bitdefender

INTERNET SECURITY v10

10th anniversary

Manuale utente

AntiVirus

Firewall

Antispam

Antispyware

Parental Control

bitdefender
secure your every bit

BitDefender Internet Security v10

Manuale utente

BitDefender

Pubblicato 2007.06.08
Version 10.2

Avvertenze Legali


bitdefender
secure your every bit

Sommario

Licenza e garanzia

SE NON SI ACCETTANO I TERMINI E LE CONDIZIONI NON INSTALLARE IL SOFTWARE. SELEZIONANDO "ACCETTO", "OK", "CONTINUA", "SI", OPPURE INSTALLANDO O UTILIZZANDO IN OGNI CASO IL SOFTWARE, STATE INDICANDO IL VOSTRO COMPLETO BENESTARE E ACCETTANDO I TERMINI DI QUESTO ACCORDO.

Questi termini ricoprono le Soluzioni e i Servizi BitDefender per gli utilizzatori Home, incluse le documentazioni relative e qualsiasi aggiornamento e rinnovo delle applicazioni rese disponibili dalla licenza acquistata o qualsiasi servizio in accordo a quanto definito nella documentazione e ogni copia di questa.

Questo accordo di Licenza è un contratto legale tra te (utente finale o individuale o entità singola) e SOFTWIN, per l'utilizzo dei prodotti Software SOFTWIN identificati sopra, che include il software e può includere supporti digitali, materiale stampato, e documentazione "online" oppure elettronica (qui di seguito designata come "BitDefender"), tutti protetti dalle leggi degli Stati Uniti ed internazionali sul copyright, e trattati di protezione internazionali. Mediante l'installazione, copia, o qualsiasi uso di BitDefender, accetti di essere vincolato ai termini di questo accordo. Se non accetti i termini di questo accordo, non installare ne usare BitDefender; puoi, in ogni caso, riportarlo al tuo punto vendita per il rimborso completo dell'importo versato, entro 30 giorni dall'acquisto del quale potrà essere richiesta una ricevuta.

Se non si è d'accordo con i termini che determinano il contratto di utilizzo della licenza, non installare o utilizzare BitDefender.

Licenza BitDefender. BitDefender è protetto da leggi e trattati internazionali sul copyright, così come da altre leggi e trattati sulla proprietà intellettuale. BitDefender è fornito su licenza d'uso, non venduto.

CONCESSIONE DI LICENZA. SOFTWIN concede,solamente all'utente che l'ha acquistata e non a terzi, la presente licenza non esclusiva, limitata e non trasferibile, a utilizzare BitDefender

APPLICAZIONE DEL SOFTWARE. Si può installare e usare BitDefender, su quanti computers è necessario ma limitatamente al numero totale di utenti autorizzati dalla licenza. E' possibile fare una copia addizionale di back-up.

LICENZA UTENTE DESKTOP. Questa licenza si applica al software BitDefender che può essere installato su un computer singolo e che non fornisce servizi di rete. Ogni utente principale può installare questo software su un computer singolo e può eseguire

una copia aggiuntiva per il backup su un dispositivo diverso. Il numero di utenti principali consentito è il numero di utenti della licenza.

PERIODO DI LICENZA. Il periodo di validità, avrà inizio dalla data in cui viene eseguita l'installazione, la copia, o quando viene usato in qualche modo, per la prima volta, BitDefender, e continuerà solamente sul computer dove è stato originariamente installato.

UPGRADE (AGGIORNAMENTO). Se BitDefender è identificato come un upgrade, per usarlo devi essere stato autorizzato precedentemente ad utilizzare un prodotto classificato da SOFTWIN come idoneo all' aggiornamento. Un prodotto BitDefender classificato come upgrade, sostituisce o complementa il prodotto originariamente installato e idoneo. Puoi usare il prodotto aggiornato esclusivamente in conformità con i termini di questo Accordo di Licenza. Se BitDefender è l' upgrade di un componente di un pacchetto di programmi software, dato in licenza come un solo prodotto, può essere utilizzato e trasferito solamente come parte integrante di questo pacchetto e non può essere separato per l'utilizzo su più di un computer.

COPYRIGHT. Tutti i diritti, titoli, e interessi derivati da o verso BitDefender e tutti i diritti di copyright derivati da o verso BitDefender (includendo ma non limitando qualsiasi immagine, fotografia, logo, animazione, video, audio, musica, testo e "applets" incorporati nel BitDefender) il materiale stampato allegato e qualsiasi copia di BitDefender sono proprietà della SOFTWIN. BitDefender è protetto dalle leggi di copyright e da quanto previsto dai trattati internazionali. Di conseguenza, BitDefender deve essere considerato come qualunque altro materiale protetto da copyright ad eccezione del fatto che è possibile installare BitDefender su un singolo computer conservando l'originale esclusivamente per scopi di backup o archiviazione. Non è permessa la copia o riproduzione del materiale stampato e allegato al prodotto o supporto BitDefender. In tutte le copie create indipendentemente dal supporto o formato in cui vi sia BitDefender, è necessario riprodurre ed includere tutte le note copyright in formato originale. Non è permesso noleggiare a terzi, vendere, dare in leasing, la licenza di BitDefender. Non è permesso smontare, raggruppare, disassemblare, creare lavori derivati, modificare, tradurre né fare alcun tentativo per scoprire, individuare, il codice fonte di BitDefender.

GARANZIA LIMITATA. SOFTWIN garantisce che il supporto con il quale viene distribuito BitDefender è esente da difetti per un periodo di trenta giorni dalla data in cui viene consegnato. In caso di difettosità riscontrate, SOFTWIN, a sua discrezione, potrà sostituire il supporto, oppure rimborsare l'importo pagato per l'acquisto, a fronte di una ricevuta. SOFTWIN non garantisce che BitDefender sarà sempre privo di errori o che gli errori verranno comunque corretti. SOFTWIN non garantisce che BitDefender soddisferà le necessità dell'utilizzatore. SOFTWIN CON LA PRESENTE NEGA QUALSIASI ALTRA GARANZIA PER BITDEFENDER, SIA ESPLICITA CHE IMPLICITA. LA SUDDETTA GARANZIA E' ESCLUSIVA E SOSTITUISCE TUTTE LE

ALTRE GARANZIE, SIA ESPLICITE CHE IMPLICITE, INCLUDENDO LE GARANZIE DI COMMERCIABILITA', DI ADEGUAMENTO AD UN PROPOSITO PARTICOLARE, O DI NON INFRAZIONE. QUESTA GARANZIA CONCEDE DIRITTI LEGALI SPECIFICI CHE POSSONO VARIARE DA STATO A STATO.

ECCETTO PER QUANTO CHIARAMENTE SOTTOLINEATO IN QUESTO ACCORDO, ESPRESSAMENTE O IMPLICITAMENTE, RISPETTO AI PRODOTTI, AI MIGLIORAMENTI, ALLA MANUTENZIONE O AL SUPPORTO AD ESSI RELATIVI, O A QUALSIASI ALTRO MATERIALE (TANGIBILE O INTANGIBILE) O SERVIZIO FORNITO DA QUESTI. SOFTWIN QUI DISCONOSCE ESPRESSAMENTE QUALSIASI GARANZIA E CONDIZIONE IMPLICITA, INCLUSO, SENZA LIMITAZIONE, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, APPROPRIATEZZA PER UNO SCOPO PARTICOLARE, TITOLO, NON INTERFERENZA, ACCURATEZZA DEI DATI, ACCURATEZZA DEL CONTENUTO INFORMATIVO, INTEGRAZIONE DEL SISTEMA, E NON VIOLAZIONE DEI DIRITTI DI TERZE PARTI ATTRAVERSO IL FILTRO, LA DISABILITAZIONE, O LA RIMOZIONE DI TALE SOFTWARE, SPYWARE, ADWARE, COOKIE, E-MAIL, DOCUMENTI, PUBBLICITÀ O SIMILI, DI TERZE PARTI, CHE SI ORIGININO DA STATUTO, LEGGE, CORSO DI TRATTATIVE, COSTUMI E PRATICA, O USI DEL COMMERCIO.

DECLINAZIONE DELLE RESPONSABILITA' DI DANNI. Chiunque utilizzi, provi oppure valuti BitDefender, si assume tutto il rischio della qualità e delle prestazioni di BitDefender. In nessun caso SOFTWIN sarà ritenuta responsabile di qualunque danno di qualsiasi tipo, inclusi senza limitazioni, danni diretti o indiretti derivati dall' utilizzo, o la consegna di BitDefender, anche nel caso in cui SOFTWIN sia informata dell'esistenza o la possibilità che tali danni possano verificarsi. ALCUNI STATI NON CONSENTONO LA LIMITAZIONE O L' ESCLUSIONE DI RESPONSABILITA' PER DANNI ACCIDENTALI O CONSEGUENTI, IN QUEL CASO LA LIMITAZIONE O ESCLUSIONE SOPRA INDICATA NON POTRA' ESSERE APPLICATA. IN NESSUN CASO COMUNQUE, LA RESPONSABILITA' DI SOFTWIN POTRA' ECCEDERE IL PREZZO CHE PAGATO PER L'ACQUISTO DI BITDEFENDER. Le restrizioni e limitazioni fissate saranno applicate indipendentemente dal modo in cui si accetta di usare, valutare o provare BitDefender.

AVVISO IMPORTANTE AGLI UTENTI. AVVISO IMPORTANTE AGLI UTENTI. QUESTO SOFTWARE NON E ESENTE DA EVENTUALI DIFETTI PROVOCATI ANCHE DALL'UTILIZZO DELLO STESSO, E NON E' STATO PROGETTATO NE' DESTINATO ALL'USO IN AMBIENTI PERICOLOSI CHE RICHIEDANO OPERAZIONI O ATTIVITA' IN MANCANZA DI SICUREZZA. QUESTO SOFTWARE NON E' ADATTO ALL'USO IN OPERAZIONI DI NAVIGAZIONE AEREA, NELLE ISTALLAZIONI NUCLEARI, NEI SISTEMI DI COMUNICAZIONE, SISTEMI DI ARMAMENTO, SISTEMI DI RESPIRAZIONE ASSISTITA DIRETTA O INDIRETTA, CONTROLLO DEL TRAFFICO AEREO O QUALUNQUE APPLICAZIONE, ISTALLAZIONE, DOVE

L'ERRORE POSSA PROVOCARE MORTE, LESIONI FISICHE GRAVI, O DANNI ALLA PROPRIETA'.

GENERALE. Questo accordo sarà regolato dalle leggi della Romania e dai regolamenti e trattati internazionali sul diritto d'autore. La giurisdizione esclusiva e la sede di decisione per qualsiasi disputa che sorga al di fuori di questi Termini di Licenza sarà in capo ai tribunali della Romania.

I prezzi, i costi e le tasse per l'uso di BitDefender sono soggetti a variazione senza preventiva notifica.

Nel caso di invalidità di qualsiasi previsione di questo Accordo, l'invalidaità non avrà effetto sulla validità delle porzioni residue di questo Accordo.

BitDefender e i lochi BitDefender sono marchi registrati di SOFTWIN. Tutti gli altri marchi registrati utilizzati nel prodotto o nei materiali associati sono di proprietà dei rispettivi titolari.

La licenza terminerà immediatamente senza notifica se si infrange uno qualsiasi dei suoi termini e condizioni. Non si ha diritto ad alcun rimborso da SOFTWIN o da qualsiasi rivenditore di BitDefender come risultato della cessazione. I termini e le condizioni che riguardano la riservatezza e le restrizioni d'uso resteranno in vigore anche dopo qualsiasi cessazione.

SOFTWIN può revisionare questi Termini in qualsiasi momento e i termini revisionati si applicheranno automaticamente alle versioni corrispondenti del Software distribuito con i termini revisionati. Se qualsiasi parte di questi Termini è giudicata nulla o non applicabile, ciò non avrà effetto sulla validità del resto dei Termini, che resteranno validi ed applicabili.

In caso di controversia o inconsistenza tra le traduzioni di questi Termini nelle altre lingue, prevarrà la versione inglese emessa da SOFTWIN.

Contattare SOFTWIN, al n.5 di via Fabrica de Glucoza, 72322-Sector 2, Bucarest, Romania, o al N. di Tel. : 40-21-2330780 o di Fax: 40-21-2330763, indirizzo e-mail: <office@bitdefender.com>.

Prefazione

Questa Guida è destinata a tutti gli utenti che hanno scelto **BitDefender Internet Security v10** come la soluzione di sicurezza per i loro personal computers. L'informazione presentata in questo manuale non è indirizzata solo agli esperti di computer, ma anche a chiunque sia in grado di lavorare con Windows.

Questa guida, descrive **BitDefender Internet Security v10**, la Società e il Team che lo ha sviluppato, inoltre vi guiderà attraverso il processo di installazione, spiegandovi come configurarlo. Troverete come utilizzare **BitDefender Internet Security v10**, come aggiornarlo, testarlo e personalizzarlo. Imparerete come ottenere il massimo da BitDefender.

Vi auguriamo una lettura gradevole e utile.

1. Convenzioni usate in questo manuale

1.1. Convenzioni tipografiche

Nel libro vengono usati diversi stili di testo per una buona leggibilità. L'aspetto e il significato è presentato nella tabella sottostante.

Aspetto	Descrizione
`sample syntax`	Gli esempi sintattici vengono scritti con caratteri `monospazio`.
http://www.bitdefender.com	I link URL indirizzano su ubicazioni esterne, su server http o ftp.
`<support@bitdefender.com>`	Gli indirizzi e-mail vengono inseriti nel testo per informazioni sui contatti.
«Prefazione» (p. xv)	Questo è un link interno, che indirizza verso documenti contenuti nel manuale.
`filename`	File e directory (cartelle) vengono scritte utilizzando fonti `monospazio`.
option	Tutte le opzioni del prodotto vengono evidenziate usando caratteri in **grassetto**.

Aspetto	Descrizione
`sample code listing`	La lista dei codici è scritta con caratteri `monospazio`.

1.2. Avvertenze

Le avvertenze appaiono in note di testo, segnalate graficamente, portando alla tua attenzione informazioni addizionali relative al paragrafo corrente.

Nota

La nota è una breve osservazione. Anche se è possibile ometterla, può indicare informazioni utili come una caratteristica specifica o un link verso argomenti relazionati.

Importante

Questa richiede attenzione, è sconsigliato saltarla. Solitamente contempla informazioni non critiche ma importanti.

Avvertimento

Questa è un'informazione critica che deve essere trattata con estrema cautela. Seguendone le indicazioni si eviteranno eventualità negative. Dovrebbe essere letta e compresa in quanto è la descrizione di qualcosa di estremamente rischioso.

2. Struttura del manuale

Il manuale consiste di 6 parti, contenenti gli argomenti principali: Installazione del prodotto, Descrizione e caratteristiche, Console di gestione, Pratiche consigliate, Rescue CD e Ottenere aiuto. Nel manuale sono presenti appendici e un glossario per chiarire e risolvere alcuni problemi tecnici che potrebbero presentarsi con BitDefender

Informazioni su BitDefender. Breve introduzione a BitDefender.

Installazione del prodotto. Istruzioni passo-passo per installare BitDefender su una postazione di lavoro (workstation). Questa è una guida esaustiva per l' installazione di **BitDefender Internet Security v10**. Iniziando con i prerequisiti per una installazione con successo, sarete guidati attraverso tutto il processo. Al termine, è descritta la procedura di disinstallazione nel caso in cui abbiate la necessità di rimuovere BitDefender.

Descrizione e caratteristiche. BitDefender Internet Security v10, presentazione delle caratteristiche e dei moduli.

Console di gestione. Descrizione dell'amministrazione di base e della manutenzione di BitDefender. I capitoli spiegano nel dettaglio tutte le opzioni di **BitDefender Internet**

Security v10, come registrare il prodotto, come eseguire la scansione del computer, come eseguire gli aggiornamenti. Vi viene insegnato come configurare e utilizzare i moduli BitDefender.

Consigli. Seguire tutte le istruzioni per ottenere il massimo da vostro BitDefender

BitDefender Rescue CD. Descrizione di BitDefender Rescue CD. Aiuta a capire e utilizzare le funzioni del CD di avvio.

Ottenere aiuto. Dove cercare e ottenere un aiuto in caso di difficoltà. E' inclusa anche una sezione FAQ (Domande frequenti).

Glossario. Il glossario cerca di spiegare alcuni termini tecnici e poco comuni che troverete tra le pagine di questo documento.

3. Richiesta di commenti

Vi invitiamo ad aiutarci a migliorare questo manuale. Abbiamo provato e verificato tutte le informazioni contribuendo con il massimo delle nostre risorse, ma se trovare errori vi invitiamo a darcene una immediata comunicazione. Per aiutarci a fornire la migliore documentazione possibile, non esitate a scriverci, comunicando i vostri consigli.

Informateci inviando una e-mail a <documentation@bitdefender.com>.

Importante

Per una comunicazione efficiente, vi invitiamo a scrivere i vostri documenti e le e-mails in lingua Inglese.

Informazioni su BitDefender

1. Chi è BitDefender?

BitDefender è un fornitore primario globale di soluzioni di sicurezza che soddisfano i requisiti di protezione degli ambienti computerizzati odierni. La società offre una delle più veloci e ed efficaci linee di software di sicurerzza, creando nuovi standard per la prevenzione delle minacce, per la rilevazione e l'attenuazione tempestive. BitDefender fornisce prodotti e servizi a oltre 41 milioni di utenti privati ed affari in più di 180 paesi. BitDefender ha uffici negli **Stati Uniti**, nel **Regno Unito**, **in Germania**, **Spagna** e **Romania**.

- Caratteristiche dell' antivirus, firewall, antispyware, antispam e parental control per aziende e utenti home;
- La linea di prodotti BitDefender è progettata per essere implementata in un complesso di strutture IT (work stations, file servers, mail servers, e gateway), su Windows, Linux e piattaforme FreeBSD;
- Il prodotto è distribuito in tutto il mondo ed è disponibile in 18 lingue;
- Facile da usare, con un wizard che guida il processo di installazione e che necessita di poche informazioni;
- Enti certificatori internazionali: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, etc;
- Il team customer care è disponibile 24 ore, 7 giorni la settimana;
- Velocità di risposta a nuovi attacchi;
- In percentuale, dei migliori sistemi di rilevazione delle minacce.
- L' aggiornamento ogni ora via Internet, automatico o programmato, delle definizioni dei virus, offre una delle migliori protezioni contro le nuove minacce.

1.1. Perché BitDefender?

E' accertato. Produttore antivirus più reattivo. La veloce reattività di BitDefender nel caso di virus epidemici è stata confermata, a cominciare dalle ultime ondate di CodeRed, Nimda e Sircam, così come Badtrans.B o altri codici maligni, pericolosi e di rapida propagazione. BitDefender è stato il primo a fornire antidoti contro questi codici ed a renderli gratuitamente disponibili su Internet per tutti i colpiti. Adesso, con la continua espansione del virus Klez – nelle diverse versioni, la protezione antivirus è diventata un'altra volta una necessità critica per qualsiasi sistema.

Innovativo. Premiato per innovazione, dalla Commissione Europea ed EuroCase. BitDefender è stato proclamato un vincitore del premio European IST, premiato dalla Commissione Europea e da rappresentanti di 18 Accademie in Europa. Adesso, nel suo ottavo anno, il Premio Europeo IST è una ricompensa per prodotti all'avanguardia che rappresentano il meglio della Innovazione europea e tecnologia dell'informazione.

Esaustivo. Copre ogni singolo punto della vostra rete, fornendo una sicurezza completa. Le soluzioni di sicurezza di BitDefender per l'ambiente aziendale soddisfano le necessità di protezione del mondo commerciale attuale, permettendo la gestione di tutte le complesse minacce che mettono in pericolo la rete, dalla piccola area locale fino a enormi WAN multi-server e multi-piattaforme.

La vostra protezione finale. L'ultima frontiera per ogni possibile pericolo per il sistema del tuo computer. Considerando che il rilevamento dei virus basato nell'analisi dei codici non ha sempre offerto buoni risultati, BitDefender ha implementato la protezione basata sul comportamento, offrendo sicurezza contro malware (software maligno) appena nato.

Questi sono **i costi** che le organizzazioni vogliono evitare e per la cui prevenzione vengono disegnati i prodotti di sicurezza:

- Attacchi Worm
- Perdita di comunicazioni per via di mail infette
- Interruzione o guasto mail
- Pulizia e recupero dei sistemi
- Perdita di produttività degli utenti finali perché i sistemi non sono disponibili
- Pirateria informatica, ed accessi non autorizzati che causano danni

Mediante l'uso del set di sicurezza BitDefender, si possono conseguire simultaneamente **sviluppi e benefici**:

- Incrementare la disponibilità della rete, fermando la diffusione di attacchi di codici maligni (Nimda, cavalli di Troia, DdoS).
- Proteggere utenti remoti dagli attacchi.
- Ridurre i costi amministrativi ed incrementare la rapidità, con le capacità gestionali di BitDefender Enterprise.
- Fermare la diffusione di malware tramite e-mail, usando una protezione di posta BitDefender sul gateway dell'azienda. Blocco temporaneo o permanente di connessioni ad applicazioni non autorizzate, vulnerabili o costose.

Maggiori informazioni su BitDefender posono essere ottenute visitando: http://www.bitdefender.com.

Installazione del prodotto

2. Installazione di BitDefender Internet Security v10

La sezione **Installazione di BitDefender Internet Security v10** di questa guida all'utente contiene i seguenti argomenti:

- Requisiti di sistema
- Fasi dell'installazione
- Procedura guidata di configurazione
- Upgrade
- Rimuovere, Riparare o Modificare BitDefender

2.1. Requisiti del sistema

Per assicurare un funzionamento appropriato del prodotto, verificare, prima dell'installazione, che sul vostro computer giri uno dei seguenti sistemi operativi e che vi siano i seguenti requisiti di sistema:

Microsoft Windows 2000 / XP 32-bit

- Pentium II 350 MHz o superiore
- Minimo 128 MB di memoria RAM (raccomandati 256 MB)
- Minimo 60 MB di spazio disponibile su hard disk
- Internet Explorer 5.5 o superiore

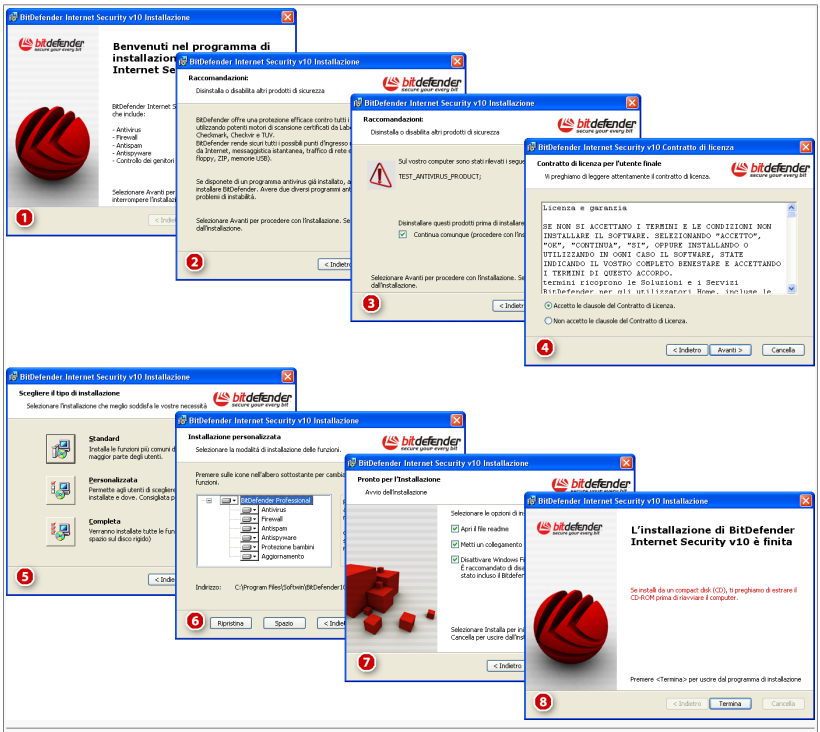
Microsoft Windows Vista 32-bit

- Processore 800 MHz o superiore
- Minimo 512 MB di Memoria RAM (raccomandati 1 GB)
- Minimo 60 MB di spazio disponibile su hard disk

BitDefender Internet Security v10 può essere scaricato per una valutazione all'indirizzo:http://www.bitdefender.com il sito di SOFTWIN corporate, dedicato alla sicurezza dei dati.

2.2. Fasi per l'installazione

Individuare il file di setup e fare click due volte con il mouse. Verrà lanciata la finestra che vi guiderà attraverso il processo di setup:



Fasi per l'installazione

1. Selezionare **Avanti** per continuare oppure **Cancella** se si desidera interrompere l'installazione.
2. Selezionare **Avanti** per continuare oppure **Indietro** per tornare al primo passaggio.
3. BitDefender Internet Security v10 vi avverte se avete altri prodotti antivirus installati sul vostro computer.

Avvertimento

Si raccomanda di disinstallare qualsiasi altro prodotto antivirus precedentemente installato. Infatti due o più antivirus sulla stessa macchina potrebbero rendere il sistema inutilizzabile.

Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare.

Nota

Se BitDefender Internet Security v10 non rileva altri prodotti antivirus sul vostro sistema, salterete questo passo.

4. Vi preghiamo di leggere il Contratto di Licenza, e selezionare **Accetto le clausole del Contratto di Licenza** quindi selezionare **Avanti**. Se non siete d'accordo con le condizioni del contratto, selezionare **Cancella**. In questo caso abbandonerete il processo di installazione e uscirete dal setup.
5. Si può scegliere il tipo di installazione che si desidera: standard, personalizzata oppure completa.

   Standard

   Il programma sarà installato con le opzioni più comuni. Questa opzione è consigliata alla maggior parte degli utenti.

   Personalizzata

   Si possono scegliere i componenti che si desiderano installare. Consigliato solo agli utenti più esperti.

   Completo

   Per l'installazione completa del prodotto. Verranno installati tutti i moduli BitDefender.

   Scegliendo l'installazione **Standard** o **Completa** dovrete saltare la fase 5.
6. Se avete selezionato l'installazione **Personalizzata**, apparirà una nuova finestra che contiene tutte i componenti BitDefender disponibili, in modo da poter scegliere quelli che desiderate installare.

   Selezionando un qualsiasi componente, apparirà sulla destra una breve descrizione (incluso lo spazio minimo richiesto sul disco fisso). Cliccando sull' icona di un qualsiasi componente, apparirà una finestra dove si può scegliere se installare o no il modulo selezionato.

   Si può selezionare la cartella dove installare il prodotto. La cartella di default è `C:\Program Files\Softwin\BitDefender 9`.

   Se desiderate selezionare un' altra cartella, eseguire un click su **Visualizza** e selezionare nella finestra che si apre, la cartella dove volete venga installato BitDefender Internet Security v10. Fare un Click su **Avanti**.
7. Verranno selezionate quattro opzioni di default:
   - **Aprire il file readme** - per aprire il file readme al termine dell'installazione.
   - **Inserire un collegamento sul desktop** - per inserire un collegamento a BitDefender Internet Security v10 sul desktop, al termine dell' installazione.

- **Disattiva il Firewall di Windows** - per disattivare il Firewall di Windows.

  Importante

  Vi raccomandiamo di disabilitare il Firewall di Windows poichè BitDefender Internet Security v10 include già un firewall avanzato. Far girare due firewall sullo stesso computer può causare problemi.

- **Disattiva Windows Defender** - per disattivare Windows Defender; questa opzione compare slo su Windows Vista.

Selezionare **Installa** per iniziare l'installazione del prodotto.

Importante

Durante il processo di installazione apparirà una guida. La guida vi aiuta a registrare il vostro **BitDefender Internet Security v10**, a creare un account BitDefender e a impostare BitDefender per eseguire importanti compiti per la sicurezza.
Completare il il processo di configurazione "wizard" per accedere al passo successivo.

8. Selezionare **Termina** per completare l'installazione del prodotto. Se avete accettato le impostazioni di default per il percorso di installazione, verrà creata una nuova cartella chiamata `Softwin` in `Programmi` che contiene la sottocartella `BitDefender 10`.

   Nota

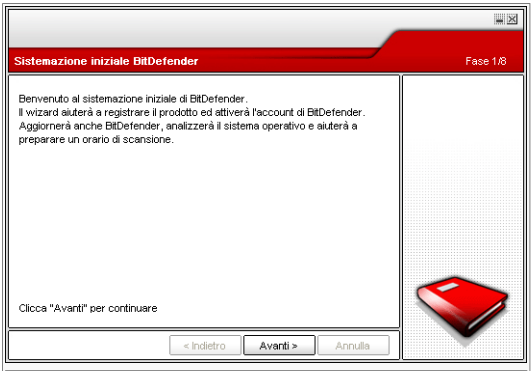
   Potrebbe essere richiesto di riavviare il sistema in modo che il setup completi il processo di installazione.

2.3. Procedura guidata di configurazione

Durante il processo di installazione comparirà una guida. La guida vi aiuta a registrare il vostro **BitDefender Internet Security v10**, a creare un account BitDefender e ad impostare BitDefender per eseguire importanti compiti per la sicurezza.

Completare la procedura guidata non è obbligatorio; in ogni caso vi raccomandiamo di farlo per guadagnare tempo e assicurare il vostro sistema prima che BitDefender Internet Security v10 sia installato.

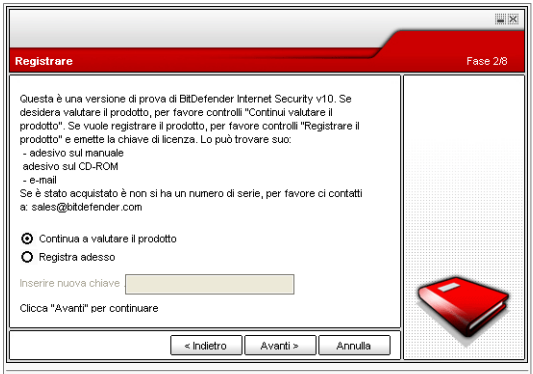
2.3.1. Passo 1/8 - Procedura iniziale di configurazione di BitDefender



Finestra di benvenuto

Selezionare **Avanti**.

2.3.2. Passo 2/8 - Registrazione di BitDefender Internet Security v10



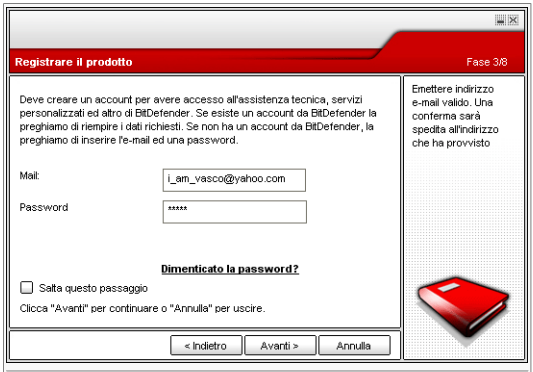
Registrazione del prodotto

Scegliere **Registra il prodotto** per registrare **BitDefender Internet Security v10**. Digitare la chiave licenza nel campo **Inserisci la nuova chiave**.

Per continuare a provare il prodotto, selezionare **Continuare a provare il prodotto**.

Selezionare **Avanti**.

2.3.3. Passo 3/8 - Creare un Account BitDefender



Creazione Account

Non possiedo un account BitDefender

Per beneficiare del supporto tecnico gratuito di BitDefender e di altri servizi gratuiti dovete creare un account.

Digitate un indirizzo e-mail valido nel campo **E-mail**. Pensate ad una password e digitatela nel campo **Password**. Confermate la password nel campo **Digitare nuovamente la password**. Utilizzare l'indirizzo e-mail e la password per identificarvi al vostro account alla pagina http://myaccount.bitdefender.com.

Nota

La password deve essere lunga almeno quattro caratteri.

Per creare un account con successo dovete prima attivare il vostro indirizzo e-mail. Controllate il vostro indirizzo e-mail e seguite le istruzioni nella e-mail spedita dal servizio di registrazione BitDefender.

Importante

Attivate il vostro account prima di passare al prossimo passo.

Se non volete creare un account BitDefender, selezionare semplicemente **Saltare questo passo**. Salterete anche il prossimo passo della guida.

Cliccare su **Successivo** per continuare o su **Annulla** per uscire dalla guida.

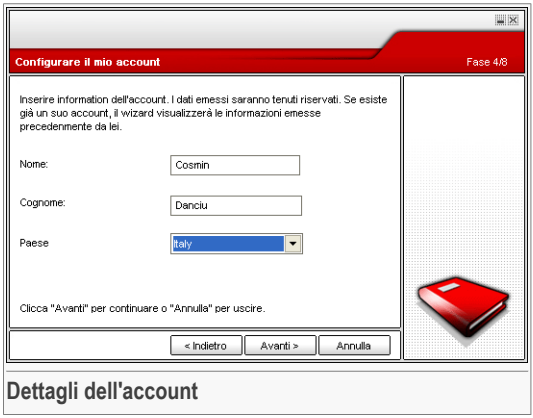
Ho già un account BitDefender

Se avete già un account attivo, fornite l'indirizzo e-mail e la password del vostro account. Se fornite una password non corretta, sarete avvisati di digitarla nuovamente quando cliccate su **Successivo**. Cliccate su **Ok** per inserire di nuovo la password o su **Annulla** per uscire dalla guida.

Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

Cliccare su **Successivo** per continuare o su **Annulla** per uscire dalla guida.

2.3.4. Passo 4/8 - Inserire i dettagli dell'account



Dettagli dell'account

Nota

Non eseguirete questo passo se avete selezionato **Saltare questo passo** nel terzo passo.

Riempite con il vostro nome e cognome, e selezionate il paese in cui risiedete.

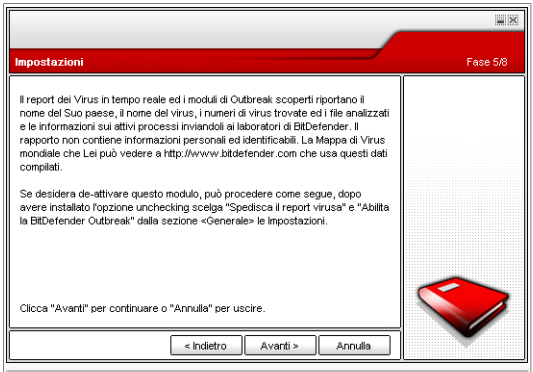
Se possedete già un account, la guida visualizzerà le informazioni che avete fornito in precedenza, se ve ne sono. Qui potete modificare queste informazioni, se volete.

Importante

I dati che fornite qui resteranno riservati.

Cliccare su **Successivo** per continuare o su **Annulla** per uscire dalla guida.

2.3.5. Passo 5/8 - Imparare riguardo a RTVR



Sistema di Informazione

Cliccare su **Successivo** per continuare o su **Annulla** per uscire dalla guida.

2.3.6. Passo 6/8 – Selezionare compiti

Selezione compiti

Impostare BitDefender Internet Security v10 per eseguire importanti compiti per la sicurezza del vostro sistema.

Sono disponibili le seguenti opzioni:

- **Aggiorna i motori di BitDefender Internet Security v10 (può richiedere un riavvio)** - durante il prossimo passo, sarà eseguito un aggiornamento dei motori di BitDefender Internet Security v10 per proteggere il vostro computer contro le ultime minacce.
- **Esegui una scansione rapida del sistema (può richiedere un riavvio)** - durante il prossimo passo, sarà esgeuita una scansione rapida del sistema in modo da consentire a BitDefender Internet Security v10 di assicurarsi che i vostri file nelle cartelle `Windows` e `File di Programma` non siano infetti.
- **Eseguire una scansione completa del sistema ogni giorno alle 2 AM** - esegue una scansione completa del sistema ogni giorno alle 2 AM.

Importante

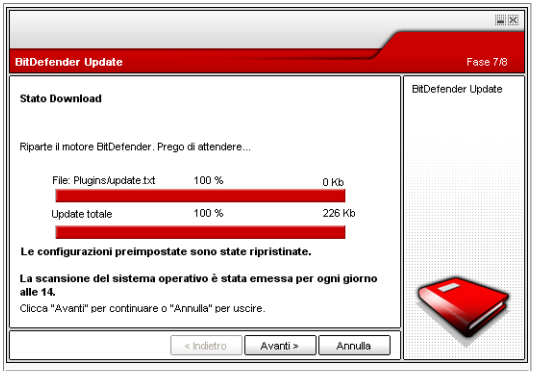
Vi raccomandiamo di abilitare queste opzioni prima di passare al passo successivo per assicurare la sicurezza del vostro sistema.

Se selezionate solo l'ultima opzione o nessuna opzione, salterete al passo successivo.

Potete fare qualsiasi cambio vogliate tornando ai passi precedenti (cliccare su **Indietro**). Più oltre, il processo diviene irreversibile: se scegliete di continuare, non sarete in grado di tornare ai passi precedenti.

Cliccare su **Successivo** per continuare o su **Annulla** per uscire dalla guida.

2.3.7. Passo 7/8 – Attendere il Completamento dei Compiti



Stato dei Task

Attendere che i compiti siano completati. Potete vedere lo stato dei compiti selezionati nel passo precedente.

Cliccare su **Successivo** per continuare o su **Annulla** per uscire dalla guida.

