra opzione.
- **Non chiedere una password e ignorare questo oggetto per la scansione.** Seleziona questa opzione per non controllare questo archivio.
- **Ignora tutti gli elementi protetti da password senza controllarli.** Seleziona questa opzione se non desideri ricevere ulteriori domande sugli archivi protetti da password.Bitdefender non sarà in grado di controllarli, ma saranno annotati nel registro della scansione.

Seleziona l'opzione desiderata e clicca su **OK** per continuare la scansione.

Fase 2 - Scegliere le azioni

Al termine della scansione, ti sarà chiesto di scegliere quali azioni intraprendere sui file rilevati, se presenti.

Nota

Eseguendo una scansione veloce o una scansione completa del sistema, Bitdefender intraprenderà automaticamente le azioni consigliate sui file rilevati durante la scansione.Se vi sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati.Clicca sul collegamento corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Puoi scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.Una o più delle seguenti opzioni possono comparire nel menu:

Esegui azioni appropriate

Bitdefender intraprenderà le azioni consigliate in base al tipo di file rilevato:

- **File infetti.** File rilevati che corrispondono a firme malware infette nel database di firme malware di Bitdefender.Bitdefender tenterà automaticamente di rimuovere il codice malware dal file infetto e di ricostruire il file originale.Questa operazione si riferisce alla disinfezione.

  I file che non possono essere disinfettati, vengono messi in quarantena per contenere l'infezione.I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione.Per ulteriori informazioni, fare riferimento a «*Gestire i file in quarantena*» (p. 92).

  Importante

  Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente maligno. In questi casi, il file infetto è eliminato dal disco.

- **File sospetti.** I file sono stati rilevati come sospetti dall'analisi euristica.I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione. Saranno messi in quarantena per impedire una potenziale infezione.

  Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori antimalware di Bitdefender.Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

- **Archivi contenenti file infetti.**

- Gli archivi che contengono solo file infetti sono eliminati automaticamente.
- Se un archivio contiene sia file puliti che infetti, Bitdefender tenterà di eliminare i file infetti a condizione che possa riformare l'archivio con i file puliti.Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Elimina
Rimuove i file rilevati dal disco.

Se i file infetti sono memorizzati in un archivio con altri file puliti, Bitdefender tenterà di eliminarli e di riformare l'archivio con i file puliti.Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Non fare nulla
Sui file rilevati non sarà eseguita alcuna azione.Dopo che la scansione è stata completata, potrai aprire il registro della scansione per visualizzare le informazioni su questi file.

Clicca su **Continua** per applicare le azioni specificate.

Fase 3 - Sommario

Quando Bitdefender termina la risoluzione dei problemi, i risultati della scansione compariranno in una nuova finestra.Se desideri ricevere informazioni esaurienti sul processo di scansione, clicca su **Registro** per visualizzare il registro della scansione.

Clicca su **Chiudi** per chiudere la finestra.

Importante

Nella maggior parte dei casi Bitdefender disinfetta con successo i file infetti che rileva o isola l'infezione.Tuttavia, ci sono problemi che non possono essere risolti automaticamente.Se richiesto, riavvia il sistema per completare il processo di pulizia.Per maggiori informazioni e istruzioni su come rimuovere i malware manualmente, fai riferimento a «*Rimuovere malware dal sistema*» (p. 171).

16.2.7. Controllare i registri di scansione

Ogni volta che viene eseguita una scansione, viene creato un registro di scansione e Bitdefender memorizza i problemi rilevati nella finestra Panoramica antivirus.Il registro di scansione contiene informazioni dettagliate sul processo di scansione registrato, sull'obiettivo della scansione, le minacce individuate e le azioni intraprese su queste minacce.

Puoi aprire il registro della scansione direttamente dalla procedura guidata di scansione, una volta completata, cliccando su **Registro**.

Per controllare un registro di scansione o qualsiasi infezione rilevata in un secondo momento, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Eventi antivirus**, seleziona la scheda **Scansione Virus**. Qui puoi trovare tutti gli eventi della scansione antimalware, incluso le minacce rilevate dalla scansione all'accesso, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.
5. Nell'elenco degli eventi, puoi controllare quali scansioni sono state eseguite di recente.Clicca su un evento per visualizzare maggiori dettagli al riguardo.
6. Per aprire il registro della scansione, clicca su **Guarda registro**.

16.3. Scansione automatica di supporti rimovibili

Bitdefender rileva automaticamente quando si collega un dispositivo di archiviazione rimovibile al computer e ne esegue una scansione in background.Questa operazione è consigliata per impedire che virus e altri malware infettino il computer.

I dispositivi rilevati rientrano in una di queste categorie:

- CD/DVD
- Dispositivi di archiviazione USB, ad esempio chiavette e dischi rigidi esterni
- Unità di rete (remote) mappate

Puoi configurare la scansione automatica separatamente per ciascuna categoria di dispositivi di memorizzazione.Di norma la scansione automatica delle unità di rete mappate è disattivata.

16.3.1. Come funziona?

Quando rileva un dispositivo rimovibile di archiviazione, Bitdefender inizia la scansione antimalware in background (a condizione che la scansione automatica sia attivata per quel tipo di dispositivo).Un'icona di scansione di Bitdefender comparirà nell'area di stato.Clicca sull'icona per aprire la finestra di scansione e visualizzarne l'avanzamento.

Se l'Autopilot è attivato, non dovrai preoccuparti della scansione.La scansione sarà solo registrata e le relative informazioni saranno disponibili nella finestra Eventi.

Se l'Autopilot è disattivato:

1. Sarai avvisato attraverso una finestra pop-up che un nuovo dispositivo è stato rilevato ed è in fase di scansione.

2. Nella maggior parte dei casi, Bitdefender rimuove automaticamente i malware rilevati o isola i file infetti mettendoli in quarantena.Se dopo la scansione ci sono minacce non risolte, ti sarà chiesto quali azioni intraprendere al riguardo.

Nota

Tieni presente che nessuna azione può essere intrapresa su file sospetti rilevati su CD/DVD. Allo stesso modo, non può essere intrapresa alcuna azione su file sospetti rilevati su unità di rete mappate, se non si dispone dei privilegi appropriati.

3. Al termine della scansione, la finestra dei risultati della scansione ti informa se puoi accedere tranquillamente ai file sui supporti rimovibili.

Queste informazioni potrebbero esserti utili:

- Fai attenzione a usare un CD/DVD infettato da malware, perché i malware non possono essere rimossi dal disco (è un supporto di sola lettura).Assicurati che la protezione in tempo reale sia attivata per impedire la diffusione di malware nel tuo sistema.Si consiglia di copiare tutti i dati importanti dal disco al proprio sistema e poi eliminare il disco.
- In alcuni casi, Bitdefender può non essere in grado di rimuovere i malware da file specifici a causa di vincoli legali o tecnici. Un esempio sono i file archiviati con una tecnologia proprietaria (questo perché l'archivio non può essere ricreato correttamente).

  Per sapere come comportarti con i malware, consulta «*Rimuovere malware dal sistema*» (p. 171).

16.3.2. Gestire la scansione di supporti rimovibili

Per gestire la scansione automatica dei supporti rimovibili, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Eccezioni**.

Per la migliore protezione, si consiglia di attivare la Scansione automatica per tutte le tipologie di dispositivi rimovibili di archiviazione.

Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione.Se vengono rilevati file infetti, Bitdefender proverà a disinfettarli (rimuovere il codice malware) o a spostarli in quarantena. Se entrambe le azioni falliscono, la procedura guidata della scansione antivirus ti permetterà di specificare altre azioni da intraprendere sui file infetti.Le opzioni di scansione sono standard e non puoi modificarle.

16.4. Configurare le eccezioni della scansione

Bitdefender consente di escludere determinati file, cartelle o estensioni di file dalla scansione. Questa funzione ha lo scopo di evitare interferenze con il tuo lavoro e può anche contribuire a migliorare le prestazioni del sistema.Le eccezioni devono essere utilizzate da utenti con conoscenze informatiche avanzate o altrimenti, si consiglia di seguire le raccomandazioni degli operatori di Bitdefender.

Puoi configurare le eccezioni da applicare solo alla scansione all'accesso o su richiesta, oppure a entrambe.Gli oggetti esclusi dalla scansione all'accesso non saranno esaminati, non importa se sono stati visitati da te o da un'applicazione.

Nota

Le eccezioni NON saranno applicate alla scansione contestuale.La scansione contestuale è un tipo di scansione su richiesta: clicca con il pulsante destro sul file o la cartella che desideri controllare e seleziona **Controlla con Bitdefender**.

16.4.1. Escludere file o cartelle dalla scansione

Per escludere determinati file o cartelle dalla scansione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Eccezioni**.
5. Attiva le eccezioni della scansione per i file usando l'interruttore corrispondente.
6. Clicca sul collegamento **File e cartelle escluse**.Nella finestra che compare, puoi gestire i file e le cartelle esclusi dalla scansione.
7. Aggiungi eccezioni seguendo questi passaggi:
   a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
   b. Clicca su **Sfoglia**, seleziona il file o la cartella che desideri escludere dalla scansione e quindi clicca su **OK**.In alternativa, puoi digitare (o copiare e incollare) il percorso del file o della cartella nello spazio apposito.
   c. Di norma, il file o la cartella selezionati sono esclusi dalla scansione all'accesso e da quella su richiesta. Per cambiare quando applicare l'eccezione, seleziona una delle altre opzioni.
   d. Clicca su **Aggiungi**.
8. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

16.4.2. Escludere estensioni di file dalla scansione

Se escludi un'estensione di un file dalla scansione, Bitdefender non controllerà più i file con tale estensione, indipendentemente dalla loro posizione nel computer.L'eccezione si applica anche ai file su supporti rimovibili, come CD, DVD, unità USB o di rete.

Importante
Usa la massima cautela nell'escludere le estensioni dalla scansione, perché tali estensioni possono rendere il computer vulnerabile ai malware.

Per escludere determinate estensioni dei file dalla scansione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Eccezioni**.
5. Attiva le eccezioni della scansione per i file usando l'interruttore corrispondente.
6. Clicca sul collegamento **Estensioni escluse**.Nella finestra che compare, puoi gestire le estensioni dei file escluse dalla scansione.
7. Aggiungi eccezioni seguendo questi passaggi:
   a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
   b. Inserisci le estensioni che vuoi escludere dalla scansione, separate da punto e virgola (;).Ecco un esempio:

      ```
      txt;avi;jpg
      ```

   c. Di norma, tutti i file con le estensioni indicate sono esclusi dalla scansione all'accesso e da quella su richiesta. Per cambiare quando applicare l'eccezione, seleziona una delle altre opzioni.
   d. Clicca su **Aggiungi**.
8. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

16.4.3. Gestire le eccezioni della scansione

Se le eccezioni della scansione configurata non sono più necessarie, si consiglia di eliminarle o disattivare le eccezioni della scansione.

Per gestire le eccezioni della scansione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.

3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Eccezioni**. Usa le opzioni nella sezione **File e cartelle** per gestire le eccezioni della scansione.
5. Per rimuovere o modificare le eccezioni della scansione, clicca su uno dei collegamenti disponibili.Procedi come segue:
   - Per rimuovere una voce dalla tabella, selezionala e clicca sul pulsante **Rimuovi**.
   - Per modificare una voce dalla tabella, cliccaci sopra due volte (o selezionala e clicca sul pulsante **Modifica**).Apparirà una nuova finestra dove potrai modificare l'estensione o il percorso da escludere e il tipo di scansione dal quale escluderlo, a seconda delle necessità. Esegui i cambiamenti necessari, poi clicca su **Modifica**.
6. Per disattivare le eccezioni, usa l'interruttore corrispondente.

16.5. Gestire i file in quarantena

Bitdefender isola i file infettati da malware che non può disinfettare e i file sospetti in un'area sicura chiamata quarantena.Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

Di norma, i file in quarantena sono inviati automaticamente ai laboratori di Bitdefender per essere analizzati dai ricercatori antimalware di Bitdefender.Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

Inoltre Bitdefender controlla i file in quarantena dopo ogni aggiornamento delle firme malware.I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Per controllare e gestire i file in quarantena, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Quarantena**.
5. I file in quarantena sono gestiti automaticamente da Bitdefender in base alle impostazioni di quarantena predefinite.Anche se non consigliato, puoi modificare le impostazioni della quarantena in base alle tue preferenze.

   Controlla nuovamente la quarantena dopo aggiornamento definizioni virus

   Mantieni questa opzione attivata per eseguire automaticamente la scansione dei file in quarantena dopo ogni aggiornamento delle definizioni dei virus.I file puliti vengono spostati automaticamente alla loro ubicazione originale.

Invia i file sospetti in quarantena per ulteriori analisi
Tieni questa opzione attivata per inviare automaticamente i file in quarantena ai laboratori di Bitdefender.I file campioni saranno analizzati dai ricercatori antimalware di Bitdefender.Se viene confermata la presenza di malware, viene rilasciata una firma per consentirne la rimozione.

Elimina i contenuti più vecchi di {30} giorni
Di norma, i file in quarantena più vecchi di 30 giorni sono eliminati automaticamente.Se vuoi modificare questo intervallo, digita un nuovo valore nel campo corrispondente.Per disattivare la rilevazione automatica dei vecchi file in quarantena, digita 0.

6. Per eliminare un file in quarantena, selezionalo e clicca sul pulsante **Elimina**.Se desideri ripristinare un file in quarantena alla sua ubicazione originale, selezionalo e clicca su **Ripristina**.

16.6. Active Virus Control

Active Virus Control di Bitdefender è una tecnologia di individuazione innovativa e proattiva che utilizza metodi euristici avanzati per rilevare nuove minacce potenziali in tempo reale.

Active Virus Control monitora continuamente le applicazioni in esecuzione sul computer, cercando azioni simili a malware. A ognuna viene assegnato un punteggio e per ogni processo viene poi assegnato un punteggio totale.Quando il punteggio totale di un processo raggiunge una certa soglia, il processo è considerato nocivo ed è bloccato automaticamente.

Se l'Autopilot è disattivato, sarai avvisato tramite una finestra pop-up sull'applicazione bloccata.Diversamente, l'applicazione sarà bloccata senza alcuna notifica.Puoi verificare quali applicazioni sono state rilevate da Active Virus Control nella finestra Eventi.

16.6.1. Verificare le applicazioni rilevate

Per verificare le applicazioni rilevate da Active Virus Control, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Eventi antivirus**, seleziona la scheda **Active Virus Control**.
5. Clicca su un evento per visualizzare maggiori dettagli al riguardo.
6. Se ti fidi dell'applicazione, puoi configurare Active Virus Control per non bloccarla più, cliccando su **Consenti e monitora**.Active Virus Control continuerà a monitorare le applicazioni escluse. Se un'applicazione esclusa viene rilevata a

eseguire attività sospette, l'evento semplicemente sarà registrato e notificato al cloud di Bitdefender come errore di rilevazione.

16.6.2. Attivare o disattivare Active Virus Control

Per attivare o disattivare Active Virus Control, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
5. Clicca sull'interruttore per attivare o disattivare Active Virus Control.

16.6.3. Impostare la protezione di Active Virus Control

Se vedi che Active Virus Control rileva spesso applicazioni legittime, devi impostare un livello di protezione più permissivo.

Per impostare la protezione di Active Virus Control, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Protezione**.
5. Assicurati che Active Virus Control sia attivato.
6. Trascina il pulsante scorrevole lungo la barra per impostare il livello di protezione desiderato.Usa la descrizione sul lato destro della barra per selezionare il livello di protezione che si adatta meglio alle tue necessità di sicurezza.

Nota
Se imposti il livello di protezione più elevato, Active Virus Control richiederà un minor numero di comportamenti simili a malware per segnalare un processo. Ciò comporterà un numero più elevato di applicazioni rilevate e, allo stesso tempo, a un aumento della probabilità di falsi positivi (applicazioni legittime rilevate come dannose).

16.6.4. Gestire i processi esclusi

Puoi configurare le regole delle eccezioni per le applicazioni di fiducia in modo che Active Virus Control non le blocchi se eseguono azioni simili a malware.Active Virus Control continuerà a monitorare le applicazioni escluse. Se un'applicazione esclusa viene rilevata a eseguire attività sospette, l'evento semplicemente sarà registrato e notificato al cloud di Bitdefender come errore di rilevazione.

Per gestire le eccezioni di Active Virus Control, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Eccezioni**.
5. Clicca sul collegamento **Processi esclusi**.Nella finestra che compare, puoi gestire le eccezioni del processo di Active Virus Control.

   Nota
   Le eccezioni relative ai processi si applicano anche al Sistema di rilevazione intrusioni incluso nel firewall di Bitdefender.

6. Aggiungi eccezioni seguendo questi passaggi:
   a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
   b. Clicca su **Sfoglia**, trova e seleziona l'applicazione che vuoi escludere e poi clicca su **OK**.
   c. Mantieni l'opzione **Consenti** selezionata per impedire ad Active Virus Control di bloccare l'applicazione.
   d. Clicca su **Aggiungi**.
7. Per rimuovere o modificare le eccezioni, procedi come segue:
   - Per rimuovere una voce dalla tabella, selezionala e clicca sul pulsante **Elimina**.
   - Per modificare una voce dalla tabella, cliccaci sopra due volte (o selezionala e clicca sul pulsante **Modifica**).Esegui i cambiamenti necessari, poi clicca su **Modifica**.
8. Salva le modifiche e chiudi la finestra.

16.7. Risolvere le vulnerabilità del sistema

Un passaggio importante nella protezione del computer contro hacker e applicazioni dannose è mantenere aggiornato il sistema operativo e le applicazioni che usi regolarmente.Dovresti anche considerare di disattivare le impostazioni di Windows che rendono il sistema più vulnerabile ai malware.Inoltre, per impedire accessi fisici non autorizzati al tuo computer, devi configurare password sicure (password che non possano essere facilmente indovinate) per ogni account di Windows.

Bitdefender offre due semplici modi per risolvere le vulnerabilità del tuo sistema:

- Puoi verificare le vulnerabilità del sistema e risolverle passaggio dopo passaggio usando la procedura guidata della **Scansione vulnerabilità**.

- Usando il monitoraggio automatico delle vulnerabilità, puoi controllare e risolvere le vulnerabilità rilevate nella finestra Eventi.

Ogni una o due settimane dovresti controllare e sistemare le vulnerabilità del sistema.

16.7.1. Controllare il sistema per rilevare vulnerabilità

Per sistemare le vulnerabilità del sistema usando la procedura guidata della Scansione vulnerabilità, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Scansione vulnerabilità** dal menu a tendina.
3. Segui la procedura guidata in sei passaggi per rimuovere le vulnerabilità dal sistema.Puoi esplorare la procedura guidata usando il pulsante **Avanti**. Per uscire dalla procedura guidata, clicca su **Annulla**.

   a. **Proteggi il PC**

      Seleziona le vulnerabilità da controllare.

   b. **Controllo problemi**

      Attendi che Bitdefender termini di controllare le vulnerabilità del tuo sistema.

   c. **Agg. Windows**

      Puoi vedere l'elenco degli aggiornamenti critici e non critici di Windows che non sono attualmente installati sul computer.Seleziona gli aggiornamenti che desideri installare.

      Per avviare l'installazione degli aggiornamenti selezionati, clicca su **Avanti**.L'installazione degli aggiornamenti potrebbe richiedere un po' di tempo e alcuni potrebbero richiedere anche un riavvio del sistema per completare l'installazione.Se necessario, riavvia il sistema al più presto.

   d. **Aggiornamenti applicazioni**

      Se un'applicazione non è aggiornata, clicca sul link fornito per scaricare la versione più recente.

   e. **Password non sicure**

      Puoi visualizzare l'elenco degli account di Windows configurati sul tuo computer e il livello di protezione che le loro password forniscono.

      Clicca su **Risolvi** per modificare le password non sicure.Puoi scegliere tra chiedere di cambiare la password al prossimo accesso o cambiare subito la password direttamente.Per avere una password sicura, utilizza una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

f. **Sommario**

Qui puoi visualizzare il risultato dell'operazione.

16.7.2. Usare il controllo automatico delle vulnerabilità

Bitdefender controlla regolarmente e in background il sistema alla ricerca di vulnerabilità, tenendo traccia dei problemi rilevati nella finestra Eventi.

Per verificare e sistemare i problemi rilevati, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Eventi** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Eventi antivirus**, seleziona la scheda **Vulnerabilità**.
5. Puoi visualizzare informazioni dettagliate sulle vulnerabilità del sistema rilevate.In base al problema, per risolvere una vulnerabilità specifica procedi come segue:
   - Se sono disponibili aggiornamenti di Windows, clicca su **Aggiorna ora** per aprire la procedura guidata della Scansione vulnerabilità e installarli.
   - Se un'applicazione non è aggiornata, clicca su **Aggiorna ora** per trovare un link alla pagina web del distributore, da dove poter installare la versione più recente dell'applicazione.
   - Se un account utente Windows ha una password poco sicura, clicca su **Sistema password** per costringere l'utente a modificare la password al prossimo accesso, oppure cambiala direttamente.Per avere una password sicura, utilizza una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).
   - Se la funzione esecuzione automatica di Windows è attivata, clicca su **Disattiva** per disattivarla.

Per configurare le impostazioni del controllo vulnerabilità, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Eventi antivirus**, seleziona la scheda **Vulnerabilità**.
5. Clicca sull'interruttore per attivare o disattivare la Scansione vulnerabilità automatica.

Importante

Per essere avvertito automaticamente sulle vulnerabilità del sistema o delle applicazioni, mantieni la **Scansione vulnerabilità automatica** attivata.

6. Seleziona le vulnerabilità del sistema che desideri siano controllate regolarmente usando gli interruttori corrispondenti.

   Aggiornamenti critici di Windows
   Verifica se il sistema operativo Windows ha gli ultimi aggiornamenti di sicurezza di Microsoft.

   Aggiornamenti regolari di Windows
   Verifica se il sistema operativo Windows ha gli ultimi aggiornamenti di sicurezza di Microsoft.

