KASPERSKY LAB

Kaspersky® Anti-Virus 7.0

MANUALE DELL'UTENTE

KASPERSKY ANTI-VIRUS 7.0

Manuale dell'utente

http://www.kaspersky.it

Data di revisione: Febbraio 2008

Sommario

CAPITOLO 1. LE MINACCE ALLA SICUREZZA DEL COMPUTER

Poiché la tecnologia informatica si è sviluppata rapidamente penetrando in ogni aspetto dell'esistenza umana, la quantità di azioni illecite volte a minare la sicurezza delle informazioni si è moltiplicata.

I criminali informatici hanno mostrato un profondo interesse nelle attività di strutture governative e imprese commerciali. Essi cercano di impadronirsi di e diffondere informazioni riservate, danneggiando la reputazione di imprese, interrompendo la continuità di attività commerciali e, di conseguenza, violando le risorse informative di organizzazioni. Questi atti possono recare gravi danni a beni materiali e immateriali.

Ma non sono solo le grandi aziende a correre rischi. Anche gli utenti privati possono cadere vittima degli attacchi informatici. Servendosi di vari strumenti, i criminali accedono ai dati personali (numero di conto corrente e carta di credito, password, ecc.), provocano anomalie di funzionamento del sistema o ottengono l'accesso completo a computer altrui. Quei computer possono quindi essere utilizzati come elementi di una rete "zombie", cioè una rete di computer infetti usati dagli hacker per attaccare server, inviare spam, impadronirsi di informazioni riservate e diffondere nuovi virus e trojan.

Oggigiorno chiunque riconosce il valore dell'informazione ed è consapevole della necessità di proteggere i dati. Al tempo stesso l'informazione deve essere facilmente accessibile a determinati gruppi di utenti (per esempio dipendenti, clienti e partner di un'impresa). Ecco perché è necessario realizzare un vasto sistema di protezione dei dati. Questo sistema deve tenere conto di tutte le possibili minacce, siano esse umane, prodotte dall'uomo o conseguenze di catastrofi naturali, e applicare una serie completa di misure protettive a livello fisico, amministrativo e di software.

1.1. Le minacce potenziali

Singole persone, gruppi di persone o perfino fenomeni non correlati ad attività umane rappresentano potenziali minacce per la sicurezza dei dati. Le minacce potenziali possono essere suddivise in tre categorie:

- **Fattore umano**. Questo gruppo riguarda le azioni di persone autorizzate o non autorizzate ad accedere ai dati. Le minacce di questo gruppo possono essere:
  - Esterne: criminali informatici, hacker, truffe via internet, partner sleali e strutture criminali.
  - Interne: azioni del personale di un'azienda e degli utenti di PC ad uso domestico. Le azioni di questo gruppo possono essere deliberate o accidentali.
- **Fattore tecnologico**. Questo gruppo si riferisce a problemi tecnici: apparecchiature obsolete o software e hardware di scarsa qualità utilizzati per l'elaborazione delle informazioni. Questi fattori determinano il malfunzionamento delle apparecchiature e frequenti perdite di dati.
- **Fattore naturale**. Questo gruppo include qualsiasi evento naturale o altri eventi non dipendenti dall'attività dell'uomo.

Un sistema di protezione dati efficiente deve tener conto di tutti questi fattori. Questo manuale dell'utente si riferisce esclusivamente a quelli di competenza diretta di Kaspersky Lab: le minacce esterne derivanti da attività umana.

1.2. La diffusione delle minacce

Man mano che la moderna tecnologia informatica e gli strumenti di comunicazione si evolvono, gli hacker possono contare su un numero crescente di opportunità per diffondere le loro minacce. Osserviamole più da vicino:

Internet

La rete Internet è unica in quanto non appartiene a nessuno e non è delimitata da confini geografici. Essa ha contribuito in molti modi allo sviluppo di innumerevoli risorse di rete e allo scambio di informazioni. Oggi tutti possono accedere ai dati disponibili su Internet o creare la propria pagina web.

Tuttavia proprio queste caratteristiche della rete offrono agli hacker la possibilità di commettere crimini via Internet, spesso senza essere individuati e puniti.

Gli hacker infettano i siti Internet con virus e altri programmi maligni facendoli passare come utili applicazioni gratuite (freeware). Inoltre gli script eseguiti automaticamente all'apertura di una pagina web sono in grado di eseguire azioni pericolose sul computer, fra cui la modifica del registro di sistema, il furto di dati personali e l'installazione di software nocivi.

Grazie alle tecnologie di rete, gli hacker possono attaccare PC e server aziendali remoti. Questi attacchi possono provocare il malfunzionamento di

parte del sistema o fornire agli hacker l'accesso completo al sistema stesso e alle informazioni in esso memorizzate. Il sistema può essere utilizzato anche come elemento di una rete "zombie".

Fin da quando è stato reso possibile l'uso delle carte di credito e di moneta elettronica su Internet per acquisti su negozi online, aste e pagine web di istituti di credito, le truffe online sono diventate uno dei crimini maggiormente diffusi.

Intranet

Intranet è una rete interna progettata specificamente per gestire le informazioni nell'ambito di un'azienda o di una rete domestica. Si tratta di uno spazio unificato per a cui tutti i computer della rete possono accedere per memorizzare, scambiare e consultare dati. Ciò significa che se un computer di tale rete è infetto, anche tutti gli altri corrono un grave rischio di infezione. Al fine di evitare una tale situazione, sia il perimetro della rete sia ogni singolo computer devono essere protetti.

E-mail

Poiché quasi tutti i computer hanno un client di posta elettronica installato e i programmi nocivi sfruttano i contenuti delle rubriche elettroniche, la diffusione di programmi nocivi può contare su condizioni ottimali. È possibile che l'utente di un computer infetto, ignaro di quanto sta avvenendo, invii e-mail infette ad amici e colleghi che, a loro volta, diffondono l'infezione. È molto comune che documenti infetti non individuati vengano inviati trasmettendo informazioni relative a grandi aziende. Quando ciò avviene, sono molti gli utenti che vengono infettati. Può trattarsi di centinaia o migliaia di persone che, a loro volta, inviano i file infetti a decine di migliaia di utenti.

Oltre alla minaccia dei programmi nocivi esiste quella della posta indesiderata, o spam. Sebbene questa non rappresenti una minaccia diretta per il computer, lo spam incrementa il carico sui server di posta, consuma larghezza di banda, riempie caselle elettroniche e determina la perdita di ore lavorative, provocando danni finanziari.

Gli hacker, inoltre, hanno iniziato a fare uso di programmi di mass mailing e di tecniche di social engineering per convincere gli utenti ad aprire messaggi e-mail o a fare clic su un determinato sito web. Le funzionalità di filtraggio antispam, di conseguenza, oltre a contrastare la posta spazzatura e i nuovi tipi di scansione online come il phishing, contribuiscono ad ostacolare la diffusione dei programmi nocivi.

Supporti di archiviazione esterni

I supporti esterni (floppy, CD-ROM e flash drive USB) sono molto usati per l'archiviazione e la trasmissione di informazioni.

All'apertura di un file contenente un codice maligno da un supporto di archiviazione esterno, è possibile che i file conservati nel computer si

infettino diffondendo il virus a tutte le altre unità del computer o agli altri computer della rete.

1.3. Tipi di minacce

Oggigiorno esistono numerosi tipi di minaccia che potrebbero pregiudicare il funzionamento di un computer. Questa sezione esamina le minacce bloccate da Kaspersky Anti-Virus.

Worm

Questa categoria di programmi nocivi si diffonde sfruttando in gran parte le vulnerabilità del sistema. Essi devono il loro nome alla capacità di "strisciare" come i vermi da un computer all'altro attraverso reti, posta elettronica e altri canali di informazione. Questa caratteristica consente ai worm di diffondersi con una velocità piuttosto elevata.

I worm penetrano all'interno di un computer, calcolano gli indirizzi di rete di altri computer e inviano loro una quantità di repliche di se stessi. Oltre agli indirizzi di rete, i worm utilizzano spesso i dati contenuti nelle rubriche dei client di posta elettronica. Alcuni di questi programmi maligni creano di quando in quando dei file di lavoro sui dischi di sistema, ma riescono a funzionare senza alcuna risorsa ad eccezione della RAM.

Virus

Programmi che infettano altri programmi aggiungendovi il proprio codice al fine di ottenere il controllo non appena un file infetto viene eseguito. Questa semplice definizione spiega il principio alla base della diffusione di un virus: l'*infezione*.

Trojan

Programmi che eseguono azioni non autorizzate, per esempio la cancellazione di dati sui drive provocando il blocco del sistema, il furto di informazioni confidenziali, ecc. Questa categoria di programmi nocivi non può essere definita virus nel senso tradizionale del termine in quanto non infetta altri computer o dati. I trojan non sono in grado di penetrare autonomamente in un computer ma vengono diffusi dagli hacker che li fanno passare per software regolare. I danni provocati dai trojan possono essere notevolmente superiori a quelli dei virus tradizionali.

Di recente, la categoria di programmi nocivi maggiormente diffusa è stata quella dei worm, seguita da virus e trojan. Alcuni programmi nocivi combinano le caratteristiche di due o addirittura tre di queste categorie.

Adware

Codice di programma incluso nel software, all'insaputa dell'utente, progettato per visualizzare messaggi pubblicitari. L'adware è solitamente incorporato nel software a distribuzione gratuita e il messaggio è situato nell'interfaccia del programma. Questi programmi spesso raccolgono anche dati personali relativi all'utente e li inviano allo sviluppatore, modificano le impostazioni del browser (pagina iniziale e pagine di ricerca, livello di protezione, ecc.) e creano un traffico che l'utente non è in grado di controllare. Tutto ciò può provocare la violazione delle regole di sicurezza e, in ultima analisi, perdite finanziarie.

Spyware

Software che raccoglie informazioni su un utente o azienda a loro insaputa. Talvolta esso si installa in un computer senza che l'utente se ne accorga. In generale gli obiettivi dello spyware sono:

- Ricostruire le azioni dell'utente su un computer;
- Raccogliere informazioni sui contenuti del disco fisso; in tal caso, ciò comporta quasi sempre la scansione di numerose directory e del registro di sistema al fine di compilare un elenco dei software installati sul computer;
- Raccogliere informazioni sulla qualità della connessione, larghezza di banda, velocità del modem, ecc.

Riskware

Software potenzialmente rischioso che non svolge una funzione nociva vera e propria ma che può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. Questi programmi includono, per esempio, alcune utilità di amministrazione remota, commutatori di tastiera, client IRC, server FTP e utilità multifunzione per interrompere processi o per nasconderne il funzionamento.

Esiste un altro tipo di programma nocivo trasmesso con adware, spyware e riskware: sono quei programmi che penetrano nel web browser e ridirigono il traffico. Chiunque abbia avuto l'esperienza di aprire un sito web credendo di caricarne uno diverso, quasi certamente ha incontrato uno di questi programmi.

Joke

Software che non reca alcun danno diretto ma visualizza messaggi secondo i quali il danno è già stato provocato o lo sarà in circostanze particolari. Questi programmi spesso comunicano all'utente la presenza di rischi inesistenti, per esempio sulla formattazione del disco fisso (anche se non ha luogo alcuna formattazione) o l'individuazione di virus in file non infetti.

Rootkit

Utilità che celano attività nocive. Essi nascondono programmi nocivi che impediscono agli antivirus di individuarli. I rootkit modificano il sistema operativo del computer e ne alterano le funzioni di base per nascondere la propria esistenza e le azioni intraprese dagli hacker sul computer infetto.

Altri programmi pericolosi

Programmi creati per lanciare attacchi DoS su server remoti e penetrare in altri computer, e programmi che fanno parte dell'ambiente di sviluppo dei programmi nocivi. Essi includono hack tool, virus builder, scanner di vulnerabilità, programmi di individuazione di password, e altri tipi di programma per penetrare in un sistema o utilizzare risorse di rete.

Kaspersky Anti-Virus utilizza due metodi per riconoscere e bloccare questi tipi di minacce:

- *Reattivo:* usa un aggiornamento continuo dai database applicativi per riconoscere oggetti pericolosi. Questo metodo richiede almeno una istanza di infezione perché il nome dell'infezione possa essere aggiunto ai database che elencano le minacce ed essere distribuiti con gli aggiornamenti.
- *Proattivo* – contrariamente al metodo reattivo questo metodo non analizza il codice degli oggetti ma piuttosto il loro comportamento nel sistema. Il suo scopo è quello di individuare minacce non ancora ufficialmente riconosciute.

Utilizzando entrambi i metodi Kaspersky assicura una adeguata protezione al vostro computer nei confronti di manacce note e nuove.

Attenzione!

In seguito useremo il termine "virus" riferendosi sia a programmi maligni sia pericolosi. Solo se necessario verrà enfatizzato il grado di malignità.

1.4. Segnali di infezione

Vi sono numerosi segnali che indicano la presenza di un virus all'interno del computer. Di solito il computer si comporta in maniera strana, in particolare:

- Il video visualizza messaggi o immagini impreviste, oppure il computer emette suoni anomali;
- Il lettore CD/DVD-ROM si apre e si chiude inaspettatamente;
- Il computer apre arbitrariamente un programma non richiesto dall'utente;

- Il video visualizza messaggi pop up che informano che un determinato programma nel computer sta cercando di accedere a Internet, anche se tale azione non è stata richiesta dall'utente.

Sono note anche alcune tipiche caratteristiche di infezione via e-mail:

- Amici e parenti sostengono di aver ricevuto messaggi che l'utente non ha mai inviato;
- La casella di posta elettronica contiene numerosi messaggi privi di mittente o intestazione.

Occorre specificare che questi segnali possono anche essere il risultato di problemi diversi dai virus. Talvolta hanno effettivamente altre cause. Per esempio, nel caso della posta elettronica, è possibile che i messaggi infetti vengano inviati con l'indirizzo di un mittente specifico ma non dal suo computer.

Vi sono anche sintomi indiretti che indicano una probabile infezione del computer:

- Il computer si blocca o ha crash frequenti;
- Il computer carica i programmi con eccessiva lentezza;
- Non si riesce ad avviare il sistema operativo;
- File e cartelle scompaiono o i loro contenuti risultano modificati;
- Si osservano frequenti accessi al disco fisso (la spia lampeggia);
- Il browser web (per esempio Microsoft Internet Explorer) si blocca o ha comportamenti anomali (per esempio non si riesce a chiudere la finestra del programma).

Nel 90% dei casi, questi segnali indiretti sono provocati da anomalie di funzionamento dell'hardware o del software. Malgrado questi segnali dipendano raramente da un'infezione del computer, si raccomanda di effettuare una scansione completa del computer (vedi 5.3 a pag. 54.) se dovessero manifestarsi.

1.5. Come comportarsi se il computer mostra segni di infezione

Se il computer ha un comportamento "sospetto":

1. Evitare il panico! Non lasciarsi prendere dal panico. È questa la regola principale da seguire in quanto può evitare la perdita di dati importanti e numerose seccature.
2. Scollegare il computer da Internet o da un'eventuale rete locale.
3. Se il sintomo riscontrato consiste nell'impossibilità di effettuare il boot dal disco fisso (il computer visualizza un messaggio d'errore all'accensione), provare ad avviare la macchina in modalità provvisoria o dal disco di boot di Windows creato durante l'installazione del sistema operativo.
4. Prima di eseguire qualsiasi operazione, effettuare una copia di backup del lavoro su un supporto esterno (floppy, CD, unità flash, ecc.).
5. Installare Kaspersky Anti-Virus, se non lo si è già fatto.
6. Aggiornare gli elenchi delle minacce del programma (vedere 5.6 a pag. 56). Se possibile, procurarsi gli aggiornamenti accedendo a Internet da un computer non infetto, per esempio da un amico, in un Internet point o in ufficio. È consigliabile utilizzare un computer diverso, poiché connettendosi a Internet da un computer infetto è probabile che il virus invii informazioni importanti agli hacker o si diffonda agli indirizzi presenti nella rubrica. In altre parole, se si sospetta un'infezione, la precauzione migliore è scollegarsi immediatamente da Internet. È possibile procurarsi gli aggiornamenti degli elenchi delle minacce anche su un dischetto floppy da Kaspersky Labs o dai suoi distributori e aggiornare le proprie firme dal dischetto.
7. Selezionare il livello di protezione Consigliato dagli esperti di Kaspersky Labs.
8. Avviare una scansione completa del computer (vedere 5.3 a pag. 54).

1.6. Prevenzione delle infezioni

Neanche le misure più affidabili e attente sono in grado di garantire una protezione assoluta dai virus e dai trojan, ma l'osservanza di queste regole

riduce significativamente la probabilità di attacchi di virus e il livello di danno potenziale.

Come in medicina, una delle regole fondamentali per evitare le infezioni è la *prevenzione*. La profilassi del computer comporta poche regole che, se rispettate, possono ridurre in maniera considerevole la probabilità di incorrere in un virus e perdere dati.

Le regole di sicurezza fondamentali sono descritte di seguito. Osservandole è possibile evitare attacchi virulenti.

Regola 1: *Usare un software antivirus e programmi di sicurezza Internet*. Procedere come segue:

- Installare al più presto Kaspersky Anti-Virus.
- Aggiornare regolarmente (vedere 5.6 a pag. 56 gli elenchi delle minacce del programma. È possibile aggiornare gli elenchi più volte al giorno durante le epidemie di virus. In tali circostanze, gli elenchi delle minacce sui server di aggiornamento Kaspersky Lab vengono aggiornate istantaneamente.
- Selezionare le impostazioni di sicurezza raccomandate da Kaspersky Lab per il computer. Esse garantiscono una protezione costante dall'accensione del computer, ostacolando la penetrazione dei virus.
- Configurare le impostazioni di scansione completa raccomandate dagli esperti di Kaspersky Lab e pianificare scansioni almeno una volta la settimana. Se non avete installato un Firewall raccomandiamo di farlo per proteggere il computer quando ci collega ad Internet.

Regola 2: *Usare cautela nella copia di nuovi dati sul computer*:

- Eseguire la scansione antivirus di tutte le unità di archiviazione esterne (vedi 5.5 a pag. 55) come floppy, CD, unità flash, ecc., prima di usarle.
- Trattare i messaggi e-mail con cautela. Non aprire alcun file arrivato per posta elettronica se non si ha la certezza di esserne l'effettivo destinatario, anche se il mittente è una persona nota.
- Trattare con prudenza qualsiasi informazione ottenuta tramite Internet. Se un sito web suggerisce di installare un nuovo programma, verificare che esso abbia un certificato di sicurezza.
- Se si copia un file eseguibile da Internet o da una rete locale, ricordarsi di esaminarlo con Kaspersky Anti-Virus.
- Selezionare con prudenza i siti web da visitare. Molti siti sono infetti da script pericolosi o worm di Internet.

Regola 3: *Prestare attenzione alle informazioni fornite da Kaspersky Lab.*

Nella maggior parte dei casi, Kaspersky Lab annuncia un'epidemia con largo anticipo rispetto al periodo di massima diffusione. In tal modo le probabilità di contrarre l'infezione sono esigue, e una volta scaricati gli aggiornamenti si disporrà di tempo a sufficienza per proteggersi dal nuovo virus.

Regola 4: *Non fidarsi delle bufale* come i programmi-scherzo (prank) e le e-mail relative a presunte infezioni.

Regola 5: *Usare lo strumento di aggiornamento di Windows* e installare regolarmente gli aggiornamenti del sistema operativo.

Regola 6: *Acquistare sempre software dotato di regolare licenza da rivenditori autorizzati.*

Regola 7: *Limitare il numero di persone che possono accedere al computer.*

Regola 8: *Contenere il rischio di conseguenze spiacevoli in caso di infezione*:

- Eseguire regolarmente una copia di backup dei dati. Se si perdono i dati, il sistema sarà in grado di ripristinarli piuttosto rapidamente se si dispone di copie di backup. Conservare in un luogo sicuro i dischetti floppy, i CD, le unità flash e altri supporti di archiviazione contenenti software e informazioni importanti.
- Creare un disco di emergenza (vedi 15.4 a pag. 184) con il quale effettuare eventualmente il boot della macchina con un sistema operativo pulito.

Regola 9: C*ontrollare regolarmente l'elenco dei programmi installati sul computer*. A tal fine, aprire **Installazione applicazioni** in **Pannello di controllo** oppure aprire la cartella **Programmi**. È possibile scoprirvi applicazioni installate all'insaputa dell'utente, per esempio durante la navigazione in Internet o l'installazione di un programma. Alcune di esse sono quasi sempre programmi potenzialmente rischiosi.

CAPITOLO 2. KASPERSKY ANTI-VIRUS 7.0

Kaspersky Anti-Virus 7.0 è la nuova generazione dei prodotti per la sicurezza dei dati.

La caratteristica che contraddistingue Kaspersky Anti-Virus 7.0 rispetto ad altri software, perfino da altri prodotti Kaspersky Lab, è l'approccio complesso alla sicurezza dei dati conservati nel computer.

2.1. Le nuove funzioni di Kaspersky Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 (di seguito definito "Kaspersky Anti-Virus", o "il programma") offre un approccio innovativo alla sicurezza dei dati. La caratteristica principale del programma è la combinazione in un'unica soluzione delle funzioni esistenti di tutti i prodotti dell'azienda, in versione potenziata. Il programma offre protezione contro i virus. Nuovi moduli offrono protezione da minacce sconosciute.

In altre parole, garantisce una sicurezza globale del computer senza la necessità di installare numerosi prodotti. Solo questo è un valido motivo per installare Kaspersky Anti-Virus 7.0.

Tutti i canali di accesso o uscita dei dati sono protetti in maniera esauriente. Le impostazioni flessibili di ciascun componente del programma consentono di adattare in maniera ottimale Kaspersky Anti-Virus alle esigenze di ogni utente. È possibile inoltre impostare tutti i componenti di protezione da una singola postazione.

Esaminiamo in dettaglio le nuove funzioni di Kaspersky Anti-Virus 7.0.

Nuove funzionalità di protezione

- Kaspersky Anti-Virus protegge il computer da programmi nocivi noti e da programmi non ancora scoperti. La difesa proattiva (vedi Capitolo 10 a pag. 117) è il vantaggio principale del programma. Esso è studiato per analizzare il comportamento delle applicazioni installate sul computer, monitorare le modifiche al registro di sistema, individuare le macro e combattere le minacce nascoste. Il componente si basa su un analizzatore euristico in grado di individuare vari tipi di programmi nocivi. Così facendo, compila una cronologia delle attività nocive grazie

alla quale è possibile retrocedere e ripristinare l'ultima versione sicuramente funzionante del sistema prima dell'attività nociva.

- La tecnologia di File Anti-Virus è stata potenziata per abbassare il carico sul processore e sui dischi di sottosistema ed incrementare la velocità delle scansioni usando iChecker e iSwift. Così facendo, il programma evita di effettuare scansioni ripetute dei file.
- Il processo di scansione si svolge adesso in modalità secondaria mentre l'utente continua a usare il computer. Se si verificassero degli inconvenienti nelle risorse di sistema la scansione virus si interrompe fino a quando l'operatore ha completato l'operazione e poi la scansione riprende dal punto in cui si era interrotta.
- Azioni specifiche sono assegnate per scansionare le Aree Critiche del computer e gli oggetti di avvio che potrebbero causare seri problemi se infettati e per rilevare rootkits usati per nascondere malware nel sistema. Queste azioni possono essere configurate in modo da attivarsi automaticamente ad ogni avvio del sistema.
- La protezione della posta elettronica contro i programmi nocivi è stata considerevolmente migliorata. Il programma esegue la scansione antivirus delle e-mail inviate con i seguenti protocolli:
  - IMAP, SMTP, POP3, indipendentemente dal client di posta utilizzato
  - NNTP, indipendentemente dal client di posta utilizzato
  - MAPI, HTTP (con il plug-in per MS Outlook e The Bat!)
- Sono disponibili plug-in specifici per i client di posta più comuni come Outlook, Microsoft Outlook Express e The Bat!, che consentono di configurare direttamente dal client la protezione antivirus della posta.
- La funzione di notifica dell'utente (vedi 15.9.1 a pag. 197) è stata ampliata includendo determinati eventi che si verificano durante il funzionamento del programma. È possibile scegliere per ciascun evento uno dei seguenti metodi di notifica: e-mail, segnalazione acustica, messaggi a comparsa.
- È stata aggiunta la possibilità di scansionare il traffico che avviene su un protocollo SSL.
- Nuove caratteristiche hanno incluso la tecnologia di autodifesa, protezione da accessi remoti non autorizzati dei servizi di Kaspersky Anti-Virus, e protezione della password nelle impostazioni del programma. Queste funzioni impediscono ai programmi nocivi, agli hacker e agli utenti non autorizzati di disabilitare la protezione.

- E' stata aggiunta la possibilità di creare un disco di emergenza. Utilizzando questo disco potete riavviare il vostro sistema operativo dopo un attacco e procedere al suo controllo con una scansione.
- E' stato aggiunto News Agent. E' un modulo progettato per pubblicare in tempo reale nuovi contenuti provenienti da Kaspersky Lab.

Nuove funzioni dell'interfaccia

- La nuova interfaccia di Kaspersky Anti-Virus agevola l'uso delle funzioni del programma. È possibile anche modificare l'aspetto del programma creando e utilizzando una grafica e uno schema cromatico personalizzati.
- Il programma offre regolarmente suggerimenti durante l'uso: Kaspersky Anti-Virus visualizza messaggi informativi sul livello di protezione ed incorpora una esauriente Guida. L'applicazione fornisce una procedura completa di immagini circa lo stato della protezione e consente di procedere direttamente alla risoluzione dei problemi.

Nuove funzioni di aggiornamento del programma

- Questa versione del programma introduce una migliorata procedura di aggiornamento: Kaspersky Anti-Virus controlla automaticamente la disponibilità di aggiornamenti dei moduli del programma.. Gli aggiornamenti vengono scaricati automaticamente non appena il programma ne rileva la disponibilità.
- Il programma scarica solo gli aggiornamenti non ancora installati. Questo riduce il traffico del download degli aggiornamenti fino a 10 volte.
- Gli aggiornamenti vengono scaricati dalle fonti più efficienti.
- E' possibile scegliere di non utilizzare un server proxy se gli aggiornamenti del programma vengono scaricati da un'origine locale. Ciò riduce considerevolmente il carico sul server proxy.
- E' stata implementata la funzionalità di rollback (ritorno) per ripristinare una precedente versione del database applicativo nel caso di file danneggiato od errori durante la copia.
- La funzione di aggiornamento comprende ora uno strumento che rende gli aggiornamenti accessibili agli altri computer della rete copiandoli da una cartella locale. Ciò riduce il traffico sulla banda di trasmissione.

2.2. Gli elementi della protezione di Kaspersky Anti-Virus

La protezione di Kaspersky Anti-Virus è stata studiata tenendo conto delle provenienze delle minacce. In altre parole, ogni tipo di minaccia è gestito da un componente distinto del programma, monitorato e affrontato con le misure necessarie a impedirne gli effetti nocivi sui dati dell'utente. Questa struttura rende flessibile il sistema, offrendo facili opzioni di configurazione per tutti i componenti in modo da soddisfare le esigenze di utenti specifici o aziende nella loro globalità.

Kaspersky Anti-Virus incorpora:

- Componenti di protezione in tempo reale (vedi 2.2.1 a pag. 22) per una difesa globale su tutti i canali di trasmissione e scambio dati del computer.
- Attività di scansione antivirus (vedi 2.2.2 a pag. 23) usati per la scansione di singoli file, cartelle, dischi o aree alla ricerca di virus o per una scansione completa del computer.
- Aggiornamenti (vedi 2.2.3 a pag. 24) che assicurano la validità dei moduli applicativi interni e dei database per la ricerca di malware.

2.2.1. Componenti di protezione in tempo reale

I componenti di protezione garantiscono la sicurezza del computer in tempo reale:

File Anti-Virus

Un file system può contenere virus e altri programmi pericolosi. I programmi nocivi possono restare nel file system per anni dopo esservi stati introdotti attraverso un dischetto floppy o navigando in Internet, senza mostrare la propria presenza. Ma è sufficiente aprire il file infetto o, per esempio, provare a copiarlo su un disco, per attivare immediatamente il file.

File Antivirus è il componente che monitora il file system del computer. Esso esamina tutti i file che possono essere aperti, eseguiti o salvati sul computer e su tutte le unità disco collegate. Kaspersky Anti-Virus intercetta ogni file che viene aperto e lo esamina per escludere la presenza di virus noti. Il file esaminato potrà essere utilizzato solo se non infetto o se successivamente trattato mediante File Anti-Virus. Se per qualsiasi motivo non fosse possibile

riparare un file infetto, esso viene eliminato dopo averne salvata una copia nella cartella Backup (vedi 15.2 a pag. 174), o trasferito in Quarantena (vedi 15.1 a pag. 170).

Mail Anti-Virus

La posta elettronica è molto utilizzata dagli hacker per diffondere programmi nocivi e rappresenta uno dei canali più diffusi per la diffusione di worm. Per questo è estremamente importante monitorare tutta la posta.

Mail Anti-Virus è il componente che esamina tutti i messaggi e-mail in entrata e in uscita dal computer, in cerca di programmi nocivi. Il programma consente al destinatario di aprire il messaggio solo se privo di oggetti pericolosi.

Web Anti-Virus

Ogni volta che si apre un sito web si corre il rischio di restare infettati dai virus presenti negli script eseguiti sui siti web, e di scaricare oggetti pericolosi sul proprio computer.

Web Anti-Virus è pensato specificamente per prevenire tali evenienze. Questo componente intercetta e blocca gli script dei siti web potenzialmente pericolosi, monitorando accuratamente tutto il traffico HTTP.

Difesa proattiva

Il numero di programmi nocivi cresce giornalmente. Essi diventano sempre più complessi combinando più tipi di minaccia, e i metodi utilizzati per diffondersi sono sempre più difficili da scoprire.

Per individuare un nuovo programma nocivo prima che abbia il tempo di provocare danni, Kaspersky Lab ha sviluppato uno speciale componente dal nome *Difesa proattiva*. Esso è progettato per monitorare e analizzare il comportamento di tutti i programmi installati sul computer. Kaspersky Anti-Virus prende una decisione in base alle azioni eseguite da un'applicazione: il programma è potenzialmente pericoloso? Difesa proattiva protegge il computer sia dai virus noti sia da quelli non ancora scoperti.

2.2.2. Attività di scansione antivirus

Oltre a monitorare costantemente i potenziali accessi di programmi nocivi, è estremamente importante eseguire periodicamente la scansione antivirus del computer. Ciò è necessario al fine di escludere la diffusione di programmi nocivi non rilevati dai componenti di sicurezza in tempo reale a causa della protezione impostata su un livello basso o per altri motivi.

Kaspersky Anti-Virus offre tre attività di scansione antivirus:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del computer, fra cui: memoria di sistema, oggetti di avvio del sistema, master boot del disco fisso, cartella di sistema di *Microsoft Windows.* L'obiettivo di questa attività è individuare rapidamente i virus attivi nel sistema senza eseguire una scansione completa del computer.

Risorse del computer

La scansione antivirus viene effettuata sull'intero computer, con un'analisi approfondita di tutte le unità disco, memoria e file.

Oggetti di avvio

La scansione antivirus viene effettuata su tutti i programmi caricati automaticamente all'avvio, sulla RAM e sui settori di boot dei dischi fissi.

Scansione Rootkit

Scansiona il computer per riconoscere rootkit che nascondono programmi pericolosi nel sistema operativo. Queste utility iniettate nel sistema, nascondono la loro presenza e la presenza di processi, cartelle e chiavi di registro dei programmi pericolosi descritti nella configurazione del rootkit.

È possibile inoltre creare altre attività di ricerca dei virus e pianificarne l'esecuzione. Per esempio, è possibile creare un'attività di scansione per i database della posta da eseguire una volta la settimana, o un'attività di scansione antivirus della cartella **Documenti**.

2.2.3. Aggiornamento

Kaspersky si avvale di aggiornamenti in tempo reale per essere sempre pronto ad eliminare un virus o altri programmi pericolosi. L'aggiornamento è progettato per consentire esattamente questo. E' responsabile dell'aggiornamento dei database e dei moduli applicativi utilizzati da Kaspersky Anti-Virus.

La caratteristica di distribuzione dell'aggiornamento permette di salvare su una cartella locale i database ed i moduli del programma reperiti dai server di Kaspersky Lab e quindi assicurare l'accesso ad essi da parte di altri computer connessi in rete per ridurre il traffico Internet.

2.2.4. Strumenti del programma

Kaspersky Anti-Virus offre una serie di strumenti di supporto progettati per fornire assistenza software in tempo reale, espandendo le funzionalità del programma e assistendo l'utente durante la procedura.

Report e File dati

Durante il funzionamento, l'applicazione genera un report per ciascun componente di protezione in tempo reale, azioni di scansione ed aggiornamento dell'applicazione. Questo contiene le informazioni circa i risultati delle operazioni eseguite. Attraverso i Report sono disponibili tutti i dettagli di ogni componente di Kaspersky Anti-Virus. In caso di problemi, è possibile inviare i report a Kaspersky Lab in modo da consentire ai nostri esperti di studiare la situazione in maniera approfondita e fornire una soluzione nella maniera più rapida possibile.

Kaspersky Anti-Virus invia tutti i file sospetti in una speciale area denominata *Quarantena*. Essi vengono salvati in forma codificata al fine di evitare di infettare il computer. Questi oggetti possono essere sottoposti a scansione antivirus, ripristinati nella posizione originaria, o eliminati. Gli oggetti possono essere messi in quarantena anche manualmente. Tutti i file che al termine della scansione antivirus non risultano infetti vengono automaticamente ripristinati nella posizione originaria.

Backup contiene le copie dei file ripuliti o eliminati dal programma. Queste copie vengono create per l'eventualità in cui si renda necessario ripristinare file o ottenere informazioni sull'infezione. Le copie di backup dei file sono salvate in forma criptata per evitare la diffusione dell'infezione. I file contenuti nell'area Backup possono essere ripristinati nella posizione originale ed eliminati.

Attivazione

Con l'acquisto di Kaspersky Anti-Virus si accetta un contratto di licenza con Kaspersky Lab che regola l'utilizzo dell'applicazione e l'accesso agli aggiornamenti ed al Supporto Tecnico per un dato periodo di tempo. Le condizioni per l'uso ed altre informazioni necessarie al completo funzionamento del programma sono contenuto in un file. Nella sezione Attivazione è possibile trovare informazioni dettagliate per la chiave che si sta utilizzando oppure acquistare un a nuova chiave.

Supporto

Tutti gli utenti registrati di Kaspersky Anti-Virus possono avvalersi del nostro servizio di assistenza tecnica. Per informazioni su come ottenere tale assistenza, usare la funzione *Supporto*.

Seguendo questi link potete accedere al forum degli utenti di Kaspersky Lab o inviare, utilizzando un apposito documento presente on-line, informazioni o identificazioni di errori al Supporto Tecnico.

Avrete anche accesso all'Assistenza web, ai servizi di Assistenza personalizzata e naturalmente i nostri esperti saranno sempre disponibili telefonicamente per risolvere qualsiasi problema legato all'uso di Kaspersky Anti-Virus.

2.3. Requisiti di sistema hardware e software

Per garantire il corretto funzionamento di Kaspersky Anti-Virus 7.0, il computer deve possedere i seguenti requisiti minimi:

Requisiti di carattere generale:

- 50 MB di spazio disponibile sul disco fisso
- CD-ROM (per installare Kaspersky Anti-Virus 7.0 dal CD di installazione)
- Microsoft Internet Explorer 5.5 o successivo (per aggiornare i database e i moduli del programma attraverso Internet)
- Microsoft Windows Installer 2.0

Microsoft Windows 2000 Professional (Sevice Pack 2 o superiore), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Sevice Pack 2 o superiore), Microsoft Windows XP Professional x64 Edition:

- Processore Intel Pentium 300 MHz o superiore (o compatibile)
- 128 MB di RAM

Microsoft WindowsVista, Microsoft WindowsVistax64:

- Processore Intel Pentium 800 MHz 32-bit (x86)/64-bit o superiore (o compatibile)
- 512 MB di RAM

2.4. Pacchetti software

Kaspersky Anti-Virus può essere acquistato presso i nostri rivenditori, nella versione in scatola, oppure via Internet (per esempio su www.kaspersky.it, nella sezione **eStore**).

La versione in scatola include:

- Una busta sigillata con CD di installazione contenente i file del programma
- Un manuale d'uso
- Il codice di attivazione del programma, applicato sulla busta del CD di installazione

- Il contratto di licenza con l'utente finale (EULA)

Prima di rompere il sigillo della busta contenente il CD di installazione, leggere attentamente l'EULA.

Chi acquista Kaspersky Anti-Virus attraverso Internet, copierà il prodotto dal sito web di Kaspersky Lab (**Downloads → Product Downloads**). Il manuale d'uso del prodotto può essere scaricato nella sezione **Downloads → Documentation**.

A pagamento avvenuto, l'utente riceverà per e-mail il codice di attivazione.

Il Contratto di licenza è un accordo con valore legale fra l'utente finale e Kaspersky Lab, volto a regolamentare le condizioni di utilizzo del prodotto acquistato.

Leggere attentamente il Contratto di licenza per l'utente finale.

Se non si accettano i termini del Contratto di licenza, è possibile restituire il prodotto completo di scatola al distributore presso cui è stato effettuato l'acquisto, e ottenere il rimborso completo dell'importo pagato. Ciò è possibile a condizione che la busta sigillata contenente il CD di installazione sia ancora sigillata.

L'apertura della busta sigillata del CD di installazione comporta l'accettazione dei termini e delle condizioni del Contratto di licenza da parte dell'acquirente.

2.5. Assistenza per gli utenti registrati

Kaspersky Lab offre ai propri utenti registrati una serie di servizi volti ad ottimizzare l'efficacia di Kaspersky Anti-Virus.

Dopo l'attivazione del programma si diventa automaticamente utenti registrati e si ha diritto ai seguenti servizi fino alla scadenza della licenza:

- Nuove versioni del programma, a titolo gratuito
- Consulenza telefonica e via e-mail su problematiche relative all'installazione, alla configurazione e al funzionamento del programma
- Comunicazioni sui nuovi prodotti di Kaspersky Lab e sui nuovi virus (questo servizio è riservato agli utenti iscritti alla newsletter di Kaspersky Lab http://support.kaspersky.com/subscribe/)

Kaspersky Lab non fornisce assistenza tecnica relativa all'uso e al funzionamento del sistema operativo o di qualsiasi altro prodotto di altri fabbricanti.

CAPITOLO 3. INSTALLAZIONE DI KASPERSKY ANTI-VIRUS 7.0

Kaspersky Anti-Virus 7.0 può essere installato su un host in vari modi:

- in modo interattivo, utilizzando la procedura guidata di installazione (vedi 3.1 a pag. 28) questa modalità richiede un'immissione da parte dell'utente affinché l'installazione proceda;
- in modo non interattivo; questo tipo di installazione è eseguito dalla riga di comando e non richiede alcuna immissione da parte dell'utente (vedere 3.3 a pag. 40).

Attenzione!

Prima di avviare l'installazione di Kaspersky Anti-Virus raccomandiamo di chiudere tutte le altre applicazioni.

3.1. Procedura di installazione utilizzando la procedura guidata

Nota:

La procedura di installazione per mezzo di un pacchetto scaricato da Internet è uguale a quella per mezzo del CD.

Per installare Kaspersky Anti-Virus sul computer, avviare il file di installazione sul CD.

Tale file cercherà di localizzare il pacchetto di installazione dell'applicazione (file con estensione *.msi) e, in caso di esito positivo, all'utente viene chiesto di verificare la presenza di aggiornamenti di Kaspersky Anti-Virus sui server Kaspersky Lab. Se non viene trovato alcun pacchetto di installazione, il prodotto dovrà essere scaricato. In seguito al download, inizia il processo di installazione. Se l'utente sceglie di non procedere al download, l'installazione continuerà normalmente.

Si apre una procedura di installazione guidata del programma. Ogni finestra contiene dei pulsanti che consentono di completare il processo. Ecco una breve descrizione delle loro funzioni:

- **Avanti** – conferma un'azione e apre la fase successiva dell'installazione.
- **Indietro** – riporta alla fase precedente dell'installazione.
- **Cancella** – annulla l'installazione del prodotto.
- **Fine** – completa la procedura di installazione del programma.

Osserviamo in dettaglio le fasi della procedura di installazione.

Passaggio 1. Verificare i requisiti di sistema per l'installazione di Kaspersky Anti-Virus

Prima di installare il programma sul computer, l'installer controlla che il sistema operativo e i service pack necessari per l'installazione di Kaspersky Anti-Virus. L'applicazione controlla inoltre che il computer disponga di altri programmi necessari e che l'utente possieda diritti sufficienti per l'installazione di software.

In assenza di uno qualsiasi dei requisiti necessari, il programma visualizza un messaggio informando l'utente dell'impossibilità di completare l'installazione. Prima di installare Kaspersky Anti-Virus si raccomanda di installare i service pack necessari attraverso **Windows Update** ed eventuali altri programmi.

Passaggio 2. Finestra di avvio dell'installazione

Se il sistema soddisfa tutti i requisiti necessari, non appena si esegue il file di installazione si apre una finestra che avvisa dell'inizio dell'installazione di Kaspersky Anti-Virus.

Per continuare l'installazione fare clic su **Avanti**. Per annullare l'installazione fare clic su **Annulla**.

Passaggio 3. Visualizzazione del Contratto di licenza per l'utente finale

La finestra di dialogo successiva contiene un Contratto di licenza tra l'acquirente e Kaspersky Lab. Leggere attentamente il contratto e, se si approvano le condizioni, fare clic su **Accetto i termini dell'accordo di licenza,** quindi premere il pulsante **Avanti**. L'installazione prosegue. Per cancellare l'installazione, cliccare su **Annulla**.

Passaggio 4. Scelta di un tipo di installazione

In questa fase si seleziona il tipo di installazione

Installazione Express. Selezionando questa opzione, si installano tutti i componenti di default consigliati da Kaspersky Lab. Al termine dell'installazione si avvierà una procedura guidata di attivazione (vedere 3.2.2 a pag. 34).

Installazione personalizzata. Questa opzione consente di selezionare i componenti del programma che si desidera installare, la cartella di installazione, quella di attivazione come pure configurare l'installazione usando una speciale procedura guidata (vedere 3.2 a pag. 33).

Nel primo caso l'installazione non richiede l'interazione con l'utente e pertanto i passaggi consecutivi verranno evitati. Al termine vi verrà chiesto di inserire o confermare alcuni dati.

Passaggio 5. Scelta di una cartella di installazione

- La fase successiva dell'installazione di Kaspersky Anti-Virus serve per stabilire la posizione in cui installare il programma sul computer. Il percorso predefinito è:
- Per sistemi a 32 bit: **<Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 7.0**
- Per sistemi a 64 bit: **<Drive>** → **Program Files (x86)** → **Kaspersky Lab** → **Kaspersky Anti-Virus 7.0**.

Per specificare una cartella diversa, fare clic sul pulsante **Sfoglia** e selezionare la nuova cartella nella finestra di selezione che si apre, oppure digitare direttamente il percorso nel campo apposito.

Attenzione!

Ricordare che, se si desidera digitare manualmente il percorso completo della cartella di installazione, esso non deve superare i 200 caratteri né contenere caratteri speciali.

Per continuare l'installazione fare clic su **Avanti**.

Passaggio 6. Scelta dei componenti da installare

Nota

Questa fase si presenta solo se è stata selezionata l'opzione **Installazione personalizzata**.

Se è stata selezionata l'installazione personalizzata, è necessario selezionare i componenti di Kaspersky Internet Security che si desidera installare. Per impostazione tutte le protezioni in tempo reale e le scansioni virus vengono selezionate.

Per selezionare i componenti da installare, fare clic con il tasto sinistro del mouse sull'icona sul nome di un componente e selezionare **Utilizzo disco** dal menu. Per ulteriori informazioni sulle funzioni di protezione di un componente selezionato e sullo spazio su disco fisso necessario per l'installazione, vedere la parte inferiore della finestra di installazione del programma.

Se non si desidera installare un componente, selezionare **Questa funzionalità non sarà più disponibile** dal menu contestuale. Ricordare che, scegliendo di non installare un componente, ci si priva di un elemento di protezione da una vasta gamma di programmi pericolosi.

Dopo aver selezionato i componenti da installare, fare clic su **Avanti**. Per tornare all'elenco dei programmi predefiniti da installare, fare clic su **Reimposta**.

Passaggio 7. Utilizzo di impostazioni di installazione salvate precedentemente

In questo passaggio, l'utente deve specificare se intende utilizzare le impostazioni di sicurezza salvate precedentemente o i database dell'applicazione, qualora questi fossero stati effettivamente salvati nel momento in cui è stata rimossa una versione precedente di Kaspersky Anti-Virus.

Alla suddetta funzionalità si accede nel seguente modo.

Se sul computer era installata una versione precedente di Kaspersky Anti-Virus e i database dell'applicazione sono stati salvati, questi possono essere importati nella versione in fase di installazione. Selezionare l'opzione **Database applicazione**. I database incorporati nell'applicazione non saranno copiati sul computer.

Per utilizzare le impostazioni di protezione configurate per una versione precedente e salvate sul computer, selezionare **Impostazioni runtime applicazione**.

Passaggio 8. Ricerca di altri programmi antivirus

In questa fase, l'installer cerca altri programmi antivirus presenti sul computer, compresi altri prodotti Kaspersky Lab, che potrebbero provocare problemi di compatibilità con Kaspersky Anti-Virus.

Se l'installer individua questo tipo di programmi, ne visualizza un elenco sul video. Il programma chiede se si desidera disinstallarli prima di proseguire l'installazione.

È possibile selezionare la disinstallazione manuale o automatica nell'elenco delle applicazioni antivirus individuate.

Se l'elenco dei programmi antivirus contiene Kaspersky Anti-Virus® 6.0, si raccomanda di salvare le chiavi di licenza utilizzate prima di eliminarle. Esse infatti possono essere utilizzate anche per Kaspersky Anti-Virus 7.0. Si raccomanda inoltre di salvare gli oggetti della Quarantena e del Backup. Essi saranno trasferiti automaticamente nelle aree Quarantena e Backup di Kaspersky Anti-Virus da dove è possibile continuare a usarli.

Qualora Kaspersky Anti-Virus 6.0 sia disinstallato automaticamente, le sue informazioni di attivazione saranno salvate dal software e saranno rimosse durante l'installazione della Versione 7.0.

Attenzione!

Kaspersky Anti-Virus 7.0 supporta i file chiave della Versione 6.0 e della Versione 7.0. Le chiavi utilizzate per le applicazioni in versione 5.0 non sono supportate.

Per continuare l'installazione fare clic su **Avanti**.

Passaggio 9. Completamento dell'installazione

In questa fase, il programma chiede di completare l'installazione del programma sul computer.

Non consigliamo di deselezionare **Abilita Auto-Difesa prima dell'installazione** quando si avvia l'installazione di Kaspersky Internet Security. Abilitando i moduli di protezione, è possibile correttamente retrocedere con l'installazione se si commettono errori durante l'installazione del programma. Se state reinstallando il programma consigliamo di deselezionare questa casella di spunta.

Se l'applicazione viene installata da remoto via **Windows Remote Desktop** consigliamo di deselezionare **Abilita Auto-Difesa prima dell'installazione**. In caso contrario la procedura di installazione potrebbe non completarsi o completarsi in modo errato.

Per continuare l'installazione fare clic su **Avanti**.

Attenzione!

Le correnti connessioni di rete sono cadute durante l'installazione di componenti di Kaspersky Anti-Virus che intercettano il traffico di rete. La maggior parte delle connessioni di rete vengono ristabilite dopo un dato intervallo di tempo.

Passaggio 10. Completamento della procedura di installazione

La finestra **Installazione completa** contiene informazioni su come portare a termine la procedura di installazione di Kaspersky Anti-Virus.

Per completare correttamente l'installazione è necessario riavviare il computer, seguendo il suggerimento del messaggio visualizzato sullo schermo. Dopo il riavvio del sistema, si apre automaticamente la finestra della procedura di ipostazione guidata di Kaspersky Anti-Virus.

Se non è richiesto il riavvio del sistema, fare clic su **Avanti** per passare alla procedura di impostazione guidata.

3.2. Installazione mediante procedura guidata

La procedura di installazione guidata di Kaspersky Anti-Virus 7.0 inizia al termine dell'installazione del programma e serve per agevolare la configurazione delle impostazioni iniziali del programma in base alle caratteristiche e agli usi del computer.

L'interfaccia della procedura guidata è analoga a quelle delle procedure guidate standard di Windows e consiste di una serie di passaggi tra i quali è possibile spostarsi per mezzo dei pulsanti **Indietro** e **Avanti**, o che è possibile portare a termine facendo clic sul pulsante **Fine.** Il pulsante **Annulla** serve per interrompere in qualsiasi momento la procedura.

È possibile omettere questa fase iniziale di impostazione durante l'installazione del programma chiudendo la finestra della procedura guidata. Sarà possibile eseguirla di nuovo in seguito dall'interfaccia del programma se si ripristinano le impostazioni predefinite di Kaspersky Anti-Virus (vedi 15.9.4 a pag. 204).

3.2.1. Uso di oggetti salvati con la versione 5.0

Questa procedura guidata appare quando si installa l'applicazione Kaspersky Anti-Virus 5.0. Vi verrà chiesto di selezionare quali dati usati con la versione 5.0 volete importare nella versione 7.0. Si possono includere i file di quarantena o di backup o le impostazioni di protezione.

Per utilizzare questi oggetti nella versione 7.0, selezionare le caselle appropriate.

3.2.2. Attivazione del programma

Prima di attivare il programma accertarsi che la regolazione della data del sistema corrisponda alla data ed ora attuale.

La procedura di attivazione prevede l'installazione di una chiave che Kaspersky Anti-Virus utilizzerà per verificare la licenza di utilizzo dell'applicazione e determinarne la data di scadenza.

La chiave di licenza contiene informazioni di sistema necessarie per il corretto funzionamento del prodotto, oltre a informazioni relative a:

- Assistenza (chi la fornisce e come ottenerla)
- Nome, numero e data di scadenza della licenza

3.2.2.1. Scelta del metodo di attivazione del programma

A seconda che si disponga di una chiave di licenza per Kaspersky Anti-Virus o sia necessario scaricarne una dal server Kaspersky Lab, è possibile scegliere varie opzioni di attivazione del programma:

- **Attiva mediante codice di attivazione**. Selezionare questa opzione di attivazione se è stata acquistata la versione completa del programma con codice di attivazione in dotazione. Questo codice consente di ottenere una chiave di licenza che garantisce l'accesso completo a tutte le funzionalità del programma fino alla scadenza della licenza.
- **Attiva versione di valutazione (30 giorni)**. Selezionare questa opzione di attivazione se si desidera installare la versione di prova del programma prima di decidere se acquistare la versione commerciale. In questo caso l'utente riceverà una chiave di licenza gratuita per la durata prevista nel relativo accordo di licenza.
- **Applica chiave di licenza**. Attivare l'applicazione usando il file della chiave per Kaspersky Anti-Virus 7.0.
- **Attiva successivamente**. Selezionando questa opzione si omette la fase di attivazione. Kaspersky Anti-Virus 7.0 viene installato sul computer e si potrà accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (è possibile aggiornare l'applicazione una sola volta dopo l'installazione del programma).

Attenzione!

È necessario disporre di una connessione Internet per le prime due opzioni di attivazione. Se al momento dell'installazione non si dispone di una connessione Internet, si può procedere all'attivazione in un secondo momento (vedere Capitolo 14 a pag. 167) utilizzando l'interfaccia dell'applicazione o collegandosi ad Internet da un altro computer, e ottenere una chiave utilizzando un codice di attivazione fornito registrandosi sul sito web del supporto tecnico di Kaspersky Lab.

3.2.2.2. Inserimento del codice di attivazione

Per attivare il programma è necessario inserire il codice di attivazione. Acquistando l'applicazione attraverso Internet il codice di attivazione è inviato via e-mail. Nel caso di acquisto da un rivenditore il codice di attivazione è riportato sul disco di installazione.

Il codice di attivazione è una sequenza di numeri, separati da trattini in quattro gruppi di cinque simboli senza spazi. Ad esempio 11AA1-11AAA-1AA11-1A111. Il codice di attivazione deve essere digitato inserendo caratteri Latini.

In caso l'utente sia già registrato sul sito web del servizio di supporto tecnico e disponga di un numero cliente e di una password, abilitare la casella di selezione **Ho già una ID cliente** e immettere i dati nella parte inferiore della finestra.

Se non ci si è ancora registrati, premere il pulsante **Avanti** lasciando la casella deselezionata. Se è già stata eseguita la procedura di registrazione cliente Kaspersky Lab e si dispone di queste informazioni, immettere il proprio numero cliente e la password nella parte inferiore della finestra. Lasciare tali campi in bianco se la registrazione non è ancora avvenuta. La procedura guidata di registrazione chiederà le informazioni di recapito ed eseguirà la registrazione nel passaggio successivo. Al termine della registrazione, l'utente riceverà un numero cliente e una password, necessari per usufruire del supporto tecnico. Quando ci si registra utilizzando la procedura guidata di attivazione, il numero cliente può essere visualizzato nella Sezione Supporto della finestra principale dell'applicazione (vedi 15.10 a pag. 205).

3.2.2.3. Registrazione dell'utente

Questo passaggio della procedura guidata di attivazione chiede di fornire le vostre coordinate: indirizzo e-mail, Paese e città di residenza. Queste informazioni sono necessarie al Supporto Tecnico di Kaspersky Lab per identificarvi correttamente come utente registrato.

Dopo questo inserimento l'informazione viene inviata dalla procedura guidata di attivazione ad un server e vi verrà assegnato un ID cliente ed una password per

la cabina personale riservata sul sito web del supporto tecnico. L'informazione circa l'ID cliente è disponibile in **Supporto** nella finestra principale dell'applicazione.

3.2.2.4. Ottenimento del file della chiave

La procedura guidata si connette ai server di Kaspersky Lab ed invia loro i vostri datai di registrazione (codice di attivazione e le informazioni personali) per una verifica.

Se il codice di attivazione passa la verifica la procedura guidata conduce a un file con la chiave. Se viene installata la versione demo del programma, si riceverà una chiave di prova sprovvista del codice di attivazione.

Il file così ottenuto viene installato automaticamente nell'applicazione e vi viene presentata la finestra di "attivazione completa" con le informazioni dettagliate della chiave utilizzata.

Nota

Quando viene selezionato questo metodo di attivazione, l'applicazione non scarica un file fisico con estensione *.key da un server, ma ricava determinati dati presenti sul registro del sistema operativo e nel the file system.

La registrazione dell'utente sul sito web di Kaspersky Lab è necessaria per ottenere una chiave di attivazione effettiva.

Se il codice di attivazione non supera l'esame, si apre sullo schermo un messaggio che informa l'utente. In questo caso occorre rivolgersi al rivenditore presso il quale si è acquistato il programma per ulteriori informazioni.

