

*bit*defender



ANTIVIRUS 2008

Manuale utente

BitDefender Antivirus 2008

Manuale utente

Pubblicato 2007.09.11

Copyright© 2007 BitDefender

Avvertenze Legali

Tutti I diritti riservati. Nessuna parte di questo manuale può essere riprodotta o trasmessa in alcuna forma o tramite qualsiasi strumento, elettronico o meccanico, incluse fotocopie, registrazioni, o attraverso qualsiasi informazione di archivio o sistema di recupero dati, senza un permesso scritto della BitDefender, ad eccezione di brevi citazioni nelle rassegne menzionando la provenienza. Il contenuto non può essere modificato in nessun modo.

Avvertenze e Limiti. Questo prodotto e la sua documentazione sono protetti dal Copyright. L'informazione su questo documento è fornita sul concetto «così come è» senza garanzia. Sebbene ogni precauzione è stata adottata nella preparazione di questo documento, gli autori non hanno alcun obbligo nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causati o che si presume essere stati causati, direttamente o indirettamente, dalle informazioni contenute in questo lavoro.

Questo manuale contiene collegamenti a siti Internet terze parti, che non sono sotto il controllo della BitDefender, conseguentemente la BitDefender non è responsabile per il contenuto di qualsiasi sito collegato. Se accedi a siti Internet di terze parti, menzionati in questo manuale, lo farai assumendotene tutti i rischi. BitDefender fornisce tali collegamenti solo come una convenienza, e l'inclusione dei collegamenti non implica che BitDefender approva o accetta alcuna responsabilità per il contenuto di questi siti di terze parti.

Marchi Registrati. Nomi e marchi registrati possono essere citati in questo manuale. Tutti i marchi registrati e non in questo documento sono di sola proprietà dei rispettivi proprietari.



Sommario

Licenza e garanzia	vii
Prefazione	xi
1. Convenzioni usate in questo manuale	xi
1.1. Convenzioni tipografiche	xi
1.2. Avvertenze	xii
2. Struttura del manuale	xii
3. Richiesta di commenti	xiii
Installazione	1
1. Installazione di BitDefender Antivirus 2008	2
1.1. Requisiti del sistema	2
1.2. Fasi per l'installazione	3
1.3. Assistente per il Setup iniziale	5
1.3.1. Passo 1/6 - Registrare Antivirus BitDefender 2008	6
1.3.2. Passo 2/6 - Creare un Account BitDefender	7
1.3.3. Passo 3/6 - Imparare riguardo a RTVR	9
1.3.4. Passo 4/6 - Seleziona l'azione	10
1.3.5. Passo 5/6 - Attendere il Completamento dei Compiti	11
1.3.6. Passaggio 6/6 - Sommario	12
1.4. Upgrade	12
1.5. Riparare o Rimuovere BitDefender	13
Amministrazione di base	15
2. Iniziando	16
2.1. Scansione Manuale di BitDefender	18
3. Stato di Sicurezza	19
3.1. Tasto Stato Antivirus	20
3.2. Tasto Stato della Privacy	21
3.3. Tasto Stato Antiphishing	22
3.4. Tasto Stato dell'Aggiornamento	22
4. Funzioni Veloci	24
4.1. Sicurezza	24
4.1.1. Aggiornamento	24
4.1.2. Scanner di BitDefender	24
5. Storia	29
Amministrazione della Sicurezza Avanzata	31

6. Iniziando	32
6.1. Configurazione delle Impostazioni Generali	33
6.1.1. Impostazioni Generali	33
6.1.2. Impostazioni Report sui Virus	34
6.1.3. Gestione Impostazioni	35
6.2. Utilizzo della Barra delle Attività di Scansione	35
7. AntiVirus	37
7.1. Scansione all'accesso	37
7.1.1. Configurazione del Livello di Protezione	38
7.1.2. Livello di Protezione Personalizzato	39
7.1.3. Disattivazione Virus Shield	43
7.2. Scansione a richiesta	43
7.2.1. Impostazioni della Scansione	45
7.2.2. Utilizzo del Menu Rapido	47
7.2.3. Creazione delle Funzioni di Scansione	48
7.2.4. Configurare un Compito di Scansione	48
7.2.5. Oggetti di Scansione	58
7.2.6. Visualizzazione dei Registri di Scansione	64
7.3. Oggetti esclusi dalla Scansione	65
7.3.1. Esclusione dei Percorsi dalla Scansione	67
7.3.2. Esclusione delle Estensioni dalla Scansione	69
7.4. Area di Quarantena	72
7.4.1. Gestione dei File in Quarantena	72
7.4.2. Configurazione delle Impostazioni di Quarantena	73
8. Controllo Privacy	75
8.1. Stato Controllo Privacy	75
8.1.1. Controllo Privacy	76
8.1.2. Protezione Antiphishing	77
8.2. Impostazioni Avanzate - Controllo Identità	78
8.2.1. Creazione delle Regole d'Identità	79
8.2.2. Definizione Eccezioni	82
8.2.3. Amministrazione delle regole	83
8.3. Impostazioni Avanzate - Controllo Registry	84
8.4. Impostazioni Avanzate - Controllo Cookie	86
8.4.1. Assistente per la Configurazione	88
8.5. Impostazioni Avanzate - Controllo Script	90
8.5.1. Assistente per la Configurazione	92
8.6. Sistema di Informazione	92
8.7. Barra degli Strumenti Antiphishing	94
9. Aggiornamento	96
9.1. Aggiornamento Automatico	97
9.1.1. Richiedere un aggiornamento	98
9.1.2. Disattivare Aggiornamento Automatico	98

9.2. Impostazioni dell'Aggiornamento	99
9.2.1. Impostare Ubicazioni Aggiornamento	100
9.2.2. Configurazione Aggiornamento Automatico	101
9.2.3. Configurazione Aggiornamento Manuale	102
9.2.4. Configurazione delle Impostazioni Avanzate	102
9.2.5. Gestione Proxies	103

BitDefender Rescue CD **105**

10. Informazioni generali sul prodotto BitDefender™ **106**

10.1. Requisiti del sistema	106
10.2. Software Incluso	107

11. BitDefender Rescue CD fai-da-te. **110**

11.1. Avviare BitDefender Rescue CD	110
11.2. Arrestare BitDefender Rescue CD	111
11.3. Come posso eseguire una scansione antivirus?	112
11.4. Come posso salvare ai miei dati?	113

Ottenere aiuto **116**

12. Supporto **117**

12.1. BitDefender Knowledge Base(Archivio di informazione BitDefender)	117
12.2. Chiedere Aiuto	118
12.2.1. Vai al Web Fai-da-te	118
12.2.2. Aprire un ticket di supporto	118
12.3. Contatti	119
12.3.1. Indirizzi Web	119
12.3.2. Uffici di Filiale	119

Glossario **121**

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 BITDEFENDER, per l'utilizzo dei prodotti Software BITDEFENDER 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 né 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. BITDEFENDER 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.

SCADENZA. Il prodotto cesserà di compiere le sue funzioni immediatamente dopo la scadenza della licenza.

UPGRADE (AGGIORNAMENTO). Se BitDefender è identificato come un upgrade, per usarlo devi essere stato autorizzato precedentemente ad utilizzare un prodotto classificato da BITDEFENDER 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 (inclusendo 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 BITDEFENDER. 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. BITDEFENDER 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, BITDEFENDER, a sua discrezione, potrà sostituire il supporto, oppure rimborsare l'importo pagato per l'acquisto, a fronte di una ricevuta. BITDEFENDER non garantisce che BitDefender

sarà sempre privo di errori o che gli errori verranno comunque corretti. BITDEFENDER non garantisce che BitDefender soddisferà le necessità dell'utilizzatore. BITDEFENDER CON LA PRESENTE NEGA QUALSIASI ALTRA GARANZIA PER BITDEFENDER, SIA ESPlicita CHE IMPLICITa. LA SUDETTA GARANZIA E' ESCLUSIVA E SOSTITUISCE TUTTE LE ALTRE GARANZIE, SIA ESPlicitE CHE IMPLICITE, INCLUDENDO LE GARANZIE DI COMMERCIALIZZABILITA', 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. BITDEFENDER QUI DISCONOSCE ESPRESSAMENTE QUALSIASI GARANZIA E CONDIZIONE IMPLICITa, INCLUSO, SENZA LIMITAZIONE, LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, 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 BITDEFENDER 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 BITDEFENDER 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 BITDEFENDER 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'invalidità non avrà effetto sulla validità delle porzioni residue di questo Accordo.

BitDefender e i lochi BitDefender sono marchi registrati di BITDEFENDER. 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 BITDEFENDER 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.

BITDEFENDER 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 BITDEFENDER.

Contattare BITDEFENDER, 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 AntiVirus v10** come soluzione di sicurezza per i loro personal computers. L'informazione presentata in questo libro è indicata non solo a esperti di computer, ma è accessibile a tutti quelli capaci di lavorare con Windows.

In questo manuale c'è la descrizione di **BitDefender Antivirus 2008**, il team che lo ha sviluppato vi guiderà attraverso il processo di installazione e vi insegnerà come configurarlo. Avrete modo di vedere come utilizzare **BitDefender Antivirus 2008 Standard**, come aggiornarlo, di provarlo e personalizzarlo. Imparerete a sfruttare BitDefender nel modo migliore.

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. xi)	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 aggiuntive 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 correlati.



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 è composto da diverse parti contenenti gli argomenti importanti. Inoltre, viene anche fornito un glossario per chiarire alcuni termini tecnici.

Installazione. Di seguito le istruzioni passo-passo per installare BitDefender su una postazione di lavoro (workstation). Questa parte del manuale è una guida esaustiva sull'installazione di **BitDefender Antivirus 2008**. Sarete guidati attraverso tutto il processo, iniziando con i prerequisiti per l'installazione. Alla fine è descritta la procedura di disinstallazione nel caso in cui sia necessario disinstallare BitDefender.

Amministrazione di base. Descrizione dell'amministrazione di base e manutenzione di BitDefender.

Amministrazione della Sicurezza Avanzata. Una presentazione dettagliata delle capacità di sicurezza fornite da BitDefender. I capitoli spiegano in dettaglio tutte le opzioni del console delle impostazioni avanzate. Vi spieghiamo come configurare ed utilizzare tutti i moduli di BitDefender in modo da proteggere efficacemente il vostro computer da ogni tipo di minaccia malware (virus, spyware, rootkit ed altro).

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.

Installazione

1. Installazione di BitDefender Antivirus 2008

La sezione **BitDefender Antivirus 2008 installation** di questa guida all'utente contiene i seguenti punti:

- **Requisiti di sistema**
- **Fasi dell'installazione**
- **Assistente per il Setup iniziale**
- **Upgrade**
- **Riparare o Rimuovere BitDefender**

1.1. 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:

- Piattaforma operativa: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (o superiore)

Windows 2000

- Processore 800 MHz o superiore
- Minimo 256 MB di memoria RAM (consigliati 512 MB)
- Minimo 60 MB di spazio disponibile su hard disk

Windows XP

- Processore 800 MHz o superiore
- Minimo 256 MB di Memoria RAM (consigliati 1 GB)
- Minimo 60 MB di spazio disponibile su hard disk

Windows Vista

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

BitDefender Antivirus 2008 può essere scaricato per una valutazione all'indirizzo: <http://www.bitdefender.com> il sito di BITDEFENDER corporate, dedicato alla sicurezza dei dati.

1.2. Fasi per l'installazione

Individuare il file di setup e cliccare due volte. Verrà lanciato l'assistente che vi guiderà attraverso il processo di setup:

Prima di lanciare l'assistente di setup, BitDefender controllerà la disponibilità di versioni più recenti del pacchetto di installazione. Se ci fosse una versione più recente disponibile, vi verrà proposto di scaricarla. Cliccare su **Sì** per scaricare la versione più recente oppure **No** per continuare con l'installazione della versione disponibile nel file di setup.



Seguire questi passi per installare BitDefender Antivirus 2008:

1. Selezionare **Avanti** per continuare oppure **Cancella** se si desidera interrompere l'installazione.
2. Selezionare **Avanti**.

L'Antivirus v10 di BitDefender vi avvisa se avete altri prodotti antivirus installati sul vostro computer. Selezionare **Rimuovi** per disinstallare il corrispondente prodotto. Se si desidera continuare senza rimuovere i prodotti rilevati, selezionare **Avanti**.



Avvertimento

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

3. 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.
4. Per default, Antivirus BitDefender 2008 verrà installato in C:\Program Files\BitDefender\BitDefender 2008. Se si desidera modificare il percorso d'installazione, fare click su **Sfoggia**, quindi selezionare, la cartella dove si desidera installare Antivirus BitDefender 2008.

Selezionare **Avanti**.

5. Selezionare le opzioni relative al processo di installazione. Alcune di loro verranno selezionate di default:
 - **Aprire il file readme** - per aprire il file readme al termine dell'installazione.
 - **Aggiungi un collegamento sul desktop** - per inserire un collegamento sul desktop al termine dell'installazione.
 - **Espellere CD al termine dell'installazione** - per che il CD venga espulso al termine dell'installazione; questa opzione apparirà se installerete il prodotto dal CD.
 - **Disattiva Windows Defender** - per disattivare Windows Defender; questa opzione compare solo su Windows Vista.

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



Importante

Durante il processo di installazione apparirà un **assistente**. L'assistente vi aiuterà a registrare il vostro **Antivirus BitDefender 2008**, creare un account BitDefender ed impostare BitDefender per eseguire importanti funzioni di sicurezza.. Completare il processo di configurazione assistita per accedere al passo successivo.

6. 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 `BitDefender in Programmi` che contiene la sottocartella `BitDefender 2008`.



Nota

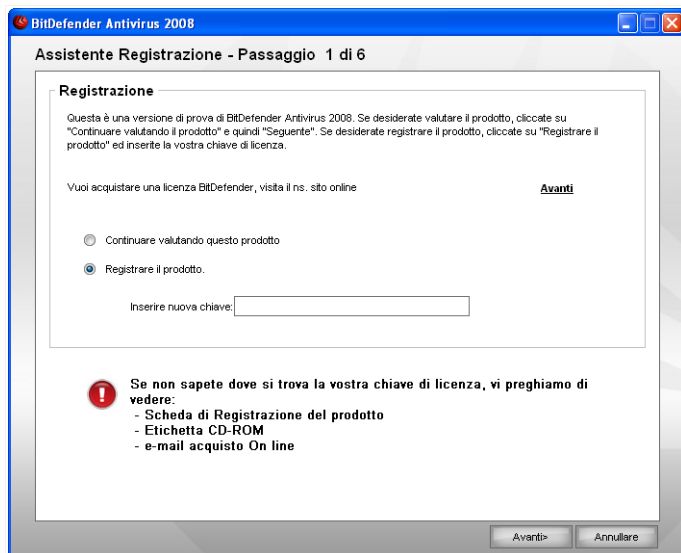
Potrebbe essere richiesto di riavviare il sistema in modo che l'assistente di setup completi il processo di installazione.

1.3. Assistente per il Setup iniziale

Durante il processo di installazione apparirà un assistente. L'assistente vi aiuterà a registrare il vostro **BitDefender Antivirus 2008**, creare un account BitDefender ed impostare BitDefender per eseguire importanti funzioni di sicurezza.

Completare il processo non è obbligatorio; in ogni caso vi consigliamo di farlo per guadagnare tempo e assicurare il vostro sistema prima che BitDefender Antivirus 2008 venga installato.

1.3.1. Passo 1/6 - Registrare Antivirus BitDefender 2008



Registrazione

Scegliere **Registrare il prodotto** per registrare l'**Antivirus v10 di BitDefender**.
Digitare la chiave licenza nel campo **Inserire la nuova chiave**.

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

1.3.2. Passo 2/6 - 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. Selezionare **Creare un nuovo Account BitDefender** e fornire le informazioni richieste. I dati che fornite qui resteranno riservati.



Nota

Se desiderate creare un account più tardi, selezionare l'opzione corrispondente.

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.

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

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.

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

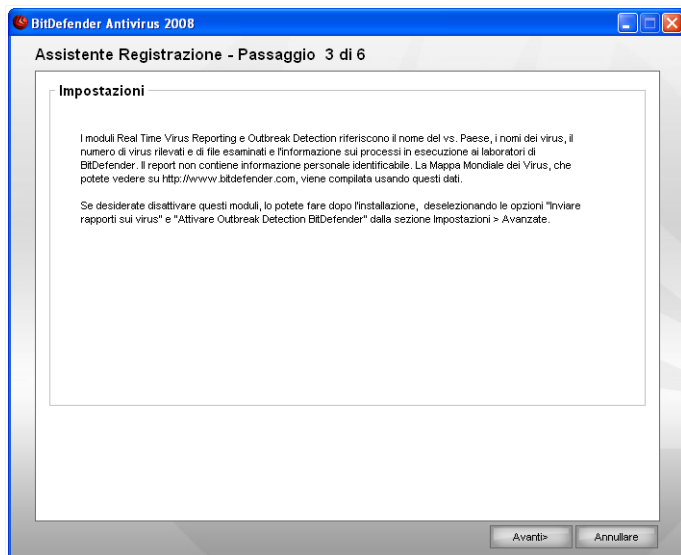
Ho già un account BitDefender

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 **Avanti**. Cliccate su **Ok** per inserire di nuovo la password o su **Annulla** per uscire dall'assistente.