   Aggiornamenti applicazioni
   Verifica se le applicazioni cruciali relative al web installate sul sistema sono aggiornate.Applicazioni datate possono essere sfruttate da software dannosi, rendendo il tuo PC vulnerabile agli attacchi esterni.

   Password non sicure
   Verifica se le password degli account Windows configurate sul sistema sono più o meno facili da indovinare.Impostare password difficili da indovinare (password sicure) ostacola l'accesso al tuo sistema da parte degli hacker.Una password sicura include una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali (come #, $ o @).

   Esecuzione automatica supporti
   Verifica lo stato della funzione di esecuzione automatica di Windows.Questa caratteristica consente alle applicazioni di essere avviate automaticamente da unità CD, DVD, USB o altri dispositivi esterni.

   Alcuni tipi di malware usano l'esecuzione automatica per diffondersi automaticamente da supporti rimovibili al PC. Ecco perché si consiglia di disattivare questa funzione di Windows.

Nota
Se disattivi il monitoraggio di una vulnerabilità particolare, i relativi problemi non saranno più registrati nella finestra Eventi.

17. Antispam

Spam è un termine usato per descrivere ogni e-mail non richiesta.Lo spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Non è piacevole, si vuole evitare che i propri figli lo ricevano, potrebbe penalizzarti (per aver sprecato troppo tempo o per aver ricevuto e-mail pornografiche in ufficio) e non puoi impedire ad alcuni di inviarlo. La miglior cosa da fare, ovviamente, è impedirne la ricezione. Purtroppo di norma lo spam abbonda, oltre a presentarsi sotto molte forme e dimensioni.

L'antispam di Bitdefender impiega notevoli innovazioni tecnologiche e filtri standard dell'industria antispam per eliminare lo spam prima che raggiunga la Posta in arrivo dell'utente.Per ulteriori informazioni, fare riferimento a «*Approfondimenti antispam*» (p. 99).

La protezione antispam di Bitdefender è disponibile solo per client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3.POP3 è uno dei protocolli più usati per scaricare messaggi e-mail da un server di posta.

Nota

Bitdefender non fornisce protezione antispam agli account e-mail cui accedi direttamente tramite Internet.

I messaggi spam rilevati da Bitdefender sono segnati con il prefisso `[spam]` nell'oggetto.Bitdefender sposta automaticamente i messaggi spam a una cartella specifica, come segue:

- In Microsoft Outlook, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Posta eliminata**.La cartella **Spam** è creata durante l'installazione di Bitdefender.
- In Outlook Express e Windows Mail, i messaggi spam sono spostati direttamente nella cartella **Posta eliminata**.
- In Mozilla Thunderbird, i messaggi spam sono spostati nella cartella **Spam**, situata nella cartella **Cestino**.La cartella **Spam** è creata durante l'installazione di Bitdefender.

Se si utilizza un altro client di posta, è necessario creare una regola per spostare i messaggi e-mail segnati come `[spam]` da Bitdefender in una cartella personalizzata di quarantena.

17.1. Approfondimenti antispam

17.1.1. Filtri Antispam

Il motore antispam Bitdefender include una protezione cloud e altri filtri, che proteggono la tua casella di posta in arrivo da ogni SPAM, come Elenco Amici, Elenco Spammer e Filtro Caratteri..

Elenco amici / Elenco spammer

La maggior parte delle persone comunica regolarmente con un gruppo di persone o riceve messaggi da organizzazioni o società nello stesso dominio. Utilizzando l'**elenco Amici o Spammer**, potrai facilmente classificare da quali persone vuoi ricevere e-mail (amici) indipendentemente dal contenuto del messaggio, o da quali persone non vuoi più ricevere nulla (spammer).

Nota

Raccomandiamo di aggiungere i nomi e gli indirizzi e-mail dei propri amici all'**elenco Amici**. Bitdefender non blocca i messaggi dai mittenti inclusi nell'elenco; perciò, aggiungendo gli amici i loro messaggi legittimi arriveranno.

Filtro caratteri

La maggior parte dei messaggi Spam sono scritti in caratteri cirillici e/o asiatici. Il filtro caratteri rileva questo tipo di messaggi e li etichetta come SPAM.

17.1.2. Operazione antispam

Il motore antispam di Bitdefender usa tutti i filtri antispam combinati per determinare se un certo messaggio e-mail dovrebbe essere consegnato alla **Posta in arrivo** o no.

Ogni e-mail che arriva da Internet viene prima controllata con il filtro Elenco Amici/Elenco Spammer. Se l'indirizzo del mittente viene trovato nell'Elenco Spammer l'e-mail viene spostata direttamente nella **Posta in arrivo**.

Diversamente, il filtro Elenco Spammer prenderà in carico l'e-mail per verificare se l'indirizzo del mittente è contenuto nel suo elenco. L'e-mail verrà contrassegnata come spam e spostata nella cartella **Spam**, qualora il confronto con l'elenco abbia dato esito positivo.

Ancora, il filtro caratteri controllerà se l'e-mail è scritta con caratteri cirillici o asiatici. In questo caso l'e-mail verrà marcata come SPAM e spostata nella cartella **Spam**.

Nota

Se l'e-mail è marcata come SEXUALLY-EXPLICIT nella riga dell'oggetto, Bitdefender la considererà SPAM.

17.1.3. Programmi e protocolli di posta elettronica supportati

È fornita una protezione antispam per tutti i client di posta POP3/SMTP.La barra degli strumenti di Bitdefender Antispam è integrata solo in:

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express e Windows Mail (su sistemi a 32 bit)
- Mozilla Thunderbird 3.0.4

17.2. Attivare o disattivare la protezione antispam

Di norma la protezione antispam è attivata.

Per disattivare il modulo antispam, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antispam**, clicca sull'interruttore per attivare o disattivare la funzione **Antispam**.

17.3. Usare la barra degli strumenti antispam nella finestra del tuo client e-mail

Nella parte superiore della finestra del client di posta puoi vedere la barra degli strumenti antispam.La barra degli strumenti Antispam aiuta a gestire la protezione antispam direttamente dal client di posta.Puoi correggere facilmente Bitdefender se segnala un messaggio legittimo come SPAM.

Importante

Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo.Per un elenco completo delle applicazioni di posta supportate, fare riferimento a *«Programmi e protocolli di posta elettronica supportati»* (p. 100).

Qui di seguito la spiegazione di ogni pulsante della barra degli strumenti di Bitdefender:

È spam - Indica che l'e-mail selezionata è spam.L'e-mail sarà spostata immediatamente alla cartella **Spam**.Se i servizi cloud antispam sono attivati, il messaggio è inviato al cloud di Bitdefender per ulteriori analisi.

Non è spam - Indica che l'e-mail selezionata non è spam e Bitdefender non deve marcarla.L'e-mail sarà spostata dalla cartella **Spam** alla **Posta in arrivo**.Se i servizi cloud antispam sono attivati, il messaggio è inviato al cloud di Bitdefender per ulteriori analisi.

Importante

Il pulsante **Non è spam** si attiva quando si seleziona un messaggio marcato come SPAM da Bitdefender (normalmente questi messaggi sono situati nella cartella **Spam**).

Aggiungi Spammer - aggiunge il mittente dell'e-mail selezionata all'elenco degli Spammer.Può essere necessario premere **OK** per confermare.I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come `[spam]`.

Aggiungi amico - aggiunge il mittente dell'e-mail selezionata all'elenco Amici.Può essere necessario premere **OK** per confermare.Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Spammer - Apre l'**elenco Spammer**, che contiene tutti gli indirizzi e-mail dai quali non vuoi ricevere messaggi, indipendentemente dal loro contenuto.Per ulteriori informazioni, fare riferimento a «*Configurazione dell'elenco Spammer*» (p. 104).

Amici - Apre l'**elenco Amici** che contiene tutti gli indirizzi e-mail dai quali desideri ricevere sempre i messaggi, indipendentemente dal loro contenuto.Per ulteriori informazioni, fare riferimento a «*Configurazione dell'elenco Amici*» (p. 103).

Impostazioni - Apre una finestra dove puoi configurare i filtri antispam e le impostazioni della barra degli strumenti.

17.3.1. Indicare gli errori di rilevazione

Se stai utilizzando un client di posta supportato, puoi correggere facilmente il filtro antispam (indicando quali messaggi e-mail non devono essere contrassegnati come `[spam]`). Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam.Attenersi alla seguente procedura:

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.
3. Seleziona il messaggio legittimo scorrettamente contrassegnato come `[spam]` da Bitdefender.
4. Clicca sul pulsante **Aggiungi amico** sulla barra degli strumenti antispam di Bitdefender per aggiungere il mittente all'elenco Amici.Può essere necessario premere **OK** per confermare.Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.
5. Clicca sul pulsante **Non è Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta).L'e-mail sarà spostata nella cartella Posta in arrivo.

17.3.2. Indicare messaggi spam non rilevati

Se si utilizza un'applicazione di posta supportata si può facilmente indicare quali messaggi e-mail avrebbero dovuto essere rilevati come spam. Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam.Attenersi alla seguente procedura:

1. Apri il tuo client e-mail.
2. Vai alla cartella Posta in arrivo.
3. Seleziona i messaggi di spam non rilevati.

4. Clicca sul pulsante **È Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta). Vengono immediatamente contrassegnati come `[spam]` e verranno spostati alla cartella posta indesiderata.

17.3.3. Configurare le impostazioni della barra degli strumenti

Per configurare le impostazioni della barra degli strumenti antispam per il tuo client e-mail, clicca sul pulsante **Impostazioni** sulla barra degli strumenti e poi sulla scheda **Impost. Barra strumenti**.

Hai le seguenti opzioni:

- **Sposta messaggio in Posta eliminata** (solo per Microsoft Outlook Express / Windows Mail)

  Nota
  In Microsoft Outlook / Mozilla Thunderbird, i messaggi spam rilevati sono spostati automaticamente nella cartella Spam, localizzata in Posta eliminata / Cestino.

- **Etichetta i messaggi di spam come "letti"** - Etichetta i messaggi di spam come letti in modo automatico, in modo tale da non disturbare quando questi vengono ricevuti.
- Puoi scegliere se visualizzare o no le finestre di conferma quando clicchi sui pulsanti **Aggiungi Spammer** e **Aggiungi Amico** nella barra degli strumenti antispam.

  Le finestre di conferma possono impedire di aggiungere accidentalmente i mittenti all'elenco Amici / Spammer.

17.4. Configurazione dell'elenco Amici

L'**elenco Amici** è un elenco di tutti gli indirizzi e-mail dai quali desideri sempre ricevere messaggi, indipendentemente dal loro contenuto. I messaggi provenienti dagli amici non verranno etichettati come spam, anche se il loro contenuto potrebbe assomigliare allo spam.

Nota
Qualsiasi e-mail in arrivo da un indirizzo contenuto nell'**elenco Amici**, sarà automaticamente consegnata nella Posta in arrivo, senza alcuna ulteriore elaborazione.

Per configurare e gestire l'elenco Amici:

- Se stai usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clicca sul pulsante **Amici** nella barra degli strumenti antispam di Bitdefender
- In alternativa, segui questi passaggi:
  1. Apri la finestra di Bitdefender.

2. Nel pannello **Antispam**, clicca su **Gestisci** e seleziona **Gestisci gli Amici** dal menu a tendina.

Per aggiungere un indirizzo e-mail, seleziona l'opzione **Indirizzo e-mail**, inserisci l'indirizzo e poi clicca su **Aggiungi**.Sintassi: name@domain.com.

Per aggiungere tutti gli indirizzi e-mail da un dominio specifico, seleziona l'opzione **Nome dominio**, inserisci il nome del dominio e clicca sul pulsante **Aggiungi**.Sintassi:

- @domain.com, *domain.com e domain.com - Tutte le e-mail provenienti da domain.com raggiungeranno la **Posta in arrivo** indipendentemente dal loro contenuto;
- *domain* - Tutte le e-mail provenienti da domain (non importa il suffisso del dominio) raggiungeranno la **Posta in arrivo** indipendentemente dal loro contenuto;
- *com - Tutte le e-mail con il suffisso di dominio com raggiungeranno la **Posta in arrivo** indipendentemente dal loro contenuto;

Si consiglia di evitare di aggiungere interi domini, ma potrebbe essere utile in alcune situazioni.Per esempio, puoi aggiungere il dominio e-mail della società per cui lavori o quello dei tuoi contatti di fiducia.

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente.Per eliminare tutti gli elementi dall'elenco clicca su **Cancella lista** e quindi su **Sì** per confermare.

Puoi salvare l'elenco Amici in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto.Per salvare l'elenco Amici, clicca sul pulsante **Salva** e salvalo nella posizione desiderata.Il file avrà estensione `.bwl`.

Per caricare un elenco Amici salvato in precedenza, clicca sul pulsante **Carica** e apri il corrispondente file `.bwl`.Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco salvato in precedenza, seleziona **Sovrascrivi l'elenco attuale**.

Clicca su **OK** per salvare le modifiche e chiudere la finestra.

17.5. Configurazione dell'elenco Spammer

L'**elenco Spammer** è l'elenco di tutti gli indirizzi e-mail dai quali non desideri ricevere messaggi, indipendentemente dal loro contenuto.Qualsiasi e-mail in arrivo da un indirizzo contenuto nell'**elenco Spammer** sarà automaticamente marcata come spam, senza alcun ulteriore processo.

Per configurare e gestire l'elenco Spammer:

- Se stai usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clicca sul pulsante **Spammer** nella barra degli strumenti antispam di Bitdefender integrata nel tuo client e-mail.
- In alternativa, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antispam**, clicca su **Gestisci** e seleziona **Gestisci gli Spammer** dal menu a tendina.

Per aggiungere un indirizzo e-mail, seleziona l'opzione **Indirizzo e-mail**, inserisci l'indirizzo e poi clicca su **Aggiungi**.Sintassi: name@domain.com.

Per aggiungere tutti gli indirizzi e-mail da un dominio specifico, seleziona l'opzione **Nome dominio**, inserisci il nome del dominio e clicca sul pulsante **Aggiungi**.Sintassi:

- @domain.com, *domain.com e domain.com - Tutte le e-mail provenienti da domain.com saranno marcate come Spam;
- *domain* - Tutte le e-mail provenienti da domain (indipendentemente dai suffissi del dominio) saranno marcate come Spam;
- *com - Tutte le e-mail con il suffisso di dominio com saranno marcate come Spam.

Si consiglia di evitare di aggiungere interi domini, ma potrebbe essere utile in alcune situazioni.

Avvertimento

Non aggiungere domini di servizi e-mail legittimi (ad esempio Yahoo, Gmail, Hotmail o altri) all'elenco Spammer. In caso contrario gli indirizzi e-mail ricevuti dagli utenti registrati di tali servizi verranno identificati come spam.Se, ad esempio, aggiungi `yahoo.com` all'elenco Spammer, tutti i messaggi e-mail provenienti da indirizzi `yahoo.com` saranno contrassegnati come `[spam]`.

Per eliminare un elemento dall'elenco, clicca sul collegamento **Rimuovi** corrispondente.Per eliminare tutti gli elementi dall'elenco clicca su **Cancella lista** e quindi su **Sì** per confermare.

Puoi salvare l'elenco Spammer in un file in modo da poterlo riutilizzare su un altro computer o dopo aver reinstallato il prodotto.Per salvare l'elenco Spammer, clicca sul pulsante **Salva** e salvalo nella posizione desiderata.Il file avrà estensione `.bwl`.

Per caricare un elenco Spammer salvato in precedenza, clicca sul pulsante **Carica** e apri il corrispondente file `.bwl`.Per ripristinare il contenuto dell'elenco esistente quando si carica un elenco salvato in precedenza, seleziona **Sovrascrivi l'elenco attuale**.

Clicca su **OK** per salvare le modifiche e chiudere la finestra.

17.6. Configurare i filtri locali antispam

Come descritto in «*Approfondimenti antispam*» (p. 99), Bitdefender usa una combinazione di diversi filtri antispam per identificare lo spam.I filtri antispam sono pre-configurati per una protezione ottimale.

Importante

A seconda che tu riceva o no e-mail legittime, scritte in caratteri asiatici o cirillici, disattiva o attiva l'impostazione che blocca automaticamente tali e-mail.L'impostazione corrispondente è disattivata nelle versioni localizzate del programma che usano tali set di caratteri (per esempio, nella versione russa e cinese).

Per configurare i filtri antispam locali, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antispam**.
4. Nella finestra **Impostazioni antispam**, hai la scheda **Impostazioni**.
5. Clicca sugli interruttori per attivare o disattivare i filtri locali antispam.

Se stai usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, puoi configurare i filtri locali dell'antispam direttamente dal tuo client di posta.Clicca sul pulsante **Impostazioni** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta) e poi sulla scheda **Filtri antispam**.

17.7. Configurare le impostazioni cloud

La rilevazione cloud sfrutta i servizi cloud di Bitdefender per fornirti una protezione antispam efficace e sempre aggiornata.

La protezione cloud funziona finché si tiene attivo l'antispam di Bitdefender.

Campioni di e-mail legittime o spam possono essere inviati al cloud di Bitdefender, indicando errori di rilevazione o messaggi spam non rilevati. Ciò contribuisce a migliorare la rilevazione antispam di Bitdefender.

Configura l'invio di un'e-mail campione al cloud di Bitdefender e seleziona le opzioni desiderate, seguendo questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antispam**.
4. Seleziona le opzioni desiderate dalla scheda **Impostazioni**.

Se stai usando Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, puoi configurare la rilevazione cloud direttamente dal tuo client di posta.Clicca sul pulsante **Impostazioni** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta) e poi sulla scheda **Impostazioni cloud**.

18. Controllo privacy

Le tue informazioni personali sono un bersaglio costante per i cyber criminali.Poiché le minacce si sono estese a quasi tutto l'intero spettro di attività online, messaggi e-mail, chat e navigazione web non protetti possono comportare il rilascio di informazioni in grado di compromettere la propria privacy.

In aggiunta, i file importanti memorizzati sul computer un giorno potrebbero trovarsi nelle mani sbagliate.

Il Controllo privacy di Bitdefender affronta tutte queste minacce con una moltitudine di componenti.

- Protezione antiphishing - offre un set completo di funzioni che proteggono la tua esperienza di navigazione web, come ad esempio evitare la diffusione di informazioni personali a siti web fraudolenti camuffati da siti legittimi.
- Crittografia chat - crittografa le conversazioni chat per assicurarsi che il contenuto resti privato.
- Protezione dati - Non consente di divulgare i tuoi dati personali dal computer senza il tuo consenso.Controlla le e-mail e i messaggi istantanei inviati dal tuo computer, oltre a qualsiasi dato inviato tramite pagine web, bloccando qualsiasi informazione protetta dalle regole di Protezione dati impostate.
- Distruttore di file - elimina in modo permanente i file e le loro tracce dal tuo computer.

18.1. Protezione antiphishing

L'antiphishing di Bitdefender ti impedisce di svelare informazioni personali mentre navighi su Internet, avvertendoti delle potenziali pagine web con phishing.

Bitdefender fornisce protezione antiphishing in tempo reale per:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger

Per configurare le impostazioni antiphishing, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Controllo privacy**.
4. Nella finestra **Impostazioni controllo privacy**, seleziona la scheda **Antiphishing**.

Clicca sugli interruttori per attivare o disattivare:

- Mostrare la barra degli strumenti di Bitdefender nel browser web.

  Nota
  Di norma, la barra degli strumenti del browser di Bitdefender non è attivata.

- Ricerca sicura, una componente che valuta i risultati delle tue ricerche e i link pubblicati sui social network, posizionando un'icona accanto a ogni risultato:

  Non dovresti visitare questa pagina web.

  Questa pagina web può contenere contenuti pericolosi. Se decidi di visitarlo, usa la massima cautela.

  Questa è una pagina sicura da visitare.

  Ricerca sicura valuta i risultati delle ricerche dei seguenti motori di ricerca via web:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Ricerca sicura valuta i link pubblicati sui seguenti servizi di social network:
  - Facebook
  - Twitter

- Controllare il traffico web SSL.

  Gli attacchi più sofisticati possono usare il traffico web sicuro per ingannare le loro vittime.Si consiglia pertanto di attivare la scansione SSL.

- Protezione dalle frodi.
- Protezione da phishing.
- Protezione per chat.

Puoi creare un elenco di siti web che non saranno controllati dai motori antiphishing di Bitdefender.L'elenco dovrebbe contenere solo siti web di cui ti fidi completamente.Ad esempio, aggiungi i siti web dove fai di solito i tuoi acquisti online.

Per configurare e gestire la white list antiphishing, clicca sul collegamento **White list**.Comparirà una nuova finestra.

Per aggiungere un sito alla white list, inserisci il suo indirizzo nel campo corrispondente e quindi clicca su **Aggiungi**.

Per rimuovere un sito web dall'elenco, selezionalo e clicca sul collegamento **Rimuovi** corrispondente.

Clicca su **Salva** per salvare le modifiche e chiudere la finestra.

18.1.1. Protezione di Bitdefender nel browser

Bitdefender si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti web browser:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

La barra degli strumenti di Bitdefender non è la tipica barra degli strumenti del browser.L'unica cosa che aggiunge al browser è una piccola linguetta nella parte superiore di ogni pagina web.Cliccaci sopra per vedere la barra degli strumenti.

La barra degli strumenti di Bitdefender include le seguenti componenti:

Valutazione pagina

In base a come Bitdefender classifica la pagina web che stai visualizzando, sul lato sinistro della barra degli strumenti viene indicata una delle seguenti valutazioni:

- Il messaggio "Questa pagina non è sicura" compare su uno sfondo rosso. Dovresti uscire subito dalla pagina web. Per scoprire altri dettagli su questa minaccia, clicca sul simbolo **+** nella valutazione della pagina.
- Il messaggio "Si consiglia cautela" compare su uno sfondo arancio. Questa pagina web potrebbe avere contenuti pericolosi.Se decidi di visitarlo, usa la massima cautela.
- Il messaggio "Questa pagina è sicura" compare su uno sfondo verde. La pagina è sicura e può essere visitata.