3.2.2.5. Selezione di un file chiave di licenza

Se si dispone di un file chiave di licenza per Kaspersky Anti-Virus 7.0, la procedura guidata chiede se si desidera installarlo. Se sì, servirsi del pulsante **Sfoglia** per selezionare il percorso del file della chiave di licenza, riconoscibile dall'estensione *.key,* nella finestra di selezione.

Al termine della procedura di installazione della chiave, nella parte inferiore della finestra vengono visualizzate tutte le informazioni relative alla licenza. il nome dell'utente, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della chiave.

3.2.2.6. Completamento dell'attivazione del programma

La procedura di impostazione guidata informa l'utente che il programma è stato attivato correttamente. Vengono visualizzate inoltre informazioni relative alla chiave di licenza installata il nome dell'utente, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della chiave.

3.2.3. Selezione della modalità di sicurezza

In questa finestra, la procedura guidata chiede di selezionare la modalità di sicurezza con la quale funzionerà il programma:

Base: Sono le impostazioni di default utili per gli utenti che non hanno dimestichezza con i computer o i software anti-virus. Indica che i componenti dell'applicazione sono impostati al livello di protezione consigliato e che l'utente viene informato solo a proposito di eventi pericolosi (come il riconoscimento di oggetti ed attività pericolose).

Interattivo: Questa modalità offre una protezione dei dati del computer più personalizzata rispetto alla modalità Base. Essa è in grado di intercettare tentativi di modifica delle impostazioni di sistema, attività sospette a livello di sistema e attività non autorizzate a livello di rete. Tutte le attività sopra elencate possono indicare la presenza di programmi nocivi o semplicemente dipendere da attività standard di programmi in uso sul computer. Spetta all'utente stabilire per ogni singolo caso se consentire o bloccare tali attività. Se si sceglie questa modalità, occorre specificare quando applicarla:

- **Abilita monitoraggio del registro di sistema** – chiede l'intervento dell'utente se riscontra un tentativo di alterare il registro di sistema.

> Se l'applicazione è installata su un computer dotato di Microsoft Windows XP Professional Edition x64. Microsoft Windows Vista o Microsoft Windows Vista x64 le impostazioni sotto elencate per la modalità interattiva non saranno disponibili.

- **Abilita Controllo Integrità dell'Applicazione** – chiede che l'utente confermi le azioni intraprese quando i moduli vengono caricati sulle applicazioni da monitorare.
- **Abilita difesa proattiva estesa** – questa modalità analizza tutte le attività sospette delle applicazioni del sistema, compresi l'apertura di un browser con impostazioni di riga di comando, inserimenti in processi di applicazioni e intercettori di hook di finestre (disabilitati per impostazione predefinita).

3.2.4. Configurazione delle impostazioni di aggiornamento

La sicurezza del computer dipende direttamente dall'aggiornamento regolare dei database e dei moduli del programma. In questa finestra, la procedura guidata chiede di selezionare una modalità di aggiornamento del programma e di configurare un piano di aggiornamento.

- **Automatica**. Kaspersky Anti-Virus controlla ad intervalli regolari la disponibilità degli aggiornamenti. Le scansioni possono essere impostate per essere più frequenti durante una infezione e meno frequenti quando il pericolo è passato. Quando il programma incontra nuovi aggiornamenti provvede a scaricarli ed installarli nel computer. È la modalità predefinita.
- **Ogni 1 giorno(i)**. Gli aggiornamenti vengono eseguiti automaticamente in base alla programmazione impostata. Per configurare la programmazione fare clic su **Cambia**.
- **Manuale**. Questa opzione consente di eseguire manualmente gli aggiornamenti.

Osservare che, al momento dell'installazione del programma, i database e i moduli del programma in dotazione con il software possono essere ormai obsoleti. Per questo motivo si raccomanda di scaricare gli ultimi aggiornamenti del programma. A tal fine, fare clic su **Aggiorna ora**. Kaspersky Anti-Virus scarica quindi gli aggiornamenti necessari dai server remoti dedicati e li installa sul computer.

Per configurare gli aggiornamenti (selezionare la fonte di aggiornamento, avviare l'aggiornamento da uno specifico login od attivare lo scarico degli aggiornamenti da un fonte locale) fare clic su **Impostazioni**.

3.2.5. Programmazione delle scansioni antivirus

La scansione di aree selezionate del computer in cerca di oggetti nocivi è una delle fasi più importanti della protezione del computer.

Al momento dell'installazione di Kaspersky Anti-Virus, vengono create tre attività di scansione antivirus predefinite. La procedura guidata di installazione ti chiederà di scegliere un'impostazione per l'attività di scansione:

Esamina oggetti di avvio

Kaspersky Anti-Virus esamina automaticamente gli oggetti di avvio ogni volta che si accende il computer. Questo è il valore predefinito. È possibile

modificare le impostazioni di scansione programmata in un'altra finestra facendo clic su **Cambia**.

Esamina aree critiche

Per eseguire automaticamente la scansione antivirus delle aree critiche del sistema (memoria di sistema, oggetti all'avvio, settori di boot, cartelle di sistema di Windows) selezionare la casella corrispondente. Per configurare la programmazione fare clic su **Cambia.**

Per impostazione predefinita, questa scansione automatica è disabilitata.

Analizza risorse del computer

Per eseguire automaticamente una scansione completa del computer, selezionare la casella appropriata. Per configurare la programmazione fare clic su **Cambia.**

Per impostazione predefinita, l'esecuzione di questa attività in base alla programmazione è disabilitata. Tuttavia, si raccomanda di eseguire una scansione completa del computer subito dopo l'installazione del programma.

3.2.6. Restrizioni di accesso al programma

Poiché è possibile che più persone facciano uso di uno stesso computer (famigliari, per esempio) senza essere necessariamente utenti avanzati, e poiché programmi nocivi possono disabilitare la protezione, esiste un'opzione di protezione dell'accesso a Kaspersky Anti-Virus mediante password. L'uso di una password è utile per proteggere il programma da tentativi non autorizzati di disabilitare la protezione o modificare le impostazioni.

Per abilitare la protezione con password, selezionare ☑ **Abilita protezione tramite password** e completa i campi **Nuova password** e **Conferma password**.

Selezionare sotto l'area alla quale si desidera applicare la protezione con password:

◉ **Tutte le operazioni (ad eccezione delle notifiche di eventi pericolosi).** Richiede la password se l'utente cerca di eseguire qualsiasi azione con il programma, ad eccezione delle risposte alle notifiche in caso di rilevamento di oggetti pericolosi.

◉ **Operazioni selezionate:**

☑ **Modifica delle impostazioni dell'applicazione** – richiede la password quando un utente cerca di salvare delle modifiche alle impostazioni del programma.

- **Uscita dal programma in esecuzione** – richiede la password se un utente cerca di chiudere il programma.
- **Arresto/sospensione dei componenti di protezione o delle operazioni di scansione** – richiede la password se l'utente cerca di sospendere o disabilitare completamente un componente di protezione in tempo reale o attività di scansione antivirus.

3.2.7. Controllo Integrità dell'Applicazione

In questa fase la procedura guidata analizzerà le applicazioni installate sul computer (librerie file dinamici, firme digitali di produzione), conterà la somma dei file dell'applicazione e creerà un elenco di programmi che possono essere sicuri dal punto di vista della sicurezza. Ad esempio questo elenco includerà automaticamente tutte le applicazioni firmate digitalmente da Microsoft.

Nel futuro Kaspersky Anti-Virus utilizzerà le informazioni ottenute mentre analizza la struttura dell'applicazione per prevenire che codici maligni possano essere inseriti nei moduli dell'applicazione.

L'analisi delle applicazioni installate sul computer può richiedere un certo tempo.

3.2.8. Completamento della procedura di installazione guidata

L'ultima finestra della procedura guidata chiede se si desidera riavviare il computer per completare l'installazione del programma. Il riavvio è necessario affinché i driver di alcuni componenti di Kaspersky Anti-Virus vengano registrati correttamente.

È possibile posticipare il riavvio, ma in tal caso alcuni componenti del programma non funzioneranno.

3.3. Installazione del programma dal prompt di comando

Per installare Kaspersky Anti-Virus digita il seguente comando:

```
msiexec /i <package_name>
```

La procedura guidata di installazione si avvierà (vedere 3.1 a pag. 28). Installato il programma è necessario riavviare il computer.

Per installare l'applicazione in modo non interattivo (senza lanciare la procedura guidata di installazione), immettere:

```
msiexec /i <package_name> /qn
```

CAPITOLO 4. INTERFACCIA DEL PROGRAMMA

Kaspersky Anti-Virus è dotato di un'interfaccia semplice e intuitiva. Questo capitolo ne descrive le caratteristiche principali:

- Icona nell'area di notifica della barra delle applicazioni (vedi 4.1 a pag. 42)
- Menu contestuale (vedi 4.2 a pag. 43)
- Finestra principale (vedi 4.3 a pag. 45)
- Finestra delle impostazioni del programma (vedi 4.4 a pag 49)

Oltre all'interfaccia principale del programma, vi sono plugin per le seguenti applicazioni:

- Microsoft Office Outlook – (vedi 8.2.2 a pag. 99)
- The Bat! – (vedi 8.2.3 a pag. 101)
- Microsoft Internet Explorer (vedi Capitolo 9 a pag. 107)
- Microsoft Windows Explorer (vedi 11.2 a pag. 137)

I plug-in estendono le funzionalità di questi programmi consentendo la gestione e l'impostazione di Kaspersky Anti-Virus dalle loro interfacce.

4.1. L'icona nell'area di notifica della barra delle applicazioni

Subito dopo l'installazione di Kaspersky Anti-Virus, nell'area di notifica della barra delle applicazioni viene visualizzata un'icona che funge da indicatore delle funzioni di Kaspersky Anti-Virus e che riflette lo stato della protezione e mostra una serie di funzioni di base eseguite dal programma.

Se l'icona è attiva  (colorata) ciò significa che sul computer sono abilitati tutti o parte dei componenti di protezione. Se l'icona è inattiva  (grigia), la protezione è stata disabilitata oppure alcuni dei componenti di protezione (vedi 2.2.1 a pag. 22) sono stati messi in pausa.

L'icona di Kaspersky Anti-Virus cambia in relazione all'operazione eseguita:

 Scansione posta elettronica.

 Scansione degli script.

 Scansione in corso di un file in fase di apertura, salvataggio o esecuzione da parte dell'utente o di un programma.

 I database di Kaspersky Anti-Virus e i moduli del programma sono in fase di aggiornamento.

 Errore in un componente di Kaspersky Anti-Virus.

 Errore in un componente di Kaspersky Anti-Virus.

L'icona consente inoltre di accedere alle funzioni di base dell'interfaccia del programma: il menu contestuale (vedi 4.2 a pag. 43) e la finestra principale (vedi 4.3 pag 45).

Per aprire il menu contestuale, fare clic con il pulsante destro del mouse sull'icona del programma.

Per aprire la finestra principale di Kaspersky Anti-Virus nella sezione **Protezione** (la prima schermata predefinita del programma), fare doppio clic sull'icona del programma. Se si fa clic una volta sola, la finestra principale si apre sulla sezione che era attiva l'ultima volta che il programma è stato chiuso.

Se sono disponibili nuove informazioni da parte di Kaspersky Lab la icona seguente apparirà nella barra di notifica della barra delle applicazioni  . Fare doppio click sull'icona per vedere le novità nella corrispondente finestra.

4.2. Il menu contestuale

È possibile eseguire semplici attività di protezione dal menu contestuale (vedi Figura 1).

Il menu di Kaspersky Anti-Virus contiene i seguenti elementi:

Analizza risorse del computer – avvia una scansione completa del computer in cerca di oggetti pericolosi. Durante l'operazione vengono esaminati i file di tutte le unità, inclusi i supporti di archiviazione esterni.

Ricerca virus – seleziona gli oggetti e ne esegue la scansione antivirus. L'elenco predefinito contiene una serie di file come quelli della cartella **Documenti**, la cartella Avvio, le caselle di posta, tutte le unità del

computer, ecc. È possibile aggiungere elementi all'elenco, selezionare file da esaminare e avviare scansioni antivirus.

Aggiornamento – avvia gli aggiornamenti di Kaspersky Anti-Virus, dei moduli e dei database e li installarli sul computer.

Attiva – serve per attivare il programma. E' necessario attivare la vostra versione di Kaspersky Anti-Virus per ottenere lo stato di utente registrato che consente l'accesso ad una completa funzionalità dell'applicazione ed al Supporto Tecnico. Questo elemento di menu è disponibile solo se il programma non è attivato.

Impostazioni – consente di visualizzare e configurare le impostazioni di Kaspersky Anti-Virus.

Apri Kaspersky Anti-Virus – apre la finestra principale del programma (vedi 4.3 a pag. 45).

Abilita protezione / Sospendi protezione – disabilita temporaneamente o abilita i componenti della protezione in tempo reale (vedi 2.2.1 a pag. 22). Questo elemento di menu non influisce sugli aggiornamenti del programma o sulle attività di scansione antivirus.

Informazioni sul programma – richiama la finestra con le informazione di Kaspersky Anti-Virus

Esci – chiude Kaspersky Anti-Virus (quando questa opzione è selezionata l'applicazione sarà scaricata dalla RAM del computer).

Figura 1. Il menu contestuale

Durante un'attività di scansione antivirus, il menu contestuale visualizza il nome dell'attività accompagnato da un indicatore della percentuale di avanzamento. Selezionando l'attività, è possibile portarsi sulla finestra dei report per visualizzare i risultati correnti.

4.3. La finestra principale del programma

La finestra principale di Kaspersky Anti-Virus (vedere Figure 2) può essere logicamente suddivisa i tre parti:

- la parte superiore della finestra mostra lo stato corrente della protezione del computer.

  Ci sono tre possibili stati di protezione (vedere 5.1 a pag. 51) ciascuno con il proprio codice colore simile ad un semaforo. Verde indica che il vostro computer è propriamente protetto mentre giallo e rosso sono indicatori dei diversi problemi nella configurazione o nella operatività di Kaspersky Anti-Virus.

  Per ottenere informazioni dettagliate circa la soluzione di errori e problemi di velocità utilizza la procedura guidata di sicurezza che si apre quando il collegamento alla notifica della minaccia viene cliccato.

Figure 2. La finestra principale di Kaspersky Anti-Virus

- *Pannello di Navigazione (parte sinistra della finestra):* assicura un accesso veloce e facile a ciascun componente, esecuzione delle attività di scansione, supporto funzionale all'applicazione.
- Pannello delle *Informazioni* (parte destra della finestra). contiene le informazioni circa la protezione del componente selezionato nella parte sinistra della finestra e presenta le impostazioni per ciascuno di loro, fornendoti gli strumenti per la ricerca dei virus, lavorare con i file in quarantena e le copie di backup, gestire le chiavi di licenza e così via.

Dopo aver selezionato una sezione o un componente nella parte sinistra della finestra, nella parte destra vengono visualizzate le informazioni relative alla selezione.

Esaminiamo adesso gli elementi del pannello di navigazione della finestra principale.

Sezione della finestra principale	Scopo
	Scopo principale della sezione **Protezione** è fornire l'accesso ai componenti base di protezione in tempo reale del computer. Per vedere lo stato di un componente di protezione o dei sui moduli, per configurare le sue impostazioni od aprire un report significativo selezione questo componente dall'elenco sotto **Protezione**. La sezione contiene anche i link alle più comuni attività: ricerca virus ed aggiornamenti del database dell'applicazione. Puoi vedere le informazioni sullo stato di queste azioni, configurarle o avviarle.

	La sezione **Scansione** fornisce acceso alle azioni di scansione degli oggetti. Mostra le azioni create dagli esperti di Kaspersky Lab (scansione delle aree critiche, avvio degli oggetti, scansione completa del computer, scansione rootkit) come pure quelle create dall'utente. Quando una azione è selezionata dalla parte destra, vengono fornite le informazioni rilevanti dell'azione, possono essere configurate le impostazioni dell'azione, viene generato un elenco degli oggetti da scansionare o l'azione viene avviata. Per scansionare un singolo oggetto (file, cartella o drive) seleziona **Scansione**, usa lo spazio di destra per aggiungere oggetti alla lista da scansionare ed avvia l'azione. Inoltre questa sezione può essere utilizzata per creare un disco di emergenza (vedi Sezione 15.4 pag 184).
	La sezione **Aggiornamento** contiene informazioni circa gli aggiornamenti dell'applicazione: data di pubblicazione degli aggiornamenti e record di conteggio dei virus. Appropriati link possono essere utilizzati per avviare un aggiornamento, vedere un dettagliato report, configurare gli aggiornamenti, ritornare ed aggiornare ad una precedente versione.

	**Report e file dati** può essere usata per vedere dettagliati report per ogni componente dell'applicazione, una scansione virus o aggiornare una azione (vedi Sezione 15.3 pag 176) e lavorare con oggetti posti in quarantena (vedi Sezione 15.1 pag 170) o con l'archivio di backup (vedi Sezione 15.2 pag 174).
	La sezione **Attivazione** è utilizzata per maneggiare le chiavi richieste dall'applicazione per essere completamente funzionale (vedi Sezione 15.5 pag 188) Se una chiave non è installata è consigliabile il suo acquisto e che l'applicazione venga attivata (vedi 3.2.2 a pag. 34). Se una chiave è installata la sezione mostra l'informazione circa il tipo di chiave usata e la data di termine. Appena una chiave si arresta può essere rinnovata sul sito di Kaspersky Lab.
	La sezione **Supporto** fornisce informazione circa il supporto disponibile per gli utenti Kaspersky Anti-Virus registrati.

Ogni elemento del pannello di navigazione è accompagnato da uno speciale menu contestuale. Esso contiene punti per i componenti di protezione e strumenti che agevolano l'utente nella configurazione e gestione dei componenti e nella visualizzazione dei report. Esiste un ulteriore elemento di menu per le attività di scansione antivirus, utilizzabile per creare la propria attività sulla base di una selezionata.

È possibile anche modificare l'aspetto del programma creando e utilizzando una grafica e uno schema cromatico personalizzati.

La parte bassa a sinistra della finestra contiene due pulsanti: **Guida** che fornisce l'accesso alla guida di Kaspersky Anti-Virus e **Impostazioni** che apre la finestra per le impostazioni dell'applicazione.

4.4. Finestra delle impostazioni del programma

La finestra delle impostazioni di Kaspersky Anti-Virus (vedi 4.3 a pg. 45) può essere aperta dalla finestra principale o dal menu contestuale dell'applicazione (vedi 4.2 a pag. 43). Cliccare su **Impostazioni** nella parte inferiore della finestra principale o selezionare l'opzione appropriata del menu contestuale.

La finestra delle impostazioni (vedi Figure 3) ha la stessa struttura della finestra principale:

- La parte sinistra della finestra consente di accedere in maniera facile e veloce alle impostazioni di ciascun componente del programma, aggiornamento, alle attività di scansione antivirus e impostazioni del programma;
- La parte destra della finestra contiene un elenco di impostazioni del componente, attività, ecc., selezionato nella parte sinistra della finestra.

Quando si seleziona qualsiasi sezione, componente o attività nella parte sinistra della finestra delle impostazioni, la parte destra ne visualizza le impostazioni di base. Per configurare le impostazioni avanzate, è possibile aprire le finestre delle impostazioni di secondo e terzo livello. Per una descrizione dettagliata delle impostazioni del programma, consultare le sezioni corrispondenti del manuale dell'utente.

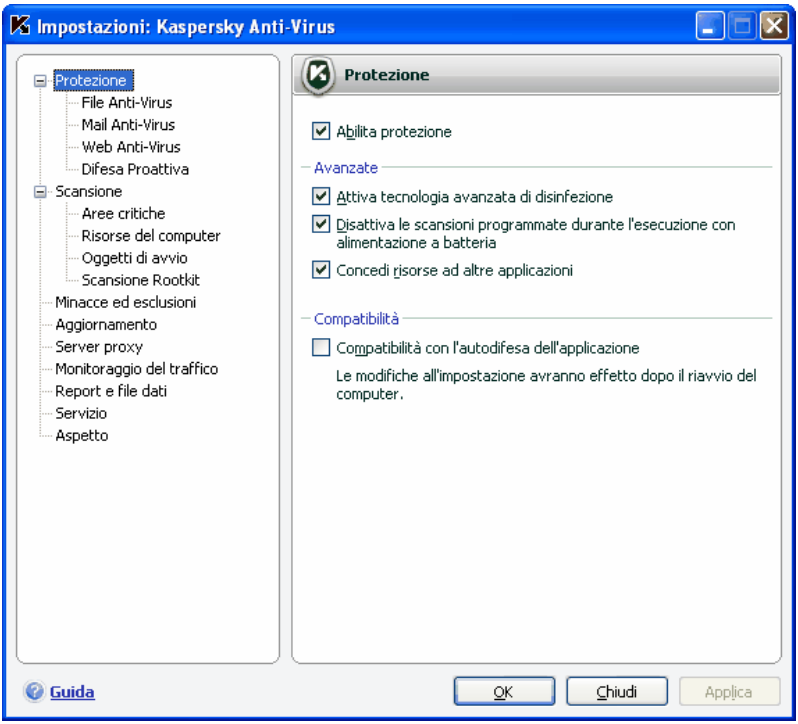


Figure 3. La finestra delle impostazioni di Kaspersky Anti-Virus

CAPITOLO 5. GUIDA INTRODUTTIVA

Uno dei principali obiettivi di Kaspersky Lab con Kaspersky Anti-Virus era fornire una configurazione ottimale per tutte le opzioni del programma. Ciò consente agli utenti a qualsiasi livello di conoscenza del computer di proteggere il PC subito dopo l'installazione, senza sprecare tempo con la configurazione.

È possibile tuttavia che il computer o il tipo di lavoro per il quale lo si utilizza richiedano delle configurazioni specifiche. Ecco perché si raccomanda di eseguire una configurazione preliminare in modo da ottenere l'approccio più flessibile e personalizzato possibile alla protezione del computer.

Per facilitare al massimo la messa in funzione del programma, abbiamo combinato tutte le fasi di configurazione preliminare in una procedura di installazione guidata (vedi 3.2 a pag. 33) che si avvia non appena inizia l'installazione del programma. Seguendo le istruzioni della procedura guidata è possibile attivare il programma, configurare le impostazioni degli aggiornamenti e delle scansioni antivirus, proteggere l'accesso al programma mediante password.

Dopo aver installato e avviato il programma, si raccomanda di eseguire i seguenti passaggi:

- Controllare lo stato corrente della protezione (vedi 5.1 a pag. 51) per garantire che Kaspersky Anti-Virus funzioni al livello appropriato.
- Aggiornare il programma (se la procedura guidata non ha provveduto automaticamente dopo l'installazione del programma) (vedi 5.6 a pag. 56).
- Eseguire la scansione antivirus del computer (vedi 5.3 a pag. 54).

5.1. Come determinare lo stato della protezione del computer

Lo stato di protezione del computer è una rappresentazione grafica delle minacce alla sicurezza complessiva del sistema in un dato momento. Ai fini del presente documento, per minacce si intendono sia malware che database dell'applicazione non aggiornati, disattivazione di alcuni componenti di protezione, uso di impostazioni minime dell'applicazione, ecc.

Lo stato della protezione è illustrato in alto nella finestra principale dell'applicazione con colori simili a quelli di un semaforo. In funzione della situazione il colore della parte superiore varia e nel caso di riscontro di minacce oltre al colore verranno aggiunti messaggi informativi, come i link alla procedura guidata di sicurezza.

I seguenti colori vengono utilizzati per mostrare lo stato della protezione:

- *Verde*. Indica che il computer è correttamente protetto.

  Ciò significa che i database sono regolarmente aggiornati, tutti componenti della protezione sono attivati, l'applicazione è avviata con le impostazioni consigliate degli specialisti di Kaspersky Lab, nessun oggetto critico è stato individuato dalla scansione completa del computer o è stato bloccato.

- *Giallo*. La vostra protezione del computer si è abbassata. Questo stato informa circa alcuni problemi per l'applicazione o le sue impostazioni.

  Per esempio, sono presenti alcune piccole discrepanze rispetto alla modalità di funzionamento, e i database dell'applicazione non sono stati aggiornati da parecchi giorni.

- *Rosso*. Avverte a proposito di problemi che potrebbero causare infezioni e perdite di dati. Ad esempio uno o più componenti hanno fallito, il prodotto non è stato aggiornato da molto tempo oppure oggetti pericolosi sono stati individuati ed è necessario rimuoverli urgentemente, il prodotto non è stato abilitato.

Se si riscontrano problemi nel sistema protettivo raccomandiamo di intervenire immediatamente. Utilizza la procedura guidata di sicurezza accessibile ciccando sulla notifica delle minacce. Questa procedura ti aiuterà a muoverti attraverso tutti le minacce e ti fornirà le indicazioni per rimuoverle. La criticità della minaccia è indicata dal colore dell'indicatore:

 - *l'indicatore attira la tua attenzione su minacce non critiche* che comunque potrebbero abbassare il livello di protezione del computer. Tieni in considerazioni i consigli degli specialisti di Kaspersky Lab.

 - *l'indicatore avverte della presenza di serie minacce* per la sicurezza del computer. Segui attentamente i consigli seguenti. Sono tutti utili per la migliore protezione del tuo computer. Le azioni consigliate sono fornite come link.

Per muoversi nell'elenco delle minacce clicca sul pulsante Avanti. Viene fornita una dettagliata descrizione di ciascuna minaccia e sono disponibili le seguenti azioni:

- *Elimina immediatamente*. Utilizzando il corrispondente link puoi eliminare direttamente la minaccia. Per informazioni più approfondite dell'evento puoi guardare il file del report. L'azione consigliata è quella di eliminare subito la minaccia.
- *Rimanda*. Se per qualsiasi ragione non puoi eliminare subito la minaccia è possibile rimandare questa azione. Usa il collegamento Rimanda.

  Nota che questa opzione non è disponibile per minacce serie, come ad esempio oggetti che non possono venir disinfettati, crasse nei componenti o database i cui file sono danneggiati.

Se rimangono presenti delle minacce dopo aver eseguito la procedura guidata di sicurezza una nota apparirà nella parte alta della finestra principale avvertendoti che devi ancora eliminarle. Se apri ancora la procedura guidata di sicurezza le minacce posposte non saranno presenti nell'elenco dei virus attivi. In ogni caso puoi ancora eliminare queste minacce ciccando sul link Visualizza le minacce il cui trattamento è stato rimandato nella finestra finale del wizard.

5.2. Verifica dello stato di ciascun componente di protezione

Per conoscere lo stato corrente di ciascun componente di protezione in tempo reale apri la finestra principale dell'applicazione e selezione il componente desiderato sotto **Protezione**. Sulla destra verrà presentato un sommario delle informazioni relative al componente selezionato.

Lo stato del componente è l'indicatore più importante:

- <*nome componente*> *in esecuzione* – la protezione fornita dal componente è al livello desiderato.
- <*nome componente*> *in sospeso* – il componente è disabilitato per un certo periodo di tempo. Verrà riavviato dopo il tempo specificato o dopo che l'applicazione viene riavviata. Il componente può essere riavviato manualmente. Clicca Ripristina funzionamento.
- <*nome componente*> – *Disattivato*. l'utente ha arrestato il componente. La protezione può essere riavviata ciccando su Abilita.
- <*nome componente*> *disabilitato (errore)* – disabilitato in seguito ad un errore.

  Se in un componente si verifica un errore prova a riavviarlo. Se il riavvio determina ancora un errore guarda il report relativo al componente che potrebbe contenere le ragioni dell'errore. Se non riesci a risolvere il

problema salva il report del componente in un file usando **Azioni** → **Salva con nome** e contatta il supporto tecnico di Kaspersky Lab.

Lo stato del componente dovrebbe seguito dalle informazioni circa le sue impostazioni (ad esempio livello di protezione, azioni da intraprendere per gli oggetti pericolosi). Se il componente è composto da più moduli, sono presentati gli stati dei moduli: abilitato o disabilitato. Per modificare le impostazioni correnti ciccare su Configura.

In aggiunta vengono fornite alcune statistiche circa l'attività. Clicca su Apri report per vedere un report dettagliato.

Se per una qualsiasi ragione un componente è in un certo momento messo in pausa o arrestato i risultati al momento di questa azione possono essere visti ciccando su Apri ultimo report di avvio.

5.3. Come eseguire la scansione antivirus del computer

Dopo l'installazione, il programma comunica all'utente con un messaggio nella parte bassa a sinistra della finestra dell'applicazione che il computer non è ancora stato esaminato e raccomanda di eseguire immediatamente una scansione antivirus.

Kaspersky Anti-Virus include un'attività di scansione antivirus predefinita. Essa si trova nella finestra principale del programma nella sezione **Scansione**.

Ciccando su **Risorse del computer** vengono presentate le impostazioni delle azioni; livello di protezione corrente, azioni da intraprendere per oggetti pericolosi. E' anche disponibile un report dell'ultima scansione.

Per eseguire la scansione del computer in cerca di programmi nocivi,

1. Seleziona **Risorse del computer** sotto **Scansione** nella finestra principale dell'applicazione.
2. Clicca il link **Avvia scansione**.

Il programma avvia la scansione del computer visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.4. Come eseguire la scansione di aree critiche del computer

Vi sono aree del computer particolarmente critiche dal punto di vista della sicurezza. Esse sono prese di mira dai programmi nocivi volti a danneggiare il sistema operativo, il processore, la memoria, ecc.

È estremamente importante garantire la sicurezza di queste aree per il corretto funzionamento del computer. Abbiamo quindi programmato un'attività di scansione antivirus specifica per queste aree. Essa si trova nella finestra principale del programma nella sezione **Scansione**.

Selezionando Aree Critiche verranno presentate le ipostazioni: livello di protezione corrente, azioni da intraprendere. è anche possibile selezionare quale area critica controllare e scansionare subito queste aree.

Per eseguire la scansione delle aree critiche del computer in cerca di programmi nocivi,

1. Seleziona **Aree Critiche** sotto **Scansione** nella finestra principale dell'applicazione.
2. Clicca il link Avvia scansione.

Il programma avvia la scansione delle aree selezionate visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.5. Come eseguire la scansione antivirus di un file, una cartella o un disco

Vi sono situazioni in è necessario eseguire la scansione antivirus di singoli oggetti anziché dell'intero computer, per esempio dell'hard drive in cui si trovano programmi, giochi, database di posta portati a casa dall'ufficio, file archiviati ricevuti come allegati, ecc. È possibile selezionare l'oggetto da esaminare per mezzo degli strumenti standard del sistema operativo Windows (per esempio dalla finestra di **Explorer** o dal **Desktop**, ecc.).

Per eseguire la scansione di un oggetto,

posizionare il cursore sopra al nome dell'oggetto selezionato, aprire il menu contestuale di Windows facendo clic con il pulsante destro del mouse e selezionare **Avvia** (vedi Figura 4).

Figura 4. Scansione antivirus di un oggetto selezionato per mezzo degli strumenti di Windows

Il programma avvia quindi la scansione dell'oggetto selezionato visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.6. Come aggiornare il programma

Kaspersky Lab aggiorna i database di Kaspersky Anti-Virus e i moduli del programma per mezzo di appositi server di aggiornamento.

I server di aggiornamento di Kaspersky Lab sono siti Internet di Kaspersky Lab Internet in cui vengono archiviati gli aggiornamenti dei programmi.

Attenzione!

E' necessario disporre di un collegamento Internet. a Kaspersky Anti-Virus

Kaspersky Anti-Virus verifica automaticamente la presenza di aggiornamenti sui server di Kaspersky Lab. Se il server dispone degli ultimi aggiornamenti Kaspersky Anti-Virus li scarica e li installa autonomamente.

Per aggiornare Kaspersky Anti-Virus manualmente,

1. Seleziona la sezione **Aggiornamento** dalla finestra principale dell'applicazione.
2. Clicca su Aggiorna database.

Kaspersky Anti-Virus avvia così il processo di aggiornamento. Tutti i dettagli del processo vengono visualizzati in un'apposita finestra.

5.7. Come comportarsi in caso di protezione non funzionante

Se si verificano problemi o errori di funzionamento di qualsiasi componente di protezione, è bene verificarne lo stato. Se lo stato del componente è *disabilitato o in esecuzione (errore di sottosistema)* cercare di riavviare il programma.

Se il problema non si risolve riavviando il programma, si raccomanda di correggere errori potenziali usando le funzioni di ripristino dell'applicazione (vedi Capitolo 17 a pag. 224).

Se il ripristino non produce risultati contatta il Supporto Tecnico di Kaspersky Lab. Potrebbe essere necessario salvare in un file il report sul funzionamento del componente e inviarlo al Supporto Tecnico per successive analisi.

Per salvare il report su un file:

1. Selezionare il componente nella sezione **Protezione** della finestra principale del programma e fare clic su Apri Report (componente corrente) oppure Apri ultimo Report (per un componente disabilitato).
2. Nella finestra del report ciccare su **Azioni** → **Salva con nome** e nella finestra che si apre, specificare il nome del file in cui il report sarà salvato. Questa sezione fornisce informazioni.

CAPITOLO 6. SISTEMA DI GESTIONE DELLA PROTEZIONE

Questa sezione fornisce informazioni sulle impostazioni comuni usate dai componenti di protezione in tempo reale dell'applicazione e dalle azioni come pure informazioni circa la creazione di protezioni specifiche ed elenchi di minacce gestite dall'applicazione ed una lista di oggetti sicuri che possono essere ignorati dalla protezione:

- gestione in tempo reale della protezione (vedi 6.1 a pag. 58);
- utilizzo della Tecnologia avanzata di disinfezione (vedi 6.2 a pag. 62);
- eseguire attività su un portatile (vedi 6.3 a pag. 63);
- cooperazione di Kaspersky Anti-Virus con altre applicazioni (vedi 6.4 a pag. 63);
- compatibilità di Kaspersky Anti-Virus con caratteristiche di auto-difesa di altre applicazioni (vedi 6.5 a pag. 63);
- elenco delle protezioni dalle minacce (vedi 6.2 a pag. 62) di cui è fornita l'applicazione;
- elenco degli oggetti attendibili (vedi 6.9 a pag. 68) che verranno ignorati dalla protezione.

6.1. Interruzione e ripristino della protezione in tempo reale del computer

Per impostazione predefinita, Kaspersky Anti-Virus viene caricato all'avvio del sistema e protegge il computer per tutto il tempo che resta in uso. Il messaggio *Kaspersky Anti-Virus 7.0* nell'angolo superiore destro dello schermo informa l'utente che tutti i componenti di protezione in tempo reale (vedi 2.2.1 a pag. 22) sono attivati.

È possibile disabilitare completamente o parzialmente la protezione offerta da Kaspersky Anti-Virus.

Attenzione!

Kaspersky Lab raccomanda caldamente di **non disabilitare la protezione in tempo reale**, poiché ciò potrebbe provocare l'infezione del computer e la perdita dei dati.

Osservare che in questo caso la protezione è descritta nel contesto dei componenti di protezione. Disabilitare o sospendere i componenti di protezione non pregiudica le prestazioni delle attività di scansione antivirus o aggiornamento del programma.

6.1.1. Sospensione della protezione

Sospendere la protezione in tempo reale significa disabilitare temporaneamente tutti i componenti di protezione che monitorano i file del computer, la posta in arrivo e in uscita, gli script eseguibili, il comportamento delle applicazioni.

Per sospendere la protezione in tempo reale del computer:

1. Selezionare **Sospendi** nel menu contestuale del programma (vedi 4.2 a pag. 43).
2. Nella finestra che si apre (vedi Figura 5), specificare quando si desidera ripristinare la protezione:
   - Tra <intervallo di tempo> – la protezione sarà ripristinata dopo questo intervallo. Per selezionare un valore usa il menu a discesa.
   - Al prossimo riavvio del programma – la protezione sarà ripristinata aprendo il programma dal menu Start o dopo aver riavviato il computer (a condizione che il programma sia impostato in modo da aprirsi automaticamente all'avvio (vedi 15.11 a pag. 206).
   - Solo su richiesta dell'utente – la protezione si arresterà fino ad un nuovo comando di avvio. Per abilitare la protezione selezione **Riprendi protezione** dal menu contestuale del programma.

Se metti in pausa la protezione lo saranno anche tutti i suoi componenti in tempo reale. Questo è indicato da:

- Nomi dei componenti inattivi (in grigio) nella sezione **Protezione** della finestra principale.
- Icona inattiva (in grigio) nella barra di notifica della barra delle applicazioni.

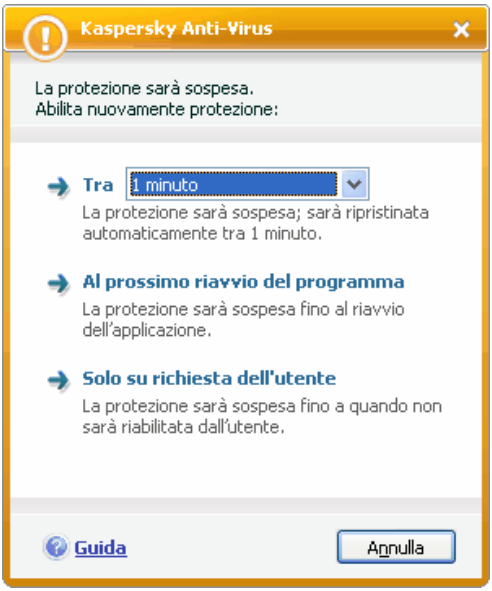


Figura 5. Finestra di sospensione della protezione

6.1.2. Interruzione della protezione

Interrompere la protezione significa disabilitare completamente i componenti in tempo reale della protezione. Le attività di scansione antivirus e di aggiornamento continuano a funzionare in questa modalità.

Se la protezione è interrotta, essa può essere ripristinata esclusivamente dall'utente. Se la protezione è stata interrotta, i suoi componenti non si ripristinano automaticamente al riavvio del sistema o del programma. Ricordare che se Kaspersky Anti-Virus è in conflitto con altri programmi installati sul computer, è possibile sospendere i singoli componenti o creare un elenco di esclusioni (vedi 6.9 a pag. 68).

Per interrompere la protezione in tempo reale:

1. Aprire la finestra delle impostazioni e seleziona **Protezione**.
2. Deselezionare ☑ **Abilita Protezione**.

Disabilitando la protezione, tutti i suoi componenti si interrompono. Questo stato è indicato da:

- Nomi inattivi (grigio) dei componenti disabilitati nella sezione **Protezione** della finestra principale.

- Icona grigia nella barra dell'area di notifica delle attività.

6.1.3. Sospensione/interruzione dei componenti della protezione

Esistono molti modi per interrompere un componente di protezione, una scansione antivirus o un aggiornamento. Tuttavia, prima di farlo, si raccomanda di decidere per quale ragione si desidera interromperli. È probabile infatti che esista una soluzione diversa al problema, per esempio modificare il livello di protezione. Se, per esempio, si lavora con un database che sicuramente non contiene virus, è sufficiente aggiungerne i file tra le esclusioni (vedi 6.9 a pag. 68).

Per sospendere un componenti della protezione:

Apri la finestra principale e seleziona il componente sotto **Protezione** e clicca su Sospendi.

Lo stato del componente/attività diventa sospeso. Il componente o attività resterà sospeso fino a quando l'utente li ripristinerà facendo clic sul link Riprendi protezione.

Quando metti in pausa un componente, vengono salvate le statistiche della corrente sessione di Kaspersky Anti-Virus e restano disponibili fino a che il componente viene aggiornato.

Per interrompere un componente della protezione:

Apri la finestra principale e seleziona il componente sotto **Protezione** e clicca su Interrompi.

Lo stato del componente diventa *Disattivato,* mentre il nome del componente diventa inattivo sotto **Protezione** (grigio). Il componente resterà interrotto fino a quando l'utente li abiliterà facendo clic sul Abilita.

Ogni componente di protezione può venir arrestato dalla finestra delle impostazioni dell'applicazione. Apri la finestra delle impostazioni, seleziona il componente sotto **Protezione** e deseleziona **Abilita <nome del componente>**.

Quando si disabilita un componente di protezione tutte le statistiche vengono azzerate e ricominciate al riavvio del componente.

I componenti di protezione vengono altresì disabilitati se la protezione in tempo reale del computer viene arrestata (vedi 6.1.2 a pag. 60).

6.1.4. Ripristino della protezione del computer

Se l'utente ha sospeso o interrotto la protezione del computer, potrà ripristinarla mediante uno dei seguenti metodi:

- Dal menu contestuale.

  Selezionare **Riprendi protezione**.

- Dalla finestra principale del programma.

  Seleziona la sezione **Protezione** nella parte sinistra della finestra principale e clicca su Abilita protezione.

Lo stato della protezione diventa immediatamente *attivo*. L'icona del programma nell'area di notifica della barra delle applicazioni diventa attiva (colorata).

6.2. Tecnologia avanzata di disinfezione

Malware sofisticati possono infiltrarsi nei bassi livelli del sistema operative rendendo impossibile la loro rimozione. Quando viene scoperto un pericolo sul sistema Kaspersky Anti-Virus 7.0 suggerisce una speciale ed estesa procedura di disinfezione che disabilita e rimuove le minacce dal computer.

Completata la procedura il computer dovrà essere riavviato. Si consiglia di avviare una completa scansione del computer dopo il riavvio. Per avviare la procedura di Disinfezione Avanzata apri la finestra delle impostazioni, seleziona **Protezione** e spunta **Attiva tecnologia avanzata di disinfezione** (vedi Figura 6).

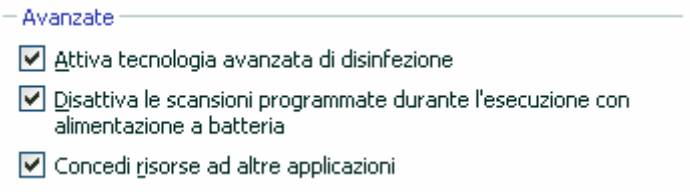


Figura 6. Configurazione delle impostazioni più diffuse

6.3. Funzionamento dell'applicazione su computer portatili

Le attività di scansione possono essere posticipate per non esaurire le batterie.

Poiché la scansione del computer e d il suo frequente aggiornamento assorbono significative risorse e tempo, consigliamo che queste attività vengano programmate. Ciò permetterà di salvaguardare la durata delle batterie. Potrai aggiornare l'applicazione (vedi 5.6 a pag. 56) o lanciare una scansione anti-virus manualmente (vedi 5.3 a pag. 54). Per salvaguardare la durata delle batterie apri la finestra delle impostazioni, seleziona **Protezione** e seleziona ☑ **Disattiva le scansioni programmate durante l'esecuzione con alimentazione a batteria** sotto **Avanzate** (vedi Figura 6).

6.4. Prestazioni del computer

Per limitare il carico della CPU e l'archivio di sottosistema le scansioni possono essere posticipate.

La scansione dei virus incrementa il carico della CPU e del sottosistema abbassando la velocità di esecuzione di altri programmi. Se questo avviene il programma sospende per impostazione la scansione dei virus e restituisce le risorse alle applicazioni in uso.

Ci sono però programmi che si avviano non appena le risorse della CPU sono disponibili e lavorano in background. Per rendere indipendente la scansione dei virus da questi programmi apri la finestra delle impostazioni dell'applicazione, seleziona **Protezione** e spunta in **Avanzate** ☑ **Concedi risorse ad altre applicazioni** (vedi Figura 6).

Notare che questo parametro può essere configurato per ogni attività di scansione. L'impostazione sulla singola attività avrà una più elevate priorità.

6.5. Compatibilità di Kaspersky Anti-Virus con altre applicazioni

Il funzionamento di Anti-Virus può a volte creare conflitti con alter applicazioni installate. Ciò è dovuto al fatto che queste applicazioni dispongono di un meccanismo di auto-difesa che si innesca quando Kaspersky Anti-Virus tenta di integrarsi con esse. Queste applicazioni incorporano plug-in di Autenticazione per Adobe Reader, che verifica l'accesso ai documenti Pdf, Oxigen Phone Manager II la gestione dei cellulari come pure alcuni giochi tamper-proof.

Per risolvere questi inconvenienti apri la finestra delle impostazioni dell'applicazione, seleziona **Protezione** e spunta **Compatibilità con l'autodifesa dell'applicazione** sotto **Compatibilità** (vedi Figura 7). Perché questa impostazione abbia effetto occorre riavviare il sistema operativo.

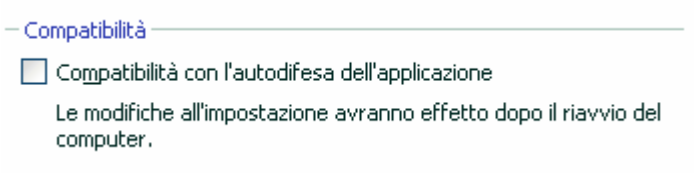


Figura 7. Configurazione delle impostazioni di Compatibilità

Attenzione!

Se l'applicazione è installata su un computer con sistema operativo Microsoft Windows Vista e Microsoft Windows Vista x64, la risoluzione dei problemi di compatibilità con i meccanismi di autodifesa di altre applicazioni non è supportata.

6.6. Avvio di attività di scansione antivirus e aggiornamento utilizzando un diverso account

Kaspersky Anti-Virus 7.0 è dotato di una funzione che consente di avviare le attività sotto un altro account. Questa funzione è normalmente disabilitata e le attività vengono eseguite con l'account con cui l'utente si collega al sistema.

Questa funzione è utile se per esempio durante una scansione occorrono determinati privilegi di accesso. Utilizzando questa funzione, puoi configurare attività da eseguire con l'account di un utente in possesso dei privilegi richiesti.

È possibile che gli aggiornamenti del programma debbano essere eseguiti da un'origine alla quale non hai accesso (per esempio la cartella aggiornamenti di rete) o da un server proxy per il quale non si hanno diritti. È possibile quindi utilizzare questa funzione per eseguire l'aggiornamento utilizzando un account in possesso dei diritti necessari.

Per configurare un'attività di scansione da eseguire con un account utente diverso:

1. Apri la finestra impostazioni dell'applicazione e seleziona l'attività sotto **Scansione**.

2. Fare clic sul pulsante **Personalizza…** nel **Livello di protezione** ed apri la scheda **Avanzate** nella finestra di dialogo che si apre.

Per configurare un'attività di aggiornamento da eseguire con un profilo utente diverso:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Aggiornamento**.
2. Fare clic sul pulsante **Configura** sotto **Impostazioni aggiornamento** ed apri la scheda **Avanzate** nella finestra di dialogo (vedi Figura 7).

Per abilitare questa funzione, selezionare la casella ☑ **Esegui questa attività come**. Inserire i dati di login del profilo con cui si desidera avviare l'attività: nome utente e password.

Nota che, se la funzione Esegui questa attività come non è abilitata, gli aggiornamenti programmati avverranno in accordo con l'utente corrente. Nel caso che nessuno sia registrato nel sistema e tale opzione non sia configurata, un aggiornamento programmato si avvierà come SISTEMA.

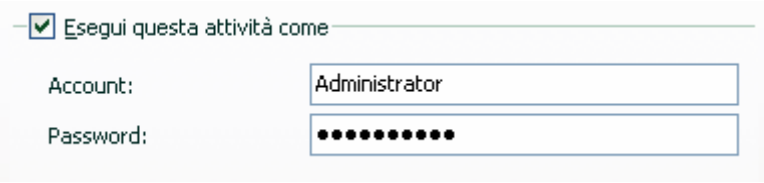


Figura 8. Configurazione di un aggiornamento utilizzando un diverso account

6.7. Configurazione di azioni programmate e notifiche

Programmare la configurazione delle scansioni, degli aggiornamenti dell'applicazione e dei messaggi di funzionamento di Kaspersky Anti-Virus è identico.

Per impostazione sono disabilitate le attività di scansione create durante l'installazione. L'unica eccezione è la scansione degli oggetti di avvio che avviene ogni volta che si avvia Kaspersky Anti-Virus. Gli aggiornamenti sono configurati per essere eseguiti automaticamente non appena un aggiornamento è disponibile sui server di Kaspersky Lab.

Nel caso tu non sia soddisfatto di queste impostazioni puoi riconfigurare la pianificazione.

Il primo valore da definire è la frequenza di un evento (esecuzione o notifica). Seleziona l'opzione desiderata sotto **Frequenza** (vedi Figure 9). Poi occorre specificare sotto **Pianificazione: Aggiornamento** l'impostazione di aggiornamento per l'opzione selezionata. Sono disponibili le seguenti selezioni:

- **A un'ora specificata**. L'azione si avvia o viene spedita la notifica alla data ed all'ora specificata.
- **All'avvio dell'applicazione**. L'azione si avvia o viene spedita la notifica ogni volta che viene avviato Kaspersky Anti-Virus. E' anche possibile specificare un ritardo dall'avvio dell'applicazione.
- **Dopo ogni aggiornamento**, L'evento si avvia dopo l'aggiornamento del database dell'applicazione (opzione valida solo per le scansioni).
- **Ogni minuto**. L'intervallo di esecuzione dell'evento è definito in minuti. Imposta i minuti. Non può superare i 59 minuti.
- **Ore**. L'intervallo di esecuzione dell'evento è definito in ore. Imposta le ore in **OGNI N ore** e imposta **N**. Ad esempio **OGNI 1 ora**.

Figure 9. Creazione del piano di esecuzione delle attività

- **Giorni**. L'intervallo di esecuzione dell'evento è definito in giorni. Imposta i giorni:
  - Seleziona **OGNI N giorni** e specifica N.
  - Seleziona **Ogni giorno feriale** se desideri che l'azione avvenga da Lunedì a Venerdì.

- Seleziona **Ogni fine settimana** per avviare l'azione il Sabato e la Domenica.

  Usa il campo **Ora** per specificare l'ora di avvio dell'azione.

Settimane. L' esecuzione dell'evento avverrà in un certo giorno della settimana. Selezionando questa frequenza spunto il giorno della settimana in cui lanciare l'azione. Usa il campo Ora per definire l'ora del lancio.

Ogni mese. L' esecuzione dell'evento avverrà una volta al mese al momento specificato.

Se una azione non riesce ad avviarsi (ad esempio non è installato un programma di posta elettronica oppure il computer è spento in quel momento)l'azione può essere configurata in modo che venga lanciata automaticamente non appena possibile. Spunta nella finestra di programmazione **Esegui attività se saltata.**

6.8. Tipi di Malware da monitorare

Kaspersky Anti-Virus ti protegge da diversi tipi di programmi pericolosi. Indipendentemente dalle impostazioni il programma protegge sempre il computer dai tipi di malware più pericolosi, come virus, trojan ed hack tools. Questi programmi possono causare significati danni al tuo computer. Per migliorare la sicurezza del tuo computer puoi espandere l'elenco delle minacce che il programma intercetterà facendogli monitorare ulteriori tipi di programmi pericolosi.

Per scegliere da quali programmi pericolosi Kaspersky Anti-Virus ti proteggerà seleziona la finestra delle impostazioni di programma e seleziona **Minacce ed Esclusioni** (vedi Figura 10).

Il box delle categorie Malware contiene i tipi di minacce (vedi 1.3 a pag. 12):

Virus, worm, Trojan, utilità di hacking. Questo gruppo comprende le categorie più comuni e pericolose. Questo è il limite minimo ammissibile di sicurezza. Su raccomandazione degli esperti di Kaspersky Lab , Kaspersky Anti-Virus verifica sempre queste categorie di programmi pericolosi.

Spyware, adware, dialer. Questo gruppo include software potenzialmente pericolosi che possono disturbare l'utente o causare seri danni.

Software potenzialmente pericoloso (riskware). Questo gruppo include programmi che non sono maligni o pericolosi. In ogni caso, in certe condizioni, potrebbero essere utilizzati per nuocere al computer**.**

I gruppi sopra riportati comprendono la totalità delle minacce che il programma riconosce durante la scansione degli oggetti.

Se si selezionano tutti i gruppi, Kaspersky Anti-Virus fornisce la più alta protezione per il tuo computer. Se il secondo e terzo gruppo sono disabilitati il programma ti proteggerà dai programmi pericolosi più comuni. Questi non comprendono programmi potenzialmente pericolosi ed altri che potrebbero venire installati sul computer e che potrebbero danneggiare i tuoi file, sottraare soldi o assorbire il tuo tempo.

Kaspersky Lab consiglia di non disabilitare il monitoraggio del secondo gruppo. Se sorge un problema con un programma che l'utente considera attendibile consigliamo di creare un'esclusione (vedi 6.9 a pag. 68).

Per selezionare il tipo di malware da monitorare:

apri la finestra impostazioni dell'applicazione e seleziona **Minacce ed esclusioni**. La configurazione si esegue nelle **Categorie malware** (vedi Figura 10).

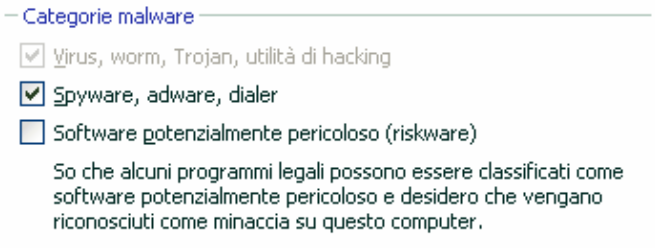


Figura 10. Selezione delle minacce da monitorare

6.9. Creazione di una zona attendibile

Una *zona attendibile* è un elenco di oggetti creato dall'utente, che Kaspersky Anti-Virus non esamina. In altre parole, si tratta di una serie di programmi esclusi dalla protezione.

L'utente crea una zona protetta sulla base delle proprietà dei file che usa e dei programmi installati sul computer. Questo elenco di esclusioni può tornare utile, per esempio, se Kaspersky Anti-Virus blocca l'accesso a un oggetto o programma della cui sicurezza l'utente è assolutamente sicuro.

È possibile escludere file dalla scansione in base al formato, oppure usare una maschera, escludere una determinata area (per esempio una cartella o un programma), processi di programmi o oggetti in base allo stato che il programma assegna agli oggetti durante una scansione.

Nota!

Gli oggetti enclisi non sono soggetti a scansione mentre avviene la scansione sul disco o sulla cartella a cui appartengono. Comunque se selezioni un oggetto in particolare la regola di esclusione non verrà applicata.

Per creare un elenco di esclusioni,

1. Apri la finestra delle impostazioni dell'applicazione e seleziona la sezione **Minacce ed esclusioni** (vedi Figura 10).
2. Fare clic sul pulsante **Area attendibile** nella sezione **Esclusioni**.
3. Configurare le regole di esclusione degli oggetti e creare un elenco di applicazioni attendibili nella finestra che si apre (vedi Figura 11).

