KASPERSKY LAB

Kaspersky® Anti-Virus for Windows Servers 6.0

MANUALE DELL'UTENTE

KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Manuale dell'utente

© Kaspersky Lab
http://www.kaspersky.com

Data revisione: Luglio 2007

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 e la gamma di azioni illecite volte a minare la sicurezza delle informazioni si è moltiplicata.

I criminali informatici hanno mostrato grande interesse per le attività delle strutture statali e delle imprese commerciali. Essi cercano di impadronirsi di e divulgare informazioni riservate, che danneggia la reputazione delle imprese, interrompe la continuità delle attività commerciali e può pregiudicare le risorse informatiche delle 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. A quel punto il computer può essere utilizzato come parte di una rete zombie, una rete di computer infetti usati dagli hacker per attaccare i server, inviare spam, raccogliere informazioni riservate e diffondere nuovi virus e Trojan.

Oggigiorno chiunque riconosce il valore delle informazioni ed è consapevole della necessità di proteggere i dati. Al tempo stesso le informazioni deve essere facilmente accessibili a chi ne ha legittimamente bisogno (per esempio dipendenti, clienti e partner di un'impresa). Ecco quindi la necessità di creare un sistema di sicurezza completo per le informazioni, che 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 addirittura fenomeni non legati ad attività umane rappresentano potenziali minacce per la sicurezza dei dati. Partendo da questo presupposto, tutte le fonti di pericolo possono essere suddivise in tre gruppi:

- **Il 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*, inclusi cyber criminal, hacker, truffatori via Internet, società senza scrupoli e organizzazioni criminose.
    - *Interne*, incluse le azioni perpetrate dal personale aziendale. Le azioni di questo gruppo possono essere deliberate o accidentali.
- **Il fattore tecnologico**. Questo gruppo di minacce si riferisce a problemi tecnici: uso di software e hardware obsoleto o di scarsa qualità per l'elaborazione delle informazioni. Questi fattori determinano il malfunzionamento delle apparecchiature e, spesso, perdite di dati.
- **Il fattore calamità naturale**. Questo gruppo include l'intera gamma di eventi naturali non dipendenti dall'attività dell'uomo.

Un sistema di protezione dati efficiente deve tener conto di tutti questi fattori. Questo manuale d'uso 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

Internet è unica in quanto non appartiene a nessuno e non è delimitata da confini geografici. Per molti aspetti, questo ha promosso lo sviluppo delle risorse Web e lo scambio di informazioni. Oggi tutti possono accedere ai dati disponibili su Internet o creare la propria pagina web.

Tuttavia, queste stesse caratteristiche della rete mondiale consentono agli hacker di commettere attività illecite su Internet, rendendosi difficili da individuare e sfuggendo quindi alle pene che meriterebbero.

Gli hacker diffondono virus e altri programmi nocivi sui siti Internet, mascherandoli come utili programmi gratuiti. Inoltre gli script eseguiti automaticamente all'apertura di alcune pagine 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 server aziendali. Questi attacchi possono provocare il malfunzionamento di parti del sistema, oppure dare 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”.

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 al quale 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.

Posta elettronica

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. L'utente di un computer infetto, può inconsapevolmente inviare messaggi di posta elettronica infetti ad amici o colleghi che a loro volta inviano ulteriori messaggi infetti. Ad esempio, succede spesso che i file infetti passino inosservati e vengano inviati unitamente a informazioni aziendali nel sistema di posta elettronica interna di una grande società. Quando ciò avviene, sono molti gli utenti che vengono infettati. Potrebbe trattarsi di centinaia o migliaia di dipendenti dell'azienda, oltre alle eventuali decine di migliaia di abbonati.

Supporti di archiviazione esterni

I supporti di memoria rimovibili (dischetti, CD/DVD-ROM, e drive flash USB) sono ampiamente utilizzati per memorizzare e trasmettere informazioni.

Quando si apre un file contenente un codice nocivo memorizzato su un dispositivo di memoria rimovibile, si possono danneggiare i dati memorizzati sul computer locale e diffondere i virus alle altre unità del computer o agli atri computer sulla rete.

1.3. Tipi di minacce

Attualmente ci sono molte minacce alla sicurezza dei computer. Questa sezione esamina le minacce bloccate da Kaspersky Anti-Virus for Windows Servers.

Worm

Questa categoria di programmi nocivi si diffonde principalmente sfruttando le vulnerabilità dei sistemi operativi. Essi devono il loro nome (in italiano, "verme") alla capacità di strisciare da un computer all'altro

attraverso le reti e la posta elettronica. Questa caratteristica consente ai worm di diffondersi molto rapidamente.

I worm entrano in un computer, ricercano l'indirizzo di rete degli altri computer e inviano molteplici copie di loro stessi a questi indirizzi. Inoltre, i work utilizzano spesso i dati prelevati dalle rubriche dei client di posta elettronica. Alcuni di questi programmi nocivi talvolta creano file funzionanti sui dischi di sistema, ma possono eseguirsi anche senza alcuna risorsa di sistema tranne la RAM.

Virus

i virus sono programmi che infettano altri file, aggiungendo ad essi il proprio codice al fine di ottenere il controllo del file infetto non appena questo viene eseguito. Questa semplice definizione spiega l'azione fondamentale svolta da un un virus – l'*infezione*.

Trojan

Sono programmi che eseguono azioni non autorizzate sui computer, per esempio la cancellazione di dati sui drive provocando il blocco del sistema, il furto di informazioni riservate, 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. Il danno che provocano può essere molto maggiore di quello inferto dai virus tradizionali.

Ultimamente, la categoria più diffusa di programmi nocivi che danneggiano i dati sui computer 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

SI tratta di programmi inclusi nel software, sconosciuti all'utente, utilizzati per visualizzare messaggi pubblicitari. L'adware è generalmente incorporato nel software distribuito gratuitamente. Il messaggio pubblicitario è situato nell'interfaccia del programma. Questi programmi spesso raccolgono anche dati personali relativi all'utente per inviarli allo sviluppatore, modificando le impostazioni del browser (pagina iniziale e pagine di ricerca, livello di sicurezza, ecc.) e creando un traffico che l'utente non è in grado di controllare. Tutto ciò può provocare violazioni di sicurezza e, in ultima analisi, perdite finanziarie dirette.

Spyware

Si tratta di software che raccoglie informazioni su un particolare utente od organizzazione a loro insaputa. Spesso lo spyware sfugge completamente a qualsiasi identificazione. In generale gli obiettivi dello spyware sono:

- registrare le azioni dell'utente su un computer
- raccogliere informazioni sul contenuto del disco fisso; in questi casi, ciò implica spesso anche la scansione di varie directory e del registro di sistema per compilare un elenco del software installato sul computer
- Raccogliere informazioni sulla qualità della connessione, larghezza di banda, velocità del modem, ecc.

Riskware

Si tratta di software potenzialmente pericoloso che non ha una funzione nociva ma può essere utilizzato dagli hacker quale componente ausiliario per un programma nocivo, in quanto contiene buchi ed errori. In determinate condizioni, la presenza di tali programmi nel computer rappresenta una fonte di rischio per i dati. Questi programmi includono, per esempio, alcune utilità di amministrazione remota, commutatori di tastiera, client IRC, server FTP e utilità multifunzione per interrompere o nascondere i processi.

Esiste un altro tipo di programma nocivo analogo ad adware, spyware e riskware: si tratta di quei programmi che penetrano nel browser Web e ridirigono il traffico.

Joke

Si tratta di 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 relativi alla formattazione del disco fisso (anche se non ha luogo alcuna formattazione) o all'individuazione di virus in file non infetti.

Rootkit

Si tratta di utility che consentono di nascondere attività nocive. Esse nascondono programmi nocivi che impediscono agli antivirus di individuarli. Essi modificano le funzioni base del sistema operativo del computer per nascondere sia la propria esistenza che le azioni intraprese dagli hacker sul computer infetto.

Altri programmi pericolosi

Si tratta di programmi creati, ad esempio, per lanciare attacchi DoS (Denial of Service) su server remoti e penetrare in altri computer; essi 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.

Attenzione!

Da qui in avanti, verrà utilizzato il termine "virus" per fare riferimento ai programmi nocivi e pericolosi. Il tipo di programma nocivo verrà specificato solo se necessario.

CAPITOLO 2. KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS 6.0

Kaspersky Anti-Virus for Windows Servers 6.0 annuncia una nuova generazione di prodotti per la sicurezza dei dati.

2.1. Novità di Kaspersky Anti-Virus for Windows Servers 6.0

Osserviamo più in dettaglio le nuove funzioni di Kaspersky Anti-Virus for Windows Servers.

Nuove funzionalità di protezione

- La tecnologia di protezione dei file del programma è stata modificata: adesso è possibile ridurre il carico sui sottosistemi disco e processore centrale ed accelerare le scansioni dei file, grazie a iCheck e iSwift. Così facendo, il programma evita di analizzare nuovamente i file già esaminati.
- Il processo di scansione si svolge ora come attività in background, consentendo all'amministratore di continuare ad usare il computer. Se più programmi si disputano le risorse di sistema, la scansione anti-virus entra in pausa finché l'utente non ha terminato la propria attività, per poi riprendere da dove era stata interrotta.
- Le aree critiche del server dove le infezioni potrebbero produrre gravi conseguenze vengono sottoposte a una scansione specifica. È possibile configurare quest'attività in modo che venga eseguita ad ogni avvio del sistema.
- La funzione di notifica dell'utente (vedere 11.8.1 a pag. 141) è stata ampliata includendo determinati eventi che si verificano durante il funzionamento del programma. Il metodo di notifica può essere selezionato autonomamente per ciascuno di questi tipi di eventi: e-mail, notifiche sonore, messaggi pop-up.
- Le nuove funzioni comprendono le tecnologia di autodifesa dell'applicazione, la protezione dall'accesso remoto non autorizzato da parte di servizi di programmi, la protezione dei file dell'applicazione

dall'accesso o dalla modifica senza autorizzazione, e la protezione con password delle impostazioni del programma.

Nuove funzioni dell'interfaccia del programma

- La nuova interfaccia di Kaspersky Anti-Virus for Windows Servers agevola l'uso delle funzioni del programma. È inoltre possibile modificare l'aspetto del programma utilizzando grafica e schemi di colori personalizzati.
- Il programma offre regolarmente suggerimenti durante l'uso: Kaspersky Anti-Virus for Windows Servers visualizza messaggi informativi sul livello di protezione, accompagna il proprio funzionamento con suggerimenti e consigli e offre un'esauriente Guida in linea.

Nuove funzioni di aggiornamento del programma

- Questa versione dell'applicazione introduce una nuova e più potente procedura di aggiornamento: Kaspersky Anti-Virus verifica automaticamente la presenza di pacchetti di aggiornamento sulla sorgente degli aggiornamenti. Quando Anti-Virus rileva nuovi aggiornamenti, li scarica e li installa sul computer.
- Il programma scarica gli aggiornamenti in maniera incrementale, ignorando i file già scaricati. Questo riduce il traffico di download degli aggiornamenti di anche 10 volte.
- Gli aggiornamenti vengono scaricati dalla sorgente più efficiente.
- Il programma è dotato di una funzione di ripristino dello stato precedente, che consente di ripristinare la precedente versione delle firme se, per esempio, le firme installate risultano danneggiate o si è verificato un errore durante la copia.
- La funzione di aggiornamento comprende ora uno strumento che rende gli aggiornamenti accessibili agli altri computer della rete copiandoli in una cartella locale, per risparmiare larghezza di banda.

2.2. I componenti di difesa di Kaspersky Anti-Virus for Windows Servers 6.0

La difesa di Kaspersky Anti-Virus for Windows Servers comprende:

- File Anti-Virus(vedere 2.2.1 a pagina 17), che monitora il file system del computer in di tempo reale.

- Attività di scansione anti-virus (vedere 2.2.2 a pag. 17) che esaminano la memoria ed il file system del computer come anche singoli file, cartelle, dischi o aree alla ricerca di virus.
- Strumenti di supporto (vedere 2.2.3 a pag. 18) che offrono assistenza sul programma e ne estendono le funzionalità.

2.2.1. File Anti-Virus

Il server è protetto in tempo reale grazie a **File Anti-Virus**.

Un file system può contenere virus e altri programmi pericolosi. I programmi nocivi possono restare in un 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 per attivare istantaneamente il virus.

File Antivirus è il componente che monitora il file system del computer. Esso esamina tutti i file che vengono aperti, eseguiti o salvati sul server e su tutte le unità disco collegate. Kaspersky Anti-Virus intercetta ogni tentativo di accedere ad un file e lo esamina alla ricerca 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 è possibile disinfettare un file, esso viene eliminato dopo averne salvata una copia nella cartella Backup (vedere 11.2 a pag. 124), o trasferito in Quarantena (vedere 11.1 a pag. 120).

2.2.2. Attività di scansione antivirus

Oltre a monitorare costantemente con File Anti-Virus i possibili percorsi accessibili ai programmi nocivi, è estremamente importante eseguire periodicamente la scansione antivirus del computer. Ciò è necessario al fine di rilevare i programmi nocivi non ancora rilevati da File Anti-Virus, ad esempio a causa della protezione impostata su un livello insufficiente.

Kaspersky Anti-Virus for Windows Servers configura per impostazione predefinita le seguenti attività di scansione:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del computer. Ciò comprende la memoria del sistema, i programmi caricati all'avvio, i settori di boot del disco fisso e le directory di sistema di*Microsoft Windows*. Tale funzione ha lo scopo di individuare rapidamente i virus senza operare la 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.

È possibile inoltre creare altre attività di scansione anti-virus e pianificarne l'esecuzione.

2.2.3. Strumenti del programma

Kaspersky Anti-Virus for Windows Servers 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.

Aggiornamento

Per poter essere sempre pronto ad eliminare virus o altri programmi pericolosi, Kaspersky Anti-Virus for Windows Servers deve essere mantenuto aggiornato. Il componente di *aggiornamento* è progettato esattamente per questo. È responsabile dell'aggiornamento dell'elenco dei virus e dei moduli del programma di Kaspersky Anti-Virus for Windows Servers.

La funzione Aggiorna distribuzione consente di salvare gli aggiornamenti al database dell'elenco dei virus ed ai moduli dell'applicazione recuperati dai server di aggiornamento di Kaspersky Lab e concedere ad altri computer l'accesso ad essi per risparmiare larghezza di banda.

File di dati

File Anti-Virus, come anche ogni attività di scansione anti-virus e di aggiornamento del programma, crea un rapporto. I rapporti contengono informazioni sulle operazioni completate e i relativi risultati. Utilizzando la funzione *Report*, l'utente sarà sempre aggiornato sul funzionamento di qualsiasi componente di Kaspersky Anti-Virus for Windows Servers. In caso di problemi, è possibile inviare i rapporti a Kaspersky Lab in modo da consentire ai nostri esperti di studiare la situazione in maniera approfondita e fornire la soluzione più rapida possibile.

Kaspersky Anti-Virus for Windows Servers invia tutti i file di cui sospetta la pericolosità in una speciale area di *Quarantena*, dove vengono conservati in formato criptato per evitare di infettare il computer. Questi oggetti possono essere sottoposti a scansione antivirus, ripristinati nella posizione originaria, eliminati o trasferiti manualmente in Quarantena.

Tutti i file che al termine della scansione antivirus non risultano infetti vengono automaticamente ripristinati nella posizione originaria.

L'area di *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. Tali copie di backup sono anch'esse memorizzate in forma criptata per impedire ulteriori infezioni.

È possibile ripristinare manualmente i file contenuti nell'area di Backup ed eliminarne la copia.

Supporto

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

Tramite i collegamenti, è possibile accedere al forum degli utenti di Kaspersky Lab e consultare le domande più frequenti con le domande che potrebbero favorire la risoluzione del problema. È inoltre possibile inviare un rapporto di errore o una domanda sul funzionamento del programma all'Assistenza tecnica, compilando un modulo on-line.

Ma è possibile anche accedere all'Assistenza tecnica online, e, naturalmente, i nostri dipendenti saranno sempre lieti di aiutarvi 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, 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 for Windows Servers 6.0 dal CD di installazione)
- Microsoft Internet Explorer 5.5 o successivo (per aggiornare gli elenchi delle minacce e i moduli del programma attraverso Internet)
- Microsoft Windows Installer 2.0

Sistema operativo:

- Microsoft Windows 2000 Server/Advanced Server Service Pack 4 o superiore, con tutti gli aggiornamenti disponibili.
- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, tutti i Service Packs, tutti gli aggiornamenti disponibili.
- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

2.4. Pacchetti software

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

La versione in scatola include:

- Una busta sigillata con CD di installazione contenente i file del programma
- Una chiave di licenza, inclusa col pacchetto d'installazione o su uno speciale dischetto, oppure un codice di attivazione dell'applicazione su CD
- Un manuale d'uso
- 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 for Windows Servers attraverso Internet, copierà il prodotto dal sito web di Kaspersky Lab (**Downloads** → **Versioni trial**). Il manuale d'uso del prodotto può essere scaricato nella sezione **Downloads** → **Documentazione**.

La chiave di licenza o il codice di attivazione verranno inviati via posta elettronica una volta ricevuto il pagamento.

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 l'EULA.

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 for Windows Servers.

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)

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 FOR WINDOWS SERVERS 6.0

Kaspersky Anti-Virus for Windows Servers 6.0 può essere installato in diversi modi:

- Installazione locale: installa l'applicazione su un solo host. È necessario l'accesso diretto all'host in questione per eseguire e portare a termine l'installazione. L'installazione locale può essere eseguita in uno dei due seguenti modi:
    - installazione interattiva tramite la Procedura guidata dell'applicazione (vedere 3.1 a pag. 23); questa modalità richiede l'input dell'utente per procedere nell'installazione;
    - un'installazione non interattiva lanciata da riga di comando utilizzando le impostazioni predefinite, che non richiede alcun input da parte dell'utente per procedere (vedere 3.3 a pag. 33).
- Installazione remota: installa l'applicazione in remoto nei computer in rete da una workstation di amministrazione, utilizzando:
    - la suite software Kaspersky Administration Kit (vedere la Guida di distribuzione di Kaspersky Administration Kit);
    - Le regole di dominio di gruppo di Microsoft Windows Server 2000/2003 (vedere 3.4 a pag. 34).