Sandbox

Clicca per lanciare il browser in un ambiente creato da Bitdefender, isolandolo dal sistema operativo. Impedisce alle minacce basate sui browser di sfruttare le vulnerabilità dei browser per ottenere il controllo del tuo sistema.Usa Sandbox quando visiti pagine web che ritieni possano contenere malware.

Le finestre del browser aperte in Sandbox saranno facilmente riconoscibili dal loro contorno modificato e inoltre avranno l'icona di Safebox al centro della barra del titolo.

Nota
Sandbox non è disponibile sui computer con Windows XP.

Impostazioni

Clicca per selezionare le singole caratteristiche da attivare o disattivare:

- Filtro antiphishing
- Filtro web antimalware
- Ricerca Sicura

Interruttore di accensione

Per attivare/disattivare completamente le funzioni della barra degli strumenti, clicca sul lato destro della barra stessa.

18.1.2. Avvisi di Bitdefender nel browser

Ogni volta che provi a visitare un sito web classificato come poco sicuro, il sito web viene bloccato e nel tuo browser compare una pagina di avvertimento.

La pagina contiene informazioni quali l'URL del sito web e la minaccia rilevata.

Devi decidere la tua prossima azione. Sono disponibili le seguenti opzioni:

- Allontanati dalla pagina web, cliccando su **Per sicurezza torna indietro**.
- Disattiva il blocco delle pagine che contengono phishing, cliccando su **Disattiva il filtro antiphishing**.
- Disattiva il blocco delle pagine che contengono malware, cliccando su **Disattiva il filtro antimalware**.
- Aggiungi la pagina alla white list dell'antiphishing cliccando su **Aggiungi alla white list**.La pagina non sarà più controllata dai motori antiphishing di Bitdefender.
- Procedi alla pagina web, malgrado l'avvertimento, cliccando su **Sono a conoscenza dei rischi, quindi prosegui**.

18.2. Crittog. chat

I contenuti dei tuoi messaggi istantanei dovrebbero restare tra te e il tuo partner di chat.Crittografando le tue conversazioni, puoi assicurarti che chiunque tenti di intercettarle durante l'invio da te ai tuoi contatti, non sarà in grado di leggerne il contenuto.

Di norma, Bitdefender esegue la crittografia di tutte le tue sessioni chat, purché:

- Il tuo partner di chat ha una versione di Bitdefender installata che supporta la Crittografia Chat, e la Crittografia Chat è abilitata per l'applicazione usata per chattare.
- Tu e la persona con cui vuoi chattare usate Yahoo! Messenger.

> **Importante**
> Bitdefender non cifrerà una conversazione se uno degli utenti in chat utilizza un'applicazione chat via web come Meebo.

Una volta soddisfatti i requisiti, Bitdefender ti informerà sullo stato della crittografia della tua sessione di chat attraverso messaggi mostrati nella finestra di chat.

Per attivare o disattivare la crittografia della chat, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Controllo privacy**.
4. Nella finestra **Impostazioni controllo privacy**, seleziona la scheda **Crittografia chat**.
5. Clicca sull'interruttore per attivare o disattivare la crittografia chat. Di norma, la crittografia è attivata.

18.3. Protezione dati

La Protezione dati impedisce la diffusione di dati sensibili quando sei online.

Considera un semplice esempio: hai creato una regola di Protezione dati che protegge il tuo numero di carta di credito.Se uno spyware in qualche modo riesce a installarsi sul tuo computer, non può inviare il tuo numero di carta di credito via e-mail, chat o tramite pagine web.Inoltre, il bambino non può usarlo per fare acquisti online o comunicarlo a persone incontrate sul web.

18.3.1. Info su Protezione dati

Che sia la tua e-mail o il numero della tua carta di credito, quando finiscono nelle mani sbagliate tali informazioni possono recarti danno: puoi ritrovarti affogato nei messaggi di spam o addirittura con il tuo conto bancario in rosso.

Basandosi sulle regole create da te, la Protezione dati esegue la scansione del traffico web, e-mail e chat in uscita dal tuo computer, cercando specifiche sequenze di caratteri (ad esempio, il tuo numero di carta di credito). Se c'è una coincidenza, la pagina web, la mail o il messaggio vengono bloccati.

Puoi creare regole per proteggere ogni informazione che consideri personale o confidenziale, dal tuo numero di telefono o l'indirizzo e-mail, fino alle informazioni sul tuo conto bancario.Viene fornito un supporto Multi-utente, in modo che gli utenti che accedano ad altri account di Windows possano configurare e usare le proprie regole.Se il proprio account Windows è un account amministratore, le regole create possono essere configurate per essere applicate anche quando altri utenti del computer accedono ai rispettivi account utente Windows.

18.3.2. Configurare la Protezione dati

Se vuoi usare la Protezione dati, segui questi passaggi:

1. Apri la finestra di Bitdefender.

2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Controllo privacy**.
4. Nella finestra **Impostazioni controllo privacy**, seleziona la scheda **Protezione dati**.
5. Assicurati che la Protezione dati sia attivata.
6. Crea regole per proteggere i tuoi dati sensibili.Per ulteriori informazioni, fare riferimento a «*Creare regole di protezione dati*» (p. 112).

Creare regole di protezione dati

Per creare una regola, clicca sul pulsante **Aggiungi regola** e segui la procedura guidata di configurazione.Puoi esplorare la procedura guidata usando i pulsanti **Avanti** e **Indietro**.Per uscire dalla procedura guidata, clicca su **Annulla**.

1. **Definizione regola**

   Devi impostare i seguenti parametri:

   - **Nome regola** - inserisci il nome della regola nel campo di modifica.
   - **Tipo di regola** - scegli il tipo di regola (indirizzo, nome, carta di credito, PIN, SSN, ecc).
   - **Dati regola** - inserisci i dati da proteggere nel campo di modifica. Ad esempio, se desideri proteggere la tua carta di credito, inserisci tutto o parte del numero in questo campo.

     Importante
     Vi consigliamo di inserire al meno tre caratteri per evitare il blocco erroneo di messaggi e pagine web. Tuttavia, per una maggiore sicurezza, inserisci solo parte dei dati (ad esempio, solo una parte del numero della carta di credito).

   - **Descrizione della regola** - inserisci una breve descrizione della regola nel campo di modifica. Siccome i dati bloccati (serie di caratteri) non vengono mostrati in plain text quando si accede alla regola, la descrizione dovrebbe aiutarti a identificarla facilmente.

2. **Configurare le impostazioni della regola**

   a. Seleziona il traffico che desideri esaminare con Bitdefender.

      - **Scansione web (traffico HTTP)** - controlla il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
      - **Scansione e-mail (traffico SMTP)** - esamina il traffico SMTP (e-mail) e blocca le e-mail in uscita contenenti i dati della regola.

      Puoi scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.

b. Specifica gli utenti a cui si applica la regola.

- **Solo per me (utente attuale)** - la regola si applica solo all'account utente attuale.
- **Tutti gli utenti** - la regola si applica a tutti gli account di Windows.
- **Account utente limitati** - la regola si applica all'utente attuale e a tutti gli account di Windows limitati.

Clicca su **Termina**. La regola apparirà nella tabella.

D'ora in poi, ogni tentativo di inviare i dati della regola attraverso i protocolli selezionati fallirà. Nella finestra Eventi sarà visualizzato un valore, indicando che Bitdefender ha impedito che contenuti relativi all'identità venissero inviati.

18.3.3. Amministrazione delle regole

Per gestire le regole della Protezione dati:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Controllo privacy**.
4. Nella finestra **Impostazioni controllo privacy**, seleziona la scheda **Protezione dati**.

Puoi visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionala e clicca sul pulsante **Rimuovi regola**.

Per modificare una regola, selezionala e clicca sul pulsante **Modificare regola**. Comparirà una nuova finestra.Qui potete modificare il nome, la definizione e i parametri della regola (tipo, dati e traffico). Clicca su **OK** per salvare le modifiche.

18.4. Eliminare i file in modo permanente

Quando elimini un file, non potrai più accedervi con i normali strumenti. Comunque, il file continuerà a essere archiviato sul disco rigido finché non sarà sovrascritto quando copierete nuovi file.

Il Distruttore di file di Bitdefender ti aiuterà a eliminare in modo permanente i dati rimuovendoli fisicamente dal tuo disco fisso.

Puoi distruggere file o cartelle rapidamente dal computer usando il menu contestuale di Windows, seguendo questi passaggi:

1. Clicca con il pulsante destro sul file o la cartella che vuoi eliminare in modo permanente.
2. Seleziona **Bitdefender** > **Distruttore di file** nel menu contestuale che apparirà.

3. Apparirà una finestra di conferma.Clicca su **Sì** per avviare la procedura guidata del Distruttore di file.
4. Attendi che Bitdefender termini la distruzione dei file.
5. I risultati sono mostrati.Clicca su **Chiudi** per uscire dalla procedura guidata.

In alternativa, puoi distruggere i file dall'interfaccia di Bitdefender.

1. Apri la finestra di Bitdefender.
2. Nel pannello **Privacy**, clicca su **Proteggi** e seleziona **Distruttore di file** dal menu a tendina.
3. Segui la procedura guidata del Distruttore di file:
   a. **Seleziona file/cartella**

      Aggiungi i file o le cartelle che vuoi rimuovere in modo permanente.

   b. **Distruzione file**

      Attendi che Bitdefender termini la distruzione dei file.

   c. **Risultati**

      I risultati sono mostrati.Clicca su **Chiudi** per uscire dalla procedura guidata.

19. Firewall

Il firewall protegge il computer da tentativi di connessione in entrata e in uscita non autorizzati, su reti locali e Internet.È abbastanza simile a una guardia a un cancello: tiene traccia dei tentativi di connessione e decide chi far entrare e chi bloccare.

Il firewall di Bitdefender utilizza un set di regole per filtrare i dati trasmessi al e dal sistema.Le regole sono suddivise in 3 categorie:

Regole generali
: Regole che determinano i protocolli tramite i quali sono consentite le comunicazioni.

  Viene usato un set di regole predefinito che fornisce una protezione ottimale.Puoi modificare le regole, consentendo o negando le connessioni su determinati protocolli.

Regole applicazione
: Le regole che determinano come ogni applicazione può accedere alle risorse di rete e a Internet.

  In condizioni normali, Bitdefender crea automaticamente una regola ogni volta che un'applicazione cerca di accedere a Internet.Puoi anche aggiungere o modificare manualmente le regole per le applicazioni.

Regole adattatore
: Regole che determinano la comunicazione del tuo computer con altri computer connessi alla stessa rete.

  È necessario creare regole per consentire o bloccare il traffico tra il tuo computer e altri computer in particolare.

Se il computer ha Windows Vista, Windows 8 o Windows 7, Bitdefender assegna automaticamente un tipo di rete a ogni connessione di rete che rileva.In base al tipo di rete, la protezione del firewall viene impostata al livello appropriato per ogni connessione.

Per scoprire altre informazioni sulle impostazioni del firewall per ogni tipo di rete e come modificare le impostazioni della rete, fai riferimento a «*Gestire le impostazioni di connessione*» (p. 116).

Una protezione aggiuntiva è fornita dal Sistema di rilevazione intrusioni (IDS).IDS monitora la rete e le attività del sistema per rilevare attività pericolose o violazioni delle policy.Può rilevare e bloccare tentativi di modificare i file critici di sistema, i file di Bitdefender o le voci del registro, l'installazione di driver malware e gli attacchi eseguiti con l'inserimento di codice (inserimento di DLL).

Bitdefender di norma è configurato per intraprendere automaticamente le azioni consigliate per la tua protezione, senza importunarti. Se desideri essere informato e decidere la migliore azione da intraprendere quando un'applicazione richiede

l'accesso a Internet o mostra un comportamento sospetto, devi attivare la modalità Paranoid.

19.1. Attivare o disattivare la protezione del firewall

Per attivare o disattivare la protezione del firewall, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Firewall**, clicca sull'interruttore Firewall.

Avvertimento

Poiché espone il computer a connessioni non autorizzate, la disattivazione del firewall dovrebbe essere solo una misura temporanea.Riattiva il firewall il prima possibile.

19.2. Gestire le impostazioni di connessione

Per visualizzare e modificare le impostazioni di connessione della rete, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Firewall**, clicca su **Gestisci adattatori**.

Comparirà una nuova finestra.Il grafico nella parte superiore della finestra mostra informazioni in tempo reale sul traffico in entrata e in uscita.

Sotto al grafico, per ogni connessione di rete sono mostrate le seguenti informazioni.

- **Tipo di rete** - Il tipo di rete a cui è connesso il computer.Bitdefender applica un set base di impostazioni del firewall secondo il tipo di rete a cui sei connesso.

  Puoi cambiare il tipo, aprendo il menu a tendina **Tipo di rete** e selezionare uno dei tipi disponibili dall'elenco.

Tipo di rete	Descrizione
Di fiducia	Disabilita il firewall per il relativo adattatore.
Casa/Ufficio	Consente tutto il traffico tra il tuo computer e quelli nella rete locale.
Pubblica	Tutto il traffico viene filtrato.
Non sicura	Blocca completamente la rete e il traffico Internet attraverso il relativo adattatore.

- **Modalità invisibile** - Possibilità di essere rilevati da altri computer.

  Per configurare la modalità invisibile, seleziona l'opzione desiderata dal menu a tendina corrispondente.

Opzione Invisibile	Descrizione
Attiva	La Modalità invisibile è attiva.Il tuo computer è invisibile sia dalla rete locale che da Internet.
Inattiva	La Modalità invisibile è disattivataTutti possono pingare e rilevare il tuo computer dalla rete locale o da Internet.
Remoto	Il tuo computer non può essere rilevato da Internet.Gli utenti della rete locale possono pingare e rilevare il tuo computer.

- **Generico** - Se regole generiche vengono applicate o no a questa connessione.

  Se l'indirizzo IP dell'adattatore di rete è stato cambiato, Bitdefender modifica il tipo di rete di conseguenza.Se vuoi mantenere lo stesso tipo, seleziona **Sì** dal menu a tendina corrispondente.

19.3. Gestire le regole del firewall

19.3.1. Regole generali

Ogni volta che si trasmettono dati su Internet, sono usati determinati protocolli.

Le regole generali ti consentono di configurare i protocolli su cui è consentito il traffico.Per modificare le regole, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Impostazioni**.
5. Nelle regole del firewall, clicca su **Regole generali**.

Comparirà una nuova finestra.Sono mostrate le regole attuali.

Per modificare una regola, clicca sulla sua freccia corrispondente nella colonna **Azione** e seleziona **Consenti** o **Nega**.

DNS su UDP / TCP
Consenti o blocca DNS su UDP e TCP.

Di norma, questo tipo di connessione è consentita.

ICMP / ICMPv6 in ingresso
Consenti o blocca i messaggi ICMP / ICMPv6.

I messaggi ICMP sono spesso usati dagli hacker per eseguire attacchi contro le reti informatiche.Di norma, questo tipo di connessione è bloccata.

Inviare e-mail
Consenti o blocca l'invio di e-mail via SMTP.

Di norma, questo tipo di connessione è consentita.

Navigazione web HTTP
Consenti o blocca la navigazione web HTTP.

Di norma, questo tipo di connessione è consentita.

Connessioni desktop remote in ingresso
Consenti o blocca l'accesso ad altri computer alle connessioni desktop remote.

Di norma, questo tipo di connessione è consentita.

Traffico Windows Explorer su HTTP / FTP
Consenti o blocca il traffico HTTP e FTP da Windows Explorer.

Di norma, questo tipo di connessione è bloccata.

19.3.2. Regole applicazioni

Per visualizzare e gestire le regole del firewall che controllano l'accesso delle applicazioni alle risorse di rete e a Internet, clicca su **Regole applicazione**.

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Impostazioni**.
5. Nelle regole del Firewall, clicca su **Regole applicazione**.

Nella tabella puoi visualizzare i programmi (processi) per i quali sono state create le regole del firewall.Per vedere le regole create per un'applicazione specifica, clicca sulla casella + accanto alla relativa applicazione o semplicemente cliccaci sopra due volte.

Per ogni regola sono visualizzate le seguenti informazioni:

- **Tipologie di processo/rete** - Le tipologie di processo e adattatore di rete sulle quali vengono applicate le regole.Le regole sono create automaticamente per filtrare l'accesso alla rete o a Internet attraverso tutti gli adattatori.Puoi creare nuove regole manualmente o modificare regole esistenti per filtrare l'accesso alla rete o a Internet di un'applicazione attraverso un adattatore specifico (ad esempio, un adattatore di rete wireless).
- **Protocollo** - il protocollo IP al quale si applica la regola.Potrai visualizzare uno dei seguenti:

Protocollo	Descrizione
Qualsiasi	Include tutti i protocolli IP.
TCP	Transmission Control Protocol – Il Protocollo TCP abilita due host a stabilire una connessione e a scambiarsi pacchetti di dati. TCP garantisce la consegna dei dati e anche che questi pacchetti saranno consegnati nello stesso ordine in cui sono stati inviati.
UDP	User Datagram Protocol – UDP è un IP progettato per elevate prestazioni. I giochi e altre applicazioni video utilizzano spesso UDP.
Un numero	Rappresenta un protocollo IP specifico (diverso da TCP e UDP).Puoi trovare l'elenco completo dei numeri di protocolli IP assegnati su http://www.iana.org/assignments/protocol-numbers.

- **Azione** - Se all'applicazione è permesso o vietato l'accesso alla rete o a Internet sotto le circostanze specificate.

Per gestire le regole, usa i pulsanti nella parte inferiore della finestra:

- **Aggiungi regola** - Apre la finestra Aggiungi regola applicazione, dove puoi creare una nuova regola.
- **Modifica regola** - Apre la finestra Modifica regola applicazione dove puoi modificare le impostazioni di una regola selezionata.
- **Rimuovi regola** - Elimina la regola selezionata.

Aggiungere / modificare le regole applicazione

Per aggiungere o modificare una regola applicazione, clicca sul pulsante corrispondente.Comparirà una nuova finestra. Procedi come segue:

- **Percorso del Programma.** Clicca su **Sfoglia** e seleziona l'applicazione sulla quale applicare la regola.
- **Indirizzo locale.** Specifica l'indirizzo IP locale e la porta sui quali sarà applicata la regola.Se hai più di un adattatore di rete, puoi deselezionare la casella **Qualsiasi** e digitare un indirizzo IP specifico.
- **Indirizzo remoto.** Specifica l'indirizzo IP remoto e la porta sui quali sarà applicata la regola.Per filtrare il traffico tra il tuo computer e un computer specifico, deseleziona la casella **Qualsiasi** e digita il suo indirizzo IP.
- **Tipo di rete.** Seleziona il tipo di rete a cui si applica la regola.
- **Eventi.** In base al protocollo selezionato, scegli gli eventi di rete sui quali la regola sarà applicata.Possono essere considerati i seguenti eventi:

Evento	Descrizione
Connessione	Scambio preliminare di messaggi standard usati da protocolli orientati alla connessione (come il TCP) per stabilire una connessione.Con protocolli orientati alla connessione, il traffico di dati tra due computer si verifica solo dopo che la connessione è stata stabilita.
Traffico	Flusso di dati tra due computer.
In ascolto	Stato in cui un'applicazione monitorizza la rete in attesa di stabilire una connessione o di ricevere informazioni da un'applicazione pari.

- **Protocollo.** Seleziona dal menu il protocollo IP sul quale la regola sarà applicata.
  - Se desideri che la regola venga applicata a tutti i protocolli, seleziona **Qualsiasi**.
  - Se desideri che la regola venga applicata a TCP, seleziona **TCP**.
  - Se desideri che la regola venga applicata a UDP, seleziona **UDP**.
  - Se desideri che la regola venga applicata su un protocollo specifico, seleziona **Altro**.Comparirà uno spazio apposito.Digita il numero assegnato al protocollo che desideri filtrare nello spazio apposito.

    Nota

    I numeri dei protocolli IP vengono assegnati dalla Internet Assigned Numbers Authority (IANA).Puoi trovare l'elenco completo dei numeri di protocolli IP assegnati su http://www.iana.org/assignments/protocol-numbers.

- **Direzione.** Seleziona dal menu la direzione del traffico alla quale sarà applicata la regola.

Direzione	Descrizione
In uscita	La regola sarà applicata solo per il traffico in uscita.
In entrata	La regola sarà applicata solo per il traffico in entrata.
Entrambi	La regola sarà applicata in entrambe le direzioni.

- **Versione IP.** Seleziona dal menu la versione IP (IPv4, IPv6 o altre) alla quale sarà applicata la regola.
- **Autorizzazione.** Seleziona uno dei permessi disponibili:

Autorizzazione	Descrizione
Consenti	L'accesso alla rete / Internet dell'applicazione sarà autorizzato quando si verifichino le circostanze specificate.
Nega	L'accesso alla rete / Internet dell'applicazione sarà negato nelle circostanze specificate.

19.3.3. Regole adattatore

Per ogni connessione di rete puoi configurare zone sicure e non sicure.

Una zona di fiducia è un dispositivo di cui ti fidi completamente, per esempio un computer o una stampante.Tutto il traffico tra il computer e un dispositivo affidabile è consentito.Per condividere delle risorse con un computer specifico in una rete wireless non sicura, aggiungerli come computer consentiti.

Una zona non sicura è un dispositivo con cui non vuoi proprio comunicare.

Per visualizzare e gestire le zone sui tuoi adattatori di rete, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Impostazioni**.
5. Nelle regole del Firewall, clicca su **Regole adattatore**.

Comparirà una nuova finestra indicante gli adattatori di rete con connessioni attive e le zone attuali, se presenti.

Per gestire le zone, usa i pulsanti nella parte inferiore della finestra:

- **Agg. zona** - Apre la finestra Aggiungi indirizzo IP, dove puoi creare una nuova zona per un adattatore selezionato.
- **Modifica zona** - Apre la finestra Modifica regola dove puoi modificare le impostazioni di una zona selezionata.
- **Rimuovi zona** - elimina la zona selezionata.