2.3.8. Passo 8/8 - Sommario

Fine

Finestra di configurazione

Selezionare **Aprire il mio Account BitDefender** - per aggiornare BitDefender al termine dell'installazione. E' necessario che il vostro sistema sia connesso ad Internet.

Selezionare **Fine** per completare la finestra e continuare con il processo di installazione.

2.4. Upgrade

L'Upgrade può essere eseguito in uno dei seguenti modi:

- Disinstallare la versione precedente ed installare quella nuova – per tutte le versioni BitDefender

  Prima di si deve rimuovere la versione precedente, quindi riavviare il computer ed installare la nuova come descritto nella sezione «*Fasi per l'installazione*» (p. 7).

Importante

Se eseguite un aggiornamento da BitDefender v8 o superiore, vi consigliamo di salvare le Impostazioni di BitDefender, l'Elenco Amici e l' Elenco Spammers. Completato il processo di aggiornamento, potrete ripristinarli.

2.5. Rimuovere, Riparare o Modificare BitDefender

Se desiderate modificare, riparare o rimuovere **BitDefender Internet Security v10**, selezionare dal menu di avvio di Windows: **Start** -> **Programmi** -> **BitDefender 10** -> **Modifica, Ripara o Disinstalla**.

Verrà richiesto di confermare la vostra scelta, facendo un click su **Avanti**. Apparirà una nuova finestra dove potrete selezionare:

- **Modifica** - per selezionare le nuove componenti del programma da aggiungere o le componenti attualmente installate da rimuovere.

  Nota

  Per imparare come completare il processo di installazione controllare il sesto passo nella sezione «*Fasi per l'installazione*» (p. 7).

- **Ripara** - per re-installare tutte le componenti del programma installate dal setup precedente.

  Importante

  Prima di riparare il prodotto raccomandiamo di salvare l' Elenco Amici e l' Elenco Spammers. Inoltre è possibile salvare le Impostazioni BitDefender e il Database Bayesiano. Una volta terminato il processo di riparazione potrete ripristiarli.

- **Rimuovi** - per rimuovere tutte le componenti installate.

  Se scegliete di rimuovere BitDefender, non sarete più protetti contro i virus, lo spyware e gli hacker. Se volete abilitare il Windows Firewall e il Windows Defender dopo aver disinstallato BitDefender, selezionate le caselle corrispondenti nel prossimo passo della guida.

  Apprezzeremmo che voi trovaste il tempo di spiegarci le ragioni per le quali avete scelto di disinstallare BitDefender. Selezionate la casella corispondente a **Invia FeedBack** e compilate il modulo online per inviarci i vostri suggerimenti.

Per continuare il processo di installazione, selezionare una delle tre opzioni elencate. Consigliamo **Rimuovi** per una re-installazione corretta. Al termine del processo di disinstallazione, consigliamo di cancellare la cartella `Softwin` dalla cartella dei `Program Files`.

Descrizione e caratteristiche

3. BitDefender Internet Security v10

Protezione completa dalle minacce Internet!

BitDefender Internet Security v10 copre tutte le necessità di sicurezza di una famiglia collegata ad Internet. Fornisce la protezione completa contro virus, spyware, spam, truffe, tentativi di phishing, intrusi e contenuti web sgradevoli.

BitDefender v10 è progettato per porre il minor carico possibile sui suoi utenti e sul sistema host, fornendo al contempo una difesa allo 'stato dell'arte' contro le attuali minacce Internet.

3.1. AntiVirus

La missione del modulo Antivirus è assicurare il rilevamento e la rimozione di tutti i virus. L'antivirus BitDefender utilizza un potente motore di scansione, certificato dai Laboratori ICSA, Virus Bulletin, Checkmark, CheckVir e TÜV.

Rilevamento Proattivo. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) emula un computer virtuale all'interno di un computer nel quale parti di software vengono eseguiti per il controllo di potenziali comportamenti anomali. Questa tecnologia rappresenta un nuovo livello di sicurezza che mantiene il sistema operativo al sicuro da virus sconosciuti rilevando codici maligni, le cui firme non sono state ancora rilasciate.

Protezione Antivirus Permanente. I nuovi e migliorati motori di scansione BitDefender effettueranno la scansione e puliranno i file infetti al momento dell'accesso, minimizzando la perdita di dati. I documenti infetti ora potranno essere recuperati e non cancellati.

Rilevamento e Rimozione Rootkit. Un nuovo modulo BitDefender cerca i rootkit (programmi malefici progettati per controllare i computer vittima, restando nascosti) e li rimuove al momento del rilevamento.

Scansione all'accesso. Il traffico web ora è filtrato in tempo reale anche prima di raggiungere il vostro browser, consentendo un'esperienza del web sicura e godibile.

Protezione delle applicazioni Peer-2-Peer. Filtri contro virus diffusi attraverso la messaggeria istantanea (instant messaging) e applicazioni di condivisione di file e software.

Protezione completa E-mail (posta elettronica). BitDefender gira a livello del protocollo POP3/SMTP, filtrando i messaggi e-mail in entrata ed in uscita,

indipendentemente dal client e-mail utilizzato (Outlook™, Outlook Express™ / Windows Mail™, The Bat!™, Netscape®, ecc.), senza nessuna configurazione aggiuntiva.

3.2. Firewall

Il modulo Firewall filtra il traffico di rete e controlla il tempo di accesso e i permessi per applicazioni mentre si è connessi a Internet. In Modo Stealth, il vostro computer risulta "nascosto" a software maligni e hackers. Il modulo Firewall è in grado di rilevare automaticamente e proteggere il computer contro port scans (linea di pacchetti spediti a una macchina per trovare punti di accesso, spesso in preparazione di un attacco).

Controllo Traffico Internet. Definisce esattamente quali connessioni in entrata o in uscita permettere/negare. Definisce le regole riguardo a protocolli specifici, porte, applicazioni e/o indirizzi remoti.

Controllo delle Applicazioni Internet. BitDefender mantiene un database di applicazioni fidate, ed informa gli utenti se le applicazioni che richiedono l'accesso alla rete siano o meno affidabili, in modo che gli utenti possano prendere delle decisioni inforlate. In alternativa, BitDefender può garantire l'accesso automaticamente alle applicazioni fidate.

Controllo Connessioni. BitDefender vi consente di vedere in tempo reale quali programmi hanno aperto quale connessione alla rete. Potete scegliere di consentire o bloccare, permanentemente o temporaneamente, con un semplice click del vostro mouse.

Modalità Invisibile (Stealth). Individui o softwares maligni non hanno necessità di scoprire se il vostro computer esiste, lasciato solo fornisce comunque servizi alla rete. La scelta Modalità Invisibile bloccherà le risposte dalla vostra macchina ai loro tentativi di scoprire quali porte sono aperte o dove si trova esattamente.

Rilevamento dei Portscan. Il modulo firewall di Bitdefender è ora in grado di rilevare e bloccare automaticamente i portscan. Un portscan è un modo semplice di scoprire se il vostro computer può essere o meno vulnerabile; consiste in un tentativo di connessione alle porte per vedere se vi è risposta, molto simile ad uno scassinatore che prova delle porte per trovarne una aperta.

Configurazione Guidata Firewall. La configurazione guidata del firewall aiuta gli utenti a selezionare il profilo di sicurezza più appropriato per la situazione in cui sono - a casa, in ufficio o in movimento.

3.3. Antispam

La nuova tecnologia migliorata di BitDefender Antispam impiega delle notevoli innovazioni tecnologiche che gli consentono di adattarsi alle nuove tecniche di spam man mano che esse emergono, e di "apprendere" le preferenze del suo utente per bloccare lo spam mantenendo al contempo un tasso molto basso di mail legittime etichettate come spam.

Filtro Adattativo. BitDefender impiega tecniche avanzate di clustering e di analisi di rete neurale per classificare le e-mail sulla base delle preferenze dell'utente e dei modelli emergenti nella raccolta locale di e-mail. Il filtro antispam Bayesiano può essere addestrato dall'utente (semplicemente classificando alcune e-mail come spam o come legittime) ed è anche auto-addestrato, sviluppando continuamente nuovi criteri di filtraggio basati sulle decisioni passate.

Anti-Phishing. Tieniti pulito da e-mail maligni che cercano la truffa facendoti dare informazione sul tuo conto bancario con Il nuovo rilevatore Phishing di BitDefender mantiene il vostro computer protetto da e-mail maligne che tentano di ottenere informazioni sul vostro conto bancario o altri dati importanti .

Heuristic, URL, White List/Black List, Filtri Charset e Immagini. Cinque tipi di filtri affinano il vostro controllo sulla posta elettronica. Il filtro euristico verifica la posta con caratteristiche di spam. Il filtro White List/Black List rifiuta le mail provenienti da indirizzi conosciuti come spammers e accetta quelle provenienti da indirizzi amici. Il filtro URL blocca mail contenti links maligni, mentre il filtro charset blocca le mail scritte con caratteri “strani”. Il filtro immagini decide se quelle contenute nelle mail sono specifiche di spam.

Compatibilità e Integrazione con Outlook™. L’antispam BitDefender è compatibile con tutti i client di posta. La barra di menù dell’antispam BitDefender in Microsoft Outlook™ e Outlook Express™ /Wondows Mail™ consente agli utenti di addestrare il filtro Bayesiano.

3.4. Antispyware

BitDefender, utilizzando un' ampio data base di firme di spyware, esegue il monitoraggio e previene potenziali minacce in tempo reale, prima che possano danneggiare il vostro sistema.

Anti-Spyware in Tempo Reale. BitDefender controlla dozzine di potenziali "hotspots" nel vostro sistema, dove spyware potrebbero agire. Inoltre BitDefender controlla qualsiasi modifica fatta sia al vostro sistema che al vostro software. Gli Spyware conosciuti sono bloccati anche in tempo reale.

Scansione e Pulizia di Spyware. BitDefender può fare la scansione di tutto il vostro sistema, o solo di una parte, per rilevare le minacce di spyware. La scansione utilizza un database di firme spyware costantemente aggiornato.

Protezione della Privacy. La guardia privacy monitorizza il traffico HTTP (web) e SMTP (posta) in usicta dal vostro computer per quelle che possono essere informazioni personali - come ad esempio numeri di carte di credito, numeri della Previdenza Sociale, ed altre stringhe definite dall'utente (es. bit di password).

Anti-Dialer. Un anti-dialer configurabile previene l'attacco di applicazioni dannose che potrebbero fare incrementare smisuratamente la bolletta telefonica a vostro carico.

3.5. Parental Control

Il modulo Parental Control può bloccare l'accesso a pagine siti web, e-mails che ritenete inappropriate, oppure l'accesso ad Internet (per alcuni periodi di tempo, come durante le ore dedicate ai "compiti di scuola") e impedire l'uso di applicazioni come giochi, chat, programmi con condivisione di file e altro.

Controllo Web. Un filtro URL vi consente di bloccare l'accesso a contenuti web inappropriati. Un elenco di siti e parti da bloccare é fornita e aggiornata da BitDefender, come parte del regolare processo di aggiornamento.

Filtro Euristico Web. I filtri euristici classificano automaticamente le pagine web sulla base del contenuto e di altri indizi. Invece di fare affidamento unicamente sulle password, questo approccio applica i principi della ricerca antispam nella classificazione delle pagine web. Sono forniti dei profili predefiniti basati sull'età dell'utente.

Filtro Parola Chiave Web. Gli utenti BitDefender possono ora bloccare esplicitamente tutte le pagine web che contengono parole o frasi specifiche.

Filtro Parola Chiave Posta. Le e-mail in arrivo contenenti parole o frasi inopportune possono essere filtrate prima di raggiungere la casella Posta in arrivo.

Limitatore Tempo Web. Usando il limitatore di tempo web, potete permettere o bloccare accessi web a utenti o applicazioni durante determinati intervalli di tempo.

Controllo Applicazioni. Qualsiasi applicazione può essere preclusa all'utilizzo. Giochi, media e software di messaggi, in questo modo possono essere bloccate altre categorie di software e malware. Utilizzando questo tipo di blocco, potete proteggere inoltre applicazioni da modifiche, copie o spostamenti.

3.6. Altre caratteristiche

Schieramento e Utilizzo. Una guida di configurazione si avvia immediatamente dopo l'installazione, aiutando l'utente a selezionare le impostazioni di aggiornamento più

appropriate, implementando un programma di scansione e fornendo un rapido percorso alla registrazione e all'attivazione del prodotto.

Esperienza dell'Utente. BitDefender ha riprogettato l'esperienza dell'utente, ponendo enfasi sulla semplicità d'uso e sull'eliminazione della confusione. Come risultato, molti moduli di BitDefender v10 richiedono un'interazione dell'utente significativamente inferiore, attraverso l'uso conveniente dell'automazione e dell'apprendimento della macchina.

Aggiornamenti Orari. Il vostro BitDefender sarà aggiornato 24 volte al giorno su internet, direttamente o tramite un Server Proxy. Il prodotto è in grado di auto-ripararsi, se fosse necessario, mediante il download dai server di BitDefender, dei file danneggiati o persi. I proprietari delle licenze BitDefender beneficeranno gratuitamente sia degli aggiornamenti delle definizioni di virus che delle migliorie apportate al prodotto.

Supporto 24/7. Il supporto è offerto on-line da personale qualificato e da un database con le risposte alle FAQs (domande frequenti).

Disco di soccorso (Rescue disk). BitDefender Internet Security v10 è consegnato su un CD avviabile. Questo CD può essere usato per analizzare/riparare/disinfettare un sistema compromesso che non può essere avviato.

4. Moduli BitDefender

BitDefender Internet Security v10 contiene i moduli: **Generale**, **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Parental Control** e **Aggiornamento**.

4.1. Modulo Generale

BitDefender arriva completamente configurato per la massima sicurezza.

Nel Modulo Generale viene presentata l'informazione essenziale sullo stato di tutti i moduli di BitDefender. In questo modulo potete registrare il vostro prodotto e impostare i parametri che determinano il livello di sicurezza di BitDefender.

4.2. Modulo Antivirus

BitDefender vi protegge da virus, spyware e altri codici dannosi per il vostro sistema, facendo una scansione dei file, dei messaggi e-mail, dei download e di tutti gli altri contenuti, al momento dell' in ingresso nel vostro computer. Dal modulo antivirus è possibile accedere a tutte le impostazioni e le funzionalità dell' Antivirus Bitdefender.

La protezione che BitDefender vi offre è divisa in due categorie:

- Scansione all'accesso - impedisce l'ingresso di nuovi virus nel vostro sistema, questa funzione viene anche chiamata virus shield. I file vengono esaminati nel momento in cui l'utente vi accede. BitDefender, ad esempio, esaminerà un documento word alla ricerca di virus nel momento in cui questo verrà aperto, oppure un messaggio e-mail al momento della ricezione. BitDefender interviene con la scansione file in tempo reale.
- Scansione a richiesta - rileva virus, spyware o altri codici dannosi presenti nel vostro sistema. Si tratta della classica scansione avviata dall'utente – scegliendo il drive, la cartella o il file che BitDefender deve esaminare.

4.3. Modulo Firewall

Il Firewall protegge il vostro computer da tentativi di connessione in ingresso ed in uscita non autorizzai. E' come una guardia al vostro cancello – manterrà sotto controllo la vostra connessione internet e mantenendo di ciò a cui è consentito l'accesso a Internet e di ciò a questo è negato.

In Modalità Stealth, il vostro computer risulta “nascosto” a software maligni e hacker. Il modulo Firewall è in grado di rilevare automaticamente e proteggere il computer contro i portscan (flusso di pacchetti spediti a una macchina per trovare "punti di accesso", spesso in preparazione di un attacco).

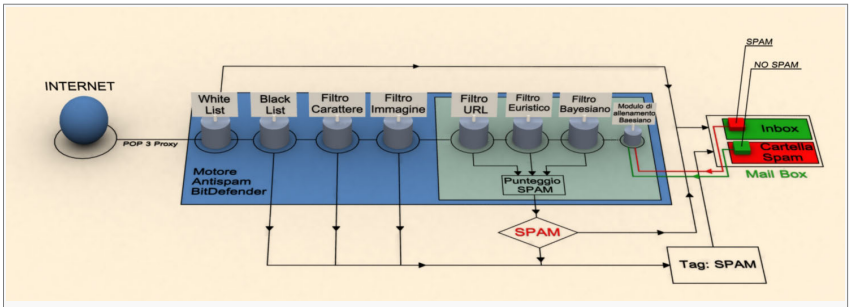
Un firewall è essenziale se si dispone di una banda larga o di una connessione DSL.

4.4. Modulo Antispam

Lo Spam rappresenta un problema in continua crescita, sia per i privati che per le aziende. Non è piacevole, vorreste evitare che i vostri figli lo vedessero, potrebbe penalizzarvi (per aver sprecato troppo tempo o per aver ricevuto mail pornografiche in ufficio) e non potete impedire ad alcuni di inviarlo. La miglior cosa da fare, ovviamente, e di bloccare la ricezione. Purtroppo lo Spam si presenta sotto molte forme e dimensioni e ce n’è tantissimo.

4.4.1. Schema di Lavoro

Lo schema mostra come funziona BitDefender.



Filtri Antispam

Il filtro Antispam dallo schema sopra (White list, Black list, Filtro Carattere, Filtro Immagine, Filtro URL , Filtro Heuristico e Filtro Bayesiano) sono utilizzati congiuntamente dal modulo Antispam di BitDefender per verificare se una determinata parte di mail deve essere inoltrata o no alla vostra **Inbox**.

Ogni e-mail che arriva da Internet viene prima controllata con la White list/Black list. Se l’indirizzo del mittente viene trovato nella White list l’e-mail viene spostata direttamente nella vostra **Inbox**.

Diversamente, il filtro Black list prenderà in carico l'e-mail per verificare se l'indirizzo del mittente è contenuto nel suo elenco. L'e-mail verrà marcata come SPAM e spostata nella cartella **Spam** (situata in Microsoft Outlook) qualora il confronto con la lista abbia dato esito positivo.

Ancora, il Filtro Carattere 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**.

Qualora l'e-mail non fosse scritta con caratteri asiatici o cirillici, la stessa verrà passata al filtro Filtro Immagine. Il **Filtro Immagine** controllerà tutti i messaggi e-mail contenenti allegati con immagini con contenuti di spam.

Il Filtro URL cercherà i link e li comparerà con quelli del database di BitDefender. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

Il Filtro Euristico prenderà in carico l'e-mail ed eseguirà una serie di test su tutte le componenti del messaggio, alla ricerca di parole, frasi, collegamenti o caratteristiche dello Spam. Il risultato sarà quello di aggiungere un altro punteggio Spam alla e-mail.

Nota

Se l'e-mail è marcata come SEXUALLY EXPLICIT nella riga del soggetto, BitDefender la considererà come SPAM.

Il modulo del Filtro Bayesiano analizzerà ulteriormente il messaggio, basandosi su informazioni statistiche relative all'incidenza con cui determinate parole appaiono nei messaggi classificati come Spam, in paragone a quelli dichiarati come non-Spam (da voi o dal filtro euristico). Verrà aggiunto un punteggio Spam alla e-mail.

Se il risultato del punteggio (punteggio URL + punteggio Euristico + punteggio Bayesiano) eccede il punteggio Spam per un messaggio (impostato dall'utente nella sezione Antispam come livello di tolleranza), il messaggio viene considerato come SPAM.

Importante

Se utilizzate un client di e-mail diverso da Microsoft Outlook o Microsoft Outlook Express, dovrete create una regola per spostare i messaggi e-mail contrassegnati come Spam da BitDefender in una cartella personalizzata di quarantena. BitDefender allega il prefisso `[SPAM]` al soggetto dei messaggi considerati come Spam.

4.4.2. Filtri Antispam

Il Motore Antispam BitDefender incorpora sette diversi filtri che assicurano l'assenza di SPAM nella vostra Inbox: White list, Black list, Filtro Carattere, Filtro Immagine, Filtro URL, Filtro Heuristico e Filtro Bayesiano.

Nota

E' possibile abilitare/disabilitare ognuno di questi filtri nel modulo **Antispam**, sezione Impostazioni.

White List / Black List

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**, potrete facilmente classificare da quali persone volete ricevere e-mail (Amici) indipendentemente dal contenuto del messaggio, o da quali persone non volete più ricevere nulla (spammer).

Nota

White list / Black list sono anche conosciute come corrispondenti a **Elenco Amici / Elenco Spammer**.

E' possibile gestire **l'elenco Amici/Spammer** dalla Console di Gestione oppure dalla barra strumenti Antispam.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; inoltre aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Filtro Carattere

La maggior parte dei messaggi Spam sono scritti in caratteri cirillici e/o asiatici. Configurate il filtro se si desiderano rifiutare tutti i messaggi scritti con questi caratteri.

Filtro Immagine

Da quando la detenzione heuristica è diventata una realtà, le cartelle di posta in arrivo sono piene di molti messaggi contenenti solo una immagine con contenuti insoliti. Per contrastare questo problema, BitDefender ha introdotto il **Filtro Immagine** che confronta le firme delle immagini contenute nelle e-mail con il proprio database. In caso di riconoscimento, la e-mail sarà etichettata come Spam.

Filtro URL

La maggior parte dei messaggi Spam contiene links a vari siti web (che solitamente contengono ulteriore pubblicità e la possibilità di acquisto). BitDefender dispone di un database che contiene i links a questo tipo di siti.

Ogni link URL contenuto in un messaggio e-mail sarà esaminatoe confrontato con il database URL. In caso di corrispondenza, il filtro aggiungerà un punteggio Spam alla e-mail.

Filtro Euristico

Il **Filtro Euristico** esegue una serie di tests a tutte le componenti del messaggio (ovvero, non solo l'intestazione ma anche il corpo del messaggio sia in formato HTML che di testo), alla ricerca di parole, frasi, links o altri elementi caratteristici dello SPAM.

Rileva anche i messaggi e-mail con SEXUALLY EXPLICIT nella riga del soggetto. Questi messaggi sono considerati SPAM.

Nota

A partire dal 19 Maggio 2004 lo Spam contenente materiale a sfondo sessuale deve includere l'avviso SEXUALLY EXPLICIT nell'oggetto, diversamente sarà passibile di sanzioni per violazione della legge federale.

Filtro Bayesiano

Il modulo **Filtro Bayesiano** classifica i messaggi secondo informazioni statistiche relative alla frequenza di specifiche parole, contenute nei messaggi classificati come Spam in comparati a quelli dichiarati come non-SPAM (da voi o dal filtro euristico).

Ciò significa, ad esempio, che se una determinata parola di quattro lettere appare più spesso in uno Spam, è naturale desumere che esiste una notevole possibilità che il successivo messaggio in entrata, contenente la stessa parola, SIA SPAM. Vengono prese in considerazione tutte le parole rilevanti all'interno di un messaggio. Sintetizzando le informazioni statistiche, viene valutata la probabilità che l'intero messaggio sia SPAM.

Questo modulo presenta un'altra interessante caratteristica: lo si può "formare", istruire. Si adegua rapidamente al tipo di messaggi ricevuti da un determinato utente e immagazzina informazioni su tutto. Per funzionare efficacemente, il filtro deve essere "istruito", ovvero gli vanno presentati esempi di SPAM e di messaggi leciti, proprio come si addestra un cane da caccia a rilevare determinati odori. A volte il filtro deve essere anche corretto – indotto a regolarsi quando prende una decisione sbagliata.

Importante

E' possibile correggere il modulo Bayesiano utilizzando dalla Barra degli strumenti Antispam i pulsanti **E' Spam** e **Non è Spam**.

Nota

Ogni volta che eseguite un aggiornamento:

- nuove impronte di immagini saranno aggiunte al **Filtro Immagine**;
- nuovi links verranno aggiunti al **Filtro URL**;
- nuove regole verranno aggiunte al **Filtro Euristico**.

Questo aiuterà ad incrementare l'efficacia del vostro motore Antispam.

Importante

Per proteggervi contro gli spammers, BitDefender può effettuare aggiornamenti automatici. Mantenere l'opzione di **Aggiornamento Automatico** attivata.

4.5. Modulo Antispyware

BitDefender esegue il monitoraggio di dozzine di potenziali "hotspots" nel vostro sistema dove lo spyware potrebbe agire; inoltre analizza qualsiasi cambiamento avvenuto sia nel sistema che sul software. Le minacce dello spyware sono quindi bloccate in tempo reale. Il modulo è attivo e blocca Trojan o altri codici installati da hackers, nel tentativo di compromettere la vostra privacy inviando informazioni personali, quali numeri di carte di credito per esempio, dal vostro computer ad altri.

4.6. Modulo Parental Control

Il modulo Parental Control può bloccare l'accesso a pagine siti web, e-mails che ritenete inappropriate, oppure l'accesso ad Internet (per alcuni periodi di tempo, come durante le ore dedicate ai "compiti di scuola") e impedire l'uso di applicazioni come giochi, chat, programmi con condivisione di file e altro.

4.7. Modulo Update

Tutti giorni vengono trovati ed identificati nuovi virus, spyware, codici dannosi; è quindi molto importante mantenere aggiornato il vostro BitDefender. Di default, BitDefender controlla automaticamente ogni ora gli aggiornamenti.

Gli aggiornamenti avvengono nei seguenti modi:

- **Aggiornamenti per motori Antivirus** - non appena compaiono nuove minacce, i files contenenti la firma dei virus devono essere aggiornati per garantire una protezione permanente in tempo reale. Questo tipo di aggiornamento è anche conosciuto come **Virus Definitions Update**.
- **Aggiornamenti per motori Antispam** - verranno aggiunte nuove regole ai filtri Euristico ed URL, e nuove immagini al filtro Immagini. Ciò contribuirà ad aumentare l'efficacia del vostro motore Antispam. Questo tipo di aggiornamento è anche conosciuto come **Antispam Update**.

- **Aggiornamento per i motori antispyware** - nuove firme antispyware saranno aggiunte al database. Questo tipo di aggiornamento è anche conosciuto come **Antispyware Update**.
- **Aggiornamenti del prodotto** - quando viene rilasciata la nuova versione di un prodotto, vengono introdotte nuove funzionalità e tecniche di scansione al fine di migliorarne l'efficienza. Questo tipo di aggiornamento è anche conosciuto come **Product Update**.

Inoltre, dal punto di vista dell'intervento da parte dell'utente, bisogna tenere in considerazione:

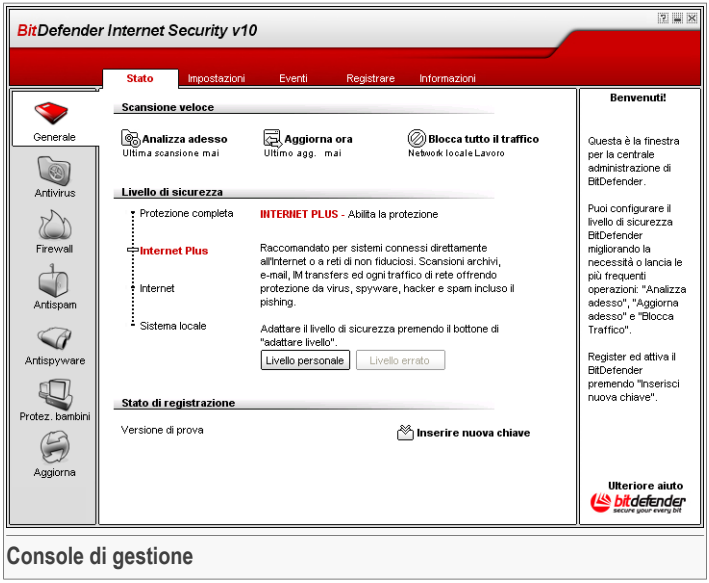
- Aggiornamento automatico - l'antivirus contatta automaticamente il server BitDefender per verificare se è stato rilasciato un aggiornamento. Se è così, BitDefender sarà aggiornato automaticamente. L'aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiorna adesso** nel Modulo di Update.
- Aggiornamento manuale - devete scaricare ed installare le ultime definizioni di virus, spyware, codici dannosi, manualmente.

Console di gestione

5. Informazioni generali sul prodotto BitDefender™

BitDefender Internet Security v10 è stato sviluppato con una console di gestione centralizzata che consente la configurazione delle opzioni di protezione per tutti i moduli di BitDefender. In altre parole, tutto quello che dovete fare è aprire la console di gestione per avere accesso a tutti i moduli: **Antivirus**, **Firewall**, **Antispam**, **Antispyware**, **Parental Control** ed **Aggiornamento**.

Per accedere alla console di gestione, usare il menu di Avvio di Windows, seguendo il percorso **Start** → **Programmi** → **BitDefender 10** → **BitDefender Internet Security v10** or più velocemente facendo un doppio click sull' **Icona BitDefender** dal vassoio di sistema.



Console di gestione

Sulla parte sinistra della console di gestione è possibile selezionare un modulo specifico:

- General - in questa sezione è possible vedere un elenco di tutte le principali impostazioni di BitDefender, dettagli del prodotto e informazioni sui contatti. Inoltre in questa sezione è possibile registrare il prodotto.

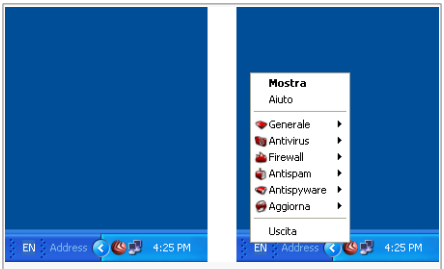
- Antivirus - in questa sezione potete configurare il modulo **Antivirus**.
- Firewall - in questa sezione potete configurare il modulo **Firewall**.
- Antispam - in questa sezione potete configurare il modulo **Antispam**.
- Antispyware - in questa sezione puoi configurare il modulo **Antispyware**.
- Parental Control - in questa sezione potete configurare il modulo **Parental Control**.
- Update - in questa sezione puoi configurare il modulo **Update**.

Nella parte destra della console di amministrazione potete vedere le informazioni relative alla sezione in cui siete. L'opzione **Ulteriore Aiuto**, posizionata in basso a destra, apre il file **Aiuto**.

5.1. Barra di Sistema

Quando la console è minimizzata, appare un'icona nella barra di sistema.

Se fate doppio clicco su questa icona, la console di amministrazione si aprirà. Inoltre, cliccando col tasto destro del mouse, apparirà un menu contestuale. Esso consente l'amministrazione rapida di BitDefender:



L'Icona BitDefender nella Barra di Sistema

- **SMostra / Chiudi** - apre la console di amministrazione o la minimizza sulla barra di sistema.
- **Aiuto** - apre il file di aiuto.
- **BitDefender Antispam** - apre la Console di Gestione.
  - **Inserisci nuova chiave** - apre una finestra con la procedura guidata del processo di registrazione.
  - **Modifica Account** - avvia una guida che vi aiuterà a creare un account BitDefender.
- **Antivirus** - gestione del moduloAntivirus
  - **La protezione in tempo reale è abilitata / disabilitata** - mostra lo stato della protezione in tempo reale (abilitata / disabilitata). Cliccare su questa opzione per disabilitare o abilitare la protezione in tempo reale.
  - **Scan** - apre un sub-menu dal quale è possibile selezionare i files di rapporto che si desiderano visionare.
- **Firewall** - apre la console di gestione del modulo Firewall.
  - **Il firewall è abilitato / disabilitato** - mostra lo stato della protezione firewall (abilitata / disabilitata). Cliccare su questa opzione per disabilitare o abilitare la protezione firewall.

- **Blocca tutto il traffico** blocca tutto il traffico della rete / Internet.
- **Antispam** - apre la console di gestione del moduloAntispam.
  - **Il filtro antispam è abilitato / disabilitato** - mostra lo stato della protezione antispam (abilitata / disabilitata). Cliccare su questa opzione per disabilitare o abilitare la protezione antispam.
  - **Elenco Amici** - apre l' Elenco Amici.
  - **Elenco Spammers** - apre l' Elenco Spammers.
- **Antispyware** - gestione del modulo Antispyware
  - **L'Antispyware Comportamentale è abilitato / disabilitato** - mostra lo stato della protezione antispyware comportamentale (abilitata / disabilitata). Cliccare su questa opzione per disabilitare o abilitare la protezione antispyware comportamentale.
  - **Impostazioni Avanzate** - consente di configurare il controllo antispyware.
- **Aggiornamento** - gestione del modulo Aggiornamento.
  - **Aggiorna adesso** - esegue un aggiornamento immediato.
  - **L'aggiornamento automatico è abilitato / disabilitato** - mostra lo stato degli aggiornamenti automatici (abilitati / disabilitati). Cliccare su questa opzione per disabilitare o abilitare l'aggiornamento automatico.
- **Uscita** - chiude l'applicazione. Selezionando questa opzione, l'icona scomparirà dalla barra di sistema. Per accedere nuovamente alla console di gestione, sarà necessario lanciarla dal menu di Avvio.

Nota

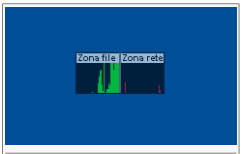
Disabilitando uno o più moduli BitDefender, l'icona diventerà nera. In questo modo sarete informati se qualche modulo è disabilitato senza dovere aprire la console di gestione.
L'icona lampeggierà quando ci sarà un aggiornamento disponibile.

5.2. Barra delle Attività di Scansione

La **Barra delle Attività di Scansione** è una visualizzazione grafica delle attività di scansione sul vostro sistema.

Le barre verdi (**Zona File**) indicano il numero di files esaminati al secondo in una scala da 0 a 50.

Le barre rosse visualizzate nella **Zona Rete** mostrano il numero di Kbyte trasferiti (inviati e ricevuti da Internet) al secondo, in una scala da 0 a 100.



Barra delle Attività

Nota

La **Barra attività di Scansione** vi avviserà quando la protezione in Tempo-Reale o il Firewall sono disabilitati con una croce rossa sopra

l'area corrispondente (**Zona File** o **Zona Rete**). In questo modo saprete se siete protetti senza aprire la console di amministrazione.

Quando non si vuole vedere la visualizzazione grafica, è sufficiente fare un click con il tasto destro del mouse sulla stessa e selezionare**Nascondi**.

Nota

Per nascondere questa finestra, de-selezionare l'opzione **Abilita barra delle attività** (dal modulo **Generale**, sezione Impostazioni).

6. Modulo Generale

La sezione **Generale** di questa guida all'utente, contiene i seguenti punti:

- Informazione Generale
- Impostazioni della Console di Gestione
- Eventi
- Registrazione del prodotto
- Info

Nota

Per ulteriori dettagli riguardanti il modulo **Generale**, consultare la descrizione del «*Modulo Generale*» (p. 27).

6.1. Amministrazione Centrale

Amministrazione Centrale

Questa sezione contiene informazioni sullo stato della vostra licenza BitDefender. Qui si può registrare il prodotto e vederne la data di scadenza.

6.1.1. Compiti Veloci

BitDefender consente l'accesso rapido ai compiti essenziali di sicurezza. Utilizzando questi compiti potete tenere aggiornato il vostro BitDefender, eseguire una scansione del vostro sistema o bloccare il traffico.

Per fare la scansione completa del sistema è sufficiente un click su **Esegui scansione**. Si aprirà la finestra di stato e avrà inizio l' analisi del sistema.

Importante

Raccomandiamo fortemente di eseguire una scansione completa del sistema almeno una volta a settimana. Per maggiori dettagli sui compiti di scansione e sul processo di scansione controllare la sezioneScansione A Richiesta di questa guida utente.

Prima di eseguire la scansione del sistema, vi raccomandiamo di aggiornare BitDefender. Per eseguire l'aggiornamento è sufficiente fare un un click su **Aggiorna adesso**. Attendere qualche secondo perchè il processo di aggiornamento sia completo o, ancora meglio, controllare la sezione Aggiornamento e verificarne lo stato.

Nota

Per maggiori dettagli sul processo di aggiornamento controllare la sezione Aggiornamento Automatico di questa guida utente.

Per bloccare tutto il traffico della rete/Internet, è sufficiente cliccare su **Blocca Traffico** e poi su **Sì** per confermare la vostra scelta. In questo modo isolerete il vostro computer da qualsiasi altro computer nella rete.

Per bloccare tutto il traffico più recente, cliccare semplicemente su **Blocca Traffico**.

Nota

Per imparare come proteggere efficientemente il vostro computer nella rete di cui fa parte, controllare il capitolo Modulo Firewall di questa guida utente.

6.1.2. Livello di Sicurezza

Potete scegliere il livello di sicurezza che meglio si adatta alle vostre necessità di protezione. Trascinare il pulsante sulla barra per impostare il livello di sicurezza appropriato.

Ci sono 4 livelli di sicurezza:

Livello di sicurezza	Descrizione
Rete Locale	Offre una protezione standard, raccomandata soprattutto per i computer senza rete o accesso Internet. Il livello di consumo risorse è basso. Tutti i files ai quali si accede verranno esaminati, indipendentemente dalla loro tipologia.
Internet	Offre una protezione standard per computer collegati direttamente ad Internet o a reti non fidate. Il livello di consumo risorse è moderato. I file a cui si esegue l'accesso, le e-mail, i trasferimenti di MI e tutto il traffico di rete sono scansionati per offrire protezione da virus, spyware e hacker.
Internet Plus	Offre una protezione avanzata per computer collegati direttamente ad Internet o a reti non fidate. Il livello di consumo risorse è moderato. I file a cui si esegue l'accesso, le e-mail, i trasferimenti di MI e tutto il traffico di rete sono scansionati per offrire protezione da virus, spyware, hacker e spam (incluso il phishing).
Protezione Totale	Offre una protezione completa per il vostro sistema. Il livello di consumo risorse è alto. Scansiona tutti i file a cui si accede, le e-mail, i trasfrimenti di MI e tutto il trafico di rete per offrire protezione da virus, spyware, hacker, spam (incluso il phishing) e contenuto inappropriato.