Si consiglia di chiudere tutte le applicazioni in esecuzione prima di installare Kaspersky Anti-Virus (comprese le installazioni remote).

Nel caso Kaspersky Anti-Virus 5.0 sia già installato, verrà disinstallato ed aggiornato a Kaspersky Anti-Virus 6.0 quando si esegue la procedura di installazione (vedere 3.5 a pag. 36 per ulteriori dettagli). Gli aggiornamenti alle build più recenti (versioni minori) di Kaspersky Anti-Virus 6.0 sono trasparenti.

3.1. Installazione tramite la procedura guidata

Per installare Kaspersky Anti-Virus for Windows Servers sul computer, aprire il file di Windows Installer nel CD di installazione.

> Nota:
>
> La procedura di installazione del programma tramite un pacchetto scaricato da Internet è uguale a quella tramite CD.

Si apre la 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.
- **Annulla** – 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 for Windows Servers

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 for Windows Servers. 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 del problema. Prima di installare Kaspersky Anti-Virus for Windows Servers si consiglia 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 for Windows Servers.

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

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

La finestra di dialogo successiva contiene il 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 annullare l'installazione fare clic su **Annulla**.

Passaggio 4. Scelta di una cartella di installazione

La fase successiva dell'installazione di Kaspersky Anti-Virus for Windows Servers serve per stabilire la posizione in cui installare il programma sul computer. Il percorso predefinito è:

- **<Drive>\Programmi\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers** – per sistemi a 32 bit
- **<Drive>\Programmi (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers** – per sistemi a 64 bit

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.

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

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

Passaggio 5. Utilizzo delle impostazioni di installazione salvate

In questa fase, viene richiesto di specificare se si desidera utilizzare impostazioni di sicurezza o elenchi dei virus precedentemente salvati, se si è effettivamente provveduto al salvataggio quando una precedente installazione di Kaspersky Anti-Virus 6.0 è stata disinstallata dal server.

Esaminiamo in dettaglio le opzioni sopra descritte.

Se precedentemente era stata installata sul computer un'altra versione o build di Kaspersky Anti-Virus for Windows Servers e ne è stato salvato l'elenco dei virus

al momento della disinstallazione, è possibile utilizzarlo anche nella nuova versione. Affinché ciò sia possibile, selezionare **Usa firme delle minacce salvate in precedenza**. In questo caso, gli elenchi dei virus inclusi nell'installazione del programma non saranno copiati sul server.

Per utilizzare le impostazioni di protezione configurate e salvate da una versione precedente, selezionare **Usa impostazioni dell'applicazione salvate in precedenza**.

Passaggio 6. Scelta di un tipo di installazione

In questa fase si selezionano i componenti del programma che si desidera installare sul computer. Sono possibili tre opzioni:

Completa. Selezionando questa opzione, si installano tutti i componenti di Kaspersky Anti-Virus for Windows Servers.

Personalizzata. Questa opzione consente di selezionare i componenti del programma che si desidera installare. Per ulteriori informazioni, vedere Passaggio 7.

Per selezionare un tipo di installazione, fare clic sul pulsante appropriato.

Passaggio 7. Scelta dei componenti da installare

Questa fase si presenta solo se è stata selezionato il tipo di installazione **Personalizzata**.

Se è stata selezionata l'installazione personalizzata, è necessario selezionare i componenti di Kaspersky Anti-Virus for Windows Servers che si desidera installare. Per impostazione predefinita, sono selezionati per l'installazione File Anti-Virus, il componente di scansione antivirus, nonché il connettore ad Administration Agent per l'amministrazione remota tramite Kaspersky Administration Kit.

Per selezionare i componenti desiderati, fare clic sull'icona a fianco del nome di un componente e selezionare **Sarà installata sul disco fisso rigido locale** dal menu apertosi. Ulteriori informazioni sul tipo di protezione offerto da un determinato componente e sulla quantità di spazio su disco necessario per l'installazione sono disponibili nella parte inferiore della finestra del programma di installazione.

Se non si desidera installare un componente, selezionare la voce **L'intera funzionalità non sarà disponibile** dal menù contestuale.

Una volta selezionati i componenti da installare, fare clic su **Avanti**. Per tornare all'elenco dei programmi predefiniti da installare, fare clic su **Reimposta**.

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 for Windows Servers.

Il programma di installazione visualizza sullo schermo un elenco di tali programmi, se rilevati. 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 (solo i prodotti Kaspersky Lab verranno eliminati automaticamente).

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 server.

È sconsigliabile deselezionare l'opzione **Abilità autodifesa prima dell'installazione** alla prima installazione di Kaspersky Anti-Virus 6.0. Abilitando i moduli di protezione, è possibile annullare l'installazione se si verificano errori durante l'installazione del programma. Se si sta reinstallando il programma, si consiglia invece di deselezionare questa casella di controllo.

Se l'applicazione è installata in remoto via **Windows Remote Desktop**, si consiglia di selezionare l'opzione **Abilita autodifesa prima dell'installazione**. In caso contrario, la procedura di installazione potrebbe non terminare o terminare erroneamente.

Se si desidera che le esclusioni raccomandate da Microsoft per i server siano aggiunte automaticamente alle esclusioni, selezionare **Escludere le aree raccomandate da Microsoft dalle scansioni antivirus**.
Se si desidera che la variabile di ambiente %Path% sia aggiunta a avp.com dopo l'installazione, selezionare **Aggiungi percorso ad avp.com alla variabile di sistema %PATH%**.

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

Attenzione!

Quando i componenti di Kaspersky Anti-Virus che intercettano il traffico di rete vengono installati, vengono interrotte le connessioni di rete correnti. La maggior parte di esse saranno ripristinate dopo breve tempo.

Passaggio 10. Completamento della procedura di installazione

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

Per avviare la procedura guidata, fare clic sul pulsante **Avanti** (vedere 3.2 a pag. 27).

Per completare correttamente l'installazione è necessario riavviare il computer, seguendo il suggerimento del messaggio visualizzato sullo schermo.

3.2. Impostazione guidata

La procedura guidata di configurazione di Kaspersky Anti-Virus for Windows Servers 6.0 si avvia al termine dell'installazione del programma. Essa è progettata per agevolare la configurazione iniziale delle impostazioni del programma in base alle specifiche funzioni e operazioni del computer dell'utente.

L'interfaccia della procedura guidata è concepita come una procedura guidata standard di Windows ed è costituita da una serie di passaggi tra i quali è possibile navigare utilizzando i pulsanti **Indietro** e **Avanti**; per completare la procedura, fare clic sul pulsante **Fine.** Per uscire dalla procedura in qualsiasi momento, fare clic su **Annulla**.

Se si arresta la procedura guidata chiudendone la finestra, l'applicazione non verrà eseguita. Ogni volta che si avvia l'applicazione, partirà la procedura guidata finché essa non sarà stata completata con successo.

3.2.1. Uso di oggetti salvati con la versione 5.0

Questa finestra della procedura guidata dopo aver terminato di installare l'applicazione su Kaspersky Anti-Virus 5.0. Verrà richiesto di selezionare quali dati utilizzati dalla versione 5.0 si desidera importare nella versione 6,0 Ciò può includere i file in quarantena o backup o le impostazioni di protezione.

Per utilizzare questi oggetti nella versione 6,0, selezionare le caselle corrispondenti.

3.2.2. Attivazione del programma

Prima di attivare il programma, verificare che la data di sistema impostata sul computer corrisponda a quella attuale.

Il programma viene attivato installando una chiave di licenza che Kaspersky Anti-Virus utilizzerà per verificare il contratto di licenza e determinarne la data di scadenza.

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

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

3.2.2.1. Scelta di un metodo di attivazione del programma

In funzione del fatto che si disponga di una chiave di licenza per Kaspersky Anti-Virus o che occorra ottenerne una dal server Kaspersky Lab, il programma può essere attivato in vari modi:

- **Attivazione attraverso il 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 di attivazione consente di ottenere un file chiave che garantisce l'accesso alla funzionalità completa 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. Si riceverà una chiave gratuita valida per il periodo descritto nell'accordo di licenza per la versione di prova.
- **Applicazione della chiave di licenza esistente**. Il programma viene attivato utilizzando un file chiave di licenza per Kaspersky Anti-Virus 6.0.
- **Attivare in seguito**. Selezionando questa opzione si omette la fase di attivazione. Kaspersky Anti-Virus for Windows Servers 6.0 viene installato sul computer e si potrà accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (è possibile aggiornare gli elenchi delle minacce solo dopo l'installazione del programma).

Le prime due opzioni di attivazione utilizzano un server web di Kaspersky Lab, che richiede una connessione a Internet. Prima di attivare, modificare le impostazioni di rete (vedere 10.4.3 a pag. 114) nella finestra che sui apre

facendo clic su **Impostazioni LAN** (se è il caso). Per informazioni più approfondite sulla configurazione delle impostazioni di rete, consultare l'amministratore di sistema o l'ISP.

Se non si dispone di connessione a Internet quando si installa il programma, si può attivare l'applicazione successivamente (vedere 11.5 a pag. 135) tramite la sua interfaccia, oppure si può utilizzare l'accesso a Internet di un altro computer per registrarsi presso il sito web Assistenza tecnica di Kaspersky Lab e ottenere la chiave di licenza utilizzando il codice di attivazione.

3.2.2.2. Inserimento del codice di attivazione

Per attivare il programma occorre inserire il codice di attivazione. Se il programma viene acquistato via Internet, il codice di attivazione verrà ricevuto via posta elettronica. Se invece il programma viene acquistato in confezione, il codice di attivazione è sulla busta del CD di installazione.

Il codice di attivazione è una sequenza di numeri e lettere separati da trattini in quattro sezioni, composte da cinque caratteri ciascuna, senza spazi. Ad esempio, 11AA1-11AAA-1AA11-1A111. Si noti che il codice deve essere inserito in caratteri latini.

Immettere i dati di contatto nella parte inferiore della finestra: Nome completo, indirizzo e-mail, Paese e città di residenza. Queste informazioni possono essere richieste per identificare un utente registrato se, per esempio, la chiave viene persa o rubata. In tal caso, le informazioni di contatto immesse consentiranno di ottenere una nuova chiave di licenza.

3.2.2.3. Come procurarsi un file chiave di licenza

La procedura guidata delle impostazioni si collega ai server di Kaspersky Lab ed invia i dati di registrazione (codice di attivazione e informazioni personali), che vengono verificati sul server.

Se il codice di attivazione viene accettato, la procedura guidata riceve un file con la chiave di licenza. Se si installa una versione demo del programma la procedura guidata delle impostazioni riceve un file con una chiave di prova senza codice di attivazione.

Il file ricevuto sarà installato automaticamente per utilizzare il programma e verrà visualizzata una finestra di completamento dell'attivazione con informazioni dettagliate sulla chiave di licenza utilizzata.

Se il codice di attivazione non viene accettato, sullo schermo verrà visualizzato un messaggio corrispondente. In tal caso, contattare il rivenditore presso il quale è stato acquistato il software per ulteriori informazioni.

3.2.2.4. Selezione di un file chiave di licenza

Se si dispone di un file contenente la chiave di licenza di Kaspersky Anti-Virus for Windows Servers 6.0, la finestra della procedura guidata chiederà di 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 a cui è intestata la registrazione del software, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della chiave di licenza.

3.2.2.5. 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 a cui è intestata la registrazione del software, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della chiave di licenza.

3.2.3. Configurazione delle impostazioni di aggiornamento

La sicurezza del computer dipende direttamente dall'aggiornamento regolare degli firme delle minacce 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.

- **Automaticamente**. Kaspersky Anti-Virus verifica ad intervalli specificati la disponibilità di nuovi pacchetti di aggiornamento presso la relativa sorgente. Le scansioni possono essere impostate in modo da essere più frequenti durante le epidemie di virus e meno frequenti quando sono passate. Quando Anti-Virus rileva nuovi aggiornamenti, li scarica e li installa sul computer. È la modalità predefinita.
- **Come pianificato**.Gli aggiornamenti saranno eseguiti automaticamente in base al programma creato. Per configurare la programmazione fare clic su **Cambia**.
- **Manualmente**. Questa opzione consente di eseguire manualmente gli aggiornamenti.

Osservare che, al momento dell'installazione del programma, gli elenchi delle minacce 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 for Windows Servers scarica quindi gli aggiornamenti necessari dai server remoti dedicati e li installa sul computer.

Per configurare le impostazioni di aggiornamento (impostare le proprietà di rete, selezionare le risorse da cui scaricare gli aggiornamenti, impostare l'esecuzione di attività con un certo account o abilitare la funzione di distribuzione degli aggiornamenti) fare clic su **Impostazioni**.

3.2.4. Pianificazione 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 for Windows Servers, vengono create tre attività di scansione antivirus predefinite. In questa finestra, viene richiesto di scegliere un'impostazione iniziale per l'attività di scansione:

Scansione oggetti ad esecuzione automatica

Kaspersky Anti-Virus esaminerà automaticamente gli oggetti ad esecuzione automatica all'avvio, per impostazione predefinita. Le impostazioni di pianificazione possono essere modificate in un'altra finestra facendo clic su **Cambia**.

Scansione aree critiche

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

Per impostazione predefinita, questa scansione automatica è disabilitata.

Scansione completa del computer

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

L'impostazione predefinita per l'esecuzione pianificata di questa scansione automatica è disabilitata. Tuttavia, si raccomanda di eseguire una scansione anti-virus completa del server subito dopo aver installato il programma.

3.2.5. Restrizioni di accesso al programma

Kaspersky Anti-Virus dà la possibilità di proteggere il programma con una password, poiché diverse persone potrebbero utilizzare lo stesso computer e diversi programmi pericolosi potrebbero disabilitare la protezione. 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 mediante password, selezionare ☑ **Abilita protezione mediante password** e compilare i campi **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 tenta di effettuare qualsiasi azione con il programma tranne rispondere agli avvisi nel momento in cui vengono rilevati oggetti pericolosi.
- ◉ **Operazioni selezionate:**
  - ☑ **Salvataggio impostazioni programma** – richiede la password quando un utente cerca di salvare le modifiche alle impostazioni del programma.
  - ☑ **Uscita dal programma in esecuzione** – richiede la password se un utente cerca di uscire dal programma.
  - ☑ **Arresto/sospensione componenti di protezione o attività di ricerca virus** – richiede la password se l'utente cerca di sospendere o di disabilitare completamente qualsiasi componente anti-virus o un'operazione di scansione anti-virus.

3.2.6. Completamento della procedura di configurazione guidata

L'ultima finestra della procedura guidata visualizza un messaggio che comunica che il programma è stato installato e configurato correttamente. È possibile avviare immediatamente l'applicazione selezionando ☑ **Avvia prodotto**.

Se qualcosa è andato storto durante l'installazione, ad esempio problemi di incompatibilità con altre applicazioni anti-virus, verrà richiesto di riavviare il computer.

3.3. Installazione del programma da riga di comando

Per installare Kaspersky Anti-Virus for Windows Servers 6.0, immettere questo comando alla riga di comando:

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

Parte l'installazione guidata (vedere 3.1 a pag. 23). Una volta installato il programma, è necessario riavviare il computer.

Per installare l'applicazione in modalità non interattiva, (senza la procedura guidata), immettere:

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

Questa opzione richiede il riavvio della macchina manualmente una volta terminata l'installazione. Per eseguire un riavvio automatico dalla riga di comando, immettere:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

Si noti che un riavvio automatico avrà luogo in modalità non interattiva (tramite il tasto /qn).

Per installare l'applicazione con una password di disinstallazione, immettere:

`msiexec /i <package_name> KLUNINSTPASSWD=******`, durante l'esecuzione di un'installazione interattiva;

`msiexec /i <package_name> KLUNINSTPASSWD=****** /qn`, durante l'esecuzione di un'installazione non interattiva senza riavvio del sistema;

`msiexec /i <package_name> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn`, durante l'esecuzione di un'installazione non interattiva con riavvio del sistema;

Se si installa Kaspersky Anti-Virus in modalità non interattiva, è possibile accedere al file *setup.ini*, che contiene le impostazioni generali per l'installazione dell'applicazione (vedere A.4 a pag. 192), al file di configurazione *install.cfg* (vedere 13.7 a pag. 180), nonché al file chiave di licenza. Si noti che questi file devono essere ubicati nella stessa cartella nella quale si trova il pacchetto di installazione di Kaspersky Anti-Virus.

3.4. Procedura per installare l'Oggetto delle Regole di Gruppo

Questa funzione è supportata sui computer che eseguono Microsoft Windows 2000 Server o versioni successive.

Utilizzando l'**Editor delle regole di gruppo**, è possibile installare, aggiornare e disinstallare Kaspersky Anti-Virus sulle workstation dell'azienda comprese nel dominio, senza utilizzare Kaspersky Administration Kit.

3.4.1. Installazione del programma

Per installare Kaspersky Anti-Virus:

1. Creare una cartella condivisa sul computer che funge da controllore del dominio, e copiare in essa il pacchetto di installazione *.msi* di Kaspersky Anti-Virus.

   È inoltre possibile copiare nella stessa posizione il file *setup.ini*, che contiene le impostazioni generali per l'installazione dell'applicazione (vedere A.4 a pag. 192), il file di configurazione *install.cfg* (vedere 13.7 a pag. 180), nonché il file chiave di licenza.

2. Aprire l'**Editor oggetti Criteri di gruppo** tramite la MMC (per maggiori informazioni sull'utilizzo dell'Oggetto Criteri di Gruppo, consultare la guida di Microsoft Windows Server).

3. Creare un nuovo pacchetto. Per fare ciò, selezionare dall'albero della console **Oggetto criteri di gruppo/ Configurazione computer/ Impostazioni del software/ Installazione software** ed utilizzare il comando **Nuovo/ Pacchetto** dal menù contestuale.