Aggiungere / modificare le zone

Per aggiungere o modificare una zona, clicca sul pulsante corrispondente.Comparirà una nuova finestra con gli indirizzi IP dei dispositivi connessi alla rete.Procedi come segue:

1. Seleziona l'indirizzo IP del computer che vuoi aggiungere o digita un indirizzo o un intervallo di indirizzi nella casella di testo.
2. Seleziona l'azione:

- **Consenti** - Per consentire tutto il traffico tra il tuo computer e quello selezionato.
- **Rifiuta** - Per bloccare tutto il traffico tra il tuo computer e quello selezionato.

3. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

19.4. Monitorare le attività della rete

Per monitorare l'attività della rete / Internet corrente (su TCP e UDP) ordinata per applicazioni e aprire il registro del firewall di Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Impostazioni**.
5. In Attività di rete, clicca su **Attività di rete**.

Comparirà una nuova finestra.È possibile visualizzare il traffico totale generato dall'applicazione. Per ogni applicazione, è possibile visualizzare le connessioni e le porte aperte, così come le statistiche riguardanti la velocità del traffico in uscita e in entrata e la quantità totale di dati inviati / ricevuti.

Accanto a ogni connessione è indicata un'icona.Ecco cosa significano le icone:

- Indica una connessione in uscita.
- Indica una connessione in entrata.
- Indica una porta aperta sul tuo computer.

La finestra presenta l'attività della rete corrente / Internet in tempo reale. Se le connessioni o le porte fossero chiuse, le statistiche corrispondenti sarebbero opache e alla fine scomparirebbero.La stessa cosa accade a tutte le statistiche corrispondenti a un'applicazione che genera traffico o ha delle porte aperte e che tu chiudi.

Per un elenco esauriente di eventi riguardanti l'utilizzo del modulo Firewall (abilitare/disabilitare il firewall, bloccare il traffico, modificare le impostazioni) o generati dalle attività rilevate da questo modulo (scansione delle porte, blocco di tentativi di connessione o del traffico secondo le regole), visualizza il file di rapporto del firewall Bitdefender cliccando su **Rapporto**.L'ubicazione del file del registro è `?\Programmi\File comuni\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

19.5. Configurare l'intensità degli avvisi

Bitdefender Internet Security è stato progettato per essere il meno invadente possibile.In condizioni normali, non devi decidere se consentire o bloccare

connessioni o azioni intraprese da applicazioni in esecuzione sul tuo sistema.Bitdefender prenderà tutte le decisioni per te.

Se desideri avere il controllo completo delle decisioni intraprese, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Impostazioni**.
5. Attiva la **modalità Paranoid** cliccando sull'interruttore corrispondente.

Nota
Quando la modalità Paranoid è attivata, l'Autopilot viene disattivato automaticamente.

Finché la modalità Paranoid è attiva, ogni volta che si verifica una delle seguenti situazioni ti sarà chiesto come comportarti:

- Un'applicazione tenta di connettersi a Internet.
- Un'applicazione prova a eseguire un'azione considerata sospetta dal Sistema di rilevazione intrusioni o da Active Virus Control.

L'avviso contiene informazioni relative all'applicazione e al comportamento rilevato.Devi selezionare **Consenti** o **Nega** usando il pulsante corrispondente.

19.6. Configurare le impostazioni avanzate

Per configurare le impostazioni avanzate del firewall, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Avanzate**.

19.6.1. Sistema di rilevazione intrusioni

Per configurare il Sistema di rilevazione intrusioni, segui questi passaggi:

1. Per attivare il Sistema di rilevazione intrusioni, clicca sull'interruttore corrispondente.
2. Trascina il pulsante scorrevole lungo la barra per impostare il livello di aggressività desiderato.Usa la descrizione sul lato destro della barra per selezionare il livello di protezione che si adatta meglio alle tue necessità di sicurezza.

Puoi verificare quali applicazioni sono state rilevate dal Sistema di rilevazione intrusioni nella finestra Eventi.

Se ci sono applicazioni di cui ti fidi e non vuoi che il Sistema di rilevazione intrusioni le controlli, puoi aggiungere delle regole di eccezione per loro.Per escludere un'applicazione dalla scansione, segui i passaggi descritti nella sezione *«Gestire i processi esclusi»* (p. 94).

Nota

Il funzionamento del Sistema di rilevazione intrusioni è legato a quello dell'Active Virus Control.Le regole di eccezione per il processo si applicano a entrambi i sistemi.

19.6.2. Altre opzioni

Le seguenti funzioni possono essere attivate o disattivate.

- **Condivisione connessione a Internet** - Attiva il supporto della Condivisione connessione a Internet.

  Nota

  Questa opzione non attiva automaticamente la **Condivisione connessione a Internet** sul sistema, ma ti consente solo questo tipo di connessione nel caso tu la attivassi dal sistema operativo.

- **Blocca port scan** - Rileva e blocca i tentativi di scoprire quali porte sono aperte.

  Le scansioni delle porte vengono comunemente usate dagli hacker per scoprire quali porte sono aperte sul tuo computer.Potrebbero quindi introdursi nel computer, se trovassero una porta meno sicura o vulnerabile.

- **Aumenta la verbosità del registro** - aumenta la verbosità del registro del firewall.

  Bitdefender conserva un registro esauriente di eventi riguardanti l'utilizzo del modulo Firewall (attivare/disattivare il firewall, bloccare il traffico, modificare le impostazioni) o generati dalle attività rilevate da questo modulo (scansione delle porte, blocco di tentativi di connessione o del traffico secondo le regole).Puoi accedere al registro dalla finestra **Attività firewall** cliccando su **Rapporto**.

- **Monitora connessioni Wi-Fi** - Se si è connessi a una rete wireless, mostra delle finestre informative relative a determinati eventi sulla rete (ad esempio, quando un nuovo computer accede alla rete).

20. Safepay: sicurezza per le transazioni online

Il computer sta diventando rapidamente lo strumento principale per fare acquisti ed eseguire transazioni bancarie online. Pagare bollette, trasferire denaro, acquistare praticamente tutto ciò che puoi immaginare non è mai stato così semplice e veloce.

Tutto ciò richiede l'invio su Internet di dati personali, come numero di conto e carta di credito, password e altre tipologie di informazioni private, in altre parole esattamente quel tipo di informazioni a cui gli hacker sono particolarmente interessati. Infatti, non conoscono soste nei loro sforzi per sottrarre tali informazioni, perciò non si è mai troppo prudenti sulla necessità di proteggere le proprie transazioni online.

Bitdefender Safepay è prima di tutto un browser protetto, un ambiente sigillato, concepito per proteggere e mantenere private le operazioni bancarie, gli acquisti e qualsiasi altro tipo di transazione online.

Per assicurare una migliore protezione della privacy, il Portafoglio Bitdefender è stato integrato in Bitdefender Safepay per proteggere le proprie credenziali ogni volta che si desidera accedere a indirizzi privati online. Per ulteriori informazioni, fare riferimento a «*Massima protezione per le tue credenziali*» (p. 129).

Bitdefender Safepay offre le seguenti funzioni:

- Blocca l'accesso al proprio desktop, impedendo qualsiasi tentativo di catturare delle immagini del proprio schermo.
- Protegge le tue password segrete mentre navighi online con il Portafoglio.
- È dotato di una tastiera virtuale che, quando viene utilizzata, rende impossibile agli hacker rilevare la combinazione di tasti premuta.
- È completamente indipendente dagli altri browser.
- È dotato di una protezione integrata degli hotspot da utilizzare quando il computer è connesso a reti Wi-Fi non protette.
- Supporta i segnalibri e consente di navigare nei propri siti bancari/commerciali preferiti.
- Non è limitato agli acquisti e alle transazioni bancarie online. Ma qualsiasi sito web può essere aperto in Bitdefender Safepay.

20.1. Utilizzare Bitdefender Safepay

Di norma, Bitdefender rileva l'accesso a un sito di online banking o a un negozio online in qualsiasi browser del computer e ti indica di eseguirlo in Bitdefender Safepay.

Per accedere all'interfaccia principale di Bitdefender Safepay, segui questi passaggi:

- Per **Windows XP**, **Windows Vista** e **Windows 7**:

1. Clicca su **Start** e poi seleziona **Tutti i programmi**.
2. Clicca su **Bitdefender**.
3. Clicca su **Bitdefender Safepay** o, più rapidamente, clicca due volte sul collegamento di Bitdefender Safepay sul desktop.

- Per **Windows 8**:

  Dal menu Start di Windows, localizza Bitdefender Safepay (puoi anche digitare direttamente "Bitdefender Safepay" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona. In alternativa, apri l'applicazione dal desktop e clicca due volte sul collegamento di Bitdefender Safepay.

Nota

Se il plugin Adobe Flash Player non è installato o aggiornato, comparirà un messaggio di Bitdefender. Clicca sul pulsante corrispondente per continuare.
Una volta completato il processo di installazione, per continuare le tue operazioni, dovrai riaprire manualmente il browser di Bitdefender Safepay.

Se sei abituato a utilizzare i browser per Internet, non avrai alcun problema con Bitdefender Safepay, poiché appare e si comporta proprio come un normale browser:

- Inserisci gli URL che desideri utilizzare nella barra degli indirizzi.
- Aggiungi schede per visitare più siti web nella finestra di Bitdefender Safepay, cliccando su  .
- Torna alla pagina precedente, vai alla successiva e aggiorna le pagine, utilizzando  rispettivamente.
- Accedi alle impostazioni di Bitdefender Safepay cliccando su  .
- proteggi le tue password con Portafoglio cliccando su  .
- Gestisci i tuoi segnalibri cliccando su  accanto alla barra degli indirizzi.
- Apri la tastiera virtuale, cliccando su  .

20.2. Configurare le impostazioni

Clicca su  per configurare le seguenti impostazioni:

Comportamento generale di Bitdefender Safepay

Scegli cosa succede quando accedi a un negozio online a un sito di online banking nel tuo browser standard:

- Apri automaticamente Bitdefender Safepay.

- Bitdefender ti chiede ogni volta come proseguire.
- Non utilizzare mai Bitdefender Safepay per le pagine visitate in un browser standard.

Elenco domini

Scegli come Bitdefender Safepay si comporterà quando visiti siti web di determinati domini nel tuo browser standard, aggiungendoli all'elenco dei domini e selezionando il comportamento per ciascuno:

- Apri automaticamente Bitdefender Safepay.
- Bitdefender ti chiede ogni volta come proseguire.
- Non utilizzare mai Bitdefender Safepay quando visiti una pagina di quel dato dominio in un browser standard.

20.3. Gestire i segnalibri

Se hai disattivato la rilevazione automatica di alcuni o di tutti i siti web, o semplicemente Bitdefender non rileva determinati siti, puoi aggiungere dei segnalibri a Bitdefender Safepay in modo da poter lanciare rapidamente i tuoi siti web preferiti in futuro.

Segui questi semplici passaggi per aggiungere un URL ai segnalibri di Bitdefender Safepay:

1. Clicca su  accanto alla barra degli indirizzi per aprire la pagina dei Segnalibri.

   Nota
   Di norma, la pagina dei Segnalibri viene aperta all'avvio di Bitdefender Safepay.

2. Clicca sul pulsante **+** per aggiungere un nuovo segnalibro.
3. Inserisci l'URL e il nome del segnalibro, poi clicca su **Crea**. L'URL viene aggiunto anche nell'elenco dei domini alla pagina delle impostazioni.

20.4. Protezione hotspot per reti non sicure

Utilizzando Bitdefender Safepay quando ci si connette a reti Wi-Fi non sicure (per esempio a un hotspot pubblico), la funzione Protezione hotspot offre un ulteriore livello di sicurezza. Questo servizio codifica le comunicazioni Internet su connessioni non sicure, garantendo la propria privacy indipendentemente dalla rete a cui si è connessi.

Per il corretto funzionamento della Protezione hotspot è necessario che i seguenti requisiti siano soddisfatti:

- Devi accedere a un account MyBitdefender da Bitdefender Internet Security.
- Il tuo computer è connesso a una rete non sicura.

Una volta soddisfatti i requisiti, Bitdefender ti segnalerà di utilizzare automaticamente la connessione sicura, ogni volta che apri Bitdefender Safepay. Devi solo inserire le tue credenziali di MyBitdefender quando ti saranno richieste.

La connessione sicura sarà inizializzata e, una volta stabilita la connessione, apparirà un messaggio nella finestra di Bitdefender Safepay. Di fronte all'URL nella barra degli indirizzi comparirà il simbolo per aiutarti a identificare facilmente le connessioni sicure.

21. Massima protezione per le tue credenziali

Oggi utilizziamo il computer per fare acquisti o pagare le bollette online, ma anche per collegarsi ai social network o per chattare.

Ma come tutti sanno bene, non è sempre facile ricordarsi le password!

E se non si fa attenzione durante la navigazione online, le nostre informazioni personali, come l'indirizzo e-mail, le credenziali d'accesso alla chat o i dati della carta di credito possono essere compromesse.

Conservare le proprie password o informazioni personali nella propria agenda o nel computer può essere pericoloso, perché potrebbero essere consultate e utilizzate da persone che intendono rubarle e sfruttarle. Inoltre, ricordare tutte le password dei propri account online o dei propri siti web preferiti non è certo un compito facile.

Quindi, non c'è un modo per trovare subito tutte le password quando ci servono? E possiamo essere certi che le nostre password segrete siano sempre al sicuro?

Il Portafoglio consente di gestire le password aiutandoti a memorizzarle, proteggendo la tua privacy e garantendoti sempre una navigazione online sicura.

Utilizzando una sola password principale per accedere alle tue credenziali, il Portafoglio semplifica la protezione delle password.

Per offrire la migliore protezione per le tue attività online, il Portafoglio è integrato in Bitdefender Safepay, garantendo così una soluzione unificata da tutti i metodi con cui i tuoi dati personali possono essere compromessi.

Il Portafoglio protegge le seguenti informazioni private:

- Informazioni personali, come l'indirizzo e-mail o il numero di telefono
- Credenziali d'accesso per i siti web
- Informazioni per il conto corrente bancario o il numero della carta di credito
- Dati di accesso per gli account e-mail
- Password per le applicazioni
- Password per le reti Wi-Fi

21.1. Configurare il Portafoglio

Una volta completata l'installazione e aperto il browser, una finestra pop-up ti avviserà della possibilità di utilizzare il Portafoglio per un'esperienza online più sicura.

Clicca su **Esplora** per avviare l'installazione guidata del Portafoglio. Segui la procedura guidata per completare l'installazione.

Durante questa fase possono essere eseguite due attività:

- Crea un nuovo database del Portafoglio per proteggere le tue password.

  Durante la fase d'installazione, ti sarà chiesto di proteggere il tuo Portafoglio con una password principale. La nuova password dovrebbe avere almeno 7 caratteri.

  Per creare una password molto sicura, utilizza almeno un numero o un simbolo e un carattere maiuscolo. Una volta impostata una password, chiunque cerchi di accedere al Portafoglio dovrà prima inserirla.

  Al termine dell'installazione, di norma vengono attivate le seguenti impostazioni del Portafoglio:

  - **Salva automaticamente le credenziali nel Portafoglio**.
  - **Chiedi la password principale quando accedo al computer**.
  - **Blocca automaticamente il Portafoglio quando lascio il PC incustodito**.
- Se in precedenza hai utilizzato il Portafoglio sul tuo sistema, puoi importare un database esistente.

Esporta il database del Portafoglio

Per esportare il database del Portafoglio, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Portafoglio**, clicca su **Gestisci** e seleziona **Esporta Portafoglio** dal menu a tendina.
3. Segui la procedura indicata per esportare il database del Portafoglio in una determinata posizione sul tuo sistema.

Crea un nuovo database del Portafoglio

Per creare un nuovo database del Portafoglio, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Portafoglio**, clicca su **Gestisci** e seleziona **Crea un nuovo Portafoglio** nel menu a tendina.
3. Comparirà una finestra di avviso per informarti che i dati attualmente memorizzati nel Portafoglio saranno eliminati. Clicca su **Sì** per eliminare il database esistente e continuare la procedura guidata. Per uscire dalla procedura guidata, clicca su **No**.

Gestisci le tue credenziali del Portafoglio

Per gestire le tue password, segui questi passaggi:

1. Apri la finestra di Bitdefender.

2. Nel pannello **Portafoglio**, clicca su **Gestisci** e seleziona **Apri Portafoglio** dal menu a tendina.

Comparirà una nuova finestra. Seleziona la categoria desiderata dalla parte superiore della finestra:

- I miei dati
- Siti web
- Online banking
- Impostazioni client e-mail
- App e abbonamenti
- Reti Wi-Fi

Aggiungere/modificare le password

- Per aggiungere una nuova password, seleziona la categoria desiderata in alto, clicca su **+ Aggiungi elemento**, inserisci le informazioni nei campi corrispondenti e clicca sul pulsante Salva.
- Per modificare una voce dalla tabella, selezionarla e fare clic sul pulsante **Modifica**.
- Per uscire, clicca su **Annulla**.
- Per rimuovere una voce, selezionala, clicca sul pulsante **Modifica** e seleziona **Elimina**.

21.2. Attivare o disattivare la protezione del Portafoglio

Per attivare o disattivare la protezione del Portafoglio, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Portafoglio**, clicca sull'interruttore per attivare o disattivare il **Portafoglio**.

21.3. Gestire le impostazioni del Portafoglio

Per configurare la password principale, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Portafoglio**.
4. Nella finestra **Impostazioni Portafoglio**, seleziona la scheda **Password principale**.

Sono disponibili le seguenti opzioni:

- **Chiedi la password principale quando accedo al computer** - Quando accedi al computer, ti sarà chiesto di inserire la password principale.
- **Chiedi la password principale quando apro il browser e le applicazioni** - Quando accedi al browser o a un'applicazione, ti sarà chiesto di inserire la password principale.
- **Blocca automaticamente il Portafoglio quando lascio il PC incustodito** - Quando torni al computer dopo circa 15 minuti, ti sarà chiesto di inserire la password principale.

Importante

Assicurati di non dimenticare la tua password principale o conservane una copia in un luogo sicuro. Se hai dimenticato la password, dovrai reinstallare il programma o contattare il supporto di Bitdefender.

Migliora la tua esperienza

Per selezionare i browser o le applicazioni in cui desideri integrare il Portafoglio, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Portafoglio**.
4. Nella finestra **Impostazioni Portafoglio**, seleziona la scheda **App avanzate**.

   Controlla se un'applicazione utilizza il Portafoglio e migliora la tua esperienza:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Yahoo! Messenger
   - Skype

Configurare l'opzione Compila automaticamente

La funzione Compila automaticamente semplifica la connessione con i tuoi siti web preferiti o l'accesso ai tuoi account online. La prima volta che inserisci le credenziali nel browser, il Portafoglio salverà automaticamente tutte le informazioni.

Per configurare le impostazioni dell'opzione **Compila automaticamente**, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Portafoglio**.

4. Nella finestra **Impostazioni Portafoglio**, seleziona la scheda **Opzioni Portafoglio**.
5. Puoi configurare le seguenti opzioni:
   - **Compila automaticamente le credenziali di accesso**:
     - **Compila automaticamente le credenziali di accesso ogni volta** - Le credenziali vengono inserite automaticamente nel browser.
     - **Chiedi la mia password principale prima della compilazione** - Devi indicare la password principale prima che le credenziali vengano inserite nel browser.
     - **Lasciami scegliere quando compilare automaticamente le mie credenziali di accesso** - Puoi inserire manualmente le credenziali nel browser.
   - **Configura la protezione dei dati di accesso del Portafoglio**:
     - **Salva automaticamente le credenziali nel Portafoglio** - Le credenziali di accesso vengono salvate e aggiornate automaticamente nel Portafoglio.
     - **Chiedi sempre** - Ti sarà chiesto ogni volta se desideri aggiungere le credenziali al Portafoglio.
     - **Non salvare, aggiornerò le informazioni manualmente** - Le credenziali possono essere aggiunte nel Portafoglio solo manualmente.

22. Contr. Genitori

Il Controllo dei Genitori vi permette di controllare l'accesso ad Internet e ad applicazioni specifiche di ogni utente che possieda un account nel sistema.

Una volta configurato il Controllo genitori, puoi scoprire facilmente ciò che i bambini fanno sul computer.

Tutto ciò che ti serve è un computer con accesso a Internet e un browser web.

Puoi configurare il Controllo genitori per bloccare:

- pagine web inappropriate.
- accesso a Internet, durante specifici periodi di tempo (come durante le ore di studio).
- applicazioni come giochi, chat, programmi di condivisione di file e altri.
- messaggi istantanei inviati da contatti chat diversi da quelli consentiti.

Controlla le attività dei bambini e modifica le impostazioni del Controllo genitori utilizzando MyBitdefender da qualsiasi computer o dispositivo mobile connesso a Internet.

22.1. Accedere alla dashboard del Controllo genitori

La dashboard del Controllo genitori è organizzata in moduli da cui puoi monitorare le attività dei bambini sul computer.

Bitdefender ti consente di limitare l'accesso a Internet e a determinate applicazioni da parte dei bambini. Allo stesso tempo, ti consente di monitorare le attività dei loro account Facebook.

Con Bitdefender puoi accedere alle impostazioni del Controllo genitori dall'account MyBitdefender su qualsiasi computer o dispositivo mobile connesso a Internet.

Accedi al tuo account online:

- Da qualsiasi dispositivo con accesso a Internet:
  1. Apri un browser web.
  2. Vai a:https://my.bitdefender.com
  3. Accedi al tuo account usando il tuo nome utente e la password.
  4. Clicca su **Controllo genitori** per accedere alla dashboard.
- Dall'interfaccia di Bitdefender:
  1. Assicurati di aver avviato il computer con un account amministratore. Solo gli utenti con diritti di amministrazione (amministratori del sistema) possono accedere e configurare il Controllo genitori.

2. Apri la finestra di Bitdefender.
3. Vai al pannello **Controllo genitori** e clicca sull'interruttore per attivarlo.
4. Clicca sul pulsante **Configura**.

   Assicurati di aver eseguito l'accesso al tuo account MyBitdefender.
5. La dashboard del Controllo genitori si aprirà in una nuova finestra. Qui puoi selezionare e configurare le impostazioni del Controllo genitori di ogni account di Windows.