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

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

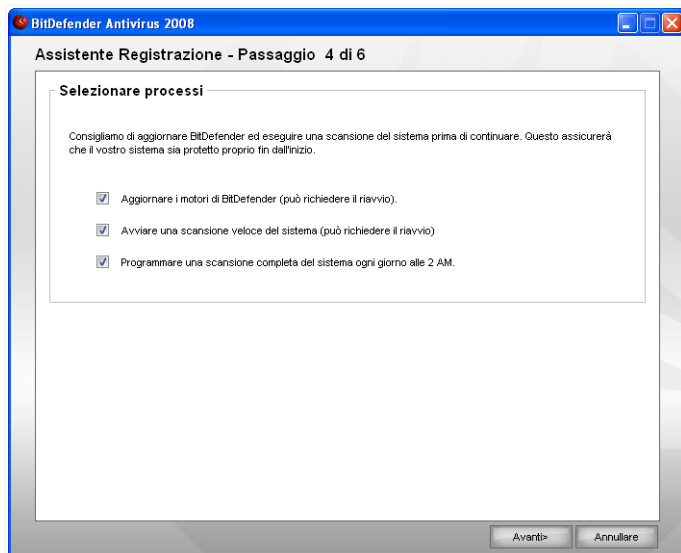
1.3.3. Passo 3/6 - Imparare riguardo a RTVR



Sistema di Informazione

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

1.3.4. Passo 4/6 – Seleziona l'azione



Selezione azioni

Impostate l'Antivirus v10 di BitDefender per eseguire compiti importanti per la sicurezza del vostro sistema.

Sono disponibili le seguenti opzioni:

- **Aggiornamento motori BitDefender (può richiedere il riavvio)** - durante il prossimo passo, verrà eseguito un aggiornamento dei motori BitDefender per proteggere il vostro computer contro le ultime minacce.
- **Eseguite una scansione rapida del sistema (può richiedere il riavvio)** - durante il prossimo passo, verrà eseguita una scansione rapida del sistema per consentire a BitDefender di assicurarsi che i vostri file nelle cartelle di `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.



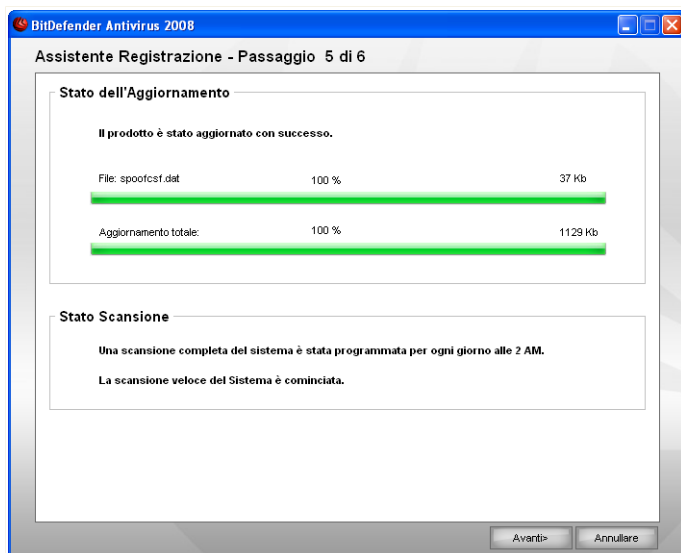
Importante

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.

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

1.3.5. Passo 5/6 – Attendere il Completamento dei Compiti

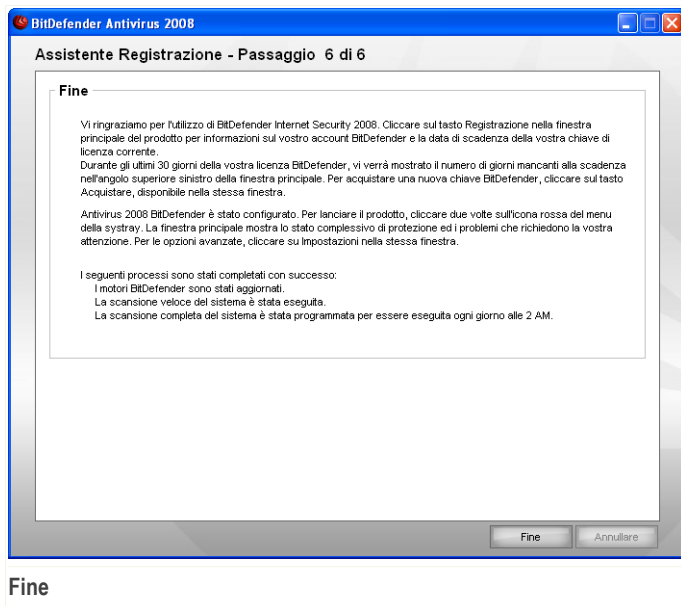


Stato dei Task

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

Cliccare su **Avanti** per continuare o su **Annulla** per uscire dall'assistente.

1.3.6. Passaggio 6/6 - Sommario



Questo è l'ultimo passo del processo di configurazione.

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

1.4. Upgrade

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

- **Installare senza rimuovere la versione precedente – solo per la versione 8 o superiore, escluso Internet Security.**

Fare doppio click sul file di setup e seguire il processo descritto nella sezione «*Fasi per l'installazione*» (p. 3).



Importante

Durante il processo di installazione apparirà un messaggio di errore causato dal servizio FilesSpy. Cliccare **OK** per continuare l'installazione.

- **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. 3).



Importante

Prima di eseguire l'aggiornamento upgrade da BitDefender v8 o superiore, consigliamo di salvare le impostazioni di BitDefender, l'elenco Amici e l'elenco Spammers. Sarà possibile caricarli dopo che il processo di upgrade sarà stato completato.

1.5. Riparare o Rimuovere BitDefender

Se si desidera riparare o rimuovere **Antivirus BitDefender 2008**, selezionare dal menu di avvio di Windows: **Start** → **Programmi** → **BitDefender 2008** → **Riparare o Rimuovere**.

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

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



Importante

Prima di riparare il prodotto, consigliamo di salvare l'elenco degli Amici e l'elenco degli Spammers. Potete inoltre salvare le impostazioni di BitDefender ed il database Bayesian. Una volta completato il processo di riparazione, si potranno ricaricare.

Scegliendo di riparare BitDefender, la seguente nuova finestra comparirà. Selezionare **Riparare** per iniziare il processo di riparazione.

Riavviare il computer quando venga richiesto, e quindi selezionare **Installare** per reinstallare Antivirus BitDefender 2008.

Una volta completato il processo di installazione, apparirà una nuova finestra. Selezionare **Termina**.

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



Nota

Vi consigliamo di scegliere **Rimuovere** per una reinstallazione pulita.

Scegliendo di rimuovere BitDefender, apparirà una nuova finestra.



Importante

Rimuovendo BitDefender, non sarete più protetti contro le minacce malware come virus e spyware. Se desiderate che Windows Defender venga attivato dopo aver disinstallato BitDefender, selezionare la casella di controllo corrispondente. Questa opzione è disponibile solo su Windows Vista.

Selezionare **Rimuovere** per iniziare la rimozione di Antivirus BitDefender 2008 dal vostro computer.

Durante il processo di rimozione vi verrà chiesto di darci il vostro feedback. Vi preghiamo di fare click su **OK** per ricevere un sondaggio on line, consistente in non più di cinque brevi domande. Se non si desidera ricevere il sondaggio, fare click su **Annulla**.

Una volta completato il processo di rimozione, apparirà una nuova finestra. Selezionare **Termina**.



Nota

Al termine del processo di disinstallazione, consigliamo di cancellare la cartella BitDefender dei Program Files.


Si è verificato un errore durante la rimozione di BitDefender

Se si fosse verificato un errore durante la rimozione di BitDefender, il processo di rimozione verrà interrotto ed apparirà una nuova finestra. Selezionare **Esegui tool di disinstallazione** per assicurarsi che BitDefender sia stato completamente rimosso. Il tool di disinstallazione rimuoverà tutti i file e chiavi di registro che non siano stati rimossi durante il processo automatico di rimozione.

Amministrazione di base

2. Iniziando

Una volta che avrete installato BitDefender il vostro computer sarà protetto. Potete aprire il Centro di Sicurezza di BitDefender per controllare lo stato di sicurezza del sistema, prendere misure preventive o configurare completamente il prodotto in qualsiasi momento.

Per accedere al Centro di Sicurezza di BitDefender, usare il menu Avvio di Windows, seguendo il percorso: **Avvio** → **Programmi** → **BitDefender 2008** → **BitDefender Antivirus 2008** o più rapidamente facendo doppio click sull'  **icona BitDefender** presente nella barra delle applicazioni in basso a destra.



Centro di Sicurezza BitDefender

Il Centro di Sicurezza BitDefender contiene due aree:

- L'area **Stato**: contiene informazioni e vi aiuta nella risoluzione delle vulnerabilità della sicurezza del vostro computer. Potete facilmente osservare quanti problemi potrebbero colpire il vostro computer. Cliccando sul corrispondente tasto rosso **Risolvere tutti i problemi** le vulnerabilità del vostro computer verranno subito

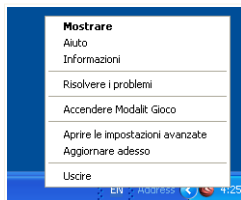
risolte oppure verrete guidati per risolverle facilmente. Nello stesso tempo, sono disponibili quattro tasti di stato corrispondenti a quattro categorie di sicurezza. I tasti di stato in verde indicano che non c'è nessun rischio. I tasti in giallo o in rosso indicano rischi di sicurezza medi o alti. Per risolverli cliccare sul tasto giallo/rosso e quindi i tasti **Risolvere**, uno per uno oppure il tasto **Risolvere tutti adesso**. Il Grigio indica una componente non configurata.

- L'area **Funzioni Veloci**: vi aiuta a mantenere sicuro il vostro sistema ed a proteggere i vostri dati.

Inoltre, il Centro di Sicurezza di BitDefender contiene diversi collegamenti utili.

<i>Link</i>	<i>Descrizione</i>
Comprare	Aprire una pagina dalla quale potete acquistare il prodotto.
Il mio Account	Aprire la pagina del vostro account BitDefender.
Registrare	Aprire l'assistente per la registrazione.
Aiuto	Aprire il file di aiuto.
Supporto	Aprire la pagina web di supporto di BitDefender
Impostazioni	Aprire il console delle impostazioni avanzate.
Storia	Aprire una finestra con la storia di BitDefender; eventi.

Per gestire l'intero prodotto più velocemente, potete anche utilizzare l'icona di BitDefender presente nella barra delle applicazioni.



Menù Contestuale

Se fate doppio click su questa icona, si aprirà il Centro di Sicurezza di BitDefender. Inoltre, cliccando col tasto destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto BitDefender.

- **Mostrare** - apre il il Centro di Sicurezza di BitDefender.

- **Aiuto** - apre il file di aiuto.
- **Info** - apre la pagina web di BitDefender.
- **Risolve tutti i problemi** - vi aiuta a rimuovere tutte le vulnerabilità di sicurezza.
- **Attivare Modalità Gioco** - disattiva gli allarmi ed i pop-up ed imposta il livello della vostra protezione in tempo reale come tollerante.
- **Aprire impostazioni avanzate** - consente l'accesso al console delle impostazioni avanzate.
- **Uscire** - termina l'applicazione.

2.1. Scansione Manuale di BitDefender

Se volete esaminare velocemente una certa cartella, potete usare la Scansione Manuale di BitDefender.

Per accedere alla Scansione Manuale BitDefender utilizzare il menu Avvio di Windows, seguendo il percorso **Avvio** → **Programmi** → **BitDefender 2008** → **Scansione Manuale di BitDefender**

Tutto quello che dovete fare è sfogliare le cartelle, selezionare quella desiderata e cliccare su **OK**.

3. Stato di Sicurezza

Lo stato di sicurezza mostra una lista organizzata sistematicamente e facilmente maneggevole delle vulnerabilità della sicurezza del vostro computer. Antivirus BitDefender 2008 vi farà sapere quando un problema può colpire la sicurezza del vostro computer.

Ci sono quattro tasti di stato di sicurezza:

- **ANTIVIRUS**
- **PRIVACY**
- **ANTIPHISING**
- **AGGIORNAMENTO**

Nello stesso tempo, sulla sinistra potrete vedere il numero dei problemi che colpiscono la sicurezza del vostro sistema, ed un tasto rosso **Risolvere Tutti i Problemi**.

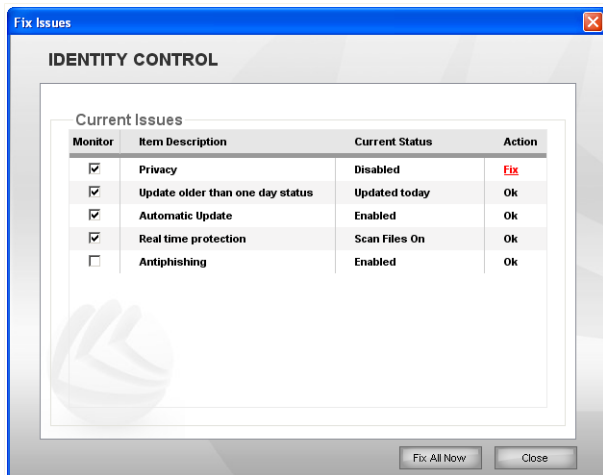
I quattro tasti di stato vengono visualizzati in verde, giallo, rosso o grigio, a seconda del livello corrente di protezione.

- **Verde** indica un livello basso di rischio di sicurezza per il vostro computer.
- **Giallo** indica un livello medio di rischio di sicurezza per il vostro computer.
- **Rosso** indica un livello alto di rischio di sicurezza per il vostro computer.
- **Grigio** indica una componente non configurata.

La risoluzione dei problemi di sicurezza non richiede sforzo alcuno e può farsi con un semplice click sul tasto **Risolvere tutti i problemi**.

Verrà visualizzata una lista di problemi di sicurezza ed una breve descrizione del loro stato.

Per risolvere solo un particolare problema, cliccare sul corrispondente tasto **Risolvere**. Verrà risolto subito oppure dopo che avrete seguito i passi dell'assistente. Se si decide di risolverli tutti, cliccare sul tasto **Risolvere tutti adesso** e seguire i passi dell'assistente corrispondente.



Problemi di Sicurezza

Per risolvere i problemi più tardi, cliccare su **Chiudere**.



Importante

Per ogni problema c'è una casella, selezionata per default. Se non si desidera che un problema specifico venga tenuto in conto per calcolare il rischio di sicurezza, deselezionare la casella corrispondente. Vi preghiamo di utilizzare questa opzione con cautela, poichè è molto facile aumentare il rischio al quale verrà esposto il vostro computer.

3.1. Tasto Stato Antivirus

Se il tasto stato dell'antivirus è verde, non c'è niente di cui preoccuparsi. Altrimenti, se il tasto è rosso o grigio, il vostro computer è esposto ad un alto rischio di sicurezza.

Il colore dei tasti di stato può cambiare, non solo quando si configurano le impostazioni che riguardano la sicurezza del vostro computer, ma anche quando si dimentica di eseguire delle funzioni importanti. Ad esempio, se è da tempo che è stata eseguita l'ultima scansione del vostro sistema, il tasto di stato della sicurezza sarà giallo. Se è da tanto tempo, sarà rosso.

La tabella sotto vi fornirà l'informazione su gli elementi tenuti in conto per il calcolo del rischio di sicurezza.

Problema	Colore
L'ultima scansione del sistema è stata eseguita tempo fa	Giallo
L'ultima scansione del sistema è stata eseguita tanto tempo fa	Rosso
La protezione in tempo reale è disattivata	Rosso
Il livello di protezione antivirus è impostato come tollerante	Giallo

Per risolvere i problemi, vi invitiamo a seguire questi passaggi:

1. Cliccare sul tasto Stato Antivirus
2. Cliccare sul tasto **Risolvere** per risolverli uno alla volta oppure il tasto **Risolvere tutti adesso** per risolverli tutti immediatamente.
3. Se un problema non venisse risolto subito, seguire i passaggi dell'assistente per risolverlo.

3.2. Tasto Stato della Privacy

Se il tasto stato della privacy è verde, non c'è niente di cui preoccuparsi. Altrimenti, se il tasto è rosso o grigio, il vostro computer è esposto ad un alto rischio di sicurezza.

La tabella sotto vi fornirà l'informazione su gli elementi tenuti in conto per il calcolo del rischio di sicurezza.

Problema	Colore
La protezione della privacy è impostata ed Attiva	Verde
La protezione della privacy è impostata e Disattivata	Rosso
La protezione della privacy non è stata impostata	Grigio

Per risolvere i problemi, vi invitiamo a seguire questi passaggi:

1. Cliccare sul tasto stato della privacy.
2. Cliccare sul tasto **Risolvere** per risolverli uno alla volta oppure il tasto **Risolvere tutti adesso** per risolverli tutti immediatamente.
3. Se un problema non venisse risolto subito, seguire i passaggi dell'assistente per risolverlo.

3.3. Tasto Stato Antiphishing

Se il tasto stato antiphishing è verde, non c'è niente di cui preoccuparsi. Altrimenti, se il tasto è rosso o grigio, il vostro computer è esposto ad un alto rischio di sicurezza.

La tabella sotto vi fornirà l'informazione su gli elementi tenuti in conto per il calcolo del rischio di sicurezza.

Problema	Colore
La protezione antiphishing è attiva	Verde
La protezione antiphishing è disattivata	Rosso

Per risolvere i problemi, vi invitiamo a seguire questi passaggi:

1. Cliccare sul tasto stato antiphishing.
2. Cliccare sul tasto **Risolvere** per risolverli uno alla volta oppure il tasto **Risolvere tutti adesso** per risolverli tutti immediatamente.
3. Se un problema non venisse risolto subito, seguire i passaggi dell'assistente per risolverlo.

3.4. Tasto Stato dell'Aggiornamento

Se il tasto stato dell'aggiornamento è verde, non c'è niente di cui preoccuparsi. Altrimenti, se il tasto è rosso o grigio, il vostro computer è esposto ad un alto rischio di sicurezza.

La tabella sotto vi fornirà l'informazione su gli elementi tenuti in conto per il calcolo del rischio di sicurezza.

Problema	Colore
L'aggiornamento automatico è attivo	Verde
L'aggiornamento automatico è disattivato	Rosso
L'ultimo aggiornamento è di un giorno fa.	Rosso

Per risolvere i problemi, vi invitiamo a seguire questi passaggi:

1. Cliccare sul tasto stato dell'aggiornamento.

-
2. Cliccare sul tasto **Risolvere** per risolverli uno alla volta oppure il tasto **Risolvere tutti adesso** per risolverli tutti immediatamente.
3. Se un problema non venisse risolto subito, seguire i passaggi dell'assistente per risolverlo.