   Nella finestra che si apre, specificare il percorso alla cartella condivisa contenente il programma di installazione di Anti-Virus (vedere 1). Selezionare **Assegna** dalla finestra di dialogo **Seleziona metodo di distribuzione** e fare clic su **OK**.

La regola di gruppo verrà applicata su ciascuna workstation alla prossima registrazione del computer nel dominio. Kaspersky Anti-Virus verrà allora installato su tutti i computer.

3.4.2. Upgrade del programma

Per effettuare l'upgrade di Kaspersky Anti-Virus:

1. Copiare nella cartella condivisa il pacchetto di installazione contenente l'aggiornamento di Kaspersky Anti-Virus in formato *.msi*.
2. Aprire l'**Editor oggetti Criteri di gruppo** e creare un nuovo pacchetto utilizzando i passaggi dettagliati sopra.
3. Selezionare il nuovo pacchetto, quindi selezionare il comando **Proprietà** dal menù contestuale. Nella finestra delle proprietà del pacchetto, scegliere la scheda **Aggiornamenti**, quindi specificare il pacchetto che contiene il programma d'installazione per la precedente versione di Kaspersky Anti-Virus. Per installare l'upgrade di Kaspersky Anti-Virus mantenendo le proprie impostazioni di protezione, selezionare l'opzione di effettuare l'upgrade della versione precedente.

La regola di gruppo verrà applicata su ciascuna workstation alla prossima registrazione del computer nel dominio.

Si noti che non è possibile eseguire l'upgrade di Kaspersky Anti-Virus utilizzando l' Editor delle regole di gruppo sui computer che utilizzano Microsoft Windows 2000 Server.

3.4.3. Disinstallazione del programma

Per disinstallare Kaspersky Anti-Virus

1. Aprire l'**Editor oggetti Criteri di gruppo**.
2. A tal fine, dall'albero della console, selezionare **Oggetto criteri di gruppo/Configurazione computer/ Impostazioni software/Installazione software**.

   Selezionare il pacchetto Kaspersky Anti-Virus dall'elenco. Aprire il menù contestuale e selezionare il comando **Tutte le attività/Elimina**.

   Nella finestra di dialogo **Rimuovi software**, **Disinstalla subito il software dagli utenti e dai computer** per disinstallare Kaspersky Anti-Virus al prossimo riavvio di un computer.

3.5. Upgrade dalla versione 5.0 alla versione 6.0

Se Kaspersky Anti-Virus 5.0 for Windows File Servers è installato sul server, è possibile eseguirne l'upgrade a Kaspersky Anti-Virus 6.0 for Windows Servers.

Una volta avviato il programma d'installazione per Kaspersky Anti-Virus 6.0, sarà possibile scegliere se prima disinstallare la versione 5.0 già installata del prodotto. Una volta disinstallato il programma, è necessario riavviare il computer, dopodiché inizierà l'installazione della versione 6.0.

Attenzione!

Se si sta installando Kaspersky Anti-Virus 6.0 for Windows Servers da una cartella di rete protetta da password su una versione precedente del programma, si tenga presente quanto segue: Dopo aver disinstallato la versione 5.0 dell'applicazione e aver riavviato il computer, il programma di installazione non consentirà di accedere alla cartella di rete dove è ubicato il pacchetto di installazione dell'applicazione. Di conseguenza, l'installazione del programma verrà interrotta. Per installare correttamente il programma, eseguire il programma d'installazione esclusivamente da una cartella locale.

CAPITOLO 4. INTERFACCIA DEL PROGRAMMA

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

- Icona dell'area di notifica (vedere 4.1 a pag. 37)
- Il menù contestuale (vedere 4.2 a pag. 38)
- Finestra principale (vedere 4.3 a pag. 39)
- Finestra delle impostazioni del programma (vedere 4.4 a pag. 41)

4.1. L'icona dell'area di notifica

Subito dopo aver installato Kaspersky Anti-Virus for Windows Servers, viene visualizzata l'icona corrispondente nell'area di notifica.

L'icona è un indicatore delle funzioni di Kaspersky Anti-Virus for Windows Servers. Riflette lo stato della protezione e visualizza numerose funzioni di base eseguite dal programma.

Se l'icona è attiva  (colorata), il computer è protetto. Se l'icona non è attiva  (bianco e nero), la protezione in tempo reale è disattivata.

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

	Scansione in corso di un file in fase di apertura, salvataggio o esecuzione da parte dell'utente o di un programma.
	Gli elenchi delle minacce di Kaspersky Anti-Virus e i moduli del programma sono in fase di aggiornamento.
	Si è verificato un errore in qualche componente di Kaspersky Anti-Virus.

L'icona consente inoltre di accedere alle funzioni di base dell'interfaccia del programma: il menu di scelta rapida (vedere 4.2 a pag. 38) e la finestra principale (vedere 4.3 a pag. 39).

Per aprire il menu di scelta rapida, fare clic con il tasto destro del mouse sull'icona del programma.

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

4.2. Il menu di scelta rapida

Il menu di scelta rapida consente di eseguire le attività di protezione di base (vedere Figura 1).

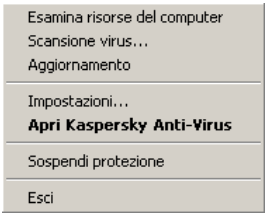


Figura 1. Il menu di scelta rapida

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

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

Scansione virus... – seleziona gli oggetti e ne esegue la scansione antivirus. L'elenco predefinito contiene diversi file, tra cui la memoria di sistema, la cartella di avvio, i database di posta, tutte le unità del computer, ecc. È possibile aggiungere elementi all'elenco, selezionare file da esaminare e avviare scansioni antivirus.

Aggiornamento – avvia l'aggiornamento dei moduli del programma e degli elenchi dei virus e li installa sul computer.

Attiva... – attiva il programma. È necessario attivare la versione utilizzata di Kaspersky Internet Security per ottenere lo status di utente registrato, che garantisce l'accesso alla piena funzionalità dell'applicazione ed al Supporto tecnico. Questa voce di menu è disponibile solo se il programma non è attivato.

Impostazioni... – visualizza e configura le impostazioni di Kaspersky Anti-Virus for Windows Servers.

Apri Kaspersky Anti-Virus – apre la finestra principale del programma (vedere 4.3 a pag. 39).

Sospendi protezione / Riprendi protezione – disabilita o abilita temporaneamente File Anti-Virus (vedere 2.2.1 a pag. 17). Questa voce di menu non influisce sugli aggiornamenti del programma o sulle attività di scansione antivirus.

Esci – chiude Kaspersky Anti-Virus for Windows Servers (quando viene selezionata questa opzione, l'applicazione viene scaricata dalla RAM del computer).

Durante un'attività di scansione antivirus, il menu di scelta rapida visualizza il nome dell'attività accompagnato da un indicatore della percentuale di avanzamento. Selezionando l'attività, è possibile aprire la finestra dei rapporti per visualizzare i risultati correnti.

4.3. La finestra principale del programma

La finestra principale di Kaspersky Anti-Virus for Windows Servers (vedere Figura 2) può essere suddivisa logicamente in due parti:

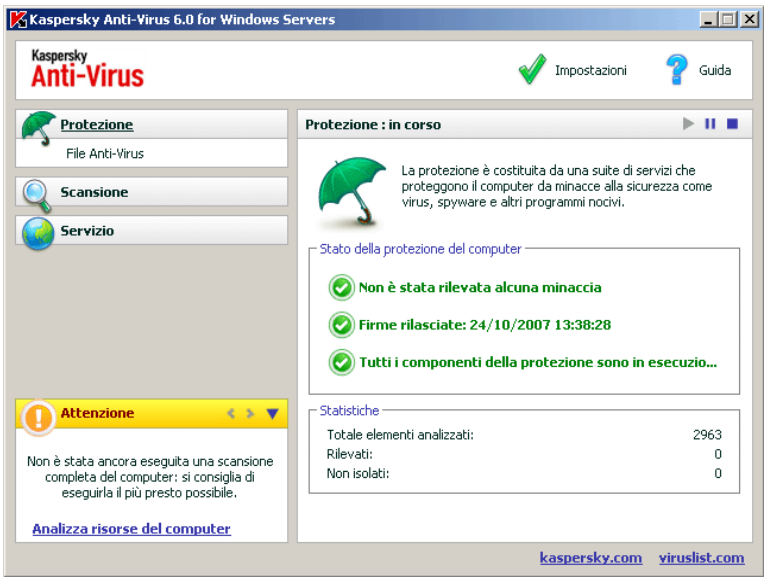
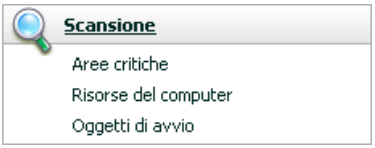


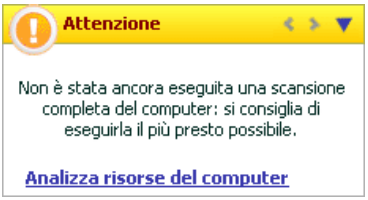
Figura 2. Finestra principale di Kaspersky Anti-Virus for Windows Servers

- la parte sinistra della finestra, il pannello di navigazione, consente di aprire in maniera semplice e veloce qualsiasi componente e di visualizzare i risultati delle scansioni antivirus o delle attività di aggiornamento o gli strumenti di supporto del programma;
- la parte destra della finestra, il pannello informativo, contiene informazioni sul componente di protezione selezionato nella parte sinistra della finestra e visualizza le impostazioni di ciascuno di essi, fornendo gli strumenti per effettuare scansioni antivirus, lavorare con i file in quarantena e le copie di backup, gestire le chiavi di licenza, e così via.

Dopo aver selezionato una sezione nella parte sinistra della finestra, la parte destra conterrà informazioni corrispondenti alla selezione effettuata.

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

Sezione della finestra principale	Scopo
Questa finestra fornisce principalmente informazioni sullo stato di protezione del computer. La sezione **Protezione** ha proprio questa funzione. 	Qui sono disponibili informazioni generali sulle attività di Kaspersky Anti-Virus for Windows Servers, che consentono di verificare che tutto stia funzionando correttamente e di esaminare le statistiche generali.
Per esaminare il computer e rilevare eventuali file o programmi nocivi, utilizzare la speciale sezione **Scansione** nella finestra principale. 	Questa sezione contiene un elenco di oggetti che è possibile sottoporre alla scansione anti-virus. Le attività più importanti e più comuni sono incluse in questa sezione. Tra queste vi sono le attività di scansione antivirus delle aree critiche, dei programmi di avvio e le scansioni complete del computer.

La sezione **Servizio** include funzioni supplementari di Kaspersky Anti-Virus for Windows Servers. 	cui è possibile aggiornare l'applicazione, visualizzare rapporti sulle attività ed i componenti in esecuzione e terminati, lavorare con gli oggetti in quarantena e le copie di backup e col manager delle chiavi di licenza, nonché ottenere informazioni sull'assistenza tecnica.
La sezione **Commenti e suggerimenti** accompagna l'utente durante l'uso del programma. 	In questa sezione, è sempre possibile leggere i suggerimenti su come aumentare il livello di protezione del server. Vi si trovano inoltre commenti sulle prestazioni correnti dell'applicazione e sulle sue impostazioni.

Ogni elemento del pannello di navigazione è accompagnato da uno speciale menu di scelta rapida. Il menu contiene voci su File Anti-Virus e strumenti che aiutano l'utente a configurarli e a gestirli velocemente, nonché a visualizzare i rapporti. È inoltre disponibile un'ulteriore voce di menù per le scansioni antivirus e le attività di aggiornamento che consente di creare un'attività personalizzata modificando la copia di un'attività esistente.

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

4.4. Finestra delle impostazioni del programma

La finestra delle impostazioni di Kaspersky Anti-Virus for Windows Servers (vedere 4.3 a pag. 39) può essere aperta dalla finestra principale. A tal fine, fare clic su Impostazioni nella parte superiore della stessa.

Il layout della finestra delle impostazioni (vedere Figura 3) è analogo a quello della finestra principale:

- la parte sinistra della finestra consente di accedere rapidamente e facilmente alle impostazioni delle attività di scansione antivirus ed aggiornamento di File Anti-Virus, nonché agli strumenti del programma;
- la parte destra della finestra contiene un elenco dettagliato di impostazioni dell'elemento selezionato nella parte sinistra della finestra.

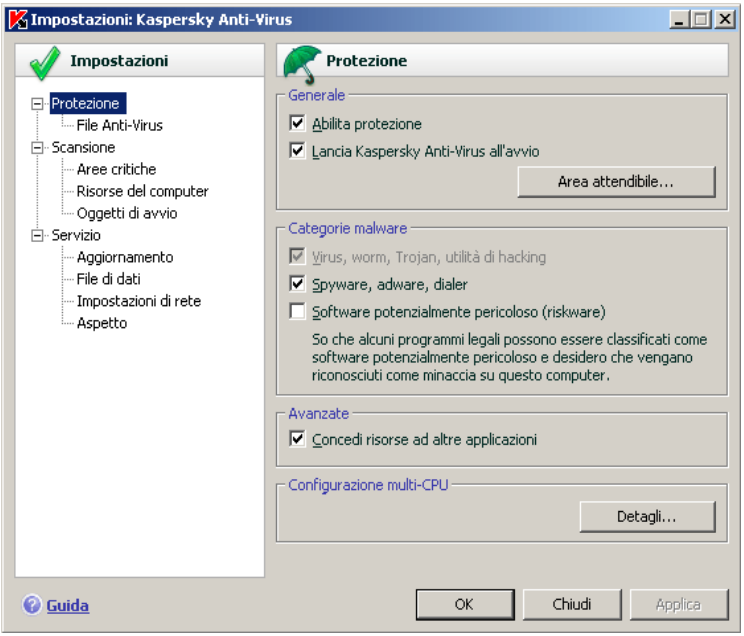


Figura 3. Finestra delle impostazioni di Kaspersky Anti-Virus for Windows Servers

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, vedere le sezioni corrispondenti della Guida.

CAPITOLO 5. GUIDA INTRODUTTIVA

Uno dei principali obiettivi di Kaspersky Lab nell'elaborazione di Kaspersky Anti-Virus for Windows Servers era quello di fornire la configurazione ottimale per ciascuna opzione del programma.

Per facilitare al massimo la messa in funzione del programma, abbiamo combinato tutte le fasi di configurazione preliminare in una procedura di configurazione guidata (vedere 3.2 a pag. 27) che si avvia al termine dell'installazione del programma. Seguendo le istruzioni della procedura guidata, è possibile attivare il programma, configurare le impostazioni per gli aggiornamenti e le scansioni anti-virus, impostare l'accesso protetto da password al programma.

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

- Controllare lo stato corrente della protezione (vedere 5.1 a pag. 43) per garantire che Kaspersky Anti-Virus for Windows Servers funzioni al livello appropriato.
- Aggiornare il programma (vedere 5.5 a pag. 51) se la procedura guidata non ha provveduto automaticamente dopo l'installazione del programma.
- Eseguire la scansione antivirus del computer (vedere 5.2 a pag. 49).

5.1. Qual'è lo stato di protezione del computer?

La finestra principale del programma fornisce informazioni sulla protezione del computer alla sezione **Protezione**. Questa sezione illustra lo *stato di protezione corrente* del computer e le *statistiche sulle prestazioni generali* del programma.

Status protezione visualizza lo stato corrente della protezione del computer per mezzo di speciali indicatori (vedere 5.1.1 a pag. 44). Le statistiche (vedere 5.1.2 a pag. 47) analizzano la sessione corrente del programma.

5.1.1. Indicatori della protezione

Lo **Stato della protezione del computer** è determinato da tre indicatori (vedere Figura 4), ciascuno dei quali riflette un differente aspetto della protezione del computer in qualsiasi momento dato, ed indica qualsiasi problema relativo alle impostazioni ed alle prestazioni del programma.

Ciascun indicatore ha tre possibili aspetti:

– *la situazione è normale*; l'indicatore indica che la protezione del computer è adeguata, e che non ci sono problemi nelle impostazioni o nelle prestazioni del programma.

Figura 4. Gli indicatori che riflettono lo stato di protezione del computer

– *ci sono una o più differenze* nelle prestazioni di Kaspersky Anti-Virus for Windows Servers rispetto al livello raccomandato, che potrebbero avere effetto sulla sicurezza delle informazioni. Si consiglia di prestare attenzione alle azioni raccomandate da Kaspersky Lab, che vengono offerte come collegamenti.

– *lo stato di sicurezza del computer e critico*. Attenersi rigidamente alle raccomandazioni per migliorare la protezione del computer in uso. Le azioni raccomandate sono indicate come collegamenti.

Esaminiamo adesso gli indicatori della protezione e le situazioni che ciascuno di essi riflette.

Il primo indicatore riflette la presenza di file e programmi nocivi sul computer. I tre valori di questo indicatore significano quanto segue:

	Non è stata rilevata alcuna minaccia Kaspersky Anti-Virus for Windows Servers non ha rilevato alcun file o programma pericoloso sul computer.

	Tutte le minacce sono state isolate Kaspersky Anti-Virus for Windows Servers ha trattato tutti i file e i programmi infetti da virus ed ha eliminato quelli che non era possibile trattare.
	*Le minacce sono state rilevate* Il computer è a rischio di infezione. Kaspersky Anti-Virus for Windows Servers ha rilevato programmi nocivi (virus, trojan, worm, ecc.) che devono essere neutralizzati. A tal fine, usare il collegamento Isola tutto. Fare clic su Dettagli per ulteriori dettagli sugli oggetti nocivi.