22.2. Aggiungere il profilo dei propri bambini

Prima di configurare il Controllo genitori, crea degli account utente di Windows separati per i bambini. In questo modo potrai sapere esattamente cosa sta facendo ognuno di loro sul computer. Dovresti creare degli account utente limitati (standard), in modo che non possano modificare le impostazioni del Controllo genitori. Per ulteriori informazioni, fare riferimento a «*Come posso creare gli account utente di Windows?*» (p. 59).

Per aggiungere il profilo dei propri bambini al Controllo genitori:

1. Accedi alla dashboard del Controllo genitori dall'account MyBitdefender.
2. Clicca su **Aggiungi bambino** nel menu di sinistra.
3. Inserisci il nome e l'età del bambino nei campi corrispondenti. Impostando l'età del bambino caricherai automaticamente le impostazioni considerate appropriate per quella categoria d'età, in base agli standard di sviluppo del bambino.
4. Sotto puoi visualizzare i dispositivi associati al tuo account MyBitdefender.
5. Seleziona il computer e l'account di Windows per il bambino.
6. Cliccare su **Crea profilo**.

   Ora il computer e l'account di Windows del bambino sono collegati al tuo account MyBitdefender.

22.2.1. Installare il Controllo genitori su un dispositivo Android

Per installare il Controllo genitori sul dispositivo mobile del bambino, segui questi passaggi:

1. Accedi alla dashboard del Controllo genitori dall'account MyBitdefender.
2. Clicca su **Aggiungi bambino** nel menu di sinistra.
3. Inserisci il nome e l'età del bambino nei campi corrispondenti. Impostando l'età del bambino caricherai automaticamente le impostazioni considerate appropriate per quella categoria d'età, in base agli standard di sviluppo del bambino.
4. Clicca su **Installa su un nuovo dispositivo** per continuare.

5. Comparirà una nuova finestra. Seleziona **Google Play** dall'elenco.
6. Per scaricare e installare il Controllo genitori sul dispositivo, clicca sul pulsante **Installa**.
7. Seleziona il dispositivo su cui vuoi installare l'applicazione.
8. Clicca su **Installa** per continuare.

   Attendi che l'applicazione sia installata sul dispositivo. Assicurati che il dispositivo del bambino sia connesso a Internet.
9. Al termine dell'installazione, ti sarà chiesto di attribuire i privilegi di amministratore all'applicazione sul dispositivo.
10. Tocca **Accetta** per completare l'installazione.

Associare il Controllo genitori a MyBitdefender

Per monitorare le attività online del bambino, devi associare il suo dispositivo con il tuo account MyBitdefender, accedendo all'account dall'applicazione.

Per associare il dispositivo al tuo account MyBitdefender, segui questi passaggi:

1. Inserisci il nome utente e la password di MyBitdefender.

   Se non possiedi un account, scegli di crearne uno nuovo utilizzando il pulsante corrispondente.

   Nota
   Puoi anche inserire un nome per il dispositivo. Se colleghi più di un dispositivo all'account, ti aiuterà a identificare più facilmente i dispositivi.

2. Tocca **Accedi**.

   Ora il dispositivo del bambino è associato al tuo account MyBitdefender, perciò puoi iniziare a monitorare le sue attività online.

22.2.2. Monitorare le attività dei bambini

Bitdefender ti aiuta a monitorare le attività online dei bambini.

In questo modo, puoi sempre scoprire esattamente quali siti web hanno visitato, quali applicazioni hanno usato o quali attività sono state bloccate dal Controllo genitori.

I rapporti contengono informazioni dettagliate per ogni evento, come:

- Lo stato dell'evento.
- Il nome del sito web bloccato.
- Il nome dell'applicazione bloccata.

- Il nome del dispositivo.
- La data e l'ora in cui si è verificato l'evento.
- Le azioni intraprese da Bitdefender.

Per monitorare il traffico web, le applicazioni utilizzate o le attività Facebook dei bambini, segui questi passaggi:

1. Accedi alla dashboard del Controllo genitori dall'account MyBitdefender.
2. Clicca su  per accedere alla finestra delle attività del modulo corrispondente.

22.2.3. Configurazione delle Impostazioni Generali

Di norma, quando il Controllo genitori è abilitato, le attività dei bambini vengono annotate.

Per ricevere e-mail di notifica, segui questi passaggi:

1. Accedi alla dashboard del Controllo genitori dall'account MyBitdefender.
2. Clicca sull'icona **Impostazioni generali**  nell'angolo in alto a destra.
3. Attiva l'opzione per ricevere dei rapporti sulle attività.
4. Inserisci l'indirizzo e-mail in cui vuoi ricevere le notifiche e-mail.
5. Imposta la frequenza selezionando: quotidianamente, settimanalmente o mensilmente.
6. Riceverai le notifiche via e-mail per le seguenti informazioni:
   - Siti web bloccati
   - App bloccate
   - Contatti chat bloccati
   - SMS da un contatto bloccato
   - Chiamate ricevute da un numero di telefono bloccato
   - Rimozione dell'applicazione Facebook Controllo genitori
7. Clicca su **Salva**.

Verifica la sezione **Informazioni Account**. Puoi visualizzare lo stato della registrazione, il codice di licenza attuale e la sua data di scadenza.

22.3. Configurazione Controllo genitori

Nella dashboard del Controllo genitori puoi gestire direttamente i moduli del Controllo genitori.

Ogni modulo contiene i seguenti elementi: il nome del modulo, un messaggio di stato, l'icona del modulo e un pulsante che ti consente di eseguire le attività più importanti per il modulo stesso.

Clicca su una scheda per configurare la caratteristica corrispondente del Controllo genitori per il computer:

- Web - Per filtrare la navigazione web e impostare limiti temporali nell'accesso a Internet.
- Applicazioni - Per bloccare o limitare l'accesso a determinate applicazioni.
- Facebook - Per proteggere l'account Facebook dei bambini.
- Chat - Per consentire o bloccare la chat con determinati contatti.

È possibile accedere ai seguenti moduli per monitorare le attività dei bambini sul dispositivo mobile:

- Ubicazione - Per trovare la posizione attuale del dispositivo dei bambini su Google Maps.
- SMS - Per bloccare i messaggi di testo in entrata da un numero di telefono.
- Chiamate - Per bloccare le chiamate da un numero di telefono, sia in arrivo che in uscita.

22.3.1. Controllo web

Il Controllo web ti aiuta a bloccare i siti web con contenuti inappropriati e a impostare limitazioni temporali nell'utilizzo di Internet.

Per configurare il Controllo web per un determinato account utente:

1. Vai alla scheda **Web**.
2. Clicca su nel pannello **Web** per accedere alla finestra **Attività web**.
3. Usa l'interruttore per attivare le **Attività web**.

Consentire o bloccare un sito web

Usa la finestra **Attività web** per visualizzare tutte le pagine web visitate dal bambino.

- Per bloccare l'accesso a un sito web, segui questi passaggi:
  1. Clicca sul pulsante **Blacklist**.
  2. Inserisci il sito web nel campo corrispondente.
  3. Clicca su **Aggiungi** per aggiungere il sito web all'elenco.

4. Seleziona dalla griglia gli intervalli di tempo durante i quali è consentito l'accesso. Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi.

   Clicca sul pulsante **Salva**.

5. Se cambiassi idea, seleziona il sito web e clicca sul pulsante **Rimuovi** corrispondente.

- Per consentire l'accesso a un sito web bloccato, segui questi passaggi:

1. Clicca sul pulsante **Blacklist**.
2. Inserisci il sito web nel campo corrispondente.
3. Clicca su **Aggiungi** per aggiungere il sito web all'elenco.
4. Seleziona dalla griglia gli intervalli di tempo durante i quali è consentito l'accesso. Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi.

   Clicca sul pulsante **Salva**.

5. Se cambiassi idea, seleziona il sito web e clicca sul pulsante **Rimuovi** corrispondente.

Controllo parole chiave

Il Controllo parole chiave ti aiuta a bloccare l'accesso degli utenti a messaggi chat e pagine web, che contengono determinate parole. Utilizzando il Controllo parole chiave, puoi impedire ai bambini di vedere parole o frasi inappropriate quando sono online. In più, puoi assicurarti che non saranno inoltrate informazioni personali (come indirizzo di casa o numeri di telefono) alle persone che incontrano su Internet.

Per configurare il Controllo parole chiave per un determinato account utente, segui questi passaggi:

1. Clicca sul pulsante **Parole chiave**.
2. Inserisci la parola chiave nel campo corrispondente.
3. Clicca su **Blocca** per aggiungere la parola all'elenco delle parole bloccate. Se cambiassi idea, clicca sul pulsante corrispondente **Rimuovi**.

Filtro categorie

Il Filtro categorie filtra dinamicamente l'accesso ai siti web in base ai loro contenuti. Impostando l'età dei bambini, il filtro viene configurato automaticamente per bloccare l'accesso alle categorie di siti web considerati inappropriati per l'età dei bambini. Questa configurazione è adatta alla maggior parte dei casi.

Se desideri controllare maggiormente i contenuti Internet a cui i bambini possono accedere, puoi selezionare quali categorie di siti web bloccare con il Filtro categorie.

Per configurare nei dettagli le impostazioni del Filtro categorie per un determinato account utente, segui questi passaggi:

1. Clicca sul pulsante **Categorie**.
2. Puoi verificare quali categorie web sono bloccate automaticamente o limitate per il gruppo d'età attualmente selezionato. Se non sei soddisfatto delle impostazioni di default, puoi configurarle a tuo piacimento.
3. Clicca su **Salva**. Se dovessi cambiare idea, clicca sul pulsante **Reimposta** per utilizzare il livello di protezione predefinito in base all'età del bambino.

Limitare gli intervalli di accesso a Internet

Puoi specificare quando è consentito al bambino di accedere a Internet usando l'opzione **Elenco** nella finestra **Attività web**.

Per configurare nei dettagli l'accesso a Internet per un determinato account utente, segui questi passaggi:

1. Clicca sul pulsante **Programmazione**.
2. Seleziona dalla griglia gli intervalli di tempo durante i quali bloccare l'accesso a Internet. Puoi cliccare sulle singole caselle oppure puoi cliccare e trascinare per coprire periodi più lunghi.
3. Clicca sul pulsante **Salva**.

22.3.2. Controllo applicazioni

Il Controllo applicazioni ti aiuta a impedire l'esecuzione di qualsiasi applicazione. Giochi, messaggi software, oltre ad altre categorie di software e minacce che in questo caso possono essere bloccati.

Per configurare il Controllo applicazioni per un determinato account utente, segui questi passaggi:

1. Vai alla scheda **Applicazioni**.
2. Clicca su  nel pannello **Applicazioni** per accedere alla finestra **Attività applicazioni**.
3. Usa l'interruttore per attivare l'opzione **Attività applicazioni**.
4. Clicca sul pulsante **Blacklist**.
5. Inserisci il nome dell'applicazione:
   - Per bloccare una app per un dispositivo mobile, seleziona le applicazioni che desideri bloccare dall'elenco **app consentite**.
   - Per bloccare un'applicazione nel sistema operativo Windows, aggiungi il file eseguibile dell'applicazione che desideri bloccare (.exe).

6. Clicca su **Blocca** per aggiungere l'applicazione all'elenco delle **App bloccate** o **Consenti** per aggiungerla all'elenco delle **App consentite**.

22.3.3. Protezione per Facebook

Il Controllo genitori monitora l'account Facebook dei bambini e segnala tutte le loro principali attività.

Queste attività online sono verificate e se si dimostrassero essere una minaccia per la privacy del tuo account, sarai avvisato.

Gli elementi monitorati dell'account online includono:

- Il numero di amici
- I commenti dei bambini o dei loro amici sui propri messaggi e sulle proprie foto
- I messaggi
- I messaggi in bacheca
- Le foto e i video inviati
- Le impostazioni della privacy dell'account

Per configurare la protezione Facebook per un determinato account utente:

1. Vai alla scheda **Facebook**.
2. Clicca su **Collega il profilo del bambino** nel pannello **Facebook**.
3. Per proteggere l'account Facebook dei bambini, installa l'applicazione utilizzando il link corrispondente.

Nota
Per installare l'applicazione ti serviranno le credenziali del profilo Facebook del bambino.

Per smettere di monitorare l'account di Facebook, utilizza il pulsante **Scollega account** in alto.

22.3.4. Controllo chat

Il Controllo chat ti consente di specificare i contatti con cui i bambini possono chattare o bloccare l'accesso a messaggi di chat che contengono determinate parole.

Nota
Il Controllo chat è disponibile solo per Yahoo! Messenger e Windows Live (MSN) Messenger.

Per configurare il Controllo chat per un determinato account utente, segui questi passaggi:

1. Vai alla scheda **Chat**.
2. Clicca su sul pannello **Chat** per accedere alla finestra **Attività chat**.
3. Usa l'interruttore per attivare l'opzione **Attività chat**.

   Limita l'accesso alla **Chat** utilizzando una delle opzioni disponibili:

   - Il pulsante **Blacklist** per inserire gli indirizzi e-mail associati con l'ID per la chat.
   - Il pulsante **Parole chiave** per bloccare l'accesso ai messaggi chat che contengono determinate parole.

22.3.5. Ubicazione

Scopri la posizione attuale del dispositivo su Google Maps. La posizione è aggiornata ogni 5 secondi, in modo da poterlo rintracciare, se è in movimento.

L'accuratezza della posizione dipende da come Bitdefender può rilevarla:

- Se nel dispositivo il GPS è attivato, la sua posizione può essere determinata con un'accuratezza di un paio di metri, finché resta nel raggio dei satelliti GPS (ad esempio, non dentro a un edificio).
- Se il dispositivo è in un edificio, la sua posizione può essere determinata entro decine di metri, se il Wi-Fi è attivato e ci sono reti wireless disponibili nel suo raggio d'azione.
- Diversamente, la posizione sarà determinata usando solo le informazioni dalla rete mobile, che offrono un'accuratezza non superiore a diverse centinaia di metri.

Nota
For the **Geolocalizzazione remota**

22.3.6. Controllo dei messaggi di testo

Il controllo dei messaggi di testo ti aiuta a bloccare messaggi di testo in arrivo e relativi a un determinato numero di telefono.

- Per bloccare i messaggi di testo ricevuti da un numero di telefono, segui questi passaggi:

  1. Vai alla scheda **SMS**.
  2. Clicca su nel pannello **SMS** per accedere alla finestra **Attività SMS**.
  3. Usa l'interruttore per attivare le **Attività SMS**.
  4. Clicca sul pulsante **Blacklist**.
  5. Aggiungi un numero di telefono nel campo corrispondente.

6. Clicca su **Blocca** per aggiungere il numero di telefono nella blacklist. Il numero di telefono sarà aggiunto all'elenco dei numeri bloccati.

- Per consentire la ricezione dei messaggi di testo da un numero di telefono bloccato, segui questi passaggi:

  1. Clicca sul pulsante **Blacklist** in alto.
  2. Selezionare il numero telefonico dall'elenco.
  3. Clicca su **Rimuovi**. Il numero di telefono sarà rimosso dall'elenco dei numeri bloccati.

Nota
Assicurati di utilizzare il codice paese corretto quando inserisci il numero di telefono nell'elenco.

22.3.7. Controllo dei numeri di telefono

Il controllo dei numeri di telefono ti aiuta a fermare l'invio o la ricezione di chiamate relative a un determinato numero di telefono.

- Per bloccare l'invio o la ricezione di chiamate relative a un determinato numero di telefono, segui questi passaggi:

  1. Vai alla scheda **Chiamate**.
  2. Clicca su nel pannello **Chiamate** per accedere alla finestra **Attività chiamate**.
  3. Usa l'interruttore per attivare le **Attività chiamate**.
  4. Clicca sul pulsante **Blacklist**.
  5. Aggiungi un numero di telefono nel campo corrispondente.
  6. Clicca su **Blocca** per aggiungere il numero di telefono nella blacklist. Il numero di telefono sarà aggiunto all'elenco dei numeri bloccati.

- Per consentire le chiamate a un numero di telefono bloccato, segui questi passaggi:

  1. Clicca sul pulsante **Blacklist** in alto.
  2. Selezionare il numero telefonico dall'elenco.
  3. Clicca su **Rimuovi**. Il numero di telefono sarà rimosso dall'elenco dei numeri bloccati.

Nota
Assicurati di utilizzare il codice paese corretto quando inserisci il numero di telefono nell'elenco.

23. Protezione di Safego per Facebook

Ti fidi dei tuoi amici online, ma ti fidi dei loro computer?Usa la protezione di Safego per Facebook per proteggere il tuo account e i tuoi amici dalle minacce online.

Safego è un'applicazione di Bitdefender sviluppata per proteggere il tuo account di Facebook.Il suo compito è controllare i link che ricevi dai tuoi amici e monitorare le impostazioni sulla privacy del tuo account.

Nota
Per usare questa caratteristica serve un account MyBitdefender.
Per ulteriori informazioni, fare riferimento a *«Account MyBitdefender»* (p. 35).

Queste sono le principali caratteristiche disponibili per il tuo account di Facebook:

- Controlla automaticamente i messaggi nelle tue notizie alla ricerca di link pericolosi.
- Protegge il tuo account dalle minacce online.

  Quando rileva un post o un commento che non è nient'altro che spam, phishing o malware, riceverai un messaggio di avvertimento.
- Avvisa i tuoi amici su eventuali link sospetti pubblicati nelle loro notizie.
- Ti aiuta a costruire una rete sicura di amici usando la funzione **Friend'O'Meter**.
- Ottieni un controllo dello stato di sicurezza del sistema fornito da Bitdefender QuickScan.

Per accedere a Safego per Facebook, segui questi passaggi:

- Dall'interfaccia di Bitdefender:
  1. Apri la finestra di Bitdefender.
  2. Nel pannello **Safego**, clicca su **Gestisci** e seleziona **Attiva per Facebook** dal menu a tendina.

     Sarai indirizzato al tuo account.
  3. Usa le tue informazioni di accesso a Facebook per connetterti all'applicazione Safego.
  4. Consenti a Safego di accedere al tuo account Facebook.

  Se Safego è già stato attivato, potrai accedere ad alcune statistiche sulla sua attività, selezionando **Rapporto per Facebook** nel menu.
- Da account MyBitdefender:
  1. Vai a: https://my.bitdefender.com.
  2. Accedi al tuo account usando il tuo nome utente e la password.

3. Clicca su **Protezione per Facebook**.

   Viene visualizzato un messaggio per informarti che la protezione per il tuo account Facebook non è stata attivata.

4. Clicca su **Attiva** per continuare.

   Sarai indirizzato al tuo account.

5. Usa le tue informazioni di accesso a Facebook per connetterti all'applicazione Safego.

6. Consenti a Safego di accedere al tuo account Facebook.

24. Bitdefender USB Immunizer

La funzione di esecuzione automatica inclusa nei sistemi operativi Windows è uno strumento molto utile che consente ai computer di eseguire automaticamente un file da un qualsiasi supporto a esso collegato. Per esempio, l'installazione di un software si avvia automaticamente, inserendo un CD nel lettore ottico.

Sfortunatamente, questa funzione può essere utilizzata anche dai malware per avviarsi automaticamente e infiltrarsi nel tuo computer da supporti riscrivibili, come unità USB e schede di memoria, collegate tramite lettori di schede. Negli ultimi anni, sono stati rilevati moltissimi attacchi basati sull'esecuzione automatica.

Con USB Immunizer puoi impedire a qualsiasi unità flash formattata in NTFS, FAT32 o FAT dall'eseguire automaticamente ogni malware. Una volta che un dispositivo USB è immunizzato, i malware non possono più configurarlo per eseguire una determinata applicazione quando il dispositivo viene collegato a un computer con Windows.

Per immunizzare un dispositivo USB, segui questi passaggi:

1. Collega l'unità flash al tuo computer.
2. Esegui una ricerca nel computer per localizzare il dispositivo di archiviazione rimovibile e clicca con il pulsante destro sulla sua icona.
3. Nel menu contestuale, seleziona **Bitdefender** e poi l'opzione **Immunizza questa unità**.

Nota

Se l'unità è già stata immunizzata, al posto dell'opzione Immunizza, comparirà il messaggio **L'unità USB è protetta da ogni malware basato sull'esecuzione automatica**.

Per impedire al computer di eseguire malware da dispositivi USB non immunizzati, disattiva la funzione di esecuzione automatica. Per ulteriori informazioni, fare riferimento a «*Usare il controllo automatico delle vulnerabilità*» (p. 97).

25. Gestire in remoto i tuoi computer

Il tuo account MyBitdefender ti consente di gestire in remoto i prodotti Bitdefender installati sui tuoi computer.

Utilizza MyBitdefender per creare ed eseguire attività per i tuoi computer da qualsiasi luogo.

Qualsiasi computer sarà gestito dall'account MyBitdefender, se soddisfa le seguenti condizioni:

- Hai installato un prodotto Bitdefender Internet Security sul computer
- Hai collegato il prodotto Bitdefender all'account MyBitdefender.
- Il computer è connesso a Internet

25.1. Accedere a MyBitdefender

Bitdefender ti consente di controllare la sicurezza dei tuoi computer aggiungendo attività ai tuoi prodotti Bitdefender.

Con Bitdefender puoi accedere al tuo account MyBitdefender da qualsiasi computer o dispositivo mobile connesso a Internet.

Accedi a MyBitdefender:

- Da qualsiasi dispositivo con accesso a Internet:
  1. Apri un browser web.
  2. Vai a:https://my.bitdefender.com
  3. Accedi al tuo account usando il tuo nome utente e la password.
- Dall'interfaccia di Bitdefender:
  1. Apri la finestra di Bitdefender.
  2. Clicca sul pulsante **MyBitdefender** nella parte superiore della finestra e seleziona **Dashboard** dal menu a tendina.

25.2. Eseguire le attività sui computer

Per eseguire un'attività su uno dei tuoi computer, accedi al tuo account MyBitdefender.

Cliccando sull'icona di un computer nella parte inferiore della finestra, puoi visualizzare tutte le attività di gestione eseguibili dal computer remoto.

Registrazione del prodotto
Ti consente di registrare Bitdefender sul computer remoto inserendo un codice di licenza.