4. Funzioni Veloci

Sotto i quattro tasti di stato si trova l'area **Funzioni Veloci**.

4.1. Sicurezza

BitDefender contiene un modulo di Sicurezza che vi aiuta a mantenere il vostro BitDefender aggiornato ed il vostro computer libero di virus.

Per accedere al modulo Sicurezza, cliccare sulla linguetta **Sicurezza**.

Sono disponibili i seguenti tasti:

- **Aggiornare adesso** - inizia un aggiornamento silenzioso.
- **Esamina Documenti** - inizia una scansione veloce dei vostri documents and settings.
- **Scansione Completa del Sistema** - inizia una scansione completa del vostro computer.

4.1.1. Aggiornamento

Il processo di aggiornamento viene eseguito involo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodottoe, nello stesso tempo, ogni vulnerabilità verrà esclusa.

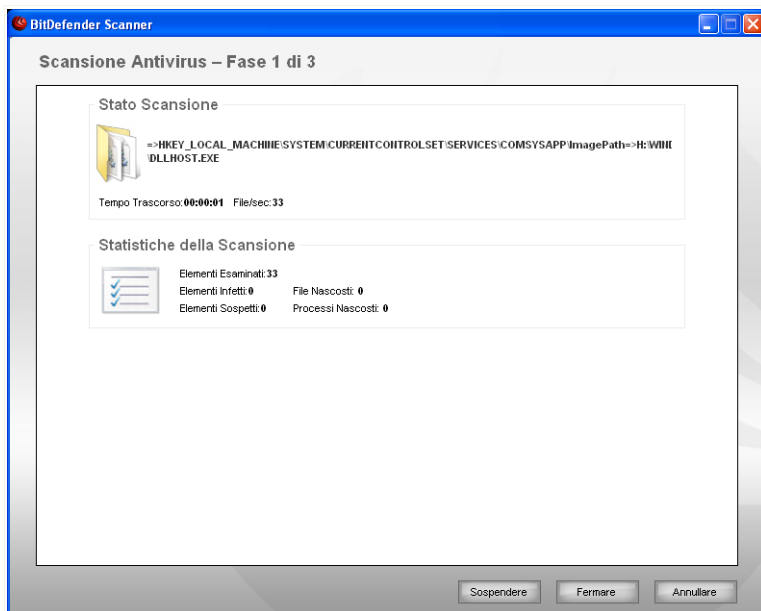
4.1.2. Scanner di BitDefender.

Quando si inizializza un processo di scansione a richiesta, sia scansione veloce o completa, lo Scanner di BitDefender apparirà.

Seguire la procedura di tre passi per completare il processo di scansione.

Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.



Scansione

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).



Nota

La durata del processo dipende dalla complessità della scansione.

Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente.



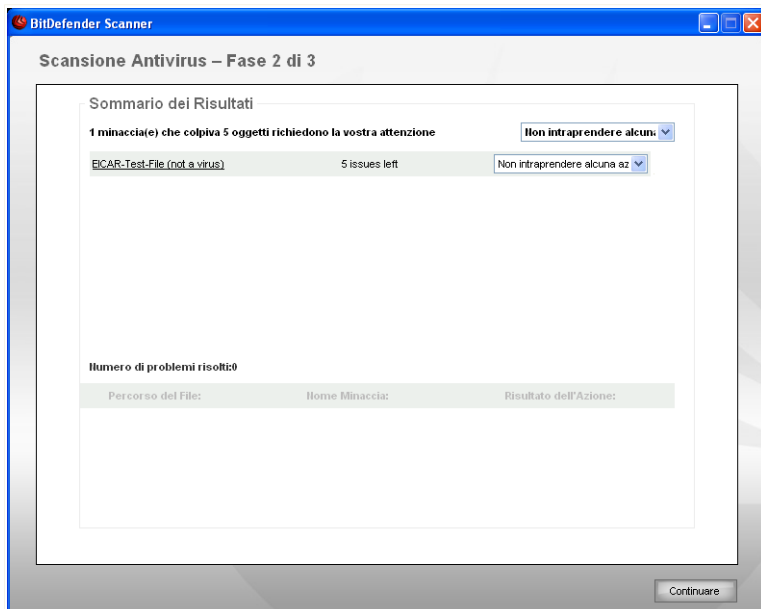
Nota

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

Attendere che BitDefender finisca la scansione.

Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.



Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.

Le seguenti opzioni possono comparire nel menu:

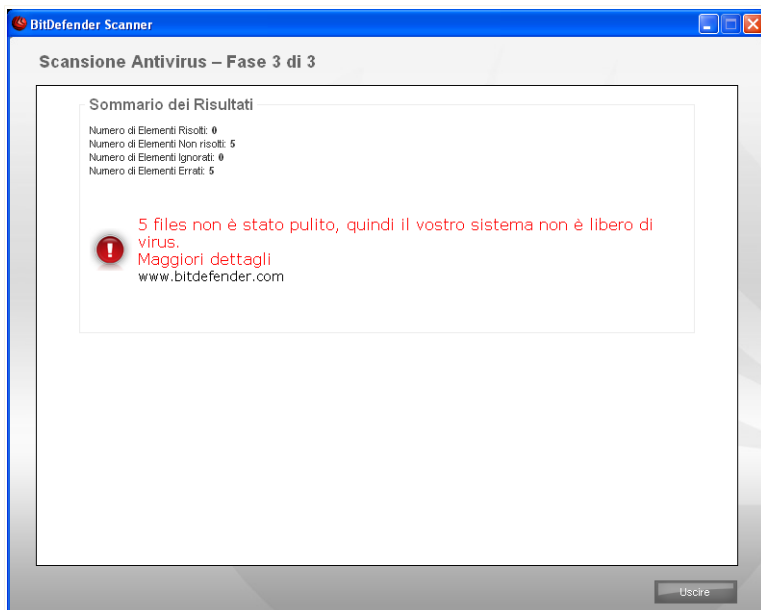
Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati.

Azione	Descrizione
Disinfettare	Disinfetta i file infetti.
Eliminare	Elimina i file infetti.
Mostrare	Rende visibili i file nascosti

Click **Risolvere i problemi** per applicare le azioni specificate.

Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.



Sommario

E' possibile visualizzare il sommario dei risultati.

Il file di report viene automaticamente salvato nella sezione **Registri** della finestra delle **Proprietà** di ogni funzione.

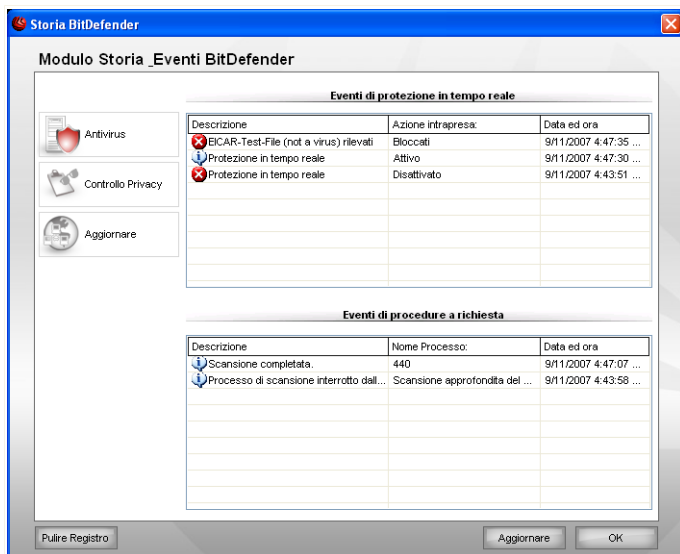


Avvertimento

Se ci sono problemi non risolti, vi consigliamo di contattare il Team di supporto di BitDefender su www.bitdefender.com.

5. Storia

Il link **Storia**, in fondo alla finestra del Centro di Sicurezza BitDefender, apre un'altra finestra con la storia ed eventi di BitDefender. Questa finestra vi offre una visione generale degli eventi relativi alla sicurezza. Per esempio, potete controllare facilmente se l'aggiornamento è stato eseguito con successo, se è stato rilevato del malware sul vostro computer, se i vostri processi di backup si eseguono senza errore, etc.



Eventi

Per aiutarvi a filtrare la storia ed eventi di BitDefender, sulla sinistra sono disponibili le seguenti categorie:

- **Antivirus**
- **Controllo Privacy**
- **Aggiornamento**

Per ogni categoria c'è una lista di eventi disponibile. Ogni evento viene con la seguente informazione: una breve descrizione, l'azione intrapresa da BitDefender quando è

successo, e la data ed ora in cui è successo. Se volete trovare ulteriori informazioni su un particolare evento della lista, cliccateci due volte sopra.

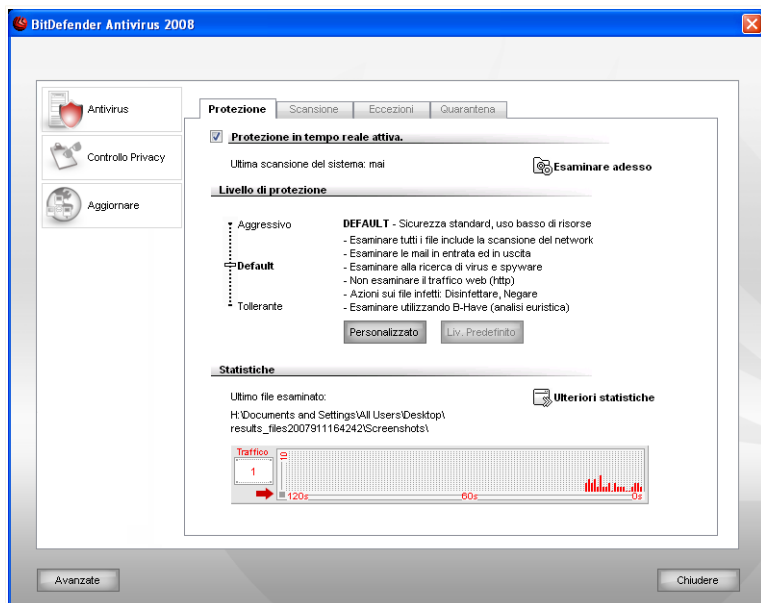
Cliccare su **Cancellare Registro** se si desidera rimuovere tutti i vecchi registri, oppure **Aggiornare** per assicurarsi di visualizzare i registri più recenti.

Amministrazione della Sicurezza Avanzata

6. Iniziando

Antivirus BitDefender 2008 arriva con un console centralizzato di configurazione, il quale permette la configurazione ed amministrazione avanzate di BitDefender.

Per accedere al console di configurazione, cliccare sul link **Impostazioni**, situato in fondo al Centro di Sicurezza.



Console di Configurazione

Il console di configurazione è organizzato in moduli: **Antivirus**, **Controllo Privacy** ed **Aggiornamento**. Questo permette di gestire facilmente BitDefender basandosi sul tipo di problema di sicurezza.

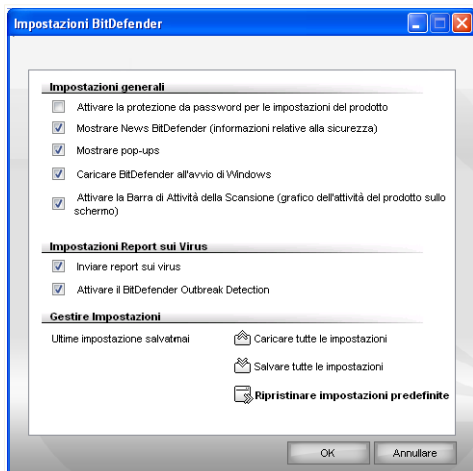
Sulla parte sinistra del console di configurazione si trova il selettore dei moduli:

- **Antivirus** - in questa sezione potete configurare il modulo **Antivirus**.
- **Controllo Genitori** - in questa sezione potete configurare il modulo **Controllo dei Genitori**.

- **Aggiornamento** - in questa sezione puoi configurare il modulo **Aggiornamento**.

6.1. Configurazione delle Impostazioni Generali

Per configurare le impostazioni generali per Antivirus BitDefender 2008 e gestionarle, cliccare su **Avanzate**. Apparirà una nuova finestra.



Impostazioni Generali

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

6.1.1. Impostazioni Generali

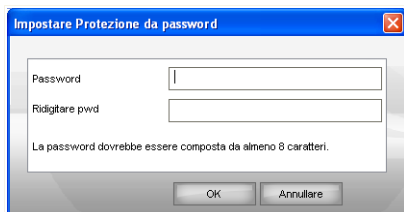
- **Abilita la protezione password per le impostazioni del prodotto** - consente l'impostazione di una password per proteggere la configurazione della Console di Gestione BitDefender.



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:



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

Inserisci password

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. Si raccomanda di lasciare questa opzione selezionata.
- **Attivare barra di attività della scansione (grafico dell'attività del prodotto sullo schermo)** - attiva / disattiva la **Barra di attività della Scansione**.

6.1.2. Impostazioni Report sui Virus

- **Inviare Report sui Virus** - invia ai Laboratori BitDefender i report relativi ai virus identificati sul vostro computer. Questo ci aiuta a tracciare la diffusione dei virus.
I report 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 report statistici.
- **Attivare Outbreak Detection BitDefender** - invia ai Laboratori BitDefender i report relativi al potenziale scoppio di un virus.

I report 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 report statistici.


6.1.3. Gestione Impostazioni

Facendo un click su  **Salva tutte le impostazioni** /  **Salva 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**.

6.2. Utilizzo della 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.



Nota

La Barra delle attività di scansione vi informerà quando la protezione in tempo reale sia disattivata mostrando una croce rossa sulla **Zona File**.



Barra delle Attività

Potete usare la **Barra delle attività di scansione** per esaminare degli oggetti. Fare semplicemente il drag & drop degli oggetti che volete esaminare sulla barra.



Nota

Per ulteriore informazione, vi preghiamo di riferirvi a «**Scansione Selezione e Trascina**» (p. 59).

Quando non si vuole vedere la visualizzazione grafica, è sufficiente fare un click con il tasto destro del mouse sulla stessa e selezionare **Nascondi**. Per nascondere completamente questa finestra, cliccare su **Avanzate** nel console delle impostazioni

e deselezionare la casella corrispondente a **Attiva la Barra delle attività di scansione** (grafica dell'attività del prodotto sullo schermo).

7. AntiVirus

BitDefender protegge il vostro computer da ogni tipo di minaccia malware (virus, troiani, spyware, rootkit ed altro).

Oltre alla classica scansione basata sulle impronte malware, BitDefender eseguirà inoltre una scansione euristica dei file esaminati. L'obiettivo della scansione euristica è quello di identificare nuovi virus, basata su determinate caratteristiche ed algoritmi, prima che un virus venga definito. Possono apparire messaggi di falso allarme. Quando viene rilevato, un file di questo tipo è classificato come sospetto. In questi casi consigliamo di inviare il file ai laboratori BitDefender per essere esaminato.

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

- **Scansione all'accesso** - impedisce alle minacce malware di entrare nel vostro sistema. Viene anche chiamata protezione in tempo reale - i file vengono esaminati durante il loro utilizzo - all'accesso. BitDefender esaminerà, ad esempio, un documento word quando verrà aperto, ed una mail quando verrà ricevuta.
- **Scansione a richiesta** - permette di rilevare e di rimuovere malware già residente nel vostro sistema. Si tratta della classica scansione dei virus avviata dall'utente – si sceglie quale drive, cartella o file BitDefender deve esaminare e BitDefender li esamina – a richiesta. I processi della scansione vi permettono di creare routine di scansione personalizzate e la loro esecuzione può essere programmata con una cadenza regolare.

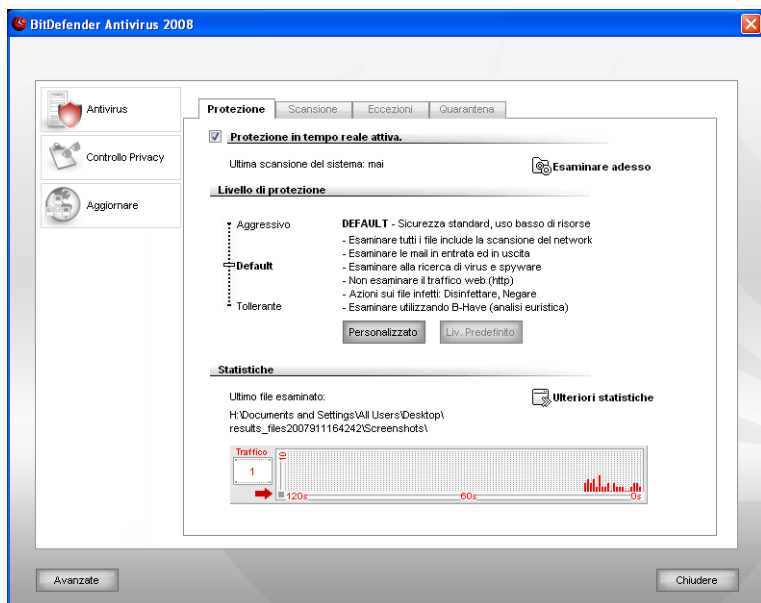
La sezione **Antivirus** di questa guida all'utente contiene i seguenti argomenti:

- **Scansione all'accesso**
- **Scansione a richiesta**
- **Oggetti Esclusi dall Scansione**
- **Quarantena**

7.1. Scansione all'accesso

Scansione all'accesso, conosciuta anche come protezione in tempo reale, mantiene il vostro computer protetto da ogni tipo di minaccia malware mediante la scansione di tutti i file acceduti, le mail e le comunicazioni tramite applicazioni Software di Messaggistica Istantanea (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Per configurare e monitorare la protezione in tempo reale, cliccare su **Antivirus Shield** nel console delle impostazioni. Apparirà la finestra seguente:



Virus Shield



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.

Per avviare una scansione file veloce del sistema, cliccare su **Esaminare Adesso**.