Potete personalizzare il livello di sicurezza clicccando su **Personalizza livello**. Nella finestra che apparirà, selezionate le opzioni di protezione per BitDefender che volete abilitare e cliccate su **OK**.

Cliccando su **Predefinito** verranno applicate le impostazioni di default.

6.1.3. Stato della Registrazione

Questa sezione contiene le informazioni sullo stato della vostra licenza BitDefender. Inoltre si può registrare il prodotto e verificare la data di scadenza.

Per inserire una nuova chiave, cliccare **Inserire Nuova Chiave**. Completare la procedura di registrazione per registrare con successo il vostro BitDefender.

Nota

Per maggiori dettagli sul processo di registrazione controllate la sezione Registrazione Prodotto di questa guida utente.

6.2. Impostazioni della Console di Gestione

Impostazioni della Console di Gestione

Da qui è possibile impostare il comportamento generale di BitDefender. BitDefender è caricato automaticamente all'avvio di Windows e successivamente minimizzato nella barra strumenti.

6.2.1. Impostazioni Generali

- **Abilita la protezione password per le impostazioni del prodotto** - consente l'impostazione di una password per proteggere la configurazione della Cconsole di Gestione BitDefender.

Nota

Se non siete l'unica persona ad utilizzare questo computer, consigliamo di proteggere le vostre Impostazioni BitDefender con una password.

Selezionando questa opzione, apparirà la finestra:

Inserisci password

Digitare la password nel campo **Password**, quindi re-inserirla campo **Ridigitare pwd** e selezionare **OK**.

Da adesso se si desidera cambiare le opzioni di configurazione di BitDefender, vi verrà richiesta la password.

Importante

Se si dimentica la password, è necessario riparare il prodotto per modificare la configurazione BitDefender.

- **Ricezione notifiche di sicurezza** - riceve di volta in volta, dai server BitDefender, segnalazioni di sicurezza relative alla diffusione di nuovi virus.
- **Mostra pop-ups (attiva la schermata delle note)** - mostra finestre a tendina relative allo stato del prodotto.
- **Caricamento di BitDefender all'avvio di Windows** - esecuzione automatica di BitDefender all'avvio del sistema.

Nota

Si raccomanda di lasciare questa opzione selezionata.

- **Abilita / Disabilita Virus Shield** - abilita/disabilita la protezione on-access.
- **Ridurre la console all' Avvio** - la Console di Gestione viene ridotta dopo l'avvio del sistema. Nella barra di sistema apparirà soltanto l' icona BitDefender.

6.2.2. Impostazioni Virus Report

- **Invia Virus Report** - invia ai Laboratori BitDefender i rapporti relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.

  I rapporti non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno solo il nome del virus e verranno utilizzate unicamente per creare rapporti statistici.

- **Invia rapporti dei virus** - invia ai Laboratori BitDefender i rapporti relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.

  I rapporti non contengono dati confidenziali, come il vostro nome, l'indirizzo IP o altri, e non verranno utilizzati per scopi commerciali. Le informazioni fornite conterranno esclusivamente il nome del virus e verranno utilizzate per creare rapporti statistici.

6.2.3. Impostazioni Skin

Consente di selezionare il colore della Console di Gestione. La Skin rappresenta l'immagine di secondo piano - sfndo - sull'interfaccia. Per selezionare sfondi diversi, fare click sul colore corrispondente.

6.2.4. Gestione Impostazioni

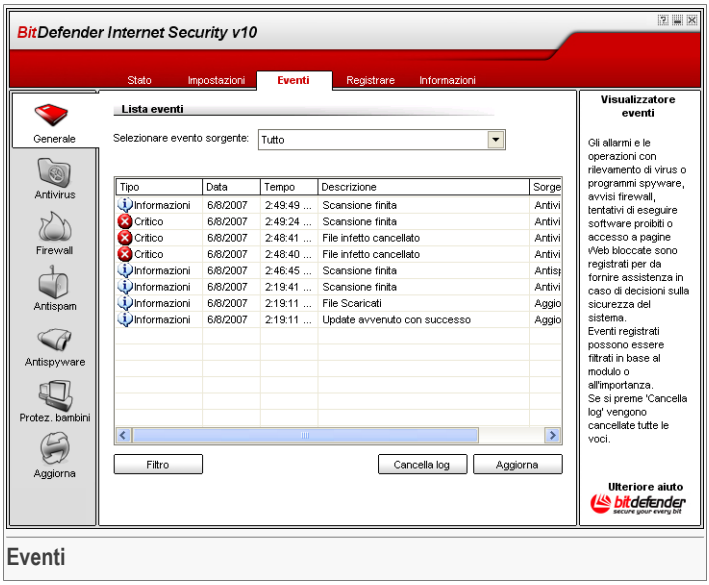
Facendo un click su **Salva tutte le impostazioni** / **Carica tutte le impostazioni** vengono salvate le impostazioni da voi eseguite per il BitDefender in una locazione desiderata. In questo modo potrete utilizzare dopo avere re-installato o riparato il vostro BitDefender.

Importante

Solo gli utenti con diritti di amministrazione possono salvare e caricare le impostazioni.

Per caricare le impostazioni di default, cliccate su **Ripristina Impostazioni di Default**.

6.3. Eventi



Eventi

In questa sezione vengono presentati tutti gli eventi generati da BitDefender.

Ci sono 3 tipi di eventi: **Informazione**, **Attenzione** e **Critico**.

Esempi di eventi:

- **Informazione** - quando è stata eseguita la scansione di una mail;
- **Attenzione** - quando è stato rilevato un file sospetto;
- **Critico** - quando è stato rilevato un file infetto.

Per ogni evento vengono fornite le seguenti informazioni: la data e l'ora in cui è avvenuto l'evento, una breve descrizione e la sorgente (**Antivirus**, **Firewall**, **Antispyware** or **Aggiornamenti**). Eseguire un doppio click sull'evento per vederne le proprietà.

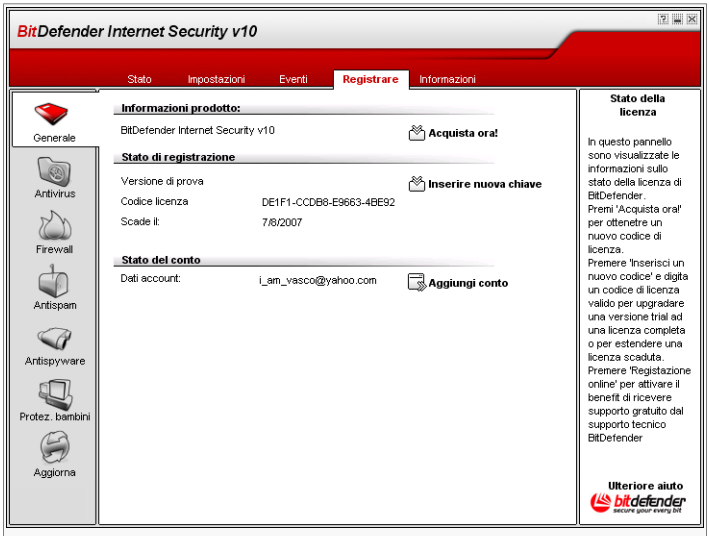
Potete filtrare questi eventi in 2 modi (per tipo o per sorgente):

- Cliccare su **Filtro** per selezionare quali tipi di evento visualizzare.
- Seleziona la sorgente dell'evento dal menu a tendina.

Se la Console di Gestione è aperta alla sezione **Eventi** e nel medesimo momento accade un evento, dovrete cliccare su **Aggiorna** per poterlo vedere.

Per cancellare tutti gli eventi dall'elenco cliccate su **Pulisci log** e quindi su **Sì** per confermare la vostra scelta.

6.4. Registrazione del Prodotto



Registrazione del Prodotto

Questa sezione contiene informazioni relative al prodotto BitDefender (stato della registrazione, ID prodotto, data di scadenza). Inoltre è possibile registrare e configurare il vostro BitDfender.

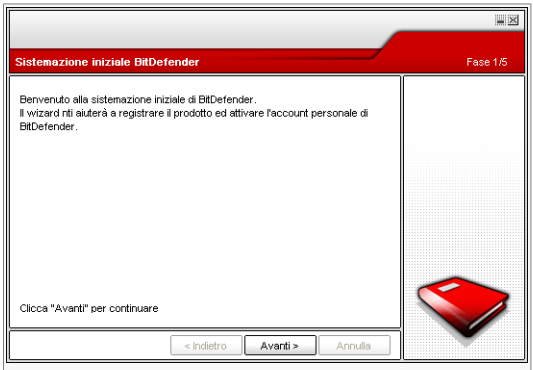
Cliccare sul pulsante **Acquista Ora** per avere una nuova chiave di licenza dal negozio BitDefender online.

Cliccando su **Inserisci la Nuova Chiave** potete registrare il prodotto, modificare la chiave di registrazione o i dettagli dell'account. Per configurare il vostro account BitDefender cliccate su **Edit Account**. In entrambi i casi, apparirà la registrazione guidata.

6.4.1. Registrazione Guidata

L'installazione guidata della configurazione corrisponde a una procedura di 5 passi.

Passo 1/5 - Benvenuti nella Registrazione Guidata BitDefender



Finestra di benvenuto

Selezionare **Avanti**.

Passo 2/5 - Registrare BitDefender

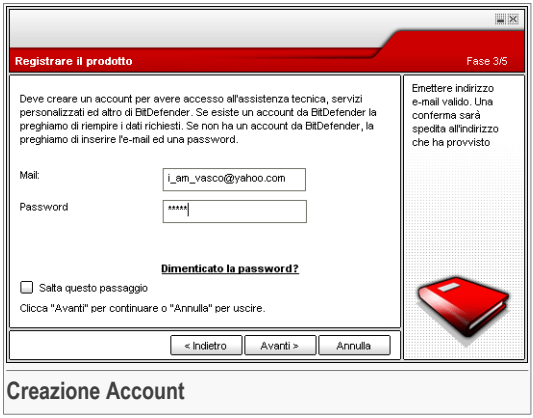
Registrazione del prodotto

Scegliere **Registra il prodotto** per registrare **BitDefender Internet Security v10**. Digitare la chiave licenza nel campo **Inserisci la nuova chiave**.

Per continuare a provare il prodotto selezionare **Continua a provare il prodotto**.

Selezionare **Avanti**.

Passo 3/5 - Creare un Account BitDefender



Creazione Account

Non possiedo un account BitDefender

Per beneficiare del supporto tecnico gratuito di BitDefender e di altri servizi gratuiti dovete creare un account.

Digitate un indirizzo e-mail valido nel campo **E-mail**. Pensate ad una password e digitatela nel campo **Password**. Confermate la password nel campo **Digitare nuovamente la password**. Utilizzare l'indirizzo e-mail e la password per identificarvi al vostro account alla pagina http://myaccount.bitdefender.com.

Nota

La password deve essere lunga almeno quattro caratteri.

Per creare un account con successo dovete prima attivare il vostro indirizzo e-mail. Controllate il vostro indirizzo e-mail e seguite le istruzioni nella e-mail spedita dal servizio di registrazione BitDefender.

Importante

Attivate il vostro account prima di passare al prossimo passo.

Se non volete creare un account BitDefender, selezionare semplicemente **Saltare questo passo**. Salterete anche il prossimo passo della guida.

Selezionare **Successivo** per continuare.

Ho già un account BitDefender

Se avete già un account attivo, fornite l'indirizzo e-mail e la password del vostro account. Se fornite una password non corretta, sarete avvisati di digitarla nuovamente quando cliccate su **Successivo**. Cliccate su **Ok** per inserire di nuovo la password o su **Annulla** per uscire dalla guida.

Se avete dimenticato la vostra password, cliccate su **Password dimenticata?** e seguire le istruzioni.

Selezionare **Successivo** per continuare.

Passaggio 4/5 - Inserire i dettagli dell'account

Dettagli dell'account

Nota

Non entrerete in questo passo se avete selezionato **Salta questo passo** al terzo passo.

Inserire il vostro nome e cognome e selezionare il paese da cui venite.

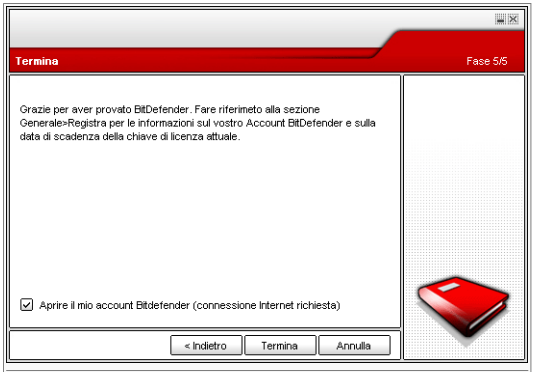
Se avete già un account, la guida visualizzerà le informazioni che avete fornito precedentemente, se ve ne sono. Qui potete anche modificare queste informazioni se lo desiderate.

Importante

I dati che fornite qui resteranno riservati.

Selezionare **Avanti**.

Passaggio 5/5 - Sommario



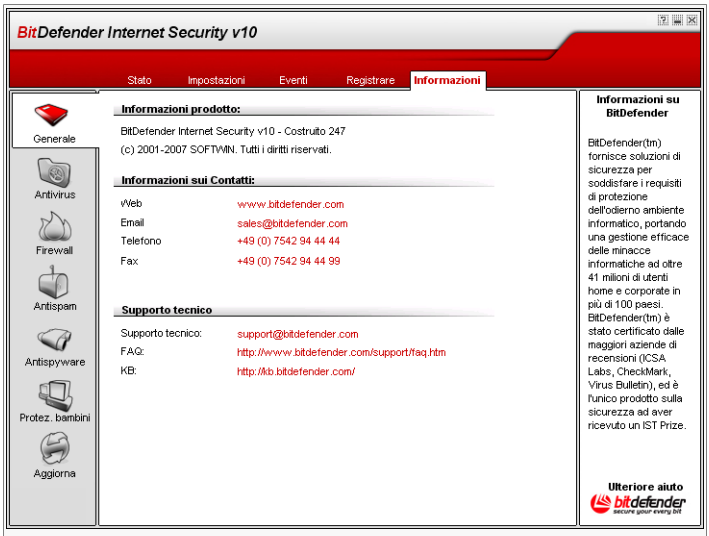
Fine

Questo è il passo finale della configurazione guidata. E' possibile fare qualsiasi modifica tornando al passo precedente (cliccando **Indietro**).

Se non volete apportare modifiche, cliccare **Fine** per terminare la configurazione.

Selezionare **Aprire il mio Account BitDefender** - per aggiornare BitDefender al termine dell'installazione. E' necessario che il vostro sistema sia connesso ad Internet.

6.5. Info



Informazioni generali

Da qui è possibile vedere le informazioni relative allo stato del prodotto.

BitDefender™ è un fornitore globale primario di soluzioni di sicurezza che soddisfano le esigenze di protezionedegli abienti coputerizzati odierni. La società offre una delle linee di software di sicurezza più veloci ed efficaci del settore, creando nuovi standard per la prevenzione, il rilevamento tempestivo e l'attenuazione delle minacce. BitDefender fornisce prodotti e servizi a più di 41 milioni di utenti privati ed affari in oltre 180 paesi.

BitDefenderTM è certificato dai maggiori revisori indipendenti - **ICSA Labs**, **CheckMark** e **Virus Bulletin**, ed è l'unico prodotto di sicurezza ad avere ottenuto un **IST Prize**.

Maggiori informazioni su BitDefender posono essere ottenute visitando: http://www.bitdefender.com.

7. Modulo Antivirus

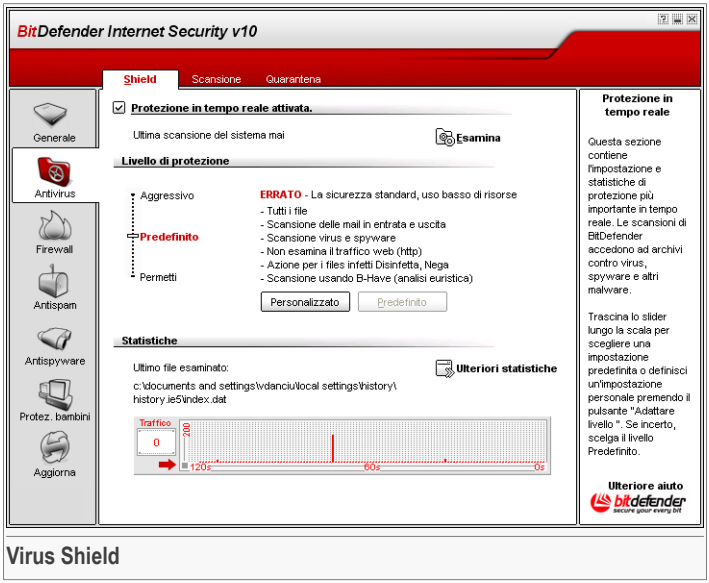
La sezione **Antivirus** di questa guida all'utente contiene i seguenti argomenti:

- Scansione all'accesso
- Scansione a richiesta
- Quarantena

Nota

Per ulteriori dettagli relativi al modulo **Antivirus** vedere la descrizione del «*Modulo Antivirus*» (p. 27).

7.1. Scansione all'accesso



Virus Shield

In questa sezione è possible configurare il **Virus Shield** e vedere le informazioni relative alla sua attività. **Virus Shield** protegge il vostro computer esaminando i messaggi e-mail, i download e tutti i file a cui si accede.

Importante

Per impedire ai virus di infettare il vostro computer, tenere abilitato il **Virus Shield**.

Nella parte inferiore della sezione è possibile osservare le statistiche **Virus Shield** relative ai file e ai messaggi e-mail. Selezionare **Ulteriori Statistiche** se si desidera visualizzare una finestra maggiormente esplicativa.

7.1.1. Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

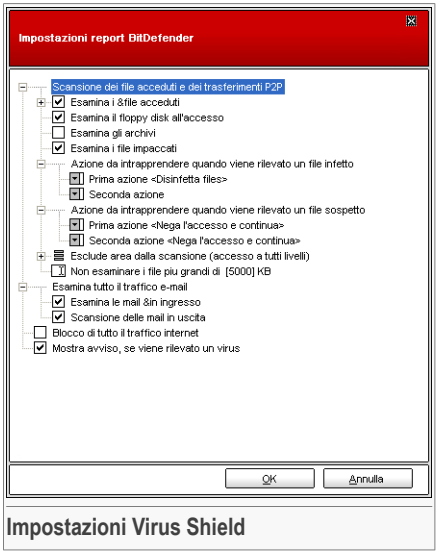
Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Permissiva	Copre le necessità di sicurezza di base. Il livello di consumo delle risorse è molto basso. I programmi e i messaggi di posta in arrivo sono scansionati solo alla ricerca di virus. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/vieta l'accesso.
Default	Offre una sicureza standard. Il livello di consumo delle risorse è basso. Tutti i file e i messaggi di posta in arrivo&in uscita sono scansionati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/vieta l'accesso.
Aggressiva	Offre una sicurezza alta. Il livello di consumo delle risorse è moderato. Tutti i file, e i messaggi e-mail in entrata&in uscita ed il traffico web sono scansionati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/vieta l'accesso.

Per applicare le impostazioni di protezione in tempo reale di default cliccare su **Livello di Default**.

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere evitata su particolari estensioni, cartelle o archivi che si conoscono come innocui, riducendo di molto i tempi di scansione e incrementandone la reattività.

Potete personalizzare la **Real-time protection** cliccando **Custom level**. Apparirà la seguente finestra:



Impostazioni Virus Shield

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows.

Selezionare la casella con "+" per aprire una opzione oppure la casella con "-" per chiudere una opzione.

Si può vedere come alcune opzioni di scansione, nonostante appaia il segno "+", non possano essere aperte. Il motivo è che queste opzioni non sono ancora state selezionate. Si può notare che sarà possibile aprirle una volta selezionate.

- **Scansione dei file in accesso e dei transferimenti P2P** - esamina i file acceduti e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Successivamente selezionare il tipo di file che si desidera esaminare.

Opzione		Descrizione
Esamina i files acceduti	**Esamina tutti i files**	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.
	Soltanto i programmi ed i documenti	Verranno esaminati solo i file di programma, con le seguenti estensioni: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`;

Opzione		Descrizione
		.pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
	Esamina le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Queste estensioni devono essere separate da ";".
	Escludere dala scansione le seguenti estensioni: [ ]	I file con le estensioni specificate dall'utente NON verranno esaminati. Le estensioni devono essere separate da ";".
	Scansione per riskware	Esegue la scansione di applicazioni riskware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva. Selezionare **Salta dialers e applicazioni dalla scansione** se si desidera escludere questi tipo di files dalla scansione.
Scansiona il floppy drive in accesso		Scansiona il drive floppy, quando viene eseguito un accesso ad esso.
Esamina gli archivi		Verranno esaminati gli archivi acceduti. Abilitando questa opzione, il computer sarà più lento.
Esamina i programmi impaccati		Verranno esaminati tutti i file impaccati.
Prima azione		Seleziona dal menù delle opzioni la prima azione da intraprendere su files infetti o sospetti:
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
	Ripulisci file	Disinfetta il file infetto.
	Cancella file	Cancella immediatamente i files infetti, senza alcun avviso.

Opzione		Descrizione
	Muovi il file in quarantena	I file infetti vengono spostati nella quarantena.
Seconda azione		Seleziona la seconda azione dalle opzioni da intraprendere sui files infetti, nel caso in cui la prima fallisse.
	Rifiuta l'accesso e continua	Nel caso di individuazione di un file infetto, l'accesso al file verrà negato.
	Cancella file	Cancella immediatamente i files infetti, senza alcun avviso.
	Muovi il file in quarantena	I file infetti vengono spostati nella quarantena.
Non esaminare i files più grandi di [x] Kb		Digitare la dimensione massima dei files da esaminare. Se la dimensione è pari a 0 Kb, tutti i files verranno esaminati.
Escludere dalla scansione le estensioni (APPLICATO A TUTTI I LIVELLI)		Cliccare "+" in corrispondenza a questa opzione per specificare una cartella che sarà esclusa dalla scansione. In questo caso l'opzione si espanderà e una nuova opzione, `Nuovo oggetto`, comparirà. Selezionare la casella corrispondente al nuovo elemento e, dalla finestra di esplorazione, selezionare la cartella che si desidera escludere dalla scansione. Gli oggetti selezionati qui saranno esclusi dalla scansione, indipendentemente dal livello di protezione scelto (non solo per il **Livello Personalizzato**).

- **Esamina il traffico e-mail** - tutti i messaggi e-mail vengono esaminati.

  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Esamina le e-mail in ingresso	Tutte le e-mail in ingresso vengono esaminate.
Esamina le e-mail in uscita	Tutte le e-mail in uscita vengono esaminate.

- **Esamina il traffico http** - tutto il traffico http viene esaminato.
- **Mostra avviso se viene rilevato un virus** - verrà visualizzata una finestra di avviso ogni volta che verrà rilevato un virus in un file o in un messaggio e-mail.

  In presenza di un virus, si aprirà una finestra contenente il nome del virus, e che permetterà di selezionare un azione sul file infetto adottata dal BitDefender, e un link al sito BitDefender dove sarà possibile trovare ulteriori informazioni al riguardo. Per una e-mail infetta, la finestra di allerta contiene anche informazioni sul mittente e il destinatario.

  Nel caso in cui un file sospetto è rilevato, potete lanciare una procedura dalla finestra di allerta che vi aiuterà a trasmettere il file ai Laboratori BitDefender per una ulteriore analisi. È possibile scrivere dalla vostra e-mail per ricevere informazioni relative a questo report.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

7.2. Scansione a richiesta

Impostazioni della Scansione

In questa sezione è possibile configurare il BiDefender per scansionare il vostro computer.

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

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

7.2.1. Impostazioni della Scansione

La scansione a richiesta è basata sui compiti di scansione. l'utente può scansionare il computer utilizzando i compiti di default o i suoi compiti personali (compiti definiti dall'utente).

Vi sono tre categorie di compiti di scansione:

- **Impostazione del Sistema** - contiene la lista delle impostazioni di default. Sono disponibili le impostazioni seguenti:

Compito di default	Descrizione
Scansione del Sistema in Profondità	Scansiona l'intero sistema, inclusi gli archivi, alla ricerca di virus e spyware.
Scansione Completa del Sistema	Scansiona l'intero sistema, esclusi gli archivi, alla ricerca di virus e spyware.
Scansione Veloce del Sistema	Scansiona tutti i programmi alla ricerca di virus e spyware.
Scansione dei dischi removibili	Scansiona i drive removibili alla ricerca di virus e spyware.
Scansione della Memoria	Scansiona la memoria per minacce spyware conosciute.
Scansione per i Rootkits	Scansiona la memoria alla ricerca di malware nascosto.

- **Impostazione Utente** - contiene le impostazioni definite dall'utilizzatore.

  Una impostazione denominata `My Documents` viene fornita. Utilizzate questa opzione per fare una scansione dei vostri documenti da `My Documents`

- **Compiti misti** - contiene un elenco di compiti di scansione misti. Questi compiti di scansione si riferiscono a tipi di scansione alternativi che non possono essere esgeuiti da questa finestra. Potete solo modificare le loro impostazioni o vedere i report delle scansioni.

Alla destra di ogni impostazione sono disponibili tre pulsanti:

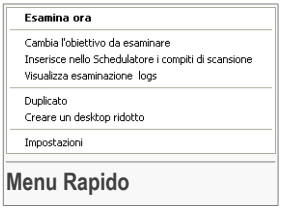
- **Funzione Programmata** - indica che la funzione selezionata è programmata per essere successivamente utilizzata. Cliccare questo bottone per andare alla sezione Programmazione dalle finestre **Proprietà** dove è possibile modificare queste impostazioni.
- **Cancella** - rimuove la funzione selezionata.

Nota
Non disposnibile per compiti di sistema. Non potete rimuovere un compito di sistema.

- **Scansiona Adesso** - esegue la funzione selezionata, iniziando una scansione immediata.

7.2.2. Menu Rapido

Un menu rapido è disponibile per ciascun compito. Cliccare col pulsante destro del mouse sul compito selezionato per aprirlo.



Menu Rapido

Nel menù collegato sono disponibili i seguenti comandi:

- **Scan Now** - esegue la funzione selezionata, avviando immediatamente una scansione.
- **Cambia il Target di Scansione** - apre la finestra**Proprietà**, la tabulazione **Percorso Scansione**, dove potete cambiare il target di scansione per i compiti selezionati.
- **Funzione di Programmazione** - apre la finestra**Proprietà**, la tabulazione **Programmatore** , dove potete programmare il compito selezionato.
- **Vedi i Log di Scansione** - apre la finestra **Proprietà**, la tabulazione **Log della Scansione**, dove potete vedere i report generati dopo che il compito selezionato è stato eseguito.
- **Duplicare** - duplica i compiti selezionati.

Nota
Ciò è utile quando si creano nuovi compiti, in quanto potete modificare le impostazioni del compito duplicato.

- **Creare un Collegamento Desktop** - crea un collegamento sul desktop al compito selezionato.
- **Cancella** - cancella i compiti selezionati.

Nota

Non disposnibile per compiti di sistema. Non potete rimuovere un compito di sistema.

- **Proprietà** - apre la finestra delle **Proprietà**, la tabulazione di **Overview**, dove potete cambiare le impostazioni del compito selezionato.

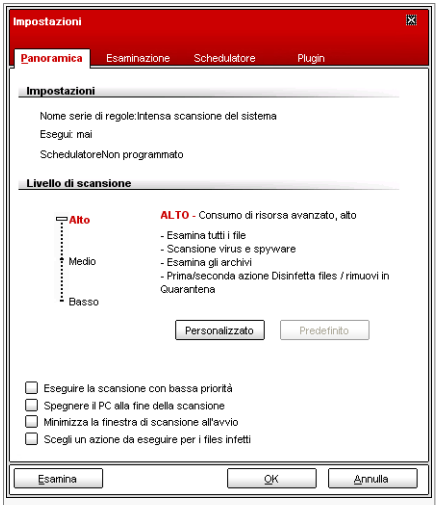
Importante

Data la loro particolare natura, solo le opzioni **Proprietà** e **View Scan Logs** sono disponibili per la categoria delle funzioni **Misc Tasks**.

7.2.3. Proprietà della Funzione di Scansione

Ogni compito di scansione ha la sua propria finestra delle **Proprietà**, dove potete configurare le opzioni di scansione, impostare il target della scansione, programmare il compito o vedere i report. Per entrare in questa finestra selezionare il compito e cliccare su **Proprietà** (o cliccare col tasto destro del mouse sul compito equindi cliccare su **Proprietà**).

Impostazioni di Scansione



Impostazioni di Scansione

Qui potete vedere le informazioni sul compito (nome, ultima esecuzione e stato della programmazione) ed impostare le impostazioni di scansione.

Livello di Scansione

Prima di tutto, dovete scegliere il livello di scansione. Trascinate il pulsante sulla barra per impostare il livello di scansione adeguato.

Ci sono 3 livelli di scansione:

Livello di protezione	Descrizione
Basso	Offre un'efficienza di rilevamento ragionevole. Il livello di consumo delle risorse è basso. Sono scansionati alla ricerca di virus solo i programmi. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.

Livello di protezione	Descrizione
Medio	Offre una buona efficienza di rilevamento. Il livello di consumo delle risorse è moderato. Tutti i file sono scansionati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.
Alto	Offre un'alta efficienza di rilevamento. Il livello di consumo di risorse è alto. Tutti i file e gli archivi sono scansionati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulla firma, è utilizzata anche l'analisi euristica. Le azioni prese sui file infetti sono le seguenti: pulisci file/sposta in quarantena.

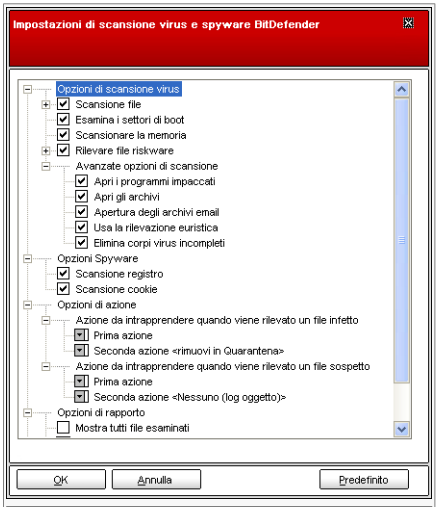
Importante

Il compito **Scansiona per i Rootkit** ha gli stessi livelli di scansione. Comunque, le opzioni sono diverse:

- **Basso** - Sono scansionati solamente i processi. Non viene intrapresa alcuna azione sugli oggetti rilevati.
- **Media** - I files e i processi sono scansionati alla ricerca di eventuali oggetti nascosti. Non viene intrapresa alcuna azione sugli oggetti rilevati.
- **Alto** - I file e i processi sono scansionati alla ricerca di oggetti nascosti. Gli oggetti rilevati sono rinominati.

Gli utenti esperti potrebbero volere approfittare delle varie possibilità di impostazione della scansione BitDefender. La scansione può essere evitata su particolari estensioni, cartelle o archivi che si conoscono come innocui. Questo potrebbe ridurre di parecchio i tempi di scansione incrementando la reattività del vostro computer.

Cliccare su **Personalizza** per impostare le vostre opzioni di scansione. Si aprirà una nuova finestra.



Impostazioni di Scansione

Le opzioni di scansione sono organizzate come menu espandibili, molto simili a quelli di esplorazione di Windows.

Le opzioni di scansione sono raggruppate in cinque categorie:

- **Opzioni di scansione virus**
- **Opzioni di scansione spyware**
- **Opzioni delle Azioni**
- **Opzioni dei Report**
- **Altre opzioni**

Selezionare la casella con "+" per aprire una opzione oppure la casella con "-" per chiudere una opzione.

Importante

Per i compiti **Scansione per i Rootkit** sono disponibili solo tre categorie: **Opzioni di scansione Rootkit**, **Opzioni di Report** e **Altre opzioni**. Dalla prima categoria potete scegliere cosa scansionare (file o memoria o entrambi) e potete impostare l'azione rpesa sugli oggetti rilevati (**Nessuna (logga oggetti)/Rinomina i file**). Le ultime due categorie sono identiche a quelle descritte sotto.

- Specificare il tipo di oggetti che devono essere scansionati (archivi, messaggi e-mail e così via) e altre opzioni. Ciò avviene attraverso la selezione di determinate opzioni dalla categoria **Opzioni di scansione virus**.

Opzione		Descrizione
Scansione files	**Esamina tutti i files**	Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.
	Soltanto i programmi ed i documenti	Saranno esaminati solamente i files di programma. Conseguentemente solo i files con le seguenti estensioni: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` e `nws`.
	Esamina le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Queste estensioni devono essere separate da ";".
	Estensioni definite dall'utilizzatore sono escluse	I file con le estensioni specificate dall'utente NON verranno esaminati. Le estensioni devono essere separate da ";".
Scansione dei settori di avvio		Esamina il settore di avvio del sistema.
Scansione della memoria		Scansiona la memoria alla ricerca di virus e altro malware.
Rilevare files riskware		Esegue la scansione in cerca di pericoli diversi dai virus, come dialers ed adware. Questi file verranno trattati come file infetti. I software che includono componenti adware potrebbero bloccarsi se questa opzione fosse attiva. Selezionare **Eccetto applicazioni e dialers** se si desidera escludere questi tipi di files dalla scansione.
Opzioni de scansione avanzate	**Apri i programmi impaccati**	Scansiona i files impaccati.
	Apri gli archivi	Scansiona l'interno degli archivi.

Opzione	Descrizione
Aperrtura degli archivi e-email	Eseguire la scansione all'interno degli archivi di posta.
Usa la rilevazione euristica	Per usare la scansione euristica. L'obiettivo della scansione euristica è quello di identificare nuovi virus, basata su determinate caratteristiche ed algoritmi, prima che un virus sia definito. Possono apparire messaggi di falso allarme. Quando viene rilevato, un file di questo tipo è classificato come sospetto. In questi casi raccomandiamo di inviare il file ai laboratori BitDefender per essere esaminato.
Rileva corpi di virus incompleti	Per rilevare anche i corpi di virus incompleti.

- Specificare l'obiettivo della scansione spyware (processi, cookies e memoria). Ciò avviene attraverso la selezione di determinate opzioni dalla categoria **Opzioni di scansione spyware**.

Opzione	Descrizione
Scansione registro	Scansione di voci di registro.
Scansionare cookies	Esamina i files cookie.

- Specificare l'azione da intraprendere sui file infetti o sospetti. Aprire **Opzioni delle Azioni** per vedere tutte le azioni possibili su questi files.

  Selezionare le azioni da intraprendere quando si è rilevato un file infettato o ritenuto sospetto. Potete anche selezionare una seconda azione se la prima fallisce.

Azione	Descrizione
Nessuno(log oggetti)	Nessuna azione verrà eseguita sui file infetti. Questi files appariranno nel file di rapporto.
Sollecito all'utente prima di agire	Quando viene rilevato un file infetto, apparirà una finestra che chiede all'utente di selezionare l'azione che si desidera eseguire su quel file. In virtù dell'importanza di quel file, è possibile scegliere se

Azione	Descrizione
	disinfettarlo, isolarlo nella zona di quarantena o cancellarlo.
Disinfetta i files	Disinfetta il file infetto.
Cancella i files	Cancella immediatamente i files infetti, senza alcun avviso.
Muovere i files in Quarantena	Sposta i file infetti nella zona di quarantena.
Rinomina i files	Per cambiare l'estensione dei file infetti. La nuova estensione dei file infetti sarà `.vir`. Rinominando i file infetti, viene rimossa la possibilità di eseguirli e pertanto di diffondere l'infezione. Contemporaneamente, potranno essere salvati per ulteriori esami ed analisi.

Importante

Per cambiare l'estensione dei file infetti. La nuova estensione dei file infetti sarà `.vir`. Rinominando i file infetti, viene rimossa la possibilità di eseguirli e pertanto di diffondere l'infezione. Contemporaneamente, potranno essere salvati per ulteriori esami ed analisi.

- Specificare le opzioni per i file di rapporto. Aprire la categoria **Opzioni di rapporto** per vedere tutte le opzioni possibili.

Opzione	Descrizione
Mostra tutti i files esaminati	Elenca tutti i files esaminati ed il loro stato (infetti o no) in un file di rapporto. Con questa opzione abilitata, il computer sarà più lento.
Cancella i logs più vecchi di [x] giorni	Questo è un campo di edit che consente di specificare quando dovrebbe essere lungo un report per essere cosnervato nella sezione Log di Scansione. Selezionare questa opzione e digitare un nuovo intervallo di tempo. L'intervallo di tempo di default è di 180 giorni.

Nota

E' possibile visualizzare il report dei files nella sezione Scan Logs dalla finestra delle **Proprietà**

- Per specificare le altre opzioni. Aprre la categoria **Altre opzioni** da dove potrete selezionare le opzioni seguenti:

Opzione	Descrizione
Sottoponi i files sospetti ai Laboratori BitDefender	Sarete invitati a inviare I files sospetti ai Laboratori BitDefender dopo il termine del processo di scansione.