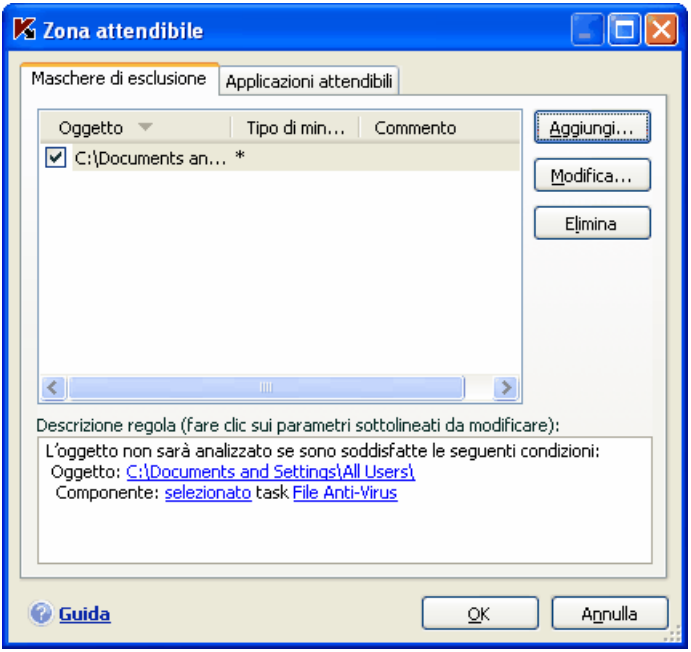


Figura 11. Creazione di una zona attendibile

6.9.1. Regole di esclusione

Le regole di esclusione sono delle condizioni in base alle quali Kaspersky Anti-Virus stabilisce quali oggetti non sottoporre a scansione.

Puoi escludere i file dalla scansione in base al formato, usare una maschera, escludere una determinata area come una cartella o un programma, processi di programmi o oggetti in base alla loro classificazione della Enciclopedia dei tipi di minaccia.

Il *Tipo di Minaccia* à lo stato che Kaspersky Anti-Virus assegna a un oggetto durante la scansione. Un verdetto si basa sulla classificazione dei programmi nocivi e potenzialmente pericolosi presenti nell'Enciclopedia dei virus di Kaspersky Lab.

Il Software potenzialmente pericoloso non svolge una funzione nociva vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. Di questa categoria fanno parte, per esempio, programmi di amministrazione remota, client IRC, servizi FTP, utilità multifunzione per interrompere o nascondere i processi, keylogger, macro per la decodifica di password, autodialer, ecc. Questi programmi non sono classificati come virus. Essi possono essere suddivisi in diverse categorie, per esempio adware, scherzi, riskware, ecc. (per ulteriori informazioni sui programmi potenzialmente pericolosi individuati da Kaspersky Anti-Virus, vedere Virus Encyclopedia su www.viruslist.com). Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di essi sono estremamente comuni, hai ha la possibilità di escluderli dalla scansione. Per questo devi aggiungere il nome della minaccia o maschera alla zona sicura usando la classificazione dell'Enciclopedia dei virus.

Poniamo per esempio di utilizzare frequentemente un programma di amministrazione remota. Si tratta di un sistema di accesso remoto che consente di lavorare da un altro computer. Kaspersky Anti-Virus visualizza questo tipo di applicazione come potenzialmente pericolosa e la blocca. Per evitare il blocco dell'applicazione, è necessario creare una regola di esclusione che specifichi *not-a-virus: RemoteAdmin.Win32RAdmin.22* come tipo di minaccia.

Quando si aggiunge un'esclusione, viene creata una regola che in seguito sarà utilizzata da numerosi componenti del programma (File Anti-Virus, Mail Anti-Virus, Difesa proattiva, Web Anti-Virus) e attività di scansione antivirus. Per creare le regole di esclusione, esiste una finestra specifica accessibile dalla finestra delle impostazioni del programma, dall'avviso di intercettazione dell'oggetto e dalla finestra dei report.

*Per aggiungere esclusioni nella scheda **Maschere di esclusione**:*

1. Fare clic sul pulsante **Aggiungi** nella scheda **Maschere di esclusione** (vedi Figura 11).
2. Nella finestra che si apre (vedi Figura 12), fare clic sul tipo di esclusione nella sezione **Proprietà**:

   Oggetto – esclusione dalla scansione di un oggetto, directory o file corrispondente a una determinata maschera.

☑ **Tipo di minaccia** – esclusione dalla scansione di oggetti in base allo stato assegnato loro dall'Enciclopedia dei virus.

Se si selezionano subito entrambe le caselle, si crea una regola con un determinato stato in accordo con la classificazione dell'Enciclopedia dei virus, In tal caso vale la seguente regola:

- Se si specifica un determinato file come **Oggetto** e un determinato stato nella sezione **Tipo di minaccia**, il file specificato sarà escluso solo se classificato come il tipo di minaccia selezionata.
- Se si seleziona un'area o cartella come **Oggetto** e lo stato (o maschera dei verdetti) come **Tipo di minaccia**, gli oggetti con quello stato saranno esclusi solo dalla scansione di quell'area o cartella.

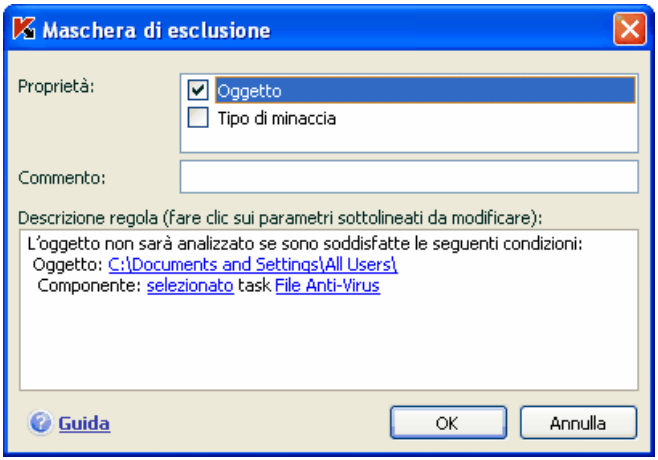


Figura 12. Creazione di una regola di esclusione

3. Assegnare dei valori ai tipi di esclusione selezionati. A tal fine, fare clic con il pulsante sinistro del mouse nella sezione **Descrizione regola** sul link specifica ubicato a fianco del tipo di esclusione:

   - Per il tipo di oggetto, digitare il nome nella finestra che si apre (può trattarsi di un file, di una directory o di una maschera di file, vedi A.2 a pag. 232). Selezionare ☑ **Includi sottocartelle** per l'oggetto (file, maschera di file, cartella) da escludere ogni volta dalla scansione. Per esempio, se si specifica **C:\Program Files\winword.exe** come esclusione selezionando l'opzione sottocartelle, il file **winword.exe** sarà escluso dalla scansione se presente in qualsiasi sottocartella di **C:\Programmi**.

- Digitare il nome completo della minaccia che si desidera escludere dalle scansioni come indicato nell'enciclopedia dei virus, oppure utilizzare una maschera (vedi A.3 a pag. 232 per il **Tipo di minaccia**.

  Per alcuni tipi di minacce, è possibile assegnare condizioni avanzate per l'applicazione di regole nel campo **Impostazioni avanzate**. In molti casi questo campo è riempito automaticamente quando aggiungi una esclusione da una notifica di Difesa Proattiva

  Tra l'altro puoi aggiungere impostazioni avanzate:

  - Invasore (inserimento nei processi del programma) In questo contesto puoi assegnare un nome, un percorso completo all'oggetto inserito (per esempio un file .dll) come condizione di esclusione addizionale.
  - Lancio del Browser Internet. Per tale contesto puoi elencare i dettagli di apertura del browser come impostazioni di esclusione addizionali. Per esempio, è possibile bloccare l'apertura dei browser con determinate impostazioni nella finestra di analisi dell'attività di Difesa Proattiva. Tuttavia, si desidera che il browser si apra per il dominio www.kaspersky.com con un link da Microsoft Office Outlook come regola di esclusione. Per fare questo selezione Microsoft Office Outlook come **Oggetto** e *Lancio del Browser Internet* come **Tipo di Minaccia**, ed inserisci una maschera di dominio nel campo **Impostazioni Avanzate**.

4. Definire quali componenti di Kaspersky Anti-Virus devono applicare questa regola. Se si seleziona qualsiasi, la regola sarà applicata a tutti i componenti. Se si desidera limitare la regola a uno o più componenti, fare clic su qualsiasi che cambia in selezionati. Nella finestra che si apre, selezionare le caselle relative ai componenti ai quali si desidera applicare questa regola di esclusione.

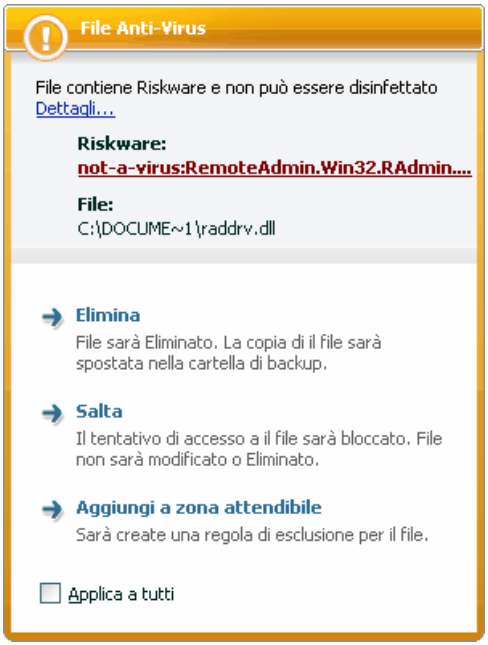


Figura 13. Notifica di rilevamento oggetto pericoloso

Per creare una regola di esclusione dall'avviso di un programma che avverte dell'individuazione di un oggetto pericoloso:

1. Usare il link Aggiungi a zona attendibile nella finestra della notifica (vedi Figura 13).
2. Nella finestra che si apre, verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome dell'oggetto e il tipo di minaccia in base alle informazioni ottenute dalla notifica. Per creare la regola, fare clic su **OK**.

Per creare una regola di esclusione dalla finestra dei report:

1. Selezionare nel report l'oggetto che si desidera aggiungere alle esclusioni.
2. Aprire il menu contestuale e selezionare **Aggiungi a zona attendibile** (vedi Figura 14).
3. Si apre quindi la finestra delle impostazioni delle esclusioni. Verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome

dell'oggetto e il tipo di minaccia in base alle informazioni ottenute dal report. Per creare la regola, fare clic su **OK**.

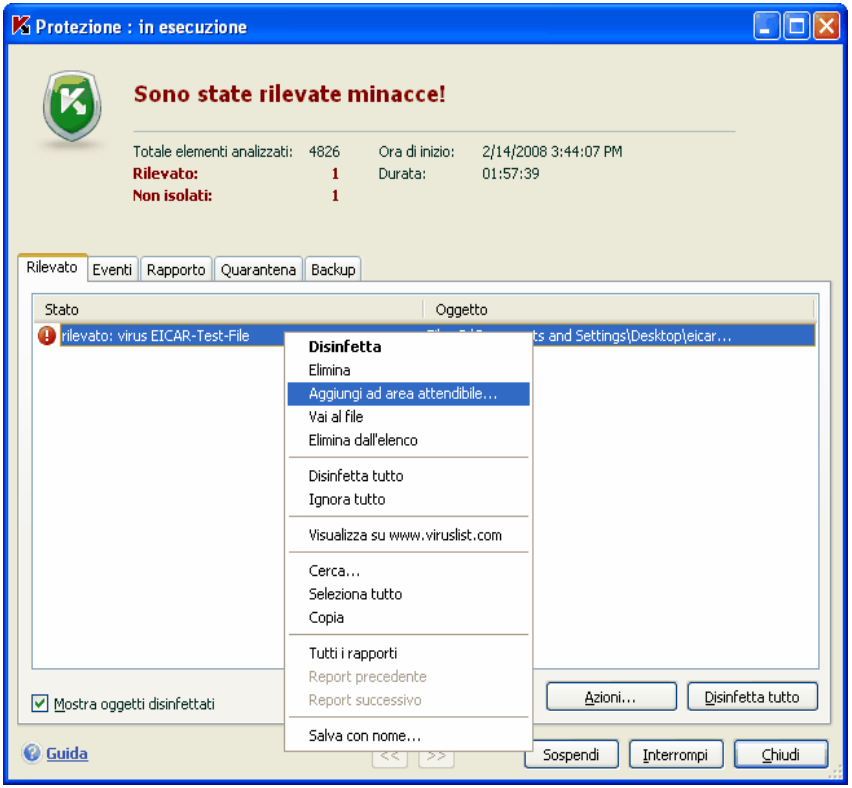


Figura 14. Creazione di una regola di esclusione da un report

6.9.2. Applicazioni attendibili

Kaspersky Anti-Virus è in grado di creare un elenco di applicazioni attendibili di cui non è necessario monitorare le attività dei loro file o della rete e dell'accesso al registro di sistema.

Per esempio, si può ritenere che gli oggetti utilizzati da Windows Notepad siano sicuri e non necessitino di scansione. In altre parole, ci si fida dei processi di questo programma. Per escludere dalla scansione gli oggetti utilizzati da questo processo, aggiungere **Notepad** all'elenco delle applicazioni attendibili. Tuttavia, il file eseguibile e il processo dell'applicazione affidabile saranno sottoposti a scansione antivirus come in precedenza. Per escludere completamente

l'applicazione dalla scansione, è necessario utilizzare le regole di esclusione (vedi 6.9.1 a pag. 69).

Inoltre, è possibile che alcune azioni classificate come pericolose siano in realtà perfettamente normali per le funzioni di determinati programmi. Per esempio, i programmi di commutazione del layout di tastiera intercettano regolarmente il testo digitato sulla tastiera. Per giustificare le operazioni specifiche di tali programmi ed escludere dal monitoraggio le loro attività, si raccomanda di aggiungerli all'elenco delle applicazioni attendibili.

Grazie alle esclusioni delle applicazioni attendibili è possibile inoltre risolvere potenziali conflitti di compatibilità tra Kaspersky Anti-Virus e altre applicazioni (per esempio il traffico di rete da un altro computer che è appena stato esaminato dall'applicazione antivirus) e incrementare la produttività del computer, particolarmente importante quando si utilizzano applicazioni server.

Per impostazione predefinita, Kaspersky Anti-Virus esamina gli oggetti aperti, eseguiti o salvati da qualsiasi processo di programma e monitora l'attività di tutti i programmi e il traffico di rete che creano.

È possibile creare un elenco di applicazioni attendibili nella scheda specifica **Applicazioni attendibili** (vedi Figura 15). L'elenco creato al momento dell'installazione contiene applicazioni sicure la cui attività non verrà controllata come consigliato da Kaspersky Lab. Se non ritieni sicura una applicazione dell'elenco deseleziona il corrispondente riquadro. È possibile aggiungere elementi e modificare l'elenco servendosi dei pulsanti **Aggiungi, Modifica** ed **Elimina** sulla destra.

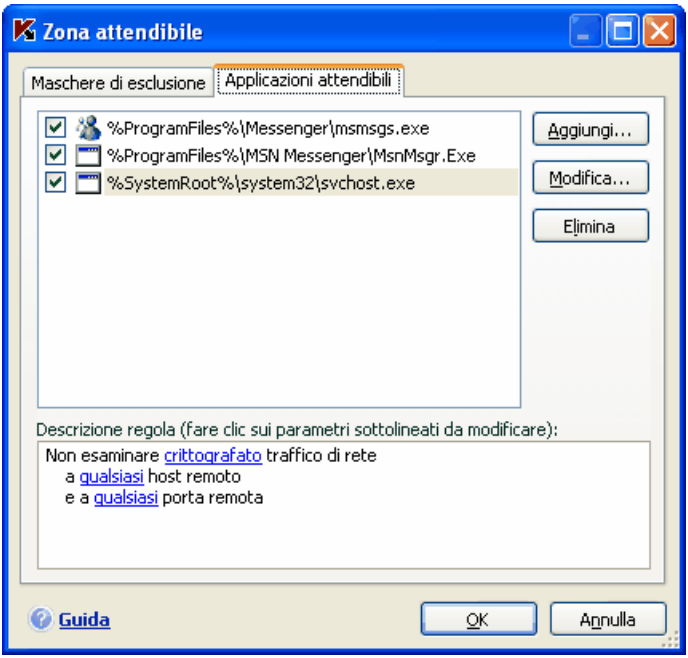


Figura 15. Elenco delle applicazioni attendibili

Per aggiungere un programma all'elenco delle applicazioni attendibili:

1. Fare clic sul pulsante **Aggiungi** nella parte destra delle **Applicazioni attendibili**.

2. Nella finestra **Applicazione attendibile** (vedi Figura 16) che si apre, selezionare l'applicazione per mezzo del pulsante **Sfoglia**. Si apre un menu contestuale. Facendo clic su **Sfoglia** è possibile aprire la finestra di selezione dei file e selezionare il percorso del file eseguibile. In alternative, facendo clic su **Applicazioni** è possibile aprire un elenco delle applicazioni correntemente in funzione e selezionare quelle desiderate.

   Quando si seleziona un programma, Kaspersky Anti-Virus ricorda gli attributi interni del file eseguibile e li usa per identificare il programma come affidabile durante le scansioni.

   Il percorso del file viene inserito automaticamente quando se ne seleziona il nome.

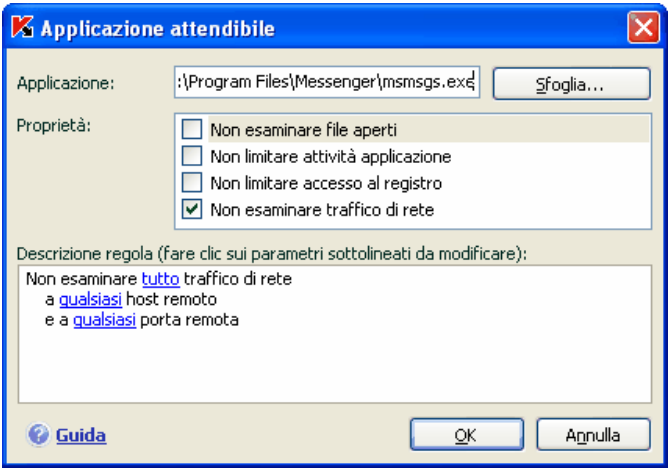


Figura 16. Aggiunta di un'applicazione all'elenco delle applicazioni attendibili

3. Specificare quindi le azioni eseguite da questo processo che Kaspersky Anti-Virus non deve monitorare:

   - **Non esaminare file aperti** – esclude dalla scansione tutti i file che il processo dell'applicazione affidabile apre.
   - **Non limitare attività applicazione** – esclude dal monitoraggio di Difesa proattiva qualsiasi attività, sospetta o no, che un'applicazione affidabile sta eseguendo.
   - **Non limitare accesso al registro** – esclude dalla scansione i tentativi di accesso al registro di sistema avviati dalle applicazioni attendibili.
   - **Non esaminare traffico di rete** – esclude dalle scansioni antivirus e antispam il traffico di rete avviato dalle applicazioni attendibili. possibile escludere dalla scansione il traffico di rete o quello protetto (SSL) generato da tali applicazioni. A tal fine, usare il collegamento tutto**.** Questo sarà modificato in crittografato. È inoltre possibile limitare l'esclusione assegnando una porta remota o un host remoto. Per creare una limitazione, fare clic su qualsiasi, che diventa selezionato, e digitare un valore per la porta/host remoto.

CAPITOLO 7. FILE ANTI-VIRUS

Kaspersky Anti-Virus contiene un componente speciale per la protezione antivirus dei file presenti nel computer, *File Anti-Virus.* Esso viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer ed esamina tutti i file aperti, salvati o eseguiti.

L'attività del componente è indicata dall'icona di Kaspersky Anti-Virus nell'area di notifica della barra delle applicazioni, che durante la scansione di un file assume questo aspetto  .

Per impostazione predefinita, File Anti-Virus *scansiona soltanto i file nuovi o modificati*. In altre parole, esamina i file che sono stati aggiunti o modificati successivamente all' accesso precedente. I file vengono esaminati con il seguente algoritmo:

1. Il componente intercetta ogni tentativo da parte dell'utente o programmi di accedere ai file.
2. File Anti-Virus esamina i database iChecker™ e iSwift™ in cerca di informazioni sul file intercettato. Sulla base delle informazioni reperiti decide se controllare il file.

Il processo di scansione prevede i due seguenti passaggi:

1. Il file viene analizzato. Oggetti maligni vengono riconosciuti per confronto con i database dell'applicazione che contengono le descrizioni di tutti i programmi pericolosi e delle minacce aggiornate, con il modo per neutralizzarli.
2. Dopo l'analisi sono previste tre azioni alternative:
    a. In caso di rilevamento di un codice nocivo, File Anti-Virus blocca il file interessato, ne salva una copia nel *Backup* e cerca di ripararlo. Se la riparazione ha esito positivo, il file viene reso nuovamente accessibile. In caso contrario il file viene eliminato.
    b. Se il codice viene rilevato in un file sospettato di essere nocivo ma senza alcuna prova di ciò, il file viene inviato in *Quarantena*.
    c. Se nel file non viene rilevato alcun codice nocivo, il file viene immediatamente ripristinato.

7.1. Selezione di un livello di protezione dei file

File Anti-Virus protegge i file in uso ad uno dei seguenti livelli (vedi Figura 17):

- **Protezione massima** – il livello di monitoraggio più approfondito dei file aperti, salvati o eseguiti.
- **Consigliato**. Kaspersky Lab raccomanda questo livello. Esso esegue la scansione delle seguenti categorie di oggetti:
  - Programmi e file in base ai contenuti
  - Solo gli oggetti nuovi e gli oggetti modificati dopo l'ultima scansione
  - Oggetti OLE incorporati
- **Alta velocità** – livello che consente di utilizzare le applicazioni che richiedono considerevoli risorse di sistema, grazie alla limitazione del numero di file esaminati.

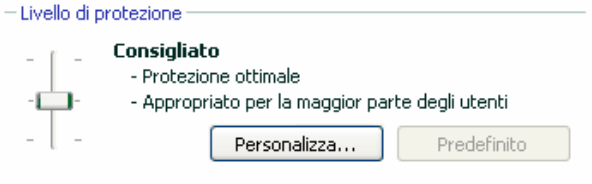


Figura 17. Livello di protezione di File Anti-Virus

Per impostazione predefinita, File Anti-Virus è impostato su **Consigliato**.

È possibile aumentare o ridurre il livello di protezione dei file di lavoro selezionando il livello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di protezione:

Regolare i cursori. Regolando il livello di protezione, si definisce il rapporto tra la velocità di scansione e il numero totale di file esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di file esaminati.

Se nessuno dei livelli di sicurezza è ritenuto soddisfacente, è possibile personalizzarne le impostazioni di protezione. Selezionare a tal fine il livello che più si approssima alle esigenze di sicurezza del computer e utilizzarlo come modello per modificare le impostazioni. In tal caso il livello diventa

Personalizzato. Osserviamo un esempio in cui un livello di protezione predefinito debba essere modificato.

Esempio:

> Il lavoro svolto sul computer comporta numerosi di tipi di file, alcuni dei quali di dimensioni piuttosto elevate. L'utente non desidera correre il rischio di omettere nella scansione eventuali file a causa delle dimensioni o dell'estensione, anche se ciò potrebbe influire sulla produttività del computer.

Suggerimento per selezionare un livello:

> In base ai dati sulla provenienza, si potrebbe concludere che il rischio di infezione da parte di un programma nocivo sia piuttosto elevato. Le dimensioni e il tipo dei file gestiti sono molto eterogenei e l'eventuale esclusione di qualsiasi file dalla scansione comporterebbe un rischio elevato per i dati del computer. L'utente desidera esaminare i file utilizzati in base al contenuto, non in base all'estensione.
>
> Si raccomanda quindi di selezionare inizialmente il livello di protezione **Consigliato** e di apportare le seguenti modifiche: rimuovere le restrizioni sui file eliminati e ottimizzare il funzionamento di File Anti-Virus esaminando solo i file nuovi e modificati. In tal modo la scansione non influirà eccessivamente sulle risorse di sistema e sarà possibile continuare a usare senza problemi altre applicazioni.

Per modificare le impostazioni di un livello di protezione:

1. Apri la finestra impostazioni dell'applicazione e seleziona **File Anti-Virus** sotto **Protezione**.
2. Clicca su **Personalizza** sotto **Livello di protezione** (vedi Figura 17).
3. Modifica i parametri del file di protezione nella finestra e premi **OK**.

7.2. Configurazione di File Anti-Virus

Il modo in cui File Anti-Virus proteggerà il computer su cui è installato dipendono dalla configurazione. Le impostazioni del programma possono essere suddivise nei seguenti gruppi:

- Impostazioni che definiscono i tipi di file (vedi 7.2.1 a pag. 81) da sottoporre alla scansione antivirus
- Impostazioni che definiscono l'ampiezza della protezione (vedi 7.2.2 a pag. 83)
- Impostazioni che definiscono le reazioni del programma agli oggetti pericolosi individuati (vedi 7.2.6 a pag. 90)

- Impostazioni che definiscono l'uso del metodo euristico (vedi 7.2.4 a pag. 88)
- Impostazioni avanzate di File Anti-Virus (vedi 7.2.3 a pag. 85)

La presente sezione prende in esame questi gruppi di impostazioni.

7.2.1. Definizione dei tipi di file da esaminare

Selezionando i tipi di file da esaminare, si specificano i formati di file, le dimensioni e le unità da sottoporre alla scansione antivirus all'apertura, esecuzione o salvataggio.

Al fine di agevolare la configurazione, tutti i file sono stati suddivisi in due gruppi: *semplici* e *complessi*. I file semplici non contengono oggetti (per esempio i file .txt). I file complessi possono contenere numerosi oggetti, ciascuno dei quali a sua volta può avere diversi livelli di nidificazione. Gli esempi sono numerosi: archivi, file che contengono macro, fogli di calcolo, e-mail con allegati, ecc.

I tipi di file esaminati vengono definiti nella sezione **Tipi di file** (vedi Figura 18). Selezionare una delle seguenti opzioni:

Esamina tutti i file. Con questa opzione selezionata tutti gli oggetti del file system che vengono aperti, eseguiti o salvati saranno esaminati senza eccezioni.

Esamina programmi e documenti (in base al contenuto). Se è stato selezionato questo gruppo di file, File Anti-Virus esaminerà solo i file potenzialmente infetti, cioè i file che possono contenere virus.

> **Nota:**
>
> Vi sono formati file nei quali è molto basso il rischio di essere infettati e conseguentemente venire attivati. Un esempio sono i file .txt.
>
> E viceversa ci sono formati file che contengono o possono contenere codici eseguibili. Ad esempio i formati .exe, .dll oppure .doc. Il rischio di infezione per questi file è piuttosto elevato.

Prima di cercare virus in un file, viene analizzata l'intestazione interna del file stesso al fine di individuare il formato (txt, doc, exe, ecc.). Se dall'analisi risulta che il formato del file non consente infezioni, il file viene escluso dalla scansione e messo immediatamente a disposizione dell'utente. Se il formato file è infettabile, il file viene sottoposto a scansione antivirus.

Esamina programmi e documenti (in base all'estensione). Se è stata selezionata questa opzione, File Anti-Virus esamina solo i file

potenzialmente infetti determinando il formato file in base all'estensione. Per mezzo del link estensione possibile consultare un elenco delle estensioni (vedi A.1 a pag. 229) esaminate con questa opzione.

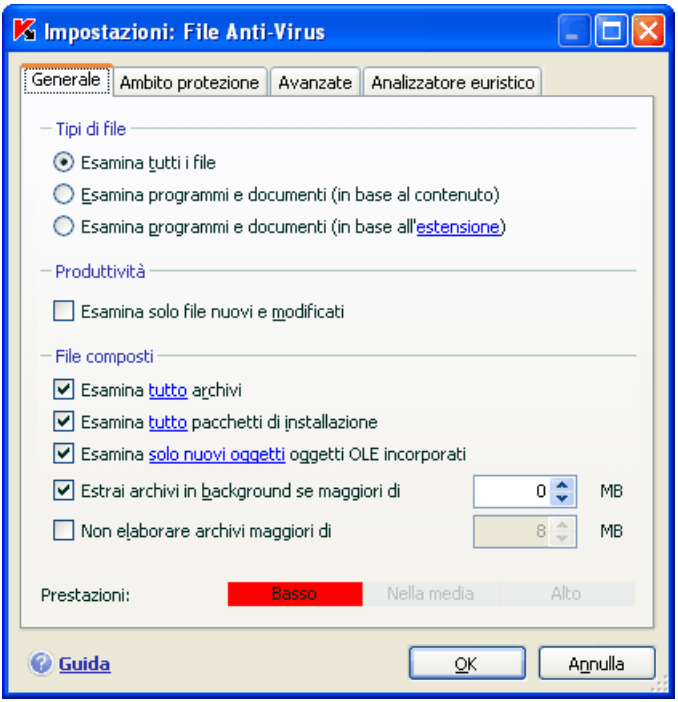


Figura 18. Selezione dei tipi di file sottoposti a scansione antivirus

Suggerimento:

Ricordare che è possibile inviare virus all'interno di file con estensione .txt che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione **Esamina programmi e documenti (in base all'estensione),** tale file sarebbe escluso dalla scansione. Selezionando invece l'opzione **Esamina programmi e documenti (in base al contenuto)** ignorando le estensioni, File Anti-Virus analizzerebbe in primo luogo le intestazioni dei file, rivelando il falso file .txt come un file .exe. Il file sarebbe quindi sottoposto a un'approfondita scansione antivirus.

Nella sezione **Produttività**, è possibile specificare di sottoporre a scansione antivirus i soli file nuovi o modificati dopo l'ultima scansione. Questa modalità riduce considerevolmente la durata della scansione e aumenta la velocità del programma. Per attivare questa modalità, selezionare la casella **Esamina**

solo file nuovi e modificati. Questa modalità si applica sia ai file semplici sia a quelli complessi.

Nella sezione **File composti**, specificare quali file complessi sottoporre alla scansione antivirus:

- **Esamina archivi** – vengono esaminati archivi .zip, .cab, .rar, e .arj.
- **Esamina pacchetti di installazione** – vengono sottoposti alla scansione antivirus gli archivi autoestraenti.
- **Esamina oggetti OLE incorporati** – vengono esaminati gli oggetti incorporati all'interno di file (per esempio fogli di calcolo Microsoft Excel o le macro incorporate in un file di Microsoft Office Word, allegati e-mail, ecc.).

Per ogni tipo di file complesso è possibile selezionare ed esaminare tutti i file o solo quelli nuovi usando il link a fianco del nome dell'oggetto. Facendovi clic sopra con il pulsante sinistro del mouse, il suo valore cambia. Se la sezione **Produttività** è stata impostata in modo da esaminare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file complesso da sottoporre a scansione.

Per specificare quali file complessi non devono essere sottoposti alla scansione antivirus utilizzare le seguenti impostazioni:

- **Estrai archivi in background se maggiori di ... MB**. Se è stata selezionata questa opzione, i file di dimensioni superiori a quella specificata saranno esclusi dalla scansione.
- **Non elaborare archivi maggiori di ... MB**. Se le dimensioni di un oggetto complesso superano questo limite, il programma lo esamina come se fosse un oggetto singolo (analizzando l'intestazione) e lo restituisce all'utente. Gli oggetti in esso contenuti saranno esaminati in un secondo momento. Se questa opzione non è stata selezionata, l'accesso ai file di dimensioni superiori sarà bloccato fino a quando saranno stati esaminati.

7.2.2. Definizione dell'ambito della protezione

File Anti-Virus esamina per impostazione predefinita tutti i file che vengono usati, indipendentemente dalla loro posizione, sia essa un disco fisso, un CD-ROM o un'unità flash.

È possibile limitare l'ambito della protezione procedendo come segue:

1. Apri la finestra impostazioni dell'applicazione e seleziona **File Anti-Virus** sotto **Protezione.**

2. Fare clic sul pulsante **Personalizza** nell'area del livello di protezione (vedi Figura 17).
3. Seleziona **Ambito protezione** nella finestra di dialogo (vedi Figura 19).

La scheda visualizza un elenco di oggetti che File Anti-Virus analizzerà. La protezione è abilitata per impostazione predefinita per tutti gli oggetti presenti sui dischi fissi, su supporti esterni e su unità di rete connesse al computer. È possibile aggiungere elementi e modificare l'elenco servendosi dei pulsanti **Aggiungi, Modifica** ed **Elimina**.

Se si desidera proteggere un numero minore di oggetti, è possibile procedere come segue:

- Specificare solo le cartelle, le unità e i file che necessitano di protezione.
- Creare un elenco di oggetti che non necessitano di protezione.
- Combinare i metodi uno e due per creare una protezione il cui ambito esclude una serie di oggetti.

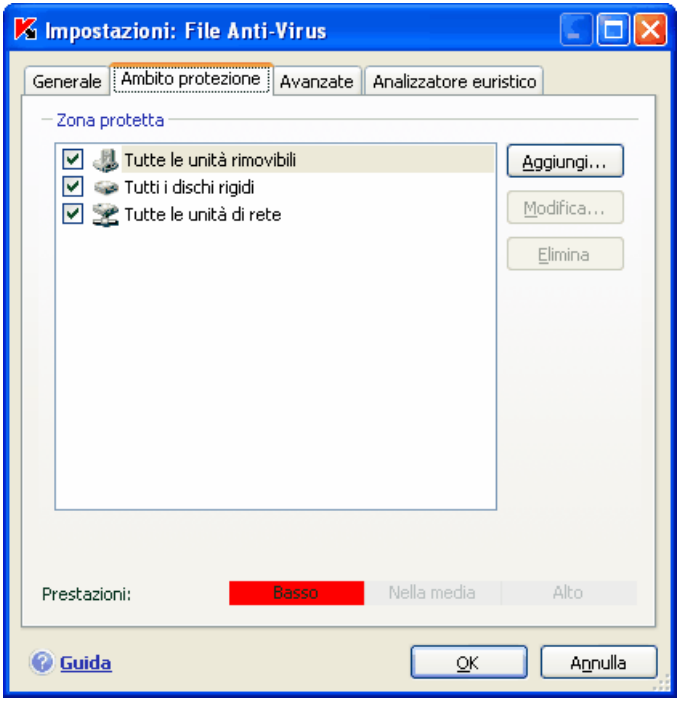


Figura 19. Definizione dell'ambito della protezione

- Puoi usare le maschere quando aggiungi oggetti da controllare. Nota che puoi inserire solo maschere con percorsi assoluti agli oggetti.
- **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file della cartella *C:\dir*
- **C:\dir*.exe** – tutti i file con estensione .exe nella cartella *C:\dir*
- **C:\dir*.ex?** – tutti i file con estensione .ex? nella cartella *C:\dir*, dove ? rappresenta un carattere qualsiasi
- **C:\dir\test** – solo il file *C:\dir\test*

Per eseguire la scansione in modo ricorrente spunta **Includi sottocartelle**.

Attenzione!

Ricordare che File Anti-Virus esamina solo i file inclusi nell'ambito della protezione creato. I file non inclusi in quell'ambito saranno disponibili per l'uso senza essere sottoposti a scansione antivirus. Ciò incrementa il rischio di infezione del computer.

7.2.3. Configurazione delle impostazioni avanzate

È possibile specificare, come impostazioni avanzate di File Anti-Virus, la modalità di scansione del sistema, nonché configurare le condizioni per mettere temporaneamente in pausa il componente.

Per configurare le impostazioni avanzate di File Anti-Virus:

1. Apri la finestra delle impostazioni dell'applicazione e seleziona **File Anti-Virus** sotto **Protezione**.
2. Clicca sul pulsante **Personalizza** nell'area **Livello Sicurezza** (vedi Figura 17).

3. Seleziona il tasto **Avanzate** nella finestra di dialogo (vedi Figura 20).

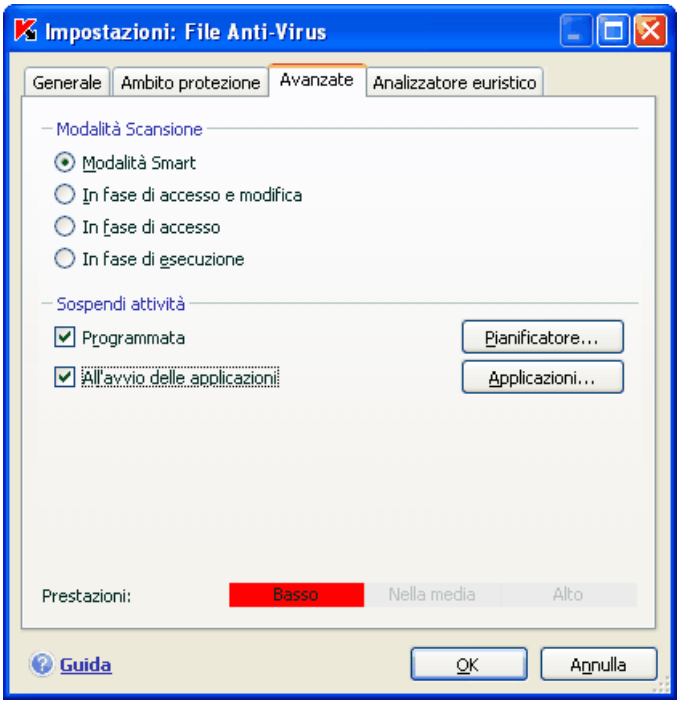


Figura 20. Configurazione delle impostazioni avanzate di File Anti-Virus

La modalità di scansione dei file determina le condizioni di elaborazione di Anti-Virus file. Sono disponibili le seguenti opzioni:

- **Modalità Smart**. Questa modalità mira ad accelerare l'elaborazione dei file per restituirli all'utente. Quando è selezionata, la decisione di scansione viene presa analizzando le operazioni eseguite col file.

  Ad esempio, quando si utilizza un file di Microsoft Office, Kaspersky Anti-Virus esamina il file all'apertura iniziale ed alla chiusura finale. Tutte le operazioni comprese tra queste due operazioni non vengono esaminate.

  La modalità Smart è quella predefinita.

- **In fase di accesso e modifica** – Anti-Virus file esamina i file quando vengono aperti o modificati.

- **In fase di accesso** – i file vengono esaminati solo quando si cerca di aprirli.

- **In fase di esecuzione** – i file vengono esaminati solo quando si cerca di eseguirli.

Potrebbe essere necessario sospendere l'attività di Anti-Virus file quando si eseguono attività che richiedano una grande quantità di risorse del sistema. Per diminuire il carico e fare in modo che l'utente recuperi rapidamente l'accesso ai file, si consiglia di configurare il componente per la disattivazione ad una certa ora o quando vengono utilizzati determinati programmi.

Per sospendere l'attività del componente per un certo tempo, selezionare **Programmata** nella finestra che si apre (vedi Figura 20) , fare clic su **Piano** e assegnare un intervallo per la disattivazione e la riattivazione del componente. Per fare ciò, inserire una valore in formato HH:MM nei campi corrispondenti.

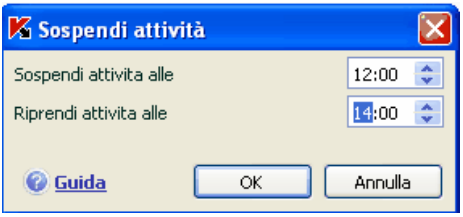


Figura 21. Sospensione dell'attività del componente

Per disattivare il componente quando si lavora con programmi che utilizzano una grande quantità di risorse del sistema, selezionare **All'avvio delle applicazioni** e modificare l'elenco di programmi nella finestra che si apre (vedi Figura 22) facendo clic su **Applicazioni**.

Per aggiungere un'applicazione all'elenco, utilizzare il pulsante **Aggiungi**. Si apre un menu sensibile al contesto, dal quale, facendo clic su **Sfoglia** si raggiunge la finestra standard di selezione file per specificare il file eseguibile dell'applicazione da aggiungere; oppure, è possibile passare all'elenco delle applicazioni attualmente in esecuzione scegliendo **Applicazioni** e selezionare quella desiderata.

Per eliminare un'applicazione, selezionarla dall'elenco e fare clic su **Elimina**.

È possibile disabilitare temporaneamente la sospensione dell'attività di File Anti-Virus con un'applicazione specifica, deselezionandone il nome. Non è necessario eliminarla dall'elenco.

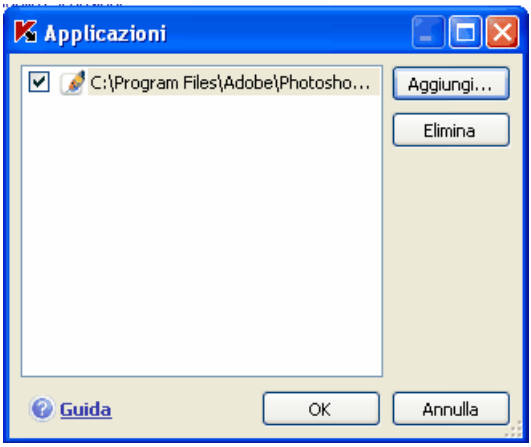


Figura 22. Creazione di un elenco di applicazioni

7.2.4. Utilizzo dell'analizzatore euristico

I metodi euristici sono utilizzati da numerosi componenti di protezione in tempo reale, come File, Mail, Web Anti-Virus come pure dalle scansioni virus.

Naturalmente la scansione che usa il metodo della firma con un database creato preventivamente e che contiene una descrizione delle minacce conosciute e del modo di trattarle fornirà una risposta definitiva riguardo la pericolosità di un oggetto ed a quale classe di programmi pericolosi esso appartiene. Il metodo euristico, diversamente dal metodo della firma, è spinto a riconoscere comportamenti od operazioni tipiche piuttosto che codici pericolosi e che porta il programma a stabilire se un file presenta queste probabilità. Il vantaggio del metodo euristico è che necessita di database precostituiti per funzionare. Per tale ragione nuove minacce sono riconosciute prima che vengano riscontrate dall'analisi dei virus.

Nel caso di una potenziale minaccia l'analizzatore euristico simula l'esecuzione dell'oggetto nell'ambiente sicuro e virtuale di Kaspersky Anti-Virus. Se viene scoperta una sospetta attività non appena l'oggetto viene eseguito, questo verrà definito come maligno e non gli si consentirà l'esecuzione sul host oppure viene presentato un messaggio che richiede altre istruzioni da parte dell'utente.

- Quarantena. le nuove minacce verranno processate in seguito utilizzando database più aggiornati
- Elimina l'oggetto
- Ignora (se si ritiene che l'oggetto non sia pericoloso)

Per usare il metodo euristico seleziona **Usa analizzatore euristico.** In più puoi selezionare il livello di dettagliodella scansione. Per fare questo muovi il cursore su una delle seguenti opzioni: **Basso, Medio o Dettaglio**. La risoluzione della scansione fornisce un modo per bilanciare la profondità e, con essa, la qualità della scansione per le nuove minacce nei confronti del carico sul sistema operativo e della sua durata. Più alto sarà il livello maggiori saranno le risorse di sistema necessarie che la scansione richiederà e più lunga la sua durata.

Avvertenza:

Le nuove minacce rilevate dall'analizzatore euristico sono velocemente analizzate da Kaspersky Lab, e i metodi per neutralizzarle sono aggiunti ai nostri aggiornamenti del database pubblicati a cadenza oraria.

Pertanto, se si aggiornano regolarmente i database dell'applicazione sul computer e i livelli di protezione si mantengono ottimizzati, non è necessario tenere abilitata l'analisi euristica in modo continuativo.

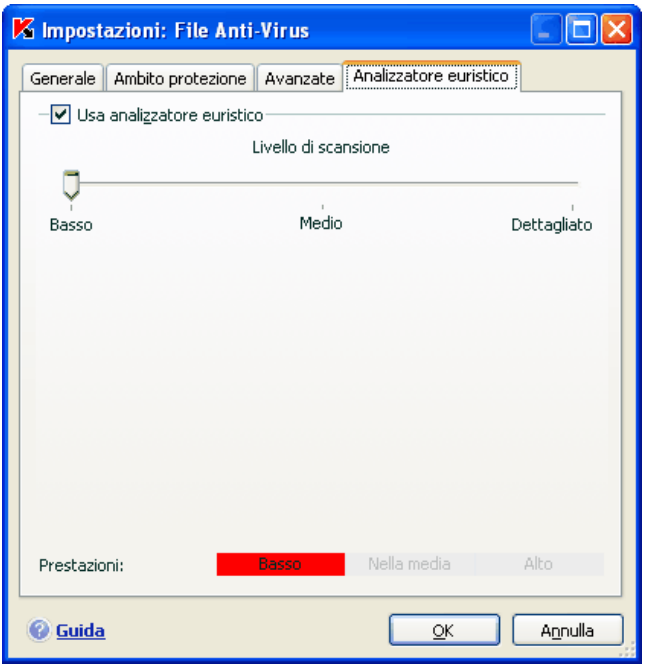


Figura 23. Usa analizzatore euristico

La scheda **Analizzatore euristico** (vedi Figura 23) può essere utilizzata per abilitare/disabilitare l'analisi euristica di File Anti-Virus verso minacce sconosciute. Occorre eseguire i seguenti passaggi:

1. Apri la finestra impostazioni dell'applicazione e seleziona **File Anti-Virus** sotto **Protezione**.
2. Clicca sul pulsante **Personalizza** nell'area del livello di protezione (vedi Figura 17).
3. Seleziona il tasto **Analizzatore euristico** nella finestra di dialogo.

7.2.5. Ripristino delle impostazioni predefinite di File Anti-Virus

Durante la configurazione di File Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni di default. Kaspersky Lab le considera ottimali e le ha riunite nel livello di protezione **Consigliato**.

Per ripristinare le impostazioni predefinite di File Anti-Virus:

1. Apri la finestra delle impostazioni dell'applicazione e seleziona **File Anti-Virus** sotto **Protezione**.
2. Fare clic sul pulsante **Predefinito** nell'area del livello di protezione (vedi Figura 17).

Se, mentre imposti File Anti-Virus, modifichi l'elenco degli oggetti compresi nella zona protetta, il programma ti chiederà se vuoi salvare l'elenco per un uso futuro nel caso dovessi ripristinare le impostazioni iniziali. Per salvare l'elenco degli oggetti selezionare la scheda **Ambito Protezione** nella finestra delle impostazioni.

7.2.6. Selezione delle azioni da applicare agli oggetti

Se durante la scansione antivirus File Anti-Virus rileva o sospetta la presenza di un'infezione all'interno di un file, le fasi successive dipendono dallo stato dell'oggetto e dall'azione selezionata.

File Anti-Virus applica agli oggetti i seguenti stati:

- Programma nocivo (per esempio, *virus, Trojan*) (vedi 1.3 a pag. 12).
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il codice del file contiene una sezione che sembra essere la variante di un virus noto o ricorda la struttura di una sequenza virale.

Per impostazione predefinita, tutti i file infetti sono sottoposti a un tentativo di riparazione e se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

apri la finestra impostazioni dell'applicazione e seleziona **File Anti-Virus** sotto **Protezione**. Tutte le possibili nazioni sono presentate nelle appropriate sezioni (vedi Figura 24).

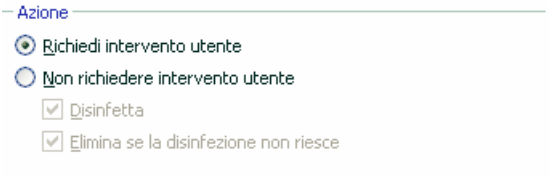


Figura 24. Azioni possibili di File Anti-Virus in caso di oggetti pericolosi

Se l'azione selezionata era	Quando viene rilevato un oggetto pericoloso
Richiedi intervento utente	File Anti-Virus visualizza un avvertimento contenente informazioni sul programma nocivo che ha o potrebbe aver infettato il file e propone una serie di azioni da scegliere. Tali azioni dipendono dallo stato dell'oggetto.
Non richiedere intervento utente	File Anti-Virus blocca l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel report (vedi 15.3 a pag. 176). In un secondo momento sarà possibile tentare di riparare l'oggetto.
Non richiedere intervento utente **Disinfetta**	File Anti-Virus blocca l'accesso all'oggetto e cerca di ripararlo. Se la riparazione ha esito positivo, il file viene ripristinato per l'uso. Se la riparazione fallisce all'oggetto viene assegnato lo stato di *potenzialmente infetto* e verrà spostato in (vedi 15.1 a pag. 170). Le informazioni relative all'evento vengono registrate nel report. In un secondo momento sarà possibile tentare di riparare l'oggetto.

Se l'azione selezionata era	Quando viene rilevato un oggetto pericoloso
Non richiedere intervento utente **Disinfetta** **Elimina se la disinfezione non riesce**	File Anti-Virus blocca l'accesso all'oggetto e cerca di ripararlo. Se la riparazione ha esito positivo, il file viene ripristinato per l'uso. Se la riparazione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene conservata nel Backup (vedi 15.2 a pag. 174).
Non richiedere intervento utente **Elimina**	File Anti-Virus will block access to the object and will delete it.

Indipendentemente dallo stato dell'oggetto (infetto o potenzialmente infetto), prima di cercare di riparare l'oggetto o di eliminarlo Kaspersky Anti-Virus crea una copia di backup e la invia nell'area di Backup, da dove potrà essere recuperata qualora si renda necessario il ripristino dell'oggetto o si presenti un'opportunità di ripararlo.

7.3. Riparazione posticipata

Se l'azione da applicare ai programmi nocivi è **Non richiedere intervento utente**, l'accesso agli oggetti viene bloccato e la riparazione non viene eseguita.

Se l'azione selezionata fosse

Non richiedere intervento utente
Disinfetta

sarebbe bloccato l'accesso anche a tutti gli oggetti non trattati.

Per poter accedere di nuovo agli oggetti bloccati è necessario prima ripararli. Procedere come segue:

1. Selezionare **File Anti-Virus** sotto **Protezione** nella finestra principale dell'applicazione e clicca **Rapporto**.
2. Selezionare gli oggetti desiderati nella scheda **Rilevato** e fare clic sul pulsante **Azioni** → **Disinfetta tutto**.

Se riparato con successo, l'oggetto sarà messo di nuovo a disposizione dell'utente. Se la riparazione non riesce, è possibile *eliminare* l'oggetto o *ignorarlo*. In quest'ultimo caso, l'accesso al file sarà ripristinato. Questo tuttavia

incrementa considerevolmente il rischio di infezione del computer, pertanto si raccomanda di non ignorare gli oggetti nocivi.

CAPITOLO 8. MAIL ANTI-VIRUS

Kaspersky Anti-Virus comprende uno speciale componente che protegge la posta in arrivo e in uscita dagli oggetti pericolosi: *Mail Anti-Virus*. Esso viene eseguito all'avvio del sistema, rimane attivo nella memoria di sistema ed esamina tutta la posta basata sui protocolli POP3, SMTP, IMAP, MAPI[1] e NNTP, nonché la crittografia per POP3 e IMAP (SSL).

L'indicatore di funzionamento del componente è l'icona della barra delle applicazioni di Kaspersky Anti-Virus, che durante la scansione di un messaggio di posta elettronica assume questo aspetto  .

La configurazione predefinita di Mail Anti-Virus è la seguente:

1. Mail Anti-Virus intercetta ciascun messaggio ricevuto o inviato dall'utente.
2. Il messaggio viene suddiviso nelle parti che lo compongono: intestazione, corpo del messaggio, allegati.
3. Il corpo del messaggio e gli allegati (inclusi gli allegati OLE) vengono esaminati per escludere la presenza di oggetti pericolosi. Gli oggetti nocivi vengono individuati per mezzo dei database inclusi nel programma e con l'algoritmo euristico. I database contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti negli elenchi.
4. Dopo la scansione antivirus è possibile scegliere tra le seguenti azioni:
    - Se il corpo del messaggio o gli allegati contengono codici nocivi, Mail Anti-Virus blocca il messaggio, salva una copia dell'oggetto infetto nella cartella *Backup* e cerca di riparare l'oggetto. Se la riparazione del messaggio ha esito positivo, esso viene reso nuovamente disponibile per l'utente. In caso contrario, l'oggetto infetto all'interno del messaggio viene eliminato. Dopo la scansione antivirus, nel campo dell'oggetto del messaggio viene inserito un testo che dichiara che il messaggio è stato esaminato da Kaspersky Anti-Virus.
    - Se nel corpo del messaggio o in un allegato viene individuato un codice che sembra nocivo ma senza alcuna certezza, la parte sospetta del messaggio viene trasferita nella cartella *Quarantena*.

[1] Le e-mail inviate con protocollo MAPI vengono esaminate per mezzo di uno speciale plug-in per Microsoft Office Outlook e The Bat!

- Se all'interno del messaggio non viene individuato alcun codice nocivo, il messaggio viene reso nuovamente disponibile.

Il programma è dotato di uno speciale plug-in (vedi 8.2.2 a pag. 99) per Microsoft Office Outlook in grado di configurare le scansioni della posta con maggior precisione.

Se il client di posta utilizzato è The Bat!, è possibile usare Kaspersky Anti-Virus in aggiunta ad altre applicazioni antivirus. Le regole di trattamento del traffico e-mail (vedi 8.2.3 a pag. 101) sono configurate direttamente da The Bat! e sostituiscono le impostazioni di protezione della posta di Kaspersky Anti-Virus.

Quando si lavora con altri programmi di posta, compresi Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail), Mail Anti-Virus esamina la posta basata sui protocolli SMTP, POP3, IMAP, MAPI ed NNTP.

Osservare che i messaggi trasmessi mediante il protocollo IMAP non vengono esaminati in Thunderbird se si fa uso di filtri che li trasferiscono fuori dalla casella di **posta in entrata.**

8.1. Selezione di un livello di sicurezza della posta elettronica

Kaspersky Anti-Virus protegge la posta elettronica in base a uno dei seguenti livelli (vedi Figura 25):

Protezione Massima – il livello che garantisce il monitoraggio più approfondito della posta in entrata e in uscita. Il programma esamina gli allegati di posta, inclusi gli archivi, indipendentemente dalla durata della scansione.

Consigliato. È il livello consigliato dagli esperti Kaspersky Lab. Esamina gli stessi oggetti del livello **Massima Protezione**, con l'eccezione degli allegati o dei messaggi la cui scansione richiederebbe più di 3 minuti.

Alta velocità – livello di protezione le cui impostazioni consentono di utilizzare applicazioni che assorbono risorse considerevoli, grazie alla limitazione nell'ambito della scansione. Il livelli esamina solo la posta in entrata, escludendo però gli archivi e gli oggetti (e-mail) allegati la cui scansione richiederebbe più di tre minuti. Questo livello è consigliato se nel computer sono installate altre applicazioni di protezione della posta elettronica.

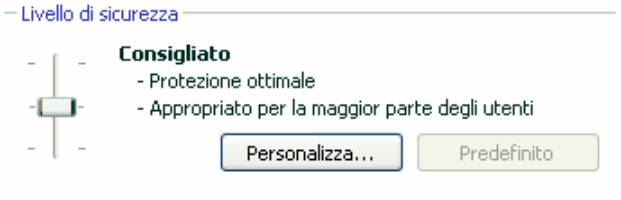


Figura 25. Selezione di un livello di protezione della posta elettronica

Per impostazione predefinita, la protezione della posta elettronica è impostata su **Consigliato**.