7.1.1. Configurazione del 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:

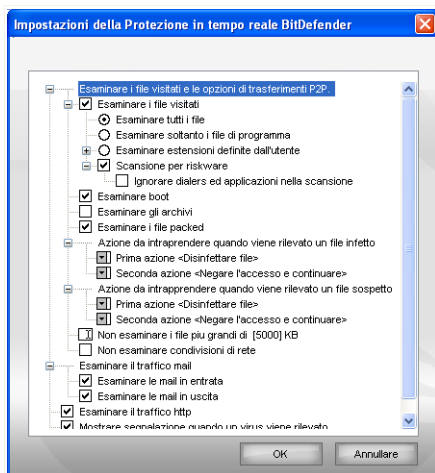
Livello di protezione	di Descrizione
Permissiva	<p>Copre le necessità di sicurezza di base. Il livello di consumo delle risorse è molto basso.</p> <p>I programmi e i messaggi di posta in arrivo sono scansionati solo alla ricerca di virus. Oltre alla classica scansione basata sulle impronte, è utilizzata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

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

7.1.2. Livello di Protezione Personalizzato

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

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.



Nota

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 trasferimenti 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 file s acceduti	Esamina tutti i files Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.

Opzione	Descrizione
Soltanto 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; .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 “;”.
Scansione per riskware	Esamina alla ricerca di 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.
Scansione del settore di avvio	Esamina il settore di avvio del sistema.
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 i file infetti.
Cancella file	Cancella immediatamente i file infetti, senza alcun avviso.

Opzione	Descrizione
Muovi il file in quarantena	Sposta i file infetti nella zona di 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 file infetti, senza alcun avviso.
Muovi il file in quarantena	Sposta i file infetti nella zona di 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.
Non esaminare condivisioni di rete	Se questa opzione è attiva, BitDefender non esaminerà le condivisioni di rete, permettendo un accesso alla rete più veloce. Vi consigliamo di attivare questa opzione solo se la rete della quale fate parte è protetta con una soluzione antivirus.

- **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

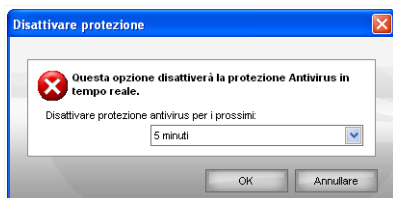
link al sito BitDefender dove sarà possibile trovare ulteriori informazioni al riguardo. Per una e-mail infetta, la finestra di allerta contiene anche informazioni sul mittente e il destinatario.

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.

7.1.3. Disattivazione Virus Shield

Se volete disattivare la protezione in tempo reale, apparirà la seguente finestra di avviso:



Disattivare Virus Shield

Dovrete confermare la vostra scelta selezionando dal menu, per quanto tempo volete disattivare la protezione in tempo reale. Potete disattivarla durante 5, 15 o 30 minuti, un'ora, permanentemente o fino al riavvio del sistema.



Avvertimento

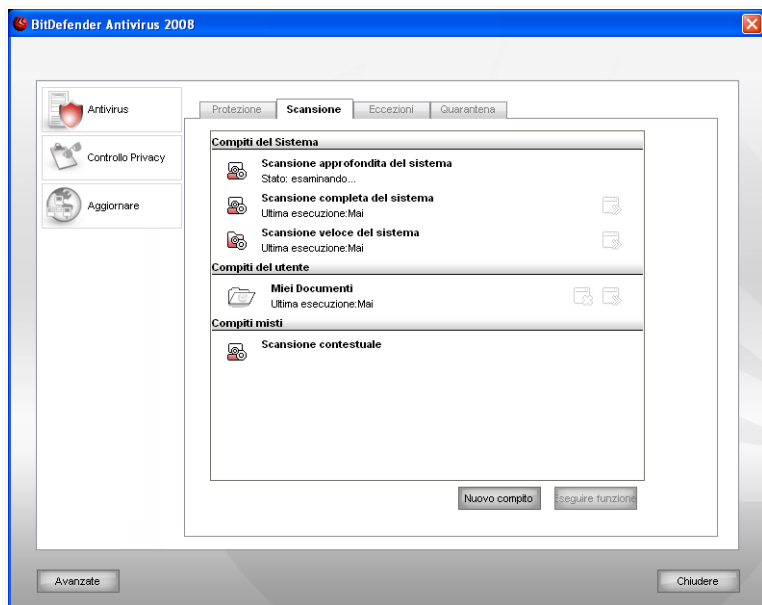
Questa è una questione di sicurezza critica. Vi consigliamo di disattivare la protezione in tempo reale per il minimo tempo possibile. Se la protezione in tempo reale non è attiva, non sarete protetti dalle minacce malware.

7.2. Scansione a richiesta

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.

Per configurare ed avviare la scansione a richiesta, cliccare su **Antivirus>Scansione** nel console di configurazione. Apparirà la finestra seguente:



Impostazioni della Scansione

La scansione a richiesta si basa sulle impostazioni della scansione. Le impostazioni della scansione specificano le opzioni della scansione e gli oggetti da esaminare. Potete esaminare il vostro computer in qualsiasi momento, eseguendo le funzioni predefinite oppure le vostre proprie (definite dall'utente). Potete anche programmarle per venire eseguite con cadenza regolare oppure quando il sistema risulti così ozioso da non interferire con il vostro lavoro.

7.2.1. Impostazioni della Scansione

BitDefender ha tante funzioni, create per default, che coprono i problemi di sicurezza comuni. Voi potete anche creare le vostre funzioni di scansione personalizzate.

Ogni funzione o compito ha una finestra delle **Proprietà** che vi permette di configurare il compito e di vedere i risultati della scansione. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Configurare un Compito di Scansione*» (p. 48).

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 approfondita	Esamina l'intero sistema. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione Completa del Sistema	Esamina l'intero sistema, esclusi gli archivi. Nella configurazione predefinita, esegue la scansione per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.
Scansione Veloce del Sistema	Esamina le cartelle Windows, Program Files e All Users. Nella configurazione predefinita, esamina per cercare tutti i tipi di malware, esclusi i rootkit, ma non esamina la memoria, il registro nè i cookies.



Nota

Poichè le funzioni **Scansione del sistema approfondita** e **Scansione completa del sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo. Quindi vi consigliamo di eseguire questi compiti con priorità bassa, o meglio, quando il vostro sistema risulti ozioso.



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

Viene fornita una funzione chiamata `My Documents`. Utilizzare questa funzione per esaminare delle cartelle importanti dell'utente corrente: `My Documents`,

Desktop e StartUp. Questo garantirà la sicurezza dei vostri documenti, uno spazio di lavoro sicuro ed applicazioni pulite al avvio.

- **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 eseguiti 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 su questo tasto per aprire la sezione **Programmatore** nella finestra delle **Proprietà**, dove è possibile visualizzare la programmazione delle funzioni e modificarla.
-  **Cancella** - rimuove la funzione selezionata.



Nota

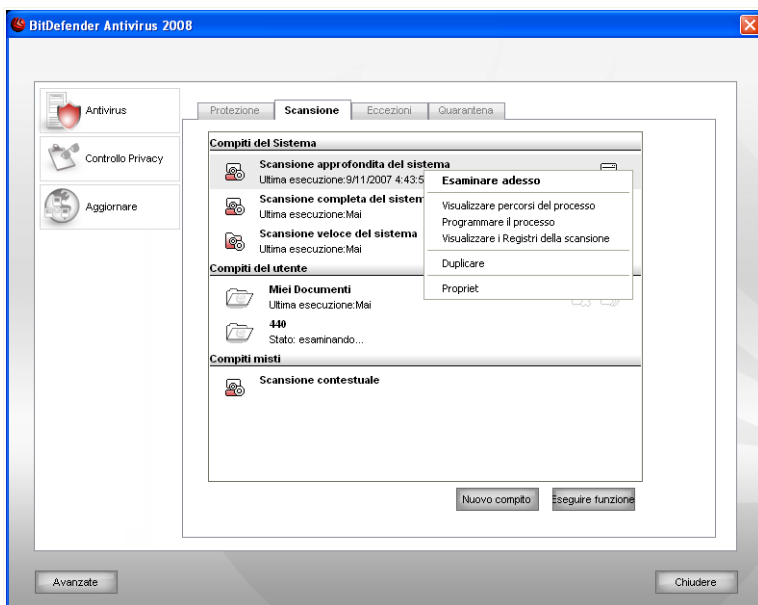
Non disponibile per compiti di sistema. Non potete rimuovere un compito di sistema.

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

Alla sinistra di ogni funzione potrete vedere il tasto delle **Proprietà**, che vi permette di configurare i compiti e visualizzare i registri della scansione.

7.2.2. Utilizzo del Menu Rapido

Un menu rapido è



Menu Rapido

disponibile per ciascun compito. Cliccare col pulsante destro del mouse sul compito selezionato per aprirlo.

Nel menù collegato sono disponibili i seguenti comandi:

- **Scan Now** - esegue la funzione selezionata, avviando immediatamente una scansione.
- **Cambiare il Target di Scansione** - apre la sezione **Percorso Scansione** nella finestra delle **Proprietà**, dove potete cambiare il target di scansione per i compiti selezionati.



Nota

Nel caso di funzioni del sistema, questa opzione viene sostituita da **Mostrare Percorsi delle Funzioni**, dato che potete vedere solo il loro target di scansione.

- **Funzione Programmazione** - apre la sezione **Programmazione** nella finestra delle **Proprietà**, dove potete programmare il compito selezionato.
- **Visualizzare i Registri di Scansione** - apre la sezione **Registri della Scansione** nella finestra delle **Proprietà**, 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.

- **Cancella** - cancella i compiti selezionati.



Nota

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

- **Proprietà** - apre la sezione **Visione generale** nella finestra delle **Proprietà**, dove potete cambiare le impostazioni del compito selezionato.



Nota

Data la loro particolare natura, solo le opzioni **Proprietà** e **Visualizzare Registri Scansione** sono disponibili per la categoria delle funzioni **Compiti Misti**.

7.2.3. Creazione delle Funzioni di Scansione

Per creare un compito di scansione, utilizzare uno di questi metodi:

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

7.2.4. Configurare un Compito di Scansione

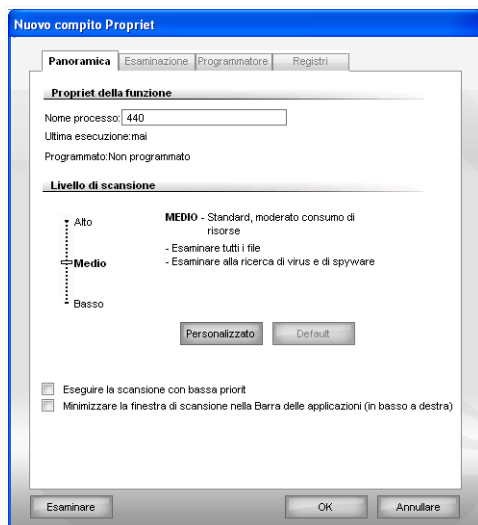
Ogni compito di scansione ha la sua propria finestra delle **Proprietà**, dove potete configurare le opzioni di scansione, impostare il target della scansione, programmare il compito o vedere i report. Per aprire questa finestra cliccare sul tasto **Aprire**, posto sulla destra della funzione (o cliccare con il tasto destro sulla funzione e quindi cliccare **Aprire**).

**Nota**

Per ulteriori informazioni sulla visualizzazione dei registri e sulla funzione **Registri**, vi preghiamo di riferirvi a «*Visualizzazione dei Registri di Scansione*» (p. 64).

Configurazione delle Impostazioni di Scansione

Per configurare le opzioni di scansione di un compito specifico, cliccare con il tasto destro e selezionare **Proprietà**. Apparirà la finestra seguente:

**Informazioni generali sul prodotto BitDefender™**

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

Scelta del Livello di Scansione

Potete facilmente configurare le impostazioni di scansione scegliendo il livello di scansione. Trascinare l'indicatore sulla barra per impostare l'appropriato livello di scansione.

Ci sono 3 livelli di scansione:

Livello di protezione	Descrizione
Basso	<p>Offre un'efficienza di rilevamento ragionevole. Il livello di consumo delle risorse è basso.</p> <p>Vengono esaminati alla ricerca di virus solo i programmi. Oltre alla classica scansione basata sull'impronta, è utilizzata anche l'analisi euristica.</p>
Medio	<p>Offre una buona efficienza di rilevamento. Il livello di consumo delle risorse è moderato.</p> <p>Tutti i file vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.</p>
Alto	<p>Offre un'alta efficienza di rilevamento. Il livello di consumo di risorse è alto.</p> <p>Tutti i file e gli archivi vengono esaminati alla ricerca di virus e spyware. Oltre alla classica scansione basata sulle impronte, è utilizzata anche l'analisi euristica.</p>

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.
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 riapirla.

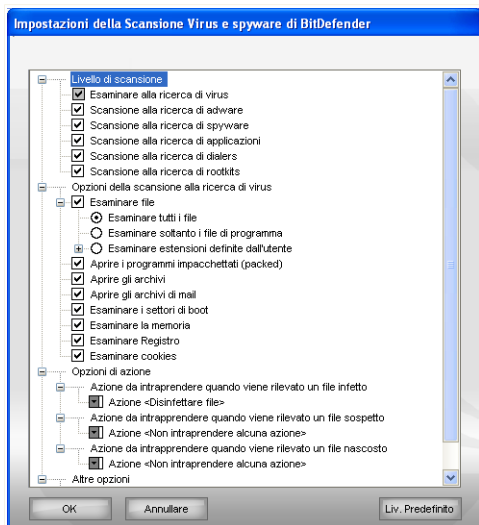
Selezionare **OK** per salvare le modifiche e chiudere la finestra. Per eseguire la funzione, selezionare **Scan**.

Personalizzazione del Livello di Scansione

Gli utenti esperti possono trarre vantaggio dalle possibilità di impostazione della scansione BitDefender. Infatti la scansione può essere impostata in modo di esaminare

solo delle specifiche estensioni, di cercare delle particolare minacce malware, o di non esaminare gli archivi. Questo può ridurre di molto i tempi di scansione ed incrementare la reattività del vostro computer durante una scansione.

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

Le opzioni di scansione sono raggruppate in quattro categorie:

- **Livello di Scansione**
 - **Opzioni di scansione virus**
 - **Opzioni delle Azioni**
 - **Altre opzioni**
- Specificare il tipo di malware che volete che Bit Defender analizzi, selezionando le opzioni appropriate dalla categoria **Livello di scansione**.

Sono disponibili le seguenti opzioni:

<i>Opzione</i>	<i>Descrizione</i>
Scansione Virus	Esamina per virus conosciuti. BitDefender rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansione applicazione	Esamina le applicazioni (.exe e i file .dll).
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.

- 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**.

Sono disponibili le seguenti opzioni:

<i>Opzione</i>	<i>Descrizione</i>
Scansione files	Esamina tutti i files Verranno esaminati tutti i file acceduti, indipendentemente dalla loro tipologia.
Soltanto programmi e documenti	i ed i 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;

Opzione	Descrizione
	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 “;”.
Apri i programmi impaccati	Scansiona i files impaccati.
Apri gli archivi	Scansiona l'interno degli archivi.
Apertura degli archivi e-mail	Eseguire la scansione all'interno degli archivi di posta.
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.
Scansione registro	Scansione di voci di registro.
Scansionare cookies	Esamina i files cookie.

- Specificare l'azione da intraprendere sui file infetti, sospetti o nascosti rilevati nella categoria **Opzioni di Azione**. Potete specificare una diversa azione per ogni categoria.
 - Selezionare l'azione da intraprendere sui file infetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Nessuno(log oggetti)	Nessuna azione verrà eseguita sui file infetti. Questi files appariranno nel file di report.
Disinfetta i files	Disinfetta i file infetti.
Cancella i files	Cancella immediatamente i file infetti, senza alcun avviso.
Muovere i files in Quarantena	Sposta i file infetti nella zona di quarantena.

- Selezionare l'azione da intraprendere sui file sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Nessuno(log oggetti)	Nessuna azione verrà eseguita sui file sospetti. Questi files appariranno nel file di report.
Cancella i files	Cancella immediatamente i files sospetti, senza alcun avviso.
Muovere i files in Quarantena	Sposta i file sospetti nella zona di quarantena.

**Nota**

La Scansione euristica ha rilevato dei file sospetti. Vi consigliamo di inviarli al laboratorio di BitDefender.

- Selezionare l'azione da intraprendere sugli oggetti nascosti (rootkits) rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Nessuno(log oggetti)	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Muovere i files in Quarantena	Sposta i file nascosti nella zona di quarantena.
Rendere visibili	Rivela i file nascosti in modo che possano essere visti.

**Nota**

Se scegliete di ignorare i file rilevati o se l'azione selezionata fallisce, dovrete scegliere un'azione nell'assistente di scansione

- Per far sì che venga richiesta di inviare tutti i file sospetti al laboratorio BitDefender dopo che il processo di scansione sia stato completato, selezionare **inviare tutti i file sospetti al laboratorio BitDefender** nella categoria **Altre Opzioni**.

Se clicchi su **Predefinito** verranno applicate le impostazioni di default. Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

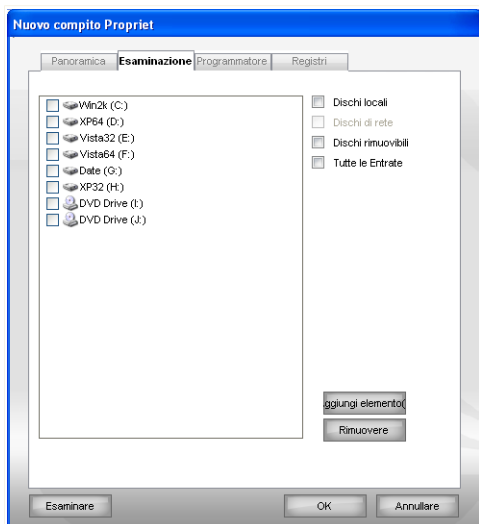
Impostazione del Target di Scansione



Nota

Non potete modificare il target di scansione delle funzioni di scansione dalla categoria **Funzioni del Sistema**. Potete solo visualizzare il target di scansione.