Se cliccate su **Livello Predefinito** verranno applicate le impostazioni di default.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

Altre Impostazioni

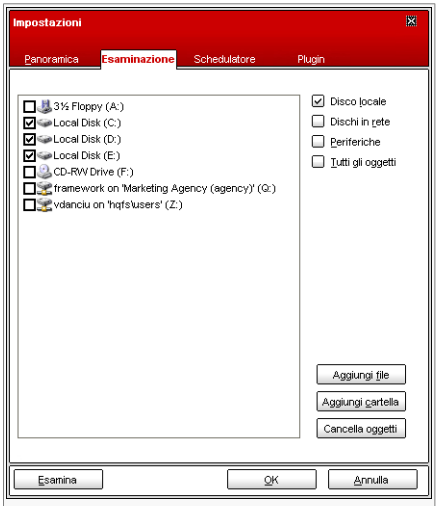
È anche disponibile una serie di opzioni generali per il processo di scansione:

Opzione	Descrizione
Esegui la scansione con priorità bassa	Riduce la priorità del processo di scansione. Consentirete ad altri programmi di essere più veloci ed incrementerete il tempo necessario per terminare il processo di scansione.
Spegnere il PC quando la scansione è completata	Spegne il computer dopo che il processo di scansione è terminato.
Sottoponi i files sospetti ai Laboratori BitDefender	Sarete invitati a inviare I files sospetti ai Laboratori BitDefender dopo il termine del processo di scansione.
Ridurre a icona la finestra di scansione nella barra degli strumenti	Riduce a icona la finestra di scansione sulla barra degli strumenti. Eseguire un doppio clic sull'icona di BitDefender per riaprirla.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

Target di Scansione

Selezionare il compito, cliccare su **Proprietà** e quindi cliccare sulla tabulazione **Percorso di Scansione** per entrare in questa sezione.



Target di Scansione

Qui potete vedere e modificare le impostazioni della scansione.

La sezione contiene i seguenti pulsanti:

- **Aggiungi file(s)** - apre una finestra di visualizzazione dove è possibile selezionare il file(s) che si desidera esaminare.
- **Aggiungi cartella** - come sopra, ma potete selezionare quale cartella(e) si desidera fare esaminare da BitDefender anziché uno specifico file(s).

Nota

Potete anche selezionare e trascinare files/cartelle da aggiungere all'elenco.

- **Cancella oggetti** - rimuove tutti i file(s)/cartelle precedentemente selezionati dall'elenco degli oggetti da esaminare.

Nota

Possono essere cancellati solo i file(s)/cartelle aggiunti successivamente ma non quelli "visti" automaticamente da BitDefender.

Oltre ai pulsanti sopra esposti, ci sono anche alcune opzioni che permettono la selezione veloce della locazione di scansione.

- **Dischi locali** - per esaminare i drives locali.
- **Dischi di rete** - per esaminare tutti i drives di rete.
- **Drives Rimovibili** - per esaminare i drives removibili (CD-ROM, floppy-disk).
- **Tutti gli elementi** - per esaminare tutti i drives, indipendentemente dal fatto che siano locali, sulla rete o rimovibili.

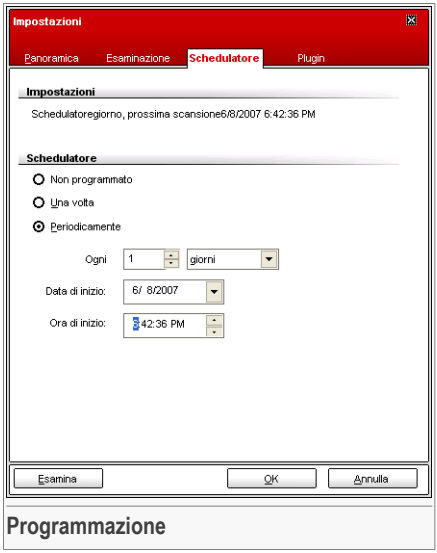
Nota

Se desiderate eseguire una scansione di tutto il vostro computer alla ricerca di virus, selezionare la casella corrispondente a **Tutti gli elementi**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

Programmazione

Selezionare il compito, cliccare su **Proprietà** e quindi cliccare sul tabulatore del **Programmatore** per entrare in questa sezione.



Programmazione

Qui potete vedere se il compito è programmato o no e potete modificare questa proprietà.

Importante

Una scansione completa può richiedere un certo tempo e agisce meglio se vengono chiusi tutti gli altri programmi. La miglior cosa da fare è programmare la scansione nel momento in cui il vostro computer non viene utilizzato.

Quando programmate un compito, dovete scegliere una delle seguenti opzioni:

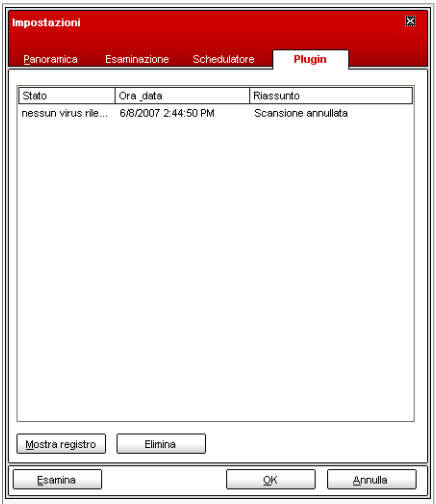
- **Non programmata** - lancia la scansione solo quando richiesta dall'utilizzatore..
- **Una volta** - lancia la scansione solo una volta, in un certo momento. Specificare la data e l'ora di avvio nel campo **Start Date/Time**.
- **Periodicamente** - lancia la scansione periodicamente, a certi intervalli di tempo (ore, giorni, settimane, mesi, anni) iniziando da una certa data ed ora specificate dall'utilizzatore.

  Se si desidera che la scansione venga ripetuta a determinati intervalli, selezionare la casella corrispondente a **Periodicamente** e digitare nel campo **Ogni** il numero di minuti / ore / giorni / settimane / mesi / anni indicando la frequenza del processo. Dovete inoltre specificare la data e l'ora di inizio nel campo **Start Date/Time**.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

Impostazioni della Scansione

Selezionare il compito, cliccare su **Proprietà** e quindi cliccare sul tabulatore **Log di Scansione** per entrare in questa sezione.



Impostazioni della Scansione

Qui potete vedere i file di report generati ogni volta che il compito è stato eseguito. Ciasun file ha allegate informazioni sul suo stato (pulito/infetto), la data e l'ora in cui la scansione è stata eseguita ed un riassunto (scansione terminata).

Sono disponibili due pulsanti:

- **Mostra** - apre il file di rapporto selezionato;
- **Cancella** - cancella il file di rapporto selezionato.

Inoltre, per vedere o cancellare un file, cliccate col tasto destro del mouse sul file e selezionate l'opzione corrispondente dal menu rapido.

Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

7.2.4. Scansione a richiesta

BitDefender consente tre tipi di scansione su richiesta:

- Scansione immediata - avvia immediatamente un evento di scansione dal sistema / funzioni utilizzatore;
- Scansione contestuale - selezionare un file o una cartella con il tasto destro e selezionare BitDefender Antivirus v10;

- Scansione Seleziona & Trascina - seleziona & trascina un file o una cartella sopra la Barra delle Attività di Scansione;

Scansione Immediata

Per eseguire una scansione del vostro computer o di parte di essi potete usare i compiti di scansione di default o potete creare i vostri compiti personalizzati. Vi sono due metodi per creare compiti di scansione:

- Duplicare un compito esistente, rinominarlo ed apportare le modifiche necessarie nella finestra delle Proprietà;
- Cliccare **Nuovo Evento** per creare un nuovo evento e configurarlo.

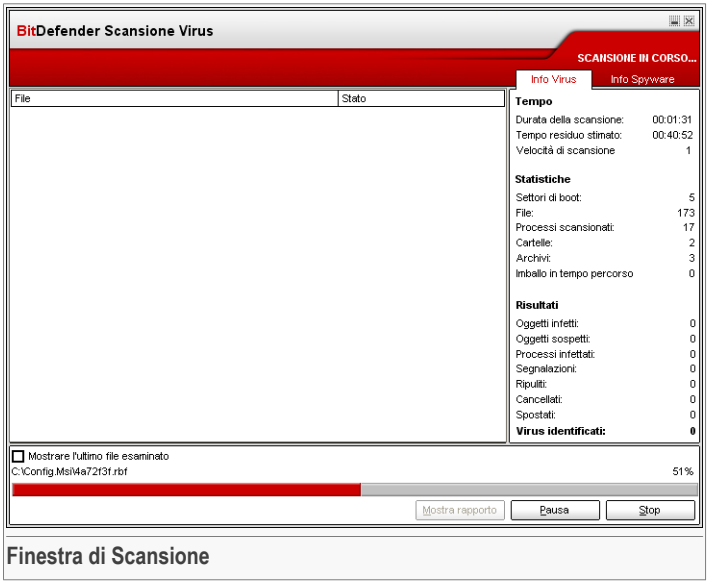
Per consentire a BitDefender di eseguire una scansione completa, dovrete chiudere tutti i programmi aperti. In particolare è importatnte chiudere il vostro client di posta (come Outlook, Outlook Express oppure Eudora).

Prima di far eseguire a BitDefender la scansione del vostro computer, dovreste assicurarvi che BitDefender sia aggiornato, in quanto ogni giorno vengono scoperti ed identificati nuovi virus. E' possibile verificare la data dell'ultimo aggiornamento nella parte superiore del modulo Update.

Per avviare la scansione, utilizzare uno di questi metodi:

- fare doppio click sul compito di scansione desiderato dall'elenco.
- cliccare sul pulsante **Esegui scansione ora** corrispondente al compito.
- selezionare il compito e quindi cliccare su **Esegui Compito**.

Apparirà la finestra di scansione.



Finestra di Scansione

Un icona apparirà nella barra di sistema quando il processo di scansione è avviato.

Durante la scansione BitDefender indica l'avanzamento vi avvisa nel caso in cui vengano trovati dei virus. Sulla destra è possibile visualizzare le statistiche relative al processo di scansione. In base all'obiettivo di scansione sono disponibili informazioni sugli spyware e/o i virus. Se entrambi sono disponibili, fare un clic sulla scheda corrispondente per avere ulteriori informazioni sul processo di scansione di spyware o virus.

Selezionando la casella corrispondente a **Mostrare l'ultimo file esaminato** e saranno visibili solo le informazioni relative agli ultimi file esaminati.

Nota

La durata del processo dipende dalla complessità della scansione.

Sono disponibili tre pulsanti:

- **Stop** - apre una nuova finestra dove potete terminare il processo di scansione. Cliccare **Si&Chiudi** per uscitre dalla finestra di scansione.

Nota

Se sono stati rilevati file sospetti durante la scansione, vi sarà richiesto di sottoporli al Lab BitDefender.

- **Pausa** - sospende temporaneamente il processo di scansione - si può continuare cliccando su **Riprendi**.
- **Mostra rapporto** - apre il rapporto di scansione.

Nota

Se cliccate col tasto destro del mouse su un compito in esecuzione, apparirà un menu rapido (contestuale) che vi consentirà di gestire la finestra di scansione. Le opzioni (**Pausa / Riprendi**, **Stop** e **Stop&Chiudi**) sono simili a quelle dei pulsanti nella finestra di scansione.

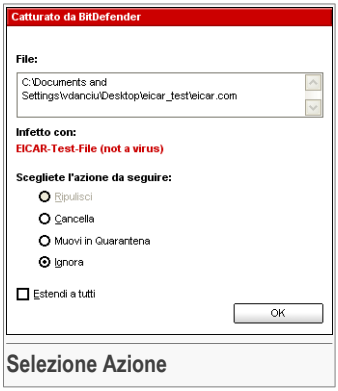
Se l'opzione **Richiedi azione all'utente** è impostata nella finestra delle Proprietà, quando viene rilevato un file infetto una finestra di allarme vi chiederà di selezionare l'azione da prendere sul file infetto.

Si possono vedere il nome del file e del virus.

Selezionare una delle azioni seguenti da intraprendere sul file infetto:

- **Ripulisci** - disinfetta il file infetto;
- **Cancella** - cancella il file infetto;
- **Sposta in quarantena** - sposta il file infetto nella zona di quarantena;
- **Ignora** - ignora l'infezione. Non verrà intrapresa alcuna azione sul file infetto.

Se esaminate una cartella e desiderate che l'azione da intraprendere sui files infetti sia la stessa per tutti, selezionare l'opzione corrispondete a **Applica a tutti**.



Selezione Azione

Nota

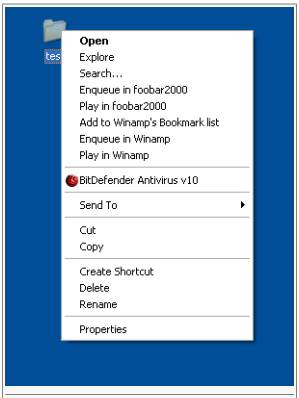
Se l'opzione **Ripulisci** non è abilitata, significa che il file non può essere disinfettato. La scelta migliore è isolarlo nella zona di quarantena e trasmetterlo a noi per una analisi opure cancellarlo.

Cliccare **OK**.

Nota

Il file di rapporto viene automaticamente salvato nella sezione Rapporto del modulo **Proprietà**.

Scansione Contestuale



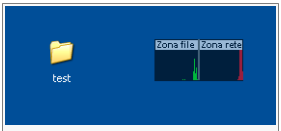
Scansione Contestuale

Premere il tasto destro del mouse sul file o la cartella che si desidera esaminare e selezionare **BitDefender Antivirus v10**.

E' possibile modificare e vedere il file di report dalla finestra delle Proprietà del **Menu Scansione Contestuale**.

Scansione Seleziona e Trascina

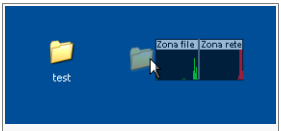
Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.



Trascinare il file

Se viene rilevato un file infetto apparirà una finestra di allarme chiedendovi di selezionare l'azione da rpendere sul file infetto.

In entrambi i casi apparirà la finestra di scansione.



Abbandonare il file

7.2.5. Scansione Rootkit

BitDefender arriva a risolvere le ultime minacce di sicurezza introducendo un rilevatore di rootkit insieme ad i suoi efficienti motori antivirus|amp;antispyware. BitDefender è roa in rado di rilevare i rootkit ricercando file, cartelle o processi nascosti. Inoltre, può proteggere il vostro sistema rinominando il malware che utilizza i rootkit.

Per scansionare il vostro computer alla ricerca di rootkit, eseguite il compito **Scansione per i Rootkit**. Una finestra di scan apparirà.

Importante

Quando controllate la presenza di rootkit, è fortemente raccomandato che impostiate BitDefender in modo da non eseguire alcuna azione sui file nascosti.

Alla fine della scansione potete vedere i risultati. Se sono stati rilevati file nascosti, controllateli accuratamente: la presenza di file nascosti potrebbe indicare una possibile intrusione.

Se siete sicuri che i file rilevati appartengono a malware, vi raccomandiamo di impostare l'azione **Rinomina file** e di eseguire il compito **Scansione per i Rootkit** nuovamente. In questo modo, i file nascosti saranno bloccati.

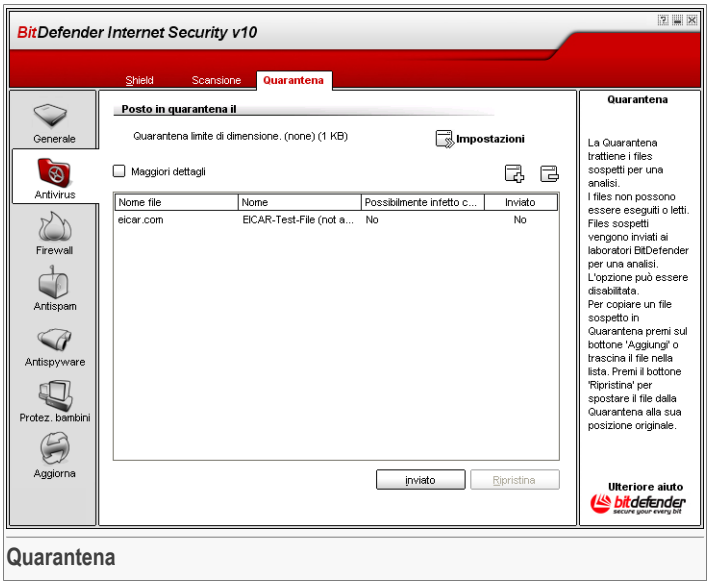
Avvertimento

NON TUTTI GLI ARTICOLI NASCOSTI SONO MALWARE! Prima di rinominare i file, assicuratevi che non appartengano ad una valida applicazione o al sistema. Rinominare tali file renderebbe il vostro sistema inutilizzabile.

Importante

Se il vostro sistema è stato hackato, vi è un solo modo sicuro di rimuovere completamente l'intrusione: reinstallare il sistema.

7.3. Quarantena



Quarantena

BitDefender consente di isolare i files infetti o sospetti in un'area sicura, chiamata quarantena. Isolando questi files in quarantena, scompare il rischio di essere infettati e contemporaneamente si ha la possibilità di inviare questi files ai Laboratori BitDefender per ulteriori analisi.

La componente che garantisce la gestione dei file isolati è la **Quarantena**. Questo modulo è stato creato con una funzione di invio automatico dei files infetti ai Laboratori BitDefender.

Come potrete notare, la sezione **Quarantena** contiene un elenco di tutti i files che sono stati isolati fino a quel momento. Ogni file ha allegato il suo nome, la dimensione, la data di isolamento e la data di invio. Se desiderate visionare maggiori informazioni sui files in quarantena, selezionare **Maggiori dettagli**.

Nota

Quando un virus è in quarantena, non può più arrecare alcun danno in quanto non può essere eseguito o letto.

Cliccando **Add** è possibile aggiungere/inviare un file sospetto in quarantena. Si aprirà una finestra dove è possibile selezionare il file dalla propria locazione. In questo caso il file è copiato nella quarantena. Se desiderate spostare il file nell'area della quarantena dovete selezionare la casella corrispondente a **Cancellare dalla locazione originale**. Un metodo veloce per inviare un file sospetto in quarantena e quello di trascinarlo direttamente nella lista corrispondente.

Per cancellare un file selezionato dalla quarantena, cliccare **Remove**. Se desiderate inviare un file selezionato alla sua posizione originale,cliccare **Restore**.

Potet inviare qualsiasi file selzionato dalla quarantena al lab BitDefender clicando su **Invia**.

Importante

Si devono specificare alcune informazioni prima di inviare questi files. Per questo, selezionare **Impostazioni** e completare i campi della sezione **Impostazioni Inoltro**, come descritto di seguito.

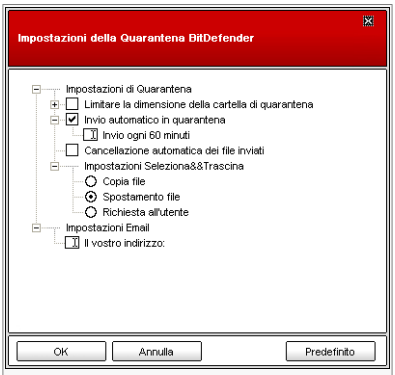
Cliccare su **Impostazioni** per aprire le opzioni avanzate per la zona di quarantena. Si aprirà una nuova finestra.

Le opzioni di Quarantena sono raggruppate in due categorie:

- **Impostazioni di Quarantena**
- **Impostazioni Inoltro**

Nota

Selezionare la casella con "+" per aprire una opzione oppure la casella con "-" per chiudere una opzione.



Impostazioni di Quarantena

Impostazioni di Quarantena

- **Limita la dimensione della cartella di quarantena** - mantiene sotto controllo la dimensione della quarantena. La dimensione di default è di 12000 kB. Se volete cambiare questo valore, digitatene uno nuovo nel campo corrispondente.

  Se selezionate la casella di spunta corrispondente a **Cancella automaticamente i vecchi file**, quando la quarantena è piena, e voi aggiungete un nuovo file, i file più vecchi nella quarantena saranno automaticamente cancellati per liberare spazio per i nuovi file aggiunti.

Nota

Di default, la cartella di quarantena non ha limiti di dimensione.

- **Invio automatico in quarantena** - invia automaticamente i files in quarantena ai Laboratori Bitdefender per ulteriori analisi. E' possibile impostare il periodo di tempo tra due processi di invio consecutivi, nel termine di minuti, nel campo **Trasmetti ogni x minuti**.
- **Cancellazione automatica dei files inviati** - cancella automaticamente i files in qarantena dopo averli inviati ai Laboratori BitDefender per l'analisi.
- **Impostazioni Seleziona & Trascina** - se state utilizzando il metodo Seleziona & Trascina per aggiungere i file alla quarantena, potete specificare l'azione: copiare, spostare o chiedere all'utente.

Impostazioni Inoltro

- **Indirizzo** - inserire il vostro indirizzo e-mail nel caso si desideri ricevere messaggi e-mail dai nostri esperti, in relazione ai files sospetti inviati per l'analisi.

Selezionare **OK** per salvare le modifiche. Selezionare **Predefinito** per tornare alle impostazioni di default.

8. Modulo Firewall

La sezione **Firewall** di questa guida all'utente comprende i seguenti punti:

- Configurazione Guidata Firewall
- Stato Firewall
- Protezione del Traffico
- Impostazioni Avanzate
- Attività Firewall

Nota

Per ulteriori dettagli relativi al modulo **Firewall** controllare la descrizione del «*Modulo Firewall*» (p. 27).

8.1. Procedura Guidata Configurazione Firewall

Quando vi loggate a una nuova rete, apparirà una procedura guidata che vi aiuterà a configurare un nuovo Profilo Firewall. La procedura guidata inoltre vi aiuterà a creare un set di regole di base per il Firewall, necessarie per la maggior parte delle applicazioni usate comunemente. Il risultato finale è un sistema protetto, con un client di posta e web browser funzionali

Nota

La procedura guidata può essere lanciata in qualsiasi momento, cliccando su **Riconfigurazione profilo** dalla sezione Traffico. Notate che se scegliete di riconfigurare il profilo tutte le regole del firewall del profilo attuale andranno perse.

Importante

Se la procedura non è completata, il Firewall sarà disabilitato. La procedura guidata apparirà automaticamente quando cercherete di abilitare il Firewall.

8.1.1. Passo 1/7 - Finestra di Benvenuto

Finestra di benvenuto

Digitare il nome del nuovo profilo di rete nel campo **Nome Profilo**.

Scegliere **Crea nuovo profilo** per seguire la procedura guidata e creare un set di regole di base per il Firewall.

Se selezionate **Importa regole da un profilo creato in precedenza** dovete scegliere un profilo di rete dall'elenco. Il nuovo profilo importa tutte le regole del profilo selezionato. Andrete direttamente all'ultimo passo della procedura guidata, senza ulteriore configurazione.

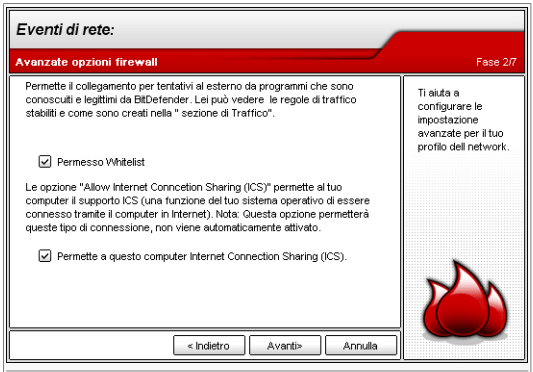
Selezionare **Rendere questo profilo generico ed applicarlo a tutte le nuove reti** per creare un profilo generico o per sovrascrivere il profilo esistente. Il profilo generico sarà applicato ogni volta che BitDefender rileva una nuova rete, senza dover eseguire la configurazione guidata firewall.

Nota

Per disabilitare questa caratteristica, andare alla sezione Avanzate e togliere la spunta all' opzione **Applica lo stesso (generico) profilo a tutte le nuove reti**.

Selezionare **Avanti**.

8.1.2. Passo 2/7 - Impostazioni Avanzate Firewall



Impostazioni Avanzate Firewall

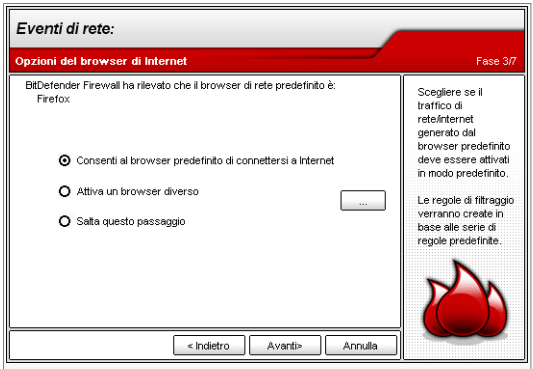
Configurare le impostazioni avanzate firewall del profilo di rete attuale.

Sono disponibili le seguenti opzioni:

Opzione	Descrizione
Autorizza le applicazioni consentite	Permette automaticamente i tentativi di connessione in uscita dai programmi conosciuti da BitDefender come legittimi. Sulla base di questa opzione, le regole che consentono i tentativi di connessione in uscita da tali programmi sono create nella sezione Traffico senza il vostro intervento. Un popup vi avviserà quando una tale regola viene creata. I programmi inclusi nella Whitelist sono le applicazioni più comunemente utilizzate al mondo. Includono i browser più conosciuti, riproduttori audio&video, programmi di chat e condivisione file, così come applicazioni client server e di sistema operativo.
Consenti la Condivisione della Connessione Internet su questo computer	Consente al vostro computer di supportare la Condivisione Connessione Internet (ICS). Questa opzione non abilità automaticamente ICS sul vostro sistema, ma consente solo questo tipo di connessione nel caso voi la abilitiate dal vostro sistema operativo.

Opzione	Descrizione
	La COndivisione Connessione Internet (ICS) abilita i membri delle reti locali a collegarsi ad Internet attraverso il vostro computer. Ciò è utile quando usufruite di una connessione Internet speciale/particolare (es. connessione wireless) e volete condividerla con gli altri membri della vostra rete.

8.1.3. Passo 3/7 – Opzioni del Browser Internet



Opzioni del Browser Internet

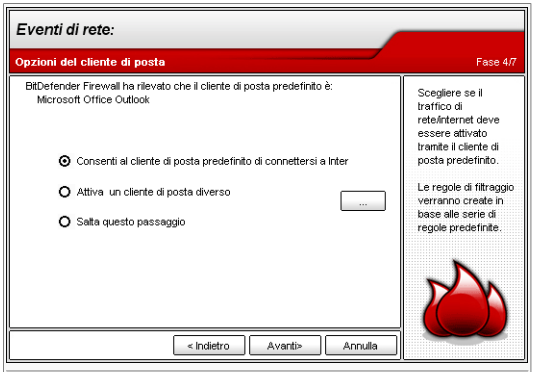
BitDefender rileverà il vostro browser predefinito. Scegliere se il traffico di rete/internet generato dal vostro browser predefinito deve essere consentito di default o selezionate un browser diverso.

Importante

Se sceglite di saltare questo passo, le regole che dipendono da questa scelta non saranno create. Dovrete creare il vostro set di regole. Non saltate questo passo se non siete sicuri di voler creare regole appropriate da voi.

Selezionare **Avanti**.

8.1.4. Passo 4/7 – Opzioni del Client di Posta



Opzioni del Client di Posta

BitDefender rileverà il vostro client di posta predefinito. Scegliere se il traffico di rete/internet generato dal vostro client di posta predefinito deve essere consentito di default o selezionate un client di posta diverso.

Importante

Se sceglite di saltare questo passo, le regole che dipendono da questa scelta non saranno create. Dovrete creare il vostro set di regole. Non saltate questo passo se non siete sicuri di voler creare regole appropriate da voi.

Selezionare **Avanti**.

8.1.5. Passo 5/7 – Opzioni Server Proxy

Opzioni Server Proxy

Se state usando un server proxy per connettervi ad Internet, BitDefender lo rileverà. Scegliere se il traffico di rete/internet verso il server proxy predefinito deve essere consentito di default o cliccare su . . . , corrispondente a **Sto usando un server proxy diverso** e digitare l'indirizzo IP del server proxy e la porta.

Selezionare **Avanti**.

8.1.6. Passo 6/7 – Selezione Tipo di Rete

Selezione Tipo di Rete

Dovete selezionare il tipo di connessione alla rete/internet. Sono disponibili le seguenti opzioni:

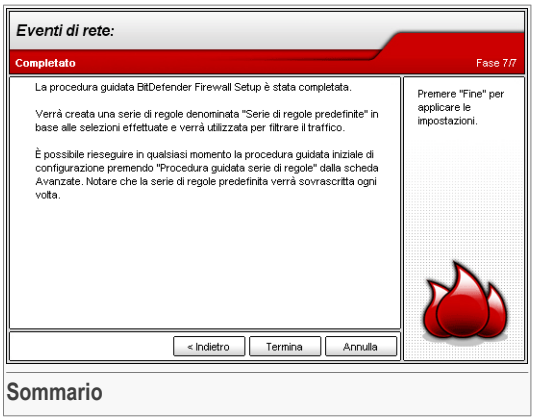
Opzione	Descrizione
Rete Locale (LAN) Affidabile	Dovreste fidarvi solo di reti che abbiano un firewall e che siano protette da un antivirus. Chiedete al vostro amministratore di rete di fare una verifica. Se non conoscete quale tipo di connessione state utilizzando, non scegliere questa impostazione.
Rete Locale (LAN) Non Affidabile	Scegliete questa impostazione se siete ospiti in una rete diversa dalla vostra rete di casa o ufficio. Se non conoscete quale tipo di connessione state utilizzando, non scegliere questa impostazione.
Connesso Direttamente	Scegliete questa impostazione se vi connettete direttamente ad internet o se non conoscete quale tipo di connessione state utilizzando. Tutte le connessioni in entrata saranno negate. Anche se questo modo potrebbe causare a qualche applicazione la perdita di connessione, vi garantirà un alto livello di sicurezza. Potete aggiungere delle regole manualmente per le applicazioni che non riescono a lavorare.

Importante

Se sceglite di saltare questo passo, le regole che dipendono da questa scelta non saranno create. Dovrete creare il vostro set di regole. Non saltate questo passo se non siete sicuri di voler creare regole appropriate da voi.

Selezionare **Avanti**.

8.1.7. Passaggio 7/7 - Sommario



Sommario

Questo è il passo finale della configurazione guidata. E' possibile fare qualsiasi modifica tornando al passo precedente (cliccando **Indietro**).

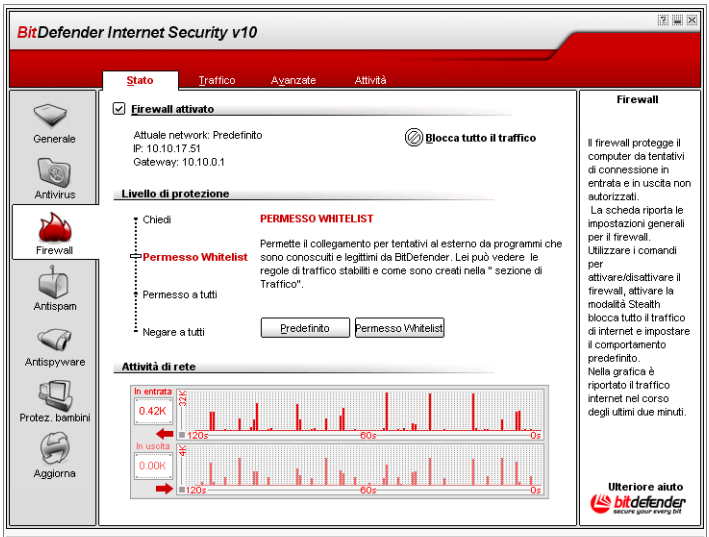
Se non volete apportare modifiche, cliccare **Fine** per terminare la procedura guidata.

Potete rieseguire la procedura di configurazione Firewall in qualsiasi momento cliccando su **Riconfigura profiloe** dalla sezione Traffico.

Nota

Notate che se scegliete di riconfigurare il profilo tutte le regole del firewall del profilo attuale andranno perse.

8.2. Stato del Firewall



Stato del Firewall

In questa sezione potete abilitare/disabilitare il **Firewall**, bloccare tutto il traffico della rete/internet e configurare il comportamento predefinito sui nuovi eventi.

Importante

Per essere protetti contro gli attacchi via Internet, mantenere il **Firewall** abilitato.

Per bloccare tutto il traffico della rete/Internet, è sufficiente cliccare su **Blocca Traffico** e poi su **Sì** per confermare la vostra scelta. In questo modo isolerete il vostro computer da qualsiasi altro computer nella rete.

Per bloccare tutto il traffico più recente, cliccare semplicemente su **Blocca Traffico**.

Nel lato inferiore della sezione potete vedere le statistiche BitDefender a proposito del traffico in arrivo e in uscita. Il grafico mostra il volume del traffico internet degli ultimi due minuti.

Nota

Il grafico appare anche se il **Firewall** è disabilitato.

8.2.1. Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 4 livelli di protezione:

Livello di protezione	Descrizione
Rifiuta tutto	Rifiuta tentativi di traffico non corrispondenti a una qualunque delle regole correnti senza solledcito. Utilizzate questa politica se avete già stabilito questa regola per tutti i programmi e le connessioni di cui avete bisogno.
Consenti tutto	Consente tentativi di traffico che non corrispondono a una qualunque delle regole correnti senza sollecito. Questa politica è fortemente sconsigliata, ma potrebbe essere utile per gli amministratori di rete.
Consenti Tutta la Whitelist	Consente tutti i tentativi di connessione in uscita dai programmi conosciuti come legittimi da BitDefender. Potete vedere le regole di traffico così come sono create nella sezione Traffico. I programmi inclusi nella Whitelist sono le applicazioni più comunemente utilizzate al mondo. Includono i browser più conosciuti, riproduttori audio&video, programmi di chat e condivisione file, così come applicazioni client server e di sistema operativo.
Chiedi	Chiedere se il traffico non corrisponde a una qualunque delle regole correnti di consenso.

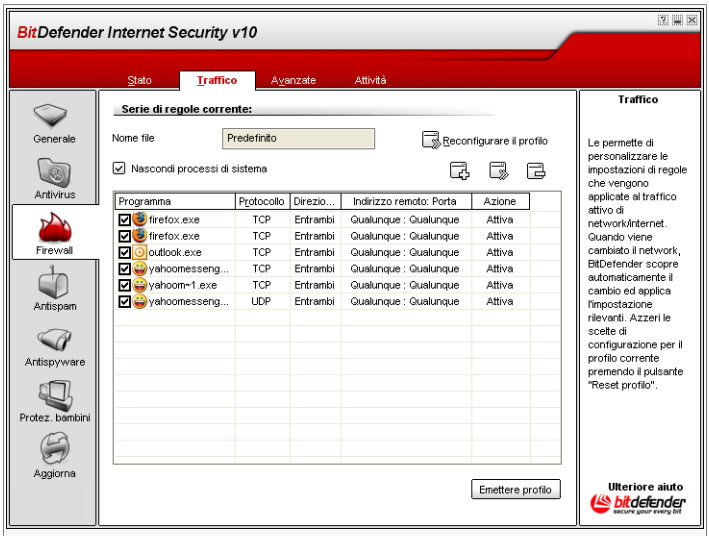
Importante

Se la console di gestione è chiusa e non è stata trovata una regola corrispondente per il nuovo evento, l' azione è **Negata**.

Cliccare **Livello Predefinito** per impostare la politica predefinita (**Consenti tutta la Whitelist**).

Se volete vedere quali programmi sono nella Whitlist, cliccare **Mostra Whitelist**.

8.3. Controllo del Traffico



Controllo del Traffico

In questa sezione potete specificare quali connessioni in arrivo o uscita consentire o negare, creando regole con protocolli specifici, porte, applicazioni e/o indirizzi remoti.

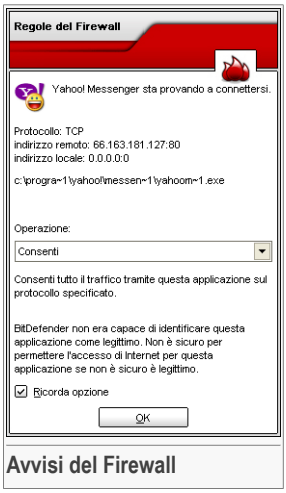
Selezionare la casella di controllo corrispondente a **Nascondere i processi di sistema** per nascondere le regole riguardanti i processi di sistema o BitDefender.

Le regole possono essere immesse automaticamente (attraverso la finestra di avviso) oppure manualmente (selezionando **Aggiungi** e scegliendo i parametri per la la regola).

8.3.1. Aggiungere Regole Automaticamente

Le regole sono aggiunte alla lista quando rispondete alle domande di BitDefender su un nuovo programma che prova ad accedere ad Internet.

Con il **Firewall** abilitato, BitDefender chiederà il vostro consenso ogni volta che viene eseguita una connessione a Internet:



Avvisi del Firewall

Potete vedere quanto segue: l'applicazione che sta provando ad accedere ad Internet, il protocollo, l'indirizzo IP e la porta sulla quale l'applicazione sta provando a connettersi.