È possibile aumentare o ridurre il livello di sicurezza della posta selezionando il livello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Modificando il livello di sicurezza, si definisce il rapporto tra la velocità di scansione e il numero totale di oggetti esaminati: La velocità di scansione è inversamente proporzionale al numero di oggetti e-mail esaminati.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile modificarne le impostazioni. Consigliamo di selezionare come base il livello il più vicino possibile alle tue necessità e modificare i suoi parametri. In questo caso il nome del livello si modificherà in Personalizzata. Osserviamo un esempio in cui le impostazioni predefinite del livello di protezione devono essere modificate.

Esempio:

Il computer si trova all'esterno della LAN e si connette a Internet mediante connessione remota. Il client installato per ricevere e inviare la posta elettronica è Outlook Express e il servizio utilizzato è gratuito. Per varie ragioni, il traffico di posta elettronica prevede un certo numero di archivi allegati. Come garantire una protezione ottimale del computer dalle infezioni trasmesse attraverso la posta elettronica?

Suggerimento per selezionare un livello:

Analizzando la situazione, si potrebbe concludere che il rischio di infezione attraverso la posta elettronica sia piuttosto elevato (a causa dell'assenza di una protezione centralizzata della posta elettronica e del metodo di connessione a Internet).

Il livello di protezione consigliato è quindi **Protezione massima**, apportando le seguenti modifiche: si consiglia di ridurre il tempo di scansione degli allegati, per esempio a 1-2 minuti. La maggior parte degli archivi allegati sarà così sottoposta a scansione antivirus ma la velocità di elaborazione non sarà pregiudicata.

Per modificare un livello di protezione predefinito:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Mail Anti-Virus** sotto **Protezione**.
2. Clicca su **Personalizza** sotto **Livello Sicurezza** (vedi Figura 25).
3. Modifica i parametri di protezione e-mail nella finestra risultante e premi **OK**.

8.2. Configurazione di Mail Anti-Virus

Le modalità di scansione della posta dipendono da una serie di impostazioni che possono essere suddivise nei seguenti gruppi:

- Impostazioni che definiscono il gruppo di messaggi protetto (vedi 8.2.1 a pag. 97)
- Impostazioni che definiscono l'uso del metodo euristico (vedi 8.2.4 a pag. 103)
- Impostazioni di scansione della posta per Microsoft Office Outlook (vedi 8.2.3 a pag. 101) e The Bat! (vedi 8.2.2 a pag. 99)
- Impostazioni che definiscono le azioni da eseguire in caso di oggetti di posta pericolosi (vedi 8.2.4 a pag. 103)

La presente sezione prende in esame queste impostazioni.

8.2.1. Selezione di un gruppo di messaggi protetto

Mail Anti-Virus consente di selezionare i gruppi di messaggi da esaminare per escludere la presenza di oggetti pericolosi.

Per impostazione predefinita, il componente protegge la posta elettronica al livello di sicurezza **Consigliato**, esaminando cioè sia i messaggi in arrivo sia quelli in uscita. La prima volta che si lavora con il programma è consigliabile esaminare la posta in uscita in quanto è probabile che il computer nasconda worm che si servono della posta elettronica come canale di diffusione. Questo accorgimento eviterà il rischio che il computer invii inavvertitamente mailing di massa con oggetti infetti.

Se si è certi che i messaggi che si inviano non contengano oggetti pericolosi, è possibile disabilitare la scansione della posta in uscita procedendo come segue:

1. Apri la finestra impostazioni dell'applicazione e selezione **Mail Anti-Virus** sotto **Protezione**.
2. Clicca il pulsante **Personalizza** nell'area **Livello di sicurezza** (vedi Figura 25).
3. Nella finestra che si apre (vedi Figura 26), seleziona **Solo posta in entrata** nella sezione **Ambito**.

Oltre a selezionare un gruppo di messaggi, è possibile specificare se sottoporre alla scansione anche gli archivi allegati e impostare la durata massima della scansione di un oggetto di posta. Queste impostazioni vengono configurate nella sezione **Restrizioni**.

Se il computer non è protetto da alcun software di rete locale e la connessione a Internet non prevede l'uso di un server proxy o di una firewall, si raccomanda di non disabilitare la scansione degli archivi allegati e di non impostare una limitazione temporale alla scansione.

Se invece si lavora in un ambiente protetto, è possibile modificare le limitazioni temporali alla scansione in modo da incrementare la velocità.

Figura 26. Impostazioni di Mail Anti-Virus

È possibile configurare anche le condizioni di filtraggio degli oggetti allegati a un messaggio nella sezione **Filtro allegati**:

- **Disattiva filtro** – consente di non utilizzare ulteriori filtri per gli allegati.
- **Rinomina tipi di allegati selezionati** – consente di escludere gli allegati di formati specifici e di sostituire l'ultimo carattere del nome di un file con un trattino di sottolineatura. Per selezionare il tipo di file, fare clic sul pulsante **Tipi di file**.
- **Elimina tipi di allegati selezionati** – consente di escludere ed eliminare gli allegati di formati specifici. Per selezionare il tipo di file, fare clic sul pulsante **Tipi di file**.

Per ulteriori informazioni sui tipi di allegati filtrati, consultare la sezione A.1 a pag. 229.

L'uso del filtro rappresenta un'ulteriore sicurezza per il computer, poiché nella maggior parte dei casi i programmi nocivi si diffondono attraverso la posta in forma di allegati. Rinominando o eliminando determinati tipi di allegati, si previene l'apertura automatica degli allegati all'arrivo di un messaggio e si evitano altri rischi potenziali.

8.2.2. Configurazione dell'elaborazione della posta in Microsoft Office Outlook

Se il client di posta utilizzato è Microsoft Office Outlook, è possibile impostare una configurazione personalizzata delle scansioni antivirus.

Durante l'installazione di Kaspersky Anti-Virus, viene installato in Microsoft Office Outlook uno speciale plug-in in grado di accedere rapidamente alle impostazioni di Mail Anti-Virus e di impostare l'ora di avvio della scansione antivirus dei messaggi.

Il plug-in ha l'aspetto di una scheda di **Mail Anti-Virus** ubicata in **Strumenti** → **Opzioni** (vedi Figura 27).

Selezionare una modalità di scansione della posta:

- **Scansiona alla consegna** – consente di analizzare ogni messaggio nel momento in cui viene consegnato.
- **Scansiona alla lettura** – consente di esaminare i messaggi nel momento in cui vengono aperti.
- **Scansiona all'invio** – consente di eseguire la scansione antivirus dei messaggi in uscita nel momento dell'invio.

Attenzione!

Se si utilizza Microsoft Office Outlook per connettersi al server di posta mediante protocollo IMAP, si raccomanda di non utilizzare la modalità **Scansiona alla consegna**. Se si abilita questa modalità, i messaggi di posta elettronica vengono copiati sul computer locale alla consegna al server, perdendo di conseguenza il vantaggio principale del protocollo IMAP, cioè la riduzione del traffico e la gestione della posta indesiderata direttamente sul server senza copiarla sul computer dell'utente.

L'azione da eseguire sugli oggetti di posta pericolosi è definita tra le impostazioni di Mail Anti-Virus. Per configurarle, fare clic su clicca qui nella sezione **Stato**.

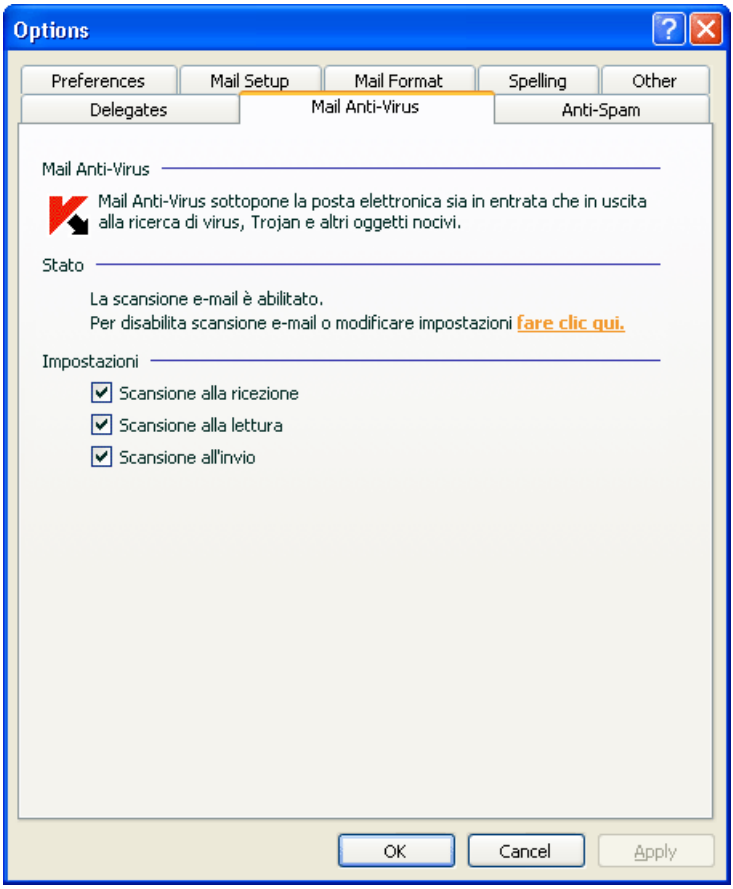


Figura 27. Configurazione delle impostazioni di Mail Anti-Virus in MS Outlook

8.2.3. Configurazione delle scansioni di posta in The Bat!

Le azioni da eseguire sugli oggetti di posta infetti in The Bat! sono definite per mezzo degli strumenti del programma.

> **Attenzione!**
>
> Le impostazioni di Mail Anti-Virus che determinano se esaminare i messaggi in arrivo e in uscita, nonché le azioni da eseguire sugli oggetti di posta pericolosi e le esclusioni, sono ignorate. Gli unici elementi di cui The Bat! tiene conto sono la scansione degli archivi allegati e le limitazioni temporali della scansione dei messaggi (vedi 8.2.1 a pag. 97).

Per impostare le regole di protezione della posta in The Bat!:

1. Selezionare **Impostazioni** dal menu **Proprietà** del programma di posta.
2. Selezionare **Protezione virus** dalla struttura ad albero delle impostazioni.

Le impostazioni di protezione visualizzate (vedi Figura 27) valgono per tutti i moduli antivirus installati nel computer che supportano The Bat!.

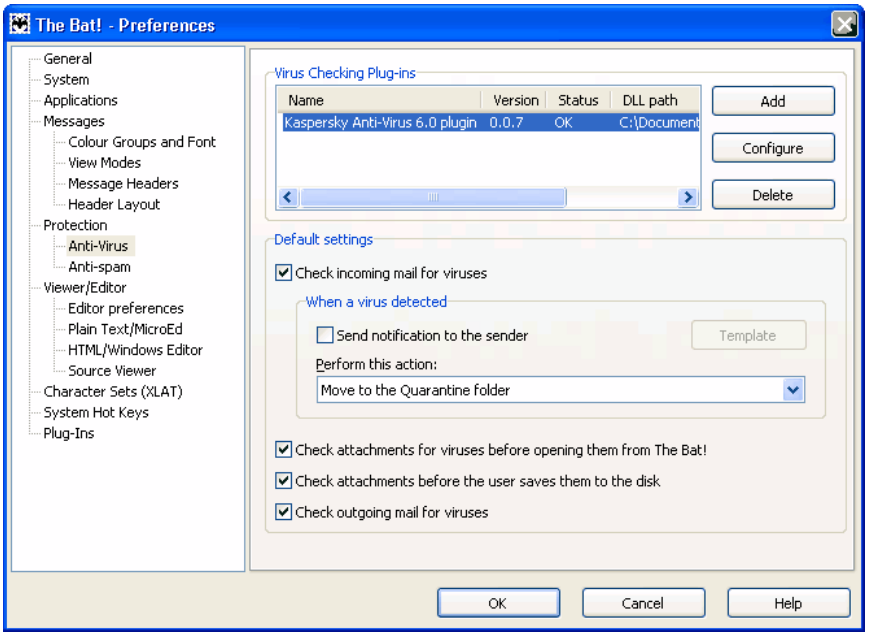


Figura 28. Configurazione delle scansioni di posta in The Bat!

A questo punto occorre stabilire:

- Quali gruppi di messaggi saranno sottoposti alla scansione antivirus (in arrivo, in uscita)
- In quale momento saranno gli oggetti di posta saranno sottoposti alla scansione antivirus (all'apertura del messaggio o prima di salvarlo sul disco)
- Le azioni da eseguire in caso di intercettazione di oggetti pericolosi nei messaggi. Per esempio, è possibile selezionare:

  Prova a curare le parti infettate – consente di riparare l'oggetto di posta infetto; se la riparazione non riesce, l'oggetto resta nel messaggio. Kaspersky Anti-Virus informa sempre l'utente ogni volta che viene individuato un messaggio infetto. Ma anche selezionando **Elimina** nella finestra degli avvisi di Mail Anti-Virus, l'oggetto rimane nel messaggio poiché l'azione selezionata in The Bat! ha la precedenza su quelle di Mail Anti-Virus.

  Rimuovi le parti infettate – consente di eliminare l'oggetto pericoloso dal messaggio, sia esso effettivamente infetto o solo sospettato di esserlo.

Per impostazione predefinita, The Bat! trasferisce tutti gli oggetti di posta infetti nella cartella Quarantena senza ripararli.

Attenzione!

The Bat! non evidenzia con intestazioni speciali i messaggi contenenti oggetti pericolosi.

8.2.4. Utilizzo dell'analisi euristica

I metodo euristici vengono utilizzati da numerosi componenti di protezione in tempo reale ed azioni di scansione virus (vedi 7.2.4 a pag. 88 per maggiori dettagli).

Figura 29. Uso Analizzatore euristico

I metodi euristici di riconoscimento di nuove minacce possono essere abilitati/disabilitati per il componente Mail Anti-Virus utilizzando il tasto **Analizzatore Euristico**. Occorre seguire i seguenti passaggi:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Mail Anti-Virus** sotto **Protezione**.

2. Clicca il pulsante **Personalizza** nell'area **Livello di sicurezza** (vedi Figura 25).
3. Seleziona il tasto **Analizzatore Euristico** nella finestra di dialogo (vedi Figura 29).

Per utilizzare il metodo euristico spunta k **Usa Analizzatore euristico.** Inoltre la risoluzione della scansione può essere selezionata muovendo il cursore su una delle seguenti opzioni: **Basso, Medio, Dettagliato**.

8.2.5. Ripristino delle impostazioni predefinite di Mail Anti-Virus

Durante la configurazione di Mail Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di protezione **Consigliato**.

Per ripristinare le impostazioni predefinite di Mail Anti-Virus:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Mail Anti-Virus** sotto **Protezione**.
2. Clicca sul pulsante **Predefinito** sotto **Livello di sicurezza** (vedi Figura 25.

8.2.6. Selezione delle azioni da eseguire sugli oggetti di posta pericolosi

Se una scansione della posta evidenzia messaggi o parti di messaggio (intestazione, corpo, allegati) infetti o sospetti, le operazioni successive di Mail Anti-Virus dipendono dallo stato dell'oggetto e dall'azione selezionata.

Dopo la scansione, agli oggetti di posta possono essere associati i seguenti stati:

- Stato di programma nocivo (per esempio, *virus, trojan*; per ulteriori informazioni, vedi 1.3 a pag. 12).
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il codice del file contiene una sezione che sembra essere la variante di un virus noto o ricorda la struttura di una sequenza virale.

Per impostazione predefinita, quando Mail Anti-Virus rileva un oggetto pericoloso o potenzialmente infetto, visualizza un avviso e invita l'utente di selezionare un'azione.

Per modificare un'azione da applicare a un oggetto:

Aprire la finestra delle impostazioni di Kaspersky Anti-Virus e selezionare la sezione **Mail Anti-Virus** sotto **Protezione**. Tutte le azioni possibili per gli oggetti pericolosi sono elencate nella casella **Azione** (vedi Figura 30).

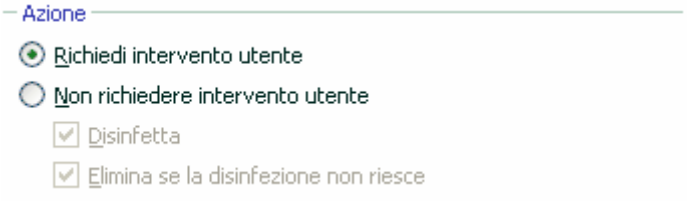


Figura 30. Selezione delle azioni da eseguire sugli oggetti di posta pericolosi

Osserviamo adesso in dettaglio le possibili opzioni di trattamento degli oggetti di posta pericolosi.

Se l'azione selezionata era	**Quando viene rilevato un oggetto pericoloso**
Richiedi intervento utente	Mail Anti-Virus visualizza un avviso con informazioni sul programma nocivo che ha infettato *probabilmente il file e offre l'opzione di una delle seguenti azioni.
Non richiedere intervento utente	Mail Anti-Virus non elabora l'oggetto. Le informazioni relative all'evento vengono registrate nel report (vedi 15.3 a pag. 176). In un secondo momento sarà possibile tentare di riparare l'oggetto.
Non richiedere intervento utente **Disinfetta**	• E-Mail Anti-Virus bloccherà l'accesso all'oggetto e cercherà di disinfettarlo. Se l'operazione ha successo esso viene ripristinato per un regolare uso. Altrimenti è spostato in Quarantena. Queste informazioni saranno riportate in un report. In seguito potrai provare a disinfettare l'oggetto.

Non richiedere intervento utente ☑ **Disinfetta** ☑ **Elimina se la disinfezione non riesce**[2]	• E-Mail Anti-Virus bloccherà l'accesso all'oggetto e cercherà di disinfettarlo. Se l'operazione ha successo esso viene ripristinato per un regolare uso. Altrimenti esso viene eliminato. Una copia dell'oggetto verrà archiviata nel Backup. • Oggetti con lo stato di potenzialmente infetto verranno spostati in Quarantena
Non richiedere intervento utente ☑ **Elimina**	Quando E-Mail Anti-Virus individua un oggetto infetto o potenzialmente infetto, lo elimina senza informare l'utente.

Nella disinfezione o cancellazione di un oggetto Kaspersky Anti-Virus crea una copia di backup (vedi 15.2 a pag. 174) prima di cercare di riparare o cancellare l'oggetto. per permettere che venga ripristinato in caso di necessità o qualora sorgesse una opportunità per pulirlo.

[2] Se si usa The Bat! Come client di posta, gli oggetti di posta pericolosi saranno disinfettati o eliminati quando Mail Anti-Virus intraprende questa azione (in funzione dell'azione selezionata in The Bat!).

CAPITOLO 9. WEB ANTI-VIRUS

Ogni volta che si usa Internet, si espongono le informazioni custodite nel computer al rischio di infezione da parte di programmi pericolosi. Questi possono essere caricati nel computer aprendo un determinato sito web o leggendo un articolo su Internet.

Kaspersky Anti-Virus include uno speciale componente per la protezione del computer durante la navigazione su Internet: Web Anti-Virus. Esso protegge le informazioni che entrano nel computer attraverso il protocollo HTTP e impedisce il caricamento di script pericolosi sul computer.

Attenzione!

Web Anti-Virus controlla solo il traffico HTTP che passa attraverso le porte elencate nell'elenco delle porte monitorate (vedi 15.4 a pag. 184). Il pacchetto del programma include un elenco delle porte più comunemente utilizzate per la trasmissione della posta e del traffico HTTP. Se si utilizzano porte non presenti in questo elenco è necessario aggiungerle al fine di proteggere il traffico che passa attraverso di esse.

Se si lavora in uno network non protetto si raccomanda di utilizzare Web Anti-Virus per proteggere il computer durante l'uso di Internet. Se il computer è collegato a una rete protetta da firewall o da filtri per il traffico HTTP, Web Anti-Virus offre un'ulteriore protezione durante la navigazione sul Web.

L'indicatore di funzionamento del componente è l'icona della barra delle applicazioni di Kaspersky Anti-Virus, che durante la scansione di uno script assume questo aspetto  .

Osserviamo in dettaglio il funzionamento del componente.

Web Anti-Virus si compone di due moduli che gestiscono:

- *Scansione traffico* – scansione degli oggetti che entrano nel computer mediante HTTP.
- *Scansione script* – scansione di tutti gli script processati in Microsoft Internet Explorer come pure gli script WSH (JavaScript, Visual Basic Script, ecc) caricati durante l'uso del computer .
- È presente inoltre uno speciale plug-in per Microsoft Internet Explorer che viene installato con Kaspersky Anti-Virus. L'icona  nella barra dei pulsanti standard del browser significa che esso è installato. Facendo clic sull'icona, si apre una finestra contenente le statistiche di Web Anti-Virus sul numero di script esaminati e bloccati.

Web Anti-Virus monitora il traffico HTTP con le seguenti modalità:

1. Ogni pagina web o file accessibile all'utente o a un determinato programma via HTTP viene intercettata e analizzata da Web Anti-Virus per escludere la presenza di codici nocivi. Gli oggetti nocivi vengono individuati per mezzo degli *elenchi delle minacce* inclusi in Kaspersky Anti-Virus e con l'algoritmo euristico. I database contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nei database.
2. Dopo l'analisi è possibile agire come segue:
   - Se una pagina web o un oggetto a cui l'utente sta cercando di accedere contengono un codice nocivo, l'accesso ad essi viene bloccato. Viene quindi visualizzato un messaggio che informa che l'oggetto o la pagina è infetta.
   - Se il file o la pagina web non contengono codici nocivi, essa è immediatamente accessibili all'utente.

Gli script vengono esaminati secondo il seguente algoritmo:

1. Web Anti-Virus intercetta ogni script eseguito in una pagina web e lo esamina per escludere la presenza di codici nocivi.
2. Se uno script contiene un codice nocivo, Web Anti-Virus lo blocca e informa l'utente con un avviso a comparsa.
3. Se nello script non viene rilevato alcun codice nocivo, esso viene eseguito.

Attenzione!

Per intercettare e sottoporre il traffico e gli script http a scansione anti-virus, Web Anti-Virus deve essere in esecuzione prima che venga stabilita una connessione con una risorsa web. In caso contrario, il traffico non sarà sottoposto a scansione.

9.1. Selezione del livello di protezione web

Kaspersky Anti-Virus protegge il computer durante la navigazione in Internet in base a uno dei seguenti livelli (vedi Figura 31):

Protezione massima – il livello che garantisce il monitoraggio più approfondito di script e oggetti in arrivo via HTTP. Il programma esegue

un'accurata scansione di tutti gli oggetti utilizzando l'intero set di database dell'applicazione. Questo livello di protezione è consigliato per gli ambienti aggressivi in cui non si utilizzano altri strumenti di sicurezza HTTP.

Consigliato. È il livello consigliato dagli esperti Kaspersky Lab. Questo livello esamina gli stessi oggetti del livello **Protezione massima**, ma riduce il tempo di cattura dei frammenti di file, accelerando la scansione e rendendo disponibili gli oggetti più rapidamente.

Alta velocità – è un livello di protezione le cui impostazioni consentono di utilizzare applicazioni che assorbono risorse considerevoli, grazie alla restrizione dell'ambito della scansione ottenuta utilizzando un elenco di minacce limitato. Questo livello è consigliato se nel computer sono installate altre applicazioni di protezione web.

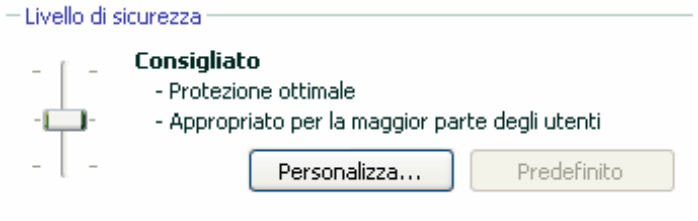


Figura 31. Selezione di un livello di sicurezza web

Per impostazione predefinita, il livello di sicurezza è impostato su **Consigliato**.

È possibile aumentare o ridurre il livello di sicurezza selezionando quello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Modificando il livello di sicurezza, si definisce il rapporto tra la velocità di scansione e il numero totale di oggetti esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di oggetti esaminati.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile crearne uno personalizzato. Raccomandiamo di selezionare il livello il più vicino alle tue necessità e modificarne i parametri. Il nome del livello di protezione verrà cambiato in personalizzato. Osserviamo un esempio in cui le impostazioni predefinite del livello di protezione devono venire modificate.

Esempio:

Il computer dell'utente si connette a Internet via modem. Non è connesso a una LAN aziendale e non è protetto da alcuna misura antivirus per il traffico HTTP in entrata.

A causa della natura stessa del suo lavoro, l'utente scarica regolarmente file di grandi dimensioni da Internet. La scansione di file di questo genere, di norma, richiede tempi piuttosto lenti.

Come assicuri una ottimale protezione del computer contro le infezioni trasmesse con il traffico HTTP o gli script?

Suggerimento per selezionare un livello:

Da queste informazioni basilari, possiamo concludere che il computer lavora in un ambiente sensibile e che il rischio di contrarre infezioni attraverso il traffico HTTP è elevato (nessuna protezione web centralizzata, metodo di connessione a Internet).

Il livello di protezione consigliato è quindi **Protezione massima**, apportando le seguenti modifiche: Si raccomanda di ridurre il tempo di caching dei frammenti di file durante la scansione.

Per modificare un livello di protezione predefinito:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Web Anti-Virus** sotto **Protezione**.
2. Clicca su **Personalizza** sotto **Livello di sicurezza** (vedi Figura 31).
3. Modifica i parametri di protezione del browser nella risultante finestra e clicca **OK**.

9.2. Configurazione di Web Anti-Virus

Web Anti-Virus esamina tutti gli oggetti caricati nel computer tramite HTTP e monitora tutti gli script WSH (JavaScript o Visual Basic Script etc.) che vengono avviati.

Per accelerare la velocità del componente è possibile configurare alcune impostazioni, in particolare:

- Impostare l'algoritmo di scansione selezionando un set completo o limitato di database dell'applicazione (vedi 9.2.1 a pag. 111).
- Creare un elenco di indirizzi web attendibili (vedi 9.2.2 a pag. 112).
- Abilita/Disabilita l'analisi euristica (vedi 9.2.3 a pag. 113).

Inoltre è possibile selezionare le azioni che Web Anti-Virus eseguirà ogni volta che rileva oggetti HTTP pericolosi.

La presente sezione prende in esame queste impostazioni.

9.2.1. Impostazioni generali di scansione

Per aumentare il livello di rilevamento di codici nocivi, Web Anti-Virus ripone nella memoria cache frammenti degli oggetti scaricati da Internet. Quando utilizza questo metodo, Web Anti-Virus scansiona un oggetto solo dopo averlo scaricato completamente. L'oggetto viene quindi sottoposto ad analisi anti-virus e, in base al risultato di scansione, il programma rimette l'oggetto a disposizione dell'utente oppure lo blocca.

Tuttavia, l'utilizzo della cache aumenta il tempo di elaborazione degli oggetti e il tempo entro il quale questi tornano disponibili all'utente; inoltre, possono verificarsi problemi durante le azioni di copia ed elaborazione di oggetti pesanti a causa del timeout della connessione del client con l'http.

Si consiglia pertanto di limitare il tempo di cache per i frammenti di oggetti web scaricati da Internet per risolvere questo problema. Allo scadere di questo intervallo di tempo, l'utente potrà disporre della parte scaricata del file che però non sarà sottoposto a scansione; la scansione avverrà infatti solo quando l'oggetto sarà stato completamente copiato. Questo rende disponibile l'oggetto in minor tempo e risolve il problema di interruzione della connessione senza tuttavia ridurre il livello di sicurezza durante la navigazione in Internet.

Come impostazione predefinita, il tempo di cache per I frammenti è limitato a un secondo. Aumentando questo valore o deselezionando il limite di tempo di cache si ottengono migliori scansioni anti-virus, ma si rallenta la consegna dell'oggetto all'utente.

Per limitare il tempo di cache per i frammenti di file o rimuovere il limite:

1. Apri la finestra delle impostazioni dell'applicazione e seleziona **Web Anti-Virus** sotto **Protezione**.
2. Fai clic su **Personalizza** nell'area **Livello di sicurezza** (vedi Figura 31).
3. Nella finestra che si apre (vedi Figura 32), seleziona l'opzione desiderata nella finestra **Impostazioni di scansione**.

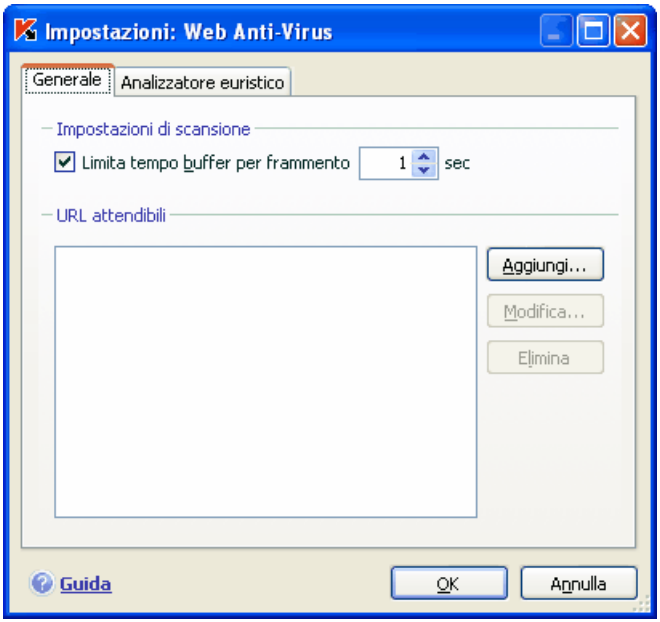


Figura 32. Selezione del livello di sicurezza sul web

9.2.2. Creazione di un elenco di indirizzi attendibili

È possibile creare un elenco di indirizzi i cui contenuti sono ritenuti attendibili. Web Anti-Virus non analizzerà i dati provenienti da quegli indirizzi. Questa opzione può essere utilizzata nei casi in cui Web Anti-Virus interferisce con il

normale uso di Internet, per esempio durante lo scaricamento di un file specifico che viene bloccato da Web Anti-Virus ogni volta che si tenta di scaricarlo.

Per creare un elenco degli indirizzi attendibili:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Web Anti-Virus** sotto **Protezione**.
2. Clicca sul pulsante **Personalizza** sotto **Livello di sicurezza** (vedi Figura 31).
3. Nella finestra che si apre (vedi Figura 32), creare un elenco dei server attendibili nella sezione **URL attendibili**. A questo scopo utilizzare i pulsanti a destra dell'elenco.

Al momento di digitare un indirizzo attendibile, è possibile creare delle maschere con i seguenti caratteri jolly:

***** – qualsiasi combinazione di caratteri.

Esempio: Se si è creata la maschera ***abc***, non verrà esaminata alcuna URL contenente la sequenza **abc**. Ad esempio: www.virus.com/download_virus/page_0-9abcdef.html

? – qualsiasi carattere singolo.

Esempio: Se si è creata la maschera **Patch_123?.com**, le URL contenenti la sequenza indicata seguita da qualsiasi carattere in sostituzione del punto interrogativo non saranno esaminate. Ad esempio: **Patch_1235.com** Tuttavia l'URL **patch_12355.com** sarà esaminata.

Se i caratteri * o ? fanno effettivamente parte dell'URL da aggiungere all'elenco, digitare una barra inversa per ignorare il carattere * o ? che segue.

Esempio: Si desidera aggiungere questa URL all'elenco degli indirizzi attendibili: www.virus.com/download_virus/virus.dll?virus_name=

Per evitare che Kaspersky Anti-Virus consideri il **?** come un carattere jolly, è necessario farlo precedere da una barra inversa (\ ). Di conseguenza, l'URL aggiunta all'elenco delle esclusioni sarà come segue: www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Utilizzo dell'analizzatore euristico

I metodi euristici vengono utilizzati da numerosi componenti di protezione in tempo reale ed azioni di scansione virus (vedi 7.2.4 a pag. 88).

I metodi euristici di riconoscimento di nuove minacce possono essere abilitati/disabilitati per il componente Mail Anti-Virus dalla scheda **Analizzatore euristico**. Occorre seguire i seguenti passaggi:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Web Anti-Virus** sotto **Protezione**.
2. Clicca il pulsante **Personalizza** nell'area **Livello di sicurezza**.
3. Seleziona la scheda **Analizzatore euristico** nella finestra di dialogo che si apre (vedi Figura 33).

Per utilizzare il metodo euristico spunta **Usa analizzatore euristico.** Inoltre la risoluzione della scansione può essere selezionata muovendo il cursore su una delle seguenti opzioni: **Basso, Medio** o **Dettagliato**.

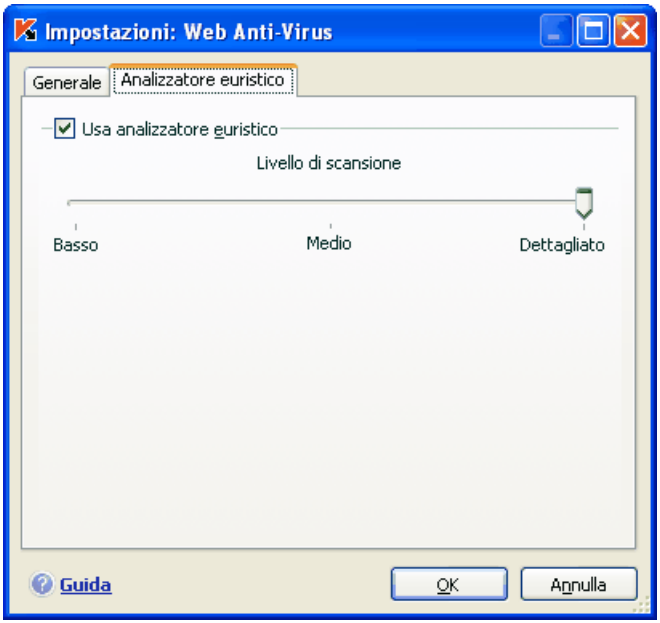


Figura 33. Utilizzo dell'analisi euristica

9.2.4. Ripristino delle impostazioni predefinite di Web Anti-Virus

Durante la configurazione di Web Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni di default che Kaspersky Lab considera ottimali e che ha riunito nel livello di sicurezza **Consigliato**.

Per ripristinare le impostazioni predefinite di Web Anti-Virus:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Web Anti-Virus** sotto **Protezione**.
2. Fai clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza** (vedi Figura 31).

9.2.5. Selezione delle azioni da compiere in caso di oggetti pericolosi

Se l'analisi di un oggetto HTTP evidenzia la presenza di un codice nocivo, la reazione di Web Anti-Virus dipende dall'azione selezionata dall'utente.

Per configurare le reazioni di Web Anti-Virus in presenza di un oggetto pericoloso:

apri la finestra delle impostazioni dell'applicazione e seleziona la sezione **Web Anti-Virus** sotto **Protezione**. Tutte le azioni possibili per gli oggetti pericolosi sono elencate nella sezione **Azione** (vedi Figura 34).

Per impostazione predefinita, in presenza di un oggetto HTTP pericoloso Web Anti-Virus visualizza un avviso e propone una scelta di azioni da eseguire sull'oggetto.

Figura 34. Selezione di azioni da eseguire su script pericolosi

Le possibili opzioni di trattamento degli oggetti HTTP pericolosi sono le seguenti:

Se l'azione selezionata era	Se viene intercettato un oggetto pericoloso nel traffico HTTP
Richiedi intervento utente	Web Anti-Virus visualizza un avviso contenente informazioni sul codice nocivo che potrebbe aver infettato l'oggetto e offre una serie di opzioni.
Blocca	Web Anti-Virus blocca l'accesso all'oggetto e visualizza un avviso in merito. Le informazioni relative all'evento vengono registrate nel report (vedi 15.3 a pag. 176).
Consenti	Web Anti-Virus consente l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel report.

Per quanto riguarda gli script pericolosi, Web Anti-Virus li blocca sempre e visualizza messaggi che avvisano l'utente dell'azione eseguita. Non è possibile modificare la reazione a uno script pericoloso; l'unica alternativa consiste nel disabilitare il modulo di scansione degli script.

CAPITOLO 10. DIFESA PROATTIVA

Attenzione!

In questa versione dell'applicazione non c'è il componente di **Controllo Integrità Applicazione** sui computer che eseguono Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64.

Kaspersky Anti-Virus protegge sia dalle minacce note sia da quelle sulle quali non si possiedono ancora informazioni nei database dell'applicazione. Questa protezione è garantita da un componente appositamente sviluppato, *Difesa proattiva.*

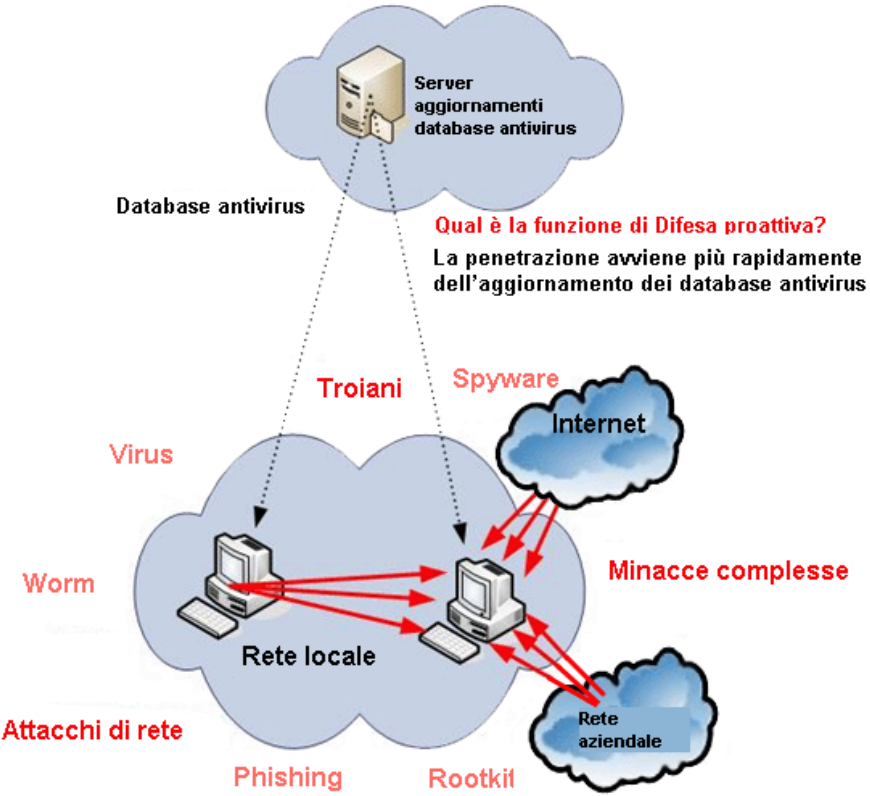
La necessità di un componente come Difesa proattiva si è fatta più pressante man mano che i programmi nocivi hanno iniziato a diffondersi più rapidamente degli aggiornamenti antivirus necessari per neutralizzarli. La tecnica di reazione sulla quale si basano le difese antivirus tradizionali richiede che almeno un computer sia infettato dalla nuova minaccia e comporta il dispendio temporale necessario per analizzare il codice nocivo e aggiungerlo al database dell'applicazione e aggiornare il database dei computer degli utenti. A quel punto è possibile che la nuova minaccia abbia già provocato danni notevoli.

Le tecnologie preventive fornite da Difesa proattiva di Kaspersky Anti-Virus sono in grado di evitare perdite di tempo e neutralizzare le nuove minacce prima che possano danneggiare il computer. Come è possibile? Contrariamente alle tecnologie reattive che analizzano i codici usando un database dell'applicazione, le tecnologie preventive riconoscono una nuova minaccia nel computer in base alle sequenze di azioni eseguite da una determinata applicazione o processo. L'installazione del programma include una serie di criteri in grado di identificare il livello di pericolosità delle attività di un programma o di un altro. Se l'analisi dell'attività mostra che le azioni di un certo programma sono sospette Kaspersky Anti-Virus eseguirà l'azione assegnata dalla regola per quello specifico tipo.

Il set totale delle azioni del programma determina la pericolosità dell'attività. Ad esempio quando l'azione rileva che un programma copia se stesso sulle risorse del network, nella cartella di avvio o nel registro di sistema e poi invia copie di se stesso è molto probabile che questo programma sia un worm. Ambienti pericolosi includono anche:

- Modifiche al file system
- Moduli che vengono incorporati in altri processi

- Processi di mascheratura nel sistema
- Modifiche alle chiavi del registro di sistema di Microsoft Window



Difesa Proattiva intercetta e blocca tutte le operazioni pericolose usando il set di regole insieme ad un elenco di applicazioni escluse.

In funzione, Difesa proattiva applica una serie di regole incluse nel programma come pure regole create dall'utente durante l'uso del programma. Una *regola* è un insieme di criteri che definiscono un set di ambienti sospetti e le reazioni ad esse di Kaspersky Anti-Virus.

Esistono regole individuali per l'attività dell'applicazione e per il monitoraggio delle modifiche al registro di sistema, e dei processi avviati sul computer. Puoi modificare le regole a tua discrezione aggiungendone o eliminando e modificando quelle esistenti. Le regole possono bloccare azioni o concedere autorizzazioni.

Esaminiamo gli algoritmi di Difesa proattiva:

1. Subito dopo l'avvio del computer, Difesa proattiva analizza i seguenti fattori, usando il set di regole ed esclusioni:

   - *Azioni di ogni applicazione in esecuzione sul computer*. Difesa proattiva registra una cronologia delle azioni eseguite in sequenza e la confronta alle sequenze caratteristiche delle attività pericoloso (con il programma è fornito un database dei tipi di attività pericolose che viene aggiornato con i database dell'applicazione).

   - *Integrità dei moduli di programma* dei programmi installati nel computer, che aiuta a impedire la sostituzione dei moduli delle applicazione a causa di codici maligni in essi introdotti.

   - *Ogni tentativo di modificare il registro di sistema* eliminando o aggiungendo chiavi del registro di sistema, assegnando strani valori alle chiavi in un formato non ammesso che ne impedisce la vista o la modifica etc.

2. L'analisi applica le regole di blocco e di permesso della Difesa proattiva.

3. Dopo l'analisi sono disponibili le seguenti possibili azioni:

   - Se l'attività soddisfa le condizioni delle regole di permesso della Difesa proattiva e non incontra alcuna regola di blocca, non viene bloccata.

   - Se le regole di blocco corrispondono all'attività, le azioni successive eseguite dal computer corrisponderanno alle istruzioni specificate nelle regole. Tali attività vengono solitamente bloccate. Sul video viene visualizzato un messaggio che specifica l'applicazione, il tipo di attività svolta dalla stessa e una cronologia delle azioni eseguite. L'utente deve accettare la decisione, bloccare o consentire questa attività. Puoi inoltre creare una regola per tale attività e annullare l' azioni eseguite nel sistema.

Le categorie di impostazioni (vedi Figura 35) per il componente Difesa Proattiva sono le seguenti:

- Se l'attività dell'applicazione è monitorata sul computer

  Questa modalità di Difesa proattiva è abilitata spuntando ☑ **Abilita Analisi attività applicazione**. Per impostazione l'analizzatore è abilitato, garantendo un attento monitoraggio delle azioni di qualsiasi programma aperto sul computer. È specificato un elenco di attività pericolose. Puoi configurare l'ordine con cui le applicazioni vengono processate per quella attività. Inoltre è possibile creare esclusioni di Difesa proattiva che escludono dal monitoraggio l'attività di applicazioni selezionate.

- Se il controllo dell'integrità dell'applicazione è abilitato

  Questa funzione tiene sotto controllo l'integrità dei moduli delle applicazioni installate sul computer e viene abilitata selezionando la casella **Abilita Controllo integrità applicazione**. L'integrità viene tracciata grazie al monitoraggio dei risultati dei moduli dell'applicazione e dell'applicazione stessa. Puoi creare regole (vedi 10.1 a pag. 121) per il monitoraggio dell'integrità dei moduli da qualsiasi applicazione. Per fare questo aggiungi quella applicazione all'elenco delle applicazioni che devono essere monitorate.

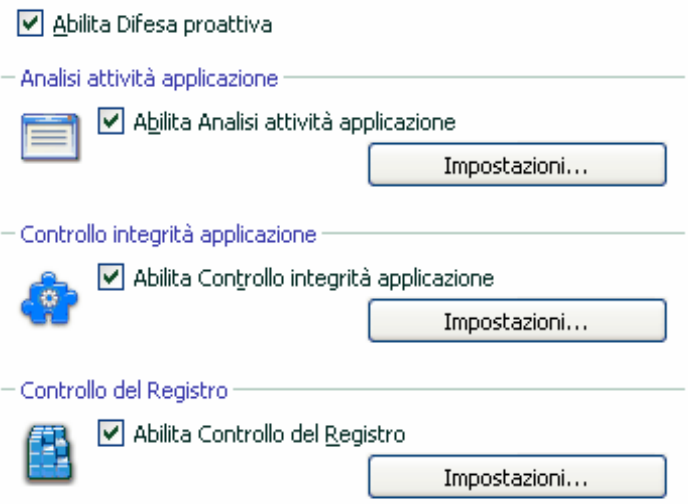


Figura 35. Impostazioni di Difesa proattiva

Questo componente di Difesa Proattiva non è disponibile per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64.

- Se le modifiche al registro di sistema vengono monitorate

  Per impostazione predefinita, l'opzione **Abilita Controllo del registro** è selezionata, consentendo a Kaspersky Anti-Virus di analizzare approfonditamente qualsiasi tentativo di modificare le chiavi di registro del sistema di Microsoft Windows.

  Puoi creare tue proprie regole (vedi 10.3.2 a pag. 132) per monitorare il registro, in base alla chiave di registro.

È possibile inoltre configurare esclusioni (vedi 6.9.1 a pag. 69) per i moduli di Difesa proattiva e creare un elenco delle applicazioni attendibili (vedi 6.9.2 a pag. 74).

Le sezioni successive prendono in esame questi aspetti in maggior dettaglio.

10.1. Regole di monitoraggio della attività

Nota che la configurazione di controllo dell'applicazione per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64 è differente dal processo di configurazione per altri sistemi operativi.

Informazioni riguardo la configurazione di controllo dell'attività per questi sistemi operativi è fornita alla fine della sezione.

Kaspersky Anti-Virus monitora tutte le applicazioni presenti sul computer. L'applicazione incorpora un set di descrizione eventi che possono essere riconosciuti come pericolosi. Una regola di monitoraggio per ciascun di questi eventi è stata creata. Se l'attività di una certa applicazione viene classificata come evento pericoloso la Difesa Proattiva aderirà strettamente alla regola prevista da quell'evento.

Se vuoi monitorare l'attività delle applicazioni spunta la casella **Abilita Analisi attività applicazione**.

Osserviamo alcuni tipi di eventi che accadono nel sistema quando l'applicazione li riconosce come sospetti:

- *Comportamento pericoloso*. Kaspersky Anti-Virus analizza l'attività delle applicazioni installate sul computer, e rileva le azioni pericolose o sospette da parte dei programmi in base alle regole create da Kaspersky Lab. Tali azioni includono, per esempio, l'installazione dissimulata di un programma, o i programmi che si replicano.
- *Avvio del browser Internet con parametri*. Analizzando questo tipo di attività puoi riconoscere i tentativi di aprire un browser con impostazioni. Questa attività è tipica dell'apertura di un browser Web da parte di un'applicazione con certe impostazioni del prompt di comando: ad esempio quando clicchi su un link ad alcuni URL in un messaggio di posta pubblicitario.
- *Intrusione nel processo (invasori)*. Consiste nell'aggiungere codice eseguibile o un flusso supplementare al processo di un determinato programma. Questa attività è tipica dei Trojan.

- *Rilevamento rootkit*. I rootkit sono un insieme di programmi utilizzati per nascondere i programmi nocivi ed i loro processi nel sistema. Kaspersky Anti-Virus analizza il sistema operativo alla ricerca di processi nascosti.
- *Hook della finestra*. È un'attività utilizzata nei tentativi di lettura di password ed altre informazioni riservate visualizzate nelle finestre di dialogo del sistema operativo. Kaspersky Anti-Virus identifica tali attività, in caso di tentativi di intercettare i dati trasferiti dal sistema operativo alla finestra di dialogo.
- *Valori sospetti nel registro*. Il registro di sistema è un database che conserva le impostazioni di sistema e dell'utente per controllare il funzionamento di Microsoft Windows, come anche qualsiasi utility stabilita sul computer. I programmi nocivi, cercando di nascondere la loro presenza nel sistema, copiano valori errati nelle chiavi di registro. Kaspersky Anti-Virus analizza le voci del registro di sistema alla ricerca di valori sospetti.
- *Attività di sistema sospetta*. Il programma analizza le azioni eseguite dal sistema operativo di Microsoft Windows e riconosce le attività sospette. Un esempio di attività sospetta potrebbe essere un varco nell'integrità che modifica uno o più moduli nell'applicazione monitorata rispetto al suo ultimo lancio.
- *Rilevamento Keylogger*. È un'attività utilizzata dai programmi nocivi per tentare di leggere password ed altre informazioni riservate digitate per mezzo della tastiera.

L'elenco delle attività pericolose viene aggiornato automaticamente durante l'aggiornamento di Kaspersky Anti-Virus e non può essere modificato. È possibile:

- Disabilitare il monitoraggio di una o più attività deselezionando la casella ☑ a fianco del nome dell'attività desiderata.
- Modificare la regola utilizzata da Difesa proattiva quando viene intercettata un'attività pericolosa.
- Creare un elenco di esclusioni (vedi 6.9 a pag. 68) includendo le applicazioni che non si considerano pericolose.

Configurazione dell'attività di monitoraggio,

1. Apri la finestra impostazioni dell'applicazione e seleziona **Difesa Proattiva** sotto **Protezione**.
2. Clicca sul pulsante **Impostazioni** nella sezione **Analisi attività applicazione** (vedi Figura 35).

I tipi di attività monitorati da Difesa proattiva sono elencati tra le **Impostazioni: Analisi attività applicazione** (vedi Figura 37).

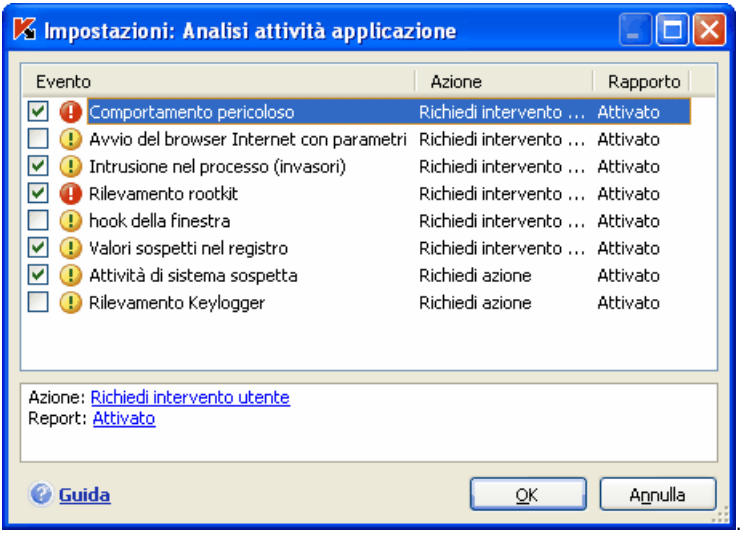


Figura 36. Configurazione del controllo delle attività dell'applicazione

Per modificare una regola di monitoraggio delle attività pericolose, selezionarla dall'elenco e assegnare le impostazioni della regola nella parte inferiore della scheda:

- Assegna la reazione di Difesa proattiva all'attività pericolosa.

  Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: Permetti, richiedi intervento utente e Termina. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata. Oltre a terminare il processo è possibile mettere in Quarantena l'applicazione che avvia l'attività pericolosa. Per fare questo usa i link Attivato / Disattivato. Puoi assegnare un intervallo di tempo con cui definire la frequenza con cui avverrà la scansione per il riconoscimento di processi nascosti nel sistema.

- Stabilire se si desideri generare un report sull'operazione eseguita, cliccando sul link Report fino a quando mostra Attivato o Disattivato come richiesto.

Per disabilitare il monitoraggio di un'attività pericolosa, deselezionare la casella ☑ accanto al nome dell'attività in questione nell'elenco. Difesa proattiva non analizzerà più il tipo di attività deselezionato.

Specifiche di configurazione del controllo attività applicazione in Kaspersky Anti-Virus per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64:

Per i sistemi operativi sopra elencati viene controllato un solo tipo di evento di sistema, *comportamento pericoloso*. Kaspersky Anti-Virus analizza l'attività delle applicazioni installate sul computer e riconosce le attività pericolo o sospette basandosi sull'elenco delle regole creato dagli specialisti di Kaspersky Lab.

Se vuoi che Kaspersky Anti-Virus monitorizzi l'attività dei processi di sistema oltre ai processi dell'utente seleziona la casella ☑ **Controllo account utenti** (vedi Figura 38). Questa opzione è disabilitata per default.

Il sistema di controllo degli account dell'utente accede al sistema ed identifica l'utente ed il suo ambiente operativo impedendo ad altri utenti di danneggiare il sistema operativo o i dati. I processi di sistema sono i processi lanciati dagli account utente di sistema.

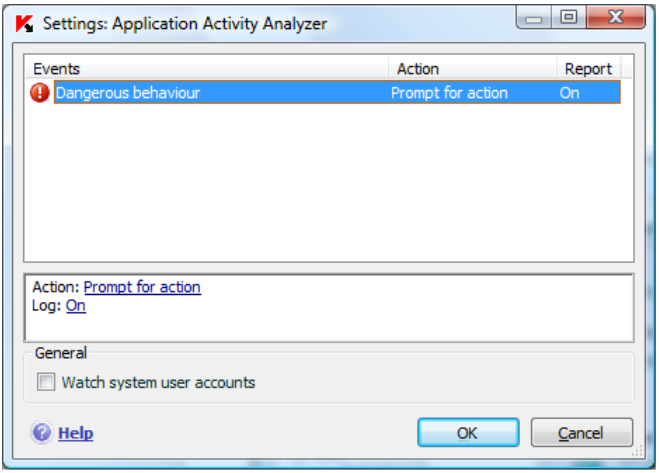


Figura 37. Configurazione del controllo attività applicazioni per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

10.2. Controllo dell'integrità delle applicazioni

Questo componente di Difesa Proattiva non si esegue su Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista e Microsoft Windows Vista x64.

Esistono diversi programmi come browser, posta elettronica etc. che risultano critici per il sistema che potrebbe venir utilizzato da programmi maligni per una diffusione degli stessi. Di norma si tratta di applicazioni e processi di sistema utilizzati per accedere a Internet e per lavorare con la posta elettronica e con altri documenti. È per questo motivo che tali applicazioni sono considerate *critiche* ai fini del controllo delle attività.