Esegui una scansione completa del tuo PC
Ti consente di eseguire una scansione completa sul computer remoto.

Esegui una scansione delle aree critiche per rilevare eventuali malware attivi
Ti consente di eseguire una scansione veloce sul computer remoto.

Risolvi i problemi critici
Ti consente di risolvere i problemi che influenzano la sicurezza del computer remoto.

Aggiornamento del Prodotto
Avvia il processo di aggiornamento per il prodotto Bitdefender installato sul computer.

Risoluzione dei problemi

26. Risolvere i problemi più comuni

Questo capitolo illustra alcuni problemi che potresti incontrare utilizzando Bitdefender e ti fornisce alcune soluzioni possibili per questi problemi.La maggior parte di questi problemi può essere risolta attraverso la configurazione appropriata delle impostazioni del prodotto.

- «*Il mio sistema sembra lento*» (p. 150)
- «*La scansione non parte*» (p. 151)
- «*Non riesco più a usare un'applicazione*» (p. 154)
- «*Non riesco a connettermi a Internet*» (p. 155)
- «*Non riesco ad accedere a un dispositivo nella mia rete*» (p. 155)
- «*Internet è lento*» (p. 157)
- «*Come aggiornare Bitdefender con una connessione a Internet lenta*» (p. 158)
- «*Il mio computer non è connesso a Internet. Come aggiornare Bitdefender?*» (p. 159)
- «*I servizi Bitdefender non rispondono*» (p. 159)
- «*Il filtro antispam non funziona correttamente*» (p. 160)
- «*L'opzione Compila automaticamente nel mio Portafoglio non funziona*» (p. 165)
- «*Rimozione di Bitdefender non riuscita*» (p. 166)
- «*Il sistema non si riavvia dopo aver installato Bitdefender*» (p. 167)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 181).

26.1. Il mio sistema sembra lento

In genere, dopo aver installato un software di sicurezza, potrebbe verificarsi un certo rallentamento del sistema, che fino a un certo grado è normale.

Se noti un rallentamento significativo, questo problema si può verificare per le seguenti ragioni:

- **Bitdefender non è l'unico programma di sicurezza installato sul sistema.**

  Sebbene Bitdefender cerchi e rimuova i programmi di sicurezza trovati durante l'installazione, si consiglia di rimuovere ogni altro programma antivirus in uso prima dell'installazione di Bitdefender.Per ulteriori informazioni, fare riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 70).

- **Non ci sono i requisiti minimi di sistema per l'esecuzione di Bitdefender.**

Se il tuo computer non soddisfa i requisiti minimi di sistema, diventerà lento, specialmente quando si eseguono più applicazioni contemporaneamente.Per ulteriori informazioni, fare riferimento a «*Requisiti minimi di sistema*» (p. 3).

- **Le tue unità disco fisso sono troppo frammentate.**

  Un'eccessiva frammentazione rallenta l'accesso ai file e diminuisce le prestazioni del sistema.

  Per deframmentare il disco usando il tuo sistema operativo Windows, segui questo percorso dal menu start di Windows: **Start** → **Tutti i programmi** → **Accessori** → **Utilità di sistema** → **Utilità di deframmentazione dischi**.

- **Hai installato applicazioni che non utilizzi**.

  Ogni computer ha programmi o applicazioni che non si utilizzano. E molti programmi indesiderati sono eseguiti in background, occupando spazio su disco e memoria. Se non utilizzi un programma, disinstallalo. Ciò vale anche per qualsiasi altro programma pre-installato o di prova che ci si è dimenticati di rimuovere.

  Importante
  Se sospetti che un programma o un'applicazione sia essenziale per il sistema operativo, non rimuoverla e contatta il supporto clienti di Bitdefender.

- **Il tuo sistema potrebbe essere infetto**.

  La velocità del tuo sistema e le sue prestazioni generali possono essere anche influenzate dai malware. Spyware, virus, Trojan e adware contribuiscono a diminuire le prestazioni del computer. Assicurati di controllare periodicamente il tuo sistema, almeno una volta alla settimana. Si consiglia di usare la Scansione completa di sistema di Bitdefender perché controlla tutti i tipi di malware che minacciano la sicurezza del tuo sistema, oltre a eseguire una scansione degli archivi.

  Per avviare la Scansione di sistema, segui questi passaggi:

  1. Apri la finestra di Bitdefender.
  2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **Scansione sistema** dal menu a tendina.
  3. Segui i passaggi della procedura guidata.

26.2. La scansione non parte

Questo tipo di problema può avere due cause principali:

- **Un'installazione precedente di Bitdefender che non è stata rimossa completamente o un'installazione difettosa di Bitdefender**.

  In questo caso, segui questi passaggi:

1. Rimuovi completamente Bitdefender dal sistema:
   - Per **Windows XP**:
     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
     b. Attendi per qualche istante, finché non compare l'elenco del software installato.
     c. Trova **Bitdefender** e seleziona **Rimuovi**.
     d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.
     e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
   - Per **Windows Vista** e **Windows 7**:
     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
     b. Attendi per qualche istante, finché non compare l'elenco del software installato.
     c. Trova **Bitdefender** e seleziona **Disinstalla**.
     d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.
     e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
   - Per **Windows 8**:
     a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
     b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
     c. Attendi per qualche istante, finché non compare l'elenco del software installato.
     d. Trova **Bitdefender** e seleziona **Disinstalla**.
     e. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.
     f. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
2. Reinstalla il tuo prodotto Bitdefender.

- **Bitdefender non è l'unica soluzione di sicurezza installata sul tuo sistema**.

In questo caso, segui questi passaggi:

1. Rimuovi l'altra soluzione di sicurezza. Per ulteriori informazioni, fare riferimento a *«Come posso rimuovere le altre soluzioni di sicurezza?»* (p. 70).
2. Rimuovi completamente Bitdefender dal sistema:
   - Per **Windows XP**:
     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
     b. Attendi per qualche istante, finché non compare l'elenco del software installato.
     c. Trova **Bitdefender** e seleziona **Rimuovi**.
     d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.
     e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
   - Per **Windows Vista** e **Windows 7**:
     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
     b. Attendi per qualche istante, finché non compare l'elenco del software installato.
     c. Trova **Bitdefender** e seleziona **Disinstalla**.
     d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.
     e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
   - Per **Windows 8**:
     a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
     b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
     c. Attendi per qualche istante, finché non compare l'elenco del software installato.
     d. Trova **Bitdefender** e seleziona **Disinstalla**.
     e. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

f. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

3. Reinstalla il tuo prodotto Bitdefender.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

26.3. Non riesco più a usare un'applicazione

Questo problema si verifica quando stai cercando di usare un programma che prima dell'installazione di Bitdefender funzionava normalmente.

Dopo aver installato Bitdefender potrebbe verificarsi una di queste situazioni:

- Potresti ricevere un messaggio da Bitdefender che il programma sta cercando di eseguire una modifica al sistema.
- Potresti ricevere un messaggio d'errore dal programma che stai cercando di usare.

Questo tipo di situazione si verifica quando il modulo Active Virus Control per errore contrassegna alcune applicazioni come nocive.

L'Active Virus Control è un modulo di Bitdefender che monitora costantemente le applicazioni in esecuzione sul tuo sistema e segnala quelle con un comportamento potenzialmente maligno. Poiché questa opzione è basata su un sistema euristico, potrebbero verificarsi dei casi in cui applicazioni legittime siano rilevate dall'Active Virus Control.

Quando si verifica questa situazione, puoi escludere la rispettiva applicazione dal controllo dell'Active Virus Control.

Per aggiungere il programma all'elenco delle eccezioni, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
4. Nella finestra **Impostazioni antivirus**, seleziona la scheda **Eccezioni**.
5. Clicca sul collegamento **Processi esclusi**. Nella finestra che compare, puoi gestire le eccezioni del processo di Active Virus Control.
6. Aggiungi eccezioni seguendo questi passaggi:
   a. Clicca sul pulsante **Aggiungi** localizzato nella parte superiore della tabella delle eccezioni.
   b. Clicca su **Sfoglia**, trova e seleziona l'applicazione che vuoi escludere e poi clicca su **OK**.
   c. Mantieni l'opzione **Consenti** selezionata per impedire ad Active Virus Control di bloccare l'applicazione.

d. Clicca su **Aggiungi**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

26.4. Non riesco a connettermi a Internet

Dopo aver installato Bitdefender, potresti rilevare che un programma o un browser non è più in grado di connettersi a Internet o accedere ai servizi di rete.

In questo caso, la miglior soluzione è configurare Bitdefender per consentire automaticamente le connessioni da e per la rispettiva applicazione:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Impostazioni**.
5. Nelle regole del Firewall, clicca su **Regole applicazione**.
6. Per aggiungere una regola applicazione, clicca sul pulsante corrispondente.
7. Clicca su **Sfoglia** e seleziona l'applicazione sulla quale applicare la regola.
8. Seleziona tutti i tipi di rete disponibili.
9. Vai ad **Autorizzazione** e seleziona **Consenti**.

Chiudi Bitdefender, apri l'applicazione e riprova a connetterti a Internet.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

26.5. Non riesco ad accedere a un dispositivo nella mia rete

In base alla rete a cui sei connesso, il firewall di Bitdefender potrebbe bloccare la connessione tra il sistema e un altro dispositivo (come un altro computer o stampante). Di conseguenza, non potresti più condividere o stampare file.

In questo caso, la miglior soluzione è configurare Bitdefender per consentire automaticamente le connessioni da e per il rispettivo dispositivo. Per ogni connessione di rete puoi configurare una speciale zona di fiducia.

Una zona di fiducia è un dispositivo del quale ti fidi completamente. Tutto il traffico tra il computer e un dispositivo affidabile è consentito. Per condividere le risorse con dispositivi specifici, come computer o stampanti, aggiungili alle zone sicure.

Per aggiungere una zona di fiducia ai tuoi adattatori di rete, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.

3. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.
4. Nella finestra **Impostazioni firewall**, seleziona la scheda **Impostazioni**.
5. Nelle regole del Firewall, clicca su **Regole adattatore**.
6. Per aggiungere una zona, clicca sul pulsante corrispondente. Comparirà una nuova finestra con gli indirizzi IP dei dispositivi connessi alla rete.
7. Seleziona l'indirizzo IP del computer o della stampante che vuoi aggiungere o digita un indirizzo o un intervallo di indirizzi nella casella di testo.
8. Seleziona **Consenti** e poi clicca su **OK** e **Chiudi**.

Se non riesci ancora a collegarti al dispositivo, il problema potrebbe non essere causato da Bitdefender.

Controllare altre potenziali cause, ad esempio le seguenti:

- Il firewall su un altro computer potrebbe bloccare la condivisione di file e stampante con il tuo computer.
  - Se viene utilizzato il firewall di Windows, è possibile configurarlo per permettere la condivisione di file e stampanti nel modo seguente:
    - Per **Windows XP**:
      1. Clicca su **Start**, vai al **Pannello di controllo** e seleziona **Centro di sicurezza**.
      2. Apri la finestra delle impostazioni di Windows Firewall e seleziona la scheda **Eccezioni**.
      3. Seleziona la casella **Condivisione file e stampanti**.
    - Per **Windows Vista e Windows 7**:
      1. Clicca su **Start**, vai al **Pannello di controllo** e seleziona **Sistema e sicurezza**.
      2. Vai a **Windows Firewall** e clicca su **Consenti un programma con Windows Firewall**.
      3. Seleziona la casella **Condivisione file e stampanti**.
    - Per **Windows 8**:
      1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
      2. Clicca su **Sistema e sicurezza**, vai a **Windows Firewall** e seleziona **Consenti una app con Windows Firewall**.
      3. Seleziona la casella **Condivisione file e stampanti** e clicca su **OK**.

- Se viene utilizzato un altro programma firewall, fare riferimento alla sua documentazione o al file della guida.

- Condizioni generiche che possono impedire l'utilizzo o la connessione a una stampante condivisa:
  - Potrebbe essere necessario accedere a un account di amministratore di Windows per poter accedere alla stampante condivisa.
  - Potrebbero essere state impostate delle autorizzazioni per la stampante condivisa che permettono l'accesso solo a specifici computer e utenti. Se stai condividendo la tua stampante, controlla le autorizzazioni impostate per la stampante per verificare che l'utente dell'altro computer sia autorizzato ad accedervi. Se stai provando a collegarti a una stampante condivisa, controlla insieme all'utente dell'altro computer di disporre delle autorizzazioni al collegamento alla stampante.
  - La stampante collegata al proprio computer o all'altro computer non è condivisa.
  - La stampante condivisa non è stata aggiunta al computer.

  Nota
  Per apprendere come gestire la condivisione di stampanti (condividere una stampante, impostare o rimuovere autorizzazioni per una stampante, collegarsi a una stampante di rete o a una stampante condivisa) vai alla Guida in Linea e Supporto Tecnico di Windows (nel menu Start, clicca su **Guida in Linea e Supporto Tecnico**).

- L'accesso a una stampante di rete potrebbe essere ristretto a specifici computer o utenti. Controlla con l'amministratore della rete, se disponi delle autorizzazioni al collegamento con tale stampante.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

26.6. Internet è lento

Questa situazione potrebbe verificarsi dopo aver installato Bitdefender. Il problema potrebbe essere causato da errori nella configurazione del firewall di Bitdefender.

Per risolvere questa situazione, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Firewall**, clicca sull'interruttore per disattivare il **firewall**.
3. Verifica se la tua connessione a Internet è migliorata con il firewall di Bitdefender disattivato.

- Se hai ancora una connessione a Internet lenta, il problema potrebbe non essere causato da Bitdefender. Contatta il tuo fornitore di servizi Internet per verificare se la connessione è attiva.

  Se ricevi conferma dal tuo fornitore di servizi Internet che la connessione è operativa e il problema persiste, contatta Bitdefender come descritto nella sezione «*Chiedere aiuto*» (p. 181).

- Se la connessione a Internet è migliorata dopo aver disattivato il firewall di Bitdefender, segui questi passaggi:

  a. Apri la finestra di Bitdefender.

  b. Nel pannello **Firewall**, clicca sull'interruttore per attivare il **firewall**.

  c. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.

  d. Nella finestra **Panoramica impostazioni**, seleziona **Firewall**.

  e. Nella finestra **Impostazioni firewall**, seleziona la scheda **Avanzate**.

  f. Vai a **Condivisione connessione a Internet** e clicca sull'interruttore per attivarla.

  g. Vai a **Blocca port scan** e clicca sull'interruttore per disattivarlo.

  h. Clicca su  per tornare alla finestra principale.

  i. Nel pannello **Firewall**, clicca su **Gestisci adattatori**.

  j. Vai a **Tipo di rete** e seleziona **Casa/Ufficio**.

  k. Vai a **Mod. invisibile** e impostala su **Remoto**. Imposta l'opzione **Generico** su **Sì**.

  l. Chiudi Bitdefender, riavvia il sistema e verifica la velocità della connessione a Internet.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

26.7. Come aggiornare Bitdefender con una connessione a Internet lenta

Se hai una connessione a Internet lenta (ad esempio modem tramite linea telefonica), potrebbero verificarsi degli errori durante l'aggiornamento.

Per mantenere aggiornato il tuo sistema con le firme Bitdefender più recenti, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.

3. Nella finestra **Panoramica impostazioni**, seleziona **Aggiorna**.
4. Nella finestra **Impostazioni aggiornamento**, seleziona la scheda **Aggiornamento**.
5. Nell'opzione **Regole esecuzione aggiornamento**, seleziona **Chiedi prima di scaricare**.
6. Clicca su  per tornare alla finestra principale.
7. Vai al pannello **Aggiornamento** e clicca su **Aggiorna ora**.
8. Seleziona solo **Aggiornamento firme** e poi clicca su **OK**.
9. Bitdefender scaricherà e installerà solo gli aggiornamenti delle firme malware.

26.8. Il mio computer non è connesso a Internet. Come aggiornare Bitdefender?

Se il tuo computer non è connesso a Internet, devi scaricare manualmente gli aggiornamenti su un computer con accesso a Internet e poi trasferirli al tuo computer usando un dispositivo rimuovibile, come una chiavetta USB.

Attenersi alla seguente procedura:

1. Su un computer con accesso a Internet, apri un browser web e vai a:

   http://www.bitdefender.it/site/view/Desktop-Products-Updates.html
2. Nella colonna **Aggiornamento manuale**, clicca sul collegamento corrispondente all'architettura del tuo sistema e prodotto. Se non sai se la tua versione di Windows sia a 32 o 64 bit, fai riferimento a «*Sto usando una versione di Windows a 32 o 64 bit?*» (p. 68).
3. Salva il file chiamato `weekly.exe` sul sistema.
4. Trasferire il file scaricato su un dispositivo rimuovibile come una chiave USB, e poi al tuo computer.
5. Clicca due volte sul file e segui la procedura guidata.

26.9. I servizi Bitdefender non rispondono

Questo articolo aiuta a risolvere i problemi nel caso in cui **I servizi Bitdefender non funzionano**. Si potrebbe trovare questo errore:

- L'icona di Bitdefender nell'area di stato è grigia e una finestra ti informa che i servizi di Bitdefender non rispondono.
- La finestra Bitdefender mostra che i servizi Bitdefender non stanno rispondendo.

L'errore potrebbe essere causato da una delle seguenti condizioni:

- errori temporanei di comunicazione tra i servizi di Bitdefender.
- alcuni servizi di Bitdefender sono arrestati.
- altri programmi di sicurezza sono in esecuzione sul computer contemporaneamente a Bitdefender.

Per risolvere questo errore, provare queste soluzioni:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il computer e aspettare alcuni attimi fino a quando Bitdefender è caricato. Aprire Bitdefender per vedere se l'errore persiste. Riavviare il computer di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di Bitdefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente Bitdefender.

   Per ulteriori informazioni, fare riferimento a «*Come posso rimuovere le altre soluzioni di sicurezza?*» (p. 70).

Se l'errore persiste, contatta i nostri operatori del supporto tecnico per ricevere assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 181).

26.10. Il filtro antispam non funziona correttamente

Questo articolo permette di risolvere i seguenti problemi delle operazioni di filtro Antispam di Bitdefender:

- Un numero di messaggi e-mail legittimi sono contrassegnati come [spam].
- Molti messaggi spam non sono contrassegnati come tali dal filtro antispam.
- Il filtro antispam non rileva nessun messaggio spam.

26.10.1. I messaggi legittimi sono contrassegnati come [spam]

I messaggi legittimi vengono contrassegnati come [spam] semplicemente perché appaiono come tali al filtro antispam di Bitdefender. Normalmente puoi risolvere questo problema configurando adeguatamente il filtro antispam.

Bitdefender aggiunge automaticamente i destinatari dei messaggi e-mail inviati all'elenco Amici. I messaggi e-mail ricevuti dai contatti nell'elenco degli Amici sono considerati legittimi. Non vengono verificati dal filtro antispam e di conseguenza non vengono mai contrassegnati come [spam].

La configurazione automatica dell'elenco Amici non impedisce gli errori di rilevamento che possono accadere in queste situazioni:

- Si ricevono molte e-mail commerciali richieste come risultato della sottoscrizione a vari siti web. In questo caso la soluzione è di aggiungere gli indirizzi e-mail da cui ricevi tali messaggi all'elenco amici.
- Una parte significativa delle tue e-mail legittime proviene da individui a cui non hai mai inviato e-mail in precedenza, ad esempio clienti, potenziali partner d'affari o altri. In questo caso sono richieste altre soluzioni.

1. Se stai utilizzando uno dei programmi di posta elettronica con cui Bitdefender si integra, indica gli errori di rilevazione.

   Nota
   Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo. Per un elenco completo delle applicazioni di posta supportate, fare riferimento a *«Programmi e protocolli di posta elettronica supportati»* (p. 100).

2. Diminuire il livello di protezione antispam. Diminuendo il livello di protezione, il filtro antispam avrà bisogno di maggiori indicazioni di spam per classificare un messaggio e-mail come spam. Utilizza questa soluzione solo se molti messaggi legittimi (inclusi i messaggi commerciali richiesti) vengono rilevati scorrettamente come spam.

Aggiungi contatti all'elenco Amici

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi legittimi all'elenco amici. Attenersi alla seguente procedura:

1. Nell'applicazione di posta seleziona un messaggio e-mail inviato dal mittente che desideri aggiungere all'elenco Amici.
2. Clicca sul pulsante **Aggiungi Amico** sulla barra degli strumenti antispam di Bitdefender.
3. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco Amici. Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

Se utilizzi un'applicazione di posta differente, puoi aggiungere i contatti all'elenco Amici dall'interfaccia di Bitdefender. Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antispam**, clicca su **Gestisci** e seleziona **Amici** dal menu a tendina.

   Apparirà la finestra di configurazione.

3. Digita l'indirizzo e-mail da cui vuoi sempre ricevere i messaggi e clicca su **Aggiungi**.Puoi aggiungere quanti indirizzi e-mail desideri.
4. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Indica errori di rilevamento

Se stai utilizzando un client di posta supportato, puoi correggere facilmente il filtro antispam (indicando quali messaggi e-mail non devono essere contrassegnati come `[spam]`). Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam.Attenersi alla seguente procedura:

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.
3. Seleziona il messaggio legittimo scorrettamente contrassegnato come `[spam]` da Bitdefender.
4. Clicca sul pulsante **Aggiungi amico** sulla barra degli strumenti antispam di Bitdefender per aggiungere il mittente all'elenco Amici.Può essere necessario premere **OK** per confermare.Riceverai sempre e-mail provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.
5. Clicca sul pulsante **Non è Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta).L'e-mail sarà spostata nella cartella Posta in arrivo.

Diminuisci il livello di protezione antispam

Per diminuire il livello di protezione antispam, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antispam**.
4. Nella finestra **Impostazioni antispam**, seleziona la scheda **Impostazioni**.
5. Spostare il selettore verso il basso lungo la scala.

26.10.2. Molti messaggi spam non vengono rilevati

Se ricevi molti messaggi spam che non vengono contrassegnati come `[spam]`, devi configurare il filtro antispam di Bitdefender in modo da migliorarne l'efficienza.