Il secondo indicatore visualizza l'efficacia della protezione del computer in uso. L'indicatore può assumere uno dei seguenti valori:

	*Firme rilasciate:: (data, ora)* Sia l'applicazione che l'elenco delle minacce utilizzati da Kaspersky Anti-Virus for Windows Servers sono le versioni più recenti.
	*Le firme non sono aggiornate* I moduli del programma e il database di Kaspersky Anti-Virus for Windows Servers non sono stati aggiornati da diversi giorni. L'utente corre il rischio di infettare il computer con nuovi programmi nocivi apparsi dopo l'ultimo aggiornamento del programma. Si consiglia di aggiornare Kaspersky Anti-Virus for Windows Servers A tal fine, usare il collegamento Aggiorna.
	Gli elenchi dei virus sono parzialmente corrotti Gli elenchi delle minacce sono parzialmente corrotti. In tal caso, è consigliabile eseguire nuovamente l'aggiornamento del programma. Se si ripresenta lo stesso messaggio d'errore, rivolgersi al servizio di assistenza tecnica Kaspersky Lab.
	Riavviare il computer Per garantire il corretto funzionamento del programma è necessario riavviare il sistema. Salvare e chiudere tutti i file su cui si sta lavorando e fare clic sul collegamento Riavviare il computer.

	Gli aggiornamenti al programma sono disabilitati Il servizio di aggiornamento all'elenco delle minacce ed ai moduli del programma è disabilitato. Per mantenere la protezione in tempo reale, si consiglia di abilitare gli aggiornamenti.
	*L'elenco dei virus è obsoleto* Kaspersky Anti-Virus for Windows Servers non è stato aggiornato per diverso tempo. I dati sul computer sono in grande pericolo. Aggiornare il programma al più presto. A tal fine, usare il collegamento Aggiorna ora.
	Gli elenchi dei virus sono corrotti Gli elenchi delle minacce sono completamente danneggiati. In tal caso, è consigliabile eseguire nuovamente l'aggiornamento del programma. Se si ripresenta lo stesso messaggio d'errore, rivolgersi al servizio di assistenza tecnica Kaspersky Lab.

Il terzo indicatore illustra la funzionalità corrente del programma. L'indicatore può assumere uno dei seguenti valori:

	*Tutti i componenti della protezione sono in esecuzione* Kaspersky Anti-Virus for Windows Servers sta proteggendo il computer su tutti i canali attraverso i quali potrebbero infiltrarsi i programmi nocivi.
	Protezione non installata Al momento dell'installazione di Kaspersky Anti-Virus for Windows Servers non è stato installato nessuno dei componenti di monitoraggio. Questo significa che è possibile solo eseguire la scansione antivirus. Per la massima sicurezza è necessario installare i componenti di protezione sul computer.
	*Tutti i componenti della protezione sono sospesi* Il componente di protezione è stato sospeso. Per ripristinare il componente, selezionare **Riprendi protezione** dal menu di scelta rapida facendo clic sull'icona dell'area di notifica.
	Tutti i componenti della protezione sono disabilitati La protezione è completamente disabilitata. Il componente di protezione non è in funzione. Per ripristinare il componente, selezionare **Riprendi istina protezione** dal menu di scelta rapida facendo clic sull'icona dell'area di notifica.

	Si è verificato un errore in alcuni componenti di protezione Si è verificato un errore interno nel componente di Kaspersky Anti-Virus. Si raccomanda in questo caso di abilitare il componente o di riavviare il computer (è possibile che i driver del componente debbano essere registrati dopo l'aggiornamento).

5.1.2. Stato dei componenti di Kaspersky Anti-Virus for Windows Servers

Per determinare come Kaspersky Anti-Virus for Windows Servers sta proteggendo il file system del computer in uso, oppure per visualizzare l'avanzamento di un'attività di scansione antivirus o di aggiornamento dell'elenco dei virus, basta aprire la sezione corrispondente della finestra principale del programma.

Ad esempio, per visualizzare lo stato corrente di File Anti-Virus, selezionare **File Anti-Virus** dal riquadro sinistro della finestra principale. Il riquadro destro visualizzerà un riassunto delle informazioni relative al funzionamento del componente.

Per File Anti-Virus, il pannello destro contiene la **barra di stato**, il riquadro di **Stato** ed il riquadro delle **Statistiche**.

Per File Anti-Virus, la *barra di stato* appare come segue:

- *File Anti-Virus: in corso* – la protezione dei file è attiva al livello selezionato (vedere 7.1 a pag. 72).
- *File Anti-Virus: in sospeso* File Anti-Virus è disabilitato per un determinato intervallo di tempo. Il componente riprenderà a funzionare automaticamente alla scadenza del periodo stabilito o dopo aver riavviato il programma. La protezione dei file può anche essere ripristinata manualmente facendo clic sul pulsante ▶ ubicato sulla barra di stato.
- *File Anti-Virus: Disattivato* – il componente è stato arrestato dall'utente. La protezione dei file può essere ripristinata manualmente facendo clic sul pulsante ▶ ubicato sulla barra di stato.
- *File Anti-Virus: non in funzione* – la protezione dei file non è disponibile per qualche ragione.
- *File Anti-Virus: disabilitato (errore)* – il componente ha provocato un errore.

Se un componente incontra un errore, provare a riavviarlo. Se il riavvio genera un errore, esaminare il rapporto sul componente che potrebbe contenere la ragione del problema. Se risulta impossibile risolvere il problema autonomamente, salvare il rapporto sul componente in un file utilizzando il pulsante **Azione → Salva con nome** e contattare il supporto tecnico di Kaspersky Lab.

Le impostazioni di funzionamento di un componente sono fornite nella sezione **Stato**:

- *File Anti-Virus* - stato corrente del componente (attivo, non attivo, sospeso, ecc.).
- *Livello di sicurezza* – l'Insieme totale di parametri per il funzionamento del componente, secondo il quale il programma protegge i file. Per impostazione predefinita, viene selezionato il livello di sicurezza **Consigliato** che esamina solo gli oggetti del file system soggetti a un'infezione. Per esempio, i file eseguibili (.exe).
- L'*azione* intrapresa al rilevamento di un oggetto nocivo.

La casella **Stato** non è disponibile per le attività di scansione antivirus e di aggiornamento. Il livello di sicurezza, l'azione applicata ai programmi pericolosi per le attività di scansione antivirus, e la modalità operativa per gli aggiornamenti sono elencati nel riquadro **Impostazioni**.

Il riquadro **Statistiche** contiene informazioni sul funzionamento dei componenti di protezione, gli aggiornamenti o le attività di scansione antivirus.

5.1.3. Statistiche sulle prestazioni del programma

Le **Statistiche di programma** si trovano nel riquadro **Statistiche** della sezione **Protezione** della finestra principale (vedere Figura 5), e visualizzano informazioni generali sulla protezione del computer, registrate a partire da quando Kaspersky Anti-Virus for Windows Servers è stato installato.

Figura 5. Il riquadro statistiche generali del programma

Fare clic su un punto qualsiasi del riquadro per visualizzare un rapporto con informazioni dettagliate. Le schede visualizzano:

- Informazioni sugli oggetti analizzati (vedere 11.3.2 a pag. 130) e sullo stato assegnato a ciascuno
- Registro degli eventi (vedere 11.3.3 a pag. 131)
- Statistiche generali sulla scansione (vedere 11.3.4 a pag. 132) per il computer in uso
- Statistiche sulle prestazioni del programma (vedere 11.3.5 a pag. 132)

5.2. Come eseguire la scansione antivirus del server

Dopo l'installazione, il programma comunica all'utente con un messaggio speciale nella parte inferiore a sinistra della finestra principale del programma che il server non è ancora stato esaminato e ne raccomanda una scansione antivirus immediata.

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

Dopo aver selezionato l'attività **Risorse del computer**, sarà possibile visualizzare le statistiche relative alla scansione più recente del computer, nonché le impostazioni dell'attività: che livello di protezione sia stato selezionato e quali azioni saranno intraprese per gli oggetti pericolosi.

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

1. Aprire la finestra principale dell'applicazione e selezionare l'attività **Risorse del computer** nella sezione **Scansione**.
2. Fare clic sul pulsante **Scansione**.

Il programma avvia la scansione del server visualizzando i dettagli in una finestra apposita. Facendo clic sul pulsante **Chiudi**, verrà nascosta la finestra contenente informazioni sul progresso dell'installazione; ciò non arresterà la scansione.

5.3. Come eseguire la scansione di aree critiche del computer

È estremamente importante proteggere queste aree per il corretto funzionamento del computer. È prevista una attività di scansione antivirus speciale per queste aree, che si trova nella finestra principale del programma nella sezione **Scansione**.

Dopo aver selezionato l'attività **Aree critiche**, è possibile visualizzare le statistiche relative alla scansione più recente, nonché le impostazioni dell'attività: le statistiche relative alla scansione più recente di queste aree; il livello di sicurezza selezionato, e quali azioni vengono applicate alle minacce alla sicurezza. Qui è anche possibile selezionare quali aree critiche si desidera esaminare, ed esaminarle immediatamente.

Per eseguire la scansione delle aree critiche del computer alla ricerca di programmi nocivi,

1. Aprire la finestra principale dell'applicazione e selezionare l'attività **Aree critiche** nella sezione **Scansione**.
2. Fare clic sul pulsante **Scansione**.

Il programma avvia la scansione delle aree selezionate visualizzando i dettagli in una finestra apposita. Facendo clic sul pulsante **Chiudi**, verrà nascosta la finestra contenente informazioni sul progresso dell'installazione; ciò non arresterà la scansione.

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

A volte è necessario eseguire la scansione antivirus di singoli oggetti anziché dell'intero computer: ad esempio, una delle unità disco. È possibile inoltre selezionare un oggetto da esaminare con gli strumenti standard del sistema operativo Microsoft Windows Server (per esempio dalla finestra di **Esplora risorse** o dal **Desktop**, ecc.).

Per esaminare un oggetto,

posizionare il cursore sul nome dell'oggetto selezionato, aprire il menu di scelta rapida di Microsoft Windows Server facendo clic con il pulsante destro del mouse e selezionare **Ricerca virus** (vedere Figura 6).

Il programma avvia quindi la scansione dell'oggetto selezionato visualizzando i dettagli in una finestra apposita. Facendo clic sul pulsante Chiudi, verrà nascosta la finestra contenente informazioni sul progresso dell'installazione; ciò non arresterà la scansione.

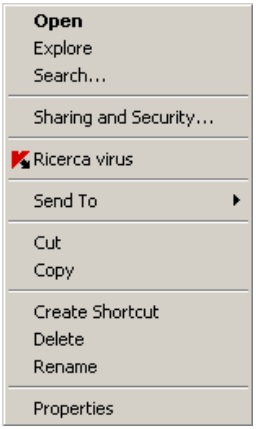


Figura 6. Scansione di un oggetto selezionato utilizzando il menù contestuale standard di Microsoft Windows Server

5.5. Come aggiornare il programma

Kaspersky Lab aggiorna gli elenchi delle minacce di Kaspersky Anti-Virus for Windows Servers e i moduli 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!

Sarà necessaria una connessione a Internet per aggiornare Kaspersky Anti-Virus for Windows Servers.

Per impostazione predefinita, Kaspersky Anti-Virus for Windows Servers controlla automaticamente la presenza di aggiornamenti sui server di Kaspersky Lab. Se questo server dispone degli ultimi aggiornamenti, Kaspersky Anti-Virus li scaricherà e li installerà in modalità invisibile.

Per aggiornare manualmente Kaspersky Anti-Virus for Windows Servers,

selezionare il componente **Aggiornamento** nella sezione **Servizio** della finestra principale del programma e fare clic sul pulsante **Aggiorna ora!** nella parte destra della finestra.

Di conseguenza, Kaspersky Anti-Virus for Windows Servers avvierà il processo di aggiornamento, visualizzando i dettagli del processo in una finestra speciale.

5.6. Come comportarsi in caso di protezione non funzionante

Se si verificano problemi o errori di funzionamento di File Anti-Virus, è bene verificarne lo stato. Se lo stato è *disattivato* oppure *errore di funzionamento*, provare a riavviare l'applicazione.

Se il problema non viene risolto dopo aver riavviato il programma, si consiglia di correggere eventuali errori utilizzando la funzione di ripristino dell'applicazione **Start → Tutti i programmi→ Kaspersky Anti-Virus 6.0 for Windows Servers → Modifica, ripristina o rimuovi**).

Se la procedura di ripristino dell'applicazione non aiuta, contattare l'assistenza tecnica di Kaspersky Lab. Potrebbe essere necessario salvare un rapporto sul funzionamento del componente o dell'intera applicazione in un file, per poi inviarlo all'assistenza tecnica per ulteriori analisi.

Per salvare il rapporto su un file:

1. Selezionare File Anti-Virus nella sezione **Protezione**della finestra principale del programma e fare clic con il pulsante sinistro del mouse ovunque nel riquadro **Statistiche**.
2. Fare clic sul pulsante **Salva con nome** e specificare nella finestra che si apre il nome del file per il rapporto sulle prestazioni del componente.

Per salvare un rapporto sull'avvio o lo stato di tutti i componenti di Kaspersky Anti-Virus in una volta sola (File Anti-Virus, attività di scansione antivirus, funzioni di supporto):

1. Selezionare la sezione **Protezione** della finestra principale del programma e fare clic ovunque nel riquadro **Statistiche**.

   oppure

   Fare clic su Elenco di tutti i rapporti nella finestra dei rapporti di qualsiasi componente. A questo punto la scheda **Rapporto** elencherà i rapporti di tutti i componenti del programma.
2. Fare clic sul pulsante **Salva con nome** e specificare nella finestra che si apre il nome del file per il rapporto sulle prestazioni del programma.

CAPITOLO 6. SISTEMA DI GESTIONE DELLA PROTEZIONE

Kaspersky Anti-Virus for Windows Servers consente di gestire la sicurezza del computer per le seguenti attività:

- Abilitare, disabilitare e sospendere (vedere 6.1 a pag. 53) il programma
- Definire i tipi di programmi pericolosi (vedere 6.2 a pag. 57) dai quali Kaspersky Anti-Virus for Windows Servers deve proteggere il computer
- Creare un elenco di esclusioni (vedere 6.3 a pag. 58) per la protezione
- Creare attività di scansione antivirus e di aggiornamento personalizzate (vedere 6.4 a pag. 65)
- Pianificare una serie di scansioni antivirus (vedere 6.5 a pag. 66)
- Configurare le impostazioni di produttività (vedere 6.6 a pag. 68) per la protezione del computer

6.1. Interruzione e ripristino della protezione 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. Le parole *Kaspersky Anti-Virus 6.0* nell'angolo superiore destro dello schermo indicano tutto ciò. File Anti-Virus (vedere 2.2.1 a pag. 17) è in funzione.

È possibile disabilitare la protezione offerta da Kaspersky Anti-Virus for Windows Servers.

Attenzione!

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

Si noti che in questo caso la protezione è descritta nel contesto di File Anti-Virus. Disabilitarlo o sospenderlo non pregiudica le prestazioni delle attività di scansione antivirus o aggiornamento del programma.

6.1.1. Sospensione della protezione

Sospendere la protezione significa disabilitare temporaneamente File Anti-Virus.

Per sospendere un'operazione di Kaspersky Anti-Virus for Windows Servers:

1. Selezionare **Sospendi protezione** nel menu di scelta rapida del programma (vedere 4.2 a pag. 38).
2. Nella finestra **Interrompi protezione** che si apre (vedere Figura 7), specificare quando si desidera ripristinare la protezione:
   - **In <intervallo di tempo>** – la protezione verrà abilitata dopo questo intervallo di tempo. Per selezionare un valore di tempo, utilizzare il menù a discesa.
   - **Al prossimo riavvio del programma** – la protezione sarà abilitata se si apre il programma dal menu Start o dopo aver riavviato il computer (se il programma è impostato per l'avvio automatico all'accensione del computer (vedere 6.1.5 a pag. 57).
   - **Solo su richiesta dell'utente** – la protezione verrà abilitata solo se avviata manualmente. Per abilitare la protezione, selezionare **Abilita protezione** dal menù contestuale del programma.

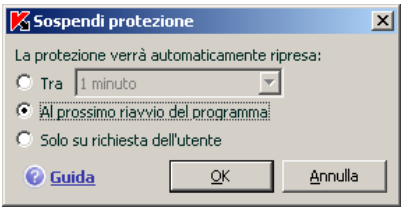


Figura 7. Finestra di sospensione della protezione

Suggerimento:

La protezione del computer può essere disabilitata anche tramite uno dei seguenti metodi:

- Fare clic sul pulsante ❚❚ nella sezione Protezione.
- Selezionare Esci dal menu di scelta rapida. A questo punto il programma verrà scaricato dalla memoria del computer.

Se si sospende la protezione, File Anti-Virus sarà in pausa. Questo stato è indicato da quanto segue:

- Il nome di File Anti-Virus nella sezione **Protezione** della finestra principale è inattivo (in grigio).
- L'icona nell'area di notifica è inattiva (grigia).
- Il terzo indicatore di protezione (vedere 5.1.1 a pag. 44) del computer segnala che **Tutti i componenti della protezione sono sospesi**.

6.1.2. Arrestare la protezione del server

Arrestare la protezione significa disabilitare completamente File Anti-Virus. 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'amministratore: File Anti-Virus non si riattiverà automaticamente dopo il riavvio del sistema o del programma. Si tenga presente che se Kaspersky Anti-Virus for Windows Servers è in conflitto con altri programmi installati sul computer, è possibile sospendere File Anti-Virus o creare un'elenco di esclusioni (vedere 6.3 a pag. 58).

Per arrestare completamente la protezione:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus e selezionare la sezione **Protezione**.
2. Deselezionare **Abilita protezione**.

Dopo aver disabilitato la protezione, File Anti-Virus si arresta. Questo stato è indicato da quanto segue:

1. Il nome di File Anti-Virus nella sezione **Protezione** della finestra principale è inattivo (in grigio).
2. L'icona nell'area di notifica è inattiva (grigia).
3. Il terzo indicatore di protezione (vedere 5.1.1 a pag. 44) del computer segnala che **Tutti i componenti della protezione sono disabilitati**.