Difesa proattiva monitorizza scrupolosamente tali applicazioni ed analizza le loro attività, l'integrità dei moduli di queste applicazioni e osserva gli altri processi avviati dalle stesse applicazioni critiche. Kaspersky Anti-Virus propone un elenco di applicazioni critiche e per ciascuna di esse una regola di monitoraggio per controllare l'attività dell'applicazione. È possibile aggiungere all'elenco altre applicazioni che l'utente considera critiche, e modificare le regole relative alle applicazioni presenti nell'elenco.

Esiste inoltre un elenco di moduli attendibili che possono venir aperti da tutte le applicazioni controllate. Per esempio i moduli firmati digitalmente da Microsoft Corporation. È altamente improbabile che le attività di applicazioni con tali moduli possano essere nocive, pertanto non è necessario monitorarle approfonditamente. Kaspersky Lab ha creato un elenco di questi moduli per alleggerire il carico sul computer durante l'uso di Difesa proattiva.

I componenti con la firma di Microsoft sono aggiunti automaticamente all'elenco delle applicazioni attendibili. Se necessario, è possibile aggiungere o eliminare componenti dall'elenco.

I processi di monitoraggio del sistema possono essere disattivati spuntando la casella **Abilita Controllo integrità applicazione** nella finestra delle impostazioni di Difesa Proattiva: essa è deselezionata per impostazione predefinita. Se si abilita questa funzione, ogni applicazione o modulo di applicazione aperto viene valutato nei confronti con le applicazioni critiche o sicure dell'elenco. Se l'applicazione è presente nell'elenco delle applicazioni critiche, la sua attività sarà sottoposta a monitoraggio da parte di Difesa proattiva in accordo con la regola creata per essa.

Per configurare il controllo dell'integrità delle applicazioni:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Difesa Proattiva** sotto **Protezione**.
2. Clicca sul pulsante **Impostazioni** nella sezione **Controllo integrità applicazione** (vedi Figura 35).

Esaminiamo il funzionamento con i processi critici e attendibili.

10.2.1. Configurazione delle regole di controllo dell'integrità della applicazione

Le *applicazioni critiche* sono file eseguibili di programmi il cui monitoraggio è estremamente importante poiché file maligni usano questi programmi per replicarsi.

La scheda **Applicazioni controllate** (vedi Figura 39) contiene un elenco di applicazioni critiche creato da Kaspersky Lab e incluso nel programma. Per ciascuna di tali applicazioni viene creata una regola di monitoraggio. Tali regole possono essere modificate oppure è possibile crearne di nuove.

Difesa proattiva analizza le seguenti operazioni che coinvolgono applicazioni critiche: esecuzione, modifica dei contenuti dei moduli dell'applicazione e avvio di un'applicazione come processo secondario. È possibile selezionare la reazione di Difesa proattiva a ciascuna delle operazioni elencate (autorizzazione o blocco dell'operazione) e specificare inoltre se registrare l'attività nel report delle operazioni del componente. In pratica, per impostazione predefinita tutte le operazioni critiche possono essere avviate, modificate o avviate come processi secondari.

Per aggiungere un'applicazione critica all'elenco e creare una regola di monitoraggio apposita:

1. Fare clic su **Aggiungi** nella scheda **Applicazioni controllate**. Si apre un menu contestuale. Facendo clic su **Sfoglia** è possibile aprire la finestra di selezione dei file. In alternativa, facendo clic su **Applicazioni** è possibile aprire un elenco delle applicazioni correntemente in funzione e selezionare quelle desiderate. L'applicazione viene aggiunta in cima all'elenco. Per impostazione predefinita viene creata per tale applicazione una regola di autorizzazione. La prima volta che questa applicazione viene avviata, viene creato un elenco dei moduli utilizzati all'avvio del programma, ai quali è altrettanto garantita l'autorizzazione.

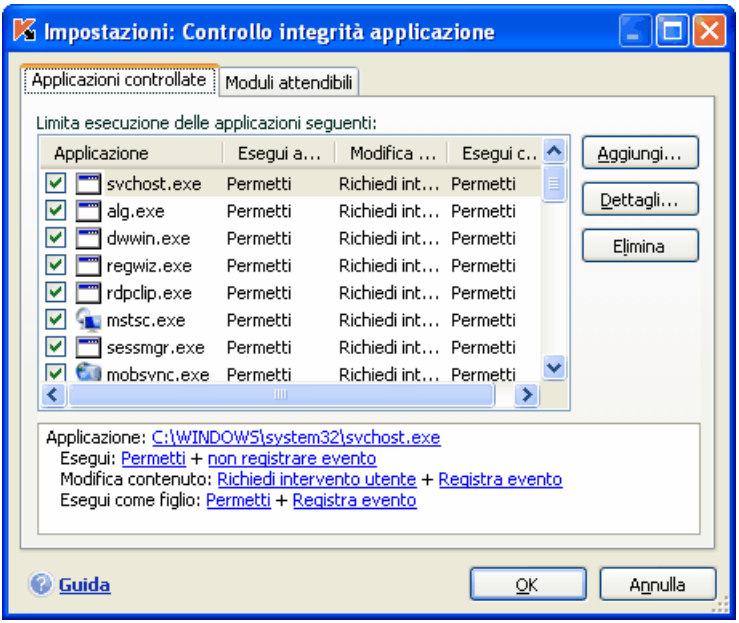


Figura 38. Configurazione di Controllo integrità applicazione

2. Selezionare una regola dall'elenco e assegnare le impostazioni necessarie nella parte inferiore della scheda:

   - Definire la reazione di Difesa proattiva ai tentativi di eseguire una applicazione critica, cambiare l'aspetto o avviarsi come processo secondario.

     Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: Permetti, Richiedi intervento utente e Blocca. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata.

   - Stabilire se si desidera generare un report dell'attività, facendo clic su Registra evento / Non registrare evento.

Per disabilitare il monitoraggio dell'attività di un'applicazione, deselezionare la casella ☑ accanto al nome.

Usa il pulsante **Dettagli…** per vedere un elenco dettagliato dei moduli per l'applicazione selezionata. La finestra **Impostazioni: Moduli Applicazione** contiene un elenco dei moduli the vengono usati quando una applicazione monitorata è avviata e profila l'applicazione stessa. Puoi modificare l'elenco usando i pulsanti **Aggiungi…** ed **Elimina** nella parte destra della finestra.

Puoi anche permettere di caricare o bloccare ogni modulo dell'applicazione controllata. Per impostazione viene creata una regola di permesso per ciascun modulo. Per modificare l'azione seleziona il modulo dall'elenco e clicca il pulsante **Modifica**. Seleziona l'azione desiderata nella finestra che appare.

Nota che Kaspersky Anti-Virus si imposta la prima volta che avvii l'applicazione dopo la sua installazione e fino alla sua chiusura. Il processo di apprendimento produce un elenco dei moduli utilizzati dall'applicazione. Le regole di Controllo Integrità verranno applicate al successivo avvio dell'applicazione.

10.2.2. Creazione di un elenco di componenti comuni

Kaspersky Anti-Virus include un elenco di componenti comuni che possono essere inseriti in tutte le applicazioni controllate. Questo elenco è consultabile nella scheda **Moduli attendibili** (vedi Figura 40). L'elenco contiene i moduli utilizzati da Kaspersky Anti-Virus, i componenti con firma di Microsoft: componenti che possono essere aggiunti o rimossi dall'utente.

Se installi sul computer dei programmi sul computer puoi accertarti che quelli con moduli firmati da Microsoft siano automaticamente aggiunti all'elenco dei moduli attendibili. Per fare ciò seleziona la casella  **Aggiungi automaticamente componenti firmati da Microsoft Corporation a questo elenco**. Poi, se l'applicazione controllata apre un modulo firmato da Microsoft, il programma ne consente automaticamente il caricamento e il modulo viene inserito nell'elenco di componenti condivisi.

Per aggiungere un modulo all'elenco dei moduli attendibili, fare clic su **Aggiungi** e selezionare il modulo nella finestra standard di selezione file.

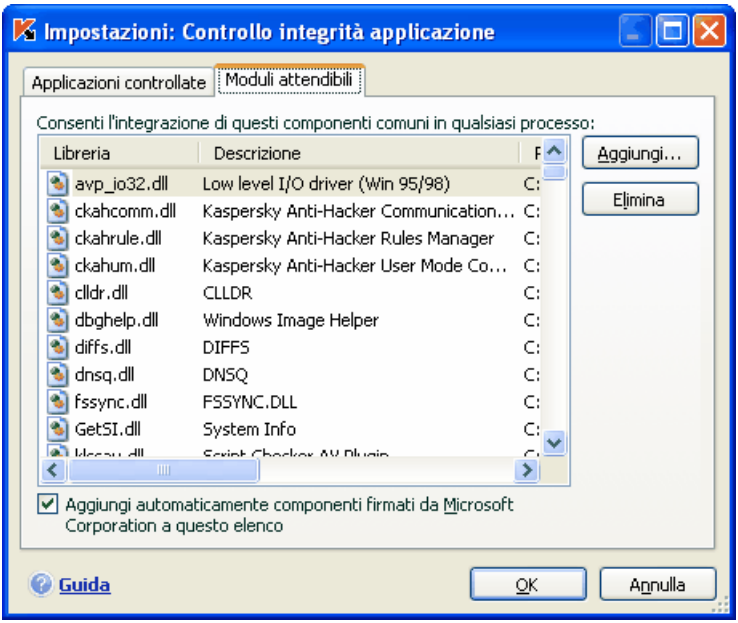


Figura 39. Configurazione dell'elenco dei moduli attendibili

10.3. Controllo del registro

Uno degli obiettivi dei programmi nocivi è spesso modificare i registri di sistema di Microsoft Windows del computer. Può trattarsi di innocui programmi-scherzo come di programmi realmente nocivi che presentano un'autentica minaccia per il computer.

Per esempio, programmi maligni possono copiare le proprie informazioni sulle chiavi di registro che determinano l'apertura automatica delle applicazioni all'avvio. Programmi maligni possono dunque partire automaticamente quanto si avvia il sistema operativo.

Il modulo Difesa proattiva traccia le modifiche degli oggetti del registro di sistema. Puoi abilitare o meno questo modulo spuntando la casella ☑ **Abilita Controllo del registro**.

Per configurare il monitoraggio dei registri di sistema:

1. Apri la finestra impostazioni e seleziona **Difesa Proattiva** sotto **Protezione**.

2. Clicca sul pulsante **Impostazioni** nella sezione **Controllo del registro** (vedi Figura 35).

Kaspersky Lab ha già creato un elenco di regole per controllare le operazioni del file di registro e lo ha incluso nel programma. Le operazioni relative alle chiavi di registro sono catalogate in gruppi logici come *System Security*, *Internet Security*, ecc. Ognuno di tali gruppi elenca i file del registro del sistema e regole per lavorare con essi. Ogni volta che il programma viene aggiornato, si aggiorna anche questo elenco.

La finestra delle impostazioni del **Controllo del registro** (vedi Figura 41) fornisce un elenco completo di regole.

Ad ogni gruppo di regole è assegnata una priorità di esecuzione che è possibile modificare per mezzo dei pulsanti **Sposta su** e **Sposta giù**. Più alto il gruppo è nell'elenco più alta è la priorità assegnata ad esso. Se il medesimo file di registro appartiene a gruppi diversi la prima regola applicata a quel file sarà quella del gruppo a più elevata priorità.

Puoi arrestare l'uso di un qualsiasi gruppo di regole nei seguenti modi:

- Deselezionare la casella ☑ accanto al nome del gruppo. Il gruppo di regole rimane presente nell'elenco ma non utilizzato.
- Eliminare il gruppo di regole dall'elenco. Si sconsiglia di eliminare i gruppi creati da Kaspersky Lab poiché contengono gli elenchi dei file del registro di sistema più spesso usati dai programmi maligni.

Figura 40. Gruppi chiavi di registro controllati

Puoi creare i tuoi gruppi di file di registro del sistema da monitorare. Per fare questo clicca **Aggiungi** nella finestra dei gruppi di file.

Nella finestra che si apre eseguire questi passaggi:

1. Digita il nome del nuovo gruppo di file per il monitoraggio delle chiavi di registro del sistema nel campo **Nome del gruppo**.
2. Seleziona la scheda **Chiavi** e crea un elenco di file di registro che apparterranno al gruppo da monitorare (vedi 10.3.1 a pag. 131) per il quale si desidera creare la regola. Può trattarsi di una o più chiavi.
3. Seleziona la scheda **Regole** e crea una regola (vedi 10.3.2 a pag. 132) per i file che verranno applicati alla chiave selezionata. È possibile creare più regole e impostarne l'ordine di applicazione.

10.3.1. Selezione delle chiavi di registro per creare una regola

Il gruppo di file creato deve contenere almeno un file di registro di sistema. La scheda Chiavi fornisce un elenco di file per la regola.

Per aggiungere una chiave di registro del sistema:

1. Fare clic sul pulsante **Aggiungi** nella finestra **Modifica regola del gruppo** (vedi Figura 42).
2. Nella finestra che si apre selezionare una chiave di registro del sistema o un gruppo di chiavi per cui si desidera creare la regola di monitoraggio.
3. Specificare il valore dell'oggetto o maschera per il gruppo di oggetti a cui si desidera applicare la regola nel campo **Valore**.
4. Selezionare la casella  **Includi sottochiavi** per la regola da applicare per tutti i file allegati al file di registro elencato.

È sufficiente utilizzare le maschere con un asterisco e un punto interrogativo contemporaneamente alla funzione **Includi sottochiavi** se nel nome della chiave sono utilizzati caratteri jolly.

Se selezioni un gruppo di chiavi che fa uso di maschera e si specifica un valore corrispondente, la regola sarà applicata a quel valore per tutte le chiavi del gruppo selezionato.

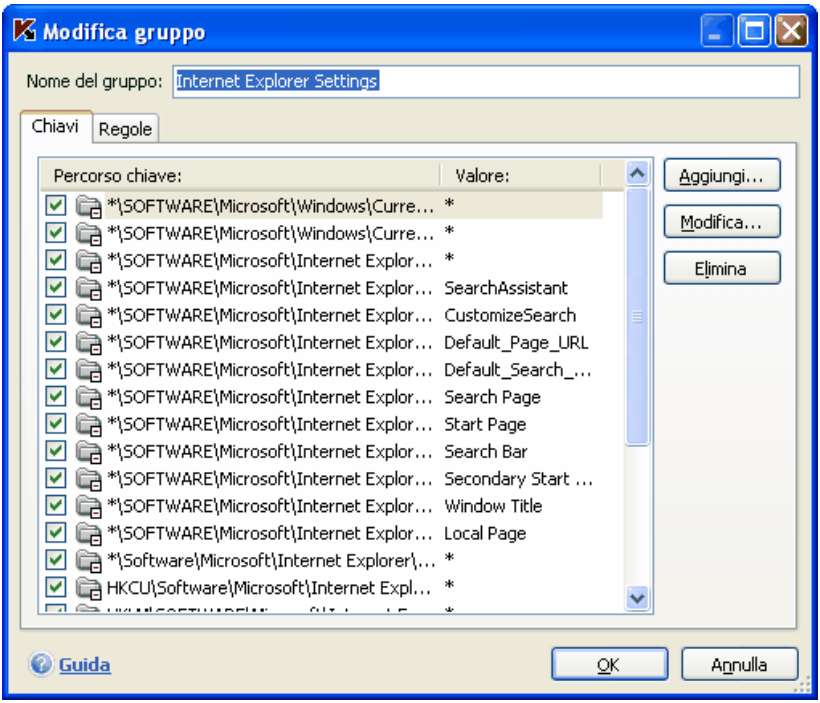


Figura 41. Aggiunta di chiavi di registro controllate

10.3.2. Creazione di una regola per il Controllo del registro

Una regola del Controllo del registro specifica:

- Il programma il cui accesso al registro di sistema viene monitorato
- La reazione di Difesa Proattiva quando un programma tenta di eseguire una operazione con un file di registro di sistema

Per creare una regola per i file di registro del sistema selezionati:

1. Fare clic su **Nuovo** nella scheda **Regole**. La regola generale sarà aggiunta alla prima posizione dell'elenco delle regole (vedi Figura 42).
2. Selezionare una regola dall'elenco e assegnare le impostazioni necessarie nella parte inferiore della scheda:
    - Specificare l'applicazione.

La regola viene creata per qualsiasi applicazione per impostazione predefinita. Se si desidera applicare la regola a un'applicazione specifica, fare clic con il pulsante sinistro del mouse su any che diventa selezionata. Quindi cliccare sul link specificare nome applicazione. Si apre un menu contestuale. Clicca su **Sfoglia** per aprire la finestra standard di selezione dei file oppure clicca su **Applicazioni** per vedere un elenco di applicazioni aperte e selezionare una di esse come desiderato.

- Definire la reazione di Difesa proattiva per l'applicazione selezionata che cerca di leggere, modificare o eliminare i file del registro di sistema.

  Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: Permetti, Richiedi intervento utente e Blocca. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata.

- Stabilire se si desidera generare un report dell'operazione eseguita, facendo clic su Registra evento / Non registrare evento.

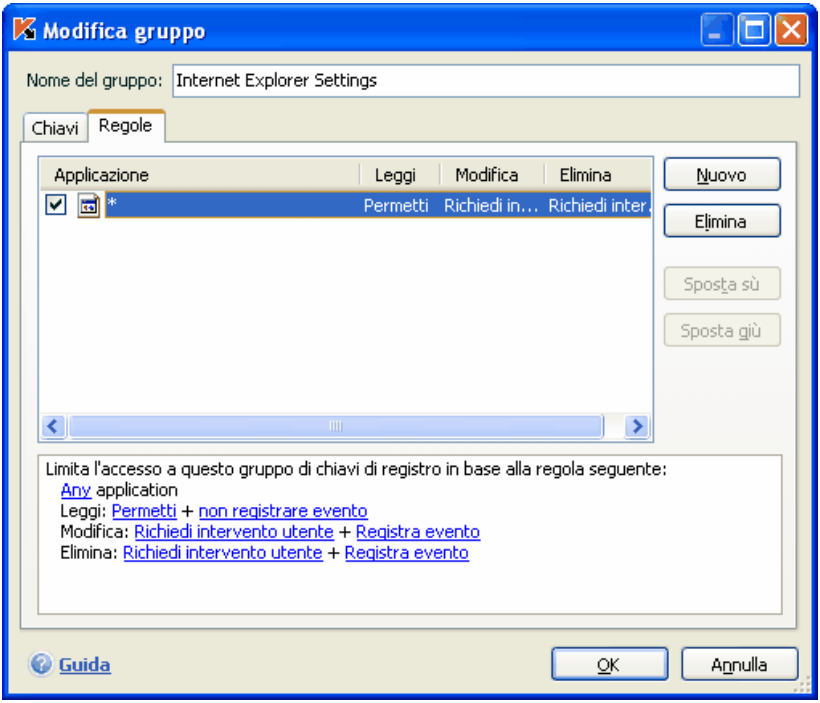


Figura 42. Creazione di una regola di monitoraggio delle chiavi di registro

È possibile creare diverse regole e modificarne la priorità per mezzo dei pulsanti **Sposta su** e **Sposta giù**. Con più alta è la regola nell'elenco con maggiore sarà la priorità assegnata ad essa.

È possibile inoltre creare una regola di autorizzazione (ad esempio tutte le azioni sono permesse) per un oggetto del registro di sistema da una notifica ammesso che un programma stia tentando di eseguire una operazione con un oggetto. Per fare questo fai clic nella finestra che si apre su Crea regola di autorizzazione nell'avviso e specifica l'oggetto del registro di sistema al quale la regola verrà applicata.

CAPITOLO 11. LA SCANSIONE ANTIVIRUS DEL COMPUTER

Un aspetto importante nella protezione di un computer dai virus è rappresentato dalla scansione anti-virus di aree definite dall'utente. Kaspersky Anti-Virus 7.0 può operare tale scansione su singoli oggetti (file, cartelle, unità disco, periferiche), o sull'intero computer. La scansione anti-virus impedisce la diffusione di quei codici dannosi che non sono stati individuati dalle componenti di protezione.

Kaspersky Anti-Virus 7.0 comprende tre modalità di scansione predefinite:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del computer, ovvero: la memoria del sistema, i programmi caricati all'avvio, i settori di boot del disco fisso e le directory di sistema *Windows* e *system32*. Tale funzione ha lo scopo di individuare rapidamente i virus presenti nel sistema senza operare la scansione completa dello stesso.

Risorse del computer

Esegue la scansione del computer, con una ispezione completa di tutte le unità disco, della memoria e dei file.

Oggetti di avvio

Esegue la scansione anti-virus dei programmi caricati all'avvio del sistema operativo.

Scansione Rootkit

Scansiona il computer per ricercare rootkits che nascondono programmi pericolosi nel sistema operativo. Queste utility inserite nel sistema, nascondono la loro presenza e la presenza di processi, cartelle, e chiavi diregistro di qualsiasi programma maligno descritto nella configurazione del rootkit.

Le impostazioni raccomandate per queste modalità sono quelle predefinite. È possibile visualizzare tali impostazioni (vedi 11.4 a pag. 139) o stabilire un programma (vedi 6.6 a pag. 64) per l'esecuzione delle azioni.

È inoltre possibile creare modalità di scansione personalizzate (vedere 11.3 a pagina 138) e pianificarne l'esecuzione. Ad esempio, è possibile pianificare la scansione anti-virus dell'archivio della posta elettronica una volta la settimana, o la scansione della sola cartella **Documenti**.

È comunque possibile eseguire la scansione anti-virus di singoli oggetti (come ad esempio il disco fisso contenente programmi e giochi, l'archivio di posta elettronica portato a casa dall'ufficio, un archivio allegato ad una e-mail, ecc.) senza dover impostare una modalità di scansione specifica. È sufficiente selezionare l'oggetto sul quale eseguire la scansione dall'interfaccia di Kaspersky Anti-Virus, o tramite i normali strumenti del sistema operativo di Microsoft Windows (ad esempio tramite **Explorer**, o direttamente dal **Desktop**, ecc.).

È possibile vedere la lista completa delle azioni di scansione del computer cliccando su Scansione nella parte sinistra della finestra principale dell'applicazione.

Puoi creare un disco di emergenza (vedi 15.4 a pag. 184) progettato per ristabilire il sistema dopo un attacco virus che ha danneggiato il file del sistema operativo impedendone l'avvio. Per fare ciò clicca su Crea Disco di emergenza.

11.1. Gestione delle attività di scansione antivirus

La scansione antivirus può essere avviata manualmente, oppure in maniera automatica, a scadenze predefinite (vedi 6.7 a pag. 65).

Per avviare manualmente un'attività di scansione:

Seleziona l'azione sotto **Scansione** nella finestra principale dell'applicazione e clicca Avvia Scansione.

Le azioni in esecuzione sono presentato nel menu contestuale cliccando con il tasto destro sulla icona della barra di sistema.

Per mettere in pausa la scansione:

Seleziona l'azione sotto **Scansione** nella finestra principale dell'applicazione e clicca **Sospendi**. La scansione sarà messa in pausa fino a quando non la riavvierai manualmente oppure riparte automaticamente in accordo con la pianificazione. Per una riavvio manuale clicca su Riprendi.

Per terminare una scansione:

Seleziona l'azione sotto Scansione nella finestra principale dell'applicazione e clicca **Interrompi.** La scansione sarà arrestata fino a quando non la riavvierai manualmente oppure riparte automaticamente in accordo con la pianificazione. Al successivo avvio dell'azione, il programma ti chiederà se desideri riprenderla dal punto in cui era stata precedentemente interrotta, o ricominciarla dal principio.

11.2. Creazione di un elenco di oggetti su cui eseguire una scansione

Per visualizzare un elenco di oggetti su cui operare una scansione per una particolare azione, seleziona il nome dell'azione (ad esempio **Risorse del computer**) nella sezione **Scansione** della finestra principale del programma. L'elenco degli oggetti sarà visualizzato sul lato destro della finestra (vedi Figura 43).

Figura 43. Elenco di oggetti su cui effettuare la scansione

Quando il programma viene installato, vengono già creati degli elenchi di oggetti su cui operare la scansione. Creando modalità di scansione personalizzate o selezionando un oggetto per la scansione, è possibile impostare un elenco di oggetti.

Puoi aggiungere o eliminare un oggetto all'elenco da scansionare usando il pulsante alla destra dell'elenco stesso. Per aggiungere un nuovo oggetto da scansionare all'elenco clicca sul pulsante **Aggiungi**; si aprirà una finestra nella quale selezionare l'oggetto su cui eseguire la scansione.

Per comodità dell'utente puoi aggiungere categorie ad una area di scansione come i database della posta, RAM, oggetti di avvio, backup del sistema operativo e file in Quarantena di Kaspersky Anti-Virus.

Inoltre, quando aggiungi ad una area di scansione una cartella che contiene oggetti incorporati puoi modificare la ripetizione. Per fare questo seleziona un oggetto dall'elenco degli oggetti da scansionare, apri il menù contestuale ed usa l'opzione Includi Sottocartelle.

Per cancellare un oggetto, selezionalo nell'elenco (il nome dell'oggetto verrà evidenziato in grigio) e cliccare sul pulsante **Elimina**. È possibile disabilitare temporaneamente la scansione su determinati oggetti di un elenco, senza doverli cancellare. Per far ciò è sufficiente spuntare gli oggetti in questione.

Per avviare una azione, cliccare su Avvia Scansione.

Oltre a questo, puoi selezionare un oggetto su cui eseguire una scansione anche utilizzando gli strumenti standard del sistema operativo di Microsoft Windows (ad esempio nella finestra di Explorer, o direttamente dal Desktop, ecc.) (vedi Figura 44). Per far ciò, seleziona l'oggetto, apri il menu contestuale di Microsoft Windows cliccando con il pulsante destro del mouse, e seleziona **Ricerca virus**.

Figura 44. Scansione di oggetti attraverso il menu contestuale di Microsoft Windows

11.3. Creazione di attività di scansione antivirus

Per eseguire la scansione antivirus di oggetti presenti sul computer, è possibile utilizzare le modalità di scansione predefinite offerte dal programma o crearne di nuove. Queste ultime vengono create a partire da attività di scansione preesistenti.

Per creare una nuova attività di scansione antivirus:

1. Selezionare, nella sezione **Scansione** della finestra principale del programma, una azione le cui impostazioni sono le più vicine alla tua necessità.
2. Apri il menu contestuale e seleziona **Salva con nome** oppure clicca su **Nuova operazione di scansione**.

3. Nella finestra che appare, inserisci il nome della nuova attività e premi **OK**. Nella sezione Scansione della finestra principale del programma apparirà, nell'elenco delle azioni, una attività con quel nome.

Attenzione!

C'è un limite al numero di azioni che l'utente può creare. Il massimo è 4 azioni.

La nuova attività di scansione eredita tutte le proprietà di quella da cui è stata creata. Per mettere ulteriormente a punto la nuova attività è necessario creare un elenco di oggetti su cui operare la scansione (vedi 11.2 a pag. 137), impostare le proprietà (vedi 11.4 a pag. 139) della modalità stessa, e, se necessario, configurare la pianificazione (vedi 6.6 a pag. 64) per l'esecuzione automatica della azione.

Per rinominare a un'attività esistente:

seleziona l'attività nella sezione **Scansione** della finestra principale del programma e clicca Rinomina.

Digitare, nella finestra che appare, il nuovo nome, e cliccare su **OK**. Il nome dell'azione verrà cambiato anche nella sezione **Scansione**.

Per eliminare un'attività esistente:

seleziona l'azione sotto **Scansione** nella finestra principale dell'applicazione e clicca su **Elimina**.

Apparirà una finestra nella quale ti verrà chiesto di confermare l'operazione di cancellazione. A conferma avvenuta, l'attività di scansione eliminata non sarà più presente nell'elenco delle attività della sezione **Scansione**.

Attenzione!

È possibile rinominare o eliminare soltanto le azioni create dall'utente.

11.4. Configurazione delle attività di scansione antivirus

Il metodo impiegato per operare la scansione degli oggetti presenti nel computer dipende da un insieme di proprietà assegnate a ciascuna azione.

Configurare le impostazioni delle modalità di scansione:

apri la finestra impostazioni dell'applicazione, seleziona il nome della attività sotto **Scansione** ed usa il link Impostazioni.

Per ciascuna modalità di scansione, è possibile utilizzare tale finestra al fine di:

- Selezionare un livello di protezione per la modalità di scansione (vedi 11.4.1 a pag. 140).
- Modificare le impostazioni avanzate:
  - definire i tipi di file da sottoporre a scansione (vedi 11.4.2 a pag. 141);
  - configura l'avvio dell'attività utilizzando un account utente diverso (vedi 6.6 a pag. 64);
  - configura le impostazioni di scansione avanzate (vedi 11.4.3 a pag. 145);
  - abilita la scansione rootkit (vedi 11.4.4 a pag. 146) e l'analizzatore euristico (vedi 11.4.5 a pag. 147);
  - ripristina le impostazioni di scansione predefinite (vedi 11.4.6 a pag. 148);
  - seleziona l'azione che il programma deve intraprendere non appena venga rilevato un oggetto infetto, o presunto tale (vedi 11.4.7 a pag. 148);
  - creare una pianificazione (vedi 6.7 a pag. 65) per l' avvio automatico della azione.

È inoltre possibile configurare delle impostazioni globali (vedi 11.4.8 a pag. 150) applicabili a tutte le modalità di scansione.

La sezione seguente del manuale d'uso esaminerà in dettaglio tutte le impostazioni sopra citate.

11.4.1. Selezione del livello di protezione

A ciascuna scansione può essere assegnato un livello di protezione (vedi Figura 45):

Protezione massima – Massima accuratezza nella scansione della macchina nel suo complesso, o di singoli dischi, cartelle o file. Se ne raccomanda l'impiego qualora si sospetti che un virus possa essere penetrato nel computer.

Consigliato. È il livello consigliato dagli esperti Kaspersky Lab. La scansione funziona in maniera analoga al livello **Protezione massima**, fatta eccezione per i file di posta.

Alta velocità – Livello che permette all'utente un agevole impiego di applicazioni che utilizzano estensivamente le risorse della macchina, poiché la gamma dei file sottoposti a scansione è ridotta.

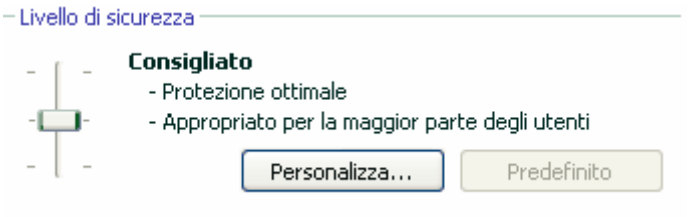


Figura 45. Selezione di un livello di protezione per la scansione antivirus

Per impostazione predefinita, File Anti-Virus è impostato su **Consigliato**.

È possibile aumentare o diminuire la sicurezza della scansione anti-virus selezionando il livello desiderato, oppure cambiando le impostazioni del livello corrente.

Per modificare il livello di protezione:

Regolare i cursori. Regolando il livello di protezione, si definisce il rapporto tra la velocità di scansione e il numero totale di file esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di file esaminati.

Se nessuno dei livelli di sicurezza è ritenuto soddisfacente, è possibile personalizzarne le impostazioni di protezione. Si raccomanda di selezionare il livello più prossimo alle tue necessità come base per modificarne i parametri. In questo caso il livello diventa **Personalizzato**.

Per modificare le impostazioni di un livello di protezione:

1. Apri la finestra impostazioni dell'applicazione e seleziona una azione sotto **Scansione**.
2. Clicca su **Personalizza** sotto **Livello Sicurezza** (vedi Figura 45).
3. Modifica i parametri di protezione nella relativa finestra e clicca **OK**.

11.4.2. Definizione del tipo di oggetti da sottoporre a scansione

Quando si specificano i tipi di oggetti da analizzare, si stabilisce il formato dei file, la dimensione e i dischi che saranno sottoposti a scansione anti-virus in una specifica modalità.

I tipi di file esaminati vengono definiti nella sezione **Tipi di file** (vedi Figura 46). Seleziona una delle tre opzioni:

- **Esamina tutti i file**. Con questa opzione, tutti gli oggetti vengono sottoposti a scansione, senza eccezioni.
- **Esamina programmi e documenti (in base al contenuto)**. Selezionando questo gruppo di programmi, si sottopongono a scansione solo i file a rischio di infezione – quelli in cui si potrebbe nascondere un virus.

  Nota:

  Vi sono file nei quali non possono annidarsi virus, poiché il codice di tali file non contiene alcun elemento a cui il virus possa attaccarsi, Un esempio è costituito dai file .txt.

  Al contrario ci sono formati file che contengono o possono contenere codici eseguibili. AD esempio i formati .exe, .dll, .doc. Per questi file il rischio di inserimento di codici maligni è piuttosto elevato.

  Prima di cercare un virus in un oggetto, la sua intestazione viene analizzata per rilevarne il formato (txt, doc, exe, ecc.).

- **Esamina programmi e documenti (in base all'estensione)**. In questo caso, il programma sottoporrà a scansione solamente i file potenzialmente infetti, determinandone il formato in base all'estensione. Utilizzando il link, è possibile accedere ad un elenco delle estensioni dei file che, con questa opzione, vengono sottoposti a scansione (vedi A.1 a pag. 229).

Suggerimento:

Ricordare che è possibile inviare virus all'interno di file con estensione .txt che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione **Esamina programmi e documenti (in base all'estensione)**, tale file sarebbe escluso dalla scansione. Invece, selezionando l'opzione **Esamina programmi e documenti (in base al contenuto)**, il programma ignorerà l'estensione del file analizzandone invece l'intestazione, e determinando così la sua vera natura di file eseguibile. Il file sarebbe quindi sottoposto a un'approfondita scansione antivirus.

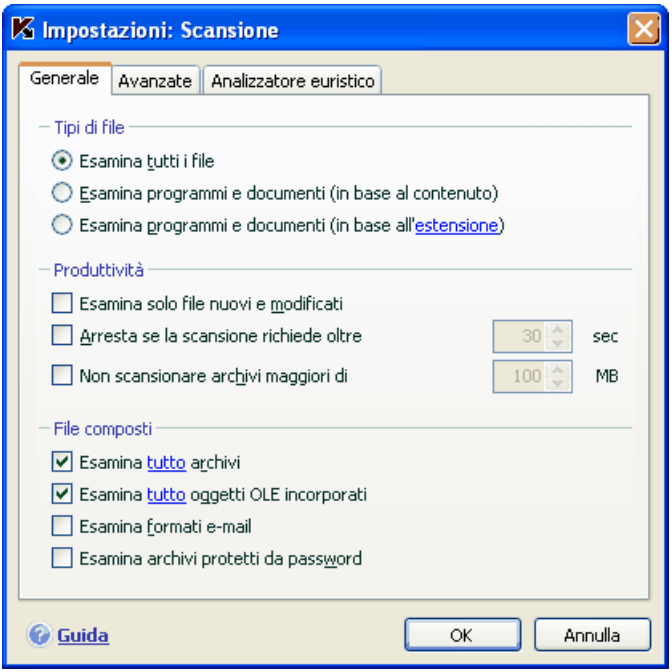


Figura 46. Configurazione delle impostazioni di scansione

Nella sezione **Produttività**, è possibile specificare se si vuole sottoporre a scansione solamente i nuovi file, oppure i nuovi file e quelli che sono stati modificati dopo la scansione precedente. Questa modalità riduce considerevolmente la durata della scansione e aumenta la velocità del programma. Per attivare questa modalità, selezionare la casella **Esamina solo file nuovi e modificati**. Questa modalità si applica sia ai file semplici sia a quelli complessi.

Nella sezione **Produttività** si possono inoltre stabilire limiti di tempo e di dimensione dei file per la scansione.

Arresta se la scansione richiede oltre ... sec. Selezionare quest'opzione ed inserire la durata massima per la scansione di un singolo oggetto. Se la scansione di un oggetto richiede un tempo superiore a quello specificato, l'oggetto viene rimosso dalla coda di scansione.

Non scansionare archivi maggiori di … MB. Selezionare quest'opzione ed inserire la dimensione massima dell'oggetto. Se la dimensione di un oggetto supera quella specificata, l'oggetto viene rimosso dalla coda di scansione.

Nella sezione **File composti**, specificare quali file composti debbano essere sottoposti a scansione anti-virus:

Esamina Tutti/Solo nuovi archivi – analizza gli archivi con estensione .rar, .arj, .zip, .cab, .lha, .jar, e .ice.

Attenzione!

Kaspersky Anti-Virus non elimina file in formato compresso che non supporta automaticamente (ad esempio .ha, .uue, .tar) anche se tu selezioni l'opzione di curarli o eliminarli automaticamente gli oggetti non verranno curati.

Per eliminare questi file compressi clicca sul link Cancella Archivi nella notifica degli oggetti pericolosi. Questa notifica verrà mostrata sullo schermo dopo che il programma inizia a controllare gli oggetti riconosciuti durante la scansione. Puoi anche eliminare manualmente gli archivi infetti.

Scansiona Tutti/Solo nuovi oggetti OLE incorporati – analizza gli oggetti incorporati nei file (per esempio fogli di calcolo di Excel o macro incorporati in un file di Microsoft Word, allegati di posta, ecc.).

Per ogni tipo di file complesso è possibile selezionare ed esaminare tutti i file o solo quelli nuovi usando il link a fianco del nome dell'oggetto. Facendovi clic sopra con il pulsante sinistro del mouse, il suo valore cambia. Se la sezione **Produttività** è stata impostata in modo da esaminare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file complesso da sottoporre a scansione.

Esamina formati e-mail – esegue la scansione dei file e dei database di posta elettronica. Se la selezione è spuntata Kaspersky Anti-Virus controllerà il file di posta analizzando tutti i suoi componenti (corpo, allegati). Se la selezione non è spuntata il file di posta sarà controllato come singolo file.

In merito alla scansione di database di posta elettronica protetti da password, si prega di notare quanto segue:

- Kaspersky Anti-Virus rileva i codici dannosi presenti nei database di Microsoft Office Outlook 2000, ma non li disinfetta;
- Il programma non supporta la scansione anti-virus dei database protetti di Microsoft Office Outlook 2003.

Esamina archivi protetti da password – esegue la scansione di archivi protetti da password. Se quest'opzione è attiva, una finestra richiederà l'inserimento di una password prima che venga eseguita la scansione di un oggetto archiviato. Se il riquadro non è selezionato, la scansione salterà gli archivi protetti.

11.4.3. Impostazioni di scansione anti-virus avanzate

Oltre alle impostazioni di base per la scansione anti-virus, è possibile configurare una serie di ulteriori impostazioni (vedi Figura 47):

Usa tecnologia iChecker – abilita l'impiego di una tecnologia che permette di incrementare la velocità di scansione escludendo certi oggetti dalla scansione. La scansione usa uno speciale algoritmo che valuta la data di pubblicazione dei database dell'applicazione, l'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

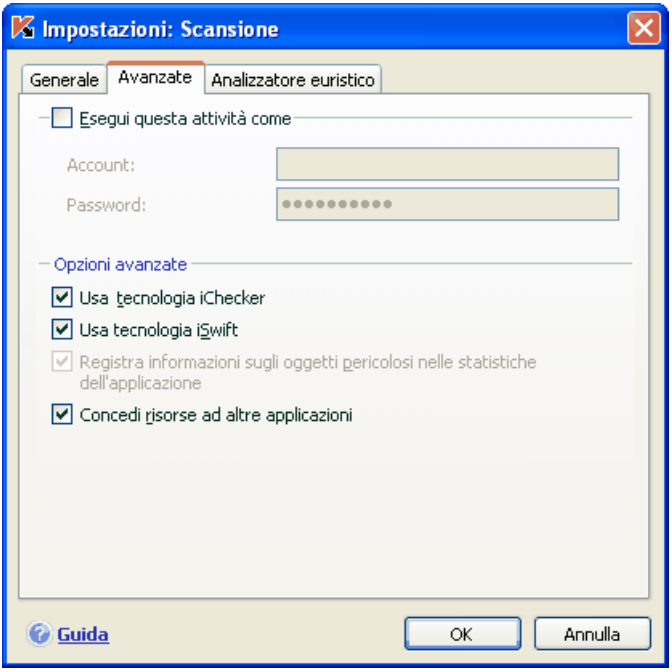


Figura 47. Impostazioni di scansione avanzate

Ad esempio, se nel computer è presente un file archivio che è stato sottoposto a scansione e classificato come non infetto, alla successiva scansione il programma ignorerà questo file, a meno che non sia stato modificato nel frattempo, o che non siano state cambiate le impostazioni di scansione. Se la struttura dell'archivio è stata modificata in seguito all'aggiunta di un oggetto, se sono state modificate le opzioni di scansione, o

se i database dell'applicazione sono stati aggiornati, il programma eseguirà nuovamente la scansione dell'archivio.

L'applicazione della tecnologia iChecker™; essa non lavora con file molto grandi e si applica solo agli oggetti la cui struttura viene riconosciuta da Kaspersky Anti-Virus (ad esempio, file con estensione .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

Usa tecnologia iSwift – Questa è uno sviluppo della tecnologia iChecker per computer che utilizzano un file system NTFS. Ci sono alcune limitazioni: è connessa ad una specifica posizione del file nel file system e può essere applicata solo ad oggetti di un file system NTFS.

Registra informazioni sugli oggetti pericolosi nelle statistiche dell'applicazione Salva informazioni sugli oggetti pericolosi rilevati nelle statistiche globali dell'applicazione e visualizza un elenco delle minacce nella scheda Rilevati della finestra dei report (vedi para. 15.3.2 a pag. 180). Se questa casella è deselezionata, i dati sugli oggetti pericolosi non saranno registrati nel report, pertanto, questi oggetti non potranno essere trattati.

Concedi risorse ad altre applicazioni – mette in pausa la scansione se il processore è troppo occupato per altre applicazioni.

11.4.4. Scansione Rootkit

Un rootkit è un gruppo di utility usato per nascondere programmi maligni all'interno del sistema operativo. Queste utility si insidiano nel sistema operativo mascherando la loro presenza e la presenza di processi, cartelle, e chiavi di registro appartenenti a qualsiasi malware descritto nella configurazione del rootkit.

Questa ricerca può essere condotta da qualsiasi scansione anti-virus (ammesso che essa sia abilitata per quella specifica azione); comunque gli esperti di Kaspersky Lab hanno creato ed ottimizzato una azione di scansione separata per la ricerca di questo tipo di malware.

Per abilitare la scansione rootkit spunta **Abilita rilevamento rootkit** sotto **Scansione Rootkit.** Se la scansione è abilitata puoi anche eseguire una più approfondita scansione spuntando la casella **Abilita scansione rootkit estesa.** In questo modo la scansione ricercherà in modo molto attento questi programmi analizzando un elevato numero e tipo di oggetti. Come impostazione queste caselle di spunta sono deselezionate in quanto questa modalità impegna significative risorse del sistema operativo.

Per configurare una scansione rootkit:

1. Apri la finestra impostazioni dell'applicazione e seleziona una azione sotto **Scansione**.

2. Clicca **Personalizza** sotto **Livello di sicurezza** (vedi Figura 45) e seleziona il tasto **Analizzatore Euristico** nella relativa finestra (vedi Figura 48).

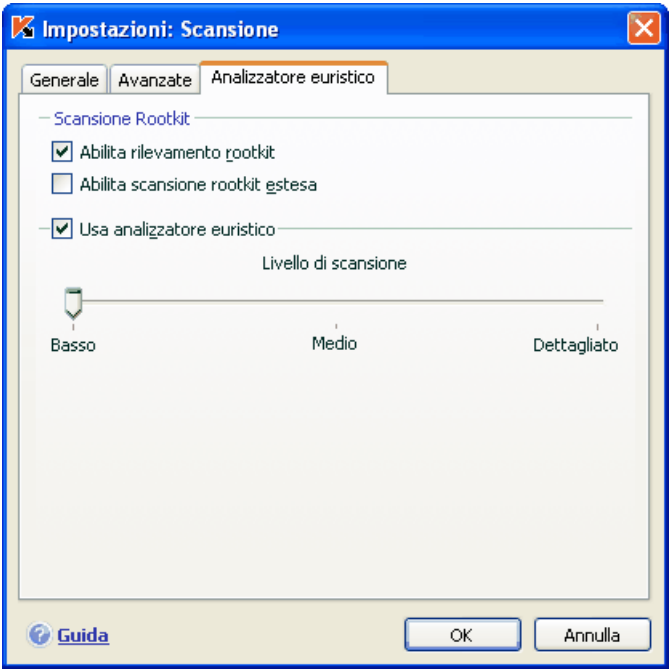


Figura 48. Configurazione scansione rootkit e metodo euristico

11.4.5. Utilizzo dell'analizzatore euristico

I metodi euristici vengono utilizzati da numerosi componenti in tempo reale di protezione e scansioni anti-virus (vedi 7.2.4 a pag. 88 per ulteriori dettagli).

La scheda **Analizzatore Euristico** (vedi Figura 48) può essere utilizzata per abilitare/disabilitare l'analisi euristica durante la scansione di minacce sconosciute. Occorre procedere come segue:

1. Apri la finestra impostazioni dell'applicazione e seleziona una azione sotto **Scansione**.
2. Clicca su **Personalizza** sotto **Livello di sicurezza** e apri **Analizzatore Euristico** nella finestra di dialogo.

Per usare il metodo euristico spunta la casella **Usa analizzatore euristico.** Un ulteriore livello di precisione può essere impostato muovendo il cursore su una delle seguenti opzioni: **Basso**, **Medio** o **Dettagliato.**

11.4.6. Ripristino delle impostazioni di scansione predefinite

Quando si configurano le impostazioni per una data modalità di scansione, è sempre possibile ripristinare le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di protezione **Consigliato**.

Per ripristinare le impostazioni predefinite della scansione:

1. Apri la finestra impostazioni dell'applicazione e seleziona una azione sotto **Scansione**.
2. Clicca sul pulsante **Predefinito** nella sezione **Livello di sicurezza** (vedi Figura 45).

11.4.7. Selezione delle azioni da applicare agli oggetti

Se durante una scansione viene rilevato un file infetto, o presunto tale, il programma reagirà in base allo stato del file e all'azione selezionata.

All'oggetto in questione può venire classificato, dopo la scansione, con dei seguenti stati:

- Programma nocivo (per esempio, *virus, Trojan*).
- *Probabilmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. E' come se il programma riconoscesse una sequenza di codici nel file di un virus sconosciuto oppure un codice modificato in un virus noto.

Per impostazione predefinita, tutti i file infetti sono sottoposti a un tentativo di riparazione e se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

apri la finestra impostazioni dell'applicazione e seleziona una azione sotto **Scansione**. Tutte le possibili azioni sono presentate nella corrispondente sezione (vedi Figura 49).

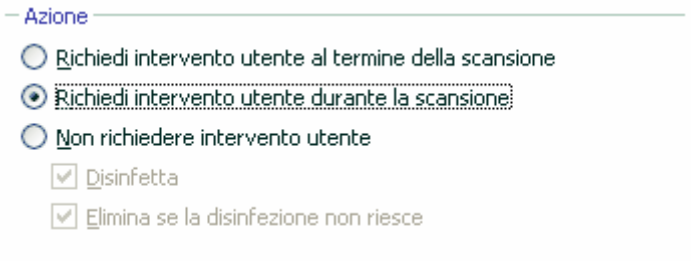


Figura 49. Selezione di un'azione per gli oggetti pericolosi

Se l'azione selezionata era	**Se viene rilevato un oggetto dannoso o potenzialmente infetto**
Richiedi intervento utente al termine della scansione	Il programma non interviene sugli oggetti prima della fine della scansione. Al termine del processo, una finestra di statistiche relative alla scansione appena ultimata mostrerà l'elenco degli oggetti rilevati, chiedendo all'utente se intervenire su di essi o meno.
Richiedi intervento utente durante la scansione	Il programma mostrerà un messaggio di allarme contenente informazioni sul codice dannoso che ha, o che potrebbe avere, infettato un file, e offrirà all'utente la possibilità di scegliere tra una delle seguenti azioni.
Non richiedere intervento utente	Il programma registra nel rapporto le informazioni relative agli oggetti rilevati, senza intervenire su di essi e senza notificare la cosa all'utente. Si sconsiglia di avvalersi di quest'opzione, poiché gli oggetti dannosi permangono sul computer, ed è praticamente impossibile evitare l'infezione.

Non richiedere intervento utente **Disinfetta**	Il programma tenta di pulire l'oggetto rilevato senza chiedere conferma all'utente. Se la disinfezione non riesce, al file verrà assegnato lo stato di *Potenzialmente infetto*, e sarà spostato in Quarantena (vedi 15.1 a pag. 170). Le informazioni in merito vengono registrate nel report (vedi 15.3 a pag. 176). In un secondo momento l'utente potrà tentare di disinfettare questo oggetto.
Non richiedere intervento utente **Disinfetta** **Elimina se la disinfezione non riesce**	Il programma tenta di trattare l'oggetto rilevato senza chiedere conferma all'utente. Se la disinfezione non riesce, è eliminato.
Non richiedere intervento utente **Disinfetta** **Elimina**	Il programma elimina automaticamente l'oggetto rilevato.

Nell'eseguire la disinfezione o l'eliminazione di un oggetto, Kaspersky Anti-Virus ne crea una copia di Backup (vedi 15.2 a pag. 174) utile nel caso in cui risulti necessario ripristinare l'oggetto, o emerga l'opportunità di disinfettarlo.

11.4.8. Configurazione di impostazioni di scansione globali per tutte le attività

Ogni operazione di scansione viene eseguita secondo una modalità definita da specifiche impostazioni. La modalità di scansione che si crea all'atto dell'installazione del programma utilizza le impostazioni predefinite raccomandate dagli esperti di Kaspersky Lab.

È possibile definire delle impostazioni globali valide per tutte le operazioni di scansione, in qualsiasi modalità. Come termine di riferimento si utilizza un gruppo di proprietà applicabili alla scansione anti-virus di un singolo oggetto.

Per assegnare impostazioni di scansione globali:

1. Apri la finestra delle impostazioni dell'applicazione e seleziona la sezione **Scansione**.

2. Configura le impostazioni: seleziona **Livello di sicurezza** (vedi 11.4.1 a pag. 140), configura il livello avanzato delle impostazioni e seleziona una azione per gli oggetti (vedi 11.4.7 a pag. 148).

3. Per applicare queste nuove impostazioni a tutte le azioni clicca sul pulsante **Applica** nella sezione **Altre impostazioni attività**. Conferma le impostazioni globali che hai selezionato nella casella pop-up di dialogo.

CAPITOLO 12. TEST DELLE CARATTERISTICHE DI KASPERSKY ANTI-VIRUS

Dopo aver installato e configurato Kaspersky Anti-Virus consigliamo di verificare che le impostazioni e l'operatività del programma siano corrette usando un test virus e le sue variazioni.

12.1. Il test virus EICAR e le sue variazioni

Il test virus è stato appositamente progettato da eicar (European Institute for Computer Antivirus Research) per testare la funzionalità antivirus.

Il test virus NON E? UN VIRUS e non contiene codici che potrebbero danneggiare il tuo computer. COmunque molti programmi anti-virus lo riconosceranno come un virus.

Non usare mai un vero virus per verificare la funzionalità di un antivirus!

Puoi scaricare il test virus dal sito ufficiale **EICAR**: http://www.eicar.org/anti_virus_test_file.htm

Il file che scarichi dal sito **EICAR** contiene il corpo di uno standard test virus che Kaspersky ANti-Virus riconoscerà, lo etichetterà come **virus** e organizzerà il set di azioni per quel tipo di oggetto.

Per testare la reazione di Kaspersky Anti-Virus quando vengono riconosciuti diversi tipo di oggetti, puoi modificare il contenuto del test virus standard aggiungendo uno dei prefissi ripoprtati nella tabella seguente.

Prefisso	**Stato Test virus**	**Azione conseguente al processo dell'oggetto da parte dell'applicazione**
Nessun prefisso, standard test virus	Il file contiene un test virus. Non puoi disinfettare l'oggetto.	L'applicazione identificherà l'oggetto come maligno, impossibile da pulire e quindi lo eliminerà.
CORR–	Danneggiato	L'applicazione potrebbe accedere all'oggetto ma non può scansionarlo poichè l'oggetto è danneggiato (ad esempio la struttura file è interrotta o è in un formato non valido)
SUSP– WARN–	Il file contiene un test virus (modificazione). Non puoi disinfettare l'oggetto.	L'oggetto è una modificazione di un virus conosciuto o un virus sconosciuto. I database dell'applicazione non contengono una descrizione della procedura per trattare questi ogfgetti. L'applicazione metterà l'oggetto in Quarantena per essere processato in seguito con database aggiornati.
ERRO–	Errore nel processare l'oggetto	Si è verificato un errore nella processione di un oggetto: l'applicazione non può accedere all'oggetto per eseguire la scansione poichè l'integrità dell'oggetto è stata corrotta (ad esempio nessuna fine per un archivio multivolume) o non esiste la connessione ad esso (se l'oggetto deve essere scansionato su un drive del network)
CURE–	Il file contiene un test virus. Può essere curato. The object is subject to disinfection, and the text of the body of the virus will change to `CURE`.	L'oggetto contiene un virus che può essere curato. L'applicazione scansionerà l'oggetto alla ricerca di virus e dopo di ciò l'oggetto verrà riparato.

Prefisso	Stato Test virus	Azione conseguente al processo dell'oggetto da parte dell'applicazione
DELE–	Il file contiene un test virus- Non puoi disinfettare l'oggetto.	L'oggetto contiene un virus che non può essere disinfettato o è un Trojan. L'applicazione elimina questo oeggetto.

La prima colonna della tabella contiene i prefissi che devono nessere aggiunti all'inizio della stringa di uno standard test virus. La seconda colonna descrive lo stato e la reazione di Kaspersky Anti-Virus ai vari tipi di test virus. La terza colonna contiene informazioni per gli oggetti aventi il medesimo stato e che l'applicazione ha processato.

I valori nelle impostazioni delle scansioni anti-virus determinano l'azione presa per ciascuno degli oggetti.

12.2. Testing di File Anti-Virus

Per testare la funzionalità di File Anti-Virus:

1. Abilita la registrazione di tutti gli eventi, in modo che il file del report contenga sia i dati degli oggetti danneggiati che quelli degli oggetti non scansionati a causa di errori. Per fare ciò spunta ☑ **Registra eventi non critici** sotto **Report e file dati** nella finestra impostazioni dell'applicazione (vedi 15.3.1 a pag. 179).
2. Crea una cartella o un disco, copia il virus di prova scaricato dal sito ufficiale dell'organizzazione (vedi 12.1 a pag. 152) e le modificazioni al test virus che hai creato.

File Anti-Virus intercetterà il tuo tentativo di accedere al file, lo scansionerà e ti informerà che è stato riconosciuto come oggetto pericoloso:

Figura 50. Oggetti pericolosi riconosciuti

Quando selezioni diverse opzioni per lavorare con gli oggetti riconosciuti puoi testare la reazione di File Anti-Virus per i diversi tipi di oggetto.