Prova le seguenti soluzioni:

1. Se stai utilizzando uno dei programmi di posta elettronica con cui Bitdefender si integra, indica i messaggi spam non rilevati.

Nota

Bitdefender si integra nella maggior parte delle applicazioni di posta elettronica comunemente utilizzate per mezzo di una barra degli strumenti antispam di facile utilizzo.Per un elenco completo delle applicazioni di posta supportate, fare riferimento a «*Programmi e protocolli di posta elettronica supportati*» (p. 100).

2. Aggiungi spammer all'elenco Spammer. I messaggi e-mail ricevuti dagli indirizzi nell'elenco Spammer sono contrassegnati automaticamente come `[spam]`.
3. Aumenta il livello di protezione antispam. Aumentando il livello di protezione, il filtro antispam avrà bisogno di minori indicazioni di spam per classificare un messaggio e-mail come spam.

Indica messaggi spam non rilevati

Se si utilizza un'applicazione di posta supportata si può facilmente indicare quali messaggi e-mail avrebbero dovuto essere rilevati come spam. Così facendo si migliorerà considerevolmente l'efficienza del filtro antispam.Attenersi alla seguente procedura:

1. Apri il tuo client e-mail.
2. Vai alla cartella Posta in arrivo.
3. Seleziona i messaggi di spam non rilevati.
4. Clicca sul pulsante **È Spam** sulla barra degli strumenti antispam di Bitdefender (in genere localizzata nella parte superiore della finestra del client di posta). Vengono immediatamente contrassegnati come `[spam]` e verranno spostati alla cartella posta indesiderata.

Aggiungi spammer a elenco Spammer

Se stai utilizzando un'applicazione di posta supportata, puoi facilmente aggiungere i mittenti dei messaggi di spam all'elenco Spammer.Attenersi alla seguente procedura:

1. Apri il tuo client e-mail.
2. Vai alla cartella posta indesiderata, dove vengono spostati i messaggi spam.
3. Seleziona i messaggi contrassegnati come `[spam]` da Bitdefender.
4. Clicca sul pulsante **Aggiungi Spammer** sulla barra degli strumenti antispam di Bitdefender.
5. Può essere richiesto di accettare gli indirizzi aggiunti all'elenco degli Spammer.Seleziona **Non mostrare di nuovo questo messaggio** e clicca su **OK**.

Se utilizzi un client di posta diverso, puoi aggiungere manualmente nuovi contatti all'elenco Spammer dall'interfaccia di Bitdefender. Si tratta di un metodo conveniente solo quando si ricevono diversi messaggi spam dallo stesso indirizzo e-mail.Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antispam**, clicca su **Gestisci** e seleziona **Spammer** dal menu a tendina.

   Apparirà la finestra di configurazione.
3. Digita l'indirizzo e-mail dello spammer e poi clicca su **Aggiungi**.Puoi aggiungere quanti indirizzi e-mail desideri.
4. Clicca su **OK** per salvare le modifiche e chiudere la finestra.

Aumenta il livello di protezione antispam

Per aumentare il livello di protezione antispam, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
3. Nella finestra **Panoramica impostazioni**, seleziona **Antispam**.
4. Nella finestra **Impostazioni antispam**, seleziona la scheda **Impostazioni**.
5. Spostare il selettore verso l'alto lungo la scala.

26.10.3. Il Filtro antispam non rileva alcun messaggio spam

Se nessun messaggio spam viene contrassegnato come `[spam]`, potrebbe esserci un problema relativo al filtro antispam di Bitdefender.Prima di risolvere questo problema, assicurati che non sia causato da una delle seguente condizioni:

- La protezione antispam potrebbe essere disattivata.Per verificare lo stato di protezione antispam, apri la finestra Bitdefender e verifica l'interruttore nel pannello **Antispam**.

  Se l'antispam è disattivato, questa è la causa dei problemi.Clicca sull'interruttore per attivare o disattivare la protezione antispam.
- La protezione antispam di Bitdefender è disponibile solo per client e-mail configurati per ricevere messaggi e-mail tramite il protocollo POP3.Questo vuol dire che:
  - I messaggi e-mail ricevuti tramite servizi e-mail web (ad esempio Yahoo, Gmail, Hotmail o altri) non sono filtrati per spam da Bitdefender.
  - Se il tuo client e-mail è configurato per ricevere messaggi e-mail usando un protocollo diverso da POP3 (per esempio, IMAP4), il filtro antispam di Bitdefender non verifica se siano spam.

Nota

POP3 è uno dei protocolli più usati per scaricare messaggi e-mail da un server di posta.Se non si conosce il protocollo usato dal proprio client e-mail per scaricare messaggi e-mail, chiedere alla persona che ha configurato il proprio client e-mail.

- Bitdefender Internet Security non esegue la scansione del traffico POP3 di Lotus Notes.

Una possibile soluzione consiste nel riparare o reinstallare il prodotto. Tuttavia puoi contattare Bitdefender per ricevere supporto, come descritto nella sezione «*Chiedere aiuto*» (p. 181).

26.11. L'opzione Compila automaticamente nel mio Portafoglio non funziona

Hai salvato le tue credenziali online nel Portafoglio di Bitdefender, notando così che l'opzione Compila automaticamente non sta funzionando. In genere, questo problema si verifica quando l'estensione del Portafoglio di Bitdefender non è installata nel tuo browser.

Per risolvere il problema, segui questi passaggi:

- In **Internet Explorer:**
  1. Apri Internet Explorer.
  2. Clicca su Strumenti.
  3. Clicca su Gestisci Add-on.
  4. Clicca su Barre degli strumenti ed Estensioni.
  5. Seleziona **Portafoglio di Bitdefender** e clicca su Attiva.
- In **Mozilla Firefox:**
  1. Apri Mozilla Firefox.
  2. Clicca su Strumenti.
  3. Clicca su Add-on.
  4. Clicca su Estensioni.
  5. Seleziona **Portafoglio di Bitdefender** e clicca su Attiva.
- In **Google Chrome:**
  1. Apri Google Chrome.
  2. Vai all'icona del menu.
  3. Clicca su Impostazioni.
  4. Clicca su Estensioni.

5. Seleziona **Portafoglio di Bitdefender** e clicca su Attiva.

Nota
L'add-on sarà disponibile una volta riavviato il browser.

Ora controlla se la funziona Completa automaticamente del Portafoglio funzioni per i tuoi account online.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

26.12. Rimozione di Bitdefender non riuscita

Se desideri rimuovere il tuo prodotto Bitdefender ma il processo o il sistema si blocca, clicca su **Annulla** per interrompere l'operazione. Se questo non dovesse funzionare, riavviare il sistema.

Se la rimozione non riesce, alcuni file e alcune chiavi di registro di Bitdefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di Bitdefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema.

Per rimuovere completamente Bitdefender dal sistema, segui questi passaggi:

- Per **Windows XP**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.
  3. Trova **Bitdefender** e seleziona **Rimuovi**.
  4. Clicca su **Rimuovi** e poi su **disinstalla COMPLETAMENTE Bitdefender**.
  5. Hai le seguenti opzioni:
     - L'opzione **Disinstalla e resta protetto** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi sarà installato sul sistema per proteggerti dai malware.
     - L'opzione **Disinstalla senza la app** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi non sarà installato.

     Seleziona l'opzione desiderata e clicca su **Avanti**.
  6. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.
- Per **Windows Vista** e **Windows 7**:
  1. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
  2. Attendi per qualche istante, finché non compare l'elenco del software installato.

3. Trova **Bitdefender** e seleziona **Disinstalla**.
4. Clicca su **Rimuovi** e poi su **disinstalla COMPLETAMENTE Bitdefender**.
5. Hai le seguenti opzioni:
   - L'opzione **Disinstalla e resta protetto** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi sarà installato sul sistema per proteggerti dai malware.
   - L'opzione **Disinstalla senza la app** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi non sarà installato.

   Seleziona l'opzione desiderata e clicca su **Avanti**.
6. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

- Per **Windows 8**:

1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
2. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.
3. Attendi per qualche istante, finché non compare l'elenco del software installato.
4. Trova **Bitdefender** e seleziona **Disinstalla**.
5. Clicca su **Rimuovi** e poi su **disinstalla COMPLETAMENTE Bitdefender**.
6. Hai le seguenti opzioni:
   - L'opzione **Disinstalla e resta protetto** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi sarà installato sul sistema per proteggerti dai malware.
   - L'opzione **Disinstalla senza la app** rimuoverà completamente Bitdefender. Bitdefender Virus Scanner 60 secondi non sarà installato.

   Seleziona l'opzione desiderata e clicca su **Avanti**.
7. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

Nota

Bitdefender Virus Scanner 60 secondi è un'applicazione gratuita che utilizza una tecnologia di scansione in-the-cloud per rilevare programmi dannosi ed eventuali minacce in meno di 60 secondi.

26.13. Il sistema non si riavvia dopo aver installato Bitdefender

Se hai appena installato Bitdefender e non riesci più a riavviare il sistema in modalità normale potrebbero esserci varie cause per questo problema.

Molto probabilmente la causa è un'installazione precedente di Bitdefender che non è stata rimossa correttamente o un'altra soluzione di sicurezza ancora presente sul sistema.

Ecco come affrontare ogni situazione:

- **In precedenza avevi Bitdefender e non l'hai disinstallato correttamente.**

  Per risolvere, segui questi passaggi:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a *«Come posso riavviare in modalità provvisoria?»* (p. 71).
  2. Rimuovi Bitdefender dal tuo sistema:
     - Per **Windows XP**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.
       b. Attendi per qualche istante, finché non compare l'elenco del software installato.
       c. Trova **Bitdefender** e seleziona **Rimuovi**.
       d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.
       e. Attendere che il processo di disinstallazione sia terminato.
       f. Riavvia il sistema in modalità normale.
     - Per **Windows Vista** e **Windows 7**:
       a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
       b. Attendi per qualche istante, finché non compare l'elenco del software installato.
       c. Trova **Bitdefender** e seleziona **Disinstalla**.
       d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.
       e. Attendere che il processo di disinstallazione sia terminato.
       f. Riavvia il sistema in modalità normale.
     - Per **Windows 8**:
       a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
       b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.

c. Attendi per qualche istante, finché non compare l'elenco del software installato.

d. Trova **Bitdefender** e seleziona **Disinstalla**.

e. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

f. Attendere che il processo di disinstallazione sia terminato.

g. Riavvia il sistema in modalità normale.

3. Reinstalla il tuo prodotto Bitdefender.

- **In precedenza avevi un'altra soluzione di sicurezza e non l'hai rimossa correttamente.**

  Per risolvere, segui questi passaggi:

  1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 71).
  2. Rimuovi Bitdefender dal tuo sistema:

     ▶ Per **Windows XP**:

     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Aggiungi / Rimuovi programmi**.

     b. Attendi per qualche istante, finché non compare l'elenco del software installato.

     c. Trova **Bitdefender** e seleziona **Rimuovi**.

     d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

     e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

     ▶ Per **Windows Vista** e **Windows 7**:

     a. Clicca su **Start**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.

     b. Attendi per qualche istante, finché non compare l'elenco del software installato.

     c. Trova **Bitdefender** e seleziona **Disinstalla**.

     d. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

     e. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

     ▶ Per **Windows 8**:

a. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (puoi anche digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.

b. Clicca su **Disinstalla un programma** o su **Programmi e funzionalità**.

c. Attendi per qualche istante, finché non compare l'elenco del software installato.

d. Trova **Bitdefender** e seleziona **Disinstalla**.

e. Clicca su **Rimuovi** e poi su **Reinstalla/modifica il mio prodotto Bitdefender**.

f. Attendi che il processo di disinstallazione sia completo, poi riavvia il sistema.

3. Per disinstallare correttamente l'altro software, vai nel sito web del produttore ed esegui lo strumento di disinstallazione o contattalo direttamente per ricevere le istruzioni di disinstallazione.
4. Riavvia il sistema in modalità normale e reinstalla Bitdefender.

Hai già seguito i passaggi sopra indicati e la situazione non è cambiata.

Per risolvere, segui questi passaggi:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 71).
2. Usa l'opzione Ripristino configurazione di sistema di Windows per ripristinare il computer a uno stato precedente all'installazione del prodotto Bitdefender. Per scoprire come fare, fai riferimento a «*Come posso usare il Ripristino di sistema in Windows?*» (p. 71).
3. Riavvia il sistema in modalità normale e contatta i nostri operatori del supporto per assistenza, come indicato nella sezione «*Chiedere aiuto*» (p. 181).

27. Rimuovere malware dal sistema

I malware possono influenzare il sistema in molti modi diversi e l'approccio di Bitdefender dipende dal tipo di attacco malware.Poiché i virus modificano spesso il loro comportamento, è difficile stabilire uno schema per il loro comportamento e le loro azioni.

Ci sono alcune circostanze in cui Bitdefender non può rimuovere automaticamente l'infezione malware dal tuo sistema.In tali casi, è richiesto il tuo intervento.

- «*Modalità soccorso di Bitdefender*» (p. 171)
- «*Cosa fare quando Bitdefender trova dei virus sui tuoi computer?*» (p. 173)
- «*Come posso rimuovere un virus in un archivio?*» (p. 174)
- «*Come posso rimuovere un virus nell'archivio delle e-mail?*» (p. 175)
- «*Cosa fare se sospetti che un file possa essere pericoloso?*» (p. 176)
- «*Come pulire i file infetti in System Volume Information*» (p. 176)
- «*Quali sono i file protetti da password nel registro della scansione?*» (p. 178)
- «*Quali sono gli elementi ignorati nel registro della scansione?*» (p. 178)
- «*Quali sono i file supercompressi nel registro della scansione?*» (p. 178)
- «*Perché Bitdefender ha eliminato automaticamente un file infetto?*» (p. 179)

Se non riesci a trovare il problema qui, o se la soluzione fornita non lo risolve, puoi contattare un operatore del supporto tecnico di Bitdefender come indicato nel capitolo «*Chiedere aiuto*» (p. 181).

27.1. Modalità soccorso di Bitdefender

La **Modalità soccorso** è una funzione di Bitdefender che ti consente di controllare e disinfettare tutte le partizioni disco esistenti al di fuori del tuo sistema operativo.

Una volta installato Bitdefender Internet Security, la Modalità soccorso può essere usata anche se non puoi più avviare Windows.

Avviare il tuo sistema in Modalità soccorso

Puoi accedere alla Modalità soccorso in uno dei due modi:

Dalla finestra di Bitdefender

Per accedere direttamente alla Modalità soccorso da Bitdefender, segui questi passaggi:

1. Apri la finestra di Bitdefender.
2. Nel pannello **Antivirus**, clicca su **Controlla ora** e seleziona **modalità soccorso** dal menu a tendina.

Apparirà una finestra di conferma. Clicca su **Sì** per riavviare il computer.

3. Dopo il riavvio del computer, comparirà un menu che ti avvisa di selezionare un sistema operativo. Seleziona **Bitdefender Rescue Image** e premi il tasto **Invio** per avviare un ambiente di Bitdefender da cui poter pulire la tua partizione Windows.
4. Se richiesto, premi **Invio** e seleziona la risoluzione dello schermo più vicina a quella che usi normalmente. Poi premi di nuovo **Invio**.

   Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.

Avvia il computer direttamente in Modalità soccorso

Se Windows non parte più, puoi avviare il tuo computer direttamente nella Modalità soccorso di Bitdefender seguendo i passaggi sottostanti:

Nota

Questo metodo non è disponibile sui computer con Windows XP.

1. Accendi / Riavvia il tuo computer e inizia a premere la **barra spaziatrice** sulla tastiera prima che compaia il logo di Windows.
2. Comparirà un menu per avvisarti di selezionare il sistema operativo da avviare. Premi **TAB** per accedere all'area degli strumenti. Seleziona **Bitdefender Rescue Image** e premi il tasto **Invio** per avviare un ambiente di Bitdefender da cui poter pulire la tua partizione Windows.
3. Se richiesto, premi **Invio** e seleziona la risoluzione dello schermo più vicina a quella che usi normalmente. Poi premi di nuovo **Invio**.

   Tra pochi istanti la Modalità soccorso di Bitdefender si caricherà.

Controllare il sistema in Modalità soccorso

Per eseguire una scansione del sistema in Modalità soccorso, segui questi passaggi:

1. Entra in Modalità soccorso, come descritto in «Avviare il tuo sistema in Modalità soccorso» (p. 171).
2. Comparirà il logo di Bitdefender e i motori antivirus inizieranno a essere copiati.
3. Comparirà una finestra di benvenuto. Clicca su **Continua**.
4. È stato avviato un aggiornamento delle firme antivirus.
5. Una volta completato l'aggiornamento, comparirà la finestra della scansione antivirus su richiesta di Bitdefender.
6. Clicca su **Controlla ora**, seleziona l'obiettivo della scansione nella finestra che compare e clicca su **Apri** per avviare la scansione.

   Si consiglia di controllare la tua intera partizione di Windows.

Nota

Quando si lavora in Modalità soccorso, avrai a che fare con nomi di partizioni tipo Linux. Le partizioni del disco compariranno come `sda1` che corrisponde alla partizione di Windows `(C:)`, `sda2` che corrisponde a `(D:)` e così via.

7. Attendi il completamento della scansione. Se venissero rilevati malware, segui le istruzioni per rimuovere la minaccia.
8. Per uscire dalla modalità soccorso, clicca con il pulsante destro in un'area libera del desktop, seleziona **Esci** nel menu che comparirà e poi seleziona se riavviare o spegnere il computer.

27.2. Cosa fare quando Bitdefender trova dei virus sui tuoi computer?

Potresti scoprire l'esistenza di un virus sul tuo computer in uno di questi modi:

- Hai controllato il tuo computer e Bitdefender ha trovato alcuni elementi infetti.
- Un avviso antivirus ti informa che Bitdefender ha bloccato uno o più virus sul tuo computer.

In tali situazioni, aggiorna Bitdefender per assicurarti di avere le ultime firme malware e avvia una Scansione del sistema per analizzarlo.

Al termine della scansione del sistema , seleziona l'azione desiderata per gli elementi infetti (Disinfetta, Elimina, Sposta in quarantena).

Avvertimento

Se sospetti che il file sia parte del sistema operativo Windows o che non sia un file infetto, non seguire questi passaggi e contatta il Servizio clienti di Bitdefender il prima possibile.

Se l'azione selezionata non può essere eseguita e il registro della scansione rivela un'infezione non eliminabile, devi rimuovere manualmente i file:

Il primo metodo può essere usato in modalità normale:

1. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
   d. Clicca sulla scheda **Protezione** nella finestra **Impostazioni antivirus**.
   e. Clicca sull'interruttore per disattivare la **scansione all'accesso**.
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a *«Come posso visualizzare gli elementi nascosti in Windows?»* (p. 69).

3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se il primo metodo non riuscisse a rimuovere l'infezione, segui questi passaggi:

1. Riavvia il sistema ed entra in modalità provvisoria. Per scoprire come fare, fai riferimento a «*Come posso riavviare in modalità provvisoria?*» (p. 71).
2. Mostra gli elementi nascosti in Windows. Per scoprire come fare, fai riferimento a «*Come posso visualizzare gli elementi nascosti in Windows?*» (p. 69).
3. Trova l'ubicazione del file infetto (controlla il registro della scansione) ed eliminalo.
4. Riavvia il sistema ed entra in modalità normale.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

27.3. Come posso rimuovere un virus in un archivio?

Un archivio è un file o una raccolta di file compressi in un formato speciale per ridurre lo spazio su disco necessario alla loro archiviazione.

Alcuni di questi formati sono aperti, offrendo così a Bitdefender l'opportunità per controllarli all'interno e intraprendere le azioni adeguate per rimuoverli.

Altri formati dell'archivio sono chiusi parzialmente o interamente, e Bitdefender può solo rilevare la presenza di virus al loro interno, senza poter intraprendere alcuna azione.

Se Bitdefender ti avvisa di aver rilevato un virus in un archivio e di non poter attuare alcuna azione, significa che non puoi rimuovere il virus a causa delle restrizioni sulle impostazioni di permesso dell'archivio.

Ecco come rimuovere un virus in un archivio:

1. Identifica l'archivio che include il virus, eseguendo una scansione del sistema.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
   d. Clicca sulla scheda **Protezione** nella finestra **Impostazioni antivirus**.
   e. Clicca sull'interruttore per disattivare la **scansione all'accesso**.
3. Vai all'ubicazione dell'archivio e decomprimilo usando un programma di compressione, come WinZip.
4. Identifica il file infetto e lo elimina.

5. Elimina l'archivio originale per assicurarti che l'infezione sia stata rimossa completamente.
6. Ricomprimi i file in un nuovo archivio usando un'applicazione di archiviazione, come WinZip.
7. Attiva la protezione antivirus in tempo reale di Bitdefender ed esegui una scansione completa del sistema per assicurarti che non ci siano altre infezioni.

Nota
È importante notare che un virus in un archivio non è una minaccia immediata al sistema, poiché deve essere decompresso ed eseguito per infettarlo.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

27.4. Come posso rimuovere un virus nell'archivio delle e-mail?

Bitdefender può anche identificare i virus nei database e negli archivi di e-mail presenti su disco.

A volte devi identificare il messaggio infetto usando le informazioni fornite nel rapporto della scansione ed eliminarlo manualmente.

Ecco come rimuovere un virus presente in un archivio e-mail:

1. Controlla il database e-mail con Bitdefender.
2. Disattiva la protezione antivirus in tempo reale di Bitdefender:
   a. Apri la finestra di Bitdefender.
   b. Clicca sul pulsante **Impostazioni** nella barra degli strumenti superiore.
   c. Nella finestra **Panoramica impostazioni**, seleziona **Antivirus**.
   d. Clicca sulla scheda **Protezione** nella finestra **Impostazioni antivirus**.
   e. Clicca sull'interruttore per disattivare la **scansione all'accesso**.
3. Apri il rapporto della scansione e usa le informazioni d'identificazione (oggetto, da, a) dei messaggi infettati per localizzarli nel client e-mail.
4. Elimina i messaggi infetti.La maggior parte dei client e-mail spostano il messaggio eliminato in una cartella di recupero, dalla quale può essere recuperato.Dovresti assicurarti che il messaggio sia eliminato anche da questa cartella di ripristino.
5. Compatta la cartella di memorizzazione del messaggio infetto.
   - In Outlook Express:Nel menu File, clicca su Cartella, poi Comprimi tutte le cartelle.