6.1.3. Sospendere / arrestare la protezione

Ci sono diversi modi per arrestare File Anti-Virus, una scansione antivirus o un aggiornamento. Prima di fare ciò, si consiglia caldamente di stabilire perché è

necessario l'arresto. È probabile infatti che esista una soluzione diversa al problema, per esempio modificare il livello di sicurezza. Se, per esempio, si lavora con un database che sicuramente non contiene virus, è sufficiente aggiungerne i file tra le esclusioni (vedere 6.3 a pag. 58).

Per sospendere File Anti-Virus, le scansioni antivirus e le attività di aggiornamento:

Selezionare il componente o l'attività dalla parte sinistra della finestra principale e fare clic sul pulsante nella barra di stato.

Lo status del componente/attività diventa ***sospeso***. Il componente o l'attività resterà in sospensione fino a quando l'utente li ripristinerà facendo clic sul pulsante .

Quando si sospende il funzionamento di un componente o un'attività al, le statistiche per la sessione corrente di Kaspersky Anti-Virus vengono salvate e continueranno ad essere elaborate dopo l'aggiornamento del componente.

Per arrestare il componente o l'attività di protezione:

Fare clic sul pulsante nella barra di stato. È inoltre possibile arrestare componente nella finestra delle impostazioni del programma, deselezionando la casella di controllo **Abilita <nome componente>** nella sezione **Generale**.

Lo status del componente/attività diventa *interrotto (disabilitato)*. Il componente o l'attività resteranno inattivi fino a quando l'utente li abiliterà facendo clic sul pulsante . Per le scansioni antivirus e le attività di aggiornamento, è possibile scegliere tra le seguenti opzioni: continuare l'attività che è stata interrotta, o riavviarla dall'inizio.

Quando si arresta un componente o un'attività, tutte le statistiche relative al lavoro precedente vengono cancellate e una volta riavviato il componente, vengono sovrascritte.

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 di scelta rapida*.

  A tal fine, selezionare **Abilita protezione**.

- *Dalla finestra principale del programma*.

A tal fine, fare clic sul pulsante sulla barra di stato nella sezione **Protezione** della finestra principale.

Lo stato della protezione si modifica immediatamente in *in corso*. L'icona dell'area di notifica diventa attiva (colorata). Anche il terzo indicatore della protezione (vedere 5.1.1 a pag. 44) informa l'utente che **Tutti i componenti della protezione sono in esecuzione**.

6.1.5. Chiusura del programma

Per chiudere Kaspersky Anti-Virus for Windows Servers, selezionare **Esci** dal menu di scelta rapida del programma (vedere 4.2 a pag. 38). Il programma si chiude lasciando il computer privo di protezione.

Se il programma è stato chiuso, la protezione del computer può essere nuovamente abilitata aprendo Kaspersky Anti-Virus for Windows Servers (**Start→ Tutti i programmi→ Kaspersky Anti-Virus 6.0 for Windows Servers → Kaspersky Anti-Virus 6.0 for Windows Servers**).

È possibile inoltre ripristinare automaticamente la protezione dopo il riavvio del sistema operativo. Per abilitare questa funzione, selezionare la sezione **Protezione** nella finestra delle impostazioni del programma e selezionare **Lancia Kaspersky Anti-Virus all'avvio**.

6.2. Tipi di programmi nocivi da monitorare

Kaspersky Anti-Virus for Windows Servers protegge da vari tipi di programmi nocivi. Indipendentemente dalle impostazioni, il programma protegge sempre il computer dai tipi di programmi nocivi più pericolosi come virus, Trojan e strumenti di hacking. Questi programmi sono in grado di danneggiare gravemente il computer. Per migliorare la sicurezza del computer, è possibile accrescere l'elenco delle minacce che il programma sarà in grado di intercettare abilitando il monitoraggio di ulteriori tipi di programmi pericolosi.

Per specificare da quali programmi nocivi Kaspersky Anti-Virus for Windows Servers proteggerà il computer, selezionare la sezione **Protezione** nella finestra delle impostazioni del programma (vedere 4.4 a pag. 41).

Il riquadro **Categorie malware** contiene i tipi di minaccia (vedere 1.1 a pag. 9):

Virus, worm, trojan, utilità di hacking. Questo gruppo combina le categorie più comuni e pericolose di programmi nocivi. Questo è il livello di sicurezza minimo ammissibile. Come da raccomandazioni degli esperti di Kaspersky

Lab, Kaspersky Anti-Virus controlla sempre questa categoria di programmi nocivi.

- **Spyware, adware, dialer.** Questo gruppo include il software potenzialmente pericoloso che potrebbe dare problemi all'utente o causare danni gravi.
- **Software potenzialmente pericoloso (riskware)**. Questo gruppo include programmi che non sono nocivi o pericolosi. Tuttavia, in determinate circostanze possono essere utilizzati per causare danni al computer in uso.

I gruppi elencati sopra comprendono l'intera gamma di minacce che il programma rileva durante la scansione degli oggetti.

Se tutti i gruppi sono selezionati, Kaspersky Anti-Virus for Windows Servers garantisce la massima protezione antivirus del computer. Se il secondo e il terzo gruppo sono disabilitati, il programma protegge solo dai programmi nocivi più comuni. Fra questi non sono compresi i programmi potenzialmente pericolosi che potrebbero essere installati sul computer e danneggiare i file, provocare perdite finanziarie e rubare tempo.

Kaspersky Lab sconsiglia di disabilitare il monitoraggio del secondo gruppo. Se si verifica una situazione in cui Kaspersky Anti-Virus classifica un programma che non viene considerato pericoloso come potenzialmente pericoloso, si consiglia di creare una esclusione apposita per esso (vedere 6.3 a pag. 58).

6.3. Creazione di una zona attendibile

Una *zona attendibile* è un elenco di oggetti creato dall'amministratore che non sono monitorati da Kaspersky Anti-Virus for Windows Servers. In altre parole, si tratta di una serie di programmi esclusi dalla protezione.

L'amministratore 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 for Windows Servers blocca l'accesso a un oggetto o programma della cui sicurezza l'utente è assolutamente certo.

È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file o escludere una certa area (per esempio una cartella o un programma), processi di programma o oggetti in base alla classificazione nella Virus Encyclopedia (lo stato che il programma assegna agli oggetti durante una scansione).

Attenzione!

Gli oggetti esclusi non vengono esaminati durante le scansioni dei dischi o delle cartelle in cui si trovano. Tuttavia, se l'oggetto viene specificatamente selezionato, la regola di esclusione non verrà applicata.

Per creare un elenco di esclusioni,

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare la sezione **Protezione**.
2. Fare clic sul pulsante **Area attendibile** nella sezione **Generale**.

Configurare le regole di esclusione per gli oggetti e creare una lista delle applicazioni attendibili nella finestra che si apre (vedere Figura 8).

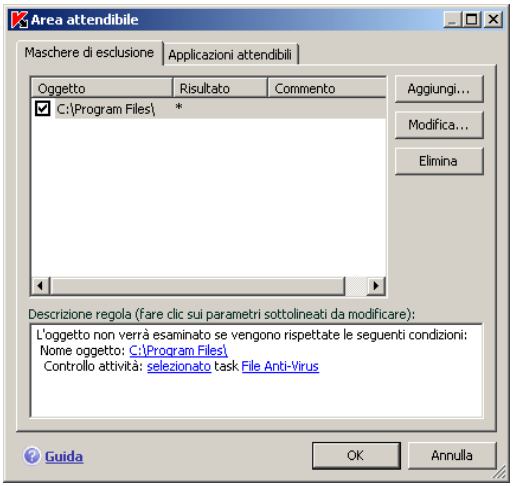


Figura 8. Creazione di una zona attendibile

6.3.1. Regole di esclusione

Le *Regole di esclusione* sono delle condizioni in base alle quali Kaspersky Anti-Virus for Windows Servers stabilisce quali oggetti non sottoporre a scansione.

È possibile escludere i file dalla scansione in base al formato, usare una maschera, escludere una determinata area, ad esempio una cartella o un programma, i processi di programmi o gli oggetti in base alla classificazione nella Virus Encyclopedia.

Il *risultato* è lo stato che Kaspersky Anti-Virus assegna a un oggetto durante la scansione. Lo stato viene assegnato in base alla categorizzazione dei

programmi nocivi e potenzialmente pericolosi che si trovano 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, i client IRC, i server FTP, le utilità multifunzione per interrompere o nascondere i processi, i keylogger, le macro per la decodifica di password, gli autodialer, ecc. Questi programmi non sono classificati come virus. Essi possono essere suddivisi in diverse categorie, per esempio adware, joke , riskware, ecc. (per ulteriori informazioni sui programmi potenzialmente pericolosi individuati da Kaspersky Anti-Virus for Windows Servers, vedere la Virus Encyclopedia all'indirizzo www.viruslist.com). Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di loro sono molto comuni, è possibile escluderli dalla scansione. A tal fine, aggiungere il nome o la maschera di minaccia dell'oggetto alla zona affidabile, utilizzando la classificazione nella Virus Encyclopedia.

È possibile, per esempio, immaginare che per ragioni di lavoro si usi spesso un programma di amministrazione remota. Si tratta di un sistema ad accesso remoto che consente di lavorare da un computer remoto. Kaspersky Anti-Virus for Windows Servers visualizza questo tipo di applicazione come potenzialmente pericolosa e la blocca. Per prevenire il blocco dell'applicazione, occorre creare una regola di esclusione che specifica "not-a-virus:RemoteAdmin.Win32.RAdmin.22" come verdetto.

Quando si aggiunge un'esclusione, viene creata una regola che in seguito sarà utilizzata da File Anti-Virus e dalle 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 rapporti.

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

1. Fare clic sul pulsante **Aggiungi** nella scheda **Maschere di esclusione**.
2. Nella finestra che si apre (vedere Figura 9), fare clic sul tipo di esclusione nella sezione **Proprietà**:

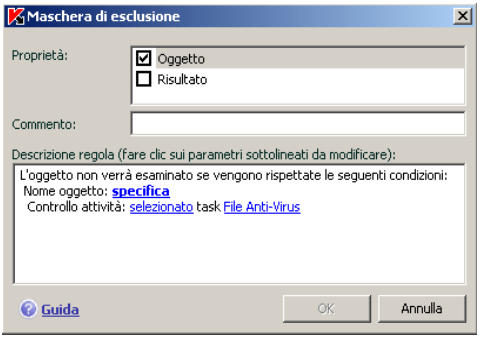


Figura 9. Creazione di una regola di esclusione

☑ **Oggetto** – esclusione dalle scansioni di un determinato oggetto, directory o file che corrisponde a una certa maschera.

☑ **Risultato** – esclusione degli oggetti dalla scansione in base allo stato ad essi assegnato dalla Virus Encyclopedia.

Se si selezionano contemporaneamente entrambe le caselle, verrà creata per quell'oggetto una regola con un certo tipo di stato, in base alla classificazione nella Virus Encyclopedia. In tal caso vale la seguente regola:

- Se si specifica un certo file come **Oggetto** e un certo stato nella sezione **Risultato**, il file specificato rappresenterà un'esclusione solo se durante la scansione viene classificato come la minaccia selezionata.
- Se si seleziona un'area o una cartella come **Oggetto** e lo stato (o maschera) come **Risultato**, gli oggetti contrassegnati da quello stato saranno esclusi solo dalla scansione in quell'area o cartella.

3. Assegnare valori **ai** tipi di esclusione selezionati. A tal fine, fare clic nella sezione **Descrizione regola** sul collegamento specifica situato accanto al tipo di esclusione:
   - Per il tipo di **Oggetto**, immettere il relativo nome nella finestra che si apre (può essere un file, una cartella particolare o una maschera di file (vedere A.2 a pag. 192). Selezionare ☑ **Includi sottocartelle** per l'oggetto (file, maschera file, cartella) affinché sia ripetutamente escluso dalla scansione.
   - Immettere il nome intero della minaccia che si intende escludere dalle scansioni come indicato nella Virus Encyclopedia o usare una maschera per il **Risultato** (vedere A.3 a pag. 192.

Per alcuni risultati, è possibile assegnare condizioni avanzate per l'applicazione delle regole nel campo **Impostazioni avanzate**.

4. È possibile definire quali componenti di Kaspersky Anti-Virus for Windows Servers utilizzeranno questa regola. Se l'opzione selezionata è tutti, questa regola verrà applicata a tutti i componenti. Per limitare la regola a uno o più componenti, fare clic su tutti, che si modificherà in selezionati. Nella finestra che si apre, selezionare le caselle relative ai componenti ai quali si desidera applicare questa regola di esclusione.

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

1. Utilizzare il collegamento Aggiungi a zona attendibile nella finestra dell'avviso.
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 una regola, fare clic su **OK**.

Per creare una regola di esclusione dalla finestra dei rapporti:

1. Selezionare nel rapporto l'oggetto che si desidera aggiungere alle esclusioni.
2. Aprire il menu di scelta rapida e selezionare **Aggiungi a zona attendibile** (vedere Figura 10).

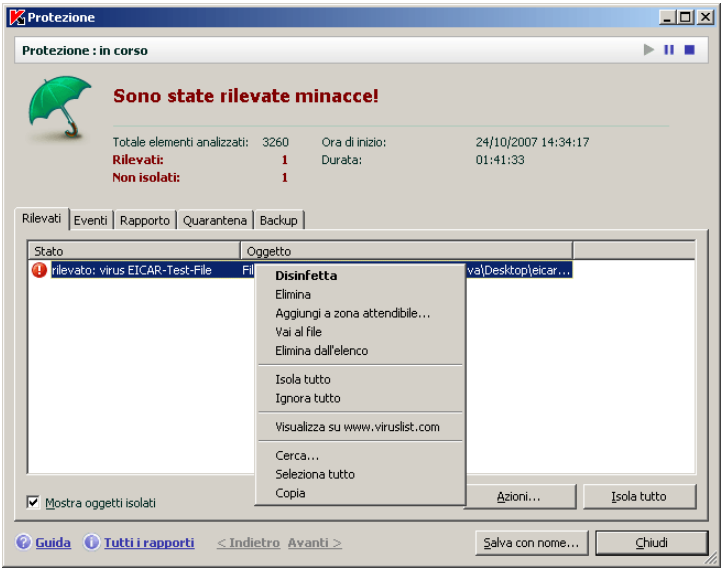


Figura 10. Creazione di una regola di esclusione da un rapporto

6.3.2. Applicazioni attendibili

Kaspersky Anti-Virus for Windows Servers è in grado di creare un elenco di applicazioni attendibili di cui non è necessario monitorare le attività dei file, siano esse sospette oppure no.

Per esempio, si può ritenere che gli oggetti e i processi utilizzati dal **Blocco note** di Windows Server siano sicuri e non necessitino di scansione. Per escludere gli oggetti utilizzati da questo processo dalla scansione, aggiungere **Notepad** alla lista 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 (vedere 6.3.1 a pag. 59).

Inoltre, è possibile che alcune azioni classificate come pericolose siano in realtà funzioni perfettamente normali di determinati programmi. Per esempio, i programmi di commutazione del layout di tastiera intercettano regolarmente il testo digitato sulla tastiera. Per smettere di monitorare l'attività di tali programmi, si consiglia di aggiungerli all'elenco delle applicazione attendibili.

Escludendo le applicazioni attendibili è possibile inoltre risolvere potenziali conflitti di compatibilità tra Kaspersky Anti-Virus for Windows Servers ed 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.

Per impostazione predefinita, Kaspersky Anti-Virus for Windows Servers esamina gli oggetti aperti, avviati o salvati da qualsiasi processo software.

È possibile creare un'elenco delle applicazioni attendibili sull'apposita scheda **Applicazioni attendibili** (vedere Figura 11). Per impostazione predefinita, tale elenco contiene le applicazioni che non saranno monitorate sulla base delle raccomandazioni di Kaspersky Lab quando s'installa Kaspersky Anti-Virus. Se non si ritiene affidabile una applicazione dell'elenco, deselezionare la relativa casella di controllo. Per modificare l'elenco, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina** sulla destra.

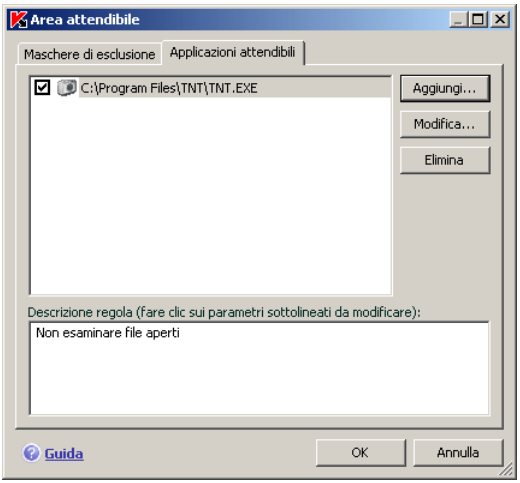


Figura 11. Elenco delle applicazioni attendibili

Per aggiungere un programma all'elenco delle applicazioni attendibili:

1. Fare clic sul pulsante **Aggiungi** sulla parte destra della scheda **Applicazioni attendibili**.
2. Nella finestra Applicazioni attendibili Figura 12 che si apre, selezionare l'applicazione utilizzando il pulsante **Sfoglia**. Si apre un menu di scelta rapida dal quale, facendo clic su **Sfoglia**, si va alla finestra di selezione file, dove è possibile selezionare il percorso al file eseguibile, oppure, facendo clic su **Applicazioni** si va a un elenco di applicazioni attualmente in funzione, che possono essere eventualmente selezionate.

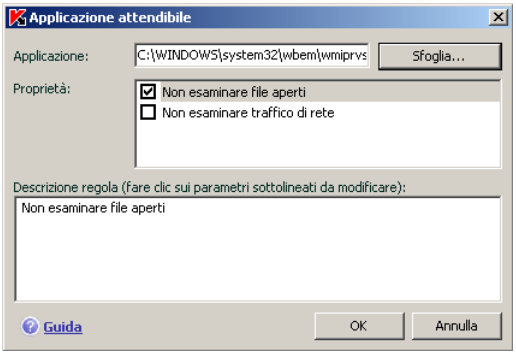


Figura 12. Aggiunta di un'applicazione all'elenco delle applicazioni attendibili

Quando si seleziona un programma, Kaspersky Anti-Virus for Windows Servers registra 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.