Controllare l'opzione **Ricorda opzione**, selezionare l'azione desiderata dal menu a tendina **Azione** e cliccare **OK** e una regola sarà creata, applicata e inserita nell'elenco delle regole. In questo modo non sarete più avvisati quando il processo si ripeterà.

E' possibile selezionare una delle seguenti azioni:

Azione	Descrizione
Consenti	Consenti tutto il traffico da questa applicazione sul protocollo specifico.
Impedisci	Blocca tutto il traffico da questa applicazione sul protocollo specifico.
Consentire tutto il traffico da questa applicazione	Consentire tutto il traffico da questa applicazione su tutti i protocolli del IP.
Impedire tutto il traffico da questa applicazione	Bloccare tutto il traffico da questa applicazione su tutti i protocolli IP.
Consentire soltanto questo host remoto	Consentire il traffico da questa applicazione sul protocollo specifico con l'host remoto specificato.
Consentire solo questa porta	Consentire il traffico da questa applicazione sul protocollo specifico sulla porta specificata per qualsiasi destinazione.
Negare solo questo host remoto	Bloccare il traffico da questa applicazione sul protocollo specifico con l'host remoto specificato.

Azione	Descrizione
Negare solo questo porta	Bloccare il traffico da questa applicazione sul protocollo specifico sulla porta specificata per qualsiasi destinazione.

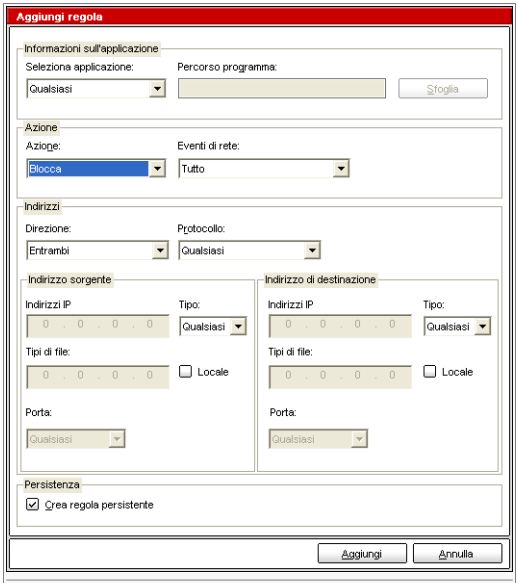
Importante

Autorizza tentativi di connessioni interne solo da IP's o domini dei quali vi fidate.

Si può accedere a ogni regola che è stata memorizzata nella sezione di **Traffico** per ulteriore modifica/aggiustamento.

8.3.2. Aggiungere Regole Manualmente

Per aggiungere una regola, selezionare **Aggiungi Regola** e scegliere i parametri. Appare la seguente finestra:



Selezionare Parametri

Potete impostare i parametri:

- **Applicazione** - selezionare l' applicazione per la regola. Potete scegliere solo una applicazione (dal menu a tendina **Selezione applicazione** selezionare **Percorso/Nome del File**, quindi fare un click su **Cerca** e selezionare l' applicazione) oppure tutte le applicazioni (dal menu a tendina **Selezione applicazione** selezionare **Qualsiasi**).
- **Azione** - seleziona l'azione della regola e il corrispondente evento(i).

Azione	Descrizione
Consenti	L'azione sarà permessa.
Impedisci	L'azione sarà negata.

- **Indirizzi** - seleziona la direzione del traffico e il protocollo per le regola.

  Direzione - seleziona la direzione del traffico.

Tipo	Descrizione
In Uscita	La regola è applicata solo al traffico in uscita.
In Entrata	La regola è applicata solo al traffico in entrata.
Entrambe	La regola sarà applicata in entrambe le direzioni.

Tipo Protocollo - seleziona uno dei protocolli ICMP, TCP, UDP, IGMP, SMP o uno qualunque.

E' disponibile una lista con i protocolli più comuni, per aiutarvi a selezionarne uno specifico. Selezionare il protocollo desiderato (sul quale si applica la regola) dal corrispondente menu a tendina o selezionare **Qualsiasi** per tutti i protocolli.

Protocollo	Descrizione
ICMP	Internet Control Message Protocol – è una estensione a Internet Protocol (IP). ICMP supporta pacchetti contenenti errori, controlli, e messaggi di informazione. Il comando PING, ad esempio, utilizza ICMP per testare una connessione Internet.
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 le garanzie che questi pacchetti saranno consegnati nello stesso ordine in cui sono stati inviati.

Protocollo	Descrizione
UDP	User Datagram Protocol – UDP è un IP progettato per elevate prestazioni. I giochi e altre applicazioni video utilizzano spesso UDP.

- **Indirizzi Sorgente** - digitare gli indirizzi IP, la maschera oppure controllare **Locale** se la regola si applica al computer locale. Se avete selezionato TCP o UDP come protocollo, potete impostare una porta specifica oppure un campo tra 0 e 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.
- **Indirizzi Destinazione** - digitare gli indirizzi IP, la maschera oppure controllare **Locale** se la destinazione della regola è il computer locale. Se avete selezionato TCP o UDP come protocollo potete impostare una porta specifica o un campo tra 0 and 65535. Se volete la regola applicata per tutte le porte, selezionare **Qualsiasi**.
- **Permanente** - selezionare la casella corrispondente a **Creare Regola Permanente** per salvare la regola per una futura "sessione". Se questa opzione non è selezionata alla fine di questa sessione la regola sarà cancellata (al riavvio del computer o all' aggiornamento di BitDefender).

Selezionare **Aggiungere**.

8.3.3. Amministrazione delle regole

Le regole sono elencate in ordine di importanza partendo dalla prima, che ha la priorità più alta. Per modificare la priorità delle regole, spostandole in alto o in basso, selezionare **Edita profilo** per visualizzare **Vista Dettagliata** dove eseguire le modifiche.

Per eliminare una regola è sufficiente selezionare **Cancella Regola**. Per modificare una regola, selezionarla e eseguire un click sul bottone **Edita Regola** oppure fare un doppio click su questa. Per disattivare temporaneamente una regola senza cancellarla, togliere la spunta nella casella corrispondente.

Nota

E' inoltre disponibile un menu contestuale che contiene le seguenti opzioni: **Aggiungi Regola**, **Elimina Regola** e **Edita Regola**.

8.3.4. Modifica dei Profili

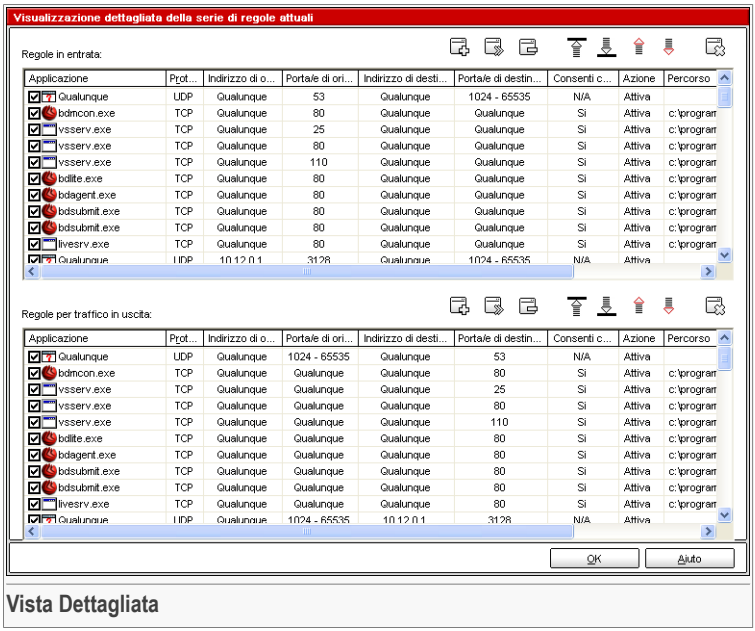
Prima di abilitare il modulo Firewall vi sarà chiesto di completare una procedura guidata per creare un nuovo profilo di rete. La procedura guidata vi aiuta a creare e impostare un set di regole di base per il firewall, necessarie per le applicazioni più comunemente

utilizzate. Cliccare su **Riconfigura Profilo** per eseguire nuovamente la procedura guidata e riconfigurare il profilo.

Importante

Tutte le regole che avete aggiunto in questa sezione andranno perse se scegliete di riconfigurare il profilo di rete.

Potete modificare un profilo facendo un click su **Editare profilo**. Comparirà la seguente finestra:



Vista Dettagliata

Le regole sono divise in 2 sezioni: regole in entrata e regole in uscita. Potete vedere l'applicazione e i parametri delle regole di ciascuna regola (indirizzo sorgente, indirizzo destinatario, porte sorgenti, porte di destinazione, azione, ecc).

Per cancellare una regola è sufficiente selezionarla e fare un click sul bottone **Cancella Regola**. Per cancellare tutte le regole fare un click sul bottone **Pulisci Elenco**. Per modificare una regola, selezionarla e fare un click sul bottone **Edita Regola** oppure eseguire un doppio click su questa. Per disattivare temporaneamente una regola senza cancellarla, togliere la spunta dalla casella corrispondente.

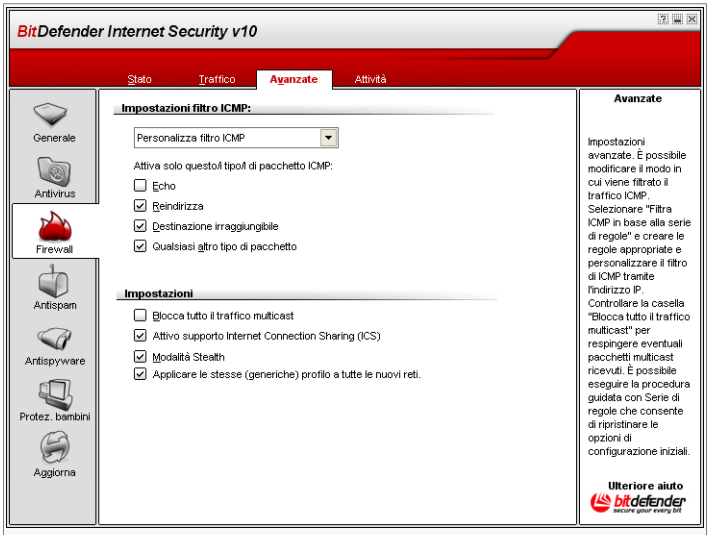
Potete alzare o abbassare la priorità di una regola. Fare un clck sul bottone **Sposta in alto** per alzare la priorità della regola selezionata di un livello, oppure fare un click sul bottone **Sposta in basso** per abbassare la priorità della regola selezionata, di un livello.

Nota

E' inoltre disponibile un menu contestuale che contiene le seguenti opzioni: **Aggiungi Regola**, **Edita Regola**, **Elimina Regola**, **Sposta in alto**, **Sposta in basso** e **Pulisci Lista**.

Fare un Click su **OK** per tornare alla console di gestione.

8.4. Impostazioni Avanzate



Impostazioni Avanzate

In questa sezione potete configurare le impostazioni avanzate del firewall BitDefeder. Le impostazioni avanzate vi consentono di specificare le regole di filtraggio per il traffico ICMP (Impostazioni Filtro ICMP) e di bloccare il traffico a trasmissioni multiple, di sondividere la vostra connessione Internet o di rendere il vsotro computer invisibile a software maligno e a hacker (Settings).

8.4.1. Impostazione Filtri ICMP

Dal menu, potete selezionare una delle seguenti politiche per filtrare il traffico ICMP:

- **Consentire tutto il traffico ICMP** - consente tutto il traffico ICMP.
- **Bloccare tutto il traffico ICMP** - blocca tutto il traffico ICMP.
- **Personalizza il filtraggio ICMP** - personalizza il modo in cui il traffico ICMP è filtrato. Sarete in grado di configurare le seguente opzioni:

Opzione	Descrizione
Echo	Questa opzione consente l'Echo Replay e i messaggi Echo Request. L'Echo Requeset è un messaggio ICMP che invia un pacchetto di dati all'host e si aspetta che questi dati siano rispediti in un Echo Replay. L'host deve rispondere a tutti gli Echo Requests con un Echo Replay contenente i dati esatti, ricevuti nel messaggio request. L'Echo Replay è un messaggio ICMP generato in risposta al messaggio ICMP Echo Request, ed è obbligatorio per tutti gli hosts e routers.
Redirect	Questo è un messaggio ICMP che informa un host, per indirizzare le sue informazioni routing (a inviare pacchetti su una via alternativa). Se l'host prova a inviare dati attraverso un router (R1) e quindi un altro router (R2) per raggiungere l'host e un percorso diretto dall'host a R2 è valido, una nuova direzione vi informerà l'host di tale route. Il router invierà ancora il datagram originale alla destinazione destinata. Tuttavia, se il datagram contiene informazioni routing, questo messaggio non sarà inviato , anche se è disponibile un'instadamento migliore.
Destinazione Irraggiungibile	Questo è un messaggio ICMP generato dal router per informare il client che l'host di destinazione è irraggiungibile, a meno che il datagram non abbia un indirizzo a diffusione multipla. Tra le ragioni che provocano il messaggio vi sono la mancanza del collegamento fisico all'host (la distanza è infinita), il protocollo o la porta indicata non sono attivi, o i dati

Opzione	Descrizione
	devono essere frammentati ma l'indicatore " non frammentate" è attivo.
Qualsiasi altro tipo di pacchetto	Con questa opzione abilitata , qualsiasi altro pacchetto di **Echo**, **Destinazione Irraggiungibile** o **Reindirizzazione**passerà.

- **Applica il set di regole corrente per ICMP** - applca al traffico ICMP le impostazioni correnti stabilite nella sezione Stato del modulo **Firewall**.

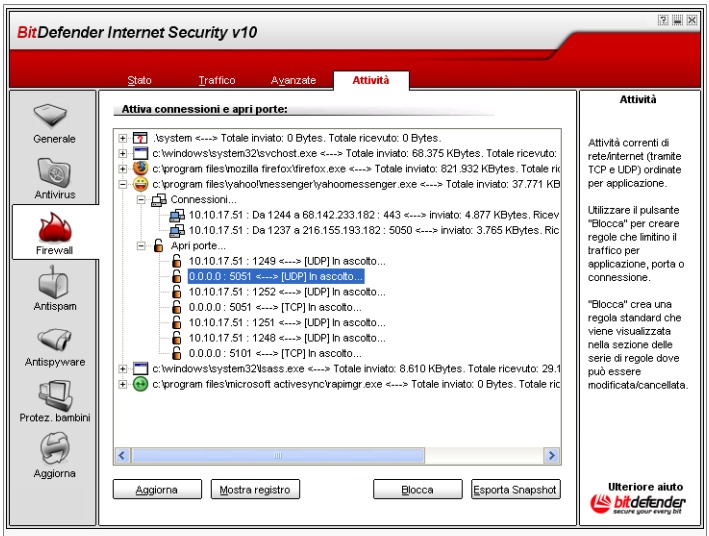
8.4.2. Impostazioni

Sono disponibili le seguenti impostazioni avanzate del firewall:

Opzione	Descrizione
Bloccare tutto il traffico multicast	Rilascia qualsiasi pacchetto multicast ricevuto. Il traffico Multicast è il tipo di traffico che si indirizza ad un gruppo particolare in una rete. I pacchetti sono inviati ad indirizzi speciali da cui il client multicast può riceverli se accetta di farlo. Ad esempio, un membro di una rete che possiede un sintonizzatore TV può trasmettere (inviare ad ogni membro della rete) o inviare in multicast (inviare ad un indirizzo speciale) il flusso video. I computer che ascoltano l'indirizzo multicast possono accettare o rifiutare il pacchetto. Se accettato, il flusso video può essere visto dai client multicast. Quantità eccessive di traffico multicast consumano banda e risorse. Con questa opzione abilitata qualsiasi pacchetto multicast ricevuto sarà rilasciato. Comunque, non si raccomanda di selezionare questa opzione.
Abilita il supporto Condivisione Connessione Internet(ICS)	Abilita il supporto per la Condivisione Connessione Internet (ICS). Questa opzione non abilita automaticamente ICS sul vostro sistema, ma consente solo questo tipo di connessione nel caso voi la abilitiate dal vostro sistema operativo.

Opzione	Descrizione
	La COndivisione Connessione Internet (ICS) abilita i membri delle reti locali a collegarsi ad Internet attraverso il vostro computer. Ciò è utile quando usufruite di una connessione Internet speciale/particolare (es. connessione wireless) e volete condividerla con gli altri membri della vostra rete. Condividere la vostra connessione Internet con i membri delle reti locali porta ad un livello di consumo risorse più alto e può comportare un certo rischio. Taglia anche alcune delle vostre porte (quelle aperte dai membri che stanno utilizzando la vostra connessione Internet).
Modalità Invisibile	Rende invisibile il vostro computer al software maligno e agli hacker. Individui malintenzionati o programmi software, non devono conoscere l'esistenza del vostro computer e tanto meno fornire servizi alla rete. L'opzione **Modalità Invisibile** impedirà alla vostra macchina di rispondere ai tentativi di scoprire quali porte sono aperte o dove sia esattamente nella rete. Un modo semplice di scoprire se il vostro computer può essere vulnerabile è collegarsi alle porte per vedere se vi è risposta. Ciò è chiamato portscan. BitDefender rileva e blocca automaticamente i portscan.
Applica lo stesso profilo (generico) a tutte le nuove reti	Applica il profilo generico, se esiste, a tutte le nuove reti rilevate da BitDefender. Non ha effetti di alcun tipo sulle reti per le quali avete specificato in precedenza un profilo di rete. Deselezionare questa opzione per eseguire la configurazione guidata del firewall quando BitDefender rileva una nuova rete. Il profilo generico è creato quando completate la configurazione guidata firewall, con l'opzione **Rendere questo profilo generico ed applicarlo a tutte le nuove reti** selezionato nel primo passo della configurazione guidata.

8.5. Controllo Connessione



Controllo Connessione

In questa sezione si può vedere l' attività della rete/internet corrente (su TCP e UDP) generata dall' applicazione. Inoltre da qui è possibile accedere al log del Firewall BitDefender.

Per creare regole che limitano il traffico dell'applicazione selezionata, porta o connessione, fare un click su **Blocca**.Vi sarà richiesto di confermare la vostra scelta. Si può accedere alla regola, per una ulteriore "messa a punto", nella sezione Traffico.

Utilizzare il pulsante **Ripristino** per riaprire la sezione **Attività** (per esaminare le ultime attività del modulo **Firewall**).

Fare un click su **Export Snapshot** per esportare la lista in un file `.txt`.

Per una lista più completa, vedere il file di registrazione degli eventi del Firewall BitDefender che può essere visualizzato facendo clic su **Visualizza eventi**. Il file è situato nella cartella Applicazioni Data dell'utente attuale Windows, sotto il percorso: `...\Aplication Data\ Bitdefender\Firewall\ log`.

9. Modulo Antispam

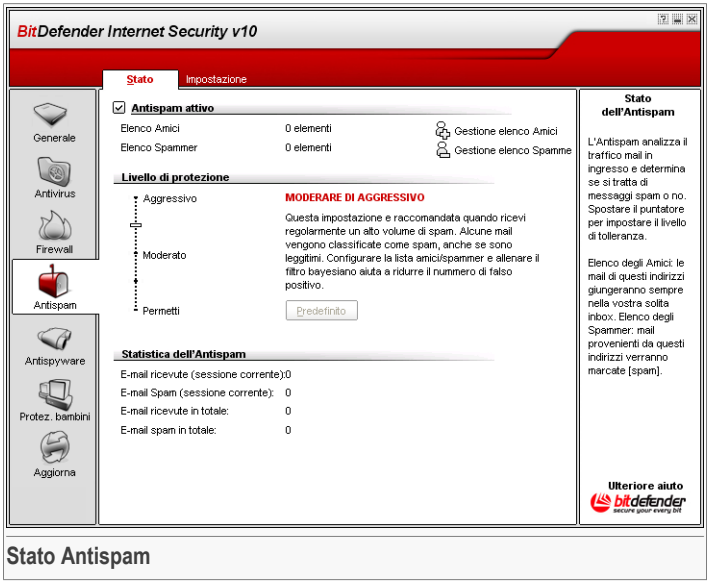
La sezione **Antispam** di questa guida all'utente comprende i seguenti argomenti:

- Stato Antispam
- Impostazioni Antispam
- Integrazione con Microsoft Outlook / Outlook Express / Windows Mail

Nota

Per ulteriori dettagli relativi al modulo **Antispam** vedere la descrizione del «*Modulo Antispam*» (p. 28).

9.1. Stato Antispam



Stato Antispam

In questa sezione potete configurare il modulo **Antispam** e visionare le informazioni relative alla sua attività.

Importante
Per impedire che lo Spam entri nella vostra **Inbox**, mantenere abilitato il **Filtro Antispam**.

Nella sezione **Statistiche** è possibile visionare i risultati della attivita dell' Antispam presentati per sessione (da quando avete avviato il vostro compiuter), oppure un riassunto (dalla installazione del BitDefender).

Per configurare il modulo **Antispam** è necessario procedere come segue:

9.1.1. Compilare l' Elenco degli Indirizzi

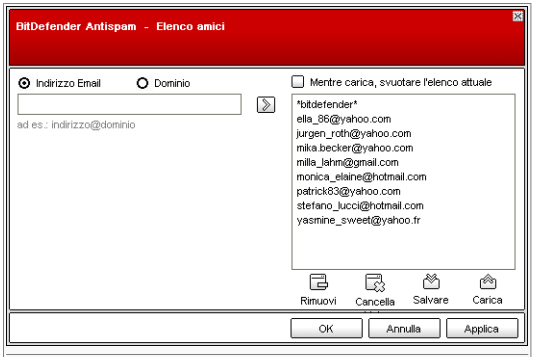
Gli elenchi degli indirizzi contengono informazioni riguardanti gli indirizzi e-mail che vi inviano mail lecite o spam.

Elenco Amici

L'**Elenco Amici** è una lista di tutti gli indirizzi email dai quali volete sempre ricevere messaggi, indipendentemente dal loro contenuto. I messaggi provenienti dai vostri amici non verranno etichettati come spam, anche se il loro contenuto potrebbe assomigliare allo spam.

Nota
Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà auotomaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.

Per gestire l' **Elenco Amici** fare un click su (corrispondente all' **Elenco Amici**) o selezionare il bottone **Amici** dalla barra degli strumenti Antispam.



Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se desiderate aggiungere un indirizzo email, selezionate l' opzione **Indirizzo Email**, digitate l'indirizzo e premete il pulsante . L'indirizzo apparirà sull'**Elenco Amici**.

Importante

Sintassi: <name@domain.com>.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare dominio e premere il pulsante . Il dominio apparirà sull'**Elenco Amici**.

Importante

Sintassi:

- <@domain.com>, <*domain.com> e <domain.com> - tutte le mail provenienti da <domain.com> raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- <*domain*> - tutte le mail provenienti da <domain> (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- <*com> - tutte le mail con il suffisso di dominio <com> raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Amici** nella posizione desiderata. Il file avrà l'estensione .bwl.

Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; inoltre aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Selezionare **Applica** e **OK** per salvare e chiudere **l'Elenco Amici**.

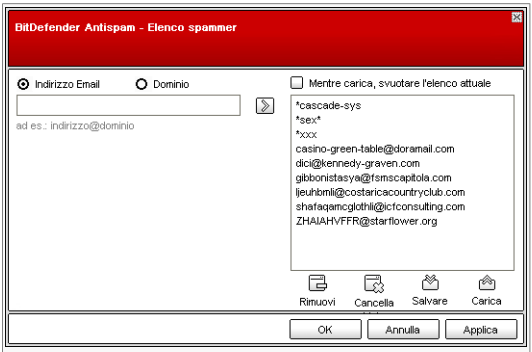
Elenco Spammers

L'**Elenco Spammers** è l'elenco di tutti gli indirizzi e-mail dai quali non volete ricevere messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail ricevuta da un indirizzo contenuto nell'**Elenco Spammers** sarà automaticamente marcato come SPAM, senza alcun ulteriore processo.

Per gestire l'**Elenco Spammers** selezionare >>> (in corrispondenza dell'**Elenco Spammers**) oppure premere il pulsante **Spammers** posizionato nella «*Barra degli Strumenti Antispam*» (p. 113).



Elenco Spammers

Qui potete aggiungere o rimuovere elementi dall'**Elenco Spammers**.

Se desiderate aggiungere un indirizzo email, selezionare il campo **Indirizzo Email**, inserire l'indirizzo e premere il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante

Sintassi: <name@domain.com>.

Se volete aggiungere un dominio, selezionare l'opzione **Dominio**, digitare il nome e fare un click su . Il dominio apparirà nell'**Elenco Spammers**.

Importante

Sintassi:

- <@domain.com>, <*domain.com> e <domain.com> - tutte le mail provenienti da <domain.com> saranno marcate come SPAM;
- <*domain*> - tutte le mail provenienti da <domain> (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- <*com> - tutte le mail ricevute con il suffisso di dominio <com> verranno marcate come Spam.

Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Spammers** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Selezionare **Appica** e **OK** per salvare e chiudere l' **Elenco Spammers**.

Importante

Se si desidera re-installare BitDefender, consigliamo di fare un salvataggio degli elenchi **Amici** / **Spammers** e quindi ricaricarli al termine del processo di re-installazione.

9.1.2. Impostazione del Livello di Tolleranza

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

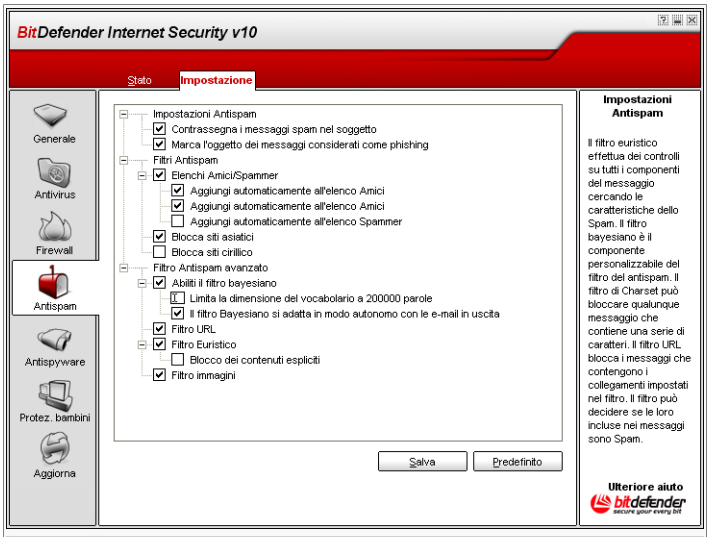
Ci sono 5 livelli di tolleranza:

Livello di tolleranza	Descrizione
Tollerante	Offre protezione per gli account che ricevono molta posta commerciale legittima. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Tra Tollerante e Moderato	Offre protezione per account che ricevono alcune mail commerciali legittime. Il filtro lasciare passare la maggior parte delle e-mail, ma potrebbe produrre dei falsi negativi (spam classificato come mail legittime).
Moderata	Offre protezione per account normali. Il filtro bloccherà la maggior parte dello spam, evitando al contempo i falsi positivi.
Da Moderata ad Aggressiva	Offre protezione per gli account che ricevono regolarmente ampi volumi di spam.

Livello di tolleranza	Descrizione
	Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Configura gli **Elenchi Amici/Spammer** e addestra il **Motore di Apprendimento (Bayesiano)** per ridurre il numero di falsi positivi.
Aggressiva	Offre protezione per gli account che ricevono regolarmente volumi di spam molto ampi. Il filtro lascerà passare pochissimo spam, ma potrebbe produrre dei falsi positivi (mail legittime etichettate erroneamente come spam). Aggiungete i vostri contatti alla **Lista Amici** per ridurre il numero di falsi positivi.

Per impostare il livello di protezine di default (**Da Moderata ad Aggressiva**) cliccare su **Livello di Default**.

9.2. Impostazioni Antispam



Impostazioni Antispam

Qui potete abilitare/disabilitare ciascuno dei filtri Antispam e inoltre è possibile specificare alcune regolazioni relativa al modulo di Antispam.

Sono disponibili tre categorie di opzioni (**Impostazioni Antispam**, **Filtri Antispam** and **Filtri Avanzati Antispam**) organizzati come menu espandibili, simili a quelli di Windows.

Nota

Selezionare la casella con "+" per aprire una categoria oppure una casella con "-" per chiudere una categoria.

9.2.1. Impostazioni Antispam

- **Contrassegna i messagi spam nell' oggetto** - tutti i messaggi email considerati come Spam saranno etichettati come SPAM nell' oggetto.
- **Marca l'oggetto dei messagi considerati phishing** - tutte le mail considerate messaggi di phishing saranno etichettate come SPAM sulla linea dell' oggetto.

9.2.2. Filtri Antispam

- **Elenchi Amici/Spammers** - attiva/disattiva gli Elenchi Amici/Spammers;
  - **Aggiungi automaticamente all'elenco degli Amici** - aggiunge automaticamente i mittenti all'**Elenco Amici**.
  - **Aggiungi Automaticamente all'Elenco Amici** - quando verrà premuto il pulsante **No Spam** dalla Barra degli strumenti Antispam il mittente verrà aggiunto automaticamente all' **Elenco Amici**.
  - **Aggiungi automaticamente all'elenco Spammer** - la prossima volta che si preme il pulsante **Spam** dalla «*Barra degli Strumenti Antispam*» (p. 113) il mittente sarà automaticamente aggiunto all'**Elenco Spammers**.

Nota

I pulsanti **No spam** e **Spam** sono utilizzati per "istruire" il filtro Bayesiano.

- **Blocca Asian** - blocca i messaggi scritti in Caratteri Asiatici.
- **Blocca Cyrillic** - blocca i messaggi scritti in Caratteri Cirillici.

9.2.3. Filtri Avanzati Antispam

- **Abilita il motore di Apprendimento (bayesiano)** - attiva/disattiva il Motore di Apprendimento (bayesiano).
  - **Limita la dimensione del dizionario a 200000 parole** - con questa opzione impostate la dimensione del dizionario Bayesiano – se minore è più veloce, se maggiore è più accurato.

Nota

La dimensione consigliata è: 200.000 parole.

  - **Istruisci il Motore di Apprendimento (bayesiano) per le e-mails in uscita** - istruisce il Motore di Apprendimento (bayesiano) per le e-mails in uscita.
- **Filtro URL** - attiva/disattiva il Filtro URL;
- **Filtro Euristico** - attiva/disattiva il Filtro Euristico;
  - **Blocco dei contenuti espliciti** - attiva/disattiva la scansione di messaggi "SESSUALMENTE ESPLICIT" nell'oggetto;
- **Filtro Immagini** - attiva/disattiva il Filtro Immagini.

Nota

Per attivare/disattivare una opzione, selezionare/pulire il checkbox corrispondente.

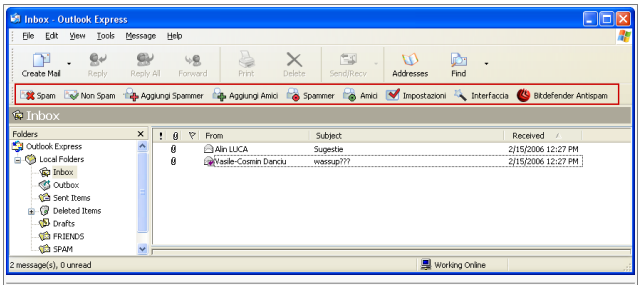
Selezionare **Applica** per salvare le modifiche oppure **Preimpostazione** per tornare alle impostazioni di default.

9.3. Integrazione con Microsoft Outlook / Outlook Express / Windows Mail

BitDefender si integra direttamente con Microsoft Outlook/Outlook Express / Windows Mail con una barra degli strumenti intuitiva e di facile uso.

9.3.1. Barra degli Strumenti Antispam

Nella parte superiore di Microsoft Outlook/Outlook Express/Windows Mail potete vedere la Barra degli Strumenti Antispam.



Barra degli Strumenti Antispam

Importante

La differenza tra BitDefender Antispam per Microsoft Outlook o Outlook Express/Windows mail consiste nel fatto che i messaggi SPAM sono spostati nella cartella **Spam** per Microsoft Outlook mentre per Outlook Express/Windows Mail sono spostati nella cartella **Elementi Cancellati**. In entrambi i casi i messaggi vengono etichettati come SPAM nella riga dell'oggetto.

La cartella **Spam** è creata automaticamente da BitDefender in Microsoft Outlook e viene inserita nel medesimo livello degli elementi dall' **Elenco Cartella**(Calendario, Contatti, ecc.)

Di seguito la spiegazione dei pulsanti nella barra degli strumenti BitDefender:

- **E' spam** - invia un messaggio al modulo Bayesiano indicando che la e-mail selezionata è spam. L'e-mail sarà marcata come SPAM e verrà spostata nella cartella **Spam**.

  I futuri messaggi e-mail con le stesse caratteristiche verranno marcati come SPAM.

  Nota
  E' possibile selezionare uno o più messaggi e-mail.

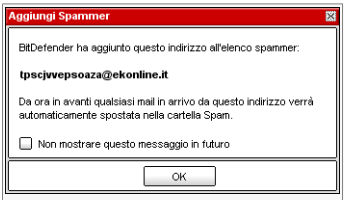
- **Non spam** - invia un messaggio al modulo Bayesiano indicando che la e-mail selezionata non è spam. BitDefender non dovrebbe classificarla. L'e-mail sarà spostata dalla cartella **Spam** alla directory **Inbox**.

  I futuri messaggi e-mail con le stesse caratteristiche non verranno marcati come SPAM.

  Nota
  E' possibile selezionare uno o più messaggi e-mail.

  Importante
  Il pulsante **Non 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 della e-mail selezionata all' **Elenco Spammers**.



Aggiungi Spammer

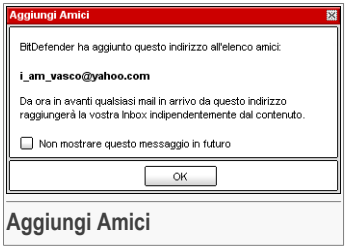
Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando un indirizzo spammer viene aggiunto all'elenco.

Selezionare **OK** per chiudere la finestra.

Le future e-mail provenienti da quell' indirizzo saranno marcate come SPAM.

Nota
E' possibile selezionare uno o più mittenti.

- **Aggiungi Amici** - aggiunge il mittente della e-mail selezionata all' **Elenco Amici**.



Aggiungi Amici

Selezionare **Non mostrare questo messaggio in futuro** se non si desidera la richiesta di conferma quando si aggiunge un indirizzo all'elenco.

Selezionare **OK** per chiudere la finestra.

Riceverete sempre le email provenienti da questo indirizzo, indipendentemente dal contenuto del messaggio.

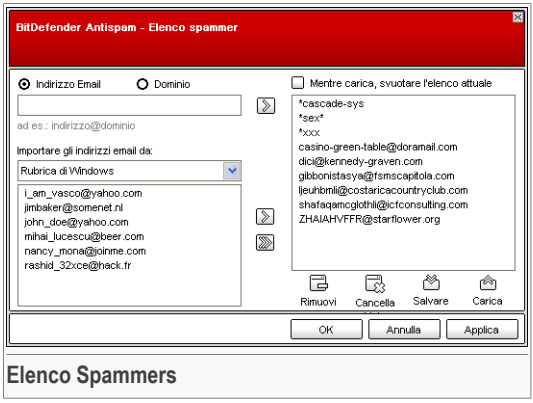
Nota

E' possibile selezionare uno o più mittenti.

- **Spammers** - apre **l'Elenco Spammers** che contiene tutte gli indirizzi e-mail dai quali non si vogliono ricevere messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail ricevuta da un indirizzo contenuto nell'**Elenco Spammers** sarà automaticamente marcato come SPAM, senza alcun ulteriore processo.



Elenco Spammers

Qui potete aggiungere o rimuovere elementi dall'**Elenco Spammers**.

Se si desidera aggiungere un indirizzo email, spuntare l' opzione **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante
Sintassi: <name@domain.com>.

Se desiderate aggiungere un dominio, selezionare il campo **Dominio**, introdurre il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Spammers**.

Importante
Sintassi:

- <@domain.com>, <*domain.com> e <domain.com> - tutte le mail provenienti da <domain.com> saranno marcate come SPAM;
- <*domain*> - tutte le mail provenienti da <domain> (indipendentemente dai suffissi del dominio) verranno marcate come Spam;
- <*com> - tutte le mail ricevute con il suffisso di dominio <com> verranno marcate come Spam.

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina**Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express / Windows Mail** apparirà una nuova finestra dove potete selezionare la cartella che contiene gli indirizzi mail che volete aggiungere all'**Elenco Spammer**. Sceglieteli e cliccate su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare click su per aggiungerli all'**Elenco Spammers**. Facendo click su tutti gli indirizzi verranno aggiunti all' elenco.

Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Spammers** nella posizione desiderata. Il file avrà l'estensione .bwl.

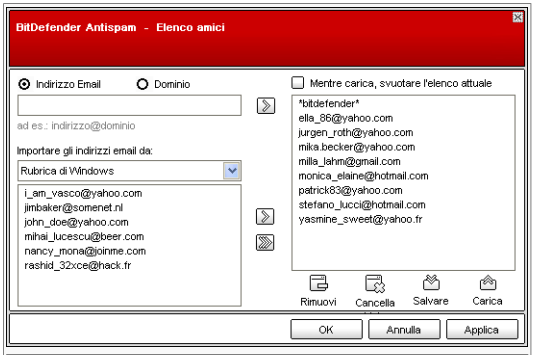
Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Selezionare **Appica** e **OK** per salvare e chiudere l' **Elenco Spammers**.