- Per Microsoft Outlook 2007:Nel menu File, clicca su Gestione file dati.Seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni.Clicca su Compatta.
- Per Microsoft Outlook 2007 / 2013:Nel menu File, clicca su Info e poi su Impostazioni account (Consente di aggiungere e rimuovere account o di modificare le impostazioni di connessione esistenti).Poi clicca su File di dati, seleziona i file delle cartelle personali (.pst) che desideri compattare e clicca su Impostazioni.Clicca su Compatta.

6. Attiva la protezione antivirus in tempo reale di Bitdefender.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

27.5. Cosa fare se sospetti che un file possa essere pericoloso?

Puoi sospettare che un file del tuo sistema sia pericoloso, anche se il prodotto Bitdefender non l'ha rilevato.

Per assicurarti che il tuo sistema sia protetto, segui questi passaggi:

1. Esegui una **Scansione del sistema** con Bitdefender. Per scoprire come fare, fai riferimento a «*Come posso eseguire una scansione del mio sistema?*» (p. 53).
2. Se il risultato della scansione non segnala nulla, ma hai ancora dubbi e vuoi essere certo che il file sia pulito, contatta gli operatori del nostro supporto tecnico per ricevere assistenza.

   Per scoprire come fare, fai riferimento a «*Chiedere aiuto*» (p. 181).

27.6. Come pulire i file infetti in System Volume Information

La cartella System volume information è una zona sul tuo disco fisso creata dal sistema operativo e usata da Windows per archiviare informazioni importanti relative alla configurazione del sistema.

I motori di Bitdefender possono rilevare qualsiasi file infetto archiviato nella cartella System Volume Information, ma essendo un'area protetta potrebbe non essere possibile rimuoverli.

I file infetti rilevati nelle cartelle del Ripristino configurazione di sistema compariranno nel registro della scansione come segue:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Per rimuovere completamente e immediatamente i file infetti o i file nell'archivio dati, disattiva e attiva nuovamente l'opzione Ripristino configurazione di sistema.

Quanto il Ripristino configurazione di sistema è disattivato, tutti i punti di ripristino sono rimossi.

Quando il Ripristino configurazione di sistema viene attivato nuovamente, vengono creati nuovi punti di ripristino come richiesto dalla programmazione e dagli eventi.

Per disabilitare il Ripristino configurazione di sistema, segui questi passaggi:

- **Per Windows XP:**
  1. Segui questo percorso: **Start → Tutti i programmi → Accessori → Utilità di sistema → Ripristino configurazione di sistema**
  2. Clicca su **Impostazioni Ripristino configurazione di sistema** sul lato sinistro della finestra.
  3. Seleziona la casella **Disattiva Ripristino configurazione di sistema** su tutte le unità e clicca su **Applica**.
  4. Quando ricevi l'avviso che tutti i punti di ripristino esistenti saranno eliminati, clicca su **Sì** per continuare.
  5. Per attivare il Ripristino configurazione di sistema, deseleziona la casella **Disattiva Ripristino configurazione di sistema** su tutte le unità e clicca su **Applica**
- **Per Windows Vista:**
  1. Segui questo percorso: **Start → Pannello di controllo → Sistema e manutenzione → Sistema**
  2. Nel pannello a sinistra, clicca su **Protezione sistema**.

     Se è richiesta una password da amministratore o una conferma, digita la password o fornisci la conferma.
  3. Per disattivare il Ripristino di sistema deseleziona le caselle corrispondenti per ogni unità e clicca su **Ok**.
  4. Per attivare il Ripristino di sistema seleziona le caselle corrispondenti per ogni unità e clicca su **OK**.
- **Per Windows 7:**
  1. Clicca su **Start**, clicca col pulsante destro su **Risorse del computer** e poi clicca su **Proprietà**.
  2. Clicca sul collegamento **Protezione sistema** nel pannello a sinistra.
  3. Nelle opzioni di **Protezione sistema**, seleziona tutte le unità e clicca su **Configura**.
  4. Seleziona **Disattiva il sistema di protezione** e clicca su **Applica**.
  5. Clicca su **Elimina**, clicca su **Continua** una volta richiesto e poi clicca su **OK**.
- **Per Windows 8:**

1. Dal menu Start di Windows, localizza l'opzione **Computer** (puoi anche digitare direttamente "Computer" nella finestra di ricerca del menu Start) e poi clicca sulla sua icona.
2. Clicca sul collegamento **Protezione sistema** nel pannello a sinistra.
3. Nelle opzioni di **Protezione sistema**, seleziona tutte le unità e clicca su **Configura**.
4. Seleziona **Disattiva il sistema di protezione** e clicca su **Applica**.

Se questa informazione non è stata utile, puoi contattare Bitdefender per avere assistenza, come descritto alla sezione «*Chiedere aiuto*» (p. 181).

27.7. Quali sono i file protetti da password nel registro della scansione?

Questa è solo una notifica per indicare che Bitdefender ha rilevato che questi file sono protetti da una password o da una qualche forma di crittografia.

In genere gli elementi protetti da password sono:

- File che appartengono a un'altra soluzione di sicurezza.
- File che appartengono al sistema operativo.

Per poter controllare i contenuti, devi estrarre o quantomeno decriptare questi file.

Qualora tali contenuti venissero estratti, la scansione in tempo reale di Bitdefender li controllerebbe automaticamente per proteggere il tuo computer. Se desideri controllare quei file con Bitdefender, devi contattare il produttore per ottenere maggiori informazioni sui file.

Ti consigliamo di ignorare quei file perché non sono una minaccia per il sistema.

27.8. Quali sono gli elementi ignorati nel registro della scansione?

Tutti i file che compaiono come Ignorati nel rapporto della scansione sono puliti.

Per prestazioni superiori, Bitdefender non controlla file che non sono stati modificati dall'ultima scansione.

27.9. Quali sono i file supercompressi nel registro della scansione?

Gli oggetti supercompressi sono elementi che non possono essere estratti dal motore di scansione o elementi per i quali la crittografia avrebbe impiegato troppo tempo, rendendo il sistema instabile.

Supercompresso significa che Bitdefender ha saltato la scansione di quell'archivio perché scompattarlo avrebbe richiesto troppe risorse di sistema. Se necessario, il contenuto sarà controllato solo durante l'accesso in tempo reale.

27.10. Perché Bitdefender ha eliminato automaticamente un file infetto?

Se viene rilevato un file infetto, Bitdefender tenterà di disinfettarlo automaticamente.Se la disinfezione dovesse fallire, il file sarà messo in quarantena per contenere l'infezione.

Per alcuni particolari tipologie di malware, non è possibile usare la disinfezione perché il file rilevato è interamente maligno. In questi casi, il file infetto è eliminato dal disco.

Questo di solito è il caso di file di installazione che vengono scaricati da siti web non attendibili.Se dovessi trovarti in tale situazione, scarica il file d'installazione dal sito web del produttore o da un altro sito web affidabile.

Contattaci

28. Chiedere aiuto

Bitdefender fornisce ai suoi clienti un supporto veloce e preciso assolutamente senza pari. Se dovessi riscontrare un problema o se avessi una qualche domanda relativa al tuo prodotto Bitdefender, puoi utilizzare una delle tante risorse online per trovare una soluzione o una risposta. Oppure, puoi contattare il Servizio clienti di Bitdefender. Gli operatori del nostro supporto risponderanno alle tue domande in modo tempestivo e ti forniranno l'assistenza necessaria.

La sezione *«Risolvere i problemi più comuni»* (p. 150) fornisce le informazioni necessarie sui problemi più frequenti che potresti incontrare usando questo prodotto.

Se non dovessi trovare la soluzione al tuo problema nelle risorse fornite, puoi contattarci direttamente:

- «Contattaci direttamente dal tuo prodotto Bitdefender» (p. 181)
- «Contattaci tramite il nostro Centro di supporto online» (p. 182)

Importante
Per contattare il Servizio clienti di Bitdefender devi registrare il prodotto di Bitdefender. Per ulteriori informazioni, fare riferimento a *«Registrare Bitdefender»* (p. 33).

Contattaci direttamente dal tuo prodotto Bitdefender

Se hai una connessione a Internet funzionante, puoi contattare Bitdefender per ricevere assistenza direttamente dall'interfaccia del prodotto.

Attenersi alla seguente procedura:

1. Apri la finestra di Bitdefender.
2. Clicca sul collegamento **Aiuto e supporto**, localizzato nell'angolo in basso a destra della finestra.
3. Hai le seguenti opzioni:
   - **Aiuto di Bitdefender**.

     Sfoglia gli articoli della documentazione di Bitdefender e prova le soluzioni proposte.
   - **Centro di supporto**

     Accedi al nostro database e cerca le informazioni necessarie.
   - **Contatta supporto**

     Usa il pulsante **Contatta supporto** per lanciare lo Strumento di supporto e contattare il Servizio clienti. Puoi esplorare la procedura guidata usando il pulsante **Avanti**. Per uscire dalla procedura guidata, clicca su **Annulla**.

     a. Seleziona la casella di accettazione e clicca su **Avanti**.

b. Completa il modulo di invio con i dati richiesti:
   i. Inserisci il tuo indirizzo e-mail.
   ii. Inserisci il tuo nome completo.
   iii. Scegli il tuo paese dal menu corrispondente.
   iv. Inserisci una descrizione del problema riscontrato.
c. Attendi qualche minuto mentre Bitdefender raccoglie le informazioni sul prodotto. Queste informazioni aiuteranno i nostri ingegneri a trovare una soluzione al tuo problema.
d. Clicca su **Termina** per inviare le informazioni sul Servizio clienti di Bitdefender. Sarai contattato il prima possibile.

Contattaci tramite il nostro Centro di supporto online

Se non puoi accedere alle informazioni necessarie usando il prodotto Bitdefender, fai ricorso al nostro Centro di supporto online:

1. Visitare http://www.bitdefender.it/support/consumer.html. Il Centro di supporto di Bitdefender include molti articoli che contengono soluzioni ai problemi inerenti Bitdefender.
2. Utilizza la barra di ricerca nella parte superiore della finestra per trovare gli articoli che possono fornire una soluzione al tuo problema. Per effettuare una ricerca, digita un termine nella barra di ricerca e clicca su **Cerca**.
3. Leggi gli articoli o i documenti rilevanti e prova le soluzioni proposte.
4. Se la soluzione non dovesse risolvere il tuo problema, vai a http://www.bitdefender.it/support/contact-us.html e contatta gli operatori del nostro supporto.

29. Risorse online

Sono disponibili diverse risorse online per aiutarti a risolvere i tuoi problemi e rispondere alle tue domande relative a Bitdefender.

- Centro di supporto di Bitdefender:http://www.bitdefender.it/support/consumer.html
- Forum del supporto di Bitdefender:http://forum.bitdefender.com
- Il portale di sicurezza informatica HOTforSecurity:http://www.hotforsecurity.com

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

29.1. Centro di supporto di Bitdefender

Il Centro di supporto di Bitdefender è un archivio online di informazioni sui prodotti di Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati di attività di risoluzione bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione antivirus, la gestione delle soluzioni di Bitdefender con spiegazioni dettagliate e molti altri articoli.

Il Centro di supporto di Bitdefender è aperto al pubblico e liberamente consultabile. Le molte informazioni contenute sono un altro mezzo per fornire ai clienti di Bitdefender le conoscenze tecniche necessarie. Tutte le richieste di informazioni o segnalazioni di bug dai clienti di Bitdefender arrivano al Centro di supporto di Bitdefender, così come segnalazioni e informazioni su bug risolti o articoli tecnici per integrare i file di supporto del prodotto.

Il Centro di supporto di Bitdefender è disponibile in qualsiasi momento all'indirizzo http://www.bitdefender.it/support/consumer.html.

29.2. Forum supporto di Bitdefender

Il forum del supporto di Bitdefender fornisce agli utenti di Bitdefender un modo semplice per ottenere aiuto e aiutare gli altri.

Se il tuo prodotto Bitdefender non funziona bene e non riesce a rimuovere virus specifici dal computer o se hai qualche domanda sul suo funzionamento, pubblica il tuo problema o la tua domanda sul forum.

I tecnici del supporto di Bitdefender controllano le nuove discussioni sul forum per poterti assistere. Potresti ricevere una risposta o una soluzione anche da un utente di Bitdefender più esperto.

Prima di postare il tuo problema o la tua domanda, cerca nel forum un'eventuale discussione simile o collegata.

Il forum del supporto di Bitdefender è disponibile all'indirizzo http://forum.bitdefender.com in 5 lingue diverse: inglese, tedesco, francese, spagnolo

e rumeno. Clicca sul link **Protezione Casa/Ufficio** per accedere alla sezione dedicata ai prodotti per utenti standard.

29.3. Portale HOTforSecurity

Il portale HOTforSecurity è una ricca fonte di informazioni sulla sicurezza informatica. Qui puoi apprendere le varie minacce a cui il computer è esposto quando ti connetti a Internet (malware, phishing, spam, cyber-criminali).

Vengono pubblicati regolarmente nuovi articoli per mantenerti sempre aggiornato sulle ultime minacce scoperte oltre alle tendenze attuali in fatto di sicurezza e altre informazioni sulla protezione del computer.

La pagina web HOTforSecurity è raggiungibile all'indirizzo http://www.hotforsecurity.com.

30. Contatti

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 10 anni BITDEFENDER ha acquisito una reputazione inestimabile superando le aspettative di clienti e partner, e sforzandosi costantemente per una comunicazione sempre più efficiente. Se hai delle domande o richieste, non esitare a contattarci.

30.1. Indirizzi web

Dipartimento vendite: sales@bitdefender.com
Centro di supporto:http://www.bitdefender.it/support/consumer.html
Documentazione: documentation@bitdefender.com
Distributori locali:http://www.bitdefender.it/partners
Programma partner: partners@bitdefender.com
Contatti stampa: pr@bitdefender.com
Lavoro: jobs@bitdefender.com
Invio virus: virus_submission@bitdefender.com
Invio spam: spam_submission@bitdefender.com
Segnala abuso: abuse@bitdefender.com
Sito web:http://www.bitdefender.com

30.2. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Visitare http://www.bitdefender.it/partners/#Partner Locator/.
2. Clicca sulla scheda **Trova partner**.
3. Le informazioni di contatto dei distributori locali di Bitdefender dovrebbero essere visualizzate automaticamente. Se non fosse così, seleziona il paese in cui risiedi per visualizzare le informazioni.
4. Se non dovessi trovare un distributore di Bitdefender nel tuo paese, contattaci via e-mail all'indirizzo sales@bitdefender.com. Scrivi la tua e-mail in inglese per permetterci di assisterti prontamente.

30.3. Uffici di Bitdefender

Gli uffici di Bitdefender sono sempre pronti a rispondere a ogni richiesta inerente le loro competenze, sia in ambito commerciale sia generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefono (ufficio e vendite): 1-954-776-6262
Vendite: sales@bitdefender.com
Supporto tecnico: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

Regno Unito e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail: info@bitdefender.co.uk
Telefono: +44 (0) 8451-305096
Vendite: sales@bitdefender.co.uk
Supporto tecnico: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.co.uk

Germania

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Deutschland
Ufficio: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendite: vertrieb@bitdefender.de
Supporto tecnico: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

Spagna

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Telefono: +34 902 19 07 65
Vendite: comercial@bitdefender.es
Supporto tecnico: http://www.bitdefender.es/support/consumer.html
Sito: http://www.bitdefender.es

Romania

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefono vendite: +40 21 2063470
Indirizzo e-mail ufficio vendite: sales@bitdefender.ro
Supporto tecnico: http://www.bitdefender.ro/support/consumer.html
Sito: http://www.bitdefender.ro

Emirati Arabi Uniti

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefono vendite: 00971-4-4588935 / 00971-4-4589186
Indirizzo e-mail ufficio vendite: sales@bitdefender.com
Supporto tecnico: http://www.bitdefender.com/support/consumer.html
Sito: http://www.bitdefender.com/world

Glossario

ActiveX

ActiveX è una tecnologia per lo sviluppo di programmi che possano essere richiamati da altri programmi e sistemi operativi. La tecnologia ActiveX è utilizzata in Microsoft Internet Explorer per generare pagine Web interattive che appaiano e si comportino come applicazioni invece che come pagine statiche. Con ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX sono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

La modalità adware è spesso combinata con un'applicazione che viene fornita gratuitamente se l'utente accetta l'adware. Considerando che le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove viene spiegato il proposito dell'applicazione, non viene commessa alcuna infrazione.

Comunque, le finestre pop-up di avvertimento possono essere fastidiose e in alcuni casi ridurre le prestazioni del sistema. Inoltre, le informazioni che vengono raccolte da alcune di queste applicazioni possono causare inconvenienti riguardo la privacy degli utenti, non sempre completamente informati sui termini dell'accordo di licenza.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer, diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone del proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Applet Java

Un programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisogna specificare il nome dell'applet e la dimensione (lunghezza e larghezza in pixel) che può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, anche se gli applet vengono lanciati sul client, non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Archivio

Un Disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Area di stato

Introdotta con Windows 95, l'area di stato è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o clicca con il pulsante destro su un'icona per visualizzare e accedere ai dettagli e i controlli.

Backdoor

Una breccia nella sicurezza di un sistema deliberatamente lasciata dal programmatore o dal manutentore. La presenza di tali “brecce” non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l’accesso con utenze privilegiate per servizi tecnici o per i programmatori del produttore a scopo di manutenzione.

Browser

Abbreviazione di browser web, un'applicazione software utilizzata per localizzare e visualizzare pagine web. I browser più diffusi sono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser grafici, ovvero in grado di visualizzare sia elementi grafici che il testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, inclusi suoni e animazioni, anche se per alcuni formati, richiedono dei plug-in.

Client mail

Un client e-mail è un'applicazione che ti consente di inviare e ricevere e-mail.

Cookie

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia di interessi e gusti online degli utenti. In questo settore, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire offerte pubblicitarie personalizzate in base agli interessi degli utenti. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Ma dall'altra, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. In considerazione di questo è in atto un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come

un "codice SKU" (il codice a barre sul retro delle confezioni che viene letto dalle casse). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Download
Per copiare dati (solitamente un file intero) da una fonte principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio online al computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete a un computer della rete.

E-mail
Posta elettronica. Un servizio che invia messaggi ai computer attraverso reti locali o globali.

Elementi di avvio
Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Estensione del nome di un file
Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni di file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi sistemi operativi non ne supportano più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScript, "txt" per testi semplici.

Euristico
Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche firme dei virus. Il vantaggio della scansione euristica è di non essere ingannata dalle nuove varianti dei virus esistenti. Tuttavia, può occasionalmente segnalare una parte di codice sospetto in programmi normali, generando i cosiddetti "falsi positivi".

Eventi
Un'azione oppure un evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera, oppure del sistema, come l'esaurimento della memoria.

Falso positivo
Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

File di rapporto
Un file che elenca le azioni avvenute. Bitdefender crea un rapporto che elenca i percorsi controllati, le cartelle, il numero di archivi e file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

Firma virus
Caratteristica binaria di un virus, utilizzata dal programma antivirus alfine di rilevare ed eliminare il virus stesso.

IP
Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Keylogger
Un keylogger è un'applicazione che registra ogni informazione digitata.

I keylogger non sono dannosi di natura. Possono essere usati anche per scopi legittimi, come monitorare le attività di dipendenti o bambini. Tuttavia, sono utilizzati anche dai criminali informatici per scopi dannosi (per esempio, ottenere dati personali, come credenziali o codici di accesso).

Linea di comando
In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di comando.

Macro virus
Un tipo di virus informatico, codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Memoria
Aree di archiviazione interne al computer. Il termine memoria identifica la memorizzazione dei dati sotto forma di chip, mentre la parola archiviazione viene utilizzata per la memoria su nastri o dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

Non euristico
Questo metodo di scansione si basa su specifiche firme di virus. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare un virus, e quindi non genera falsi allarmi.

Pacchetti di programmi

Un file in un formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di compattare un file in modo da occupare meno memoria. Ad esempio, supponiamo di avere un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che compatta i file potrebbe sostituire gli spazi dei caratteri con un carattere speciale seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di compattazione, ma ce ne sono molte altre.

Percorso

I percorsi esatti per raggiungere un file su un computer. Questi percorsi vengono solitamente descritti attraverso il file system gerarchico dall'alto verso il basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

Phishing

L'atto d'inviare un'e-mail a un utente fingendo di essere una società legittima e affermata, nel tentativo di truffarlo, facendogli cedere informazioni private che saranno usate per furti d'identità. L'e-mail invita gli utenti a visitare una pagina web, dove gli sarà chiesto di aggiornare determinate informazioni personali, come password e numero di carta di credito, codice fiscale o coordinate bancarie. In ogni caso, la pagina web è falsa e creata solo per rubare i dati personali dell'utente.

Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Rootkit

Un rootkit è una serie di strumenti software che consente di accedere a un sistema come amministratore. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza, in modo da non essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, gli accessi e i registri. Se incorporano il software adeguato, possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati ai malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Settore di boot

Un settore all'inizio di ogni disco che ne identifica l'architettura (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuto come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessone a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un cavallo di Troia che gli utenti installano inconsapevolmente con altri applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Trojan

Un programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus dal computer, ma al contrario li introduce.

Il termine deriva da una storia dell'Iliade di Omero, in cui i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Unità disco

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

Le unità disco possono essere interne (incorporate all'interno di un computer) oppure esterne (collocate in un meccanismo separato e connesso al computer).

Virus

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus informatici sono creati dall'uomo. È relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Virus di boot

Un virus che infetta il settore di avvio di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infettato con un virus di boot, farà sì che il virus venga attivato in memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo in memoria.

Virus polimorfico

Un virus che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, questi virus sono difficili da identificare.

Worm

Un programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.