3. È possibile quindi se necessario, specificare quali azioni eseguite da questo processo non verranno monitorate da Kaspersky Anti-Virus:

   Non esaminare file aperti – esclude dalla scansione tutti i file aperti dal processo dell'applicazione attendibile.

6.4. Avvio di attività con un altro profilo

Kaspersky Anti-Virus for Windows Servers 6.0 presenta una funzione che consente di avviare le operazioni di scansione sotto un altro profilo utente. Questa funzione è normalmente disabilitata e le attività vengono eseguite con il profilo con cui l'utente si è collegato al sistema.

Questa funzione è utile se, per esempio, sono necessari diritti di accesso a un certo oggetto durante una scansione. Utilizzando questa funzione, è possibile configurare le attività da eseguire con il profilo di un utente in possesso dei privilegi richiesti.

È possibile che gli aggiornamenti del programma debbano essere eseguiti da un'origine alla quale non si ha 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 con un profilo diverso in possesso dei diritti necessari.

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

1. Selezionare il nome dell'attività nelle sezioni **Scansione** (per le attività di scansione antivirus) o **Servizio** (per attività di aggiornamento) della finestra principale ed utilizzare il collegamento Impostazioni per aprire la finestra delle impostazioni delle attività.
2. Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni dell'attività e andare alla scheda **Avanzate** nella finestra che si apre (vedere Figura 13).
3. Per abilitare questa funzione, selezionare ☑ **Esegui questa attività come**. Inserire i dati di login del profilo con cui si desidera avviare l'attività: nome utente e password.

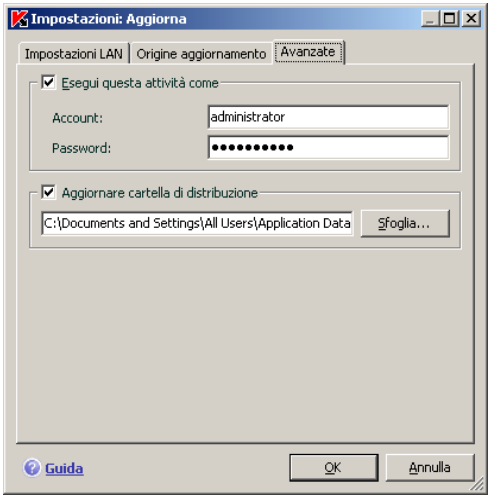


Figura 13. Configurazione di un'attività di aggiornamento da un altro profilo

6.5. Configurazione delle attività pianificate e delle notifiche

Le impostazioni di pianificazione sono identiche per le attività di scansione antivirus, per l'aggiornamento dell'applicazione, e per la notifica degli eventi di Kaspersky Anti-Virus.

Per impostazione predefinita, le attività di scansione antivirus create all'installazione dell'applicazione sono disabilitate. Fanno eccezione gli oggetti di avvio, che vengono esaminati ogni volta che viene avviato Kaspersky Anti-Virus. Per impostazione predefinita, gli aggiornamenti sono configurati per avvenire automaticamente, non appena tali aggiornamenti sono disponibili sui server di aggiornamento di Kaspersky Lab.

Nel caso non si fosse soddisfatti di tali impostazioni, la pianificazione può essere riconfigurata. Selezionare il nome di un'attività in **Scansione antivirus** (per le attività di scansione antivirus), oppure in **Servizio** (per gli aggiornamenti e la distribuzione degli stessi) ed aprire la relativa finestra delle impostazioni facendo clic su Impostazioni.

Per fare avviare le attività in base a una pianificazione, selezionare la casella dell'avvio automatico delle attività nella sezione **Modalità esecuzione**. L'orario di avvio dell'attività di scansione può essere modificato nella finestra **Pianificazione** (vedere Figura 14), che si apre facendo clic su **Cambia**.

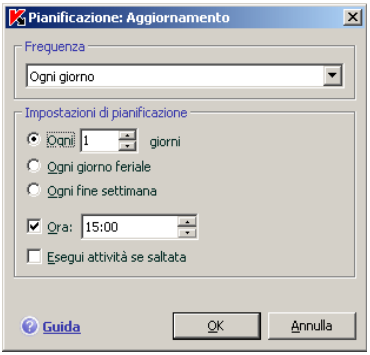


Figura 14. Pianificazione delle attività

L'impostazione primaria da definire è la frequenza di un evento (esecuzione o notifica di un'attività). Selezionare l'opzione desiderata in **Frequenza** (vedere Figura 14). Quindi, le impostazioni per l'opzione selezionata devono essere specificate in Impostazioni di pianificazione. Sono disponibili diverse opzioni:

- **A un'ora specificata.** Avvia un'attività o invia una notifica alla data ed all'ora specificate.
- **All'avvio del programma.** Avvia un'attività o invia una notifica ogni volta che Kaspersky Anti-Virus viene avviato. È inoltre possibile specificare un ritardo in relazione all'avvio di un'attività da parte dell'applicazione.
- **Dopo ogni aggiornamento.** L'attività viene eseguita dopo ciascun aggiornamento all'elenco delle minacce (quest'opzione si applica solo alle scansioni antivirus).

- **Ogni minuto.** L'intervallo di tempo tra le scansioni è di parecchi minuti. Specificare l'intervallo di tempo in minuti nelle impostazioni di pianificazione. Non deve essere superiore a 59 minuti.
- **Ogni ora.** L'intervallo tra le scansioni o le notifiche è di diverse ore. Se questa opzione viene selezionata, specificare l'intervallo temporale nelle impostazioni di pianificazione: **Ogni N ora/e** e specificare *N*. Per esempio, immettere **Ogni 1 ora/e** se si intende eseguire l'operazione a cadenza oraria.
- **Ogni giorno.** L'attività viene avviata o la notifica viene inviata ad intervalli di diversi giorni. Specificare l'intervallo nelle impostazione di pianificazione:
  - Selezionare **Ogni N giorno(i)** ed immettere un valore per N se si desidera mantenere un intervallo di diversi giorni. Selezionare **Ogni giorno feriale** per eseguire l'attività quotidianamente, dal lunedì al venerdì.
  - Selezionare **Ogni fine settimana** per eseguire l'attività o inviare la notifica solo di sabato e domenica.

  Utilizzare il campo **Ora** per specificare a che ora del giorno verrà eseguita l'attività di scansione.
- **Ogni settimana.** L'attività viene avviata o la notifica inviata in certi giorni della settimana. Se si seleziona questa opzione, apporre i segni di spunta accanto ai giorni della settimana in cui si desidera lanciare l'attività. Inserire l'ora del giorno nel campo **Ora**.
- **Ogni mese.** L'attività viene avviata o la notifica inviata una volta al mese, ad un'ora specificata.

Se è impossibile lanciare un'attività per qualsiasi ragione (ad esempio non è installato un programma di posta elettronica, oppure il computer era spento in quel momento), è possibile configurare l'attività perché sia eseguita automaticamente non appena possibile. Selezionare **Esegui attività se saltata** nella finestra di pianificazione.

6.6. Opzioni di alimentazione

Le scansioni antivirus aumentano il carico sul processore centrale e sui sottosistemi del disco, rallentando di conseguenza altri programmi. Per impostazione predefinita, in tali circostanze l'applicazione sospende temporaneamente la scansione antivirus e libera risorse di sistema per le applicazioni dell'utente.

Esistono tuttavia numerosi programmi che possono essere avviati non appena si liberano risorse di sistema e funzionano in modalità secondaria. Affinché le

scansioni antivirus non dipendano dal funzionamento di tali programmi, deselezionare **Concedi risorse ad altre applicazioni** (vedere Figura 15).

Si noti che questa impostazione può essere configurata individualmente per ciascuna attività di scansione anti-virus. In tal caso, la configurazione per un'attività specifica ha maggiore priorità.

Nella finestra che si apre, quando si fa clic sul pulsante **Configurazione Multi-CPU**, è possibile assegnare le impostazioni di Kaspersky Anti-Virus per l'esecuzione su un server multi-processore (vedere 6.7 a pag. 69).

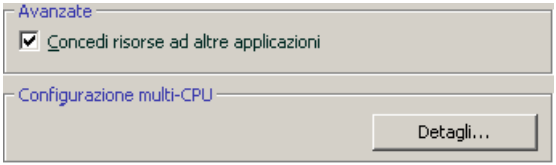


Figura 15. Configurazione delle impostazioni di alimentazione

Per configurare le impostazioni di alimentazione:

Selezionare la sezione **Protezione** della finestra principale del programma e fare clic sul collegamento Impostazioni. Configurare le impostazioni di alimentazione nella casella **Avanzate**.

6.7. Configurazione di un server multiprocessore

Questa finestra consente di configurare le impostazioni di efficienza operativa del server in una configurazione multiprocessore.

Numero di istanze kernel anti-virus – numero di copie della kernel anti-virus da caricare quando Anti-Virus Kaspersky è in esecuzione sul server. Questo numero determina il numero di processi anti-virus in esecuzione in parallelo.

Più copie del motore anti-virus sono esecuzione, più velocemente verranno elaborate le attività anti-virus. Tuttavia, ciò ha effetto sulle prestazioni generali del server.

Inoltre, l'esecuzione simultanea di diversi processi anti-virus sul server garantisce che il server sia sempre protetto nel caso in cui un motori abbia dei problemi.

Per distribuire automaticamente tra i processori i processi anti-virus, selezionare **Usa driver speciale per gestire processi paralleli**.

Se questa casella di controllo è selezionata, è possibile regolare manualmente il carico sul server, ad esempio riservando un gruppo di processori per l'elaborazione anti-virus ed un'altro alle attività vere e proprie del server. A tal fine, deselezionare i processori dedicati al server nella casella **Processori utilizzati**.

Kaspersky Lab raccomanda di riservare almeno un processore alle attività del server, in caso di server multiprocessore.

CAPITOLO 7. PROTEZIONE ANTI-VIRUS DEL FILE SYSTEM DEL SERVER

Kaspersky Anti-Virus include *File Anti-Virus*, che protegge i file del computer uso dalle infezioni. 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 viene indicata dall'icona di Kaspersky Anti-Virus for Windows Servers nell'area di notifica, che ha il seguente aspetto  ogniqualvolta viene esaminato un file.

Per impostazione predefinita, File Anti-Virus esamina solo i *file nuovi o modificati*, ovvero, i file che sono stati aggiunti o modificati dall'ultima scansione. I file vengono esaminati con il seguente algoritmo:

1. Il componente intercetta i tentativi da parte di utenti o programmi di accedere a qualsiasi file.
2. File Anti-Virus esamina i database di iChecker™ e iSwift™ in cerca di informazioni sul file intercettato. La decisione se esaminare o meno il file viene presa in base alle informazioni recuperate.

Il processo di scansione si svolge come segue:

1. Il file viene sottoposto a scansione antivirus. Gli oggetti nocivi vengono rilevati confrontandoli con l'*l'elenco delle minacce* del programma, che contiene la descrizione di tutti programmi nocivi e delle minacce conosciute fino ad ora, ed i metodi per la neutralizzazione.
2. Dopo l'analisi, sono possibili tre linee di azione:
    a. Se nel file viene rilevato un codice nocivo, File Anti-Virus blocca il file, ne memorizza una copia nella cartella di *Backup*, e tenta di neutralizzarlo. Se la riparazione ha esito positivo, il file viene reso nuovamente accessibile. In caso contrario il file viene eliminato.
    b. Se nel file si rileva un codice che appare nocivo ma senza certezza, quel file viene trasferito nella cartella di *Quarantena*.
    c. Se nel file non viene rilevato alcun codice nocivo, il file viene immediatamente ripristinato.

7.1. Selezione di un livello di sicurezza dei file

File Anti-Virus protegge i file in uso ad uno dei seguenti livelli (vedere Figura 16):

- **Alto** – il livello di monitoraggio più approfondito dei file aperti, salvati o eseguiti.
- **Consigliato** – Kaspersky Lab raccomanda questo livello. Vengono esaminate le seguenti categorie di oggetti:
    - Programmi e file in base ai contenuti
    - Nuovi oggetti ed oggetti modificati dall'ultima scansione
    - Oggetti OLE integrati
- **Basso** – livello che consente di utilizzare le applicazioni che richiedono considerevoli risorse di sistema, grazie alla limitazione del numero di file esaminati.

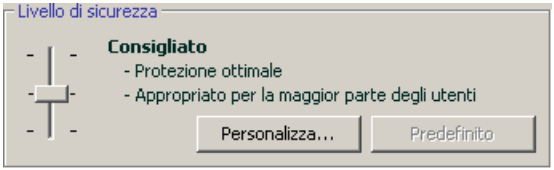


Figura 16. Livello di sicurezza di File Anti-Virus

L'impostazione predefinita per File Anti-Virus è **Consigliato**.

È possibile aumentare o ridurre il livello di protezione per i file utilizzati selezionando il livello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Regolando il livello di sicurezza, 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 predefiniti è ritenuto soddisfacente, è possibile personalizzare le impostazioni di protezione. Selezionare a tal fine il livello che più si approssima alle esigenze di sicurezza del computer, e utilizzarlo come punto di partenza per modificarne le impostazioni. In tal caso, il livello sarà impostato sul valore **Impostazioni personalizzate**. Osserviamo un esempio in

cui un livello di sicurezza dei file definito dall'utente può essere particolarmente utile.

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 dalla scansione eventuali file a causa delle dimensioni o dell'estensione, anche se ciò potrebbe influire sulla produttività del computer.

Suggerimento per la selezione di 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 consiglia di iniziare con il livello di sicurezza **Consigliato** apportando 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 sicurezza:

> Fare clic sul pulsante **Impostazioni** nella finestra delle impostazioni di File Anti-Virus. Modificare le impostazioni di File Anti-Virus nella finestra che si apre e fare clic su **OK**.

Viene quindi creato un quarto livello di sicurezza, **Impostazioni personalizzate**, che contiene le impostazioni di protezione configurate dall'utente.

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 possono essere suddivise nei seguenti gruppi:

- Impostazioni che definiscono i tipi di file (vedere 7.2.1 a pag. 74) da sottoporre alla scansione antivirus
- Impostazioni che definiscono l'ambito della protezione (vedere 7.2.2 a pag. 76)

- Impostazioni che definiscono le reazioni del programma agli oggetti pericolosi individuati (vedere 7.2.5 a pag. 81)
- Impostazioni supplementari di File Anti-Virus (vedere 7.2.3 a pag. 78)

La presente sezione prende in esame dettagliatamente questi gruppi.

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 *composti*. I file semplici, ad esempio i file .txt, non contengono oggetti. Gli oggetti composti possono includere diversi oggetti, ciascuno dei quali può a sua volta contenere altri oggetti. 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** (vedere Figura 17). Selezionare una delle seguenti tre 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)**. Selezionando questo gruppo di file, File Anti-Virus esamina solo i file potenzialmente infetti, che potrebbero contenere un virus.

  Nota:

  Esistono diversi formati di file che presentano un rischio assai basso di infezione con codice nocivo e di conseguente attivazione. Un esempio ne sono i file .txt.

  Esistono viceversa formati di file che contengono o possono contenere codice eseguibile. Ne sono un esempio i formati *.exe, *.dll, o *.doc. Il rischio di infezione con codice nocivo e conseguente attivazione in tali file è assai alto.

  Prima dell'analisi anti-virus di un file, viene analizzato il formato della sua intestazione (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 determinandone il formato file in base all'estensione. Per mezzo del collegamento estensione, è possibile consultare un elenco delle estensioni (vedere A.1 a pag. 188) esaminate con questa opzione.

> Suggerimento:
>
> Ricordare che è possibile inviare virus all'interno di file con estensione (ad esempio, .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)**, il programma ignorerà l'estensione del file analizzandone invece l'intestazione, determinandone così la reale natura di file eseguibile. File Anti-Virus esaminerà il file alla ricerca di virus.

La sezione **Produttività** consente di specificare che solo i file nuovi e quelli modificati dalla scansione precedente devono essere esaminati. Questa modalità riduce considerevolmente la durata della scansione e aumenta la velocità del programma. A tal fine, selezionare l'opzione **Esamina solo file nuovi e modificati**. Questa modalità si applica ai file sia semplici che compositi.

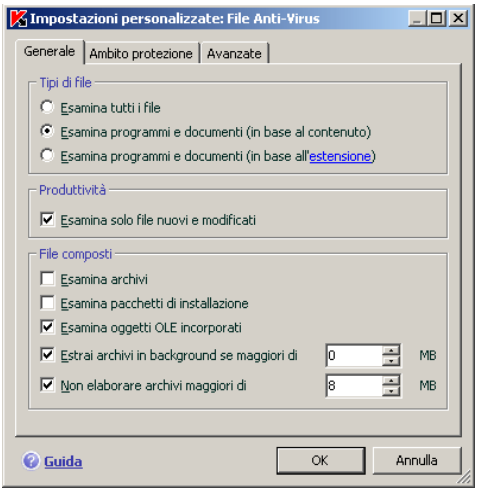


Figura 17. Seleziona file da esaminare

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

Esamina Tutti/Solo nuovi archivi – esamina archivi .zip, .cab, .rar, e .arj.

- **Esamina Tutti/Solo nuovi pacchetti d'installazione** – analizza gli archivi autoestraenti alla ricerca di virus.
- **Esamina Tutti/Solo nuovi oggetti OLE incorporati** – analizza gli oggetti incorporati nei file (per esempio i fogli di lavoro di Microsoft Office Excel o le macro incorporate in un file di Microsoft Office Word, gli allegati di posta elettronica, ecc.).

Per ogni tipo di file complesso è possibile selezionare ed esaminare tutti i file o solo quelli nuovi. A tal fine, fare clic sul collegamento accanto al nome dell'oggetto per modificarne il valore. Se la sezione **Produttività** è stata impostata per analizzare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file compositi da esaminare.

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

- **Estrai archivi in background se 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 rende nuovamente disponibile. 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.
- **Non elaborare archivi maggiori di... MB**. Se è stata selezionata questa opzione, i file di dimensioni superiori a quella specificata saranno esclusi dalla scansione.