Puoi vedere i dettagli circa le prestazioni di File Anti-Virus nel report relativo al componente.

12.3. Test della scansione anti-virus

Per testare un'attività di scansione:

1. Crea una cartella su un disco nella quale copiare il virus di prova scaricato dal sito ufficiale dell'organizzazione (vedi 12.1 a pag. 152) e le variazioni al virus di prova da te create.
2. Crea una nuova operazione di scansione virus (vedere 11.3 a pag. 138) e seleziona la cartella contenente il set di virus di prova per l'oggetto da scansionare (vedi 12.1 a pag. 152).
3. Permetti che tutti gli eventi vengano registrati in modo che il report presenti i dati per gli oggetti scansionati e per gli oggetti non scansionati a causa di

errori. A tal fine ☑ spunta **Registra eventi non critici** sotto **Report e file dati** nella finestra impostazioni dell'applicazione (vedi 15.3.1 a pag. 179).

4. Avvia l'operazione di scansione (vedi 11.1 a pag. 136).

Durante la scansione, se rileva oggetti sospetti od infetti, viene fornita a video una notifica circa gli oggetti chiedendo all'utente quale successiva azione intraprendere.

Figura 51. Oggetti pericolosi rilevati

In questo modo, scegliendo per le azioni differenti opzioni, puoi verificare la reazione di Kaspersky Anti-Virus alla rilevazione dei diversi tipi di oggetti.

Puoi vedere i dettagli circa le prestazioni della scansione nel report del componente.

CAPITOLO 13. AGGIORNAMENTI DEL PROGRAMMA

Mantenere aggiornato il software antivirus costituisce un investimento in termini di sicurezza per il proprio computer. Poiché ogni giorno nascono nuovi virus, trojan e altri software dannosi, per proteggere costantemente le proprie informazioni è fondamentale aggiornare regolarmente l'applicazione di protezione.

L'aggiornamento dell'applicazione implica lo scaricamento e l'installazione, sul proprio computer, dei seguenti componenti:

- **Database Anti-virus e driver di rete**

  Per proteggere le informazioni presenti sul computer l'applicazione fa uso dei database dell'applicazione. I componenti software che assicurano la protezione usano il database delle firme delle minacce per ricercarle e disinfettare gli oggetti nocivi presenti. I database sono aggiornati di ora in ora con la registrazione di nuove minacce e dei metodi per debellarle, ed è pertanto consigliabile aggiornarle in maniera regolare.

  Oltre all'elenco delle minacce vengono anche aggiornati i driver di rete che abilitano in componenti di protezione ad intercettare il traffico di rete.

  Le precedenti versioni di Kaspersky Lab supportavano il database sia in assetto *standard* che *esteso*, ciascuno dei quali implicato nella protezione del computer da diversi tipi di oggetti dannosi. Con Kaspersky Anti-Virus non è più necessario decidere quale set di database adottare. Ora i nostri prodotti usano database che proteggono sia dai malware sia dai riskware.

- **Moduli dell'applicazione**

  Oltre ai database dell'applicazione, Kaspersky Anti-Virus consente anche l'aggiornamento dei moduli di programma. Nuovi aggiornamenti dell'applicazione vengono elaborati con regolarità.

La principale fonte di aggiornamenti per Kaspersky Anti-Virus è rappresentata dai server di Kaspersky Lab. Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet.

Il tuo computer deve essere connesso ad Internet per poter scaricare gli aggiornamenti dai server di aggiornamento. Nel caso utilizzi un server proxy dovrai configurare le impostazioni di connessione (vedi 15.7 a pag. 192).

Qualora non disponessi di un accesso ai server di Kaspersky Lab (ad esempio, se il computer non fosse connesso ad Internet), è possibile rivolgersi

direttamente all'ufficio di Kaspersky Lab chiamando il +7 (495) 797-87-00, +7 (495) 645-79-39 chiedendo di essere messi in contatto con partner di Kaspersky Lab che siano in grado di fornire gli aggiornamenti desiderati in formato compresso su floppy disk o CD.

Gli aggiornamenti possono essere scaricati secondo una delle seguenti modalità:

- *Automatica*. Kaspersky Anti-Virus verifica ad intervalli regolari la disponibilità di pacchetti aggiornati presso la fonte di aggiornamento. La scansione può essere pianificata per essere più frequente nei casi di pericolo o meno quando il pericolo è passato. Quando il programma rileva freschi aggiornamenti li scarica e li installa sul computer. Questa è l'impostazione predefinita.
- *Programmata*. L'aggiornamento è programmato in modo da cominciare ad un tempo prestabilito.
- *Manuale*. Con questa opzione, la procedura di aggiornamento viene avviata manualmente.

Durante l'aggiornamento, l'applicazione confronta i database ed i moduli di programma presenti sul computer con le versioni disponibili sul server. Se il computer dispone delle versioni più recenti, la cosa verrà notificata in una apposita finestra, confermando che la macchina è aggiornata. Qualora le versioni presenti sul computer non corrispondano a quelle disponibili sul server, il programma scaricherà le sole parti mancanti. Gli aggiornamenti non scaricano i database ed i moduli già presenti nell'applicazione il che aumenta la velocità di download e riduce il traffico Internet.

Prima di aggiornare i database, Kaspersky Anti-Virus ne esegue una copia di backup, che può venir utilizza se è necessario un rollback (ritorno) (vedere 13.2 a pag. 159). Se ad esempio il processo di aggiornamento danneggia i database e li rende inutilizzabili, puoi facilmente ritornare alla precedente versione e provare ad aggiornare i database in seguito.

Puoi distribuire gli aggiornamenti posti su una fonte locale durante l'aggiornamento dell'applicazione (vedere 13.3.3 a pag. 164). Questa caratteristica ti permette di aggiornare sui computer di rete i database ed i moduli usati dalla versione 7.0 risparmiando sulla occupazione di banda.

13.1. Avvio della procedura di aggiornamento

È possibile iniziare l'aggiornamento in qualsiasi momento. Il processo opererà dall'origine dell'aggiornamento selezionata dall'utente (vedi 13.3.1 pag. 160).

La procedura di aggiornamento può essere avviata da:

- il menu contestuale (vedere 4.2 a pag. 43);
- la finestra principale del programma (vedere 4.3 a pag. 45).

Per avviare la procedura di aggiornamento dal menu di scelta rapida:

1. Clicca con il tasto destro sulla icona del programma nella barra di sistema per aprire il menù.
2. Seleziona **Aggiornamento**.

Per avviare la procedura di aggiornamento dalla finestra principale del programma:

1. Apri la finestra principale dell'applicazione e seleziona il componente **Aggiornamento**.
2. Clicca sul link Aggiorna database.

Informazioni circa l'aggiornamento sono riportate nella finestra principale. Clicca su Dettagli per i dettagli del processo di aggiornamento. Questo mostrerà un report dettagliato dell'azione di aggiornamento. Puoi chiudere la finestra del report cliccando su **Chiudi**. L'aggiornamento proseguirà.

Nota che gli aggiornamenti sono distribuiti ad una fonte locale durante il processo di aggiornamento, ammesso che questo servizio sia abilitato (vedi 13.3.3 a pag. 164).

13.2. Ritorno all'aggiornamento precedente

Ogni volta che si avvia la procedura di aggiornamento, Kaspersky Anti-Virus crea innanzitutto una copia di backup dei database e moduli del programma correnti, e solo successivamente inizia a scaricarne le nuove versioni. In tal modo, qualora l'aggiornamento non vada a buon fine, è possibile tornare ad utilizzare i database precedenti.

Per *ripristinare la versione precedente del database delle minacce:*

1. Apri la finestra principale dell'applicazione e seleziona il componente **Aggiornamento**.
2. Clicca Ritorno ai database precedenti.

13.3. Configurazione delle impostazioni di aggiornamento

La procedura di aggiornamento opera secondo impostazioni che definiscono i seguenti aspetti:

- La sorgente da cui l'aggiornamento viene scaricato e installato (vedi 13.3.1 a pag. 160)
- La modalità operativa della procedura di aggiornamento ed i specifici elementi aggiornati (vedi 13.3.2 a pag. 163)
- La frequenza con cui l'aggiornamento è pianificato (vedi 6.7 a pag. 65)
- L'account per il quale avverrà l'aggiornamento (vedi 6.6 a pag. 64)
- Se gli aggiornamenti scaricati devono essere copiati in una directory locale (vedi 13.3.3 a pag. 164)
- Le azioni da compiere al termine dell'aggiornamento (vedi 13.3.4 a pag. 166)

Le sezioni seguenti prendono in esame questi aspetti in dettaglio.

13.3.1. Selezione di un'origine per l'aggiornamento

L'*origine degli aggiornamenti* è una certa risorsa contenente gli aggiornamenti per i database e per i moduli dell'applicazione di Kaspersky Anti-Virus. Le origini degli aggiornamenti possono essere server HTTP e FTP, cartelle locali o cartelle di rete.

L'origine di aggiornamento principale è costituita dai *server degli aggiornamenti di Kaspersky Lab*. Si tratta di speciali siti web contenenti gli aggiornamenti disponibili per i database e i moduli delle applicazioni per tutti i prodotti Kaspersky Lab.

Se non si è in grado di accedere ai server degli aggiornamenti di Kaspersky Lab (per esempio perché manca la connessione Internet), è possibile rivolgersi alla sede di Kaspersky Lab chiamando il numero +7 (495) 797-87-00 per richiedere i nominativi dei partner Kaspersky Lab in grado di fornire gli aggiornamenti in file compressi su dischetto o CD.

Attenzione!

Per richiedere gli aggiornamenti salvati su un supporto, è necessario specificare se si desiderano anche gli aggiornamenti dei moduli dell'applicazione.

È possibile copiare gli aggiornamenti da un disco e caricarli su un sito FTP o HTTP oppure salvarli in una cartella locale o di rete.

Selezionare l'origine dell'aggiornamento dalla scheda **Origine aggiornamento** (vedere Figura 52).

Come impostazione predefinita gli aggiornamenti sono scaricati dai server degli aggiornamenti di Kaspersky Lab. L'elenco degli indirizzo non può essere modificato. Durante l'aggiornamento, Kaspersky Anti-Virus chiama questo elenco, seleziona l'indirizzo del primo server e cerca di scaricare i file. Se lo scarico dei file dal primo server non va a buon fine, l'applicazione cerca di connettersi agli indirizzi successivi fino a quando l'operazione ha successo. L'indirizzo dal quale si riesce a scaricare gli aggiornamenti va automaticamente ad occupare la prima posizione dell'elenco. All'aggiornamento successivo, l'applicazione cercherà inizialmente di connettersi a questo server.

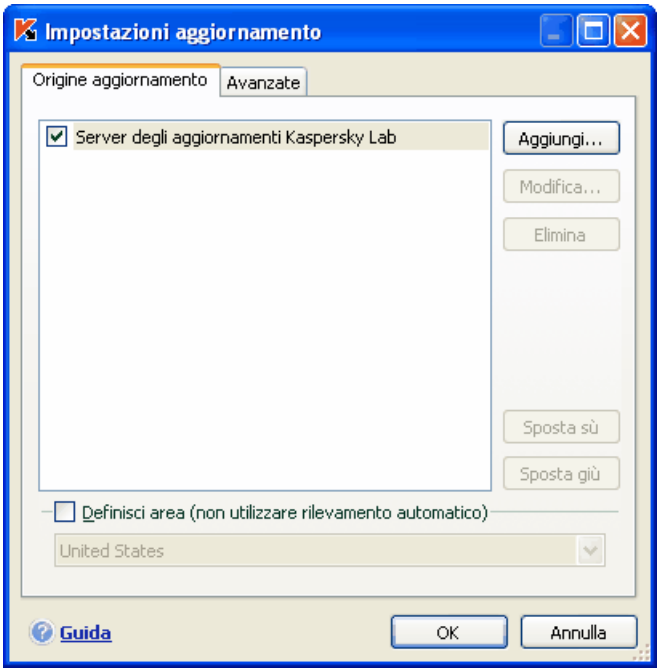


Figura 52. Selezione di un'origine per l'aggiornamento

Per scaricare gli aggiornamenti da un altro sito FTP o HTTP:

1. Fare clic su **Aggiungi**.
2. Nella finestra di dialogo **Seleziona origine aggiornamento**, selezionare l'FTP di destinazione o il sito HTTP o specificare un indirizzo IP, o indirizzo URL nel campo **Origine**. Selezionando un sito ftp come fonte di aggiornamento le impostazioni di autenticazione devono essere inserite nell'URL del server con il formato ftp://user:password@server.

Attenzione!

Se come origine degli aggiornamenti è stata selezionata una risorsa esterna alla LAN devi avere una connessione Internet per gli aggiornamenti.

Per scaricare l'aggiornamento da una cartella locale:

1. Fare clic su **Aggiungi**.
2. Nella finestra di dialogo **Seleziona origine aggiornamento**, seleziona una cartella o specifica il percorso completo di questa cartella nel campo **Origine**.

Kaspersky Anti-Virus aggiunge la nuova origine all'inizio dell'elenco e la abilita automaticamente.

Se sono state selezionate più risorse, l'applicazione cerca di connettersi ad esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco, e preleva gli aggiornamenti dalla prima disponibile. È possibile modificare l'ordine delle origini nell'elenco servendosi dei pulsanti **Sposta su** e **Sposta giù**.

Per modificare l'elenco, usare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. L'unico tipo di origine che non può essere modificato né eliminato sono i server degli aggiornamenti di Kaspersky Lab.

Se si prelevano gli aggiornamenti dai server di Kaspersky Labs, è possibile selezionare la posizione ottimale del server da cui scaricare i file. Kaspersky Lab dispone di server in diversi paesi. La scelta del server di Kaspersky Lab più vicino aiuta a risparmiare tempo e ad accelerare il prelievo degli aggiornamenti.

Per scegliere il server più vicino, selezionare la casella  **Definisci area (non utilizzare rilevamento automatico)** e selezionare quindi dall'elenco a discesa il paese più vicino al proprio paese di residenza. Se spunti questa casella gli aggiornamenti a partire dalla regione selezionata nell'elenco. Questa casella è deselezionata per impostazione e vengono usate le informazioni circa la regione contenute nel registro di sistema.

13.3.2. Selezione di un metodo di aggiornamento e cosa aggiornare

Durante la configurazione delle impostazioni di aggiornamento è importante definire cosa sarà aggiornato e con quale metodo.

Aggiorna oggetti (vedi Figura 53) definisce i componenti che saranno aggiornati:

- Database dell'applicazione
- Driver di rete che abilitano i componenti di protezione all'intercettazione sul traffico di rete
- Moduli del programma

I database dell'applicazione ed i driver del network vengono sempre aggiornati mentre i moduli dell'applicazione vengono aggiornati solo se configurati per questa operazione.

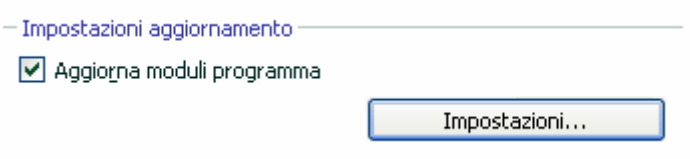


Figura 53. Selezione degli oggetti da aggiornare

Se si desidera scaricare e installare gli aggiornamenti dei moduli del programma:

Apri la finestra impostazioni dell'applicazione seleziona **Aggiornamento** e spunta **Aggiorna moduli programma**.

Se nell'origine prescelta sono disponibili aggiornamenti per i moduli del programma, apparirà sullo schermo una speciale finestra contenente la descrizione di tutti i cambiamenti dei moduli di programma. Su questa base puoi decidere se installare l'aggiornamento.

La Modalità di aggiornamento (vedi Figura 54) definisce come viene avviato. Seleziona una delle modalità seguenti sotto **Modalità di esecuzione**:

Automatica. Kaspersky Anti-Virus verifica la disponibilità degli aggiornamenti ad intervalli regolari (vedi 13.3.1 a pag. 160). Quando trova degli aggiornamenti recenti li scarica e li installa sul computer. Questa modalità è selezionata per impostazione predefinita.

Se una risorsa di rete è specificata come fonte di aggiornamento, Kaspersky Anti-Virus cerca di lanciare l'aggiornamento dopo un certo tempo come specificato nel precedente pacchetto di aggiornamento. Se come origine di

aggiornamento è stata selezionata una cartella locale, l'applicazione cerca di scaricare gli aggiornamenti da quest'ultima con la frequenza specificata nell'ultimo pacchetto di aggiornamento scaricato. Questa opzione consente a Kaspersky Lab di regolare la frequenza di aggiornamento del programma in caso di epidemie o di altre situazioni potenzialmente pericolose. L'applicazione riceverà regolarmente gli aggiornamenti più recenti dei database e dei moduli del software, impedendo ai programmi nocivi di penetrare nel computer.

Figura 54. Selezione di una modalità di esecuzione degli aggiornamenti

Pianificazione. L'aggiornamento è programmato per avviarsi in un momento preciso. La frequenza predefinita è una volta al giorno. Per modificare la pianificazione predefinita, clicca sul pulsante **Cambia…** vicino al titolo della modalità e apporta le modifiche desiderate nella finestra che si apre (per ulteriori informazioni, vedi 6.7 a pag. 65)

Manuale. Questa opzione consente di avviare Updater manualmente. Kaspersky Anti-Virus informa l'utente quando è necessario provvedere all'aggiornamento.

13.3.3. Distribuzione aggiornamenti

Se i computer di casa sono collegati in una rete domestica, non è necessario scaricare ed installare gli aggiornamenti individualmente, poiché ciò aumenterà notevolmente il traffico di rete. Puoi usare la caratteristica aggiorna distribuzione che consente di ridurre il traffico ritrovando gli aggiornamenti nei modi seguenti:

1. Uno dei computer della rete trova un pacchetto di aggiornamento dell'applicazione sui server di aggiornamento di Kaspersky Lab o da una diversa fonte web contenente un set degli aggiornamenti correnti. Gli aggiornamenti così recuperati vengono salvati in una cartella ad accesso pubblico.
2. Gli altri computer della rete accedono alla cartella ad accesso pubblico per recuperare gli aggiornamenti all'applicazione.

Per abilitare la distribuzione degli aggiornamenti spunta la casella **Aggiornare cartella di distribuzione** nella sezione **Avanzate** (vedi Figura 55) e nel campo sottostante specifica la cartella condivisa in cui verranno posti

gli aggiornamenti. Puoi inserire il percorso manualmente oppure selezionarlo dalla finestra che si apre facendo clic su **Sfoglia.** Se la casella è selezionata gli aggiornamenti verranno automaticamente copiati in essa.

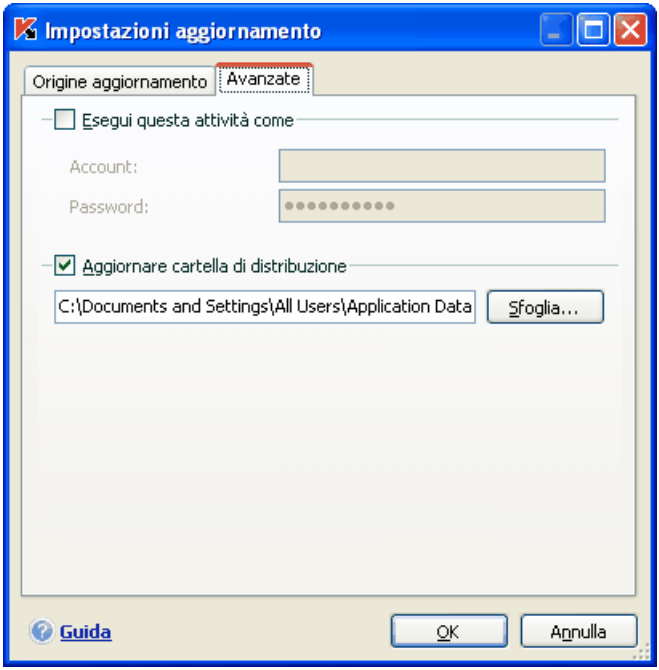


Figura 55. Impostazione dello strumento di Copia gli aggiornamenti

Si noti che Kaspersky Anti-Virus 7.0 recupera dai server di aggiornamento di Kaspersky Lab esclusivamente i pacchetti di aggiornamento relativi alla versione 7.0.

Se si desidera che altri computer nella rete si aggiornino dalla cartella contenente gli aggiornamenti copiati da Internet, attieniti alla seguente procedura:

1. Consenti l'accesso pubblico alla cartella.
2. Specifica la cartella di accesso pubblico quale origine degli aggiornamenti per gli altri computer di rete nelle impostazioni di aggiornamento.

13.3.4. Azioni post-aggiornamento

Ogni aggiornamento degli elenchi delle minacce contiene nuovi elementi che proteggono il computer dalle minacce più recenti.

Kaspersky Lab raccomanda di esaminare ogni volta gli *oggetti in quarantena* e gli *oggetti all'avvio* dopo l'aggiornamento del database.

Perché è necessario esaminare questi oggetti?

La cartella Quarantena contiene oggetti che il programma ha catalogato come sospetti o probabilmente infetti (vedi 15.1 a pag. 170). Utilizzando la versione più recente dei database, Kaspersky Anti-Virus potrebbe essere in grado di identificare la minaccia e di eliminarla.

Per impostazione predefinita, l'applicazione esamina gli oggetti in quarantena dopo ogni aggiornamento degli elenchi delle minacce. Si raccomanda inoltre di consultare periodicamente gli oggetti in quarantena poiché il loro stato può cambiare in seguito alle scansioni. Alcuni oggetti possono quindi essere ripristinati nelle posizioni originarie per continuare a lavorare con loro.

Per disabilitare la scansione degli oggetti in Quarantena, deselezionare la casella **Ripeti scansione Quarantine** nella sezione **Azione post-aggiornamento**.

Gli oggetti all'avvio sono di importanza vitale per la sicurezza del computer. Se uno di essi è infetto da un'applicazione nociva, potrebbe verificarsi un errore di avvio del sistema operativo. Kaspersky Anti-Virus è dotato di un'attività di scansione degli oggetti all'avvio per quest'area (vedi Capitolo 11 a pag. 135). Si raccomanda di pianificare un calendario di esecuzione per questa attività in modo da avviarlo automaticamente ad ogni aggiornamento dei database (vedi 6.7 a pag. 65).

CAPITOLO 14. GESTIONE DELLE CHIAVI

Kaspersky Anti-Virus abbisogna di un file chiave per operare. Quando compri il programma ti viene fornita questa chiave. Ti assicura il diritto di utilizzare il programma dal giorno in cui hai installato la chiave.

Senza la chiave, a meno che non sia stata attivata una versione di prova del programma, Kaspersky Anti-Virus lavorerà con un solo aggiornamento. Il programma non scaricherà alcun nuovo aggiornamento disponibile.

Se è stata attivata la versione di prova del programma, al termine del periodo di prova, Kaspersky Anti-Virus non lavorerà più.

All'esaurimento di una chiave il programma continuerà a funzionare ma non ti sarà possibile aggiornare i database dell'applicazione. Il computer continuerà ad essere scansionato e protetto dai componenti di protezione ma secondo la versione corrente al momento della scadenza della chiave. Non possiamo garantire che sarai protetto dai virus generati dopo il termine della chiave.

Per evitare che il tuo computer venga infettato da nuovi virus consigliamo di estendere la validità della tua chiave. Il programma ti informerà due settimane prima del termine di validità della chiave e in questo periodo il messaggio verrà ripetuto ogni volta che lo apri.

Le informazioni circa la chiave corrente sono mostrate sotto **Attivazione** (vedi Figura 56) nella finestra principale dell'applicazione. La sezione **Chiavi installate** mostra l'ID della chiave, il tipo (commerciale, di prova, per i beta test), numero di computer su cui installarla, data di scadenza e numero di giorni prima della scadenza. Clicca su Informazioni dettagliate della chiave per ulteriori informazioni.

Per vedere le clausole del contratto di licenza clicca su Visualizza contratto di licenza con l'utente finale. Per rimuovere una chiave dall'elenco clicca su Elimina Chiave.

Per acquistare o rinnovare una chiave:

1. Acquista una nuova chiave cliccando Acquista chiave (l'applicazione non è stata attivata) oppure Estendi chiave. La corrispondente pagina web conterrà tutte le informazioni per comprare una chiave dall'online di Kaspersky Lab o da un suo partner aziendale.

   Se acuisti online una chiave o un codice di attivazione ti sarà inviato via posta elettronica all'indirizzo specificato nel modulo d'ordine non appena eseguito il pagamento.

2. Installa la chiave cliccando Installa chiave sotto **Attivazione** nella finestra principale di Kaspersky Anti-Virus o **Attivazione** nel menù contestuale. Verrà avviata la procedura di impostazione guidata (vedi 3.2.2 a pag. 34).

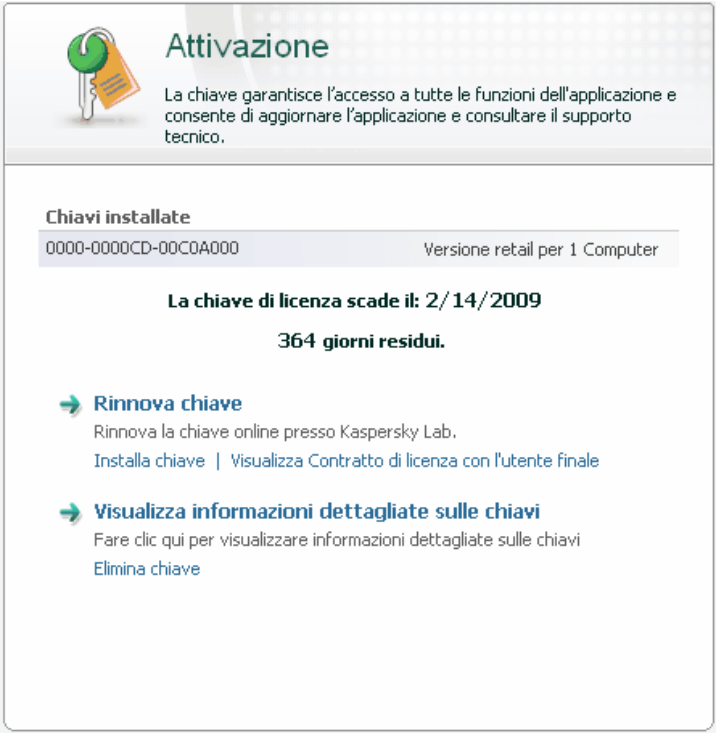


Figura 56. Gestione della chiave

Kaspersky Lab confeziona regolarmente offerte speciali per l'estensione della licenza dei propri prodotti. Controlla sul sito Kaspersky Lab nell'area **Prodotti → Vendita ed offerte speciali**.

CAPITOLO 15. OPZIONI AVANZATE

Kaspersky Anti-Virus è dotato di altre funzioni che ne espandono la funzionalità.

Il programma colloca alcuni oggetti in apposite aree di archiviazione al fine di garantire la massima protezione dei dati riducendo al minimo le perdite.

- La cartella Backup contiene copie degli oggetti modificati o eliminati da Kaspersky Anti-Virus (vedi 15.2 a pag. 174). Se un oggetto conteneva informazioni importanti e non è stato possibile recuperarlo completamente durante l'elaborazione antivirus, è possibile ripristinare l'oggetto dalla copia di backup.
- La Quarantena contiene oggetti potenzialmente infetti che non è stato possibile elaborare con le firme correnti (vedi 15.1 a pag. 170).

Si raccomanda di esaminare periodicamente l'elenco degli oggetti. Alcuni di essi infatti possono essere già obsoleti e altri possono essere stati ripristinati.

Alcune funzioni sono state ideate per aiutare l'utente durante l'uso del programma. Ad esempio:

- Il servizio di Supporto Tecnico offre un'assistenza completa per Kaspersky Anti-Virus (vedi 15.10 a pag. 205). Kaspersky offre una scelta di canali di supporto più vasta possibile: assistenza on-line, forum degli utenti e Conoscenze di Base.
- La funzione di Notifica serve per configurare le notifiche agli utenti relative a eventi chiave di Kaspersky Anti-Virus (vedi 15.9.1 a pag. 197). Può trattarsi di eventi di natura informativa o di errori da eliminare immediatamente, ed è estremamente importante esserne a conoscenza.
- La funzione di Auto-Difesa protegge i file del programma da qualsiasi modifica o danno perpetrati dagli hacker, blocca l'uso delle funzioni del programma da parte di amministrazioni remote e proibisce ad altri utenti del computer di eseguire determinate azioni in Kaspersky Anti-Virus (vedi 15.9.2 a pag. 201). Per esempio, la modifica del livello di protezione può influire considerevolmente sulla sicurezza del computer.
- La Gestione della configurazione dell'applicazione archivia i parametri di funzionamento dell'applicazione e facilita la replica di tali parametri su altri computer (vedi 15.9.3 a pag. 203) come pure un ripristino delle impostazioni di default (vedi 15.9.4 a pag. 204).

Il programma offre anche dettagliati report (vedi 15.3 a pag. 176) sul funzionamento di tutti i componenti di protezione, attività di scansione antivirus ed aggiornamenti.

Il monitoraggio delle porte può regolare quali moduli controllano i dati trasferiti sulle porte stesse (vedere 15.4 a pag. 184). La configurazione delle impostazioni del server proxy (vedere 15.7 a pag. 192) assicura l'accesso dell'applicazione ad Internet che è critica per alcuni componenti di protezione in tempo reale e per gli aggiornamenti.

Il disco di emergenza può agevolare il ripristino della funzionalità del computer dopo un'infezione (vedere 15.4 a pag. 184). Si tratta di una funzione particolarmente utile quando non si riesce a caricare il sistema operativo del computer in seguito al danneggiamento dei file di sistema da parte di un codice nocivo.

È possibile inoltre modificare l'aspetto di Kaspersky Anti-Virus e personalizzare l'interfaccia del programma (vedere 15.7 a pag. 192).

Di seguito esaminiamo in dettaglio queste funzioni.

15.1. Quarantena per gli oggetti potenzialmente infetti

La **Quarantena** è una speciale area di archiviazione che contiene gli oggetti potenzialmente infetti.

Gli **oggetti potenzialmente infetti** sono oggetti sospettati di contenere un virus o la variante di un virus.

Perché *potenzialmente infetti*? Non sempre è possibile stabilire con certezza se un oggetto sia infetto oppure no. Questo è dovuto a diverse ragioni:

- *Il codice dell'oggetto esaminato somiglia a una minaccia nota ma appare parzialmente modificato.*

  I database dell'applicazione contengono minacce già studiate da Kaspersky Lab. Se un programma nocivo è stato modificato e le variazioni non sono ancora state registrate nei database, Kaspersky Anti-Virus classifica l'oggetto contenente il programma nocivo modificato come potenzialmente infetto e indica la minaccia a cui il codice somiglia.

- *Il codice dell'oggetto intercettato ricorda per struttura un programma nocivo. Tuttavia nessun oggetto simile è ancora registrato nei database.*

  È possibile che si tratti di un nuovo tipo di minaccia, perciò Kaspersky Anti-Virus classifica l'oggetto come potenzialmente infetto.

L'analizzatore del *codice euristico* intercetta i virus potenziali. Questo meccanismo è abbastanza efficace e molto raramente produce un falso positivo.

Un oggetto potenzialmente infetto può essere intercettato e trasferito in Quarantena da File Anti-Virus, Mail Anti-Virus , Difesa proattiva o nel corso di una scansione antivirus.

Per mettere un oggetto in quarantena, clicca Quarantena nella notifica visualizzata al rilevamento di un oggetto potenzialmente infetto.

Quando un oggetto viene messo in Quarantena, esso non viene copiato ma trasferito. L'oggetto viene quindi eliminato dal disco o messaggio e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in uno speciale formato e pertanto non sono pericolosi.

15.1.1. Azioni da eseguire sugli oggetti in Quarantena

Il numero totale degli oggetti presenti nella cartella Quarantena è visualizzato nella sezione **Report e file dati** della finestra principale. Nella parte destra dello schermo si trova uno speciale riquadro **Quarantena** che indica:

- Il numero dei file potenzialmente infetti intercettati da Kaspersky Anti-Virus.
- Le dimensioni correnti della cartella Quarantena.

Da qui puoi eliminare tutti gli oggetti in Quarantena per mezzo del pulsante Elimina.

Per accedere agli oggetti in Quarantena:

Clicca Quarantena.

Nella scheda **Quarantena** (vedere Figura 57) è possibile compiere le seguenti azioni:

- Trasferire in Quarantena un file sospettato di contenere un'infezione che il programma non ha rilevato. Per questo clicca su **Aggiungi** e seleziona il file desiderato nella finestra di selezione. Il file viene.
- Esaminare e riparare tutti gli oggetti potenzialmente infetti in Quarantena per mezzo delle versione corrente dei database dell'applicazione facendo clic su **Scansione completa**.

  Dopo la scansione e l'eventuale riparazione di oggetti in Quarantena usando il suo stato può cambiare in infetto, potenzialmente *infetto,falso positivo, OK etc*.

Lo stato *infetto* significa che l'oggetto è stato riconosciuto come infetto ma non è stato possibile ripararlo. Si raccomanda di eliminare gli oggetti appartenenti a questa categoria.

Tutti gli oggetti classificati come *falso positivo* possono essere ripristinati poiché il precedente stato di *potenzialmente infetto* non è stato confermato dal programma in seguito alla nuova scansione.

- Ripristinare i file in una cartella selezionata dall'utente o nella cartella in cui si trovavano prima della Quarantena (impostazione predefinita). Per ripristinare un oggetto, selezionarlo dall'elenco e fare clic su **Ripristina**. Durante il ripristino di oggetti da archivi, database di posta e file in formato posta trasferiti in Quarantena, è necessario selezionare anche la directory in cui ripristinarli.

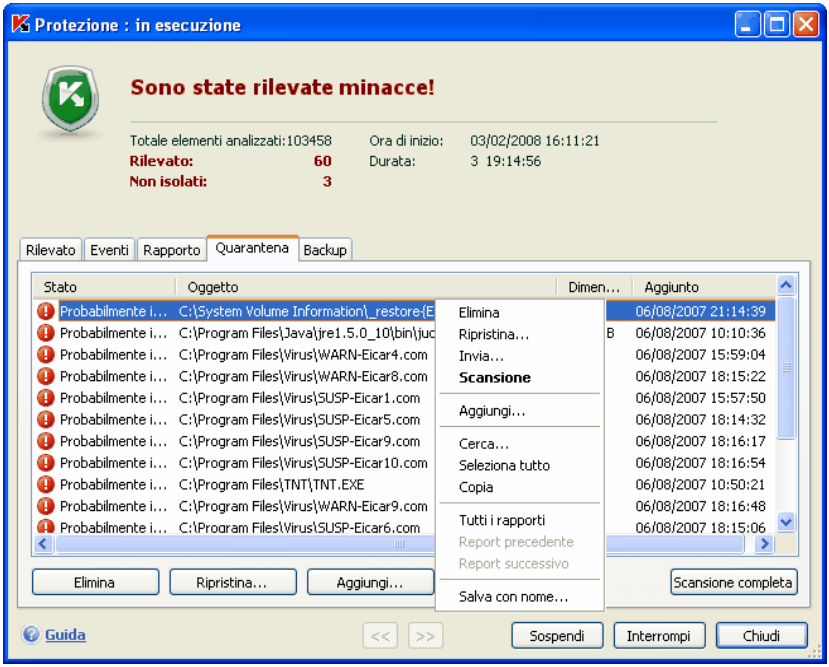


Figura 57. Elenco di oggetti in Quarantena

Suggerimento:

Si consiglia di ripristinare solo oggetti con lo stato *falso positivo, OK* e *disinfettato,* in quanto il ripristino di altri oggetti potrebbe determinare l'infezione del computer.

- Eliminare oggetti o gruppi selezionati di oggetti in Quarantena. Eliminare solo gli oggetti che non possono essere riparati. Per eliminare questi oggetti, selezionarli nell'elenco e fare clic su **Elimina**.

15.1.2. Configurazione della Quarantena

È possibile configurare le impostazioni di layout e funzionamento della Quarantena, in particolare:

- Impostare scansioni automatiche di oggetti in Quarantena dopo ogni aggiornamento degli elenchi delle minacce (per ulteriori informazioni vedi 13.3.4 a pag. 166).

> **Attenzione!**
>
> Se stai accedendo a Quarantena, il programma non è in grado di esaminare gli oggetti subito dopo l'aggiornamento dei database.

- Impostare la durata massima della conservazione degli oggetti in Quarantena.

  La durata predefinita è di 30 giorni, allo scadere dei quali gli oggetti vengono eliminati. È possibile modificare la durata di conservazione nella Quarantena o disabilitare del tutto questa limitazione.

Per fare questo:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Report e file dati.**
2. Nella sezione **Quarantena e Backup** (vedi Figura 58), digitare il tempo massimo allo scadere del quale gli oggetti saranno automaticamente eliminati. In alternativa deseleziona la casella per disabilitare la cancellazione automatica.

Figura 58. Configurazione del periodo di conservazione degli oggetti in Quarantena

15.2. Copie di Backup di oggetti pericolosi

A volte, in seguito alla riparazione, gli oggetti perdono la propria integrità. Se un file riparato contiene informazioni importanti e dopo la riparazione risulta parzialmente o completamente corrotto, si può tentare di ripristinare l'oggetto originario da una copia di backup.

Una **copia di backup** è una copia dell'oggetto pericoloso creata prima di riparare o eliminare l'originale. Le copie di backup vengono salvate nella cartella Backup.

La cartella **Backup** è una particolare area di archiviazione che contiene copie di oggetti pericolosi da riparare o eliminare. Il Backup consente di ripristinare l'oggetto originale in qualsiasi momento. I file in Backup vengono salvati in uno speciale formato e pertanto non sono pericolosi.

15.2.1. Azioni da eseguire sulle copie di backup

Il numero totale delle copie di backup a disposizione è visualizzato nella sezione **Report e File dati** della finestra principale. Nella parte destra della schermata si trova una speciale sezione **Backup** che indica:

- Il numero di copie di backup degli oggetti create da Kaspersky Anti-Virus.
- Le dimensioni correnti della cartella Backup.

Da qui è possibile eliminare tutte le copie di backup per mezzo del link **Cancella**.

Per accedere alle copie di oggetti pericolosi:

Clicca Backup.

Viene visualizzato un elenco di copie di backup al centro della scheda Backup (vedi Figura 59). Per ogni copia sono fornite le seguenti informazioni: il percorso completo ed il nome dell'oggetto, lo stato dell'oggetto assegnato dalla scansione e le sue dimensioni.

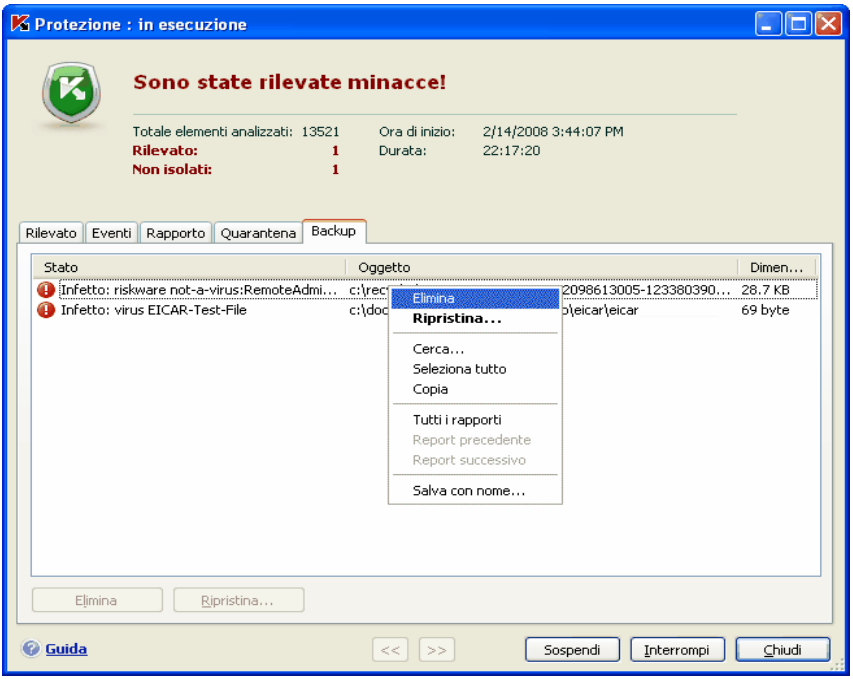


Figura 59. Copie di backup di oggetti eliminati o riparati

È possibile ripristinare le copie selezionate per mezzo del pulsante **Ripristina**. L'oggetto viene così ripristinato dalla cartella Backup con lo stesso nome dell'originale prima della riparazione.

Se esiste già un oggetto con quel nome nella posizione originaria (ciò è possibile se prima della riparazione è stata creata una copia dell'oggetto che si desidera ripristinare), viene visualizzato un apposito messaggio. È possibile quindi cambiare posizione all'oggetto da ripristinare oppure rinominarlo.

Si raccomanda di sottoporre l'oggetto a scansione antivirus subito dopo il ripristino. È possibile che le firme aggiornate consentano di ripulirlo senza perdere l'integrità del file.

Si sconsiglia di ripristinare le copie di backup degli oggetti solo se strettamente necessario. Ciò potrebbe provocare l'infezione del computer.

Si raccomanda di esaminare periodicamente la cartella Backup e di vuotarla servendosi del pulsante **Elimina**. È possibile inoltre configurare il programma in modo da eliminare automaticamente dal Backup le copie di più vecchia data (vedi 15.2.2 a pag. 176).

15.2.2. Configurazione delle impostazioni del Backup

È possibile definire la durata massima di conservazione nella cartella Backup.

La durata predefinita è di 30 giorni, allo scadere dei quali le copie vengono eliminate. È possibile inoltre modificare la durata di conservazione o disabilitare del tutto questa limitazione procedendo come segue:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Report e file dati**.
2. Impostare la durata della conservazione delle copie di backup nella sezione **Quarantena e Backup** (vedi Figura 58) nella parte destra della finestra. In alternativa deseleziona la casella per disabilitare la cancellazione automatica.

15.3. Rapporti

Le azioni dei componenti di Kaspersky Anti-Virus e le attività di scansione anti-virus sono registrate in appositi report.

Il numero totale dei report creati dal programma in un certo momento e le loro dimensioni totali in bite sono visualizzate nella sezione **Report e File dati** nella finestra principale del programma. Queste informazioni sono presentate nella sezione **Rapporto** *dei file*.

Per visualizzare i rapporti:

Clicca Rapporto.

La scheda Rapporto (vedi Figure 60) elenca i report più recenti di tutti i componenti, le attività di scansione e degli aggiornamenti eseguite durante la sessione corrente di Kaspersky Anti-Virus. Il loro stato è indicato vicino a ciascun componente od azione: per esempio, *in esecuzione, in pausa o completato*. Se si desidera visualizzare la cronologia completa della creazione dei report per la sessione corrente del programma, selezionare la casella ☑ **Mostra cronologia rapporto**.

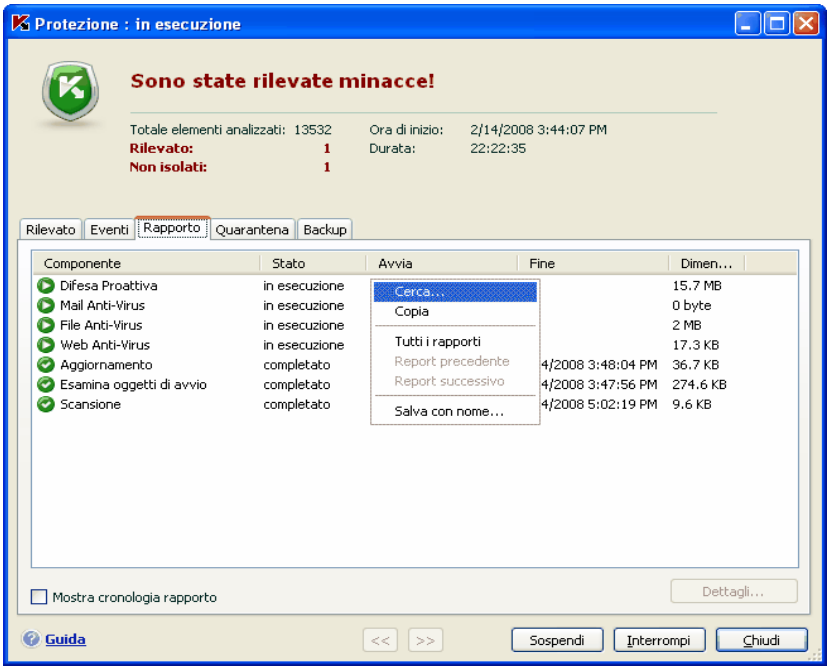


Figure 60. Rapporti sul funzionamento di un componente

Per consultare tutti gli eventi registrati nel report di un componente o attività:

Selezionare il nome del componente o attività nella scheda **Rapporto** e fare clic sul pulsante **Dettagli**.

Si apre una finestra contenente informazioni dettagliate sulle prestazioni del componente o attività selezionati. Le statistiche sulle prestazioni sono visualizzate nella parte superiore della finestra, mentre le informazioni dettagliate sono riportate nelle schede. Le schede sono diverse a seconda del componente o attività:

- La scheda **Rilevato** contiene un elenco di oggetti pericolosi individuati da un componente o da un'attività di scansione antivirus.
- La scheda **Eventi** visualizza gli eventi relativi al componente o attività.
- La scheda **Statistiche** contiene le statistiche dettagliate su tutti gli oggetti esaminati.
- La scheda **Impostazioni** visualizza le impostazioni utilizzate da componenti di protezione, scansioni antivirus o aggiornamenti dei database.

- Le schede **Registro** sono presenti solo nel report di Difesa proattiva e contengono informazioni su tutti i tentativi di modificare il registro del sistema operativo.

I report possono essere interamente esportati in formato testo. Questa funzione è utile nei casi in cui in un componente o attività si è verificato un errore impossibile da eliminare autonomamente, per il quale si necessita di assistenza tecnica. In tali casi è necessario inviare il report in formato .txt al servizio di Assistenza tecnica per consentire ai nostri specialisti di studiare approfonditamente il problema e risolverlo nel più breve tempo possibile.

Per esportare un report in formato testo:

Clicca **Azioni** → **Salva con nome** e specificare dove vuoi salvare il file del report.

Al termine del lavoro con il report, fare clic su **Chiudi**.

Esiste un pulsante **Azioni** su tutte le schede ad eccezione di **Impostazioni** e **Statistiche**, che può essere utilizzato per definire le reazioni agli oggetti presenti nell'elenco. Facendo clic su di esso, si apre un menu contestuale con i seguenti elementi di menu (il menu è diverso a seconda del componente; di seguito sono elencate tutte le opzioni possibili):

Disinfetta – il programma cerca di riparare l'oggetto pericoloso. Puoi lasciarlo nell'elenco per scansionarlo in seguito con database aggiornati o cancellarlo. Puoi applicare questa azione ad un singolo oggetto o a molti degli oggetti elencati.

Elimina gli oggetti pericolosi dal computer.

Elimina dall'elenco – elimina il record dell'oggetto riconosciuto dal report.

Aggiungi a zona attendibile – l'oggetto viene escluso dalla protezione. Si apre una finestra con una regola di esclusione per l'oggetto.

Vai a file – si apre la cartella in cui è stato salvato l'oggetto in Microsoft Windows Explorer.

Disinfetta tutto – tutti gli oggetti presenti nell'elenco vengono neutralizzati. Kaspersky Anti-Virus cerca di elaborare gli oggetti per mezzo dei database dell'applicazione.

Cancella tutto – il report sugli oggetti rilevati viene azzerato. Con questa funzione, tutti gli oggetti pericolosi rilevati restano nel computer.

Visualizza su www.viruslist.com – vengono cercate le descrizioni dell'oggetto nell'Enciclopedia dei Virus nel sito web di Kaspersky Lab.

Cerca – consente di inserire caratteri di ricerca per nome o stato degli oggetti in elenco.

Salva con nome – salva il report come file di testo.

Inoltre è possibile organizzare le informazioni visualizzate in ordine crescente o decrescente per ciascuna colonna cliccando sull'intestazione della colonna.

Per processare gli oggetti pericolosi riconosciuti da Kaspersky Anti-Virus premi il pulsante **Disinfetta** (per un oggetto o gruppo di oggetti) o **Disinfetta Tutto** (per processare tutti gli oggetti dell'elenco). Dopo che ogni oggetto è stato processato apparirà un messaggio sullo schermo. Qui dovrai decidere cosa fare con gli stessi in seguito.

Se spunti ☑ **Applica a tutti** nella finestra di notifica l'azione scelta verrà applicata a tutti gli oggetti con lo stato selezionato dall'elenco prima di essere processati.

15.3.1. Configurazione delle impostazioni dei report

Per configurare le impostazioni di creazione e salvataggio dei reports:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Report e File dati**.
2. Modifica le impostazioni sotto **Rapporto** (vedere Figura 61) come segue:
   - Consentire o disabilitare la registrazione di eventi informativi. Questi eventi di solito non sono rilevati ai fini della sicurezza. Per registrare gli eventi, selezionare la casella ☑ **Registra eventi non critici**.
   - Scegliere di salvare nel report solo gli eventi verificatisi successivamente all'ultima scansione. Questa impostazione consente di salvare spazio su disco riducendo le dimensioni del report. Se la casella ☑ **Mantieni solo eventi recenti** è selezionata, le informazioni contenute nel report saranno salvate ogni volta che si riavvia l'attività. Tuttavia saranno sovrascritte solo le informazioni non critiche.
   - Impostare la durata della conservazione dei report. La durata predefinita è di 30 giorni, allo scadere dei quali i report vengono eliminati. È possibile modificare la durata massima di conservazione o disabilitare del tutto questa limitazione.

Figura 61. Configurazione delle impostazioni dei report

15.3.2. La scheda *Rilevato*

Questa scheda (vedi Figura 62) contiene un elenco di oggetti pericolosi rilevati da Kaspersky Anti-Virus. Per ogni oggetto è indicato il nome completo, accompagnato dallo stato assegnatogli dal programma in seguito alla scansione o all'elaborazione.

Se si desidera che l'elenco contenga sia gli oggetti pericolosi sia quelli neutralizzati con successo, selezionare la casella **Mostra oggetti disinfettati**.

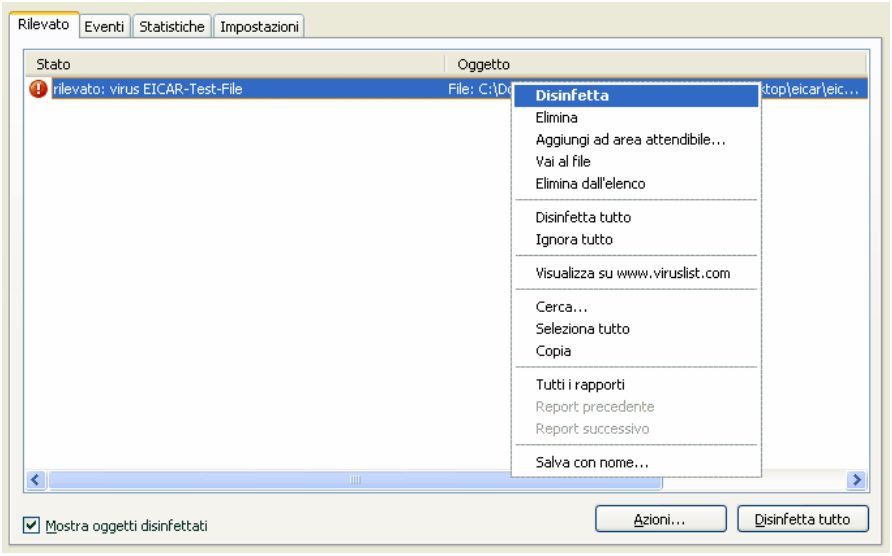


Figura 62. Elenco degli oggetti pericolosi rilevati

Gli oggetti pericolosi rilevati da Kaspersky Anti-Virus vengono processati con l'uso del pulsante **Disinfetta** (per l'oggetto o gruppo di oggetti selezionati) oppure **Disinfetta tutto** (per processare tutti gli oggetti dell'elenco). Dopo essere

stati processati verrà presentata una notifica sullo schermo, dovrai decidere quale azione dovrà essere fatta successivamente
Se spunti ☑ **Applica a tutti** nella finestra di notifica l'azione scelta verrà applicata a tutti gli oggetti aventi il medesimo stato selezionato dall'elenco prima di iniziare il controllo.

15.3.3. La scheda *Eventi*

Questa scheda (vedi Figura 63) contiene un elenco completo degli eventi importanti verificatisi durante il funzionamento di un componente, la scansione antivirus e gli aggiornamenti degli elenchi delle minacce non ignorati da una regola di controllo delle attività (vedi 10.1 a pag. 121).

Questi eventi possono essere:

Eventi critici – eventi di importanza critica che segnalano problemi di funzionamento del programma o vulnerabilità del computer. Per esempio, *virus rilevato*, *errore di funzionamento*.

Eventi importanti – eventi da approfondire poiché riflettono situazioni importanti nel funzionamento del programma. Per esempio, *terminato.*

Messaggi informativi – messaggi di riferimento che di solito non contengono informazioni rilevanti. Per esempio, *OK, non elaborato*. Questi eventi sono riportati nel registro eventi solo se spunti la casella ☑ **Tutti i rapporti**.

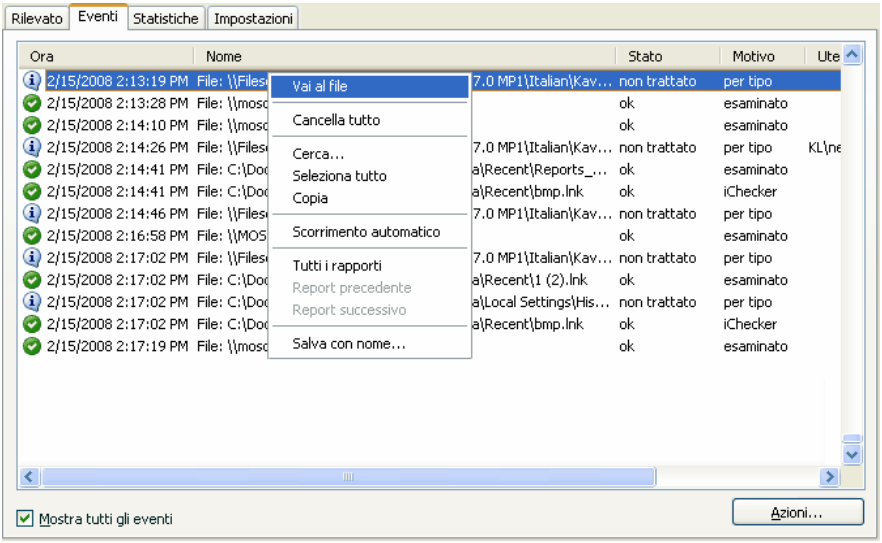


Figura 63. Eventi che si verificano durante il funzionamento di un componente

Il formato di visualizzazione degli eventi nel registro può variare in base al componente o all'attività. Per ogni attività di aggiornamento sono riportate le seguenti informazioni:

- Nome dell'evento
- Nome dell'oggetto interessato dall'evento
- L'ora in cui si è verificato l'evento
- Le dimensioni del file caricato

Per le attività di scansione antivirus, il registro degli eventi contiene il nome dell'oggetto esaminato e lo stato assegnatogli in seguito alla scansione/elaborazione.