Per impostare il target di scansione di un compito di scansione specifico, cliccare con il tasto destro sul compito e selezionare **Modificare Target di Scansione** (o **Mostrare Percorsi delle funzioni** per le funzioni di sistema, per visualizzare il loro target). Apparirà la finestra seguente:



Target di Scansione

Potete vedere la lista di dischi locali, di rete e rimovibili, ed anche i file e cartelle aggiunti in precedenza, se ci sono. Tutti gli oggetti selezionati verranno esaminati all'esecuzione della funzione.

La sezione contiene i seguenti pulsanti:

- **Aggiungere Oggetto (i)** - apre una finestra di visualizzazione dove è possibile selezionare il (i) file / cartella(e) che si desidera esaminare.



Nota

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

- **Cancellare Oggetti** - rimuove il (i) file / cartella(e) 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 rimovibili (CD-ROM, floppy-disk).
- **Tutti gli elementi** - per esaminare tutti i drives, indipendentemente dal fatto che siano locali, sulla rete o rimovibili.



Nota

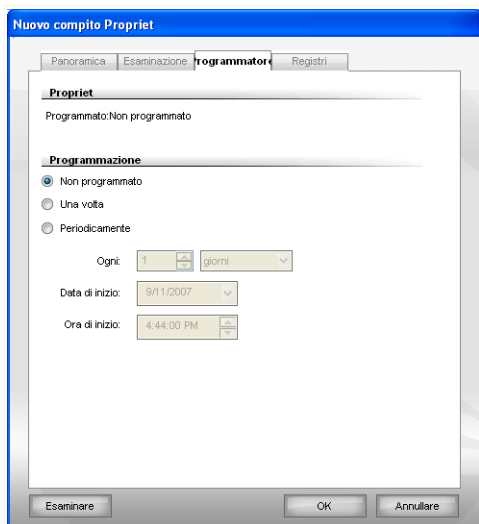
Se desiderate eseguire una scansione di tutto il vostro computer alla ricerca di virus, selezionare la casella corrispondente a **Tutti gli elementi**.

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

Programmazione delle Funzioni di Scansione

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.

Per visualizzare la programmazione di un compito specifico o per modificarla, cliccare con il tasto destro e selezionare **Programmare Funzione**. Apparirà la finestra seguente:



Programmatore

Potete vedere la programmazione delle funzioni, se ci sono.

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

- **Non programmata** - lancia la funzione solo quando richiesta dall'utente.
- **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**.

7.2.5. Oggetti di Scansione

Prima di iniziare il processo di scansione, dovrete assicurarvi che BitDefender sia aggiornato con le impronte malware. Eseguire la scansione usando un database delle impronte obsoleto può impedire BitDefender di rilevare nuovo malware, trovato dopo l'ultimo aggiornamento. Per verificare quando è stato eseguito l'ultimo aggiornamento, cliccare su **Aggiornamento>Aggiornamento** nel console di configurazione.



Nota

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

Metodi di Scansione


BitDefender consente quattro tipi di scansione a richiesta:

- **Scansione immediata** - avvia immediatamente un processo di scansione dal sistema / funzioni utente.
- **Scansione contestuale** - selezionare un file o una cartella con il tasto destro e selezionare Antivirus BitDefender 2008;
- **Scansione Seleziona & Trascina** - seleziona & trascina un file o una cartella sopra la **Barra delle Attività di Scansione**.
- **Scansione manuale** - Utilizzare Scansione Manuale di BitDefender per selezionare direttamente i file o cartella da esaminare.

Scansione Immediata

Per eseguire una scansione del vostro computer o di parte di essi potete usare i compiti di scansione di default oppure i vostri propri compiti di scansione. Ciò si chiama scansione immediata

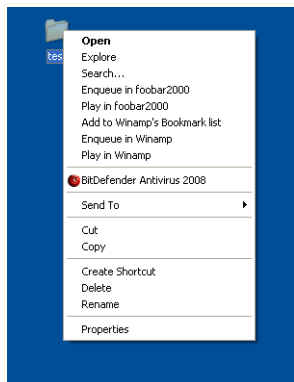
Per eseguire un compito di scansione, utilizzare uno dei seguenti metodi:

- 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**.

Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Scanner di BitDefender.*» (p. 60).

Scansione Contestuale

Per esaminare un file o cartella senza configurare un nuovo compito di scansione, si può usare il menu contestuale. ciò si chiama scansione contestuale



Scansione Contestuale

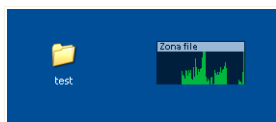
Cliccare con il tasto destro sul file o la cartella che si desidera esaminare e selezionare **Antivirus BitDefender 2008**.

Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a *«Scanner di BitDefender.»* (p. 60).

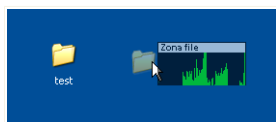
E' possibile modificare e vedere il file di report dalla finestra delle **Proprietà** del **Menu Scansione Contestuale**.

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



Abbandonare il file

Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Scanner di BitDefender.*» (p. 60).

Scansione Manuale

La scansione manuale consiste in selezionare direttamente l'oggetto da esaminare, utilizzando l'opzione Scansione Manuale BitDefender dal gruppo di programmi BitDefender nel Menu di Avvio.

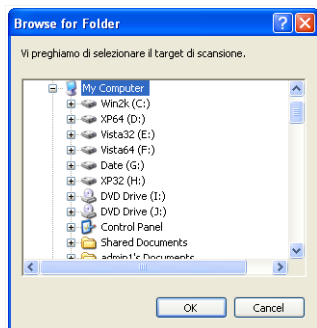


Nota

La scansione manuale è molto utile, poichè può essere eseguita anche quando Windows lavora in Modalità Provvisoria.

Per selezionare l'oggetto da esaminare, nel menu Avvio di Windows, seguire il percorso **Avvio** → **Programmi** → **BitDefender 2008** → **Scansione Manuale di BitDefender**.

Apparirà la finestra seguente:



Scansione Manuale

Scegliere l'oggetto che si desidera esaminare e cliccare **OK**.

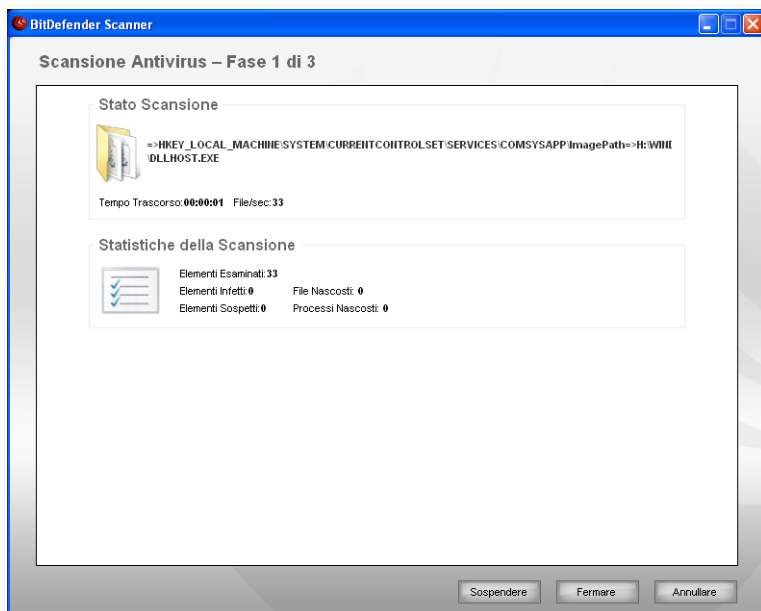
Lo Scanner BitDefender apparirà e la scansione verrà avviata. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Scanner di BitDefender.*» (p. 60).

Scanner di BitDefender.

Quando il processo di scansione a richiesta si avvierà, lo Scanner BitDefender apparirà. Seguire la procedura di tre passi per completare il processo di scansione.

Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.



Scansione

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).



Nota

La durata del processo dipende dalla complessità della scansione.

Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente.



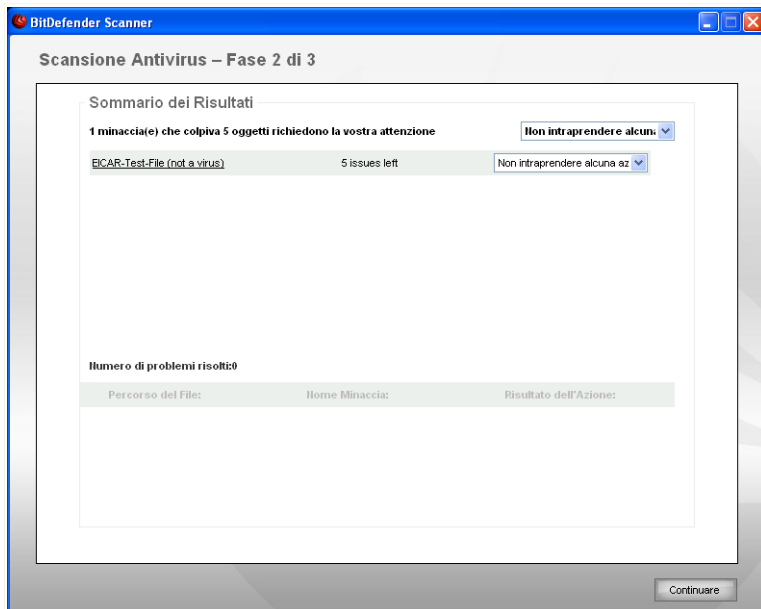
Nota

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

Attendere che BitDefender finisca la scansione.

Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.



Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.

Le seguenti opzioni possono comparire nel menu:

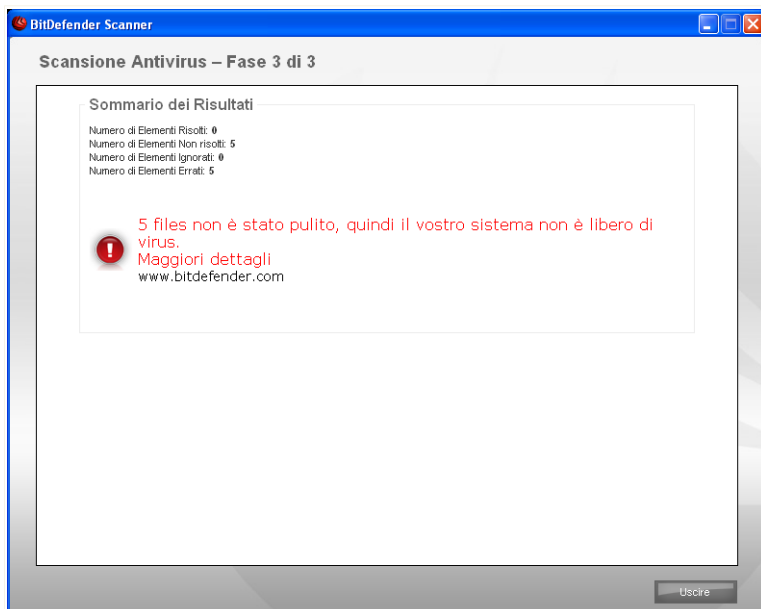
Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati.

Azione	Descrizione
Disinfettare	Disinfetta i file infetti.
Eliminare	Elimina i file infetti.
Mostrare	Rende visibili i file nascosti

Click **Risolvere i problemi** per applicare le azioni specificate.

Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.



Sommario

E' possibile visualizzare il sommario dei risultati.

Il file di report viene automaticamente salvato nella sezione **Registri** della finestra delle **Proprietà** di ogni funzione.

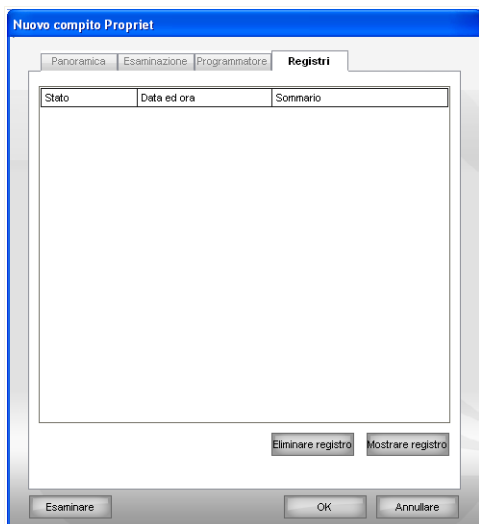


Avvertimento

Se ci sono problemi non risolti, vi consigliamo di contattare il Team di supporto di BitDefender su www.bitdefender.com.

7.2.6. Visualizzazione dei Registri di Scansione

Per visualizzare i risultati della scansione una volta completato un compito di scansione, cliccare con il tasto destro sul compito e selezionare **Visualizzare Registri di Scansione**. Apparirà la finestra seguente:



Registri di Scansione

Qui potete vedere i file di report generati ogni volta che il compito è stato eseguito. Ciascun 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:

- **Mostrare registro** - per visualizzare il file di report selezionato;
- **Cancellare registro** - per cancellare il file di report selezionato.

Inoltre, per vedere o cancellare un file, cliccare con il tasto destro sul file e selezionare l'opzione corrispondente dal menu rapido.

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

7.3. Oggetti esclusi dalla Scansione

Ci sono dei casi in cui si può avere bisogno di escludere certi file dalla scansione. Ad esempio, si può volere escludere un file di testo EISCAR dalla scansione all'accesso, oppure i file `.avi` dalla scansione a richiesta.

BitDefender permette di escludere oggetti dalle scansioni all'accesso ed a richiesta, o da entrambi. Questa caratteristica cerca di ridurre i tempi di scansione e di evitare le interferenze con il vostro lavoro.

Due tipi di oggetti possono essere esclusi dalla scansione:

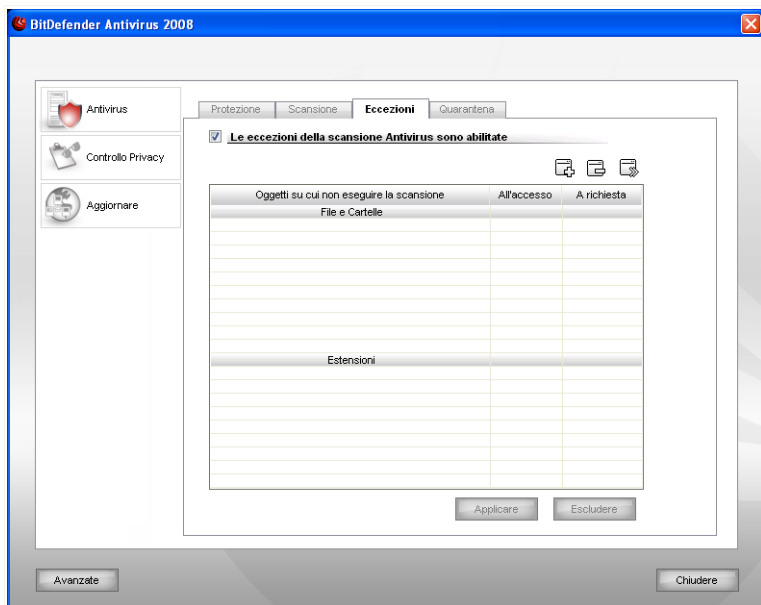
- **Percorsi** - Il file o cartella (inclusi tutti gli oggetti che essi contiene) indicato da un percorso specifico verrà escluso dalla scansione.
- **Estensioni** - tutti i file che hanno una specifica estensione verranno esclusi dalla scansione.



Nota

Gli oggetti esclusi dalla scansione all'accesso non verranno esaminati, non importa se sono visitati da voi o da un'applicazione.

Per visualizzare e gestire gli oggetti esclusi dalla scansione, cliccare **Antivirus>Eccezioni** nel console di configurazione. Apparirà la finestra seguente:



Eccezioni


Si possono visualizzare gli oggetti (file, cartelle, estensioni) esclusi dalla scansione. Potete vedere se ogni oggetto è stato escluso dalla scansione all'accesso, dalla scansione a richiesta o da entrambi.



Nota

Le eccezioni qui specificate NON verranno applicate nella scansione contestuale.

Per rimuovere un'entrata dalla tabella, selezionarla e cliccare il tasto  **Eliminare**.

Per modificare un'entrata dalla tabella, selezionarla e cliccare il tasto  **Modificare**. Apparirà una nuova finestra dove si potrà modificare l'estensione od il percorso da escludere ed il tipo di scansione dal quale escluderlo, a seconda delle necessità. Apportare le necessarie modifiche e cliccare **OK**.




Nota

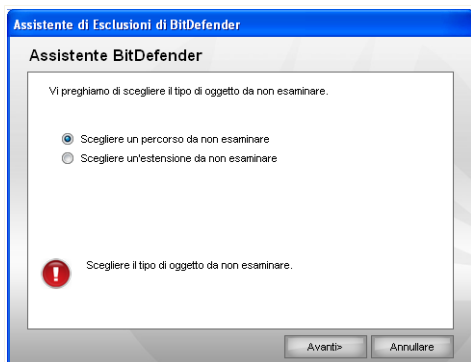
Potete anche cliccare con il tasto destro sull'oggetto ed utilizzare le opzioni del menu rapido per modificarlo o eliminarlo.

Potete cliccare su **Ignorare** per ritornare alla situazione precedente alle modifiche effettuate alla tabella delle regole, sempre che non le abbiate salvate cliccando su **Applicare**.

7.3.1. Esclusione dei Percorsi dalla Scansione

Per escludere dei percorsi dalla scansione, cliccare sul tasto  **Aggiungere**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione dei percorsi dalla scansione.

Passo 1/3 – Selezione tipo di oggetto

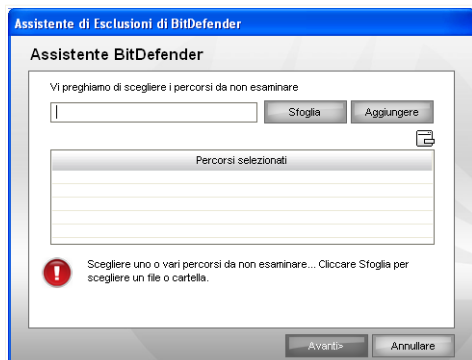


Tipo di Oggetto.

Selezionare l'opzione di escludere un percorso dalla scansione.

Selezionare **Avanti**.