- **Amici** - apre l'**Elenco Amici** che contiene tutti gli indirizzi e-mail dai quali volete sempre ricevere i messaggi, indipendentemente dal loro contenuto.

Nota

Qualsiasi mail in arrivo da un indirizzo contenuto nella lista **Elenco Amici**, sarà auotomaticamente consegnato alla vostra Inbox senza alcun ulteriore processo.



Elenco Amici

Qui potrete aggiungere o rimuovere elementi dall'**Elenco Amici**.

Se si desidera aggiungere un indirizzo email, spuntare il campo **Indirizzo Email**, digitare l'indirizzo e selezionare il pulsante . L'indirizzo apparirà nell'**Elenco Spammers**.

Importante

Sintassi: `<name@domain.com>`.

Se desiderate aggiungere un dominio, selezionare l' opzione **Dominio**, digitare il nome e premere il pulsante . Il dominio apparirà nell'**Elenco Amici**.

Importante

Sintassi:

- `<@domain.com>`, `<*domain.com>` e `<domain.com>` - tutte le mail provenienti da `<domain.com>` raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- `<*domain*>` - tutte le mail provenienti da `<domain>` (non importa il suffisso del dominio) raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;
- `<*com>` - tutte le mail con il suffisso di dominio `<com>` raggiungeranno la vostra **Inbox** indipendentemente dal loro contenuto;

Per importare gli indirizzi e-mail da **Rubrica di Windows** / **Cartelle di Outlook Express** a **Microsoft Outlook** / **Outlook Express** / **Windows Mail** selezionare l'opzione appropriata dal menu a tendina**Importa indirizzi e-mail da**.

Per **Microsoft Outlook Express** apparirà una nuova finestra dove potrete selezionare la cartella che contiene gli indirizzi mail che vorrete aggiungere all'**Elenco Amici**. Sceglierli e cliccare su **Seleziona**.

In entrambi i casi gli indirizzi e-mail appariranno nella lista di importazione. Selezionare quelli desiderati e fare click su per aggiungerli all'**Elenco Amici**. Facendo click su tutti gli idirizzi verranno aggiunti all'elenco.

Per cancellare un elemento dalla lista, selezionarlo e cliccare il bottone **Rimuovi**. Se selezionate **Pulisci la Lista** cancellerete tutti gli elenti, ma notate che sarà impossibile recuperarli.

Utilizzare i pulsanti **Salva**/ **Carica** per salvare/caricare **l'Elenco Amici** nella posizione desiderata. Il file avrà l'estensione `.bwl`.

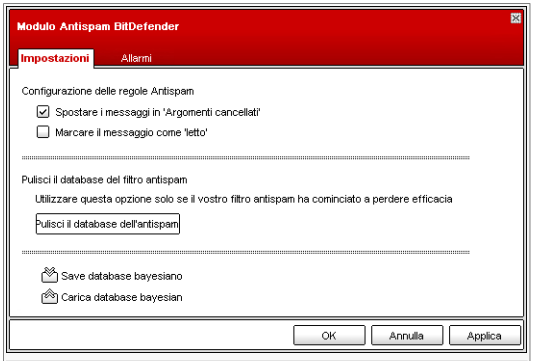
Per ripristinare il contenuto dell'elenco attuale quando caricate un elenco precedentemente salvato selezionate **Quando si carica, svuotare l'elenco attuale**.

Nota

Raccomandiamo di aggiungere i nomi dei vostri amici e gli indirizzi e-mail all'**Elenco Amici**. BitDefender non blocca i messaggi di coloro che sono nell'elenco; inoltre aggiungere amici aiuta a garantire che i messaggi leciti vengano recapitati.

Selezionare **Applica** e **OK** per salvare e chiudere **l'Elenco Amici**.

- **Impostazioni** - apre la finestra **Impostazioni** dove potete specificare alcune opzioni per il modulo **Antispam**.



Impostazioni

Sono disponibili le seguenti opzioni:

- **Sposta il messaggio in Elementi Cancellati** - sposta i messaggi spam nella cartella **Elementi Cancellati** (solo per Microsoft Outlook Express / Windows Mail);
- **Marcare il messaggio come letto** - marca tutti i messaggi spam come letti così da non essere disturbati quando arrivano nuovi messaggi spam.

Se il vostro filtro antispam è molto impreciso, può rendersi necessario pulire il database del filtro e istruire nuovamente il Filtro Bayesiano. Selezionare **Pulisci il database dell'antispam** per resettare il Database Bayesiano.

Utilizzare i tasti **Salva Database Bayesiano**/ **Carica Database Bayesiano** per salvare/caricare l'elenco del Database Bayesiano nell'ubicazione desiderata. Il file avrà l'estensione `.dat`.

Selezionare la tabella **Avvisi** se si desidera accedere alla sezione dove è possibile disattivare la comparsa della finestra di conferma per i pulsanti **Aggiungi spammer** e **Aggiungi amici**.

Nota

Nella finestra **Avvisi** potete anche abilitare / disabilitare la comparsa dell'avviso **Seleziona un messaggio e-mail**. Questo avviso compare quando selezionate un gruppo invece di un messaggio e-mail.

- **Interfaccia** - apre la Procedura guidata che vi guidera attraverso il processo di istruzione del Filtro Bayesiano, così da incrementare l' efficienza dell' Antispam di BitDefender. Potete inoltre aggiungere indirizzi dalla vostra **Rubrica** all' **Elenco Amici** / **Elenco Spammers**.
- **BitDefender Antispam** - apre la Console di Gestione.

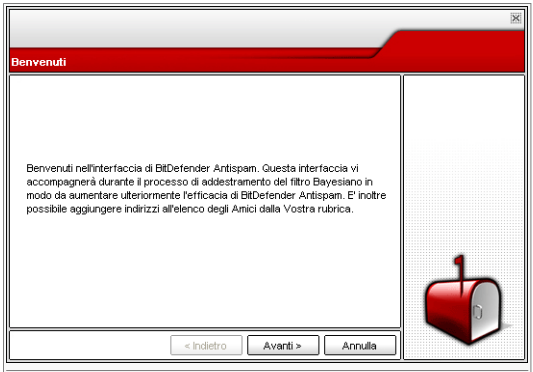
9.3.2. Procedura Guidata della Configurazione Antispam

La prima volta che lanciate Microsoft Outlook / Outlook Express / Windows Mail con BitDefender installato, apparirà la procedura guidata per aiutarvi a configurare l' Elenco Amici, l' Elenco Spammer e per addestrare il Filtro Bayesiano in modo da aumentare l' efficienza dei filtri Antispam.

Nota

La creazione guidata può essere lanciata quando vuoi, cliccando sul tasto **Interfaccia** nella «*Barra degli Strumenti Antispam*» (p. 113).

Passaggio 1/6 - Finestra di Benvenuto



Finestra di benvenuto

Selezionare **Avanti**.

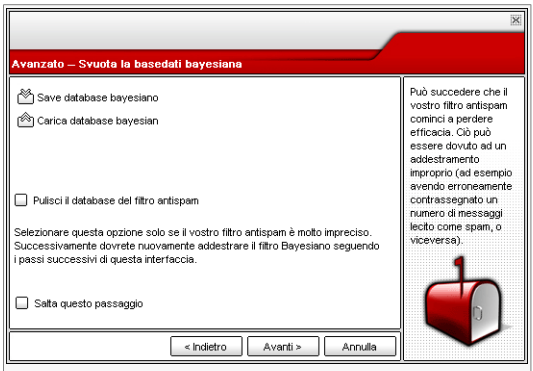
Passaggio 2/6 - Compilare l' Elenco Amici

Compilare l' Elenco Amici

Da qui è possibile vedere tutti gli indirizzi della vostra **Rubrica**. Selezionare quelli che si intende aggiungere all' **Elenco Amici** (suggeriamo di selezionarli tutti). Riceverete tutti i messaggi e-mail provenienti da questi indirizzi, indipendentemente dal loro contenuto.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passaggio 3/6 - Cancellare il Database Bayesiano



Cancellare il Database Bayesiano

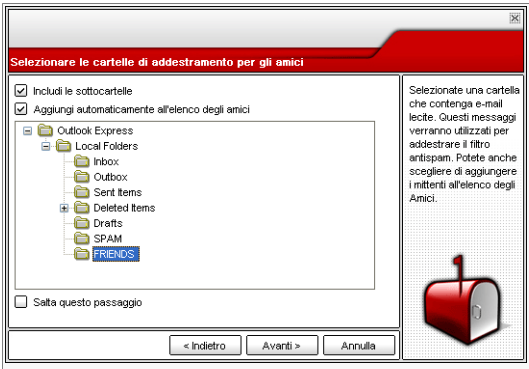
Potreste notare che il vostro Filtro Antispam ha iniziato a perdere efficienza. Questo potrebbe essere dovuto a una "istruzione" impropria. (per esempio nel caso in cui si sia erroneamente marcato un certo numero di messaggi legittimi come Spam o viceversa). Se il vostro filtro risulta molto inaccurato, potrebbe essere necessario pulire il database del filtro e istruirlo nuovamente, seguendo le fasi successive di questa procedura guidata.

Selezionare **Pulire il database del filtro antispam** se si desidera resettare il database Bayesiano.

Utilizzare i tasti **Salva database Bayesiano**/ **Carica database Bayesiano** per salvare / caricare il Database Bayesiano nell'ubicazione desiderata. Il file avrà l' estensione `.dat`.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passaggio 4/6 - Istruzione del Filtro Bayesiano con messaggi e-mail Leciti



Istruzione del Filtro Bayesiano con messaggi e-mail Leciti

Selezionare una cartella che contenga messaggi e-mail leciti. Questi messaggi verranno utilizzati per istruire il filtro Antispam.

Nella parte superiore della finestra sono disponibili 2 opzioni:

- **Includi sotto-cartelle** - per includere le sottocartelle alla vostra selezione;
- **Aggiungere automaticamente all'elenco degli amici** - per aggiungere i mittenti all'**Elenco Amici**.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passaggio 5/6 - Istruzione del Filtro Bayesiano con SPAM

Istruzione del Filtro Bayesiano con SPAM

Selezionare una cartella che contiene messaggi e-mail spam. Questi messaggi saranno utilizzati per istruire il filtro Antispam.

Importante

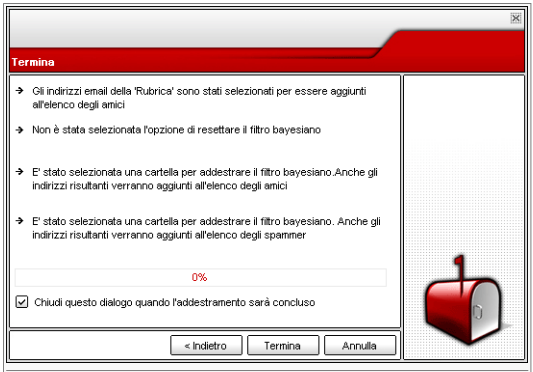
Assicurarsi che la cartella scelta contenga e-mail non lecite, altrimenti la prestazione antispam verrà ridotta considerevolmente.

Nella parte superiore della finestra sono disponibili 2 opzioni:

- **Includi sotto-cartelle** - per includere le sottocartelle alla vostra selezione;
- **Aggiungi automaticamente all'elenco degli spammers** - per aggiungere i mittenti all'**Elenco Spammers**.

Selezionare **Salta questo passaggio** se si desidera andare oltre. Selezionare **Indietro** per tornare al passaggio precedente oppure **Avanti** per continuare la procedura guidata.

Passo 6/6 – Sommario



Sommario

In questa finestra si possono vedere tutte le impostazioni della procedura guidata alla configurazione. Potrete eseguire qualsiasi modifica, tornando al passo precedente (selezionare **Indietro**).

Se non volete apportare alcuna modifica, selezionare **Fine** per terminare la procedura guidata di configurazione.

10. Modulo Antispyware

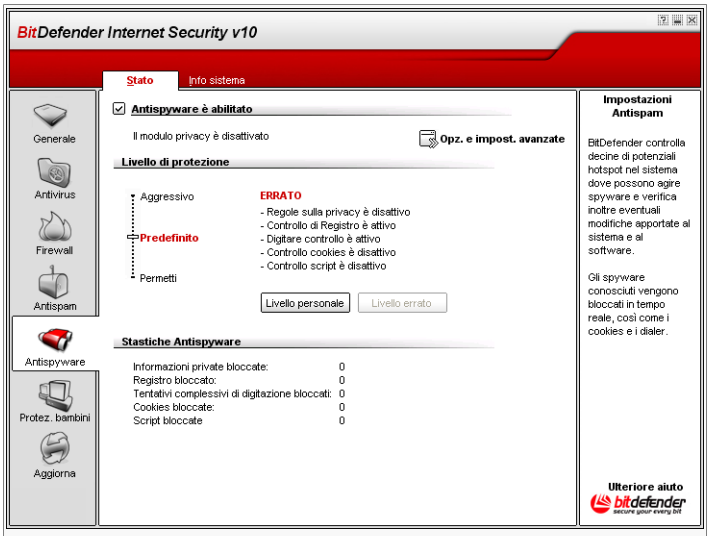
La sezione **Antispyware** di questa guida all' utente contiene i seguenti argomenti:

- Stato Antispyware
- Impostazioni Avanzate - Controllo della Privacy
- Impostazioni Avanzate - Controllo Registrazione
- Impostazioni Avanzate - Dial Control
- Impostazioni Avanzate - Controllo Cookie
- Impostazioni Avanzate - Script Control
- Informazioni di Sistema

Nota

Per maggiori dettagli relativi al modulo **Antispyware** controllare la descrizione del «*Modulo Antispyware*» (p. 32).

10.1. Stao Antispyware



Stao Antispyware

In questa sezione è possibile configurare il modulo **Behavioral Antispyware** e visionare le informazioni relative alla sua attività.

Importante

Per prevenire che gli spyware infettino il vostro computer, mantenere la **Behavioral Antispyware** abilitata.

Nel lato inferiore della sezione è possibile vedere le **Statistiche Antispyware**.

Il modulo **Antispyware** protegge il vostro computer contro gli spywares, attraverso 5 importanti controlli di protezione.

- Controllo Privacy - protegge i vostri dati riservati filtrando tutto il traffico HTTP e SMTP in uscita secondo le regole da voi create nella sezione Privacy.
- Il **Controllo dei Registri** sorveglia il Registro di Windows – azione utile per rilevare i Trojan (Cavalli di Troia). Verrete avvisati ogni volta che un programma tenterà di modificare una entrata del registro per poter essere eseguito all'avvio di Windows.

- IlControllo di Composizione - vi chiede il permesso ogni volta che un dialer tenta di accedere al modem del computer.
- Il **Controllo dei Cookie** quando è attivato, chiederà il vostro consenso ogni volta che un sito web tenterà di impostare un cookie.
- Il **Controllo degli Script** quando è attivato, chiederà il vostro consenso ogni volta che un sito web tenterà di attivare uno script o un altro contenuto attivo:

Per configurare le impostazioni per questi controlli, cliccare Impostazioni Avanzate.

10.1.1. Livello di Protezione

Potete scegliere il livello di protezione che meglio si adatta alle vostre necessità di sicurezza. Trascinate il pulsante sulla barra per impostare il livello di protezione appropriato.

Ci sono 3 livelli di protezione:

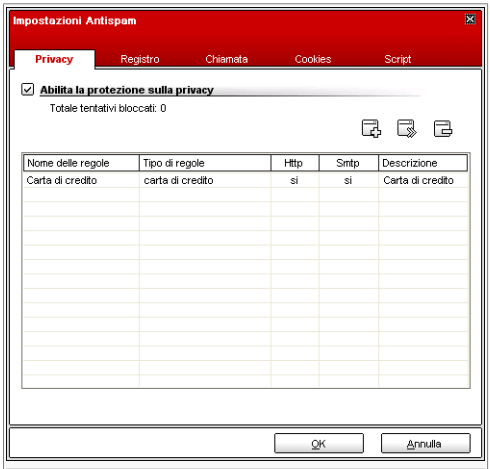
Livello di protezione	Descrizione
Permissiva	Solo il **Controllo di Registro** è abilitato.
Default	**Controllo di Registro** e **Dial Control** sono abilitati.
Aggressiva	**Controllo di Registro**, **Dial Control** and **Controllo della Privacy** sono abilitati.

Potete personalizzare il livello di protezione cliccando su **Personalizza livello**. Nella finestra che apparirà, selezionate i controlli Antispyware che volete abilitare e cliccate su **OK**.

Cliccando su **Predefinito** verranno applicate le impostazioni di default.

10.2. Impostazioni Avanzate - Controllo della Privacy

Per accedere a questa sezione, cliccare il bottone delle **Impostazioni Avanzate** dal modulo **Antispyware**, sezione Stato.



Controllo della Privacy

Tenere sicuri i dati riservati è una questione importante che ci preoccupa tutti. I furto di dati ha tenuto il passo con lo siluppo delle comunicazioni via Internet e fa uso di nuovi metodi per ingannare le persone inducendole a dare via informazioni private.

Che sia la vostra e-mail o il numero della vostra carta di credito, quando finiscono nelle mani sbagliate tali informazioni possono recarvi danno: potete trovarvi affogati nei messaggi di spam o potreste essere sorpresi nell'accedere ad un conto svuotato.

Il**Controllo Privacy** vi aiuta a tenere al sicuro i dati riservati. Esso scansiona il traffico HTTP o SMTP, o entrambi, alla ricerca di determinate stringhe che avete definito. Se viene trovata una corrispondenza, la pagina web o la e-mail corrispondente viene bloccata.

Le regole devono essere inserite manualmente(cliccando sul pulsante **Aggiungi** e scegliendo i parametri per le regole). Apparirà l'installazione guidata.

10.2.1. Installazione Guidata della Configurazione

La procedura di installazione guidata, comprende 3 passaggi.

Passaggio 1/3 - Impostazione Regola e Dati

Impostare il Tipo di Regola e i Dati

Inserire il nome della regola nel campo di editing.

Dovete impostare i parametri seguenti:

- **Tipo di Regola** - scegliere il tipo di regola (indirizzo, nome, carta di credito, PIN, SSN etc).
- **Dati della Regola** - inserire i dati della regola.

Tutti i dati che inserite sono criptati. Per una sicurezza maggiore, non inserire tutti i dati che volete proteggere.

Selezionare **Avanti**.

Passaggio 2/3 - Selezione del Traffico

Selezione del Traffico

Selezionare il traffico che si desidera esaminare con BitDefender. Sono disponibili le seguenti opzioni:

- **Indirizzi** - esamina il traffico HTTP (web) e blocca i dati in uscita corrispondenti ai dati della regola.
- **Scansione delle mail in uscita** - esamina il traffico SMTP (mail) e blocca le mail in uscita corrispondenti ai dati della regola.

Selezionare **Avanti**.

Passo 3/3 – Definizione Regola

Definizione Regola

Inserire una breve descrizione della regola nel campo di editing.

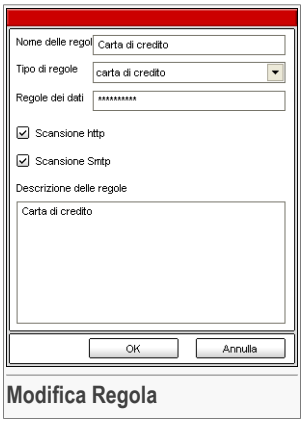
Selezionare **Termina**.

10.2.2. Gestione delle Regole

Potete vedere l'elenco delle regole sulla scheda.

Per cancellare un elemento dall'elenco, selezionarlo e premere il pulsante **Rimuovi**. Per disattivare temporaneamente una regola senza cancellalrla, disattivare la casella corrispondente.

Per editare una regola, selezionarla e cliccare sul pulsante di **Edit** oppure fare un doppio click. Apparirà una nuova finestra.



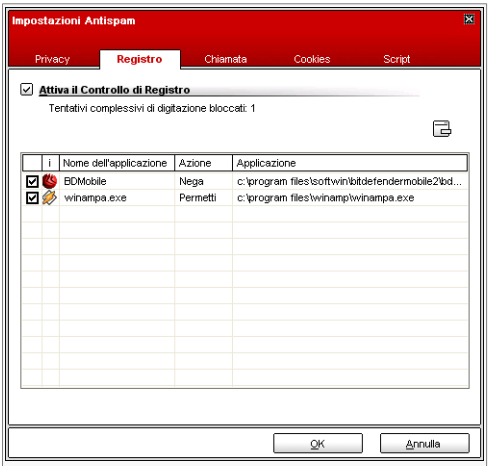
Modifica Regola

Qui potete modificare il nome, la definizione e i parametri della regola (tipo, dati e traffico). Cliccate su **OK** per salvare le modifiche.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

10.3. Impostazioni Avanzate - Controllo Registry

Per accedere a questa sezione, aprire la finestra **Impostazioni Avanzate Antispyware** (andare alla sezione Status nel modulo **Antispyware**, fare un clik su **Impostazioni Avanzate**) e fare un click nella scheda **Registry**.



Controllo Registry

Una componente molto importante del sistema operativo di Windows si chiama **Registry**. Qui è dove Windows tiene le informazioni relative alle proprie configurazioni, ai programmi installati, all'utente e così via.

Il **Registry** è inoltre utilizzato per definire quali Programmi devono essere eseguiti automaticamente all'avvio di Windows. Spesso i virus lo utilizzano per essere eseguiti automaticamente quando l'utente riavvia il proprio computer.

Il **Controllo del Registry** sorveglia il Registry di Windows – azione utile per rilevare i Trojan (Cavalli di Troia). Vi avviserà ogni volta che un programma tenterà di modificare una entrata del registry per poter essere eseguito all'avvio di Windows.

Allarme sul Registry

E' possibile vietare questa modifica selezionando **No** oppure consentirla selezionando **Sì**.

Se si desidera che BitDefender memorizzi questa risposta, si dovrà selezionare la casella: **Ricorda questa risposta**.

Nota

Le vostre risposte saranno la base dell'elenco delle regole.

Per cancellare una entrata al registro, è sufficiente selezionarla e fare click su **Cancella**. Per disattivare temporaneamente una entrata di registro senza però cancellarla, rimuovere la spunta dalla casella corrispondente.

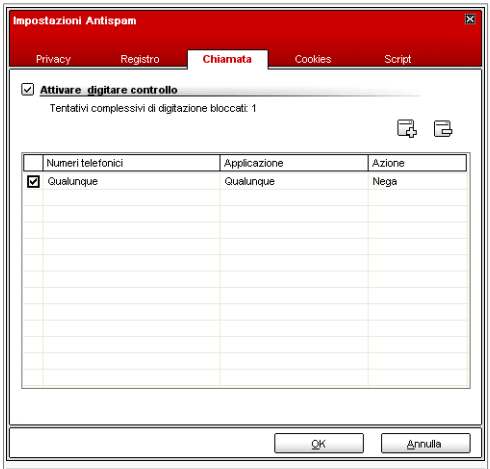
Nota

BitDefender vi allerterà quando installerete nuovi programmi che necessitano di esecuzione immediata dopo il successivo avvio del vostro computer. Nella maggior parte dei casi questi programmi sono leciti e ci si può fidare.

Selezionare **OK** per chiudere la finestra.

10.4. Impostazioni Avanzate - Controllo Chiamate

Per accedere a questa sezione aprire la finestra **Impostazioni Avanzate Antispyware** (andare al modulo **Antispyware**, alla sezione Status, fare un click su **Impostazioni Avanzate**) e quindi selezionare la scheda **Chiamate**.



Controllo Chiamate

I dialer sono applicazioni che usano i modem dei computer per comporre diversi numeri telefonici. Solitamente i dialer vengono utilizzati per accedere a varie locazioni componendo numeri telefonici molto costosi.

Con il **Controllo delle Chiamate** si dovrà decidere quali connessioni a diversi numeri telefonici consentire o bloccare. Questa funzione monitorizza tutti i dialer che tentano di accedere al modem del computer, avvisando immediatamente l'utente e chiedendogli di scegliere se bloccare o consentire tali operazioni:

Avvisi Chiamate

Si potranno vedere il nome dell'applicazione e il numero di telefono.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando l'applicazione tenterà di comporre lo stesso numero telefonico.

E' possibile accedere a qualsiasi regola memorizzata dalla sezione **Chiamata** per ulteriori perfezionamenti della configurazione.

Importante

La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

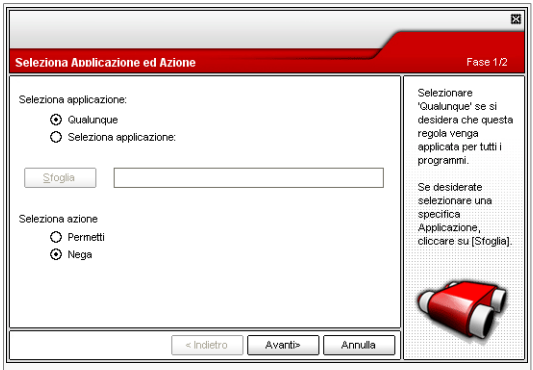
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare i parametri di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondente.

Le regole possono essere immesse automaticamente (attraverso la finestra di avviso) o manualmente (cliccare sul pulsante **Aggiungi** e scegliere i parametri per la regola). Apparirà l'installazione guidata.

10.4.1. Installazione Guidata della Configurazione

L' installazione guidata è una procedura composta da 2 passaggi.

Passaggio 1/2 - Selezione Applicazione e Azione



Selezione Applicazione ed Azione

Potete impostare i parametri:

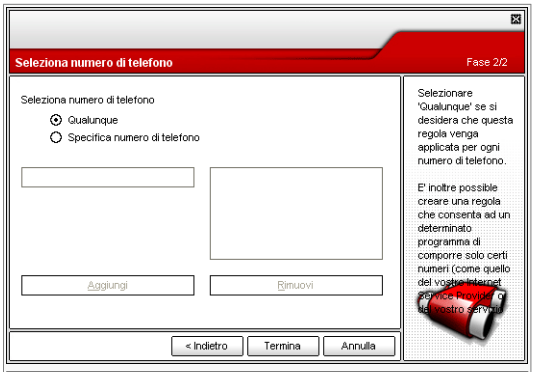
- **Applicazione** - selezionare l'applicazione per la regola. E' possibile scegliere solo una applicazione (selezionare **Seleziona applicazione** successivamente **Visualizza** e selezionare l'applicazione) oppure tutte le applicazioni (è sufficiente selezionare **Qualsiasi**).

- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Abilitazione	L'azione sarà permessa.
Impedisci	L'azione sarà negata.

Selezionare **Avanti**.

Passaggio 2/2 - Selezione dei Numeri Telefonici



Selezione dei Numeri Telefonici

Selezionare **Specifica numero di telefono**, digitare il numero di telefono per il quale verrà creata una regola e selezionare **Aggiungi**.

Nota

E' possibile utilizzare caratteri jolly nell'elenco dei numeri telefonici banditi; ad es.: 1900* significa che tutti i numeri che iniziano con 1900 verranno bloccati.

Selezionare **Qualsiasi** se volete che questa regola venga applicata a qualsiasi numero di telefono. Se desiderate cancellare un numero è sufficiente selezionarlo e premere **Rimuovi**.

Nota

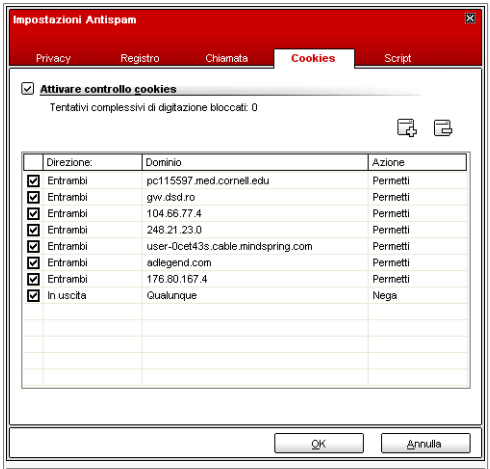
E' inoltre possibile creare una regola che consenta ad un determinato programma di comporre solo determinati numeri (come ad esempio quello del vostro Service Provider oppure quello del vostro servizio fax).

Selezionare **Termina**.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

10.5. Impostazioni Avanzate - Controllo Cookie

Per accedere a questa sezione aprire la finestra **Impostazioni Avanzate Antispyware**(andare al modulo **Antispyware**, alla sezione Status e selezionare **Impostazioni Avanzate**) quindi fare un click sulla scheda **Cookie**.



Controllo Cookie

I Cookies sono molti frequenti su Internet. Si tratta di piccoli files immagazzinati sul vostro computer. I siti web creano questi cookies per mantenere traccia di specifiche informazioni che vi riguardano.

Generalmente i Cookies vengono creati per rendere facilitare la navigazione nei siti web. Ad esempio possono aiutare i siti web a ricordare il vostro nome e le vostre preferenze, evitandovi così di doverli inserire ad ogni visita.

I cookie però possono anche essere utilizzati per compromettere la vostra privacy, tenendo traccia delle vostre abitudini di navigazione.

E' in questo caso che il **Controllo dei Cookies** vi sarà di aiuto. Quando è attivato, il **Controllo dei Cookies** chiederà il vostro consenso ogni volta che un sito web tenta di impostare un cookie:

Allarme Cookie

E' possibile visualizzare il nome dell'applicazione che sta tentando di inviare un file cookie.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando ci si collegherà successivamente allo stesso sito.

Questo vi aiuterà a scegliere i siti web di cui fidarsi o no.

Nota

A causa del notevole numero di cookie utilizzati oggi giorno su Internet, il **Controllo dei Cookies** può risultare inizialmente abbastanza noioso. All'inizio porrà molte domande riguardo ai siti che tentano di piazzare i cookies sul vostro computer. Non appena si aggiungeranno i vostri siti abituali all'elenco delle regole, la navigazione diventerà semplice come prima.

E' possibile accedere a qualsiasi regola memorizzata nella sezione **Cookies** per ulteriori perfezionamenti.

Importante

La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

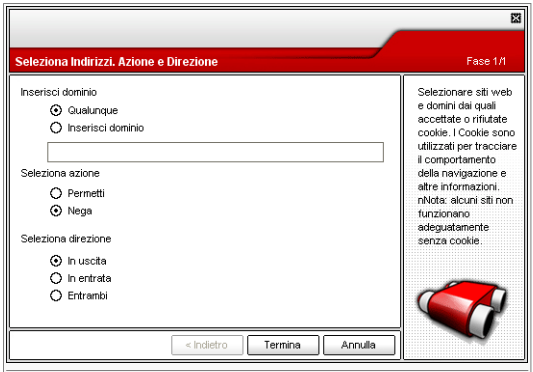
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare i parametri di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondente.

Le regole possono essere immesse automaticamente (attraverso la finestra di avviso) o manualmente (cliccare sul pulsante **Aggiungi** e scegliere i parametri per la regola). Apparirà l'installazione guidata.

10.5.1. Installazione Guidata della Configurazione

L'installazione guidata consiste in 1 passo.

Passo 1/1 - Selezione Indirizzo, Azione e Direzione



Selezione Indirizzo, Azione e Direzione

Potete impostare i parametri:

- **Indirizzo Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Abilitazione	I cookies da quel dominio verranno eseguiti.
Impedisci	I cookies da quel dominio non verranno eseguiti.

- **Direzione** - seleziona la direzione del traffico.

Tipo	Descrizione
In Uscita	La regola sarà applicata solo ai cookies che vengono rispediti al sito connesso.
In Entrata	La regola sarà applicata solo ai cookies che vengono ricevuti dal sito connesso.
Entrambe	La regola sarà applicata in entrambe le direzioni.

Selezionare **Termina**.

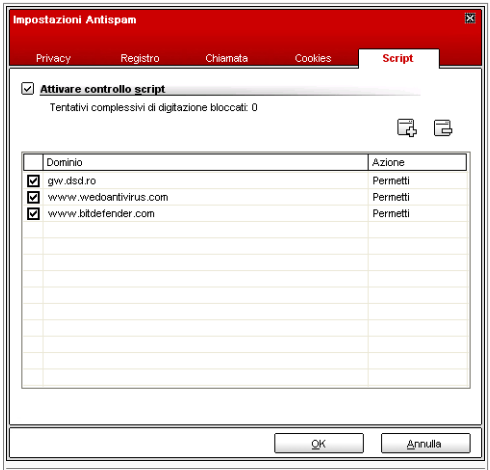
Nota

Si possono accettare i cookie, ma non conviene mai rispedirli, impostando l'azione **Divieto** e la direzione **In uscita**.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

10.6. Impostazioni Avanzate - Controllo Script

Per accedere a questa sezione aprire la finestra **Impostazioni Avanzate Antispyware**(andare al modulo **Antispyware**, alla sezione Status e selezionare **Impostazioni Avanzate**) quindi fare un click sulla scheda **Script**.

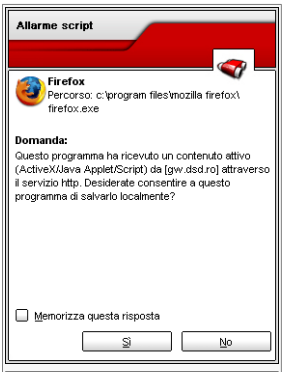


Controllo degli Script

Gli Scripts e altri codici come ActiveX controls e Java applets, che sono utilizzati per creare pagine interattive, possono essere programamti per avere effetti dannosi. Per esempio gli elementi ActiveX , possono ottenere l' accesso ai dati del vostro computer, cancellare informazioni, catturare passwords e intercettare messaggi mentre siete online. Dovreste accettare contenuti attivi esclusivamente da siti che si conoscono come affidabili.

BitDefender vi consente di scegliere se eseguire questi elementi oppure bloccare la loro esecuzione.

Con il **Controllo degli Script** sarete voi a decidere quali siti web sono affidabili e quali no. BitDefender chiederà il vostro consenso ogni volta che un sito web tenterà di attivare uno script o altri contenuti attivi:



Allarme Script

E' possibile visualizzare il nome della risorsa.

Selezionare la casella **Memorizza questa risposta** e fare click su **Sì** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando lo stesso sito tenterà di inviarvi contenuti attivi.

E' possibile accedere a qualsiasi regola memorizzata dalla sezione **Script** per ulteriori perfezionamenti.

Importante

La priorità delle regole è dal basso in alto, cioè l'ultima regola ha la più alta priorità. Seleziona & Trascina le regole per cambiare la loro priorità.

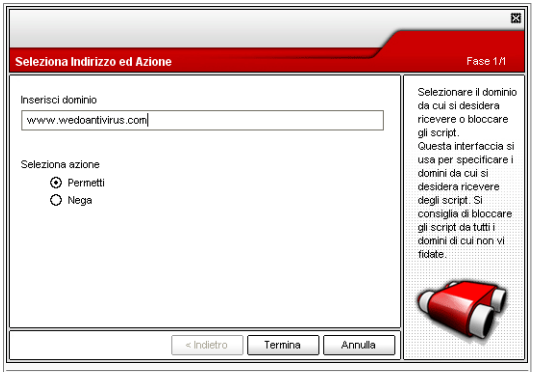
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare i parametri di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondente.

Le regole possono essere immesse automaticamente (attraverso la finestra di avviso) o manualmente (cliccare sul pulsante **Aggiungi** e scegliere i parametri per la regola). Apparirà l'installazione guidata.

10.6.1. Installazione Guidata della Configurazione

L'installazione guidata consiste in 1 passo.

Passaggio 1/1 - Selezione Indirizzo ed Azione



Selezione Indirizzo e Azione

Potete impostare i parametri:

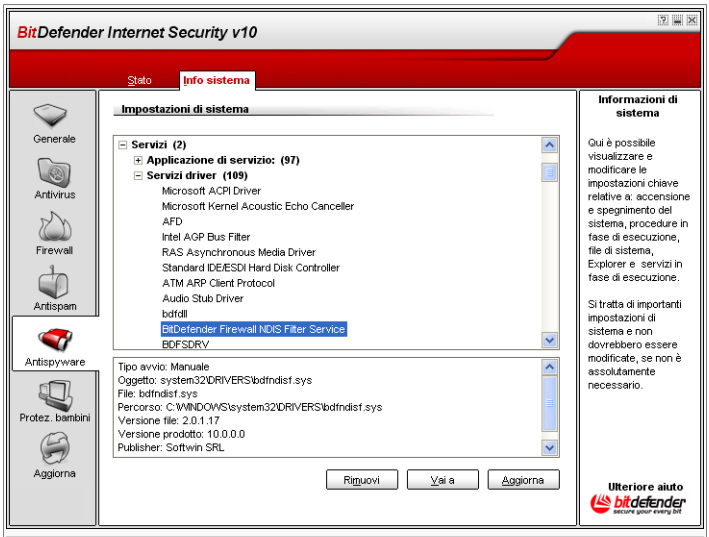
- **Indirizzo Dominio** - digitare il dominio sul quale applicare la regola.
- **Azione** - selezionare l'azione della regola.

Azione	Descrizione
Abilitazione	Gli scripts da quel dominio saranno eseguiti.
Impedisci	Gli scripts da quel dominio non saranno eseguiti.

Selezionare **Termina**.

Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

10.7. Sistema di Informazione



Sistema di Informazione

Qui potete vedere e modificare le impostazioni delle informazioni relative alla chiave.