7.2.2. Definizione dell'ambito della protezione

Per impostazione predefinita, File Anti-Virus analizza tutti i file nel momento in cui vengono utilizzati, indipendentemente da dove siano memorizzati, sia su un disco fisso, un CD/DVD-ROM, o un'unità flash.

È possibile limitare la portata della protezione. Per fare ciò:

1. Selezionare **File Anti-Virus** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Personalizza** e selezionare la scheda **Ambito protezione** (vedere Figura 18) nella finestra che si apre.

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. Utilizzare

i pulsanti **Aggiungi, Modifica** ed **Elimina** per aggiungere elementi della lista e modificarla.

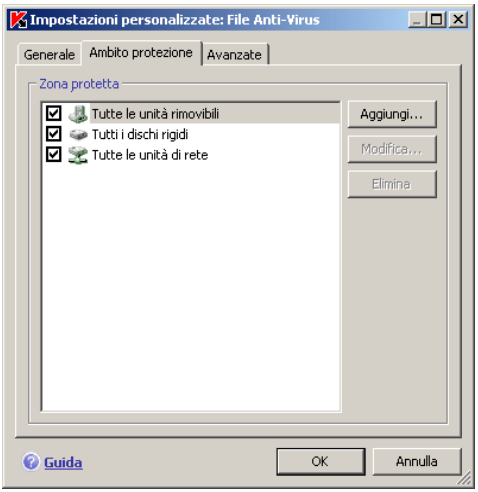


Figura 18. Creazione di una zona protetta

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 (vedere 6.3 a pag. 58).
- Combinare i metodi uno e due per creare una protezione il cui ambito esclude una serie di oggetti.

È possibile utilizzare le maschere quando si aggiungono oggetti da esaminare. Si noti che è possibile immettere solo maschere con percorsi assoluti agli oggetti:

- **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*, dove ? può rappresentare qualsiasi carattere
- **C:\dir\test** – solo il file *C:\dir\test*

Per eseguire la scansione in modo ripetitivo, selezionare ☑ **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. Selezionare **File Anti-Virus** nella finestra principale e passare alla finestra delle impostazioni del componente facendo clic sul collegamento Impostazioni.
2. Fare clic sul pulsante **Personalizza** e selezionare la scheda **Avanzate** nella finestra che si apre (vedere Figura 19).

La modalità di scansione dei file determina le condizioni di elaborazione 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 che sovrascrivono il file comprese tra queste due operazioni non vengono esaminate.

  La modalità Smart è quella predefinita.

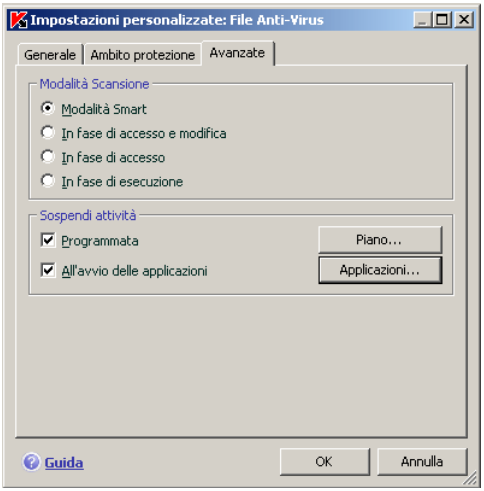


Figura 19. Configurazione delle impostazioni supplementari Anti-Virus file

- **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 riottenga 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, selezionare ☑ **Programmata**, quindi selezionare un intervallo temporale per arrestare ed avviare il componente nella finestra che si apre (vedere Figura 20) facendo clic sul pulsante **Piano**. Per fare ciò, inserire una valore in formato HH:MM nei campi corrispondenti.

Figura 20. 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 (cfr. Figura 21) facendo clic su **Applicazioni**.

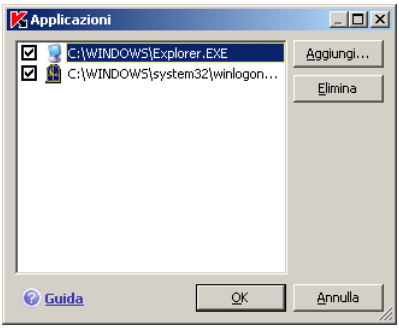


Figura 21. Creazione di un elenco di applicazioni

Per aggiungere un'applicazione all'elenco, utilizzare il pulsante **Aggiungi**. Si apre un menu di scelta rapida, 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 Anti-Virus file con un'applicazione specifica, deselezionandone il nome. Non è necessario eliminarla dall'elenco.

7.2.4. Ripristino delle impostazioni di File Anti-Virus

Durante la configurazione di File Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni predefinite. Gli esperti Kaspersky Lab considerano queste impostazioni come ottimali e le hanno raccolte nel livello di sicurezza **Consigliato**.

Per ripristinare le impostazioni predefinite di File Anti-Virus:

1. Selezionare **File Anti-Virus** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni.

2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

Se la lista di oggetti inclusi nella zona protetta è stato modificato durante la configurazione delle impostazioni di File Anti-Virus, il programma chiede se si desidera salvare tale lista per utilizzarla in futuro quando si ripristinano le impostazioni iniziali. Per salvare l'elenco di oggetti, selezionare **Zona protetta** nella finestra **Ripristina impostazioni** che viene visualizzata.

7.2.5. 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 status dell'oggetto e dall'azione selezionata.

File Anti-Virus applica agli oggetti i seguenti stati:

- *Programma nocivo* (ad esempio, *virus, Trojan*) (vedere 1.1 a pag. 9).
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il programma ha rilevato nel file una sequenza di codice proveniente da un virus sconosciuto, o modificato da un virus conosciuto.

Per impostazione predefinita, tutti i file infetti sono sottoposti a disinfezione, mentre se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

selezionare **File Anti-Virus** nella finestra principale e andare alla finestra delle impostazioni del componente facendo clic su Impostazioni. Nelle sezioni corrispondenti vengono visualizzate tutte le potenziali azioni (vedere Figura 22).

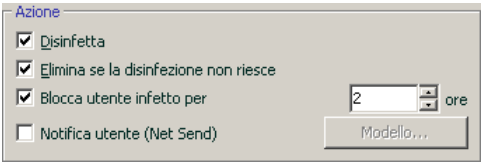


Figura 22. Azioni possibili di File Anti-Virus in caso di oggetti pericolosi

Se l'azione selezionata è	Quando viene rilevato un oggetto pericoloso
☑ **Disinfetta** ☐ **Elimina se la disinfezione non riesce**	L'accesso all'oggetto viene bloccato tentando di disinfettarlo. Una copia dell'oggetto viene memorizzata nella memoria di Backup. Se la disinfezione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non riesce, l'oggetto viene trasferito nella cartella di Quarantena. Le informazioni relative all'evento vengono registrate nel rapporto. In un secondo tempo sarà possibile tentare di disinfettare l'oggetto.
☑ **Disinfetta** ☑ **Elimina se la disinfezione non riesce**	L'accesso all'oggetto viene bloccato tentando di disinfettarlo. Una copia dell'oggetto viene memorizzata nella memoria di Backup. Se la disinfezione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non riesce, l'oggetto viene eliminato.
☐ **Disinfetta** ☑ **Elimina**	File Anti-Virus blocca l'accesso all'oggetto e lo elimina.
☑ **Blocca l'utente infetto per … ore**	Blocca l'accesso al server o al computer dal quale è stato fatto il tentativo di copiare il file infetto o potenzialmente infetto. Questa azione può inoltre essere applicata alle azioni relative all'elaborazione del file (disinfezione o eliminazione). SI noti che se l'utente esce da una sessione ed accede nuovamente al sistema, Kaspersky Anti-Virus considererà tale evento come una nuova connessione e la disabilitazione verrà annullata.

Se l'azione selezionata è	Quando viene rilevato un oggetto pericoloso
☑ **Notifica utente (Net Send)**	Notifica l'utente dal cui computer sono stati effettuati tentativi di copiare il file infetto o potenzialmente infetto sul server, tramite NetSend. Per configurare il modello di notifica, fare clic sul pulsante **Modello** (vedere 7.2.6 a pag. 83).

Quando disinfetta o elimina un oggetto, Kaspersky Anti-Virus ne crea una copia di backup e la invia nella cartella Backup, qualora l'oggetto dovesse essere ripristinato o si presentasse la possibilità di trattarlo.

Attenzione! Le azioni **Blocca utente** e **NetSend** non sono disponibili se si sta eseguendo l'applicazione in Microsoft Windows NT Server.

7.2.6. Creazione di un modello di notifica

Questa finestra consente di formattare il testo per il modello di notifica per l'utente il cui computer abbia cercato di copiare un file infetto o potenzialmente tale sul server.

Il testo di notifica può contenere macro per fornire ulteriori informazioni: il percorso all'oggetto nocivo e il nome della minaccia. Per aggiungere macro al testo di notifica, fare clic su **Macro.**

Per ripristinare il testo iniziale utilizzato per il modello di notifica, fare clic sul pulsante **Predefinito**.

7.3. Riparazione posticipata

In Kaspersky Anti-Virus for Windows Servers, l'accesso ai file infetti viene bloccato se vengono disinfettati, e, se eliminati, nei casi in cui la disinfezione o l'eliminazione non sono state possibili.

In Kaspersky Anti-Virus for Windows Servers, l'accesso ai file infetti viene bloccato se vengono disinfettati, e, se eliminati, nei casi in cui la disinfezione non è stata possibile.

Per riottenere l'accesso agli oggetti bloccati, essi devono essere disinfettati. Per fare ciò:

1. Selezionare **File Anti-Virus**nella finestra principale del programma e fare clic con il tasto sinistro del mouse ovunque nel riquadro **Statistiche**.
2. Selezionare gli oggetti di interesse nella scheda **Rilevati** e fare clic sul pulsante **Azioni** → **Isola tutto**.

I file disinfettati con successo verranno resi nuovamente disponibili all'utente. Qualsiasi file impossibile da trattare può essere *eliminato* o *ignorato*. In quest'ultimo caso, l'accesso al file sarà ripristinato. Ciò tuttavia aumenta considerevolmente il rischio di infezione del computer.

CAPITOLO 8. LA SCANSIONE ANTIVIRUS DEL COMPUTER

Kaspersky Anti-Virus for Windows Servers può operare la scansione su singoli oggetti (file, cartelle, unità disco, dispositivi plug-and-play), o sull'intero computer. La scansione anti-virus impedisce la diffusione di quei codici dannosi che non sono stati individuati da File Anti-Virus.

Kaspersky Anti-Virus for Windows Servers include le seguenti attività di scansione predefinite:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del compute, tra cui: memoria di sistema, programmi caricati all'avvio, settori di avvio sul 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.

Le impostazioni raccomandate per queste modalità sono quelle predefinite. È possibile modificare tali impostazioni (vedere 8.4 a pag. 89) o pianificare l'esecuzione delle attività (vedere 6.5 a pag. 66).

È inoltre possibile creare modalità di scansione personalizzate (vedere 8.3 a pag. 88) e pianificarne l'esecuzione. Per esempio, si può pianificare un'attività di scansione antivirus del database di posta una volta alla settimana, oppure una scansione antivirus per la cartella **Documenti**.

Inoltre, è possibile esaminare qualsiasi oggetto alla ricerca di virus senza creare speciali attività di scansione. L'oggetto da esaminare può essere selezionato dall'interfaccia di Kaspersky Anti-Virus for Windows Servers o tramite gli strumenti standard del sistema operativo Windows Server (per esempio, dalla finestra di **Esplora risorse** o dal **Desktop**).

L'elenco completo delle attività di scansione antivirus per il computer è disponibile nella sezione **Scansione** della porzione sinistra della finestra principale del programma.

8.1. Gestione delle attività di scansione antivirus

La scansione antivirus può essere avviata manualmente, oppure in maniera automatica, a scadenze predefinite (vedere 6.5 a pag. 66).

Per avviare manualmente un'attività di scansione:

Selezionare la casella accanto al nome dell'attività nella sezione **Scansione** della finestra principale del programma e fare clic sul pulsante nella barra di stato.

Le attività attualmente in esecuzione (comprese quelle create tramite Kaspersky Administration Kit) vengono visualizzate nel menu di scelta rapida facendo clic col tasto destro del mouse sull'icona nell'area di notifica.

Per sospendere un'attività:

Fare clic sul pulsante nella barra di stato. Lo stato dell'attività si modifica in *sospeso*. In tal modo la scansione risulterà sospesa finché non sarà riavviata manualmente, o fino all'occorrenza della successiva scansione pianificata.

Per terminare un'attività di scansione:

Fare clic sul pulsante nella barra di stato. Lo stato dell'operazione si modifica in *fermato*. Ciò determinerà l'arresto della scansione, che potrà essere riavviata manualmente, o che sarà riavviata automaticamente secondo quanto pianificato. Alla prossima esecuzione della scansione, il programma chiederà all'utente se desidera riprendere la scansione dal punto in cui era stata interrotta, o ricominciarla da capo.

8.2. Creazione di un elenco di oggetti da esaminare

Per visualizzare una lista di oggetti da sottoporre a scansione con una particolare attività, selezionare il nome dell'attività (per esempio, Risorse del computer**)** nella sezione **Scansione** della finestra principale del programma. L'elenco degli oggetti sarà visualizzato sul lato destro della finestra, sotto la barra di stato (vedere Figura 23).

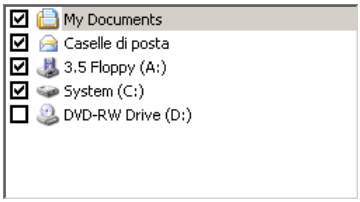


Figura 23. Elenco di oggetti su cui operare la scansione

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.

È possibile ampliare o modificare un elenco di oggetti da esaminare utilizzando i pulsanti sulla destra dell'elenco. Per aggiungere un nuovo oggetto da scansionare alla lista, fare clic su **Aggiungi** e nella finestra che si apre selezionare l'oggetto da analizzare.

Per comodità dell'utente, è possibile aggiungere categorie ad un'area di scansione, ad esempio le caselle di posta dell'utente, la RAM, gli oggetti di avvio, il backup del sistema operativo, e i file nella cartella Quarantena di Kaspersky Anti-Virus.

Inoltre, quando si aggiunge ad un'area di scansione una cartella che contiene oggetti incorporati, è possibile modificarne la ricorsività selezionando un oggetto nell'elenco corrispondente per aprirne il menù di scelta rapida ed utilizzare l'opzione **Includi sottocartelle**.

Per eliminare un oggetto, selezionarlo nell'elenco (così facendo, il nome dell'oggetto risulta evidenziato in grigio) e fare clic sul pulsante **Elimina**. È possibile disabilitare temporaneamente la scansione su singoli oggetti per qualsiasi attività, senza doverli cancellare dalla lista. Per far ciò è sufficiente deselezionare la casella accanto agli oggetti in questione.

Per avviare un'operazione di scansione, fare clic sul pulsante **Scansione**, oppure selezionare **Avvia** dal menu che si apre facendo clic sul pulsante **Azioni**.

Inoltre, l'oggetto da esaminare può essere selezionato dagli strumenti standard del sistema operativo Windows Server (per esempio dalla finestra di Esplora risorse o dal Desktop, ecc.) (vedere Figura 24). Selezionare l'oggetto, aprire il menù di scelta rapida di Windows Server facendo clic col tasto destro del mouse, e selezionare **Ricerca virus**.

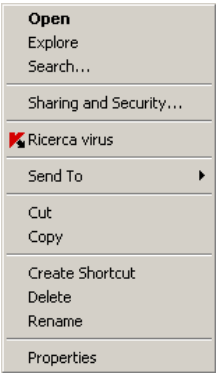


Figura 24. Scansione di oggetti attraverso il menu di scelta rapida di Windows

8.3. 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. Le nuove attività di scansione vengono create utilizzando le attività esistenti come modello.

Per creare una nuova attività di scansione antivirus:

1. Selezionare l'attività con le impostazioni più simili a quelle desiderate nella sezione **Scansione** della finestra principale del programma.
2. Aprire il menu di scelta rapida facendo clic con il pulsante destro del mouse sul nome dell'attività, o fare clic su **Azioni** a destra della lista di oggetti da sottoporre a scansione e selezionare **Salva con nome...**.
3. Immettere il nome della nuova attività nella finestra che si apre e fare clic su **OK**. Un'attività con il nome corrispondente appare quindi nella lista di attività nella sezione **Scansione** della finestra principale del programma.

Attenzione!

Il numero di attività che l'utente può creare è limitato. Possono essere create quattro attività al massimo.

La nuova attività è una coppia di quella sulla quale è stata basata. Per mettere ulteriormente a punto la nuova attività è necessario creare l'elenco di oggetti su cui operare la scansione (vedere 8.2 a pag. 86), impostarne le proprietà (vedere

8.4 a pag. 89), e, se necessario, pianificarne (vedere 6.5 a pag. 66) l'esecuzione automatica.

Per rinominare un'attività creata:

Selezionare l'attività nella sezione **Scansione** della finestra principale del programma. Fare clic col tasto destro del mouse sul nome dell'attività per aprire il menù contestuale, o fare clic sul pulsante **Azioni** a destra dell'elenco degli oggetti da esaminare, quindi selezionare **Rinomina**.

Immettere il nome della nuova attività finestra che si apre e fare clic su **OK**. Il nome dell'attività risulterà modificato anche nella sezione **Scansione**.

Per eliminare un'attività creata:

Selezionare l'attività nella sezione **Scansione** della finestra principale del programma. Fare clic col tasto destro del mouse sul nome dell'attività per aprire il menù contestuale, o fare clic sul pulsante **Azioni** a destra dell'elenco degli oggetti da esaminare, quindi selezionare **Elimina**.

Verrà richiesta conferma dell'eliminazione dell'attività. L'attività risulta quindi eliminata dalla lista di attività nella sezione **Scansione**.

Attenzione!

È possibile rinominare od eliminare soltanto le attività create dall'utente.