Passo 2/3 – Specificare i percorsi esclusi



Percorsi Esclusi

Per specificare i percorsi da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Cliccare **Sfogliare**, selezionare il file o cartella che volete venga escluso dalla scansione e quindi cliccare su **Aggiungere**.
- Scrivere il percorso che volete venga escluso dalla scansione nel campo modifica e cliccare **Aggiungere**.



Nota

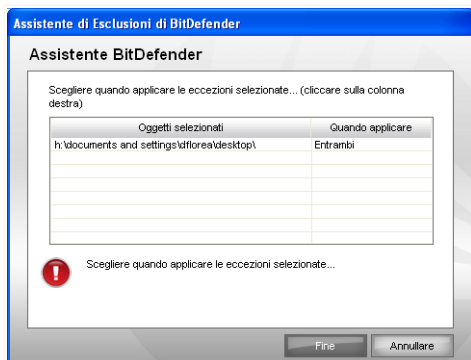
Se il percorso inserito non esiste, comparirà un messaggio di errore. Cliccare **OK** e controllare la validità del percorso.

I percorsi appariranno nella tabella man mano che vengono aggiunti. Potete aggiungere quanti percorsi volete.

Per rimuovere un'entrata dalla tabella, selezionarla e cliccare il tasto  **Eliminare**.

Selezionare **Avanti**.

Passo 3/3 – Selezionare tipo di scansione



Tipo di Scansione


Potete vedere una tabella contenente i percorsi da escludere dalla scansione ed il tipo di scansione dal quale vengono esclusi.

Per default i percorsi selezionati verranno esclusi da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

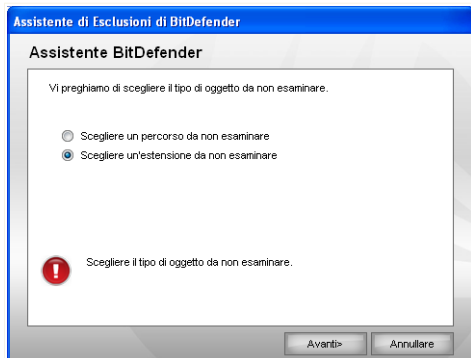
Selezionare **Termina**.

Cliccare **Applica** per salvare le modifiche.

7.3.2. Esclusione delle Estensioni dalla Scansione

Per escludere delle estensioni dalla scansione, cliccare sul tasto  **Aggiungere**. Verrete guidati dall'assistente di configurazione attraverso il processo di esclusione delle estensioni dalla scansione.

Passo 1/3 – Selezione tipo di oggetto



Tipo di Oggetto.

Selezionare l'opzione di escludere una estensione dalla scansione.

Selezionare **Avanti**.

Passo 2/3 – Specificare le estensioni escluse



Estensioni Escluse

Per specificare le estensioni da escludere dalla scansione, utilizzare uno dei seguenti metodi:

- Selezionare dal menu l'estensione che volete venga esclusa dalla scansione e quindi cliccare su **Aggiungere**.



Nota

Il menu contiene un elenco di tutte le estensioni registrate sul vostro sistema. Quando selezionate un'estensione, potrete vedere la sua descrizione, se disponibile.

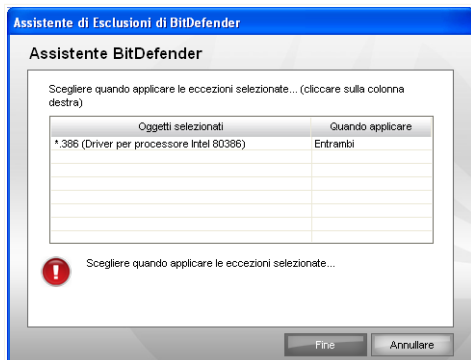
- Scrivere l'estensione che volete venga esclusa dalla scansione nel campo modifica e cliccare **Aggiungere**.

Le estensioni appariranno nella tabella man mano che vengono aggiunte. Potete aggiungere quante estensioni volete.

Per rimuovere un'entrata dalla tabella, selezionarla e cliccare il tasto  **Eliminare**.

Selezionare **Avanti**.

Passo 3/3 – Selezionare tipo di scansione



Tipo di Scansione

Potete vedere una tabella contenente le estensioni da escludere dalla scansione ed il tipo di scansione dal quale vengono escluse.

Per default le estensioni selezionate verranno escluse da entrambe le scansioni, all'accesso ed a richiesta. Per modificare quando applicare l'eccezione, cliccare nella colonna di destra e selezionare dall'elenco l'opzione desiderata.

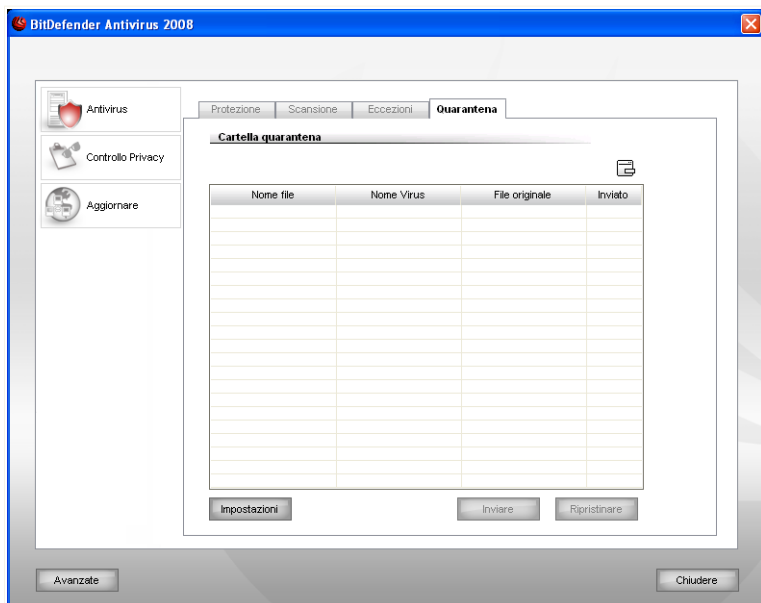
Selezionare **Termina**.

Cliccare **Applica** per salvare le modifiche.

7.4. Area di 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.

Per visualizzare e gestire i file in quarantena e per configurare le impostazioni della quarantena, cliccare su **Antivirus>Quarantena** nel console di configurazione.



Quarantena

7.4.1. Gestione dei File in Quarantena

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.

**Nota**

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

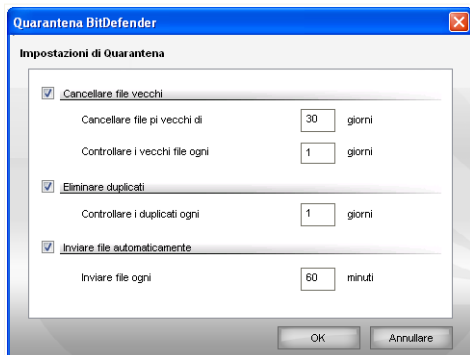
Per cancellare un file selezionato dalla quarantena, cliccare **Remove**. Se desiderate inviare un file selezionato alla sua ubicazione originale, cliccare **Restore**.

Potete inviare qualsiasi file selezionato dalla quarantena al lab BitDefender cliccando su **Invia**.

Menù contestuale. E' disponibile un menu contestuale che vi permette di gestire facilmente i file in quarantena. Sono disponibili le stesse opzioni su menzionate. Potete anche selezionare **Aggiornare** per aggiornare la sezione di Quarantena.

7.4.2. Configurazione delle Impostazioni di Quarantena

Per configurare le impostazioni di quarantena, cliccare su **Impostazioni**. Apparirà una nuova finestra.



Impostazioni di Quarantena

Utilizzando le impostazioni di quarantena, potete configurare BitDefender per eseguire automaticamente le seguenti azioni:

Eliminare i vecchi file. Per eliminare automaticamente i vecchi file, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni dopo i quali i file in quarantena devono essere eliminati e la frequenza con cui BitDefender deve effettuare il controllo dei vecchi file.



Nota

Per default, BitDefender effettuerà il controllo dei vecchi file ogni giorno ed eliminerà i file più vecchi di 10 giorni.

Eliminare duplicati. Per eliminare automaticamente i file duplicati in quarantena, selezionare l'opzione corrispondente. Dovete specificare il numero di giorni tra due controlli consecutivi dei duplicati.



Nota

Per default, BitDefender effettuerà il controllo dei file duplicati in quarantena ogni giorno.

Invio automatico dei file. Per inviare automaticamente i file in quarantena, selezionare l'opzione corrispondente. Dovete specificare la frequenza con cui inviare i file.



Nota

Per default, BitDefender invierà automaticamente i file in quarantena ogni 60 minuti.

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

8. Controllo Privacy

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.

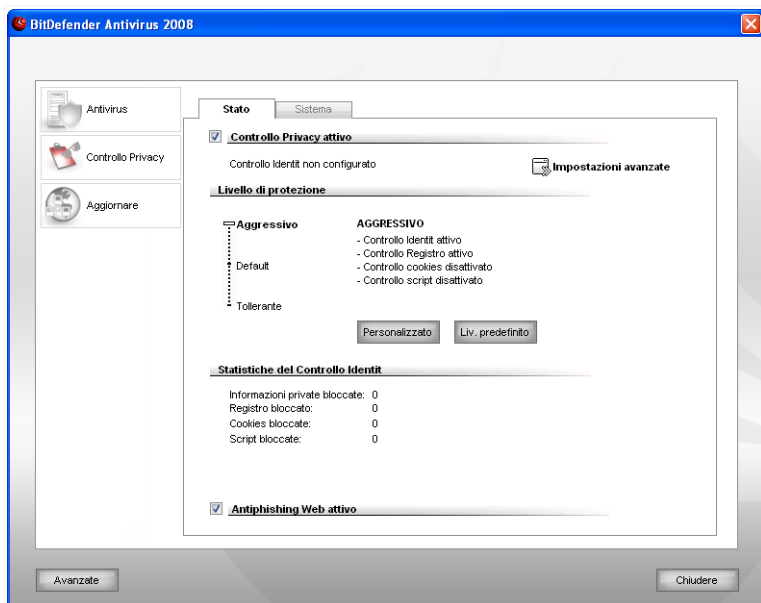
BitDefender esamina anche i siti web visitati ed avvisa se viene rilevata qualche minaccia di phishing.

La sezione **Controllo Privacy** di questa guida all'utente contiene i seguenti punti:

- **Stato Controllo Privacy**
- **Impostazioni Avanzate - Controllo Identità**
- **Impostazioni Avanzate - Controllo Registrazione**
- **Impostazioni Avanzate - Controllo Cookie**
- **Impostazioni Avanzate - Script Control**
- **Informazioni di Sistema**
- **Barra degli strumenti Antiphishing**

8.1. Stato Controllo Privacy

Per configurare il Controllo Privacy e visualizzare informazioni riguardanti la sua attività, cliccare su **Controllo Privacy>Stato** nel console di configurazione. Apparirà la finestra seguente:



Stato Controllo Privacy

8.1.1. Controllo Privacy



Importante

Per evitare che gli spyware infettino il vostro computer, mantenere il **Controllo Privacy** attivo.

Il Controllo Privacy protegge il vostro computer utilizzando 5 importanti controlli di protezione:

- **Controllo Identità** - protegge i vostri dati riservati filtrando tutto il traffico HTTP e SMTP in uscita secondo le regole da voi create nella sezione **Identità**.
- **Controllo di Registro** - chiede il vostro permesso ogni volta che un programma cerca di modificare una chiave di registro per essere eseguita all'avvio di Windows.
- 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**.

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

Configurazione del 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 protezione	di	Descrizione
Permissiva		Solo il Controllo di Registro è abilitato.
Default		Controllo di Registro e Controllo identità sono abilitati.
Aggressiva		Controllo di Registro , Controllo Identità e Controllo degli Script 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.

8.1.2. Protezione Antiphishing

Phishing è un'attività criminale su Internet che utilizza tecniche sociali d'ingegneria per indurre la gente con l'inganno a fornire informazione personale.

Il più delle volte, i tentativi di phishing consistono nell'invio massiccio di e-mail che sostengono di arrivare da un'azienda affermata e legittima. Questi messaggi ingannevoli vengono inviati nella speranza che almeno qualcuno dei ricevitori, il cui profilo corrisponde con il target del phishing, venga persuaso a divulgare informazioni private.

Un messaggio di phishing presenta normalmente una questione relativa al vostro account on line. Cerca di convincervi a cliccare su un link, fornito nel messaggio, per accedere ad un sito web presumibilmente legittimo (in realtà contraffatto) dove vengono richieste informazioni personali. Vi può venir chiesto, per esempio, di confermare

informazioni sull'account, come nome utente e password, e di fornire il numero del vostro conto bancario o il codice fiscale. A volte, per essere più convincente, il messaggio potrebbe fingere che il vostro account è stato o minaccia di essere sospeso se non usate il link fornito.

Il phishing fa anche uso di spyware, come i Troiani registratori di chiavi, per rubare informazioni sull'account direttamente dal vostro computer.

I principali obiettivi del phishing sono i clienti dei servizi di pagamento on line, come eBay e PayPal, come anche le banche che offrono servizi on line. Recentemente, anche gli utenti di siti web di reti sociali sono stati presi di mira dal phishing per ottenere dati d'identificazione personale usati poi per il furto d'identità.

Per essere protetti dai tentativi antiphishing quando navigate su Internet, mantenere **Antiphishing** attivo. In questo modo, BitDefender esaminerà ogni sito web prima che accediate e vi avvertirà dell'esistenza di minacce di phishing. Può essere configurata una White List di siti web che non volete vengano esaminati da BitDefender.

Per gestire facilmente la protezione antiphishing e la White List, utilizzare la barra degli strumenti Antiphishing integrata nel Internet Explorer. Per ulteriori informazioni, vi preghiamo di riferirvi a «*Barra degli Strumenti Antiphishing*» (p. 94).

8.2. Impostazioni Avanzate - Controllo Identità

Tenere sicuri i dati riservati è una questione importante che ci preoccupa tutti. Il furto di dati ha tenuto il passo con lo sviluppo 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 Identità 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 mail corrispondente viene bloccata.

Viene fornito un supporto Multi-utente, in modo che nessun altro utente del sistema possa vedere le regole che avete configurato.

Le regole della privacy possono essere configurate nella sezione **Identità**. Per accedere a questa sezione, aprire la finestra **Impostazioni avanzate del Controllo Privacy** e quindi cliccare sulla sezione **Identità**.

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.



Nota

Se inserite meno di tre caratteri, vi verrà chiesto di validare i dati. Vi consigliamo di inserire al meno tre caratteri per evitare il blocco erroneo di messaggi e pagine web.

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

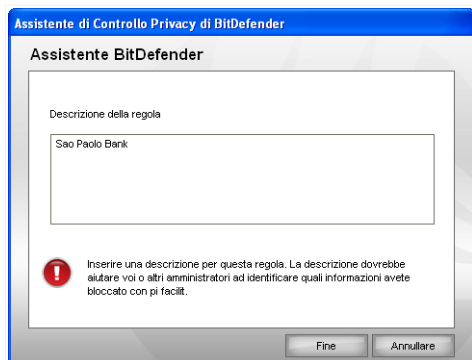
Selezionare il traffico che si desidera esaminare con BitDefender. Sono disponibili le seguenti opzioni:

- **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.

Potete scegliere di applicare la regola solo se i dati della regola corrispondono completamente oppure se le maiuscole/minuscole corrispondono.

Selezionare **Avanti**.

Passo 3/3 – Definizione Regola



Definizione Regola


Inserire una breve descrizione della regola nel campo di editing.

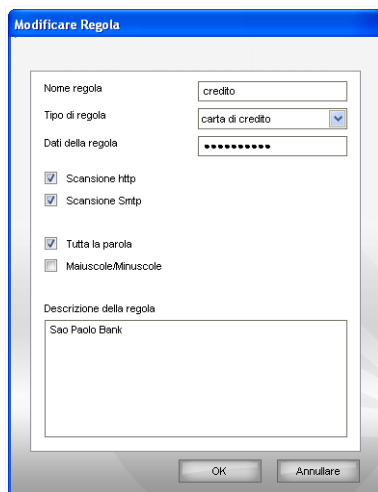
Selezionare **Termina**.

8.2.2. Definizione Eccezioni

Ci sono dei casi in cui dovrete definire eccezioni a specifiche regole d'identità. Consideriamo il caso in cui voi create una regola che impedisca l'invio attraverso HTTP (web) del numero della vostra carta di credito. Ogni volta che il numero della vostra carta di credito verrà inviato ad un sito web dal vostro account, la rispettiva pagina verrà bloccata. Se volete, per esempio, comprare delle scarpe in un negozio on line (che sapete che è sicuro), dovrete specificare un'eccezione alla rispettiva regola.

Per aprire la finestra dove si possono gestire l'eccezioni, cliccare su **Eccezioni**.

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.

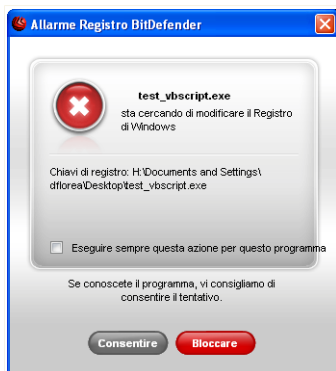
Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

8.3. Impostazioni Avanzate - 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 Registro

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

Se si desidera che BitDefender memorizzi questa risposta, selezionare **Applicare sempre questa azione a questo programma**. In questo modo, verrà creata una regola e la stessa azione verrà sempre applicata ogni volta che questo programma cerchi di modificare una chiave di registro per essere eseguita all'avvio di Windows.