15.3.4. La scheda Statistiche

Questa scheda (vedi Figura 64) contiene le statistiche dettagliate sui componenti e le attività di scansione antivirus. Da questa finestra risulta:

- Quanti oggetti sono stati esaminati in cerca di tratti pericolosi nella sessione corrente di un componente o dopo il completamento di un'attività. Il numero degli archivi, dei file compressi e degli oggetti protetti da password e corrotti esaminati.
- Quanti oggetti pericolosi sono stati rilevati, non riparati, eliminati e trasferiti in Quarantena.

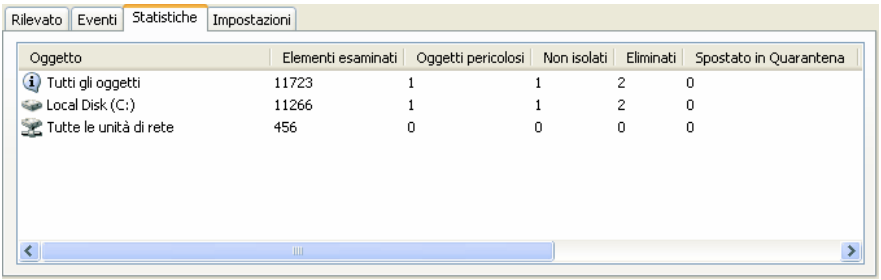


Figura 64. Statistiche dei componenti

15.3.5. La scheda *Impostazioni*

La scheda **Impostazioni** (vedi Figura 65) visualizza l'elenco completo delle impostazioni dei componenti, delle scansioni antivirus e degli aggiornamenti del programma. È possibile vedere il livello di esecuzione di un componente o di una scansione antivirus, le azioni compiute sugli oggetti pericolosi o le impostazioni

in uso per gli aggiornamenti del programma. Usare il link Modifica impostazioni per configurare il componente.

È possibile configurare impostazioni avanzate per le scansioni antivirus:

- Stabilire la priorità delle attività di scansione in caso di sovraccarico sul processore. L'impostazione predefinita per **Concedi risorse ad altre applicazioni** è spuntata. Con questa funzione, il programma individua il carico sul processore e sui sottosistemi del disco per l'attività di altre applicazioni. Se il carico sul processore aumenta considerevolmente e impedisce alle applicazioni dell'utente di funzionare normalmente, il programma riduce l'attività di scansione. In tal modo si riduce il tempo di scansione e si liberano risorse per le applicazioni dell'utente.

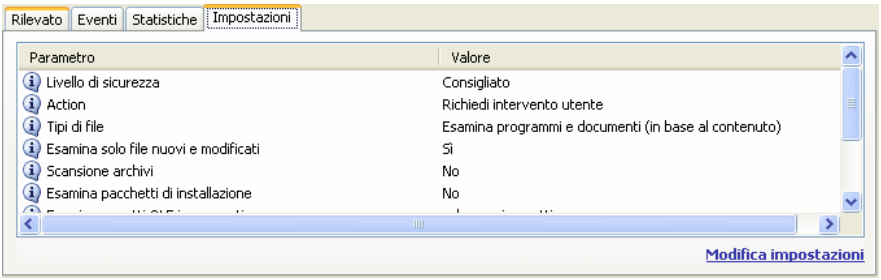


Figura 65. Impostazioni dei componenti

- Impostare la modalità operativa del computer per il periodo successivo al completamento della scansione antivirus. È possibile configurare il computer in modo da spegnersi, riavviarsi o funzionare in standby o in modalità di risparmio. Per selezionare un'opzione, fare clic con il pulsante sinistro del mouse sull'ipertesto fino a visualizzare l'opzione desiderata.

  Questa funzione può risultare utile se, per esempio, si avvia una scansione antivirus al termine della giornata lavorativa e non si desidera aspettarne la conclusione.

  Tuttavia, per poter utilizzare questa funzione è necessario eseguire i seguenti passaggi supplementari: prima di lanciare la scansione è necessario disabilitare le richieste di password per gli oggetti esaminati, se abilitata, e abilitare l'elaborazione automatica degli oggetti pericolosi. Le funzioni interattive del programma saranno quindi disabilitate e il programma non richiederà più l'intervento dell'utente interrompendo il processo di scansione.

15.3.6. La scheda *Registro*

Il programma registra nella scheda **Registro** le operazioni tentate sulle chiavi di registro dall'avvio del programma (vedi Figura 66), a meno che non vengano inibite da una regola (vedi 10.3.2 a pag. 132).

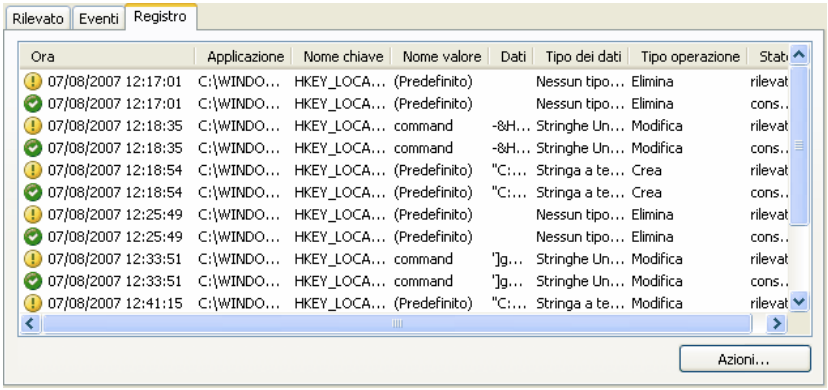


Figura 66. Lettura e modifica degli eventi del registro di sistema

La scheda riporta il nome completo della chiave, il suo valore, il tipo di dati e le informazioni relative all'operazione che ha avuto luogo: l'azione tentata, l'ora e l'eventuale autorizzazione.

15.4. Disco di emergenza

Kaspersky Anti-Virus dispone di uno strumento per creare un disco di emergenza.

Il disco di emergenza è progettato per consentire il ripristino della funzionalità del sistema dopo un attacco virale che ha danneggiato i file di sistema rendendo impossibile l'avvio del sistema operativo. Il disco include:

- File di sistema di Microsoft Windows XP Service Pack 2
- Una serie di utilità diagnostiche per il sistema operativo
- I file del programma Kaspersky Anti-Virus
- I file contenenti i database

Per creare un disco di emergenza:

1. Aprire la finestra principale dell'applicazione e selezionare **Scansione**.

2. Fare clic sul link Crea disco di emergenza per procedere alla creazione del disco.

Il disco di emergenza viene creato per il computer sul quale è stato creato. L'utilizzo del disco su altri computer può determinare conseguenze imprevedibili, poiché contiene informazioni sui parametri relativi ad un computer specifico (le informazioni sui settori di boot, ad esempio).

La creazione di un disco di emergenza è possibile solo con Microsoft Windows XP o Microsoft Windows Vista. Non è possibile creare dischi di emergenza sui computer che eseguono Microsoft Windows XP Professional x64 Edition e Microsoft Windows Vista x64.

15.4.1. Creazione di un disco di emergenza

Attenzione! Per creare un disco di emergenza è necessario disporre del disco di installazione di Microsoft Windows XP Service Pack 2.

Per creare il Disco di emergenza è necessario il programma **PE Builder**.

Prima di creare un disco di emergenza è necessario installare PE Builder sul computer.

Una un'apposita procedura guidata ti guiderà nella creazione del disco di emergenza. Consiste di una serie di finestre/passaggi fra i quali navigare servendosi dei pulsanti **Indietro** e **Avanti**. Per completare la procedura guidata fare clic su **Fine**. Il pulsante **Annulla** serve per interrompere in qualsiasi momento la procedura.

Passaggio 1. La scrittura del disco

Per creare un disco di emergenza indicare i percorsi alle seguenti cartelle:

- Cartella del programma PE Builder.
- Cartella in cui sono stati salvati i file del disco di emergenza prima di masterizzare il CD/DVD.
- Se non è la prima volta che si crea un disco di emergenza, questa cartella contiene già una serie di file creati la volta precedente. Per usare i file salvati in precedenza, selezionare la casella corrispondente.

> Osservare che i file del disco di emergenza creati precedentemente contengono i vecchi database dell'applicazione. Per ottimizzare la scansione antivirus e ripristinare il sistema, si raccomanda di aggiornare i database e di creare un nuovo disco di emergenza.

- Il CD di installazione di Microsoft Windows XP Service Pack 2.

Dopo aver indicato i percorsi alle cartelle richieste, fare clic su **Avanti**. PE Builder si avvia e ha inizio il processo di creazione del disco di emergenza. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.

Passaggio 2. Creazione di un file .iso

Dopo che PE Builder ha completato la creazione dei file del disco di emergenza, si apre la finestra **Crea file .iso**.

Il file .iso è un'immagine su CD del disco di emergenza salvata come archivio. La maggior parte dei programmi di masterizzazione CD è in grado di riconoscere correttamente i file .iso (Nero, per esempio).

Se non è la prima volta che si crea un disco di emergenza, è possibile selezionare il file .iso dal disco precedente selezionando **File .iso esistente**.

Passaggio 3. Predisposizione alla masterizzazione

Durante la procedura guidata viene chiesto di scegliere se masterizzare il disco di emergenza su CD: adesso o più tardi.

Se si decide di masterizzare immediatamente il disco, specificare se si desidera formattare il disco prima di procedere, selezionando la casella corrispondente. Questa opzione è disponibile solo se si usano dischi CD-RW.

Per avviare la masterizzazione del CD fare clic sul pulsante **Avanti**. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.

Passaggio 4. Completamento del disco di emergenza

Questa finestra della procedura guidata informa che il disco di emergenza è stato creato correttamente.

15.4.2. Uso del disco di emergenza

Osservare che Kaspersky Anti-Virus funziona in modalità provvisoria solo se la finestra principale è aperta. Chiudendo la finestra principale si chiude anche il programma.

Bart PE, il programma predefinito, non supporta i file .chm o i browser di Internet, pertanto in modalità provvisoria non è possibile visualizzare la Guida di Kaspersky Anti-Virus o i link dell'interfaccia del programma.

Se in seguito a un attacco di virus è impossibile caricare il sistema operativo, procedere come segue:

1. Creare un disco di emergenza utilizzando Kaspersky Anti-Virus su un computer non infetto.
2. Inserire il disco di emergenza nell'unità CD del computer infetto e riavviare. Microsoft Windows XP SP2 si avvia con l'interfaccia di Bart PE.
3. Bart PE è dotato di assistenza di rete incorporata per usare la LAN. All'avvio del programma, viene richiesto se si desidera abilitarlo. Se non è necessario aggiornare i file, disabilitare il supporto di rete.
4. Per aprire Kaspersky Anti-Virus, fare clic su **Start→Programmi→Kaspersky Anti-Virus 7.0**.
5. Si apre la finestra principale di Kaspersky Anti-Virus. In modalità provvisoria è possibile accedere solo alle scansioni antivirus e agli aggiornamenti degli elenchi delle minacce dalla LAN (se era stato abilitato il supporto di rete in Bart PE).
6. Avviare la scansione antivirus.

Nota che i database dell'applicazione vengono usati come default dalla data in cui è stato creato il disco di emergenza. Per questa ragione raccomandiamo di aggiornare i database prima di avviare la scansione.

Occorre anche notare che l'applicazione userà soltanto i database aggiornati con il disco di emergenza durante la corrente sessione, prima di riavviare il computer.

Attenzione!

Se sono stati individuati oggetti infetti o potenzialmente infetti e questi sono stati processati e posti in Quarantena o nel contenitore dei Backup allora consigliamo di completare, durante la sessione corrente, il controllo di questi oggetti con un disco di emergenza.

Altrimenti questi oggetti andranno perduti al riavvio del computer.

15.5. Creazione di un elenco delle porte monitorate

Durante l'uso di componenti come Mail Anti-Virus, Web Anti-Virus vengono monitorati i flussi di dati trasmessi mediante protocolli specifici attraverso determinate porte aperte del computer. Così, per esempio, Mail Anti-Virus analizza le informazioni trasmesse per mezzo del protocollo SMTP mentre Web Anti-Virus analizza quelle trasmesse mediante HTTP.

Il pacchetto del programma include un elenco delle porte più utilizzate per la trasmissione della posta e del traffico HTTP. È possibile aggiungere una nuova porta o disabilitare il monitoraggio di una esistente disabilitando in tal modo il rilevamento di oggetti pericolosi del traffico che passa attraverso la porta in questione.

Per modificare l'elenco delle porte monitorate procedere come segue:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Monitoraggio del traffico**.
2. Cicca **Porte monitorate**.
3. Aggiorna l'elenco delle porte monitorate nella finestra di dialogo **Impostazioni Porta** (vedi Figura 67).

Figura 67. Elenco delle porte monitorate

Questa finestra presenta un elenco di porte monitorate da Kaspersky Anti-Virus. Per scansionare il flusso di dati vai su tutte le porte aperte del network, seleziona l'opzione **Controlla tutte le porte.** Per modificare manualmente l'elenco delle porte monitorate seleziona **Controlla solo le porte selezionate**.

Per aggiungere una nuova porta all'elenco delle porte monitorate:

1. Fare clic sul pulsante **Aggiungi** nella finestra **Impostazioni porta**.
2. Digitare il numero della porta e una descrizione della stessa negli appositi campi della finestra **Nuova porta**.

Per esempio, il computer possiede una porta non standard attraverso la quale vengono scambiati dati con un computer remoto per mezzo del protocollo HTTP. Web Anti-Virus monitora il traffico HTTP. Per analizzare questo traffico in cerca di codici nocivi, è possibile aggiungere la porta a un elenco di porte controllate.

All'avvio di uno qualsiasi dei suoi componenti, Kaspersky Anti-Virus apre la porta 1110 come porta di ascolto per tutte le connessioni in entrata. Se in quel momento la porta è occupata, seleziona le porte 1111, 1112, ecc.

Se usi contemporaneamente Kaspersky Anti-Virus ed un firewall di un'altra società devi configurare il firewall per permettere l'acceso del processo *avp.exe* (il processo interno di Kaspersky anti-Virus) a tutte le porte elencate sopra.

Per esempio diciamo che il tuo firewall contiene una regola per *iexplorer.ex* che consente a quel processo di stabilire una connessione sulla porta 80.

Quando Kaspersky Anti-Virus intercetta la query di connessione avviata da *iexplorer.ex* sulla porta 80, la trasferisce su avp.exe che a rotazione tenta di stabilire una connessione con la pagina web in maniera indipendente. Se non c'à la regola di permesso per *avp.exe* il firewall bloccherà quella query. L'utente non potrà avere accesso alla pagina web.

15.6. Scansione delle connessioni crittografate

Le connessioni effettuate con il protocollo SSL proteggono lo scambio di dati tramite Internet. Il protocollo SSL è in grado di identificare le parti che si scambiano dati tramite certificati elettronici, crittografare i dati trasferiti e garantirne l'integrità durante il trasferimento.

Queste funzioni del protocollo vengono utilizzate dai pirati informatici per diffondere programmi nocivi, poiché quasi tutti i programmi antivirus non esaminano il traffico SSL.

Kaspersky Anti-Virus 7.0 offre l'opzione di esaminare il traffico SSL alla ricerca di virus. In caso di tentativo di connessione protetta ad una risorsa Web, verrà visualizzata una notifica sullo schermo (vedi Figura 68) che richiede un intervento dell'utente.

Essa contiene informazioni sul programma che ha avviato la connessione protetta, unitamente all'indirizzo remoto ed alla porta remota. Selezionare una delle opzioni sotto riportate per continuare o interrompere la scansione:

- **Elabora** – esamina il traffico alla ricerca di virus in caso di connessione protetta ad un sito Web.
- **Ignora** – continua la connessione protetta senza esaminare il traffico alla ricerca di virus.

Per applicare l'azione selezionata a tutti i futuri tentativi di stabilire una connessione SSL, selezionare **Applica**.

Figura 68. Notifica su rilevamento di una connessione SSL

Per esaminare le connessioni crittografate, Kaspersky Anti-Virus sostituisce il certificato di sicurezza richiesto con un certificato firmato dall'applicazione stessa. In alcuni casi, i programmi che stabiliscono la connessione non accetteranno questo certificato e la connessione non può essere stabilita. Nei seguenti casi di consiglia di selezionare l'opzione **Ignora** relativamente alla notifica riguardo la scansione di una connessione protetta:

- Durante il collegamento ad una risorsa Web attendibile, ad esempio la pagina Web della propria banca, dal quale gestire il proprio conto corrente. In questo caso, è importante che l'autenticità del certificato della banca venga confermata.
- Se il programma che stabilisce la connessione verifica il certificato del sito web al quale si accede. Ad esempio, MSN Messenger verifica l'autenticità della firma digitale di Microsoft Corporation quando stabilisce una connessione al server.

È possibile configurare le impostazioni della scansione SSL dalla scheda **Monitoraggio del traffico** nella finestra delle impostazioni dell'applicazione (vedi Figura 69):

Controlla tutte le connessioni crittografate – esamina tutto il traffico in entrata tramite protocollo SSL alla ricerca di virus.

Richiesta di scansione al rilevamento di una nuova connessione criptata – visualizza un messaggio che richiede l'intervento dell'utente ogniqualvolta viene stabilita una connessione SSL.

Non controllare connessioni crittografate – non esamina il traffico in entrata tramite protocollo SSL alla ricerca di virus.

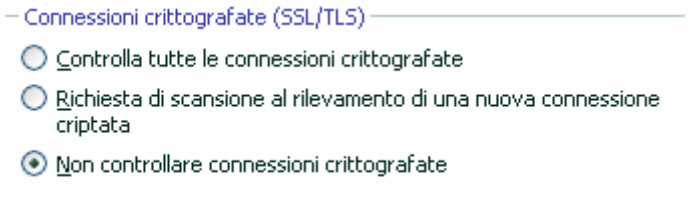


Figura 69. Configurare la scansione su connessioni sicure

15.7. Configurazione del Server Proxy

La connessione ad un server proxy può essere configurata usando la sezione **Server Proxy** (vedi Figura 70) nella finestra impostazioni dell'applicazione (se la connessione a Internet avviene attraverso un proxy). Kaspersky Anti-Virus utilizza questa impostazioni per molti moduli di protezione in tempo reale e per aggiornare i database ed i moduli dell'applicazione.

Se usi un serve proxy per connetterti ad Internet spunta **Usa Server Proxy** e configura le seguenti impostazioni secondo necessità:

- Seleziona i parametri del server proxy da usare:

  Usa impostazioni proxy Microsoft Internet Explorer. Se questa opzione è selezionata le impostazioni del server proxy sono riconosciute automaticamente usando il protocollo WPAD (Web Proxy Auto-Discovery Protocol). Se il protocollo non riesce a determinare l'indirizzo Kaspersky Anti-Virus usa le impostazioni specificate per Microsoft Internet Explorer.

  Usa impostazioni server proxy specificate: usa un server proxy diverso da quello specificato nelle impostazioni della connessione al browser. Digita un indirizzo IP o il nome di un dominio nel campo **Indirizzo** e il numero della porta del server proxy nel campo **Porta**.

  Per non usare un server proxy per gli aggiornamenti da directory locali o di rete, spunta **Ignora server proxy per indirizzi locali.**

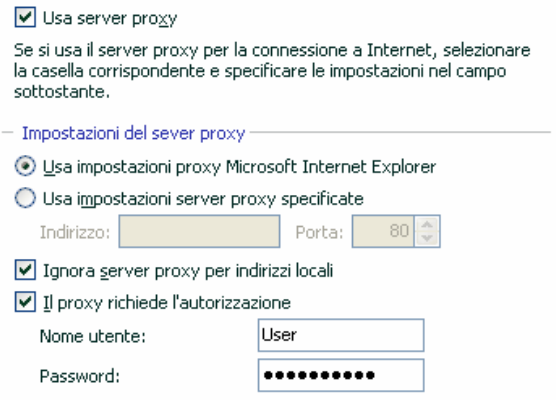


Figura 70. Configurazione di Server Proxy

- Specifica se il server proxy utilizza l'autenticazione. L'Autenticazione è una procedura per verificare le informazioni dell'utente allo scopo di controllarne l'accesso.

  Se è richiesta l'autenticazione per connettersi al server proxy spunta **Il proxy richiede l'autorizzazione** ed inserisci nome utente e password nei campi appropriati. Verrà eseguita una autorizzazione NTLM seguita da una autorizzazione BASIC.

  Se la casella non è spuntata l'autorizzazione NTLM verrà condotta usando il login con cui viene avviata l'azione (come per un aggiornamento, vedi Sezione 6.6 a pag. 64).

  Se il server proxy richiede una autorizzazione ma il nome utente e la password non sono indicati o rifiutati dal proxy per qualsiasi ragione, verrà presentata una finestra di dialogo che richiederà nome utente e password. Se l'autorizzazione ha esito positivo lo specifico nome utente e password verranno ricordati per un uso successivo. Altrimenti verrà nuovamente richiesta l'autorizzazione.

  Premendo il pulsante **Annulla** nella finestra di dialogo di richiesta di autorizzazione, l'origine di aggiornamento corrente viene sostituita con la successiva in elenco; i parametri di autenticazione specificati in quella finestra o definiti nell'interfaccia del programma saranno ignorati. Pertanto, l'applicazione tenterà un'autenticazione NTLM in base all'account utilizzato per lanciare l'attività.

Se usi un server ftp per gli aggiornamenti viene eseguita una connessione passiva al server. SE questa connessione ritorna un errore viene tentato di stabilire una connessione attiva.

Per impostazione il tempo di connessione al server degli aggiornamenti è di 1 minuto. Se la connessione cade si tenterà la connessione ad un altro server di aggiornamento al termine del periodo. Questo si ripete fino a che l'operazione ha successo oppure fino a che tutti i server degli aggiornamenti sono stati contattati.

15.8. Configurazione dell'interfaccia di Kaspersky Anti-Virus

Kaspersky Anti-Virus offre la possibilità di modificare l'aspetto del programma creando e utilizzando nuovi stili. È possibile inoltre configurare l'uso degli elementi di interfaccia attiva come l'icona della barra delle applicazioni e i messaggi a comparsa.

Per configurare l'interfaccia del programma procedere come segue:

Apri la finestra impostazioni dell'applicazione e seleziona **Aspetto** (vedi Figura 71).

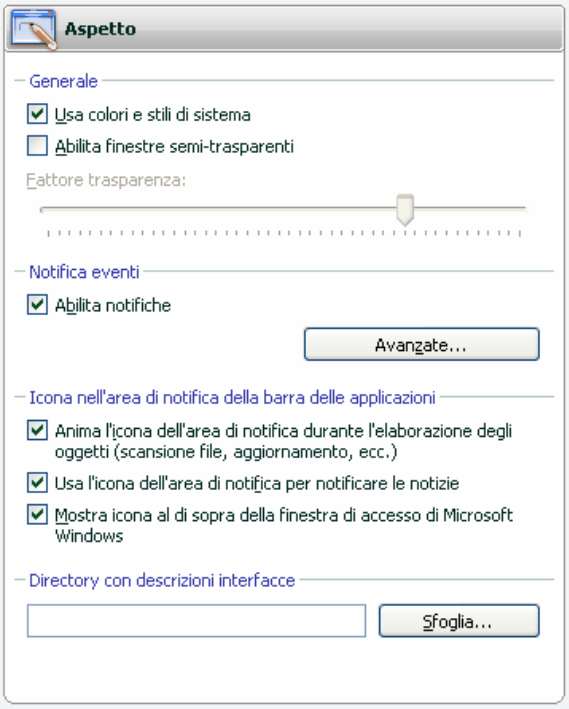


Figura 71. Configurazione delle impostazioni dell'interfaccia del programma

Nella parte destra della finestra delle impostazioni, puoi configurare:

- Componenti grafici definiti dsall'utente e schema colori nell'interfaccia dell'applicazione.

  Per impostazione predefinita, l'interfaccia grafica usa un insieme di colori e stili. Questi possono essere modificati spuntando **Usa colori e stili di sistema**. Questo abilita gli stili specificati nella configurazione dei temi del display.

  Tutti i colori, i font, le icone ed i testi usati nell'Interfaccia di Kaspersky Anti-Virus sono configurabili. Possono essere anche creati skin personalizzati per l'applicazione. L'applicazione stessa può essere localizzata in un'altra lingua. Per mappare una skin, immettere la directory contenente la descrizione corretta nel campo **Directory con descrizioni interfacce**. Usare il pulsante **Sfoglia** per selezionare una directory

- Fattore di trasparenza dei messaggi pop-up.

  Tutte le operazioni di Kaspersky Anti-Virus che richiedono l'informazione dell'utente o il suo intervento immediato sono comunicate in un messaggio a comparsa sopra l'icona della barra delle applicazioni. Le finestre del messaggio sono trasparenti in modo da non interferire con il lavoro. Se si muove il cursore sul messaggio, la trasparenza svanisce. Il grado di trasparenza di questi messaggi può essere modificato regolando la scala del **Fattore trasparenza** sulla posizione desiderata. Per eliminare la trasparenza del messaggio, deselezionare la casella **Abilita finestre semi-trasparenti**.

- Animazione dell'icona sulla barra delle applicazioni.

  A seconda dell'operazione eseguita dal programma, l'icona della barra di sistema cambia. Per esempio, durante la scansione di uno script compare sullo sfondo dell'icona una piccola rappresentazione, mentre durante la scansione di un messaggio e-mail compare una busta. L'animazione delle icone è abilitata per impostazione predefinita. Se si desidera disabilitare l'animazione, deselezionare la casella **Anima l'icona dell'area di notifica durante l'elaborazione degli oggetti**. Da quel momento in poi l'icona rappresenta solo lo stato di protezione del computer: se la protezione è abilitata l'icona è a colori, mentre se la protezione è in pausa o disabilitata l'icona diventa grigia.

- Notifica delle novità da parte di Kaspersky Lab.

  Per impostazione predefinita se ricevi delle news viene presentata una icona speciale sulla barra di sistema che, quando spuntata, mostra il contenuto della notizia. Per disabilitare la notifica deseleziona **Usa l'icona dell'area di notifica per notificare le notizie.**

- Visualizzazione dell'icona di Kaspersky Anti-Virus all'avvio del sistema operativo.

  Per impostazione questo indicatore appare nell'angolo superiore destro dello schermo quando si carica il programma. Esso ti informa che il tuo computer è protetto da tutti i tipi di minaccia. Se non vuoi usare questo indicatore deseleziona ☑ **Mostra l'icona al di sopra della finestra di accesso di Microsoft Windows**

Osservare che le impostazioni dell'interfaccia di Kaspersky Anti-Virus definite dall'utente non vengono salvate in caso di ripristino delle impostazioni predefinite o di disinstallazione del programma.

15.9. Uso delle opzioni avanzate

Kaspersky Anti-Virus offre le seguenti funzioni avanzate (vedi Figura 72):

- avvio di Kaspersky Anti-Virus all'avvio del sistema operativo (vedere 15.11 a pag. 206);
- notifica all'utente di certi eventi dell'applicazione (vedere 15.9.1 a pag. 197);
- Auto-Difesa di Kaspersky Anti-Virus da modulo chiudi, modifica, protezione password dell'applicazione (vedere 15.9.2 a pag. 201);
- esportazione/importazione delle impostazioni di funzionamento di Kaspersky Anti-Virus (vedere 15.9.3 a pag. 203);
- ripristino delle impostazioni predefinite (vedere 15.9.4 a pag. 204).

Per configurare queste funzioni:

Apri la finestra impostazioni dell'applicazione e seleziona **Servizio**.

Nella parte destra dello schermo è possibile specificare se abilitare le funzioni supplementari durante l'uso del programma.

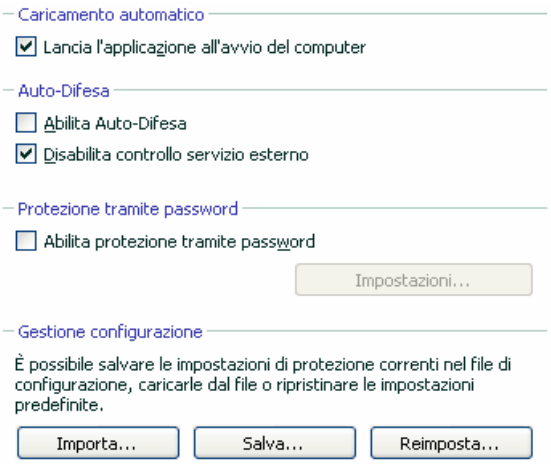


Figura 72. Configurazione di Opzioni Avanzate

15.9.1. Notifiche eventi di Kaspersky Anti-Virus

Durante l'uso di Kaspersky Anti-Virus si verificano diversi tipi di evento. Le notifiche corrispondenti possono essere informative o contenere dati importanti. Per esempio, un messaggio può informare dell'avvenuto aggiornamento del programma oppure registrare l'errore di un componente che deve essere risolto immediatamente.

Per ricevere gli aggiornamenti sul funzionamento di Kaspersky Anti-Virus è possibile utilizzare la funzione di notifica.

Le notifiche possono essere trasmesse in vari modi:

- In forma di messaggi pop-up sopra l'icona del programma nella barra di sistema.
- Con segnali acustici.
- Con e-mail.
- Con un registro eventi.

Per usare questa funzione procedere come segue:

1. Selezionare la casella ☑ **Abilita notifiche** sotto **Notifica eventi** nella sezione Aspetto della finestra impostazione dell'applicazione (vedi Figura 71).

2. Definisci i tipi di evento per cui vuoi ricevere la notifica di Kaspersky Anti-Virus ed il metodo di consegna della stessa (vedere 15.9.1.1 a pag. 198).
3. Configura le impostazioni di consegna della notifica via email, se questo è il metodo di notifica da usare (vedere 15.9.1.2 a pag. 199).

15.9.1.1. Tipi di eventi e metodo di consegna della notifica

Durante l'uso di Kaspersky Anti-Virus, possono verificarsi i seguenti tipi di eventi:

Notifiche critiche – sono eventi di importanza cruciale. Si raccomanda di abilitare gli avvisi, poiché questo tipo di eventi segnala la presenza di problemi di funzionamento del programma o di vulnerabilità della protezione del computer. Per esempio, *database dell'applicazione corrotti* o *licenza scaduta*.

Errori funzionali – sono eventi che impediscono l'attività dell'applicazione. Ad esempio nessuna chiave o database.

Notifiche importanti – sono eventi che devono essere investigati poiché riflettono importanti situazioni nell'operatività del programma. Ad esempio *protezione disabilitata o computer non scansionato per molto tempo*.

Notifiche informative - sono messaggi che non contengono informazioni importanti. Ad esempio *disinfettati tutti gli oggetti pericolosi.*

Per specificare gli eventi da comunicare e le modalità di notifica:

1. Apri la finestra impostazioni dell'applicazione e seleziona Aspetto (vedi Figura 71).
2. Spunta ☑ **Abilita Notifiche** sotto **Notifica Eventi** e vai sulle impostazioni avanzate cliccando **Avanzate**.

È possibile configurare i seguenti metodi di notifica per gli eventi sopra elencati nella finestra di dialogo **Impostazioni di notifica eventi** (vedi Figura 73):

- *Messaggi pop-up* sopra l'icona del programma nella barra di sistema, contenenti informazioni sull'evento verificatosi.

  Per usare questo tipo di notifica, selezionare la casella ☑ nella sezione **Area commenti** dell'evento del quale si desidera essere informati.

- Segnale acustico

  Se si desideri che l'avviso sia accompagnato da un segnale acustico, selezionare la casella ☑ **Suono** dall'evento.

- Notifica E-mail

  Per utilizzare questo tipo di notifica, selezionare la casella **E-mail** dall'evento del quale si desidera essere informati, e configurare le impostazioni di invio degli avvisi (vedere 15.9.1.2 a pag. 199).

- *Registro eventi*

  Per registrare le informazioni a proposito degli eventi avvenuti spunta la casella nella colonna **Registro** e configura le impostazioni del registro eventi 15.9.1.3 a pag. 201).

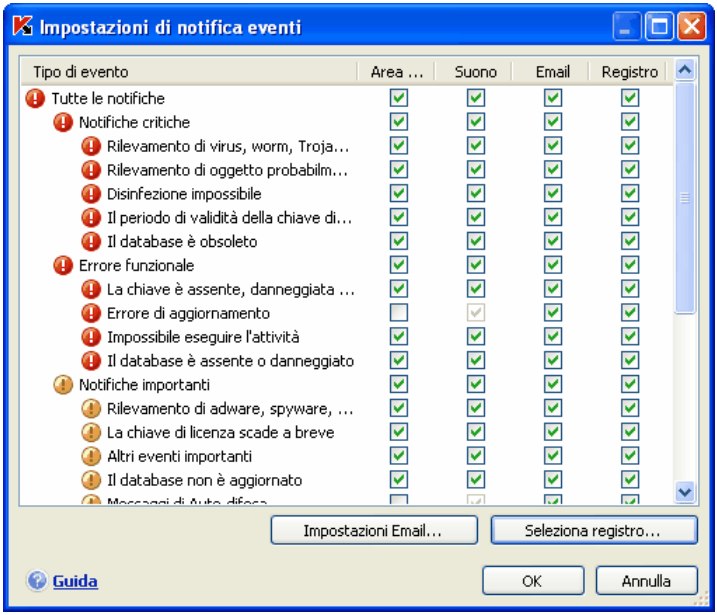


Figura 73. Eventi del programma e metodi di notifica

15.9.1.2. Configurazione delle notifiche via e-mail

Dopo aver selezionato gli eventi (vedi 15.9.1.1 a pag. 198) dei quali si desidera essere informati per e-mail, è necessario configurare la consegna dell'avviso procedendo come segue:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Aspetto** (vedi Figura 71).
2. Clicca **Avanzate** sotto **Notifica Eventi**.

3. Usa la finestra **Impostazioni di notifica eventi** (vedi Figura 73) per spuntare gli eventi che dovrebbero innescare la notifica e-mail nella colonna **E-mail**.

4. Nella finestra che si apre (vedi Figura 74) quando clicchi su **Impostazioni E-mail**, configura le seguenti impostazioni per le notifiche e-mail:

   - Impostare la notifica di invio per **Da: Indirizzo E-mail**.
   - Specificare l'indirizzo e-mail a cui inviare gli avvisi in **A: Indirizzo E-mail**.
   - Impostare il metodo di consegna della notifica per e-mail in **Modalità invio**. Se si desidera che il programma invii il messaggio non appena l'evento si verifica, selezionare **Immediatamente quando l'evento si verifica**. Per la notifica di eventi entro un determinato periodo di tempo, impostare il calendario di invio dei messaggi informativi facendo clic su **Cambia**. Gli invii quotidiani sono l'impostazione predefinita.

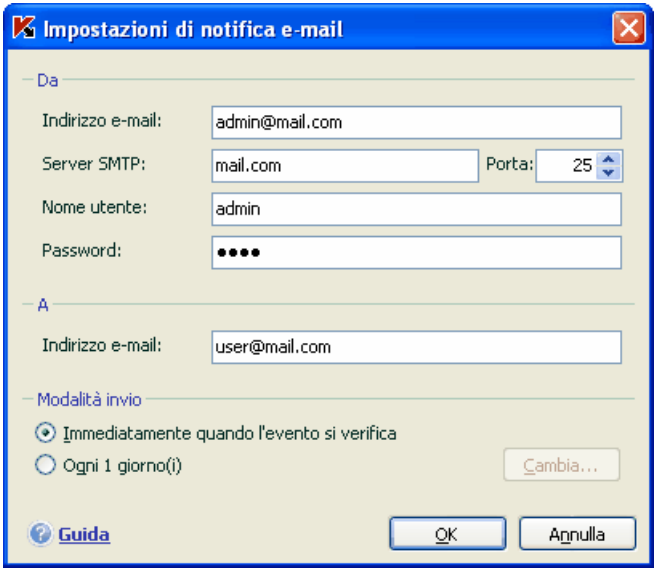


Figura 74. Configurazione impostazioni notifiche e-mail

15.9.1.3. Configurazione delle impostazioni del registro eventi

Per configurare queste impostazioni:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Aspetto** (vedi Figura 71).
2. Clicca **Avanzate** sotto **Notifica Eventi**.

Usa la finestra **Impostazioni di notifica eventi** per selezionare l'opzione di log informativo per un evento e clicca il pulsante **Seleziona registro**.

Kaspersky Anti-Virus ha la possibilità di registrare l'informazione circa l'evento che sorge mentre il programma è funzionante, sia nel log degli eventi generali di Microsoft Windows (**Applicazioni**) o in uno dedicato di Kaspersky Anti-Virus (**Registro eventi Kaspersky**).

I registri possono essere visti nel **Visualizzatore Eventi** di Microsoft Windows che puoi aprire attraverso **Start/Pannello di controllo/Strumenti di amministrazione/Visualizzatore eventi.**

15.9.2. Auto-Difesa e limitazioni d'accesso

Kaspersky Anti-Virus è una applicazione che garantisce la protezione del computer dai programmi nocivi e, proprio per questo, è spesso oggetto di attacchi da parte di programmi nocivi che cercano di bloccarne l'attività o perfino di eliminarlo dal computer.

Inoltre è possibile che più utenti si servano di un unico computer, non tutti ugualmente esperti nell'uso. Lasciare libero accesso al programma e alle sue impostazioni, pertanto, riduce considerevolmente la sicurezza del computer.

Per garantire la stabilità del sistema operativo, il programma è stato dotato di meccanismi di protezione automatica, protezione dall'accesso remoto e protezione mediante password.

Sui computer dotati di sistema operativo a 64-bit e Microsoft Windows Vista l'auto-difesa è disponibile solo per evitare che i file propri del programma sui drive locali e sul registro di sistema sia modificati o cancellati.

Per abilitare Auto-Difesa:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Servizio** (vedi Figura 72).
2. Effettuare le seguenti configurazioni nell'area **Auto-Difesa**:

Abilita Auto-Difesa. Se questa casella è selezionata, il programma protegge i propri file, processi nella memoria e voci del registro di sistema dalla cancellazione o dalla modifica.

Disabilita controllo servizio esterno. Se questa casella è selezionata, qualsiasi tentativo di uso del programma da parte di amministrazioni remote viene bloccato.

Affinché itool di amministrazione remota (come RemoteAdmin) possano accedere a Kaspersky Anti-Virus, devono essere aggiunti all'elenco delle applicazioni attendibili e l'impostazione **Non controllare attività applicazione** dovrebbe essere abilitata (vedere 6.9.2 a pag. 74).

In presenza di qualsiasi azione tra quelle sopra elencate, viene visualizzato un messaggio sopra l'icona del programma nella barra di sistema (se il servizio di notifica non è stato disabilitato dall'utente).

Per proteggere il programma mediante password, selezionare la casella **Abilita protezione tramite password** nell'area con lo stesso nome. Clicca sul pulsante **Impostazioni…** per aprire la finestra **Protezione tramite password** e digita la password e l'ambito che la restrizione all'accesso coprirà (vedi Figura 75). Puoi bloccare qualsiasi operazione del programma, ad eccezione della notifica di rilevamento di oggetti pericolosi, o impedire l'esecuzione di qualsiasi tra le seguenti azioni:

- Modifica delle impostazioni dell'applicazione.
- Uscita dal programma in esecuzione.
- Arresto/Sospensione dei componenti di protezione o delle operazioni di scansione.

Ciascuna delle azioni sopra elencate riduce la sicurezza del computer ed è quindi necessario stabilire quali tra gli utenti del computer sono sufficientemente attendibili da poter compiere tali azioni.

Selezionando questa opzione, ogni volta che un utente del computer cerca di eseguire le azioni selezionate, il programma richiede una password.

Figura 75. Impostazioni della password di protezione del programma

15.9.3. Importazione ed esportazione delle impostazioni di Kaspersky Anti-Virus

Kaspersky Anti-Virus offre la possibilità di importare ed esportare le impostazioni dell'applicazione.

Questa funzione risulta particolarmente utile nei casi in cui, per esempio, il programma è installato sia nel computer di casa sia in quello dell'ufficio. È possibile configurare le impostazioni preferite del programma sul computer di casa, salvare queste impostazioni su un disco e, servendosi della funzione di importazione, caricarle sul computer in ufficio. Le impostazioni vengono salvate in uno speciale file di configurazione.

Per esportare le impostazioni correnti del programma:

1. Apri la finestra impostazioni del programma e seleziona la sezione **Servizio** (vedi Figura 72).
2. Clicca sul pulsante **Salva** nella sezione **Gestione Configurazione**.
3. Digita un nome per il file di configurazione e seleziona una destinazione in cui salvarlo.

Per importare le impostazioni da un file di configurazione:

1. Apri la finestra impostazioni del programma e seleziona la sezione **Servizio**.
2. Clicca sul pulsante **Importa** e seleziona il file dal quale vuoi importare le impostazioni di Kaspersky Anti-Virus.

15.9.4. Ripristino delle impostazioni predefinite

È possibile ripristinare le impostazioni di default del programma in qualsiasi momento. Esse infatti sono considerate ottimali e consigliate dagli esperti di Kaspersky Lab. Questo può avvenire dalla procedura guidata:

Per ripristinare le impostazioni di protezione:

1. Apri la finestra impostazioni dell'applicazione e seleziona **Servizio** (vedi Figura 72).
2. Clicca sul pulsante **Reimposta** nella sezione **Gestione configurazione**.

La finestra elenca i componenti del programma le cui impostazioni sono state cambiate dall'utente. Verranno mostrate anche le eventuali e speciali impostazioni create per i componenti.

Esempi di impostazioni speciali potrebbero essere un elenco di indirizzi sicuri usato da Kaspersky Anti-Virus, l'esclusione di regole create i componenti del programma, regole applicative per l'Auto-Difesa.

Questi elenchi vengono creati man mano che si utilizza il programma, in base alle attività individuali e ai requisiti di sicurezza. Questo processo di solito richiede tempo, pertanto si consiglia di salvare tali impostazioni prima di ripristinare le impostazioni predefinite del programma.

Il programma salva per impostazione predefinita tutte le impostazioni personalizzate dell'elenco (sono deselezionate). Se non desideri salvare una delle impostazioni, selezionare la casella corrispondente.

Al termine della configurazione delle impostazioni, premere il pulsante **Avanti**. Si apre la procedura guidata (vedere 3.2, pg. 33). Seguire le istruzioni.

Al termine della procedura guidata, per tutti i componenti viene impostato il livello di protezione **Consigliato**, con l'eccezione delle impostazioni che decidi di mantenere. Vengono applicate inoltre le impostazioni configurate con la procedura guidata.

15.10. Supporto Tecnico

Informazioni circa il supporto tecnico reso disponibile da Kaspersky Anti-Virus sono fornite sotto Supporto (vedi Figura 76) nella finestra principale dell'applicazione.

La sezione superiore presenta informazioni generali dell'applicazione, data di pubblicazione del database come pure un sommario del sistema operativo del tuo computer.

Se dovesse sorgere un problema durante il funzionamento di Kaspersky Anti-Virus, per prima cosa verifica che istruzioni circa l'inconveniente riscontrato non siano presenti nell'aiuto o nella Knowledge Base sul sito web del Supporto Tecnico di Kaspersky Lab. La Knowledge Base è una sezione separata del sito del Supporto Tecnico e comprende consigli per i prodotti di Kaspersky Lab e le risposte alle domande più frequenti. Prova ad usare questa risorsa per una risposta alla tua domanda o una soluzione ad essa. Clicca su **Assistenza Web** per spostarsi sulla Knowledge Base.

Se non trovi una soluzione al tuo problema nella Guida, nella Knowledge Base o nel Forum per gli utenti ti consigliamo di contattare il Supporto Tecnico di Kaspersky Lab.

Nota che devi essere un utente registrato di una versione commerciale di Kaspersky Anti-Virus per ottenere il supporto tecnico. Nessun supporto è fornito per le versioni di prova.

La registrazione dell'utente avviene attraverso la procedura guidata di attivazione (vedere 3.2.2, pg. 34), se l'applicazione è stata attivata con un codice di attivazione. Verrà assegnato un ID cliente ed al termine della registrazione che puoi vedere sotto **Supporto** (vedere Figura 76) della finestra principale. Il numero cliente è un ID personale che viene richiesto per il supporto telefonico o dalla modulistica presente sul sito web.

Se viene utilizzato un file della chiave di attivazione registrati direttamente su Technical Support web site.

Un nuovo servizio detto Assistenza personalizzata fornisce agli utenti l'accesso ad una sezione personale del Supporto Tecnico sul web. La Vetrina Personale ti abilita a:

- inviare richieste al Supporto Tecnico senza collegarsi;
- scambiare messaggi con il Supporto Tecnico via email;
- monitorare le richieste in tempo reale;
- vedere la cronistoria delle tue richieste al Supporto Tecnico;

- ottenere una copia di backup del file della chiave.

Usa il link Sottoporre una domanda per inviare con un modulo on-line la tua richiesta al Supporto Tecnico. Entra nell'area Assistenza personalizzata sul sito del Supporto Tecnico che si apre e completa il modulo di richiesta.

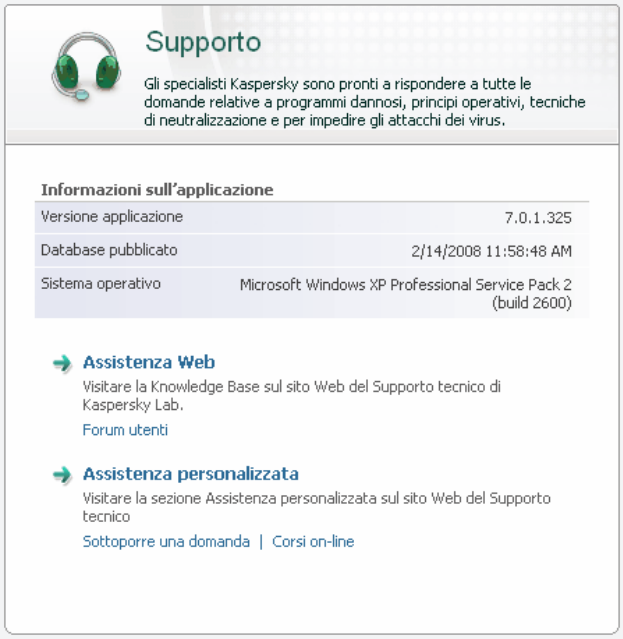


Figura 76. Informazioni sul Supporto Tecnico

Per una assistenza urgente usa il numero telefonico fornito nella Guida (vedere B.2 a pag. 243). Il supporto telefonico è sempre attivo (24 ore su 24 ore per 7 giorni la settimana) in Russo, Inglese, Francese, Tedesco e Spagnolo.

Il link Corsi online fornisce ulteriori informazioni sugli eventi di training per prodotti Kaspersky Lab.

15.11. Chiusura dell'applicazione

Se è necessario chiudere Kaspersky Anti-Virus seleziona Esci nel menù contestuale dell'applicazione (vedi 4.2 a pag. 43). Ciò causerà lo scarico dell'applicazione dalla RAM il che significa che il tuo computer non sarà più protetto.

Qualora fossero aperte delle connessioni di rete al momento della chiusura, verrà presentato un messaggio che informa che queste connessioni sono state interrotte. Ciò è richiesto affinché l'applicazione si chiuda correttamente. La disconnessione avviene automaticamente dopo 10 secondi oppure quando viene cliccato **Sì**. La maggior parte di queste connessioni vengono ristabilite dopo un certo periodo di tempo.

Nota che qualsiasi download in corso durante l'interruzione della connessione viene altrettanto interrotto a meno che non stia usando un download manager . Per ottenere il file occorre che tu riavvii il download.

Puoi evitare che la connessione venga interrotta cliccando **NO** nella finestra di notifica. Di conseguenza l'applicazione continuerà a funzionare.

Se l'applicazione viene arrestata, la protezione può essere riabilitata riavviando Kaspersky Anti-Virus selezionando **Start → Tutti i programmi → Kaspersky Anti-Virus 7.0 → Kaspersky Anti-Virus 7.0**.

La protezione ripartirà automaticamente in seguito ad un reboot del sistema operativo. Per abilitare questa modalità seleziona **Servizio** (vedi Figura 72) nella finestra impostazioni dell'applicazione e spunta ☑ **Lancia l'applicazione all'avvio del computer** sotto **Caricamento automatico.**

CAPITOLO 16. USO DEL PROGRAMMA DALLA RIGA DI COMANDO

Kaspersky Anti-Virus può essere utilizzato anche dalla riga di comando eseguendo le seguenti operazioni:

- Avvio, arresto, pausa e ripristino dell'attività dei componenti dell'applicazione
- Avvio, arresto, pausa e ripristino delle scansioni antivirus
- Ottenimento di informazioni sullo stato corrente di componenti, attività e statistiche
- Scansione di oggetti selezionati
- Aggiornamento dei database e dei moduli del programma
- Accesso alla Guida per consultare la sintassi dei prompt di comando
- Accesso alla Guida per consultare la sintassi dei comandi

La sintassi della riga di comando è la seguente:

```
avp.com <command> [Impostazioni]
```

Devi accedere al programma dal prompt dei comandi dalla cartella di installazione del programma o specificando il percorso a avp.com.

Possono essere usati come **<comandi>** i seguenti:

ACTIVAE	Attiva l'applicazione via Internet usando un codice di attivazione
ADDKEY	Attiva l'applicazione usando un file di chiave (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
START	Avvia un componente od una azione

PAUSE	Mette in pausa un componente o una azione (il comando può essere eseguito solo se viene inserita la impostata nell'interfaccia del programma)
RESUME	Riavvia un componente o attività
STOP	Termina un componente o attività (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
STATO	Visualizza lo stato del componente o attività correnti
STATISTICS	Visualizza le statistiche del componente o attività
HELP	Fornisce indicazioni sulla sintassi dei comandi e sull'elenco dei comandi
SCAN	Esegue la scansione antivirus di oggetti
UPDATE	Avvia l'aggiornamento del programma
ROLLBACK	Ritorna all'ultimo aggiornamento eseguito (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
EXIT	Chiude il programma (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
IMPORT	Importa le impostazioni di Kaspersky Anti-Virus (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
EXPORT	Esporta le impostazioni di Kaspersky Anti-Virus

Ogni comando corrisponde alle impostazioni specifiche del componente di Kaspersky Anti-Virus.

16.1. Attivazione dell'applicazione

Puoi attivare il programma in due modi:

- via Internet usando un codice di attivazione (comando ATTIVAZIONE)
- usando un file con la chiave (comando ADDKEY)

Sintassi di comando:

```
ACTIVATE <codice_attivazione>
ADDKEY <nome_file> /password=<la_tua_password>
```

Descrizione dei parametri:

<codice_attivazione>	Il codice di attivazione del programma fornito con l'acquisto
<nome_file>	Nome del file della chiave con l'estensione *.key*
<la_tua_password>	La password impostata con l'interfaccia di Kaspersky Anti-Virus
Nota che non puoi eseguire il comando **ADDKEY** senza digitare la password	

Esempio

```
avp.com ACTIVATE 00000000-0000-0000-0000-000000000000
avp.com ADDKEY 00000000.key /password=<la_tua_password>
```

16.2. Gestione di componenti del programma e attività

Sintassi dei comandi:

```
avp.com <command> <profilo|nome_azione>
[/R[A]:<report_file>]
avp.com STOP |PAUSE <profile|nome_azione>
/password=<la_tua_password> [/R[A]:<report_file>]
```

Descrizione parametri:

<command>	Puoi gestire i componenti Kaspersky Anti-Virus e le azioni dal prompt dei comandi con i comandi seguenti: **START** – carica un componente di protezione o una azione **STOP** – arresta un componente di protezione in tempo reale o una azione **PAUSE** – mette in pausa un componente di protezione in tempo reale o una azione **RESUME** – riavvia un componente di protezione o una azione **STATISTICS** – statistica a schermo circa l'operazione del componente di protezione in tempo reale o azione Nota che non puoi eseguire i comandi PAUSE o STOP senza inserire la password
<profilo | nome_azione>	Puoi specificare ogni componente di protezione in tempo reale, moduli dei componenti, scansioni su richiesta o aggiornamenti per il valore del **<profilo>** (i valori standard usati nel programma sono mostrati nella tabella sottostante) Puoi specificare il nome ogni scansione su richiesta o aggiornare una azione con il valore del **<nome_azione>**
<la_tua_password>	La password impostata nell'interfaccia del programma
/R[A]:<report_file>	**R:<report_file> -** registra solo gli eventi importanti nel report **/RA:<report_file> -** registra tutti gli eventi nel report Puoi usare un percorso assoluto o relativo per il file. Se il parametro non è definito i risultati della scansione sono presentati sullo schermo con tutti gli eventi

A <profilo> viene assegnato uno dei seguenti valori:

RTP	Tutti i componenti di protezione Il comando avp.com START RTP avvia tutti i componenti di protezione in tempo reale se la protezione è completamente disabilitata (vedi 6.1.2 pag 60) o in pausa (vedi 6.1.1 pag 59). Questo comando avvierà qualsiasi componente di protezione in tempo reale messo in pausa da GUI o dal comando PAUSE dal prompt dei comandi Se il componente è stato disabilitato da GUI o dal comando STOP dal prompt dei comandi, il comando avp.com START RTP non lo avvierà. Per avviarlo devi eseguire il comando avp.com START <profilo> digitando per <profilo> il valore per lo specifico componente di protezione.
FM	File Anti-Virus
EM	Mail Anti-Virus
WM	Web Anti-Virus Valori per i sottocomponenti di Web Anti-Virus **httpscan** – scans http traffic **sc** – scans scripts
BM	Difesa Proattiva Valori per i sottocomponenti di Difesa Proattiva **pdm** – application activity analysis
UPDATER	Per aggiornare
SCAN_OBJECTS	Attività di scansione antivirus
SCAN_MY_COMPUTER	Attività sul Mio Computer

SCAN_CRITICAL_AREAS	Attività sulle aree critiche
SCAN_STARTUP	Attività sugli oggetti di avvio
SCAN_QUARANTENA	Attività sugli oggetti in Quarantena
SCAN_ROOTKIT	Attività sui rootkit
I componenti e le azioni avviate dal prompt dei comandi sono eseguiti con le impostazioni configurate nell'interfaccia del programma.	