La lista contiene sia gli elementi caricati all' avvio del sistema che quelli caricati da applicazioni diverse.

Sono disponibili tre pulsanti:

- **Rimuovi** - cancella l'elemento selezionato.
- **Vai a** - apre una finestra dove e situato l'elemento selezionato (la **Registy** ad esempio).
- **Aggiorna** - riapre la sezione del **Sistema Informazione**.

11. Modulo Parental Control

La sezione **Parental Control** di questa guida all'utente contiene i seguenti punti:

- Stato Parental Control
- Controllo Web
- Controllo Applicazioni
- Filtro parola chiave
- Limitatore Tempo sul Web

Nota

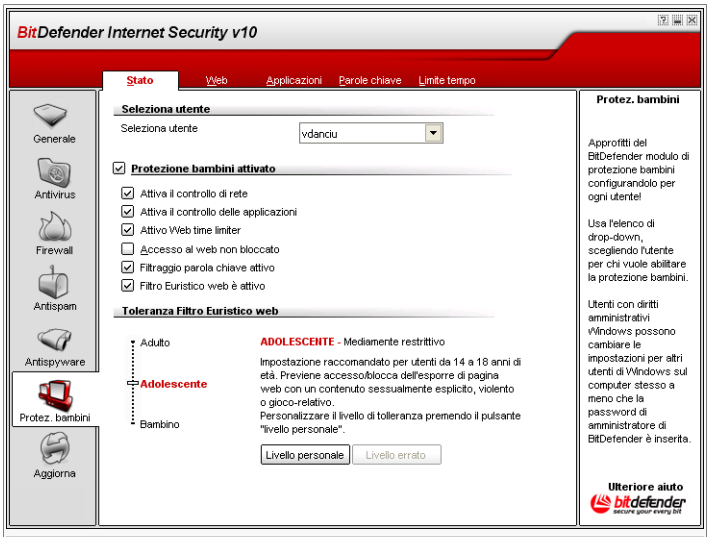
Per ulteriori dettagli riguardanti il modulo **Protezione bambini** e' possibile accedere alla descrizione del «*Modulo Parental Control*» (p. 32).

Importante

È possibile accedere e configurare questo modulo solo da parte di utenti con diritti di amministratore (amministratori di sistema). Se le impostazioni sono protette da password, esse possono essere modificate solo se la password è fornita. Un amministratore non può imporre un set di regole ad un utente per il quale siano state definite regole in precedenza da un altro amministratore.

Se non siete l'unica persona ad usare questo computer, vi raccomandiamo di proteggere le vostre impostazioni del BitDefender con una password. Per impostare una password, entrare nel modulo **Generale** accedere alla sezione Impostazioni e usare l'opzione **Abilita la protezione password**.

11.1. Stato del Parental Control



Stato del Parental Control

In questa sezione, potete configurare il livello generale di protezione **Parental Control** per un utente selezionato.

Importante

Mantenere il **Parental Control** abilitato per proteggere i vostri bambini dai contenuti inopportuni utilizzando le vostre regole di accesso al computer personalizzate.

Per configurare il livello di protezione dovete prima selezionare l'utente a cui volete applicare queste impostazioni. Quindi configurate il livello di protezione utilizzando i seguenti controlli:

- **Controllo Web** - abilitate il **Controllo Web** per filtrare la navigazione sul web secondo le regole da voi impostate nella sezione Web.
- **Controllo Applicazioni** - abilitate il **Controllo Applicazioni** per bloccare l'accesso alle applicazioni sul vostro computer secondo le regole da voi impostate nella sezione Applicazioni.

- **Limitatore di Tempo su Web** - abilitate il **Limitatore di Tempo su Web** per consentire l'accesso al web secondo l'orario da voi stabilito nella sezione Limitatore Tempo.
- **Accesso Web** - abilitate questa opzione per bloccare l'accesso a tutti i siti web (non solo a quelli nella sezione Web).
- **Filtraggo Parola Chiave** - abilitate il **Filtraggio Parola Chiave** per filtrare l'accesso al web e alla posta secondo le regole da voi impostate nella sezione Parole Chiave.
- **Filtro web euristico** - abilitate questa opzione per filtrare l'accesso al web secondo le regole prestabilite sulla base delle categorie di età.

11.1.1. Tolleranza Filtro Euristico Web

Trascinate il pulsante scorrevole lungo la barra per impostare il livello di protezione che considerate appropriato per l'utente selezionato.

Ci sono 3 livelli di protezione:

Livello di protezione	Descrizione
Bambino	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti al di sotto dei 14 anni. Le pagine web con contenuto potenzialmente dannoso per i bambini (porno, sessualità, droghe, hacking ecc.) sono bloccate.
Adolescenti	Offre un accesso web limitato, secondo le impostazioni raccomandate per gli utenti con età tra i 14 e i 18 anni. Le pagine web con contenuto sessuale, pornografico o per adulti sono bloccate.
Adulti	Offre un accesso illimitato a tutte le pagine web indipendentemente dal loro contenuto.

Cliccare su **Personalizza Livello** per impostare le vostre regole di filtraggio personalizzate. Nella finestra che apparirà, selezionate le categorie di contenuto (gioco d'azzardo, hacking, porno ecc) per le quali BitDefender deve impedire l'accesso su web da parte dell'utente e cliccare su **OK**.

Cliccare su **Livello di Default** per impostare il pulsante scorrevole al livello di default.

11.2. Controllo Web

Controllo Web

Il **Web Control** ti aiuta a bloccare l'accesso ai siti web inappropriati. Una lista di utenti per bloccare i siti inappropriati e una parte é fornita e aggiornata da BitDefender come parte del processo di aggiornamento regolare.

Per abilitare questa protezione selezionate la casella di controllo che corrisponde a **Abilita il Controllo Web**.

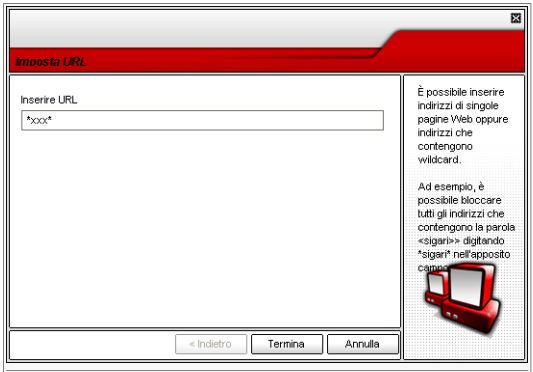
Selezionate **Consenti l'accesso a queste pagine**/**Blocca l'accesso a queste pagine** per vedere l'elenco dei siti permessi/bloccati. Cliccate su **Eccezioni** per accedere ad una finestra in cui potete vedere l'elenco complementare.

Le regole devono essere inserite manualmente. Prima di tutto, selezionate **Consenti accesso a queste pagine**/**Blocca accesso a queste pagine** per consentire/bloccare l'accesso ai siti web che specificherete nella procedura guidata. Quindi, cliccate sul pulsante **Aggiungi...** per avviare la procedura di configurazione guidata.

11.2.1. Installazione Guidata della Configurazione

L'installazione guidata consiste in 1 passo.

Passo 1/1 – Specificare i siti web



Specifica i siti web

Digitare il sito web per il quale la regola sarà applicata e cliccare su **Fine**.

Importante

Sintassi:

- `*.xxx.com` - l'azione della regola si applicherà a tutti i siti web che terminano con `.xxx.com`;
- `*porn*` - l'azione della regola sarà applicata in tutti i siti web che contengono `porn` nell'indirizzo del sito web;
- `www.*.com` - l'azione della regola sarà applicata in tutti i siti web aventi come suffisso del dominio `com`;
- `www.xxx.*` - l'azione della regola sarà applicata in tutti i siti web che iniziano con `www.xxx.` indipendentemente dal suffisso del dominio.

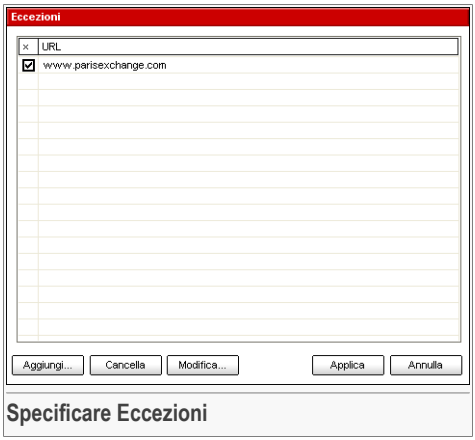
Cliccare **Applica** per salvare le modifiche.

Per cancellare una regola, selezionarla semplicemente e cliccare sul pulsante **Cancella**. Per modificare una regola selezionarla e cliccare sul pulsante **Modifica...** o fare doppio clic su di esso. Per disattivare temporaneamente una regola senza cancellarla, pulire la casella di spunta corrispondente.

11.2.2. Specifica Eccezioni

A volte potreste aver bisogno di specificare delle eccezioni ad una regola particolare. Ad esempio, avete impostato una regola che blocca i siti che contengono la parola "killer" nell'indirizzo (sintassi: `*killer*`). Siete anche coscienti dell'esistenza di un sito chiamato `killer-music` dove i visitatori possono ascoltare musica on-line. Per fare un eccezione alla regola precedentemente creata, accedete alla finestra **Eccezioni** e definite un'eccezione alla regola.

Cliccare su **Eccezioni...**. Apparirà la seguente finestra:



Specificare Eccezioni

Cliccare su **Aggiungi...** per specificare le eccezioni. La procedura di configurazione guidata apparirà. Completate la procedura guidata per impostare l'eccezione.

Cliccare **Applica** per salvare le modifiche.

Per cancellare una regola, basta solo selezionarla e fare click su **Cancella**. Per modificare una regola, selezionarla e cliccare su **Modifica...** o fare doppio click. Per disattivare temporaneamente una regola senza eliminarla, pulite la casella di spunta corrispondente.

11.2.3. Blacklist Web BitDefender

Per aiutarvi a proteggere i vostri bambini, BitDefender fornisce una blacklist di siti web con contenuto inopportuno o probabilmente dannoso. Per bloccare i siti che appaiono in questo elenco selezionate **Utilizza l'elenco di siti bloccati fornito da BitDefender**.

11.3. Controllo Applicazioni

Controllo Applicazioni

Il **Controllo Applicazioni** ti aiuta a bloccare qualsiasi applicazione in esecuzione. Giochi, messaggi software, oltre ad altre categorie di software e minacce che in questo caso possono essere bloccati. Le applicazioni bloccate sono così protette da modifiche, e non possono essere copiate o spostate.

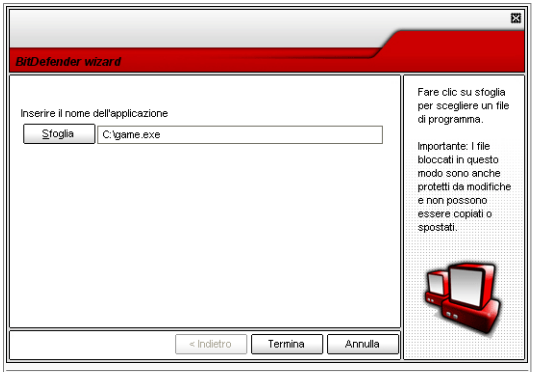
Per abilitare questa protezione seleziona la casella di controllo che corrisponde a **Abilita Controllo Applicazioni**.

Le regole devono essere inserite manualmente. Cliccare sul pulsante **Aggiungi...** per avviare la procedura di configurazione guidata.

11.3.1. Installazione Guidata della Configurazione

L'installazione guidata consiste in 1 passo.

Passo 1/1 – Seleziona l'Applicazione da Bloccare



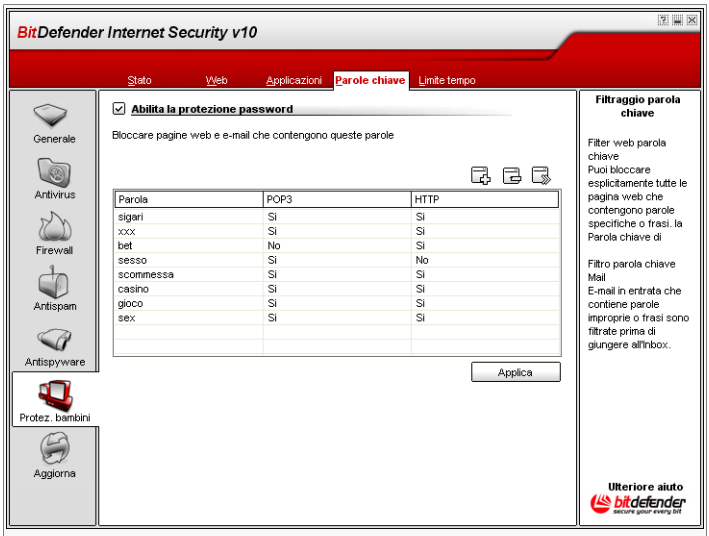
Seleziona l'Applicazione da Bloccare

Cliccate su **Esplora**, selezionate l'applicazione da bloccare e cliccate su **Fine**.

Cliccare **Applica** per salvare le modifiche.

Per cancellare una regola, selezionarla semplicemente e cliccare sul pulsante **Cancella**. Per modificare una regola selezionarla e cliccare sul pulsante **Modifica...** o fare doppio clic su di esso. Per disattivare temporaneamente una regola senza cancellarla, pulire la casella di spunta corrispondente.

11.4. Filtraggio Parola Chiave



Filtraggio Parola Chiave

Il **Filtro Parola Chiave** vi aiuta a bloccare l'accesso ai messaggi e-mail o alle pagine web che contengono una parola specifica. In questo modo potete evitare che gli utenti vedano parole o frasi inopportune.

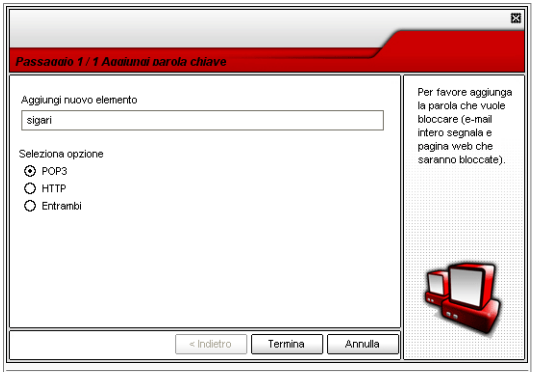
Per abilitare questa protezione selezionate la casella di spunta che corrisponde a **Filtraggio Parola Chiave**.

Le regole devono essere inserite manualmente. Cliccare sul pulsante **Aggiungi...** per avviare la procedura di configurazione guidata.

11.4.1. Installazione Guidata della Configurazione

La procedura di configurazione guidata comprende 3 passaggi.

Passo 1/1 - Inserire la Parola Chiave



Inserite la parola chiave

Dovete impostare i parametri seguenti:

- **Parola chiave** - digitare nel campo di edit la parola o la frase che volete bloccare.
- **Protocollo** - scegliere il protocollo che BitDefender dovrebbe scansionare per la parola sepcificata.

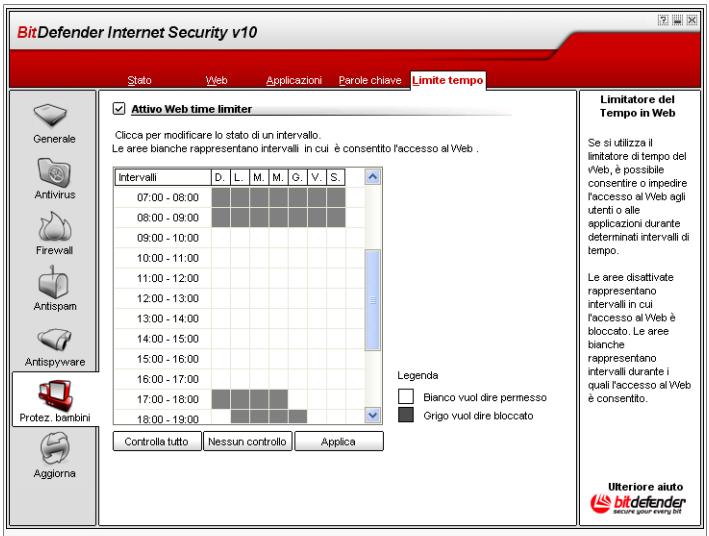
  Sono disponibili le seguenti opzioni:

Opzione	Descrizione
POP3	I messaggi e-mail che contengono la parola chiave sono bloccati.
HTTP	Le pagine web che contengono la parola chiave sono bloccate.
Entrambe	sia i messaggi e-mail che le pagine web che contengono la parola chiave sono bloccate.

Cliccare **Applica** per salvare le modifiche.

Per cancellare una regola, selezionarla semplicemente e cliccare sul pulsante **Cancella**. Per modificare una regola selezionarla e cliccare sul pulsante **Modifica...** o fare doppio clic su di esso. Per disattivare temporaneamente una regola senza cancellarla, pulire la casella di spunta corrispondente.

11.5. Tempo limitato sul web



Tempo limitato sul web

Il **Tempo limitato sul web** ti aiuta a bloccare l'accesso a internet per determinati periodi di tempo.

Nota

BitDefender eseguirà aggiornamenti ogni ora indipendentemente dall'impostazione **Tempo limitato sul web**.

Per abilitare questa protezione seleziona la casella di controllo che corrisponde a **Abilita Tempo limitato sul web**.

Seleziona l'intervallo di tempo quando sei connesso a internet, sarà così bloccato. Tu puoi cliccare su celle individuali, o puoi bloccare l'intervallo per un lungo periodo di tempo. È possibile fare clic su **Controla tutto** per selezionare tutte le caselle e, implicitamente, bloccare tutto l'accesso alla rete. Se si fa clic su **Non controllare tutto**, le connessioni a Internet verranno consentite sempre.

Importante

I box colorati in grigio rappresentano l'intervallo di tempo quando la connessione internet è bloccata.

Cliccare **Applica** per salvare le modifiche.

12. Modulo Update

La sezione **Update** di questa guida all'utente comprende i seguenti argomenti:

- Aggiornamento Automatico
- Aggiornamento Manuale
- Impostazioni dell'Aggiornamento

Nota

Per ulteriori dettagli relativi al modulo **Update** vedere la descrizione del «*Modulo Update*» (p. 32).

12.1. Aggiornamento Automatico

Aggiornamento Automatico

In questa sezione potete vedere le informazioni relative all' aggiornamento e quelli in esecuzione.

Importante
Per essere sempre protetti, tenete l' **Aggiornamento Automatico** abilitato.

Se siete connessi a Internet con banda larga o DSL, BitDefender effettuerà automaticamente un controllo degli aggiornamenti, ogni volta che avvierete il vostro computer. Il controllo viene eseguito ogni **ora**.

Se è stato rilevato un aggiornamento, secondo le opzioni impostate nella sezione di Aggiornamento Automatico, vi verrà chiesto di confermare l' aggiornamento oppure verrà eseguito automaticamente.

L'aggiornamento automatico può essere eseguito in qualsiasi momento, cliccando su **Aggiorna adesso**. Questo aggiornamento è conosciuto anche come **Aggiornamento su richiesta dell'utente**.

Il modulo **Update** si collegherà al server di aggiornamento di BitDefender e verificherà la disponibilità. Se viene rilevato un nuovo aggiornamento, secondo le opzioni impostate nella sezione Impostazioni update Manuale, verrà chiesto di confermarlo oppure sarà eseguito automaticamente.

Importante
Potrebbe essere necessario riavviare il computer una volta completato l'aggiornamento. Vi consigliamo di farlo appena possibile.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento di BitDefender su richiesta dell'utente.

Potete verificare la firma dei malware del vostro BitDefender cliccando **Mostra Elenco dei Virus**. Sarà creato un file HTML che contiene tutte le firme disponibili. Cliccare nuovamente **Mostra la Lista dei Virus** per vederla. Potete cercare la firma di uno specifico malware attraverso il database oppure clicare **Lista dei Virus BitDefender** per andare online al database delle firme di BitDefender.

12.2. Aggiornamento Manuale

Questo metodo consente di installare le ultime definizioni di virus. Per installare un aggiornamento del prodotto nella sua ultima versione, utilizzare l'Aggiornamento Automatico.

Importante
Utilizzare l'aggiornamento manuale quando quello automatico non può essere eseguito oppure quando il computer non è collegato ad Internet.

Ci sono 2 modi per eseguire l'Aggiornamento Manuale:

- con il file `weekly.exe`;
- con gli `archivi zip`.

12.2.1. Aggiornamento Manuale con il file `weekly.exe`

Il pacchetto di aggiornamento `weekly.exe` viene rilasciato ogni Venerdì e include tutte le definizioni di virus e aggiornamenti dei motori di scansione, disponibili fino alla data di rilascio.

Per aggiornare BitDefender usando `weekly.exe`, seguire i passi seguenti:

1. Scaricare weekly.exe e salvarlo sul vostro hard disk.
2. Localizzare il file scaricato e fare un doppio click per lanciare la guida all'aggiornamento.
3. Selezionare **Avanti**.
4. Controllare **Accetto i termini dell'accordo di licenza** e fare un click su **Avanti**.
5. Cliccare su **Installa**.
6. Selezionare **Termina**.

12.2.2. Aggiornamento Manuale con `archivi zip`

Ci sono due archivi zip sul server di aggiornamento. Gli gli archivi contengono gli aggiornamenti dei motori di scansione e le firme dei virus: `cumulative.zip` e `daily.zip`.

- Il `cumulative.zip` viene rilasciato il Lunedì di ogni settimana e include tutti gli aggiornamenti sulle definizioni di virus e dei motori di scansione fino alla data di rilascio.
- Il `daily.zip` viene rilasciato ogni giorno e include tutti gli aggiornamenti sulle definizioni di virus e dei motori di scansione, dall'ultimo cumulative fino alla data corrente.

BitDefender utilizza una architettura basata sul servizio. Quindi la procedura per sostituire le definizioni di virus è diversa, a seconda del Sistema Operativo:

- Windows 2000, Windows XP, Windows Vista

Windows 2000, Windows XP, Windows Vista

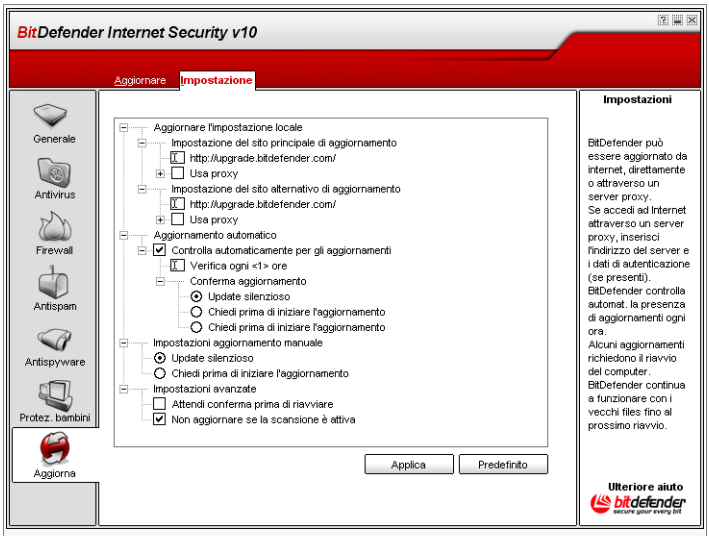
Passi da seguire:

1. **Scaricare l'aggiornamento appropriato.** Se è Lunedì, scaricare il cumulative.zip e salvarlo sul disco. Altrimenti, scaricare il daily.zip e salvalo sul disco. Se è la prima volta che viene eseguito l'aggiornamento usando il processo manuale, scaricare entrambi gli archivi.
2. **Bloccare la protezione antivirus BitDefender.**
   - **Uscire dal Pannello di Controllo di BitDefender.** Cliccare con il tasto destro sull'icona di BitDefender nella barra degli strumenti e selezionare **Esci**.
   - **Aprire i Servizi.** Cliccare su **Avvio**, poi **Pannello di Controllo**, e eseguire un doppio clic su **Strumenti di Amministrazione**, quindi cliccare su **Servizi**.
   - **Bloccare il servizio Virus Shield di BitDefender.** Selezionare il servizio **Virus Shield di BitDefender** dalla lista e cliccare su **Bloccare**.
   - **Bloccare il servizio Server di Scansione di BitDefender.** Selezionare il servizio **Scansione Server di BitDefender** dalla lista e cliccare su **Bloccare**.
3. **Estrarre il contenuto dall'archivio.** Se sono disponibile entrambi gli archivi, iniziare dal `cumulative.zip`. Estrarre il contenuto nella cartella `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` e accettare di sovrascrivere sui files esistenti.
4. **Riavviare la protezione antivirus BitDefender.**
   - **Iniziare il servizio Server di Scansione di BitDefender.** Selezionare il servizio **Server di Scansione di BitDefender** della lista e cliccare su **Inizia**.
   - **Iniziare il servizio Virus Shield di BitDefender.** Selezionare il servizio **Virus Shield di BitDefender** dalla lista e cliccare su **Inizia**.
   - **Aprire il Panello di controllo di BitDefender.**

Nota

Se avete installato Windows Vista, vi sarà richiesto di confermare la maggior parte di queste azioni.

12.3. Impostazioni dell'Aggiornamento



Impostazioni dell'Aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy.

La finestra con le impostazioni dell'aggiornamento contiene 4 categorie di opzioni (**Indirizzo di aggiornamento**, **Aggiornamento automatico**, **Impostazioni update manuale** e **Opzioni avanzate**) organizzate in un menu espandibile, simile a quello di Windows.

Nota

Selezionare la casella con "+" per aprire una categoria oppure una casella con "-" per chiudere una categoria.

12.3.1. Indirizzo di aggiornamento

Per aggiornamenti più affidabili e veloci, potete configurare 2 locazioni per l'aggiornamento: **Locazione principale dell'aggiornamento** e **locazione alternativa dell'aggiornamento**. Per entrambe dovete configurare le seguenti opzioni:

- **Locazione aggiornamento** - Se siete connessi ad una rete locale che ha le firme dei virus di BitDefender, potete cambiare direttamente la locazione degli aggiornamenti. Di default è: http://upgrade.bitdefender.com.
- **Usa il proxy** - Selezionare questa opzione nel caso in cui l'azienda utilizzi un server proxy. Devono essere specificate le seguenti impostazioni:
  - **Proxy sets** - inserire l'indirizzo IP o il nome del server proxy e la porta che utilizza BitDefender per accedere al server proxy.

    Importante

    Sintassi: `name:port` o `ip:port`.

  - **Utente** - inserire un nome utente riconosciuto dal proxy.

    Importante

    Sintassi: `domain\user`.

  - **Proxy Password** - inserire la password valida per l'utenza, già specificata precedentemente.

12.3.2. Opzioni Aggiornamento Automatico

- **Controllo automaticamento per gli aggiornamenti** - BitDefender controlla automaticamente i nostri server per gli aggiornamenti disponibili.
- **Verificare ogni x ore** - Imposta con quale frequenza BitDefender esegue un controllo per gli aggiornamenti. L'intervallo di tempo predefinito è di un'ora.
- **Update silenzioso** - BitDefender scarica ed implementa l'aggiornamento automaticamente.
- **Chiedi prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.
- **Chiedi prima di installare gli aggiornamenti** - ogni volta che si scarica un aggiornamento, vi verrà richiesto se installarlo.

Importante

Se selezionate **Chiedi prima di scaricare gli aggiornamenti** e poi chiudi& exit del pannello di controllo, l'aggiornamento manuale non verrà eseguito.

12.3.3. Impostazioni Aggiornamento Manuale

- **Update silenzioso** - l'aggiornamento manuale sarà eseguito automaticamente in background.
- **Chiedi prima di scaricare gli aggiornamenti** - ogni volta che eseguite un aggiornamento manuale, vi sarà richiesto se scaricare ed installare gli aggiornamenti.

Importante

Se selezionate **Chiedi prima di scaricare gli aggiornamenti** e poi chiudi& exit del pannello di controllo, l'aggiornamento manuale non verrà eseguito.

12.3.4. Opzioni Avanzate

- **Attendi conferma prima di riavviare** - Se un aggiornamento richiede un riavvio, il prodotto continuerà a lavorare con i vecchi files fino a quando il sistema non sarà riavviato. Non verrà richiesto di riavviare il computer, per non interferire con il lavoro dell'utente.
- **Non aggiornare se la scansione è in corso** - BitDefender non verrà aggiornato se è in corso un processo di scansione. In questo modo la procedura di aggiornamento BitDefender non interferirà con le operazioni di scansione.

Nota

Se BitDefender viene aggiornato durante una scansione, la procedura di scansione sarà interrotta.

Selezionare **Applica** per salvare le modifiche oppure **Default** per tornare alle impostazioni di default.

Consigli

13. Consigli

La sezione **Pratiche consigliate** di questa guida all'utente, comprende i seguenti argomenti:

- Come proteggere il vostro Computer connesso a Internet
- Come proteggere il vostro computer dalle minacce dei Malware
- Come configurare una Applicazione di Scansione
- Come Configurare il Modulo Firewall
- Come mantenere il vostro Computer libero da SPAM
- Come Proteggere il Vostro Bambino dai Contenuti Inopportuni

13.1. Come Proteggere il Vostro Computer Connesso ad Internet

Seguite questi passi per proteggere il vostro computer connesso ad Internet:

1. **Completare la procedura guidata di configurazione iniziale.** Durante il processo di installazione apparirà una guida. Essa vi aiuterà a registrare BitDefender e a creare un account BitDefender per usufruire del supporto tecnico gratuito. Vi aiuterà anche ad impostare BitDefender ad eseguire importanti compiti di sicurezza.

   Importante

   Se avete un CD di Soccorso di BitDefender Internet Security v10, eseguite una scansione del vostro sistema prima di installare BitDefender per assicurarvi di non avere alcun malware già esistente sul vostro sistema.

2. **Aggiornare BitDefender.** Se non avete completato l'impostazione iniziale guidata durante il processo di installazione, eseguire un aggiornamento richiesto dall'utente (andare al modulo **Update**, alla sezione Update, e fare un click su **Aggiorna adesso**).
3. **Eseguire una scansione completa del sistema.** Accedere al modulo **Antivirus**, sezione Shield e eseguire un click su **Scansiona adesso**.

   Nota

   Potete anche iniziare una scansione completa del sistema dalla sezione Scan Selezionare **Scansione Completa del Sistema** e eseguire un click su **Esegui il processo**.

4. **Prevenire le infezioni.** Nella sezione **Scudo**, tenere la protezione in tempo reale on per essere protetti da virus, spyware e altro malware. Impostare il livello di protezione che meglio si adatta alle vostre necessità. Lo potete personalizzare ogni volta che volete cliccando su **Personalizza Livello**.

   Importante

   Programmate il vostro BitDefender per eseguire una scansione del sistema almeno una volta alla settimana schedulando l' azione**Scansione dell'intero sistema** dalla sezione Scan.

5. **Mantenere il vostro BitDefender aggiornato.** Nel modulo di **Aggiornamento**, sezione Aggiornamento ,mantenere l' **Aggiornamento Automatico** abilitato per essere sempre protetti dagli ultimi malware dannosi.
6. **Prevenire attacchi da Internet.** Configura il Firewall BitDefender per essere protetto contro gli attacchi Internet.
7. **Strumenti di blocco spyware.** Nel modulo **Antispyware**, la sezione Stato mantiene la protezione al livello raccomandato o superiore. In questo modo, sarete protetti contro programmi illegittimi che cercano di cabiare le chiavi del registro e contro i dialer ad alto costo. Se volete tenere al sicuro i vostri dati riservati abilitate il Controllo Privacy e create delle regole appropriate.
8. **Tenere lontano lo spam.** Se avete un account e-mail che volete proteggere, configurate il modulo Antispam.
9. **Blocca l'accesso al contenuto inappropriato.** Se i vostri bambini utilizzano il computer, proteggeteli contro il contenuto inappropriato configurando il modulo Parental Control.

13.2. Come proteggere il vostro computer dalle minacce dei Malware

Seguire questi passi per proteggere il vostro computer da virus, spyware e altro malware:

1. **Completare la procedura guidata di configurazione iniziale.** Durante il processo di installazione apparirà una guida. Essa vi aiuterà a registrare BitDefender e a creare un account BitDefender per usufruire del supporto tecnico gratuito. Vi aiuterà anche ad impostare BitDefender ad eseguire importanti compiti di sicurezza.

Importante

Se avete un Disco di Soccorso BitDefender, scansionate il vostro sistema prima di installare BitDefender per assicurarvi di non avere nessun malware già esistente sul vostro sistema.

2. **Aggiornare BitDefender.** Se non avete completato l'impostazione iniziale guidata durante il processo di installazione, eseguire un aggiornamento richiesto dall'utente (andare al modulo **Update**, alla sezione Update, e fare un click su **Aggiorna adesso**).
3. **Eseguire una scansione completa del sistema.** Accedere al modulo **Antivirus**, sezione Shield e eseguire un click su **Scansiona adesso**.

Nota

Potete anche iniziare una scansione completa del sistema dalla sezione Scan Selezionare **Scansione Completa del Sistema** e eseguire un click su **Esegui il processo**.

4. **Prevenire le infezioni.** Nella sezione **Scudo**, tenere la protezione in tempo reale on per essere protetti da virus, spyware e altro malware. Impostare il livello di protezione che meglio si adatta alle vostre necessità. Lo potete personalizzare ogni volta che volete cliccando su **Personalizza Livello**.

Importante

Programmate il vostro BitDefender Internet Security v10 per eseguire la scansione del vostro sistema almeno una volta alla settimana Programmando il compito di **Scansione Completa del Sistema** dalla sezione Scansione.

5. **Mantenere il vostro BitDefender aggiornato.** Nel modulo di **Aggiornamento**, sezione Aggiornamento ,mantenere l' **Aggiornamento Automatico** abilitato per essere sempre protetti dagli ultimi malware dannosi.
6. **Programmare una scansione completa del sistema.** Andare alla sezione **Scan** e programmare BitDefender per esaminare il vostro sistema almeno una volta la settimana da programmazione dell' azione **Scansione Completa del Sistema**.

13.3. Come Configurare un Compito di Scansione

Seguire questi passi per creare e configurare un compito di scasione:

1. **Creare un nuovo compito.** Andate alla sezione Scansione e cliccate su **Nuovo Compito**. La finestra Proprietà apparirà.

Nota

Potete creare un nuovo compito anche duplicando un compito già esistente. Per far ciò, cliccate col tasto destro del mouse su un compito e selezionate **Duplicare** dal menu rapido. Slezionate il duplicato e cliccate su **Proprietà** per aprire la finestra delle **Proprietà**.

2. **Impostazione del livello di scansione.** Andare alla sezione **Overview** per impostare il livello di scansione. Se volete, potete personalizzaree le impostazioni della scansione cliccando **Custom**.
3. **Impostare il tipo di scansione:** Andare alla sezione **Scan Path** e scegliere gli oggetti che volete scansionare.
4. **Schedulazione delle azioni.** Se il compito di scansione è complesso, potreste programmarlo per un momento successivo, quando il vostro computer è in modalità inattiva. Questo aiuterà BitDefender ad eseguire una scansione accurata del vostro sistema. Andate alla sezione **Programmatore** per programmare il compito.

13.4. Come Configurare il Modulo Firewall

Seguite questi passi per configurare il modulo **Firewall**:

1. **Creare un nuovo profilo di rete.** Ogni volta che vi collegate ad una nuova rete, una procedura guidata apparirà. Completate la procedura guidata firewall per creare un set di regole base per il firewall per il profilo di rete.

   Nota

   La procedura guidata può essere lanciata in qualsiasi momento, cliccando su **Riconfigura profilo** nella sezione Traffico.

2. **Impostare il livello di protezione.** Andate alla sezione **Stato** per impostare la politice del firewall (**Nega Tutto**, **Consenti Tutto**, **Consenti Tutto se presente in Whitelist**, **Chiedi**).

   Importante

   Raccomandiamo di mantenere la protezione al livello **Consenti tutto se presente in whitelist**. In questo modo, BitDefender creerà regole per le applicazioni più comuni senza disturbarvi.

3. **Creare Regole.** Andate alla sezione **Traffico** e cliccate sul pulsante **Aggiungi** per creare regole per le vostre applicazioni più comunemente utilizzate. Dovete specificare i parametri delle regole.

4. **Impostare le opzioni avanzate del firewall.** Andate alla sezione **Avanzate** per specificare le regole di filtraggio per il traffico ICMP e le altre impostazioni del firewall.

13.5. Come Tenere il Vostro Computer Libero dallo Spam

Seguite questi passi per tenere lontano lo SPAM dal vostro computer:

1. **Impostazione del livello di tolleranza.** Accedere al modulo **Antispam**, sezione Stato per impostare il livello di tolleranza. Scegliere il livello di tolleranza appropriato aiuterà tutta la vostra posta legittima ad andare nella cartella Posta n Arrivo, sia che voi riceviate usualmente molta posta commerciale legittima sia un ampio volume di spam.
2. **Completare la procedura guidata della configurazione.** Se state utilizzando Microsoft Outlook o Microsoft Outlook Express / Windows Mail, seguire la procedura guidata di configurazione che si apre la prima volta che accedete al vostro client di posta. Inoltre potete aprire la procedura guidata dalla Barra degli strumenti Antispam.
3. **Compilare l' Elenco Amici.** Accedere al modulo **Antispam**, sezione Status e fare un click su oppure cliccare il bottone **Amici** dalla Barra degli Strumenti Antispam per aprire l' **Elenco Amici**. Aggiungere gli indirizzi delle persone dalle quali è assolutamente necessario ricevere le mail dall' Elenco Amici.