Nota

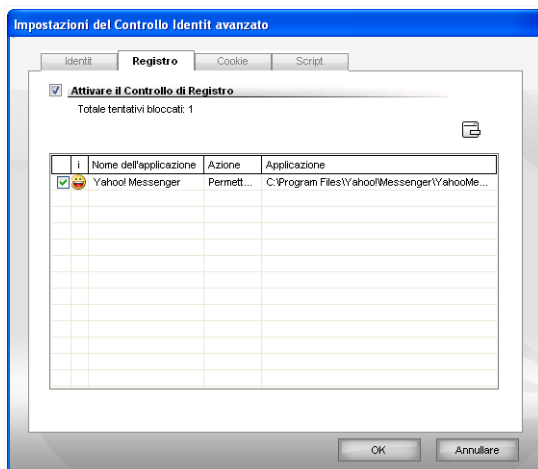
BitDefender vi allenterà quando installerete nuovi programmi che necessitano di esecuzione immediata dopo il successivo avvio del vostro computer. Nella maggior parte dei casi questi programmi sono leciti e ci si può fidare.

Si potrà accedere ad ogni regola memorizzata nella sezione **Registro** per ulteriori migliorie. Per accedere a questa sezione aprire la finestra **Impostazioni Avanzate del Controllo Privacy** e quindi cliccare sulla sezione **Registro**.



Nota

Per aprire la finestra **Impostazioni avanzate del Controllo Privacy**, cliccare su **Stato Controllo Privacy** nel console di configurazione e quindi cliccare su  **Impostazioni Avanzate**.



Controllo Registro

Potete visualizzare l'elenco delle regole create finora nella tabella.

Per eliminare una regola, selezionarla e cliccare sul tasto **Rimuovi**. Per disattivare temporaneamente una regola senza eliminarla, deselegionare la casella corrispondente.

Per cambiare l'azione di una regola, cliccare due volte sul campo dell'azione e selezionare l'opzione appropriata dal menu.

Selezionare **OK** per chiudere la finestra.

8.4. Impostazioni Avanzate - 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 **Si** 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

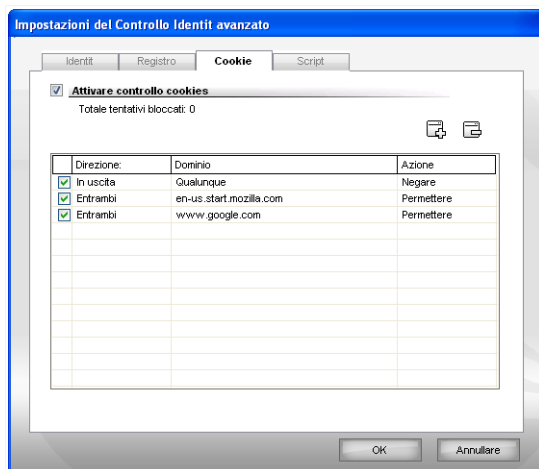
A causa del notevole numero di cookie utilizzati oggi giorno su Internet, il **Controllo dei Cookies** può risultare inizialmente abbastanza noioso. All'inizio porrà molte domande riguardo ai siti che tentano di piazzare i cookies sul vostro computer. Non appena si aggiungeranno i vostri siti abituali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

E' possibile accedere a qualsiasi regola memorizzata nella sezione **Cookies** per ulteriori perfezionamenti. Per accedere a questa sezione, aprire la finestra **Impostazioni Avanzate del Controllo della Privacy** e cliccare la sezione **Cookie**.



Nota

Per aprire la finestra **Impostazioni avanzate del Controllo Privacy**, cliccare su **Stato Controllo Privacy** nel console di configurazione e quindi cliccare su  **Impostazioni Avanzate**.



Controllo Cookie

Potete visualizzare l'elenco delle regole create finora nella tabella.



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.

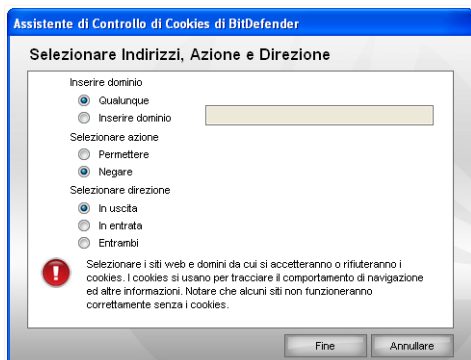
Per cancellare una regola è sufficiente selezionarla e premere **Cancella regola**. Per modificare i parametri di una regola, fare doppio click sul suo campo. Per disattivare temporaneamente una regola senza però cancellarla, rimuovere la spunta dalla casella corrispondente.

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'assistente di configurazione.

8.4.1. Assistente per la Configurazione

Assistente per la Configurazione consiste in una procedura di un solo 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.
Impedisce	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 rispettarli, impostando l'azione **Divieto** e la direzione **In uscita**.

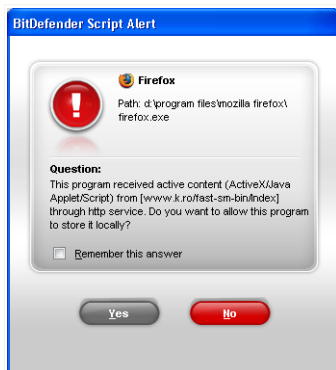
Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

8.5. Impostazioni Avanzate - Controllo Script

Gli **Scripts** e altri codici come **ActiveX controls** e **Java applets**, che sono utilizzati per creare pagine interattive, possono essere programmati 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.

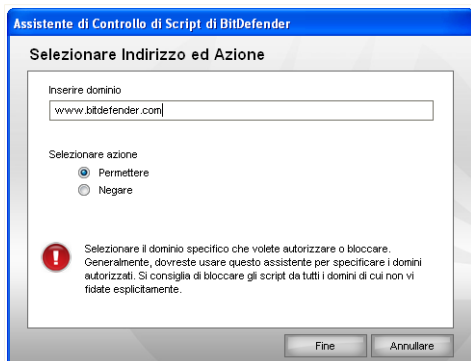
Selezionare la casella **Memorizza questa risposta** e fare click su **Si** oppure **No** e verrà creata una regola, applicata ed elencata nella tabella delle regole. Non si verrà più avvisati quando lo stesso sito tenterà di inviarvi contenuti attivi.

E' possibile accedere a qualsiasi regola memorizzata dalla sezione **Script** per ulteriori perfezionamenti. Per accedere a questa sezione, aprire la finestra **Impostazioni Avanzate del Controllo Privacy** e cliccare la sezione **Script**.

8.5.1. Assistente per la Configurazione

Assistente per la Configurazione consiste in una procedura di un solo 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**.

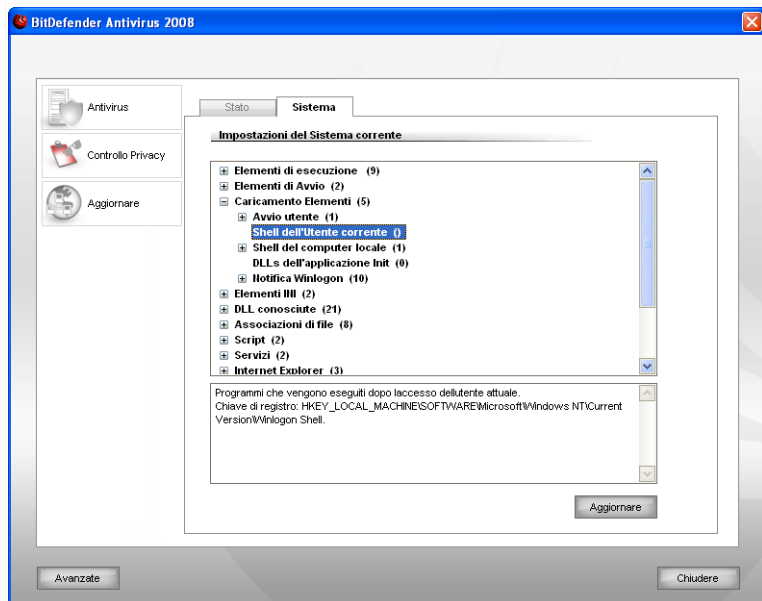
Selezionare **Applica** per salvare le modifiche e chiudere la finestra.

8.6. Sistema di Informazione

BitDefender vi permette di visualizzare, da una singola ubicazione, tutta la configurazione del sistema e le applicazioni che verranno eseguite all'avvio. In questo

modo potrete monitorare l'attività del sistema e delle applicazioni installate così come identificare possibili infezioni del sistema.

Per ottenere informazioni sul sistema cliccare su **Controllo Privacy>Informazioni di Sistema** nel console di configurazione. Apparirà la finestra seguente:



Sistema di Informazione

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. Cliccare **Si** per confermare la vostra scelta.



Nota


Se desiderate che non vi venga chiesto di nuovo di confermare la vostra scelta durante la sessione corrente, selezionare **Non chiedermi di nuovo in questa sessione**.

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

8.7. Barra degli Strumenti Antiphishing

BitDefender vi protegge da tentativi di phishing mentre navigate in Internet. Esamina i siti web visitati e vi allerta se ci sono minacce di phishing. Può essere configurata una White List di siti web che non volete vengano esaminati da BitDefender.

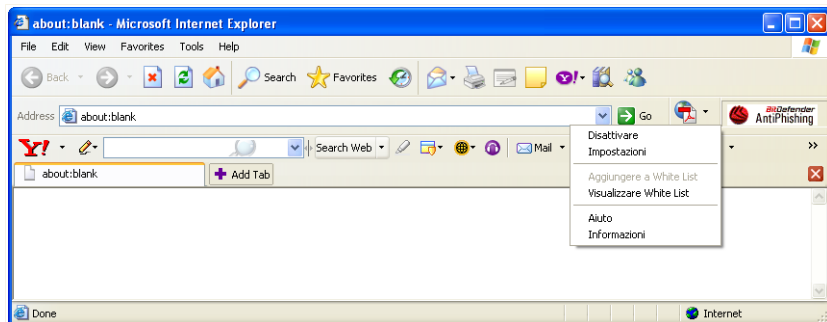
Potete gestire facilmente ed efficacemente la protezione antiphishing e la White List utilizzando la barra degli strumenti Antiphishing BitDefender integrata nell'Internet Explorer.

La barra degli strumenti antiphishing, rappresentata dall' **icona BitDefender**, si trova nella parte superiore dell'Internet Explorer. Cliccare sopra per aprire il menu della barra degli strumenti.



Nota

Se non potete visualizzare la barra degli strumenti, aprire il menu **Visualizzare**, puntare su **Barre degli strumenti** e selezionare **Barra degli strumenti BitDefender**.



Barra degli Strumenti Antiphishing

Nella barra degli strumenti sono disponibili i seguenti comandi:

- **Attivare / Disattivare** - attiva / disattiva la barra degli strumenti Antiphishing BitDefender.



Nota

Se scegliete di disattivare la barra degli strumenti Antiphishing, non sarete più protetti dai tentativi di phishing.

- **Impostazioni** - apre una finestra dove potete specificare le impostazioni della barra degli strumenti Antiphishing.

Sono disponibili le seguenti opzioni:

- **Attivare Scansione** - attiva la scansione antiphishing.
 - **Chiedere prima di aggiungere alla White List** - vi viene chiesto prima di aggiungere un sito web alla White List.
- **Aggiungere alla White List** - aggiunge il sito web corrente alla White List.



Nota

Aggiungere un sito alla White List significa che BitDefender non esaminerà più il sito per tentativi di phishing. Vi consigliamo di aggiungere alla White List solo siti di cui vi fidate pienamente.

- **Visualizzare White List** - apre la White List.

Potete vedere la lista di tutti i siti web che non vengono controllati dai motori di antiphishing BitDefender.

Se volete rimuovere un sito dalla White List in modo che vi sia notificata qualsiasi minaccia di phishing su quella pagina, cliccare sul tasto **Rimuovere**.

Potete aggiungere i siti di cui vi fidate pienamente alla White List, in modo che non verranno più esaminati dai motori antiphishing. Per aggiungere un sito alla White List, inserire il suo indirizzo nel campo corrispondente e quindi cliccare **Aggiungere**.

- **Aiuto** - apre il file di aiuto.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.

9. Aggiornamento

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

Se siete connessi ad Internet con banda larga o DSL, BitDefender si prenderà cura di sé da solo. Per default, esso cercherà degli aggiornamenti, ogni volta che avvierete il vostro computer ed ogni **orad**opo l'avvio.

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.

Il processo di aggiornamento viene eseguito involo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodottoe, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Gli aggiornamenti avvengono nei seguenti modi:

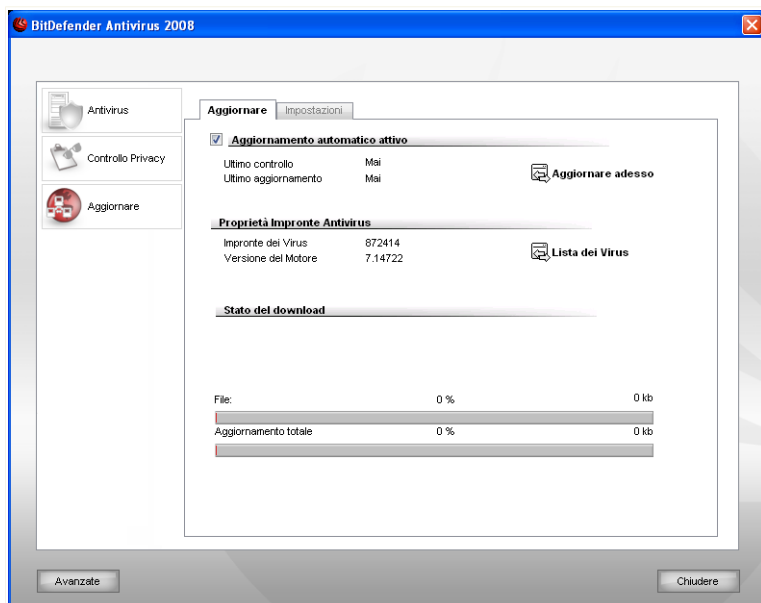
- **Aggiornamenti per motori Antivirus** - non appena compaiono nuove minacce, i files contenenti l'impronta dei virus devono essere aggiornati per garantire una protezione permanente in tempo reale. Questo tipo di aggiornamento è anche conosciuto come **Virus Definitions Update**.
- **Aggiornamenti 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 impronte antispyware saranno aggiunte al database. Questo tipo di aggiornamento è anche conosciuto come **Aggiornamento Antispyware**.
- **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**.

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

- **Aggiornamento Automatico**
- **Impostazioni dell'Aggiornamento**


9.1. Aggiornamento Automatico

Per visualizzare informazioni relative all'aggiornamento ed eseguire aggiornamenti automatici, cliccare su **Aggiornamento>Aggiornamento** nel console di configurazione. Apparirà la finestra seguente:



Aggiornamento Automatico

Qui è possibile visualizzare quando sono stati eseguiti l'ultimo controllo degli aggiornamenti e l'ultimo aggiornamento, così come le informazioni sull'ultimo aggiornamento eseguito (se con successo o gli errori verificatisi). Inoltre si mostrano informazioni sulla versione del motore corrente ed il numero di impronte.

Potete verificare le impronte dei malware del vostro BitDefender cliccando  **Mostrare Elenco dei Virus**. Verrà creato e aperto in un browser web un file HTML che contiene tutte le impronte disponibili. Potete cercare le impronte di uno specifico malware attraverso il database oppure cliccare **Lista dei Virus BitDefender** per andare al database on line delle impronte di BitDefender.


se aprite questa sezione durante un aggiornamento potrete visualizzare lo stato del download.



Importante

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

9.1.1. Richiedere un aggiornamento

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



Importante

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

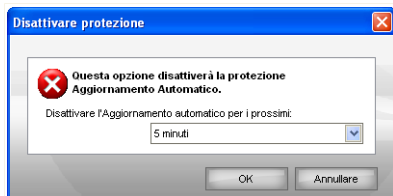


Nota

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

9.1.2. Disattivare Aggiornamento Automatico

Scegliendo di disattivare l'aggiornamento automatico, apparirà una finestra di avviso.



Disattivare Aggiornamento Automatico

Dovete confermare la vostra scelta selezionando dal menu per quanto tempo volete che l'aggiornamento automatico venga disattivato. Potete disattivare l'aggiornamento

automatico per 5, 15 o 30 minuti, per un'ora, permanentemente o fino al riavvio del sistema.



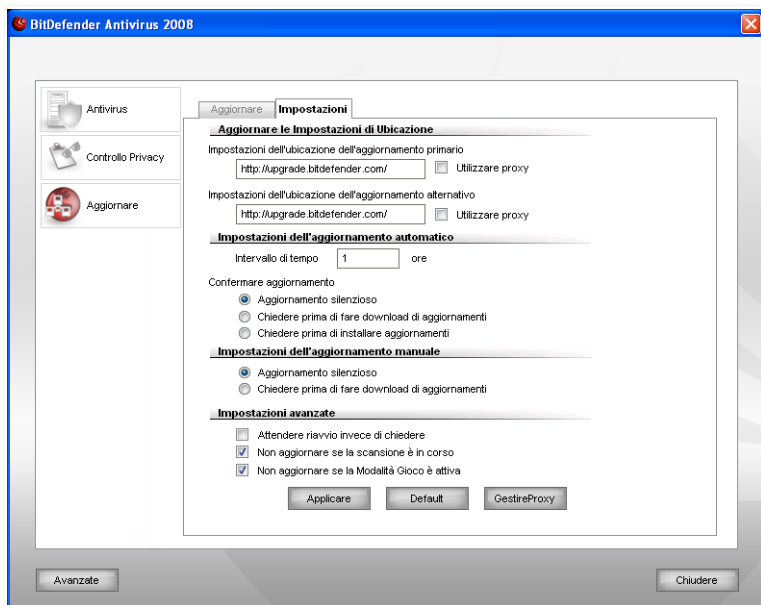
Avvertimento

Questa è una questione critica di sicurezza. Vi consigliamo di disattivare l'aggiornamento automatico per il minimo tempo possibile. Se BitDefender non verrà aggiornato regolarmente non sarà in grado di proteggervi dalle minacce più recenti.

9.2. Impostazioni dell'Aggiornamento

Gli aggiornamenti possono essere eseguiti dalla rete locale, su Internet, direttamente o attraverso un server proxy. Per default, BitDefender controllerà la disponibilità di aggiornamenti ogni ora sulla Internet ed installerà gli aggiornamenti disponibili senza avvisarvi.