Esempi:

Per abilitare File Anti-Virus, digitare la seguente stringa nel prompt di comando:

```
avp.com START FM
```

Per visualizzare lo stato corrente di Difesa proattiva sul computer, digitare il testo seguente nel prompt di comando:

```
avp.com STATUS BM
```

Per terminare un'attività di scansione di Risorse del computer dal prompt di comando, digitare:

```
avp.com STOP SCAN_MY_COMPUTER
/password=<la_tua_password>
```

16.3. Scansioni antivirus

L'avvio della scansione antivirus di una determinata area e l'elaborazione degli oggetti nocivi dal prompt di comando generalmente appare così:

```
avp.com SCAN [<oggetto scansionato>] [<azione>] [<tipo
file>] [<esclusione>] [<file configurazione>]
[<impostazioni report>] [<impostazioni avanzate>]
```

Per eseguire la scansione di oggetti è possibile utilizzare anche le attività create in Kaspersky Anti-Virus avviando quella desiderata dal prompt di comando (vedere 16.1 a pag. 210). L'attività viene eseguita con le impostazioni configurate nell'interfaccia del programma.

Descrizione dei parametri:

<table>
<tr><td colspan="2"><object scanned> - questo parametro produce un elenco degli oggetti che saranno sottoposti alla scansione in cerca di codici nocivi.

Può includere diversi valori dall'elenco fornito, separati da uno spazio.</td></tr>
<tr><td><files></td><td>Elenco dei percorsi ai file e/o cartelle da sottoporre a scansione antivirus. Puoi inserire percorsi assoluti o relativi. Gli elementi dell'elenco devono essere separati da uno spazio.

Note:

• Se il nome dell'oggetto contiene uno spazio, esso deve essere incluso tra virgolette.

• Se si seleziona una cartella specifica, saranno sottoposti a scansione tutti i file in essa contenuti.</td></tr>
<tr><td>/MEMORY</td><td>Oggetti della memoria di sistema.</td></tr>
<tr><td>/STARTUP</td><td>Oggetti ad esecuzione automatica.</td></tr>
<tr><td>/MAIL</td><td>Database di posta.</td></tr>
<tr><td>/REMDRIVES</td><td>Tutte le unità estraibili.</td></tr>
<tr><td>/FIXDRIVES</td><td>Tutte le unità interne.</td></tr>
<tr><td>/NETDRIVES</td><td>Tutte le unità di rete.</td></tr>
<tr><td>/QUARANTINE</td><td>Oggetti in quarantena.</td></tr>
<tr><td>/ALL</td><td>Scansione completa.</td></tr>
</table>

/@:<filelist..lst>	Percorso al file con un elenco di oggetti e cartelle inclusi nella scansione. Il file deve essere in formato testo e ogni oggetto della scansione deve iniziare una nuova riga. È possibile indicare un percorso assoluto o relativo. Il percorso deve essere inserito tra virgolette se contiene uno spazio.
<azione> - questo parametro imposta le reazioni agli oggetti nocivi rilevati durante la scansione. Se questo parametro non è definito, l'azione predefinita è quella con il valore per **/i8**.	
/i0	Nessuna azione sull'oggetto; solo registrazione delle informazioni nel report.
/i1	Trattare gli oggetti infetti e, se la riparazione non riesce, ignorare.
/i2	Trattare gli oggetti infetti e, se la disinfezione non riesce, eliminare, ma non eliminare gli oggetti appartenenti ad oggetti composti, ed eliminare gli oggetti composti con intestazione eseguibile (archivi sfx) (impostazione predefinita).
/i3	Trattare gli oggetti infetti e, se la riparazione non riesce, eliminare, ed eliminare completamente tutti gli oggetti composti se non si riesce ad eliminare l'allegato infetto.
/i4	Eliminare gli oggetti infetti e, se la riparazione non riesce, eliminare. Inoltre eliminare completamente tutti gli oggetti composti se non si riesce ad eliminare il contenuto infetto.
/i8	Avvisa l'utente di intraprendere una azione se viene riconosciuto un oggetto infetto.
/i9	Avvisa l'utente di intraprendere una azione alla fine della scansione.
<file types> - questo parametro definisce il tipo di file soggetti a scansione anti-virus. Se il parametro non è definito, il valore predefinito è /fi.	

/fe	Esaminare solo i file potenzialmente infetti in base all'estensione.
/fi	Esaminare solo i file potenzialmente infetti in base ai contenuti.
/fa	Esaminare tutti i file.
<esclusioni> - questo parametro definisce gli oggetti da escludere dalla scansione. Può includere diversi valori dall'elenco fornito, separati da uno spazio.	
-e:a	Non esaminare archivi.
-e:b	Non esaminare i database di posta.
-e:m	Non esaminare i messaggi di testo semplice.
-e:<maschera file>	Non esaminare oggetti in base alle maschere.
-e:<secondi>	Ignorare oggetti esaminati più a lungo del tempo specificato dal parametro <secondi>.
-es:<dimensioni>	Ignora i file più grandi (in MB) del valore impostato per <dimensione>.
<file di configurazione> - questo parametro definisce il percorso al file di configurazione che contiene le impostazioni del programma per la scansione. Il file di configurazione è un file in formato testo che contiene un set di parametri per la linea di comando della scansione anti-virus. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono applicati i valori impostati dall'interfaccia di Kaspersky Anti-Virus.	
/C:<nome_file>	Usare i valori delle impostazioni assegnati nel file **<nome_file>**.

<impostazioni report> - questo parametro definisce il formato del report sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, vengono visualizzati i risultati della scansione e tutti gli eventi.	
/R:<report_file>	Registrare in questo file solo gli eventi importanti.
/RA:<report_file>	Registrare tutti gli eventi in questo file.
<impostazioni avanzate> - impostazioni che definiscono l'uso delle tecnologie di scansione anti-virus.	
/iChecker=<on|off>	Abilita/Disabilita iChecker.
/iSwift=<on|off>	Abilita/Disabilita iSwift.

Esempi:

Avvio di una scansione della RAM, programmi ad esecuzione automatica, database di posta, le directory **Documenti e Programmi***, e il file* **test.exe***:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Sospensione temporanea della scansione di oggetti selezionati e avvio di una scansione completa del computer, quindi proseguimento della scansione antivirus degli oggetti selezionati:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

Scansione RAM e degli oggetti elencati nel file ***object2scan.txt****. Uso del file di configurazione* ***scan_setting.txt****. Dopo la scansione, creazione di un report con registrazione di tutti gli eventi:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_Impostazioni.txt /RA:scan.log
```

Esempio di configurazione file:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

16.4. Aggiornamenti del programma

La sintassi per l'aggiornamento dei moduli di Kaspersky Anti-Virus e dei database dal prompt di comando è la seguente:

```
avp.com UPDATE [<aggiorna_fonte>] [/R[A]:<fiel_report>]
[/C:<nome_file>] [/APP=<on ! off>]
```

Descrizione dei parametri:

[<update_source>]]	Server HTTP o FTP o cartella di rete per il prelievo degli aggiornamenti. Come valore del parametro puoi specificare il percorso completo o l'URL per la fonte di aggiornamento. In assenza di un percorso selezionato, la fonte di aggiornamento sarà quella delle impostazioni di Aggiornamento.
/R[A]:<report_file>	**/R:<report_file>** – registrare solo gli eventi importanti nel report. **/R[A]:<report_file>** – registrare tutti gli eventi nel report. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, vengono visualizzati i risultati della scansione e tutti gli eventi.
/C:<file_name>	Percorso al file di configurazione con le impostazioni degli aggiornamenti del programma. Il file di configurazione è un file in formato testo che contiene un set di parametri per la riga di comando per l'aggiornamento dell'applicazione È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono applicati i valori impostati dall'interfaccia di Kaspersky Anti-Virus.
/APP=<on ! off>	Abilita/Disabilita gli aggiornamenti dei moduli del programma

Esempi:

Aggiornamento degli elenchi delle minacce dopo la registrazione di tutti gli eventi nel report:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Aggiornamento dei moduli di Kaspersky Anti-Virus applicando le impostazioni nel file di configurazione **updateapp.ini**:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

Esempio di configurazione file:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

16.5. Impostazioni di ritorno (rollback)

Sintassi del comando:

```
ROLLBACK [/R[A]:<report_file>] [/password=<password>]
```

/R[A]:<report_file>	**/R:<report_file>** - registra nel report solo gli eventi importanti **/RA:<report_file>** - registra nel report tutti gli eventi. È possibile indicare un percorso assoluto o relativo. Se il parametro non è impostato i risultati della scansione e tutti gli eventi saranno presentati sullo schermo.
<password>	Password per accedere a Kaspersky Anti-Virus impostata nell'interfaccia dell'applicazione.
Nota che non puoi eseguire questo comando senza digitare la password.	

Esempio:

```
avp.com ROLLBACK /RA:rollback.txt
/password=<la_tua_password>
```

16.6. Esportazione delle impostazioni

Sintassi dei comandi:

```
avp.com EXPORT <profile > <nome_file>
```

Descrizione dei parametri:

<profile>	Componente o attività le cui impostazioni vengono esportate. Può essere usato uno dei valori elencati in 16.2 a pag 210.
<nome_file>	Percorso al file su cui sono esportate le impostazioni di Kaspersky Anti-Virus. È possibile inserire percorsi assoluti o relativi. Il file di configurazione è salvato in formato binario (.dat) e può essere usato in seguito per importare le impostazioni dell'applicazione su altri computer. Il file di configurazione può essere salvato come file testo. Per fare questo specifica l'estensione .txt nel nome del file. Questo file può essere utilizzato solo per specificare le principali impostazioni per l'operatività del programma.

Esempio:

```
avp.com EXPORT c:\settings.dat
```

16.7. Importazione delle impostazioni

Sintassi dei comandi:

```
avp.com IMPORT <nome_file> [/password=<password>]
```

<file_name>	Percorso al file da cui sono importate le impostazioni di Kaspersky Anti-Virus. È possibile inserire percorsi assoluti o relativi. Le impostazioni possono essere importate solo da file binari.
<your_password>	La password di Kaspersky Anti-Virus impostata nell'interfaccia del programma

Esempi:

```
avp.com IMPORT c:\settings.dat /password=<password>
```

16.8. Avvio del programma

Sintassi dei comandi:

```
avp.com
```

16.9. Arresto del programma

Sintassi dei comandi:

```
EXIT /password=<la_tua_password>
```

<password>	La password di Kaspersky Anti-Virus impostata dall'interfaccia del programma.
Osservare che non è possibile eseguire questo comando senza digitare la password.	

16.10. Creazione di un file di tracciato

Potresti aver bisogno di creare un file di tracciato nel caso tu abbia problemi con il programma e voglia approfondirli con gli specialisti del Supporto Tecnico.

Sintassi dei comandi:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

Descrizione dei parametri:

[on|off]	Abilita/Disabilita la creazione del tracciato.
[file]	file del tracciato.
<trace_level>	Questo parametro può essere un numero tra 0 (livello minimo, solo messaggi critici) e 700 (livello massimo, tutti i messaggi). Contattando il Supporto Tecncio vi diranno quale valore di lvello avete bisogno. Se non viene specificato consigliamo di impostarlo su 500.

Attenzione!

Consigliamo di creare un file di tracciato solo per specifici problemi. L'abilitazione regolare della tracciatura potrebbe rallentare il tuo computer e saturare il tuo disco fisso.

Esempi:

Per disabilitare la creazione di un tracciato:

```
avp.com TRACE file off
```

Per creare un file di tracciato ed inviarlo al Supporto Tecnico con un livello massimo impostato a 500:

```
avp.com TRACE file on 500
```

16.11. Visualizzazione della Guida

Questo comando è disponibile per visualizzare la Guida con la sintassi del prompt di comando:

```
avp.com [ /? | HELP ]
```

Per ricevere aiuto sulla sintassi di un comando specifico, è possibile usare uno dei seguenti comandi:

```
avp.com <command> /?
avp.com HELP <command>
```

16.12. Codici di ritorno dall'interfaccia della riga di comando

Questa sezione contiene un elenco di codici di ritorno dalla riga di comando. Codici generici possono sempre essere ritornati da qualsiasi comando della riga di comando. I codici di ritorno includono codici generici e codici specifici per speficii tipi di azioni.

Codici di ritorno generici	
0	Operazione completata con successo

1	Valore di impostazione non valido
2	Errore sconosciuto
3	Errore nel completamento dell'azione
4	Azione cancellata
Codici di ritorno delle scansioni anti-virus	
101	Processati tutti gli oggetti pericolosi
102	Rinvenuti oggetti pericolosi

CAPITOLO 17. MODIFICA, RIPARAZIONE E DISINSTALLAZIONE DEL PROGRAMMA

Puoi disinstallare l'applicazione nei seguenti modi:

- usando la procedura guidata di installazione dell'applicazione (vedere 17.2 a pag. 226)
- dal prompt di comando (vedere 17.2 a pag. 226)

17.1. Modifica, riparazione e rimozione del programma usando la procedura guidata di nstallazione

In caso di errori di funzionamento dovuti a un'errata configurazione o al danneggiamento dei file può rendersi necessario riparare il programma.

La modifica del programma consente di installare componenti di Kaspersky Anti-Virus assenti o di eliminare quelli che non si desiderano.

Per riparare o modificare i componenti assenti di Kaspersky Anti-Virus o disinstallare il programma:

1. Inserisci l'eventuale CD di installazione nell'unità CD-ROM (se utilizzato per installare il programma). Se Kaspersky Anti-Virus è stato installato da una diversa origine (cartella condivisa, cartella nel disco fisso, ecc.), verificare che la cartella contenga il pacchetto di installazione e di potervi accedere.
2. Selezionare **Start → Tutti i programmi → Kaspersky Anti-Virus 7.0 → Modifica, ripara o rimuovi**.

Si apre una procedura di installazione guidata del programma. Osserviamo in dettaglio i passaggi necessari per riparare, modificare o eliminare il programma.

Passaggio 1. Selezione di un'operazione

In questa fase è richiesto di selezionare l'operazione che si desidera eseguire. È possibile modificare i componenti del programma, riparare i componenti già installati o rimuovere dei componenti o l'intero programma. Per eseguire l'operazione desiderata, fare clic sul pulsante appropriato. La reazione del programma dipende dall'operazione selezionata.

La modifica del programma è analoga all'installazione in cui è possibile specificare quali componenti si desidera installare e quali eliminare.

La riparazione del programma dipende dai componenti installati. Saranno riparati i file di tutti i componenti installati e per ciascuno di essi sarà impostato il livello di protezione consigliato.

Se si rimuove il programma, è possibile selezionare quali dati creati e usati dal programma si desidera salvare sul computer. Per eliminare tutti i dati di Kaspersky Anti-Virus, selezionare **Disinstallazione completa**. Per salvare i dati, selezionare **Salva oggetti applicazione** e specificare quali oggetti non eliminare:

- *Mantieni dati di attivazione* – il file della chiave di attivazione.
- *Database dell'applicazione* – serie completa delle firme di programmi pericolosi, virus e altre minacce correnti all'ultimo aggiornamento.
- *Mantieni file backup* – copie di backup di oggetti eliminati o riparati Si raccomanda di salvarli per poterli eventualmente ripristinare in un secondo momento.
- *Mantieni file quarantena* – file potenzialmente infetti da virus o varianti di essi. Questi file contengono codici simili a quelli di virus noti ma è difficile stabilire se siano nocivi. Si raccomanda di salvare questi file poiché potrebbero essere normali o riparati dopo l'aggiornamento degli elenchi delle minacce.
- *Mantieni impostazioni di protezione* – configurazioni per tutti i componenti del programma.
- *Mantieni dati iSwift* – database con informazioni sugli oggetti esaminati nel file system NTFS. Può accelerare la scansione. Quando usa questo database, Kaspersky Anti-Virus esamina solo i file che hanno subito modifiche in seguito all'ultima scansione.

Attenzione!

Se trascorre un lungo periodo tra la disinstallazione di una versione di Kaspersky Anti-Virus e l'installazione di un'altra, si sconsiglia di utilizzare il database *iSwift* di una versione precedente. Un programma pericoloso potrebbe essere penetrato nel computer nel frattempo e i suoi effetti non sarebbero rilevati dal database, con conseguente rischio di infezione.

Per avviare l'operazione selezionata fare clic sul pulsante **Avanti**. Il programma inizia a copiare i file necessari sul computer o a eliminare i componenti e i dati selezionati.

Passaggio 2. Completamento della modifica, riparazione o rimozione del programma

L'avanzamento del processo di modifica, riparazione o rimozione del programma viene seguito sullo schermo. Al termine l'utente viene informato del completamento dell'operazione.

La rimozione del programma richiede solitamente il riavvio del computer, necessario per applicare le modifiche al sistema. Il programma chiede quindi se si desidera riavviare il computer. Fare clic su **Sì** per riavviarlo subito. Per riavviarlo in un secondo momento, scegliere invece **No**.

17.2. Disinstallazione del programma dalla riga di comando

Per disinstallare Kaspersky Anti-Visrus dalla riga di comando, digita:

```
msiexec /x <package_name>
```

Si aprirà la procedura guidata di configurazione. Puoi usarlo per disinstallare l'applicazione (vedi Capitolo 17 pag 224).

Per disinstallare l'applicazione in background senza riavviare il computer (il computer dovrà essere riavviato manualmente dopo la disinstallazione) digita::

```
msiexec /x <package_name> /qn
```

CAPITOLO 18. DOMANDE FREQUENTI

Questo capitolo è dedicato alle domande più frequenti poste dai nostri utenti sull'installazione, la configurazione e il funzionamento di Kaspersky Anti-Virus; faremo il possibile per fornire risposte più esaurienti possibile.

Domanda: È possibile usare Kaspersky Anti-Virus 7.0 con prodotti antivirus di altri fabbricanti?

No. Si raccomanda di disinstallare altri prodotti antivirus eventualmente presenti sul computer prima di installare Kaspersky Anti-Virus per evitare conflitti di software.

Domanda: Kaspersky Anti-Virus non riesamina i file precedentemente sottoposti alla scansione? Perché?

È vero. Kaspersky Anti-Virus non riesamina i file che non hanno subito variazioni dalla scansione precedente.

Ciò è possibile grazie alle nuove tecnologie iChecker e iSwift. La tecnologia viene implementata nel programma utilizzando un database di checksum dei file e un archivio di checksum dei file in flussi NTFS alternati.

Domanda: Perché è richiesta l'attivazione? Kaspersky Anti-Virus funzionerà senza il file della chiave?

Kaspersky Anti-Virus funziona anche senza chiave di licenza ma il programma non è in grado di accedere agli aggiornamenti ed all'assistenza tecnica.

Se non si è ancora deciso se acquistare Kaspersky Anti-Virus, possiamo fornire una chiave di licenza in prova per due settimane o un mese. Trascorso questo periodo, la chiave scade.

Domanda: Dopo l'installazione di Kaspersky Anti-Virus il sistema operativo ha iniziato a "comportarsi" in maniera strana (schermo blu, riavvii frequenti, ecc.). Cosa devo fare?

Sebbene si tratti di una circostanza rara, è possibile che Kaspersky Anti-Virus e altri software presenti sul computer siano in conflitto.

Per ripristinare la funzionalità del sistema operativo procedere come segue:

1. Premere il tasto **F8** non appena il computer inizia a caricarsi fino a visualizzare il menu di boot.
2. Selezionare la **Modalità provvisoria** e caricare il sistema operativo.
3. Aprire Kaspersky Anti-Virus.
4. Apri la finestra impostazioni dell'applicazione e seleziona **Servizio**.
5. deselezionare **Lancia l'applicazione all'avvio del computer** e premi **OK**.
6. Riavvia il sistema operativo in modalità regolare.

Inviare una richiesta al Supporto Tecnico di Kaspersky Lab. Apri la finestra principale dell'applicazione, seleziona **Supporto** e clicca Lancia Richiesta. Descrivi il problema e la sua firma nel modo più dettagliato possibile.

Ricordare di allegare alla domanda un file contenente un'immagine completa della memoria del sistema operativo Microsoft Windows. Per creare questo file procedere come segue:

1. Fare clic con il pulsante destro del mouse su **Risorse del computer** e selezionare l'elemento **Proprietà** del menu di scelta rapida che si apre.
2. Selezionare la scheda **Avanzate** nella finestra **Proprietà del sistema**, quindi premere il pulsante **Impostazioni** nella sezione **Avvio e Ripristino**.
3. Selezionare l'opzione **Immagine memoria completa** dal menu a discesa della sezione **Scrivi informazioni di debug** nella finestra **Avvio e Ripristino**.

   Per impostazione predefinita, il file di scarico della memoria viene salvato nella cartella di sistema come *memory.dmp*. È possibile cambiare la cartella rinominando la cartella nel campo corrispondente.
4. Riprodurre il problema relativo al funzionamento di Kaspersky Anti-Virus.
5. Accertarsi che il file di scarico della memoria completato sia stato salvato correttamente.

APPENDICE A. RIFERIMENTI

Questa appendice contiene materiale di riferimento sui formati dei file e le maschere delle estensioni utilizzate nelle impostazioni di Kaspersky Anti-Virus.

A.1. Elenco dei file esaminati in base all'estensione

Se si seleziona **Esamina programmi e documenti (in base all'estensione)**, File Anti-Virus sottopone a un'approfondita scansione antivirus i file con le estensioni sotto elencate. Se si abilita il filtro degli allegati, anche Mail Anti-Virus esaminerà questi file.

com – file eseguibile di un programma di dimensioni non superiori a 65 KB

exe – file eseguibile o archivio autoestraente

sys – file di sistema

prg – testo di programma per dBase, Clipper o Microsoft Visual FoxPro, o programma di WAVmaker

bin – file binario

bat – file batch

cmd – file di comando per Microsoft Windows NT (simile a un file .bat per DOS), OS/2

dpl – libreria compressa Borland Delphi

dll – libreria di caricamento dinamico

scr – splash screen di Microsoft Windows

cpl – modulo del pannello di controllo di Microsoft Windows

ocx – oggetto Microsoft OLE (Object Linking and Embedding)

tsp – programma eseguito in modalità split-time

drv – driver di periferica

vxd – Microsoft Windows virtual device driver

pif – file informazione programma (program information file)

lnk – file link di Microsoft Windows

reg – file della chiave di registro del sistema di Microsoft Windows

ini – file di inizializzazione

cla – classe Java

vbs – Visual Basic script

vbe – estensione video BIOS

js, jse – testo origine JavaScript

htm – documento ipertestuale

htt – intestazione ipertesto di Microsoft Windows

hta – file di ipertesto usato per aggiornare il registro del sistema operativo

asp – script Active Server Pages

chm – file HTML compilato

pht – HTML con script PHP incorporati

php – script incorporato in file HTML

wsh – file Windows Windows Script Host

wsf – script Microsoft Windows

the – wallpaper di Microsoft Windows 95

hlp – file Win Help

eml – file di posta di Microsoft Outlook Express

nws – nuovo file di posta di Microsoft Outlook Express

msg – file di posta Microsoft Mail

plg – e-mail

mbx – estensione dei messaggi di Microsoft Office Outlook salvati

doc – documento di Microsoft Office Word

dot – modello di documento di Microsoft Office Word

fpm – programma di database, file di avvio di Microsoft Visual FoxPro

rtf – documento Rich Text Format

shs – frammento Shell Scrap Object Handler

dwg – database blueprint AutoCAD

msi – pacchetto Microsoft Windows Installer

otm – progetto VBA per Microsoft Office Outlook

pdf – documento di Adobe Acrobat

swf – file Shockwave Flash

jpg, jpeg, png – formato immagini compresso

emf – formato Enhanced Metafile, la prossima generazione di metafile per Microsoft Windows OS. I file EMF non sono supportati da Microsoft Windows a 16 bit.

ico – icona di un programma (Windows, Unix, Gimp)

ov? – file eseguibili MS DOC

*xl** – documenti e file di Microsoft Office Excel, come: *xla* – estensione Microsoft Office Excel, *xlc* – diagramma, *xlt* – modelli di documento, ecc.

*pp** – documenti e file di Microsoft Office PowerPoint, come: *pps* – diapositiva Microsoft Office PowerPoint, *ppt* – presentazione, ecc.

*md** – documenti e file di Microsoft Office Access, come: *mda* – gruppo di lavoro di Microsoft Office Access, mdb – database, ecc.

Ricordare che il formato effettivo di un file può non corrispondere al formato indicato dall'estensione.

A.2. Maschere di esclusione file valide

Osserviamo alcuni esempi delle maschere possibili per la creazione di elenchi di esclusione di file:

- Maschere senza percorso file:
  - ***.exe** – tutti i file con estensione exe
  - ***.ex?** – tutti i file con estensione *.ex?,* dove ? può rappresentare qualsiasi carattere singolo
  - **test** – tutti i file di nome *test*
- Maschere con percorso file assoluto:
  - **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file nella cartella *C:\dir*
  - **C:\dir*.exe** – tutti i file con estensione *.exe* contenuti nella cartella C:\dir\
  - **C:\dir*.ex?** – tutti i file con estensione *.ex?* nella cartella *C:\dir*, in cui ? è utilizzato in sostituzione di un carattere
  - **C:\dir\test** – solo il file *C:\dir\test*
  - Se non si desidera che il programma esamini i file nelle sottocartelle di questa cartella, selezionare  **Includi sottocartelle** durante la creazione della maschera.
- Maschere con percorso file relativo:
  - **dir*.*** o **dir*** o **dir** – tutti i file in tutte le cartelle *dir*
  - **dir\test** – tutti i file *test* nelle cartelle *dir*
  - **dir*.exe** – tutti i file con estensione *.exe* in tutte le cartelle in *dir*
  - **dir*.ex?** – tutti i file con estensione *.ex?* in tutte le cartelle di *C:\dir*, in cui ? è utilizzato in sostituzione di un carattere

- Se non si desidera che il programma esamini i file nelle sottocartelle di questa cartella, selezionare **Includi sottocartelle** durante la creazione della maschera.

Suggerimento:

Le maschere di esclusione *.* e * possono essere usate se definisci l'esclusione di un tipo di minaccia in accordo con la Enciclopedia dei Virus. In caso contrario, la minaccia specificata non sarà rilevata in alcun oggetto. L'uso di queste maschere senza selezionare il tipo di minaccia disabilita il monitoraggio.

Non consigliamo di selezionare un drive virtuale creato sulla base di un file system che usa il comando *subst* come una esclusione. Non avrebbe alcun senso farlo poiché, durante la scansione, il programma percepisce questa unità virtuale come cartella e di conseguenza la esamina.

A.3. Maschere di esclusione valide per la classificazione dell'Enciclopedia dei Virus.

Durante l'aggiunta di esclusioni di minacce con un determinato stato dalla classificazione dell'Enciclopedia dei virus, è possibile specificare:

- Il nome completo della minaccia come indicato nell'Enciclopedia dei virus all'indirizzo www.viruslist.com (per esempio, **not-a-virus:RiskWare.RemoteAdmin.RA.311** o **Flooder.Win32.Fuxx**);
- Il nome della minaccia mediante maschera. Ad esempio:
  - **not-a-virus*** – esclude dalla scansione potenziali programmi pericolosi e programmi jolly.
  - ***Riskware.*** – esclude dalla scansione i riskware.
  - ***RemoteAdmin.*** – esclude dalla scansione tutti i programmi di amministrazione remota.

APPENDICE B. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è diventata un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce una vasta gamma di applicazioni per la sicurezza dei dati e offre soluzioni complete di alto livello per garantire la sicurezza di computer e reti contro ogni tipo di programma dannoso, messaggi di posta elettronica non sollecitati e indesiderati e attacchi di pirateria informatica.

Kaspersky Lab è un'azienda internazionale con sede nella Federazione Russia e rappresentanti nel Regno Unito, Francia, Germania, Giappone, USA (CA), Benelux, Cina, Polonia e Romania. Recentemente è stato inaugurato un nuovo reparto, l'European Anti-Virus Research Centre, in Francia. Kaspersky Lab conta su una rete di partner costituita da oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab si avvale di oltre 550 esperti, tutti specializzati in tecnologie antivirus, 10 dei quali in possesso di laurea in amministrazione aziendale, 16 di specializzazione postlaurea, e vari membri della Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offre soluzioni di sicurezza di alto livello, elaborate grazie a un'esperienza esclusiva accumulata in più di 15 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus consente all'azienda di offrire una protezione completa contro minacce presenti e future. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. L'azienda si trova costantemente all'avanguardia rispetto a numerosi altri produttori offrendo una protezione antivirus completa per utenti domestici e commerciali.

Anni di duro lavoro ne hanno fatto un'azienda leader tra i principali produttori di software per la sicurezza informatica. Kaspersky Lab è stata una delle prime aziende di questo tipo a sviluppare i più severi standard della protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, server di file, sistemi di posta elettronica, firewall e gateway di Internet e computer portatili. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'impresa. Numerose imprese di grande notorietà si affidano a Kaspersky Anti-Virus, per esempio Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di una vasta serie di servizi supplementari volti a garantire sia un funzionamento stabile dei prodotti dell'azienda, sia la conformità a qualsiasi esigenza aziendale specifica. Il database antivirus di Kaspersky Lab viene aggiornato ogni ora. L'azienda offre ai

propri clienti un servizio di assistenza tecnica 25 ore su 25, disponibile in diverse lingue per soddisfare le esigenze di una clientela internazionale.

B.1. Altri prodotti Kaspersky Lab

Kaspersky Lab News Agent

News Agent и progettato per comunicare tempestivamente le notizie pubblicate da Kaspersky Lab, per le notifiche relative allo stato corrente dell'attività dei virus e per notizie fresche. Il programma legge l'elenco dei canali news disponibili e il loro contenuto dai server di notizie di Kaspersky Lab con la frequenza specificata.

Il programma permette all'utente le seguenti funzioni:

- Visualizza nella barra di sistema il giudizio sul virus corrente.
- Iscriviti ad un canale di news.
- Recupera le news da ogni canale selezionato con la frequenza specificata e ricevi una notifica sulle ultime notizie.
- Rivedi le notizie sui canali selezionati.
- Rivedi l'elenco dei canali e il loro stato.
- Apri nel browser il testo completo di un articolo.

News Agent è un'applicazione Microsoft Windows stand-alone che può essere utilizzata da sola o con varie soluzioni integrate offerte da Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Questo programma è un servizio gratuito offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer. Kaspersky OnLine Scanner funziona direttamente dal tuo browser . Gli utenti hanno così la possibilità di esaminare velocemente il computer in caso di sospetto di infezione virale. Con questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta.
- Selezionare per la scansione database antivirus standard/estesi.
- Salvare un report dei risultati di scansione in formato txt o html.

Kaspersky® OnLine Scanner Pro

Questo programma è un servizio che richiede una iscrizione offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer e di riparare i file pericolosi. Kaspersky OnLine

Scanner Pro funziona direttamente dal tuo browser . Grazie a questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta.
- Selezionare per la scansione database antivirus standard/estesi.
- Salvare un report dei risultati di scansione in formato txt o html.

Kaspersky ® Internet Security 7.0

Kaspersky Internet Security 7.0 è una soluzione integrata progettato per proteggere i personal computer dalle più diffuse minacce (virus, hacker, spam e spyware). Una singola interfaccia abilita gli utenti a configurare tutti i componenti del programma.

La protezione anti-virus include:

- **Scansione Anti-Virus del traffico e-mail** a livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per posta in arrivo e SMTP per messaggi in uscita), indipendentemente dal client mail che viene utilizzato. Il programma include plug-in per conosciuti client e-mail (come Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail e The Bat) e supporta la disinfezione dei loro database delle e-mail.
- Scansione anti-virus in tempo reale del traffico Internet trasferito via HTTP.
- **Protezione del file system**: scansione anti-virus di file individuali, cartelle o drive. In aggiunta l'applicazione può condurre il controllo anti-virus solo per le aree critiche del sistema operativo e gli oggetti di avvio di Microsoft Windows.
- **Protezione Proattiva**: il programma monitorizza costantemente l'attività dell'applicazione e dei processi lavorando sulla RAM, prevenendo modifiche importanti al file system ed al registro e ripristinando il system.

Protezione contro le frodi Internet: viene assicurata dal riconoscimento dagli attacchi phishing, evitando la sottrazione di dati riservati (soprattutto password, numeri dei conti bancari e delle carte di credito), e bloccando l'esecuzione di script pericolosi sulle pagine web, finestre di pop-up e banner pubblicitari. La caratteristica **di blocco degli autodialer** aiuta ad identificare software che tentano di usare il tuo modem per connessioni nascoste e non autorizzate a numerazioni telefoniche a pagamento e blocca tali attività.

Kaspersky Internet Security 7.0 **registra i tentativi di scansionare le porte del tuo computer** che frequentemente precedono gli attacchi sul network e con successo difende contro i tipici attacchi al network. Il programma utilizza **come base regole definite** per il controllo delle transazioni sulla rete tracciando tutti i

pacchetti di dati in ingresso ed uscita. La **Modalità Stealth** (di proprietà di SmartStealth™ technology) **previene gli attacchi dall'esterno**. Quando ti sposto su Modalità Stealth il sistema blocca tutta l'attività di rete escluse poche transazioni permesse nelle regole definite dall'utente.

Il programma impiega un approccio tutto compreso per filtrare gli spam in ingresso con i messaggi di posta:

- Verifica contro liste bianche e nere del destinatario (compresi indirizzi dei siti di phishing)
- Ispezione delle frasi contenuto nel corpo del messaggio
- Analisi del testo dei messaggi utilizzando un algoritmo di apprendimento
- Riconoscimento di spam inviato nei file immagine

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile fornisce una protezione per apparati mobili funzionanti con Symbian OS e Microsoft Windows Mobile. Il programma assicura una scansione esaustiva comprendente:

- **Scansione su richiesta** della memoria del dispositivo, schede di memoria o cartelle individuali o uno specifico file; se viene rilevato un file infetto questo viene spostato in Quarantena o eliminato
- **Scansione in tempo reale** – tutti i file in ingresso ed uscita sono scansionati automaticamente, come pure i file oggetti di tentativi di accesso
- **Protezione da spam** contenuto nei messaggi di testo

Kaspersky Anti-Virus per File Server

Questo pacchetto fornisce una affidabile protezione da tutti i tipi di malware per i file di sistema su server che operano con Microsoft Windows, Novell NetWare, Linux e Samba. La suite include le seguenti applicazioni Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Caratteristiche e funzionalità:

- *Protegge i file system dei server in tempo reale*. Tutti i file dei server sono scansionati quando aperti o salvati sul server
- Evita l'epidemia virus

- *Scansione* su richiesta dell'intero file system o di file o cartelle individuali
- *Usa tecnologie di ottimizzazione* nella scansione degli oggetti nel file system del server
- Possibilità di rollback (ritorno) dopo un attacco virus
- *Scalabilità del pacchetto software* in accordo con la capacità delle risorse disponibili di sistema
- Monitoraggio del sistema di cattivo bilanciamento
- *Creazione di un elenco di processi* sicuri la cui attività sul server non è soggetta a controllo dal pacchetto software
- *Amministrazione remota* del pacchetto software, compreso installazione, configurazione ed amministrazione centralizzata
- Salvataggio di copie di backup degli oggetti infettati o cancellati nel caso tu abbia bisogno di ripristinarle
- Messa in Quarantena degli oggetti sospetti
- *Invio di notifiche degli eventi* nell'esecuzione del programma all'amministratore di sistema
- Registrazione di dettagliati report
- *Aggiornamento automatico* dei database del programma

Sicurezza Kaspersky Open Space

Kaspersky Open Space Security è un pacchetto software con un nuovo approccio alla sicurezza per le rete aziendali attuali di qualsiasi dimensione assicurando un sistema informativo di protezione centralizzato ed il supporto per uffici remoti e utenti in movimento.

La suite comprende quattro programmi:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifiche per ogni programma sono fornite di seguito.

Kaspersky WorkSpace Security è un programma per la protezione centralizzata di workstation interne ed esterne alla rete aziendale contro tutte le minacce attuali di Internet (virus, spyware, attacchi di hacker e spam)

Caratteristiche e funzionalità:

- Affidabile protezione da virus, spyware, attacchi hacker e spam
- Difesa Proattiva da nuovi programmi maligni le cui firme non sono ancora state aggiunte al database
- Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete
- Rollback per modifiche pericolose del sistema
- Protezione dagli attacchi phishing mail indesiderate
- Ridistribuzione dinamica delle risorse durante la completa scansione del sistema
- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata
- Supporto per *Cisco® NAC* (Network Admission Control)
- Scansione e-mail e traffico Internet in tempo reale e, blocco delle finestre pop-up e banner pubblicitari su Internet
- Operatività sicura in qualsiasi tipo di Network compreso Wi-Fi
- Creazione del disco di emergenza per permetterti di ripristinare il tuo sistema dopo una invasione virus
- Ampio sistema di reportistica sugli stati della protezione
- Aggiornamento automatico dei database
- Supporto completo per sistemi operativi a 64-bit
- Ottimizzazione delle prestazioni del programma su laptop (tecnologia Intel® Centrino® Duo)
- Capacità di disinfezione remota (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security fornisce una ottima protezione alle risorse informative aziendali dalle odierne minacce Internet. Kaspersky Business Space Security protegge workstation e file server da tutti i tipi di virus, Trojan e worm, impedisce la diffusione dei virus ed assicura le informazioni mentre garantisce un accesso immediato alle risorse di rete per l'utente.

- Caratteristiche e funzionalità
- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata
- Supporto per *Cisco® NAC* (Network Admission Control)

- Protezione di workstations e file server da tutti i tipi di minacce
- tecnologia iSwift per evitare la ripetizione della scansione file internamente alla rete
- Distribuzione del carico tra i server
- Oggetti sospetti in Quarantena da workstation
- Rollback per modifiche pericolose del sistema
- Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema
- Difesa Proattiva per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database
- Scansione e-mail e traffico internet in tempo reale
- Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete
- Protezione mentre si usa un network Wi-Fi
- Auto-Difesa da programmi maligni
- Oggetti sospetti in Quarantena
- Aggiornamento automatico dei database

Kaspersky Enterprise Space Security

Questo programma comprende componenti per la protezione dalle attuali minacce Internet collegati a workstation e server. Cancella i virus dalle email, rendendo sicura l'informazione mentre fornisce un accesso sicuro alle risorse di rete per l'utente.

Caratteristiche e funzionalità:

- Protezione delle workstation e file server da virus, Trojan e worm
- Protezione di Sendmail, Qmail, Postfix e Exim mail server
- Scansione di tutte le e-mail su microsoft Ecxchange Server compreso le cartelle condivise
- Processo di tutte le e-mail, database ed altri oggetti per i server Lotus Domino
- Protezione dagli attacchi phishing e junk mail
- Prevenzione infezione virus e mass mailing

- Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema
- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata
- Supporto per *Cisco® NAC* (Network Admission Control)
- Difesa Proattiva per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database
- Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete
- Protezione sicura mentre si usa un network Wi-Fi
- Scansione traffico Internet in tempo reale
- Rollback per modifiche pericolose del sistema
- Ridistribuzione dinamica delle risorse durante la completa scansione del sistema
- Oggetti sospetti in Quarantena
- Ampio sistema di reportistica sugli stati della protezione
- Aggiornamento automatico dei database

Kaspersky Total Space Security

Questo programma esegue il monitoraggio del flusso dati in ingresso ed uscita (e-mail,Internet e tutte le interazioni di rete). Comprende i componenti per la protezione di workstation ed apparati mobili,mantenendo sicura l'informazione mentre fornisce per l'utente un accesso sicuro alle risorse informative della rete aziendale e di Internet e una sicura comunicazione via e-mail.

Caratteristiche e funzionalità:

- Protezione completa da virus, spyware, attacchi hacker e spam a qualsiasi livello della rete aziendale da workstation a gateway Internet
- Difesa Proattiva per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database
- Protezione dei server di posta e server collegati
- Scansione del traffico Internet (HTTP/FTP) in tempo reale sull'area del network locale
- Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema
- Blocco degli accessi da workstation infettate

- Prevenzione epidemia virus
- Reportistica centralizzata sugli stati di protezione
- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata
- Supporto per *Cisco® NAC* (Network Admission Control)
- Supporto per hardware server proxy
- Filtraggio del traffico Internet usando elenchi di server, tipi di oggetto e gruppi utenti sicuri
- Tecnologia iSwift per evitare la ripetizione della scansione di file nella rete
- Ridistribuzione dinamica delle risorse durante la completa scansione del sistema
- Firewall personale con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete
- Sicura operatività per gli utenti in qualsiasi tipo di Network compreso Wi-Fi
- Protezione dagli attacchi phishing e junk mail
- Capacità di disinfezione remota (Intel® Active Management, Intel® vPro™)
- Rollback per modifiche pericolose del sistema
- Auto-Difesa da programmi maligni
- Completo supporto per sistemi operativi a 64-bit
- Aggiornamento automatico dei database

Kaspersky Security per Server di Posta

Questo programma è per proteggere i server di posta ed i server collegati da programmi pericolosi e da spam. Il programma comprende l'applicazione per proteggere tutti server di posta standard (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix ed Exim) e ti abilita a configurare un gateway e-mail dedicato. La soluzione include:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.

- Kaspersky Anti-Virus for Linux Mail Server.

Le sue caratteristiche comprendono:

- Affidabile protezione contro programmi maligni op potenzialmente pericolosi
- Filtraggio di junk mail
- Scansione di tutti i messaggi ed si Microsoft Exchange Server per virus compreso le cartelle condivise
- Controllo di e-mail, database ed altri oggetti per server Lotus Notes/Domino
- Filtraggio delle e-mail per tipo di allegato
- Oggetti sospetti in Quarantena
- Semplice sistema di gestione del programma
- Prevenzione epidemia virus
- Monitoraggio stato protezione a mezzo notifiche
- Sistema di reportistica per l'operatività del programma
- Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema
- Aggiornamento automatico dei database

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina una tecnologia all'avanguardia in cui il programma analizza dal punto di vista linguistico il testo dei messaggi, i moderni metodi di filtraggio della posta elettronica (incluse le liste nere DNS e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, dove controlla le e-mail in arrivo dallo spam, Kaspersky® Anti-Spam funziona come barriera alle e-mail indesiderate. Il prodotto è compatibile con qualsiasi sistema di posta e può essere installato sia su server di posta esistente sia su server dedicati.

L'elevato grado di efficacia di Kaspersky Anti-Spam è consentito dall'aggiornamento quotidiano del database di filtraggio dei contenuti,con l'aggiunta di campioni forniti specialisti del laboratorio linguistico della Società. I database vengono aggiornati ogni 20 minuti.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper assicura una elevata velocità di scansione del traffico sui server funzionanti con Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

Il programma è un plug-in e scansiona contro i virus e processa in tempo reale il traffico e-mail in ingresso ed in uscita.

B.2. Per contattarci

Per qualsiasi domanda, commento o suggerimento, l'utente può rivolgersi ai distributori o direttamente a Kaspersky Lab. che sarà lieta di offrire assistenza per qualsiasi problematica relativa ai suoi prodotti, sia per telefono che per e-mail. Tutte le raccomandazioni e i suggerimenti pervenuti saranno presi in considerazione e valutati con attenzione.

Supporto Tecnico	Trovi le informazioni di supporto tecnico su http://www.kaspersky.com/supportinter.html Helpdesk: http://support.kaspersky.ru/helpdesk.html?LANG=it
Informazioni generali	WWW: http://www.kaspersky.it http://www.viruslist.com E-mail: info@kaspersky.com

APPENDICE C. CONTRATTO DI LICENZA

Contratto di licenza standard con l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: SI RACCOMANDA DI LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO DI LICENZA ("CONTRATTO"), PER LA LICENZA DEL SOFTWARE KASPERSKY ANTI-VIRUS ("SOFTWARE") PRODOTTO DA KASPERSKY LAB.

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, FACENDO CLIC SUL PULSANTE DI ACCETTAZIONE, L'UTENTE ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO E A DIVENTARNE UNA DELLE PARTI. IN CASO CONTRARIO, FACENDO CLIC SUL PULSANTE CHE INDICA LA MANCATA ACCETTAZIONE DI TUTTE LE CONDIZIONI DEL PRESENTE, L'UTENTE RINUNCIA A INSTALLARE IL SOFTWARE.

SE IL SOFTWARE È STATO ACQUISTATO SU SUPPORTO FISICO E L'UTENTE HA ROTTO IL SIGILLO DELLA BUSTA DEL CD, ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO. SE L'UTENTE NON ACCETTA TUTTE LE CONDIZIONI DEL PRESENTE CONTRATTO, EGLI DOVRÀ ASTENERSI DAL ROMPERE IL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE.

AI SENSI DELLA LEGISLAZIONE VIGENTE, PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI, ACQUISTATO ONLINE DAL SITO WEB DI KASPERSKY LAB O DEI SUOI PARTNER, IL CLIENTE HA QUATTORDICI (15) GIORNI LAVORATIVI DI TEMPO DALLA CONSEGNA DEL PRODOTTO PER RESTITUIRLO AL RIVENDITORE A FINI DI SOSTITUZIONE O DI RIMBORSO, A CONDIZIONE CHE IL SOFTWARE NON SIA STATO DISSIGILLATO.

PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI NON ACQUISTATO ONLINE VIA INTERNET, QUESTO SOFTWARE NON POTRÀ ESSERE RESTITUITO NÉ SOSTITUITO, ECCEZION FATTA PER LE CLAUSOLE CONTRARIE DEL PARTNER CHE VENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON SARÀ RITENUTO RESPONSABILE DELLE CLAUSOLE DEL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SI RIFERISCE SOLO ALL'ACQUIRENTE ORIGINARIO.

Qualsiasi riferimento al "Software" nel presente documento sarà da intendersi comprensivo di codice di attivazione fornito da Kaspersky Lab come parte integrante di Kaspersky Anti-Virus 7.0.

1. *Concessione della licenza.* Previo pagamento delle tasse di licenza applicabili e nel rispetto dei termini e delle condizioni del presente Contratto, con il presente Kaspersky Lab concede all'utente il diritto non esclusivo e non trasferibile di utilizzare una copia della versione specificata del Software e la documentazione in accompagnamento (la "Documentazione") per la durata del presente Contratto e unicamente a uso aziendale interno. È possibile installare una copia del Software su un computer.

1.1 *Uso.* Il Software è concesso in licenza in qualità di singolo prodotto; non può essere utilizzato su più di un computer o da più di un utente per volta, salvo diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un computer quando è caricato nella memoria temporanea (per esempio random access memory o RAM) oppure installato nella memoria permanente (per esempio disco fisso, CD-ROM o altro dispositivo di memorizzazione) di quel computer. La presente licenza autorizza l'utente a creare il numero di copie di backup del Software necessarie per il suo utilizzo legale e unicamente a scopi di archivio, a condizione che tutte le copie contengano le informazioni di proprietà del software. L'utente è tenuto a mantenere traccia del numero e dell'ubicazione di tutte le copie del Software e della Documentazione e a prendere tutte le ragionevoli precauzioni per proteggere il Software da copia o utilizzo non autorizzati.

1.1.2 Il software protegge il computer dai virus le cui firme sono contenute nel database di descrizione delle minacce che è disponibile sui server di aggiornamento di Kaspersky Lab.

1.1.3. Se vendi il computer sul quale è installato il Software dovrai assicurare che tutte le copie del Software siano state precedentemente eliminate.

1.1.4 È fatto divieto all'utente di decompilare, reverse engineer, disassemblare o altrimenti ridurre qualsiasi parte di questo Software in forma umanamente leggibile o consentire a terzi di farlo. Le informazioni di interfaccia necessarie per ottenere l'interoperatività del software con programmi indipendenti per computer saranno fornite da Kaspersky Lab dietro richiesta e pagamento dei ragionevoli costi e delle spese sostenute per procurarsi e fornire tali informazioni. Qualora Kaspersky Lab ti notificasse che, per qualsiasi ragione, inclusi (senza limitazioni) i costi, non intende fornire tali informazioni, l'utente sarà autorizzato a intraprendere le azioni necessarie per ottenere l'interoperatività a condizione di eseguire solo le operazioni di decompilazione o reverse engineering nei limiti previsti dalla legge.

1.1.5 L'utente non deve né deve permettere ad altri (in modo diverso da quanto espressamente permesso nel presente) di effettuare la correzione di errori o

altrimenti modificare, adattare o tradurre il Software né creare opere derivate dal Software.

1.1.6 È fatto divieto all'utente di concedere in locazione, in leasing o in prestito a terzi il Software o trasferire o cedere in sublicenza a terzi i diritti a lui conferiti dalla licenza.

1.1.7 E' vietato all'utente fornire il codice di attivazione o la chiave di licenza a terze parti o permettere a terze parti l'accesso ai codici di attivazione o alla chiave della licenza. Il codice di attivazione e la chiave della licenza sono dati riservati

1.1.8 Kaspersky Lab può richiedere all'utente di installare l'ultima versione del Software (l'ultima versione ed il più recente pack di manutenzione)

1.1.9 All'utente è fatto divieto di utilizzare il Software con strumenti automatici, semi-automatici o manuali progettati per creare firme virus, routine di rilevazione virus, qualsiasi altro dato o codice per la rilevazione di codici o dati maligni.

2. *Assistenza.*

(i) Kaspersky Lab metterà a disposizione dell'utente i servizi di assistenza ("Servizi di assistenza") specificati di seguito per un periodo, specificato nel File della Chiave di Licenza ed indicato nella finestra Servizio, dal momento dell'attivazione, previo:

(a) pagamento della tariffa di assistenza corrente; e

(b) compilazione del Modulo di iscrizione ai Servizi di assistenza fornito in allegato al presente Contratto o disponibile nel sito web di Kaspersky Lab, nel quale sarà richiesto all'utente di fornire il proprio codice di attivazione fornito all'utente da Kaspersky Lab con il presente Contratto. Kaspersky Lab ha il diritto di stabilire, a propria assoluta discrezione, se l'utente abbia soddisfatto o meno questa condizione per la fornitura dei Servizi di Assistenza.

Il servizio di assistenza diventerà disponibile in seguito all'attivazione del Software. Il servizio di assistenza tecnica di Kaspersky Lab ha facoltà di richiedere all'utente finale un'ulteriore registrazione per poter usufruire dei servizi di assistenza.

Fino all'attivazione del Software e/o all'ottenimento dell'identificativo dell'utente finale (ID cliente) il servizio di assistenza tecnica offre assistenza esclusivamente per l'attivazione del Software e la registrazione dell'utente finale.

(ii) Con la compilazione del Modulo di sottoscrizione ai servizi di assistenza, l'utente accetta i termini della politica di tutela della riservatezza adottata da Kaspersky Lab e consultabile su www.kaspersky.com/privacy, e acconsente esplicitamente al trasferimento dei propri dati in paesi esterni

a quello di residenza, come specificato nella politica di tutela della riservatezza.

(iii) I Servizi di Assistenza termineranno alla scadenza, salvo rinnovo annuo dietro il pagamento della tariffa annuale corrente e dietro soddisfacente nuova compilazione del Modulo di sottoscrizione ai servizi di assistenza.

(iv) Per "Servizi di assistenza" si intendono

(a) Aggiornamento del database antivirus ogni ora

(b) Aggiornamenti gratuito del software compresi le versioni aggiornate;

(c) Assistenza tecnica via Internet e numero verde fornita dal distributore e/o dal rivenditore;

(f) Aggiornamenti per il rilevamento e l'eliminazione di virus entro 24 ore.

(v) I servizi di assistenza sono forniti solo se e quando l'utente dispone della versione del Software più recente (compresi i pacchetti di manutenzione) disponibile sul sito web ufficiale Kaspersky Lab (www.kaspersky.com) installata sul computer.

3. *Diritti di proprietà.* Il Software è protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorità e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprietà, i brevetti, i marchi commerciali e gli altri diritti di proprietà intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

4. *Riservatezza.* L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del codice di attivazione.

5. *Garanzia limitata.*

(i) Kaspersky Lab garantisce che per un periodo di [6] mesi a decorrere dal primo caricamento o installazione il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(ii) L'utente si assume ogni responsabilità relativamente al fatto che il presente Software soddisfi i propri requisiti. Kaspersky Lab non garantisce che il Software e/o la Documentazione siano idonei a soddisfare le esigenze dell'utente né che il suo utilizzo sia esente da interruzioni o privo di errori.

(iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) L'indennizzo dell'utente e la completa responsabilità di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che deciderà se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia. L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.

(v) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.

(vi) Le garanzie e le condizioni stabilite dal presente Contratto sostituiscono eventuali altre condizioni, garanzie o termini relativi alla fornitura o fornitura presunta dello stesso; la mancata fornitura o eventuali ritardi nella fornitura del Software o della Documentazione che, salvo per il presente paragrafo (vi) potrebbero avere effetto tra Kaspersky Lab e l'utente o potrebbero essere diversamente impliciti o integrati nel presente Contratto o in un eventuale accordo collaterale mediante statuto, diritto consuetudinario o altrimenti, sono esclusi mediante il presente (inclusi, senza tuttavia ad essi limitarsi, le condizioni implicite, le garanzie o altri termini relativi a qualità soddisfacente, idoneità per l'uso previsto o esercizio di ragionevoli competenze e cautele).

6. *Responsabilità limitata.*

(i) Nessun elemento del presente Contratto escluderà o limiterà la responsabilità di Kaspersky Lab in merito a (a) responsabilità civile per frode, (b) decesso o lesioni personali causate da un suo mancato esercizio di cautela ai sensi del diritto consuetudinario o dalla violazione negligente di una delle condizioni del presente Contratto, (c) eventuali altre responsabilità che non possano essere escluse per legge.

(ii) Ai sensi del paragrafo (i) di cui sopra, Kaspersky Lab non deve essere ritenuto responsabile (relativamente al contratto, per responsabilità civile, restituzione o altro) per i seguenti danni o perdite (siano questi danni o perdite previsti, prevedibili, noti o altro):

(a) perdita di reddito;

(b) perdita di utili effettivi o presunti (inclusa la perdita di utili sui contratti);

(c) perdita di liquidità;

(d) perdita di risparmi presunti;

(e) perdita di affari;

(f) perdita di opportunità;

(g) perdita di avviamento;

(h) danni alla reputazione;

(i) perdita, danni o corruzione di dati; o

(j) eventuali perdite indirette o conseguenti o danni arrecati in qualsiasi modo (inclusi, a scanso di dubbi, i danni o le perdite del tipo specificato nei paragrafi (ii), da (a) a (ii), (i).

(iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessuna altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

7. Il presente Contratto contiene per intero tutti gli intendimenti delle parti relativamente all'oggetto del presente e sostituisce tutti gli eventuali accordi, impegni e promesse precedenti tra l'utente e Kaspersky Lab, sia orali che per iscritto, che possano scaturire o essere impliciti da qualsiasi cosa scritta o pronunciata oralmente in fase di negoziazione tra Kaspersky Lab o suoi rappresentanti e l'utente precedentemente al presente Contratto; tutti gli accordi precedenti tra le parti relativamente all'oggetto di cui sopra decadranno a partire dalla Data di entrata in vigore del presente Contratto.

Quando si utilizza il Software demo, l'utente non può usufruire del Servizio Tecnico specificato nella Clausola 2 di questo EULA e neppure ha diritto di vendere la copia in possesso a terze parti.

All'utente è concesso l'uso del software a scopi dimostrativi per il periodo riportato nel file della chiave di avvio dal momento dell'attivazione (questo periodo può essere visto nella finestra Servizio del GUI del software).