   Nota

   BitDefender non blocca i messaggi da quelli inclusi nell'elenco; in questo caso, aggiungere amici garantisce l'arrivo diretto dei messaggi legittimati.

4. **Addestrare il Motore di Apprendimento (bayesiano).** Ogni volta che ricevete una mail che considerate SPAM, ma BitDefender non ha etichettato come tale, selezionarla, cliccare il tasto **E' SPAM** nella Barra degli strumenti Antispam. I messaggi che si riceveranno con caratteristiche simili saranno etichettati come SPAM.

   Nota

   Il **Motore di Apprendimento** si attiva solo dopo essere stato "istruito" con almeno 60 messaggi e-mail legittimi. Per istruirlo, dovete seguire la Procedura di configurazione guidata.

5. **Mantenere il vostro BitDefender aggiornato.** Nel modulo **Aggiornamento**, allasezione Aggiornamento, mantenere l' **Aggiornamento Automatico** abilitato per essere sempre protetti contro le nuove minacce in tempo reale.

Nota

Ogni volta che eseguite un aggiornamento:
- nuove impronte di immagini saranno aggiunte al **Filtro Immagine**;
- nuovi links verranno aggiunti al **Filtro URL**;
- nuove regole verranno aggiunte al **Filtro Euristico**.

Questo aiuterà ad incrementare l'efficacia del vostro motore Antispam.

6. **Configurare il filtro Caratteri.** La maggior parte dei messaggi di spam sono scritti in caratteri cirillici e / o asiatici. Accedete al modulo **Antispam**, sezione Impostazioni e selezionate **Blocca Asiatico/Blocca Cirillico** se volete rifiutare tutti i messaggi e-mail scritti con questi caratteri.

Nota

E' possibile abilitare/disabilitare ognuno dei filtri Antispam accedendo alla sezione Impostazioni nel modulo **Antispam**.

13.6. Come Proteggere il Vostro Bambino dai Contenuti Inappropriati

Seguite questi passi per proteggere il vostro bambino dai contenuti inappropriati:

1. **Creare un account utente Windows limitato.** Per evitare che il vostro bambino acceda al modulo **Parental Control** o modifichi le sue impostazioni, egli o ella deve avere diritti limitati sul vostro sistema
2. **Selezione utente.** L'elenco di persone che utilizzano il computer è visualizzato nella sezione Stato. Scegliete da questo elenco l'utente che volete proteggere utilizzando il **Parental Control**.
3. **Impostare una protezione generale.** Andate alla sezione **Stato** per abilitare i controlli di protezione per il vostro bambinod. Se avete abilitato il **filtro web euristico**, impostare il livello di protezione appropriato.
4. **Bloccare i siti.** Andate alla **Sezione web** per fare un elenco di siti web di cui volete negare l'accesso al vostro bambino. Ove necessario, potete specificare eccezioni. Potete anche bloccare l'accesso ad un elenco di siti web fornito da BitDefender. Questi siti web hanno un contenuto inappropriato o potenzialmente dannoso.

5. **Bloccare le applicazioni.** Andate alla sezione **Applicazioni** per bloccare l'accesso alle applicazioni che no volete far utilizzare dal vostro bambino.

Nota

Se pensate che il vostro bambino passi troppo tempo giocando, utilizzando i media o software di messaggistica o altre applicazioni, potete bloccargli l'accesso ad essi.

6. **Bloccare le parole.** Per evitare che il vostro bambino possa vedere conetnuti potenzialmente dannosi sul web o nella posta, utilizzate il **Filtraggio Parola Chiave** per cercare parole o frasi particolari indicative di tale contenuto. Andate alla sezione **Parola Chiave** per definire le regole che bloccano l'accesso ai siti web o ai messaggi e-mail, o ad entrambi, se contengono stringhe specifiche.
7. **Controllare l'accesso al web.** Andate alla sezione **Limitatore tempo** per specificare l'orario secondo il quale l'accesso al web è consentito.
8. **Proteggere le vostre impostazioni con una password.** Accedete al modulo **Generale**, sezione Impostazioni e selezionate **Abilita la password di protezione per le impostazioni del prodotto**. Solo gli utenti che conoscono la password saranno in grado di modificare le impostazioni che avete imposto ad un certo utente.

BitDefender Rescue CD

BitDefender Internet Security v10 arriva con un CD avviabile (CD di soccorso BitDefender basato su LinuxDefender), capace di eseguire la scansione e disinfettare tutti gli hard drive esistenti prima che il vostro sistema operativo sia avviato.

Dovreste usare il Rescue CD ogni volta che il vostro sistema operativo non lavora correttamente per via di infezioni di virus. Generalmente accade quando non viene utilizzato un prodotto antivirus.

L'aggiornamento della firma dei virus è eseguita automaticamente, senza l'intervento dell'utente, ogni volta che si avvia il Rescue CD BitDefender.

LinuxDefender è una distribuzione di Knoppix ri-masterizzato di BitDefender, che integra l'ultima soluzione di sicurezza di BitDefender per Linux nel CD GNU/Linux Knoppix Live, offrendo protezione istantanea SMTP antivirus/antispam e un antivirus desktop capace di eseguire la scansione e disinfettare tutti gli hard disks esistenti (includendo partizioni NTFS di Windows), condivisioni remote di Samba /Windows o NFS mount points. E' inoltre inclusa una configurazione di interfaccia basata su web,con le soluzioni BitDefender.

14. Informazioni generali sul prodotto BitDefender™

Funzionalità Importanti

- Protezione istantanea della posta (Antivirus & Antispam)
- Soluzioni Antivirus per il vostro hard disk
- Supporto di scrittura NTFS (usando Captive project)
- Disinfezione di files infetti dalle partizioni di Windows XP

14.1. Cos'è KNOPPIX?

Citazione da http://knopper.net/knoppix:

« KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. »

14.2. Requisiti del sistema

Prima di avviare LinuxDefender, dovete verificare se il vostro sistema ha i seguenti requisiti.

Tipo di processore

Compatibile x86, minimo 166 MHz, ma non attendetevi un alto rendimento in questo caso. Un processore di generazione i686, a 800 MHz sarebbe una scelta migliore.

Memoria

Il valore minimo accettato è 64MB, per una migliore prestazione è consigliato 128MB.

CD-ROM

LinuxDefender si esegue da un CD-ROM, per cui sono richiesti un CD-ROM ed un BIOS in grado di avviarlo.

Connessione Internet

Anche se LinuxDefender funzionerà senza connessione alla rete, le procedure di aggiornamento richiederanno un link HTTP attivo, persino attraverso alcuni

server proxy. Di conseguena, per una protezione aggiornata, la connessione ad Internet è obbligatoria.

Risoluzione grafica

E' consigliata una risoluzione grafica di almeno 800x600 per la amministrazione basata su web.

14.3. Software Incluso

Il BitDefender Rescue CD include i seguenti pacchetti software.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- Amministratore Remoto BitDefender (configurazione basata su web)
- BitDefender Linux Edition (scanner antivirus) + interfaccia GTK
- Documentazione BitDefender (in formato PDF & HTML)
- BitDefender Extras (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Strumenti per il recupero dati e riparazione del sistema, anche per altri sistemi operativi
- Strumenti di analisi della rete e della sicurezza per amministratori di rete
- Amanda backup solution
- thttpd
- Analizzatore del traffico di rete Ethereal, IPTraf IP LAN Monitor
- Nessus network security auditor
- Soluzione per ridimensionamento, salvataggio e recupero di partizioni
- Adobe Acrobat Reader
- Mozilla Firefox Web browser

14.4. Soluzioni di Sicurezza Linux BitDefender

Il CD LinuxDefender include BitDefender SMTP proxy Antispam / Antivirus per Linux, Amministrazione Remota BitDefender (un interfaccia basato su web per configurare il Proxy SMTP BitDefender) e lo scanner antivirus Bitdefender, Linux Edition on-demand.

14.4.1. Proxy SMTP BitDefender

BitDefender per Server di posta Linux – SMTP Proxy è una soluzione d'ispezione di contenuto sicuro, che fornisce protezione antivirus e antispam a livello gateway, mediante la scansione di tutto il traffico di posta per malware conosciuto o sconosciuto.

Come risultato di una proprietà unica della tecnologia, BiDefender per Server di posta è compatibile con la maggioranza delle piattaforme di posta esistenti e certificate “RedHat Ready”.

Questa soluzione Antivirus e Antispam esegue la scansione, disinfetta e filtra il traffico di posta per ogni server di posta esistente, indipendentemente della piattaforma e dal sistema operativo. Il Proxy SMTP BitDefender si attiva all' avvio ed esegue la scansione di tutto il traffico mail in entrata. Per configurare il Proxy SMTP, BitDefender utilizza l’Amministratore Remoto BitDefender , seguendo le seguenti istruzioni.

14.4.2. Amministratore Remoto BitDefender

Potete configurare e gestire i servizi BitDefender in remoto (dopo avere configurato la vostra rete) oppure localmente, seguendo i passi successivi:

1. Avviate il browser Firefox e caricate l' URL dell’Amministratore Remoto BitDefender: https://localhost:8139 (oppure eseguire un doppio click sull’icona dell’Amministratore Remoto BitDefender del vostro desktop)
2. Fare il log con nome utente “bd” e password “bd"
3. Scegliere “SMTP Proxy” dal menu a sinistra
4. Impostare il server Real SMTP e la porta di listening
5. Aggiungere i domini della posta da trasmettere
6. Aggiungere i domini della rete da trasmettere
7. Selezionare “Antispam” dal menu di sinistra per configurare le capacità dell’antispam
8. Selezionare “Antivirus” per configurare le azioni dell’Antivirus BitDefender (cosa fare quando è rilevato un virus, locazione di quarantena)
9. Inoltre potete configurare “le Mail di notifica” e le capacità di logging (“Logger”)

14.4.3. BitDefender Linux Edition

Lo scanner antivirus incluso nel LinuxDefender è integrato direttamente sul desktop. Questa versione utilizza una interfaccia grafica GTK+.

Semplicemente sfogliando il vostro hard disk (o condivisioni remote montate), fare un click con il tasto destro su qualsiasi file o cartella e selezionare “Esamina con BitDefender”. BitDefender Linux Edition eseguirà la scansione degli elementi selezionati e mostrerà un rapporto sullo stato. Per opzioni più dettagliate vedere la documentazione di BitDefender Linux Edition (nella cartella Documentazione oppure nella pagina del manuale) e il programma **/opt/BitDefender/lib/bdc**.

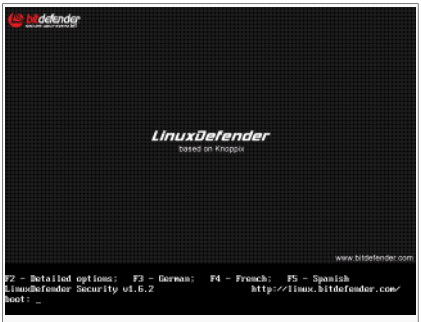
15. Guida a LinuxDefender

15.1. Avvio e Chiusura

15.1.1. Avvio di LinuxDefender

Per avviare il CD, configurare il BIOS del vostro computer per avviarlo dal CD, inserire il CD nel dreve e riavviare il computer. Assicurati che il vostro computer possa avviarsi dal CD.

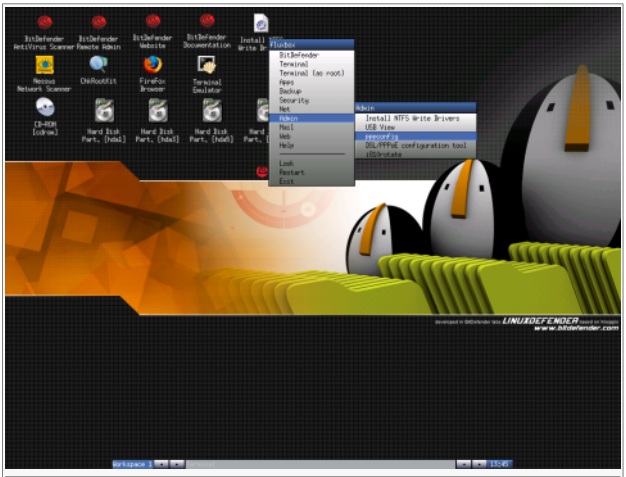
Attendere che venga mostrata la finestra successiva e seguire le istruzioni per avviare LinuxDefender.



Boot Splash Screen

Premere `F2` per le opzioni dettagliate. Premere `F3` per le opzioni dettagliate in tedesco. Premere `F4` per le opzioni dettagliate in francese. Premere `F5` per le opzioni dettagliate in spagnolo. Per un avvio veloce con le opzioni predefinite, è sufficiente premere `ENTER`.

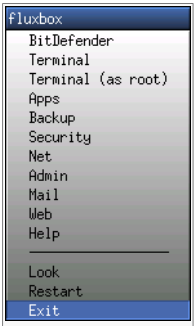
Quando il processo di avvio è finito vedrete il successivo desktop. Adesso puotete iniziare utilizzandoLinuxDefender.



Il Desktop

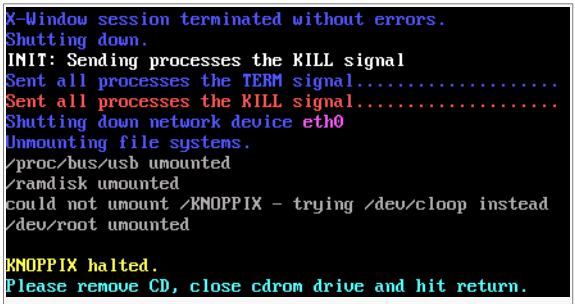
15.1.2. Chiusura di LinuxDefender

Per uscire correttamente da LinuxDefender è consigliato smontare tutte le partizioni montate usando il commando **umount** o cliccando con il tasto destro sulle icone delle partizioni sul desktop e selezionando **Unmount**. Quindi potete chiudere il vostro computer in modo sicuro selezionando **Exit** dal menu di LinuxDefender (tasto destro per aprirlo) o usando il commando **halt** su un terminale.



Scegliere “Uscire”

Quando LinuxDefender avrà chiuso tutti i programmi con successo, mostrerà una schermata come l’immagine seguente. Potrete rimuovere il CD per fare l'avvio dall' hard disk. Adesso potete spegnere oppure riavviare il vostro computer.



Attendere questo messaggio alla chiusura

15.2. Configurare la Connessione a Internet

Se siete in una rete DHCP e avete una scheda di rete ethernet, la connessione Internet dovrebbe già essere rilevata e configurata. Per una configurazione manuale, seguire i passi successivi.

1. Aprire il menu di LinuxDefender (tasto destro) e selezionare **Terminal** per aprire una sessione.
2. Scrivere **netcardconfig** nella sessione aperta per lanciare lo strumento di configurazione della rete.
3. Se la vostra rete utilizza DHCP, selezionare **yes** (se non siete sicuri, chiedere all'amministratore della vostra rete). Altrimenti, vedere sotto.
4. Adesso la connessione di rete dovrebbe essere configurata automaticamente. Potete vedere il vostro IP e le configurazioni della scheda di rete con il comando **ifconfig**.
5. Se avete una IP statica (non dtate utilizzando DHCP), rispondete **No** alla domanda DHCP.
6. Seguire le istruzioni sullo schermo. Se non siete sicuri di cosa scrivere, contattate il vostro amministratore di sistema o della rete per i dettagli.

Se tutto va bene, potete controllare la vostra connessione Internet facendo un “ping” su `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Se state usando una connessione telefonica, scegliere **pppconfig** dal menu Amministrazione di LinuxDefender. Quindi seguire le istruzioni sullo schermo per configurare una connessione ad Internet PPP.

15.3. Aggiornamento di BitDefender

I pacchetti di BitDefender per LinuxDefender utilizano i dischi di memoria del sistema per i files aggiornabili. In questo modo, potete aggiornare tutte le impronte dei virus, motori di scansione o database antispam, anche quando state eseguendo il sistema da un supporto di sola lettura, come il cd LinuxDefender.

Assicurarsi di avere una connessione ad Internet funzionante. Aprire l'Amministratore Remoto di BitDefender e selezionare **Live! Update** dal menu a sinistra. Premere **Update Now** per controllare se sono disponibili nuovi aggiornamenti.

In alternativa, potete emettere il comando seguente in una sessione.

```
# /opt/BitDefender/bin/bd  update
```

Tutti i processi di aggiornamento vengono inseriti nel Registro predefinito di BitDefender. Potete vederlo con il comando seguente.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Se state usando un proxy per le connessioni in uscita, configurate le impostazioni del Proxy nel menu **Live! Update** tasto **Configuration**.

15.4. Scansione Virus

15.4.1. Come posso accedere ai miei dati di Windows?

Supporto Scrittura NTFS

Il supporto scrittura NTFS è disponibile usando il Captive NTFS write project. Aavete bisogno di due file drivers dalla vostra installazione Windows: `ntoskrnl.exe` e `ntfs.sys`. Attualmente, solo i drivers di Windows XP sono supportati. Notare che potete usarli per accedere anche a partizioni Windows 2000/NT/2003.

Installare i Drivers NTFS

Per accedere alle vostre partizioni NTFS di Windows e potere scrivere dei dati su queste, dovete prima installare i drivers NTFS. Se non state usando NTFS per le partizioni Windows, ma FAT, o necessitate solo dell' accesso ai vostri dati, potete montare direttamente i drivers e accedere a Windows come a qualsiasi drive di Linux.

Per aggiungere un supporto per le partizioni NTFS, dovete installare prima i drivers NTFS, dai vostri hard drivers, condivisioni remote, penne USB o dal Aggiornamento Windows. È consigliato usare i drivers da un'ubicazione sicura perché i drivers locali dall' host di Windows possono essere infetti o corrotti.

Eseguire un doppio click sull'icona **Install NTFS Write Drivers** sul desktop per eseguire **BitDefender Captive NTFS Installer**. Se volete installare i drivers dal disco locale, selezionare la prima opzione.

Se i drivers sono in un'ubicazione comune, usare **Quick search** per trovarli.

In alternativa, potete specificare dove si trovano i vostri drivers. Oppure potete scaricare i drivers dall'aggiornamento di Windows SP1.

I drivers non sono installati nel hard disk, ma vengono usati temporaneamente da LinuxDefender per accedere alle partizioni di Windows NTFS. Se il programma installa i drivers NTFS, potete fare un doppio click sulle icone delle Partizioni NTFS del desktop e sfogliare il contenuto. Per un potente file manager, usare il Midnight Commander dal menu di LinuxDefender (o scrivire **mc** in una console).

15.4.2. Come posso eseguire una scansione antivirus?

Sfogliare le vostre cartelle, fare un click con il tasto destro su un file o una directory e selezionare **Send to**. Quindi scegliere **BitDefender Scanner**.

Oppure potete emettere il comanso successivo come root, da un terminale. Il **BitDefender Antivirus Scanner** inizierà con il file o la cartella selezionati come ubicazioni predefinite dove eseguire la scansione.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Quindi fare un click su **Start Scan**.

Se volete configurare l'opzione antivirus, selezionare il tasto **Configure Antivirus** dal pannello sinistro del programma.

15.5. Costruire una Soluzione Istantanea per il Filtraggio delle Mail (TOASTER)

Potete usare LinuxDefender per creare ad hoc una soluzione per il filtraggio delle mail, senza installare alcun software ne modificare il server di posta. L'idea è mettere un sistema LinuxDefender di fronte al vostro server di posta, permettendo a BitDefender

di eseguire la scansione per virus e spam su tutto il traffico SMTP e trasmetterlo al server di posta reale.

15.5.1. Prerequisiti

Sarà necessario un PC con CPU Pentium 3 o compatibile, almeno 256 MB di RAM e unità CD/DVD da dove farlo partire. Sarà il sistema LinuxDefender a dover ricevere tutto il traffico SMTP al posto del server di posta reale. Ci sono molti modi di fare questa configurazione.

1. Cambiare l'IP del vostro server di posta reale ed assegnare la vecchia IP al sistema LinuxDefender
2. Cambiare i records DNS in modo tale che l'entrata MX per i vostri domini sia puntata al sistema LinuxDefender
3. Configurare i vostri Clients di posta per usare il nuovo sistema LinuxDefender come server SMTP
4. Cambiare le impostazioni del firewall in modo che inoltri / reindirizzi tutte le connessioni SMTP verso il sistema LinuxDefender invece del server di posta reale

Nessuno dei temi sopra-citati sarà spiegato da LinuxDefender. Per informazioni detagliate dovrete consultare le guide di rete Linux e la documentazione su Netfilter.

15.5.2. L'email Toaster

Lanciare il CD di LinuxDefender e attendere finche il sistema Windows X sia caricato e funzionante.

Per configurare il Proxy SMTP BitDefender, eseguire un doppio click sull'icona **BitDefender Remote Admin** dal desktop. Apparirà la seguente finestra. Utilizzare nome utente `bd` e password `bd` per accedere l'Amministratore Remoto BitDefender.

Dopo l'acesso, sarete nelle condizioni di potere configurare il Proxy SMTP BitDefender.

Scegliere **SMTP Proxy** per configurare il server di posta reale che volete proteggere contro spam e virus.

Selezionare **Email domains** per inserire tutti i domini di posta dai quali accettare le email.

Premere **Add Email Domain** o **Add Bulk Domains** e seguire le istruzioni per impostare il collegamento ai domini di posta.

Selezionare **Net domains** per inserire tutte le reti dove volete trasmettere le email.

Premere **Add Net Domain** o **Add Bulk Net Domains** e seguire le istruzioni per impostare il collegamento ai domini di rete.

Selezionare **Antivirus** dal menu di sinistra, per scegliere cosa fare quando un virus viene trovato, e per configurare altre opzioni antivirus.

Adesso, tutto il traffico SMTP è esaminato e filtrato da BitDefender. Di default, tutti i messaggi infetti saranno puliti o cestinati e tutti i messaggi spam rilevati da BitDefender saranno segnati nell' Oggetto con la parola `[SPAM]`. L'intestazione (`X-BitDefender-Spam: Yes/No`) viene aggiunta su tutte le email per facilitare il filtraggio dal lato client.

15.6. Eseguire una Verifica della Sicurezza di Rete

Assieme ale capacità anti-malware, recupero dati e filtraggio mail, LinuxDefender arriva con un set di strumenti che eseguono una revisione approfondita della sicurezza di rete & host. Anche l'analisi forense dei sistemi compromessi è possibile usando gli strumenti di sicurezza inclusi nel LinuxDefender. Leggete questa breve guida per imparare come avviare una revisione veloce della sicurezza dei vostri host o reti.

15.6.1. Controllo per i Rootkits

Prima di iniziare una analisi di sicurezza sui computers in rete, assicurarsi che l' host LinuxDefender non sia compromesso. Potete eseguire la scansione degli hard-disks installati, come descritto nella **Scan for viruses** oppure eseguire la scansione Rootkits per Unix.

Prima di tutto, montare tutte le partizioni del vostro hard disk, facendo un doppio click sulle loro icone nel desktop o usando il commando **mount** nella console. Quindi eseguire un doppio click sull'icona **ChkRootKit** per controllare il contenuto del CD o lanciare il comando **chkrootkit** nella console, usando `-r NEWROOT` il parametro per specificare la nuova / (root) directory dell' host.

```
# chkrootkit -r /dev/hda3
```

Se viene trovato un rootkit, chkrootkit mostrerà la scoperta in **GRASSETTO**, usando lettere maiuscole.

15.6.2. Nessus – Lo Scanner della Rete

> Nessus è lo scanner open-source di vulnerabilità più popolare, usato in più di 75.000 organizzazioni in tutto il mondo. Molte delle organizzazioni più gandi al mondo stanno ottenendo un significativo risparmio sui costi mediante l'uso di Nessus per la revisione di dispositivi ed applicazioni commercialmente critici per l'azienda.
>
> —*www.nessus.org*

Nessus è lo scanner open-source di vulnerabilità più popolare, usato in più di 75.000 organizzazioni in tutto il mondo. Molte delle organizzazioni più gandi al mondo stanno ottenendo un significativo risparmio sui costi mediante l'uso di Nessus per la revisione di dispositivi ed applicazioni commercialmente critici per l'azienda.

Fare un doppio click sull'icona **Nessus Security Scanner** sul desktop, o eseguire **startnessus** da un terminale. Attendere finche viene mostrata la finestra seguente. In base alla configurazione e alle risorse hardware, il caricamento di Nessus può richiedere fino a 10 minuti, con oltre i 5.000 plugins contenenti i database di vulnerabilità. Utilizzare il nome utente `knoppix` e la password `knoppix` per loggarsi.

Cliccare **Target selection** ed inserire l'indirizzo IP del computer o i nomi degli hosts sui quali dovete eseguire la scansione per le vulnerabilità. Assicurarsi di personalizzare tutte le opzioni di scansione in accordo con la rete o la configurazione del vostro sistema, prima di iniziare la scansione, per risparmiarvi tonnellate di banda e risorse ed avere un risultato più accurato. Quindi cliccare su **Start the scan**.

Quando il processo di scansione è stato completato, Nessus mostra le scoperte ed i relativi suggerimenti. Potete salvare il rapporto in diversi formati, anche HTML con grafici e torte. Il rapporto salvato può essere visualizzato nel vostro browser preferito.

15.7. Controlla lo stato della RAM del vostro sistema

Solitamente, quando il vostro sistema ha un comportamento inaspettato(si blocca o si riavvia da solo ogni tanto), può essere dovuto ad un problema di memoria. Potete controllare i moduli della vostra RAM con il programma **memtest** così come descritto sotto.

Avviare il computer dal CD LinuxDefender. Scrivere **memtest** al momento dell' avvio e premere Invio.

Il programma Memtest inizierà immediatamente eseguendo numerosi tests per controllare lo stato della memoria. Potete configurare quali tests eseguire ed altre opzioni del Memtest, premendo `c`.

Un'esecuzione completa del Memtest può richiedere fino a 8 ore, in base alla capacità e la velocità dei vostri sistemi RAM. È consigliato lasciare eseguire a Memtest tutti i tests per controllare completamente eventuali di RAM. Potete uscire in qualsiasi momento, premendo `ESC`.

Se intendete acquistare un nuovo Hardware (un sistema completo o soltanto alcuni componenti), è consigliato utilizzare LinuxDefender ed il memtest per controllare eventuali errori o problemi di compatibilità.

Ottenere aiuto

16. Supporto

16.1. Dipartimento di Supporto

Come fornitore di valore, BitDefender si opera al massimo per offrire ai propri clienti un alto livello di supporto, veloce ed accurato. Il Centro di Supporto (che potete contattare all'indirizzo fornito di seguito) è in continuo aggiornamento con le ultime e nuove descrizioni dei virus. In questo modo avrete sempre una risposta puntuale alle vostre domande / richieste.

Con BitDefender, è considerata prioritaria l'ottimizzazione del tempo e della spesa necessari alla sicurezza degli utenti, con la fornitura dei prodotti più avanzati ai migliori prezzi. Inoltre crediamo che un business di successo sia basato in una buona comunicazione ed un impegno costante nel dare supporto all'utente.

Potete chiedere supporto in qualsiasi momento a <support@bitdefender.com>. Per una risposta veloce, vi chiediamo di includere nella vostra mail il maggior numero di dettagli possibile sul vostro BitDefender, sul sistema e di descrivere i problema con la maggior accuratezza possibile.

16.2. Aiuto On-line

16.2.1. BitDefender Knowledge Base(Archivio di informazione BitDefender)

L' Archivio di informazione BitDefender è un deposito di informazioni sui prodotti BitDefender. Immagazzina, in un formato facilmente accessibile, rapporti sui risultati del supporto tecnico in corso e attività di disinfezione dei team di supporto e sviluppo di BitDefender , insieme a più articoli sulla prevenzione dai virus, la gestione delle soluzioni BitDefender e spiegazioni dettagliate, oltre a molti altri articoli.

L'Archivio D'informazione BitDefender è aperto al pubblico e usufruibile gratuitamente. Questa ricchezza di informazioni è uno dei tanti modi di fornire ai clienti di BitDefender le conoscenze tecniche e la comprensione necessarie. Tutte le richieste valide di informazione o rapporti su difetti, provenienti da clienti di BitDefender trovano la loro esatta collocazione nell'Archivio di informazione BitDefender, come rapporti di disinfezione, i modi di aggirare le truffe, oppure gli articoli informativi, in modo di implementare i files di aiuto al prodotto.

L' Archivio di informazione BitDefender è disponibile in qualsiasi momento all'indirizzo: http://kb.bitdefender.com.

16.3. Contatti

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 10 anni SOFTWIN ha acquisito una reputazione inestimabile superando le aspettative di clienti e partners, sforzandosi costantemente per una comunicazione sempre più efficiente. Se avete delle domande o richieste, non esitare a contattarci.

16.3.1. Indirizzi Web

Dipartimento vendite: <sales@bitdefender.com>
Supporto tecnico: <support@bitdefender.com>
Documentazione: <documentation@bitdefender.com>
Programma Partner: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Rapporti con i Media: <pr@bitdefender.com>
Opportunità di lavoro: <jobs@bitdefender.com>
Invio Virus: <virus_submission@bitdefender.com>
Invio Spam: <spam_submission@bitdefender.com>
Report Abuse: <abuse@bitdefender.com>
Pagina web prodotto: http://www.bitdefender.com
Archivi ftp del prodotto: ftp://ftp.bitdefender.com/pub
Distributori locali: http://www.bitdefender.com/partner_list
Archivio di Informazione BitDefender: http://kb.bitdefender.com

16.3.2. Uffici di Filiale

Gli uffici di BitDefender sono pronti a rispondere a qualunque richiesta relativamente alle loro aree di operazione, sia in materia commerciale che generale. I loro rispettivi indirizzi e contatti sono elencati sotto.

Germany

Softwin GmbH
Quartier generale Europa Occidentale
Karlsdorferstrasse 56
88069 Tettnang
Germany
Tel: +49 7542 9444 44
Fax: +49 7542 9444 99

E-mail: <info@bitdefender.com>
Vendite: <sales@bitdefender.com>
Web: http://www.bitdefender.com
Supporto tecnico: <support@bitdefender.com>

Italy

Shaft Srl
Torino
B1 1BD
Phone: +39 011 659 60 87
Fax: +39 011 833 86 59
E-mail: <info@bitdefender.com>
Vendite: <sales@bitdefender.com>
http://www.shaft.it
Supporto tecnico: <support@bitdefender.com>

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Supporto tecnico: <support@bitdefender.com>
Servizio Clienti: 954-776-6262
Web: http://www.bitdefender.com

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest

Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

Glossario

ActiveX

ActiveX è una modalità di scrittura di Programmi che possano essere richiamati da altri Programmi e sistemi operativi. La tecnologia ActiveX è utilizzata con 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 ed 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

L' adware è spesso combinato con un' applicazione host che è offerta senza spese quando l'utente accetta l'adware. Considerando che 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, i pop-up di avvertimento possono diventare un fastidio, ed in alcuni casi riduce le performance del sistema. Inoltre, l'informazione che viene raccolta da queste applicazioni può causare inconvenienti riguardo la privacy degli utenti non sempre completamente informati sui termini dell'accordo di licenza.

Archivio

Disco, nastro o cartella che contiene files memorizzati.

Un file che contiene uno o più files in forma compressa.

Backdoor

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.

Settore di Boot

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.

Virus di Boot

Virus che infetta il settore di boot 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 nella memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.

Browser

Abbreviazione di Web browser, un'applicazione software utilizzata per localizzare e visualizzare pagine Web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono Browser grafici, ovvero in grado di visualizzare sia la grafica che il testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, inclusi suoni e animazioni, nonostante richiedano i plug-in per alcuni formati.

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.

Cookie

Nell'industria di Internet, i cookies vengono descritti come piccoli files contenenti informazioni relative ai computers individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia dei vostri interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire direttamente ciò che si dichiara essere di proprio interesse. 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. Dall'altra parte, 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 " SKU number" (il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Disk drive

È un dispositivo che legge e scrive dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy ospita i flpopy disks.

I drive di disco possono essere sia interni (incorporati all'interno di un computer) che esterni (collocati in un meccanismo separato e connesso al computer).

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 on-line sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

E-mail

Posta elettronica. Servizio che invia messaggi ai computers attraverso reti locali o globali.

Eventi

Azione oppure evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come un click con il mouse o premere un tasto sulla tastiera oppure accadimenti del sistema, come l'esaurimento della memoria.

Falso positivo

Si verifica quando una scansione individua un file come come infetto quando di fatto non lo è.

Estensione del nome di un file

La 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 del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScipt, "txt" per testi arbitrari.

Euristico

Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche impronte dei virus. Il vantaggio della scansione euristica è di non venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".

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.

Applet Java

Programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisognerà 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 Applets differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, nonostante gli applets vengano lanciati sul client, non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applets sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Macro virus

Tipo di virus del computer che è 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 questo viene aperto.

Client mail

La client e-mail è un'applicazione che vi consente di inviare e ricevere e-mail.

Memoria

Aree di immagazzinaggio interne al computer. Il termine memoria identifica l'immagazzinaggio dati sotto forma di chip; la parola storage viene utilizzata per la memoria su nastri o su 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 impronte di virus. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare un virus e non genera falsi allarmi.

Programmi impaccati

File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che impacca i files potrebbe sostituire gli spazi dei caratteri con un carattere speciale space_series seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.

Percorso

I percorsi esatti per raggiungere un file su un computer. Questi percorsi vengono solitamente descritti attraverso il sistema di casellario gerarchico dall'alto al basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazione tra due computer.

Phishing

L'atto d'inviare una mail ad un utente fingendo di essere una ditta legittima ed affermata, nel tentativo di truffare l'utente, facendogli cedere informazione private che verranno usati per furti d'identità. La e-mail indirizza gli utenti a visitare una pagina Web, dove viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto in banca. In ogni caso, la pagina Web è falsa e organizzata soltanto per rubare le informazioni dell' utente.

Virus Polimorfico

Virus che modifica la propria forma da ogni file che infetta. Non disponendo di caratteristiche binarie costanti, questi virus sono difficili da identificare.

Porta

Interfaccia su un computer dalla quale è possibile connettere un supporto. I Personal Computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitors e tastiere. Esternamente i Personal Computer hanno porte per la connessione dei modems, delle stampanti, del mouse e altri supporti periferici.

Nelle reti TCP/IP e UDP, un punto di arrivo ad una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

File di rapporto

File che elenca le azioni avvenute. BitDefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi, i files esaminati, quanti files infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore ad un sistema. 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 loro presenza in modo da non dover essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono maligni per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file crirtici utilizzando rootkit. Comunque, essi vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati al 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 log ed evitare il rilevamento.

Script

Altro termine per macro o bat ch file, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiai e-mail non richiesta.

Spyware

Qualsiasi software che accede alla connessione internet dell'utente senza che questo se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware arrivano tipicamente come un componente nascosto di programmi freeware o shareware che possono essere scaricati da Internet. Tuttavia, deve essere segnalato che la maggioranza delle applicazioni shareware o freeware non arrivano con spyware. Una volta installato, lo spyware esegue il monitoraggio dell'attività dell' utente su Internet e trasmette questa informazione di nascosto a qualcun altro. Lo spyware può anche raccogliere informazioni su indirizzi mail e addirittura passwords e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano inconsapevolmente installando applicazioni diverse. Un modo comune per diventare vittima dello spyware è scaricare alcuni files peer-to-peer scambiando prodotti che sono disponibili oggi.

Non rispettando l'etica e la privacy, lo spyware approfitta dell' utente usando risorse di memoria del computer "assorbendo" larghezza di banda dal momento in cui invia informazioni alla sua "base" utilizzando la connessione internet dell' utente. Dato che lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in sottofondo (background) possono portare alla caduta del sistema o alla sua instabilità.

Elementi di startup

Qualsiasi file posizionato in questa cartella si aprirà quando il computer sarà avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il file stesso.

Barra di sistema

Introdotta con Windows 95, la barra di sistema è situata nella barra strumenti di Windows (solitamente in basso vicino all'orologio) e contiene icone miniaturizzate per un semplice accesso alle funzioni di sistema, come ad esempio il fax, la stampante, il modem, il volume ed altro. Fare doppio click o fare click con il tasto destro su un'icona per vedere ed accedere ai dettagli ed ai controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di networking largamente utilizzati su Internet che consentono le comunicazioni attraverso le reti interconnesse di computers con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computers e le convenzioni per connettere le reti e il traffico di instradamento.

Trojan

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 del vostro computer ma che al contrario li introduce.

Il termine deriva dalla storia dell'Iliade di Omero, dove 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 catturare Troia.

Aggiornamento

La 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 vostro computer; diversamente non sarà possibile installare l'aggiornamento.

BitDefender dispone del proprio modulo che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Virus

Programma o parte di codice caricato sul vostro computer a vostra insaputa e che viene eseguito contro la vostra volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus del computer sono creati dall'uomo. E' 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.

Definizione di virus

Caratteristica binaria di un virus, utilizzata dal programma antivirus al fine di rilevare ed eliminare il virus stesso.

Worm(baco)

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.