Per configurare le impostazioni di aggiornamento e gestire i proxy, cliccare su **Aggiornamento>Impostazioni** nel console di configurazione. Apparirà la finestra seguente:



Impostazioni dell'Aggiornamento

Le impostazioni dell'aggiornamento sono raggruppate in 4 categorie (**Impostazioni Ubicazione Aggiornamento**, **Impostazioni Aggiornamento Automatico**, **Impostazioni Aggiornamento Manuale** ed **Impostazioni Avanzate**). Ogni categoria verrà descritta separatamente.

9.2.1. Impostare Ubicazioni Aggiornamento

Per configurare le ubicazioni dell'aggiornamento utilizzare le opzioni della categoria **Impostazioni Ubicazione Aggiornamento**.



Nota

Configurare queste impostazioni solo se siete connessi ad una rete locale che immagazzini localmente le impronte malware di BitDefender o se vi connettete ad Internet attraverso un server proxy.

Per aggiornamenti più affidabili e veloci, potete configurare due ubicazioni per l'aggiornamento: **Ubicazione principale dell'aggiornamento** e **Ubicazione**

alternativa dell'aggiornamento. Di default, queste ubicazioni sono la stessa:<http://upgrade.bitdefender.com>.

Per modificare una delle ubicazioni dell'aggiornamento, inserire l'URL dello specchio locale nel campo **URL** corrispondente all'ubicazione che si desidera modificare.



Nota

Vi consigliamo di impostare come ubicazione principale dell'aggiornamento lo specchio locale e di non modificare l'ubicazione alternativa, come piano di sicurezza interna nel caso in cui lo specchio locale non fosse disponibile.

Nel caso in cui l'azienda usi un server proxy per connettersi ad internet, selezionare **Usare proxy** e poi cliccare su **Gestione proxies** per configurare le impostazioni proxy.



Nota

Per ulteriori informazioni, vi preghiamo di riferirvi a «*Gestione Proxies*» (p. 103)

9.2.2. Configurazione Aggiornamento Automatico

Per configurare l'esecuzione automatica del processo di aggiornamento da parte di BitDefender, utilizzare le opzioni della categoria **Impostazioni Aggiornamento Automatico**.

Potete specificare il numero di ore tra due controlli consecutivi per aggiornamento nel campo **Intervallo di tempo**. Di default l'intervallo di tempo tra aggiornamenti è fissato in un'ora.

Per specificare come dovrebbe essere eseguito il processo di aggiornamento automatico, selezionare una delle seguenti opzioni:

- **Aggiornamento silenzioso** - BitDefender scarica ed implementa l'aggiornamento automaticamente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.



Nota

Vi verrà richiesto prima che gli aggiornamenti vengano scaricati anche se uscite dal Centro di Sicurezza.

- **Chiedere prima di installare gli aggiornamenti** - ogni volta che si scarica un aggiornamento, vi verrà richiesto se installarlo.



Nota

Vi verrà richiesto prima che gli aggiornamenti vengano installati anche se uscite dal Centro di Sicurezza.

9.2.3. Configurazione Aggiornamento Manuale

Per specificare come dovrà essere eseguito l'aggiornamento manuale (aggiornamento a richiesta dell'utente) selezionare una delle seguenti opzioni dalla categoria **Impostazioni Aggiornamento Manuali**:

- **Aggiornamento silenzioso** - l'aggiornamento manuale verrà eseguito automaticamente in background, senza l'intervento dell'utente.
- **Chiedere prima di scaricare gli aggiornamenti** - ogni volta che un aggiornamento è disponibile, vi verrà richiesto se eseguire il download.



Nota

Vi verrà richiesto prima che gli aggiornamenti vengano scaricati anche se uscite dal Centro di Sicurezza.

9.2.4. Configurazione delle Impostazioni Avanzate

Per evitare che il processo di aggiornamento di BitDefender interferisca con il vostro lavoro, configurare le opzioni nella categoria **Impostazioni 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.

- **Non aggiornare se la modalità gioco è attiva** - BitDefender non eseguirà l'aggiornamento se la modalità gioco è attiva. In questo modo si può minimizzare l'influenza del prodotto sulla performance del vostro sistema durante i giochi.

9.2.5. Gestione Proxies

Se la vostra azienda utilizza un server proxy per connettersi ad Internet, dovrete specificare le impostazioni di proxy perchè BitDefender si possa aggiornare da solo. Altrimenti, esso utilizzerà le impostazioni proxy dell'amministratore che installò il prodotto o, se ci sono, le impostazioni predefinite del browser dell'utente corrente.



Nota

Le impostazioni del proxy possono essere configurate solo da utenti con diritti di amministratore sul computer oppure da "power users" (utenti che conoscono la password per le impostazioni del prodotto).

Per gestire le impostazioni del proxy, cliccare su **Gestione proxies**. Apparirà la finestra **Gestore Proxy**.

Gestore del proxy

Impostazioni del proxy

Amministratore delle impostazioni del proxy (rilevato al momento dell'installazione)

Indirizzo: Porta: Nome Utente:
 Password:

Impostazioni del proxy dell'utente corrente (dal browser predefinito)

Indirizzo: Porta: Nome Utente:
 Password:

Specificare le vostre proprie impostazioni del proxy

Indirizzo: Porta: Nome Utente:
 Password:

OK Annullare

Gestore Proxy

Vi sono tre gruppi di impostazioni del proxy:

- **Impostazioni del proxy dell'Amministratore (rilevate al momento dell'installazione)** - impostazioni del proxy rilevate sull'account dell'amministratore

durante l'installazione le quali possono essere configurate solo utilizzando tale account. Se il server proxy richiede un nome utente ed una password, dovrete specificarli nei rispettivi campi.

- **Impostazioni del proxy dell'utente corrente (dal browser di default)** - Impostazioni del proxy dell'utente corrente, ricavate dal browser predefinito. Se il server proxy richiede un nome utente ed una password, dovrete specificarli nei rispettivi campi.



Nota

I browser web supportati sono Internet Explorer, Mozilla Firefox ed Opera. Se usate un altro browser di default, BitDefender non sarà in grado di ottenere le impostazioni del proxy dell'utente corrente.

- **Il vostro proprio set di impostazioni del proxy** - impostazioni del proxy che potrete configurare se vi siete registrati come amministratore.

Le seguenti impostazioni devono essere specificate:

- **Indirizzo** - inserire l'IP del server proxy.
- **Porta** - inserire la porta che utilizza BitDefender per connettersi al server proxy.
- **Nome Utente** - inserire un nome utente riconosciuto dal proxy.
- **Password** - inserire la password valida per l'utenza, già specificata precedentemente.

Quando ci si tenta di connettere ad Internet, ogni set di impostazione del proxy viene tentato uno alla volta, finchè BitDefender non riesce a connettersi.

In primo luogo verrà usato il set contenente le vostre impostazioni per connettersi ad Internet. Se questo non funzionasse, verranno utilizzate successivamente le impostazioni del proxy rilevate al momento dell'installazione. Ed infine, se neanche queste funzionassero, le impostazioni del proxy dell'utente corrente verranno ricavate dal browser predefinito ed utilizzate per connettersi ad Internet.

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

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

BitDefender Rescue CD

10. Informazioni generali sul prodotto

BitDefender™

Antivirus BitDefender 2008 arriva con un CD avviabile (BitDefender Rescue CD), in grado di eseguire la scansione e disinfettare tutti i dischi rigidi esistenti prima che il vostro sistema operativo si avvii.

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 dell'impronta dei virus viene eseguita automaticamente, senza l'intervento dell'utente, ogni volta che si avvia il Rescue CD BitDefender.

BitDefender Rescue CD 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 un antivirus di desktop capace di eseguire la scansione e disinfettare tutti i dischi rigidi esistenti (inclusando partizioni NTFS di Windows). Nello stesso tempo BitDefender Rescue CD può essere utilizzato per recuperare i vostri dati preziosi quando non si può avviare Windows

10.1. Requisiti del sistema

Prima di avviare BitDefender Rescue CD, dovete innanzitutto 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

Minimo 512 MB di Memoria RAM (raccomandati 1 GB)

CD-ROM

BitDefender Rescue CD si esegue da un CD-ROM, per cui sono richiesti un CD-ROM ed un BIOS in grado di avviarlo.

Connessione Internet

Anche se BitDefender Rescue CD funzionerà senza connessione alla rete, le procedure di aggiornamento richiederanno un link HTTP attivo, persino attraverso

alcuni server proxy. Di conseguenza, per una protezione aggiornata, la connessione ad Internet è obbligatoria.

Risoluzione grafica

Scheda grafica standard SVGA-compatibile.

10.2. Software Incluso

Il BitDefender Rescue CD include i seguenti pacchetti software.

Xedit

Questo è un editore di file di testo.

Vim

Questo è un potente editore di file di testo, contenente evidenziatore di sintassi, un GUI, e molto altro. Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di Vim](#).

Xcalc

Questa è una calcolatrice.

RoxFiler

RoxFiler è un veloce e potente gestore di file grafici.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di RoxFiler](#).

MidnightCommander

GNU Midnight Commander (mc) è un gestore di file text-mode.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di MC](#).

Pstree

Pstree mostra i processi in corso.

Top

Top mostra le funzioni Linux.

Xkill

Xkill blocca tutte le X risorse di un client.

Partition Image

Partition Image vi aiuta a salvare le partizioni nei formati dei file di sistema EXT2, Reiserfs, NTFS, HPFS, FAT16, e FAT32 in un file di immagine. Questo programma può essere utile a fini di backup.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di Partimage](#).

GtkRecover

GtkRecover è una versione GTK del console del programma di recupero. Aiuta a recuperare dei file.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di GtkRecover](#).

ChkRootKit

ChkRootKit è uno strumento che vi aiuta ad effettuare la scansione del vostro computer in cerca di rootkits.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di ChkRootKit](#).

Nessus Network Scanner

Nessus è uno scanner di sicurezza remota per Linux, Solaris, FreeBSD, e Mac OS X.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di Nessus](#).

lptraf

lptraf è un Software di monitoraggio di rete IP.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di lptraf](#).

lftop

lftop mostra l'uso di larghezza di banda su di un interfaccia.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di lftop](#).

MTR

MTR è uno strumento di diagnosi di rete.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di MTR](#).

PPPStatus

PPPStatus mostra le statistiche sul traffico TCP/IP in entrata ed in uscita.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di PPPStatus](#).

Wavemon

Wavemon è un'applicazione di monitoraggio per dispositivi di rete wireless.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di Wavemon](#).

USBView

USBView mostra informazioni sui dispositivi connessi al bus USB.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di USBView](#).

Pppconfig

Pppconfig aiuta a configurare automaticamente una connessione dial up ppp.

DSL/PPPoE

DSL/PPPoE configura una connessione PPPoE (ADSL).

I810rotate

I810rotate cambia l'output su video a i810 hardware usando i810switch(1).

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di I810rotate](#) .

Mutt

Mutt è un potente mail client MIME basato su testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di Mutt](#).

Mozilla Firefox

Mozilla Firefox è un noto browser web.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di Mozilla Firefox](#).

Elinks

Elinks browser di web in modo testo.

Per ulteriori informazioni, vi preghiamo di riferirvi alla [homepage di Elinks](#).

11. BitDefender Rescue CD fai-da-te.

Questo capitolo contiene informazioni su come iniziare e fermare il BitDefender Rescue CD, come eseguire la scansione del vostro computer alla ricerca di malware e anche come salvare dati dal vostro PC Windows compromesso su un dispositivo rimovibile. In ogni caso, utilizzando le applicazioni software contenute nel CD, potrete eseguire molti processi, la cui descrizione va oltre gli obiettivi di questo manuale.

11.1. Avviare BitDefender Rescue CD

Per avviare il CD, configurare il BIOS del vostro computer per avviarlo dal CD, inserire il CD nel drive e riavviare il computer. Assicuratevi che il vostro computer possa avviarsi dal CD.

Attendere che venga mostrata la finestra successiva e seguire le istruzioni per avviare BitDefender Rescue CD.



Boot Splash Screen

L'aggiornamento delle impronte dei virus è eseguita automaticamente. Questo potrebbe richiedere qualche istante.

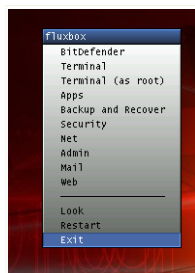
Quando il processo di avvio è finito vedrete il successivo desktop. Adesso potete cominciare ad utilizzare il BitDefender Rescue CD.



Il Desktop

11.2. Arrestare BitDefender Rescue CD

Potete chiudere il vostro computer in modo sicuro selezionando **Uscire** dal menu contestuale di BitDefender Rescue CD (tasto destro per aprirlo) o usando il comando **Fermare** su un terminale.



Scegliere "Uscire"

Quando BitDefender Rescue CD 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.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufs) (aufs) (aufs) (aufs)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksusper
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufs) (aufs) (aufs) (aufs)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Attendere questo messaggio alla chiusura

11.3. Come posso eseguire una scansione antivirus?

Un assistente apparirà quando il processo di avvio sarà terminato e vi permetterà di eseguire una scansione completa del vostro computer. Tutto quello che dovete fare è cliccare sul tasto **Avvio**.



Nota

Se la risoluzione del vostro schermo non è abbastanza alta, vi verrà chiesto di cominciare la scansione in modalità di testo.

Seguire la procedura di tre passi per completare il processo di scansione.

1. Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).



Nota

La durata del processo dipende dalla complessità della scansione.

2. Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

I problemi vengono mostrati in gruppi. Selezionare la casella "+" per aprire un gruppo oppure la casella "-" per chiudere un gruppo.

Potete scegliere di intraprendere un'azione globale per ogni gruppo di problemi oppure selezionare azioni separate per ogni problema.

3. E' possibile visualizzare il sommario dei risultati.

Se si vogliono esaminare solo alcune directory, fare come segue:

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 comando 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.

```
# bdsan /path/to/scan/
```

11.4. Come posso salvare ai miei dati?

Supponiamo che non potete avviare il vostro PC Windows a causa di problemi sconosciuti. Nello stesso tempo, avete un bisogno disperato di accedere ad alcuni dati importanti sul vostro computer. Questo è il momento in cui BitDefender Rescue CD diventa utile.

Per salvare i vostri dati dal computer ad un dispositivo rimovibile, come una penna USB, basta seguire questi passaggi:

1. Inserire BitDefender Rescue CD nel lettore CD, la penna USB nella porta USB e quindi riavviare il computer.
2. Attendere finchè BitDefender Rescue CD completi l'avvio. Apparirà la seguente finestra.



Schermo del Desktop

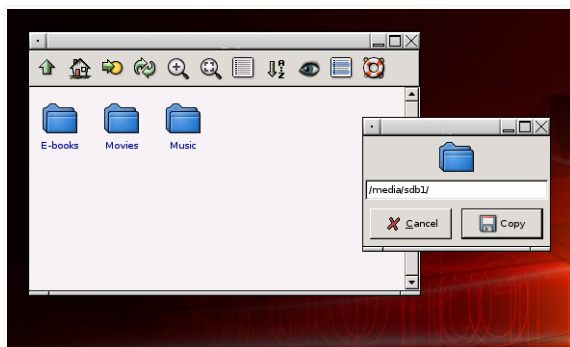
3. Cliccare due volte sulla partizione dove sono ubicati i dati che volete salvare (e.g. [sda3]).



Nota

Quando lavorate con BitDefender Rescue CD, avrete a che fare con nomi di partizioni Linux. Quindi, [sda1] probabilmente corrisponderà alla partizione Windows (C:), [sda3] alla (F:), e [sdb1] alla penna USB.

4. Sfogliare le vostre cartelle ed aprire la directory desiderata. Per esempio, MyData, contenente le sottodirectory Movies, Music ed E-books.
5. Cliccare con il tasto destro sulla directory desiderata e selezionare **Copiare**. Apparirà la seguente finestra.



Salvataggio dei dati

6. Scrivere `/media/sdb1/` nella corrispondente casella di testo e cliccare **Copiare**.

Ottenere aiuto

12. 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 il problema con la maggior accuratezza possibile.

12.1. 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>.

12.2. Chiedere Aiuto

12.2.1. Vai al Web Fai-da-te

Avete una domanda? I nostri esperti di sicurezza sono disponibili per aiutarvi 24/7 al telefono, via e-mail o chat senza costi aggiuntivi.

Vi preghiamo di seguire i links sotto:

Inglese

Antivirus 2008

<http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/>

Tedesco

Antivirus 2008

<http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/>

Francese

Antivirus 2008

<http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/>

Romeno

Antivirus 2008

<http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/>

12.2.2. Aprire un ticket di supporto

Se desiderate aprire un ticket di supporto e ricevere aiuto via mail, utilizzare uno di questi link:

Inglese: <http://www.bitdefender.com/site/Main/contact/1/>

Tedesco: <http://www.bitdefender.de/site/Main/contact/1/>

Francese: <http://www.bitdefender.fr/site/Main/contact/1/>

Romeno: <http://www.bitdefender.ro/site/Main/contact/1/>

Spagnolo: <http://www.bitdefender.es/site/Main/contact/1/>

12.3. Contatti

Una comunicazione efficiente è la chiave di un business di successo. Negli ultimi 10 anni BITDEFENDER ha acquisito una reputazione inestimabile superando le aspettative di clienti e partners, sforzandosi costantemente per una comunicazione sempre più efficiente. Se avete delle domande o richieste, non esitate a contattarci.

12.3.1. 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>

12.3.2. 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

BitDefender GmbH
Quartier generale Europa Occidentale
Karlsdorferstrasse 56
88069 Tettngang
Germany
Tel: +49 7542 9444 60
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

Supporto tecnico: support@bitdefender.com

Vendite: sales@bitdefender.com

Tel: +39 011 659 60 87

Fax: +39 011 833 86 59

http://www.bitdefender.com/it/Main/view/Prices_home.html

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 infetto 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 floppy 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 un'origine 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 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 fonte C, "ps" per PostScript, "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 report

File che elenca le azioni avvenute. BitDefender mantiene un file di report che elenca i percorsi esaminati, le cartelle, il numero di archivi, i file esaminati, quanti file 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 critici 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 qualsiasi 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.