8.4. Configurazione delle attività di scansione antivirus

I metodi utilizzati per esaminare gli oggetti sul computer sono determinati dalle proprietà assegnate ad ogni attività.

Per configurare le impostazioni dell'attività:

aprire la finestra delle impostazioni dell'applicazione e selezionare il nome dell'attività nella sezione **Scansione**.

Per ciascuna attività di scansione, è possibile utilizzare tale finestra per:

- Selezionare il livello di sicurezza che sarà utilizzato dall'attività (vedere 8.4.1 a pag. 90)
- Modificare le impostazioni avanzate:
    - definire i tipi di file da sottoporre a scansione antivirus (vedere 8.4.2 a pag. 91)

- configurare l'avvio dell'attività utilizzando un profilo utente diverso (vedere 6.4 a pag. 65)
- configurare le impostazioni avanzate di scansione (vedere 8.4.5 a pag. 97)

- configurare le impostazioni predefinite di scansione (vedere 8.4.3 a pag. 94)
- selezionare l'azione che il programma applicherà non appena rileva un oggetto infetto, o potenzialmente tale (vedere 8.4.4 a pag. 95)
- pianificare (vedere 6.5 a pag. 66) l'avvio automatico delle attività

È inoltre possibile configurare le impostazioni globali (vedere 8.4.6 a pag. 98) applicabili all'esecuzione di tutte le attività.

La presente sezione della Guida esaminerà le impostazioni delle attività elencate sopra in dettaglio.

8.4.1. Selezione di un livello di sicurezza

A ciascuna attività di scansione antivirus può essere assegnato un livello di sicurezza (vedere Figura 25):

Alto – la scansione più completa dell'intero computer o di singoli dischi, cartelle o file. Se ne raccomanda l'impiego qualora si sospetti che un virus possa essere penetrato nel computer.

Consigliato – gli esperti di Kaspersky Lab raccomandano questo livello. Verranno esaminati gli stessi file dell'impostazione **Alto**, fatta eccezione per i database di posta.

Basso – livello che permette all'utente un agevole impiego di applicazioni che utilizzino estensivamente le risorse della macchina, poiché la gamma dei file sottoposti a scansione è ridotta.

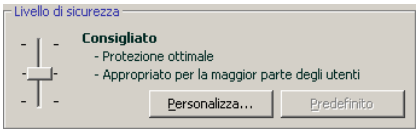


Figura 25. Selezione di un livello di sicurezza per la scansione antivirus

Per impostazione predefinita, la scansione dei file è impostata sul livello **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 sicurezza:

Regolare i cursori. Regolando il livello di sicurezza, 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 personalizzare le impostazioni di scansione. Selezionare a tal fine il livello che più si approssima alle esigenze di sicurezza del computer, e utilizzarlo come punto di partenza per modificarne le impostazioni. In tal caso, il livello verrà rinominato come **Impostazioni personalizzate**.

Per modificare le impostazioni di un livello di sicurezza:

fare clic sul pulsante **Personalizza** nella finestra delle impostazioni delle attività. Nella finestra che appare, aggiustare i parametri di scansione e premere **OK**.

Così facendo, viene creato un quarto livello di sicurezza, **Impostazioni personalizzate**, che contiene le impostazioni di scansione configurate dall'utente stesso.

8.4.2. Definizione dei tipi di oggetti da sottoporre a scansione

Specificando 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** (vedere Figura 26). Selezionare una delle seguenti tre opzioni:

- **Esamina tutti i file**. Con questa opzione, tutti i file saranno esaminati 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.

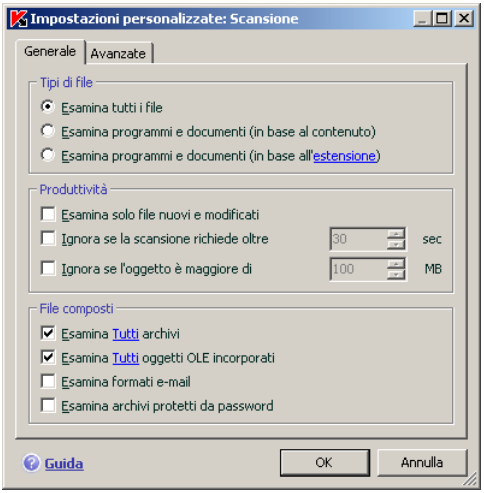


Figura 26. Configurazione delle impostazioni di scansione

> Nota:
>
> Ci 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. Un esempio ne sono i file .txt.
>
> Inoltre, esistono viceversa formati di file che contengono o possono contenere codice eseguibile. Ne sono un esempio i formati *.exe, *.dll, o *.doc. Il rischio di infezione con codice nocivo e conseguente attivazione in tali file è assai alto.

Prima dell'analisi antivirus in un oggetto, viene analizzato il formato della sua intestazione interna (txt, doc, exe, ecc.).

- **Esamina programmi e documenti (in base all'estensione)**. In questo caso, il programma esaminerà solo i file potenzialmente infetti, determinandone il formato in base all'estensione. Utilizzando il link, è possibile accedere ad un elenco di estensioni file che, con questa opzione, vengono sottoposti a scansione (vedere A.1 a pagina 188).

Suggerimento:

Si tenga presente che è possibile inviare virus con estensione .txt che sono in realtà file eseguibili rinominati come file .txt. 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)**, il programma analizzerà l'intestazione dei file, determinandone così la reale natura di file .exe ed esaminandolo attentamente alla ricerca di virus.

Nella sezione **Produttività**, è possibile specificare di eseguire l'analisi anti-virus solo sui file nuovi o su quelli modificati dalla scansione precedente. Questa modalità riduce considerevolmente la durata della scansione e aumenta la velocità del programma. A tal fine, selezionare l'opzione **Esamina solo file nuovi e modificati**. Questa modalità si applica sia ai file semplici che a quelli compositi.

La sezione **Produttività** consente inoltre di stabilire limiti di tempo e di dimensione dei file per la scansione.

- **Ignora se la scansione richiede oltre ... sec.** Selezionare quest'opzione ed inserire la durata massima di scansione per un oggetto. Se la scansione di un oggetto richiede un tempo superiore a quello specificato, l'oggetto viene rimosso dalla coda di scansione.
- **Ignora se l'oggetto è maggiore di … MB.** Selezionare quest'opzione ed inserire la dimensione massima dell'oggetto. Se viene superata questa dimensione, l'oggetto viene rimosso dalla coda di scansione.

Nella sezione **File compositi**, specificare quali file compositi sottoporre all'analisi anti-virus:

- **Esamina Tutti/Solo nuovi archivi** – esegue la scansione sugli archivi con estensione .rar, .arj, .zip, .cab, .lha, .jar, e .ice.

Attenzione!

Kaspersky Anti-Virus non elimina automaticamente i formati di file compressi che non supporta (ad esempio, .ha, .uue, .tar), anche se si seleziona l'opzione di disinfezione o eliminazione automatica se i file non possono essere trattati.

Per eliminare questi file compressi, fare clic sul collegamento Elimina archivi nella notifica di rilevamento di un oggetto pericoloso. Lo schermo visualizza questo messaggio quando l'opzione **Richiedi intervento utente durante la scansione/Richiedi intervento utente al termine della scansione** è selezionata (vedere 8.4.4 a pag. 95). È anche possibile eliminare gli archivi infetti manualmente.

☑ **Esamina Tutti/Solo nuovi oggetti OLE incorporati** – Analizza gli oggetti incorporati nei file (per esempio fogli di lavoro in Excel o macro incorporati in un file di MS Word, allegati di posta elettronica, ecc.).

Per ogni tipo di file complesso è possibile selezionare ed esaminare tutti i file o solo quelli nuovi A tal fine, utilizzare il collegamento 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 per analizzare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file compositi da esaminare.

☑ **Esamina formati e-mail** – esamina i file in formato e-mail ed i database della posta elettronica. Se questa casella di controllo è deselezionata, i file in formato posta verranno esaminati come file binari (senza dissezionare il formato), e se il file non è infetto ed è selezionata l'opzione Esamina tutti i file, le informazioni in merito vengono registrate nel rapporto con lo stato *OK*. Se le impostazioni di scansione dei file sono state selezionate per tipo ed estensione, l'oggetto verrà ignorato, col verdetto *escluso per tipo*.

Si noti quanto segue per la scansione dei database di e-mail protetti da password:

- Kaspersky Anti-Virus for Windows Servers rileva i codici nocivi nei database di Microsoft Office Outlook 2000 ma non li disinfetta;
- Kaspersky Anti-Virus for Windows Servers non supporta le scansioni di codici nocivi in database protetti di Microsoft Office Outlook 2003.

☑ **Esamina archivi protetti da password** – analizza gli archivi protetti da password. Con questa funzione, una finestra richiederà l'inserimento di una password per la scansione di un oggetto compresso. Se la casella non è selezionata, la scansione salterà gli archivi protetti da password.

8.4.3. Ripristino delle impostazioni di scansione predefinite

Quando si configurano le impostazioni per una data attività di scansione, è sempre possibile ripristinare le impostazioni raccomandate. Gli esperti Kaspersky Lab considerano queste impostazioni come ottimali e le hanno raccolte nel livello di sicurezza **Consigliato**.

Per ripristinare le impostazioni di scansione predefinite:

1. Selezionare il nome dell'attività nella sezione **Scansione** della finestra principale e usare il collegamento Impostazioni per aprire la finestra delle impostazioni dell'attività.

2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

8.4.4. 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 assegnato uno dei seguenti stati, dopo la scansione:

- Programma nocivo (per esempio, *virus, trojan*).
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. È probabile che il programma abbia rilevato nel file una sequenza di codice proveniente da un virus sconosciuto, o modificato da un virus conosciuto.

Per impostazione predefinita, tutti i file infetti vengono disinfettati, mentre se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

selezionare il nome dell'attività nella sezione **Scansione** della finestra principale del programma e usare il collegamento Impostazioni per aprire la finestra delle impostazioni dell'attività. Nelle sezioni corrispondenti vengono visualizzate tutte le potenziali reazioni (vedere Figura 27).

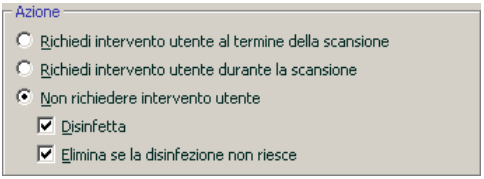


Figura 27. Selezione di un'azione per gli oggetti pericolosi

Se l'azione selezionata è	**Se viene rilevato un oggetto nocivo o potenzialmente infetto**
Richiedi intervento utente al termine della scansione	Il programma non elabora gli oggetti prima della fine della scansione. Al termine del processo, la finestra delle statistiche mostrerà l'elenco degli oggetti rilevati uno dopo l'altro,

Se l'azione selezionata è	Se viene rilevato un oggetto nocivo o potenzialmente infetto
	chiedendo all'utente l'azione da compiere per ciascuno di essi.
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 né notificare l'utente. Si sconsiglia di utilizzare quest'opzione, poiché gli oggetti infetti e potenzialmente infetti restano sul computer, ed è praticamente impossibile evitare l'infezione.
Non richiedere intervento utente **Disinfetta**	Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Se la disinfezione non riesce, l'oggetto viene trasferito nella cartella di Backup per futura disinfezione. Se il programma non riesce a disinfettare l'oggetto, blocca l'accesso ad esso.
Non richiedere intervento utente **Disinfetta** **Elimina se la disinfezione non riesce**	Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Se la disinfezione non riesce, l'oggetto viene eliminato. Ne viene salvata una copia nella memoria di backup.
Non richiedere intervento utente **Disinfetta** **Elimina**	Il programma elimina automaticamente l'oggetto rilevato.

Quando disinfetta o elimina un oggetto, Kaspersky Anti-Virus ne crea una copia di backup e la invia nella cartella di Backup, (vedere 12.2 a pag. 156), qualora l'oggetto dovesse essere ripristinato o si presentasse la possibilità di trattarlo.

Con lo stato *potenzialmente infetto*, l'oggetto viene spostato in quarantena senza alcun tentativo di disinfettarlo.

8.4.5. Ulteriori impostazioni di scansione antivirus

Oltre alle impostazioni di base per la scansione anti-virus, è possibile configurare una serie di impostazioni avanzate (vedere Figura 28):

- **Attiva tecnologia iChecker** – usa una tecnologia che aumenta la velocità di scansione escludendo determinati oggetti dalla scansione. Un oggetto viene escluso dalla scansione utilizzando uno speciale algoritmo che prende in considerazione la data di rilascio dell'elenco dei virus, la data dell'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

  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 risulta modificata perché è stato aggiunto un nuovo oggetto o perché le impostazioni di scansione sono state modificate o gli elenchi dei virus aggiornati, il programma sottoporrà nuovamente l'archivio a scansione anti-virus.

  iChecker™ presenta tuttavia delle limitazioni: non funziona con file di grandi dimensioni e si applica solo ad oggetti con una struttura che Kaspersky Anti-Virus for Windows Servers è in grado di riconoscere (per esempio file di tipo exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).
- **Attiva tecnologia iSwift**. Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche iSwift presenta delle limitazioni: è legato ad una posizione specifica dei file nel file system e può essere applicato esclusivamente agli oggetti di un file system NTFS.
- **Registra informazioni su oggetti pericolosi in statistiche programma** – salva le informazioni sugli oggetti pericolosi rilevati nelle statistiche generali del programma e visualizza un elenco di minacce rilevate durante la scansione nella scheda **Rilevati** della finestra di rapporto (vedere 11.3.2 a pag. 130) . Se questa opzione è disabilitata le informazioni sugli oggetti pericolosi non verranno visualizzate nel rapporto e sarà impossibile elaborare i dati.

Concedi risorse ad altri applicazioni – sospende la scansione antivirus in corso se il processore è occupato con altre applicazioni.

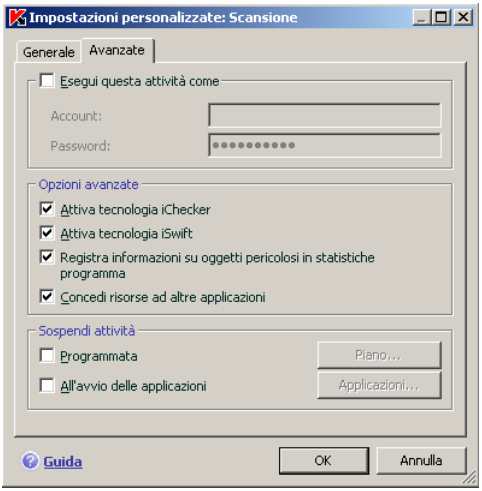


Figura 28. Impostazioni di scansione avanzate

8.4.6. Configurazione delle impostazioni di scansione globali per tutte le attività

Ogni operazione di scansione è eseguita in base alle proprie impostazioni. La modalità di scansione che si crea all'atto dell'installazione del programma utilizza le impostazioni predefinite raccomandate da 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. Selezionare la sezione **Scansione** nella parte sinistra della finestra principale del programma e fare clic su Impostazioni.
2. Configurare, nella finestra che appare, le impostazioni di scansione: Selezionare il livello di sicurezza (vedere 8.4.1 a pag. 90), configurare le impostazioni di livello avanzato, e selezionare un'azione (vedere 8.4.4 a pag. 95) per gli oggetti.

3. Per applicare queste nuove impostazioni a tutte le attività, fare clic sul pulsante **Applica** nella sezione **Altre impostazioni attività**. Confermare le impostazioni globali selezionate nella successiva finestra di dialogo.

CAPITOLO 9. TESTARE KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Dopo aver installato e configurato Kaspersky Anti-Virus, si raccomanda di verificare la correttezza delle impostazioni e del funzionamento, servendosi di un virus di prova o di sue varianti.

9.1. Test del virus EICAR e delle sue varianti

Questo virus di prova è stato sviluppato specificamente da EICAR (European Institute for Computer Antivirus Research) per il collaudo dei prodotti antivirus.

NON SI TRATTA DI VIRUS, e non contiene codici di programma in grado di danneggiare il computer. Ciononostante la maggior parte dei programmi antivirus lo identifica come tale.

> Non utilizzare mai un vero virus per testare la funzionalità di un programma antivirus!

Il virus di prova può essere scaricato dal sito web ufficiale dell'organizzazione **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

Il file scaricato dal sito web della **EICAR** contiene il corpo di un virus di prova standard. Kaspersky Anti-Virus lo rileva, lo etichetta come **virus**, ed esegue l'azione prevista per quel tipo di oggetto.

Per verificare le reazioni di Kaspersky Anti-Virus quando vengono rilevati diversi tipi di oggetti, è possibile modificare i contenuti del virus di prova standard aggiungendo uno dei prefissi elencati nella seguente tabella.

Prefisso	**Stato del virus di prova**	**Azione corrispondente quando l'applicazione elabora l'oggetto**
Nessun prefisso, virus di prova standard	Il file contiene un virus di prova. Non è possibile disinfettare l'oggetto.	L'applicazione identifica l'oggetto come nocivo e non disinfettabile, quindi lo elimina.
CORR–	Corrotto.	L'applicazione ha potuto accedere all'oggetto ma non ha potuto esaminarlo, poiché l'oggetto è corrotto (ad esempio, è danneggiata la struttura del file, oppure il formato non è valido).
SUSP– WARN–	Il file contiene un virus di prova (variante). Non è possibile disinfettare l'oggetto.	Questo oggetto è una variante di un virus noto o è un virus sconosciuto. Al momento del rilevamento, il database dei virus non contiene una descrizione della procedura per trattare questo oggetto. L'applicazione mette in quarantena l'oggetto, per trattarlo successivamente con un database dei virus aggiornato.
ERRO–	Errore di elaborazione.	Si è verificato un errore durante l'elaborazione dell'oggetto: l'applicazione non può accedere all'oggetto da esaminare, poiché l'integrità dell'oggetto è stata violata (ad esempio, manca la parte finale di un volume a più archivi), oppure non c'è nessun collegamento ad esso (se l'oggetto viene esaminato su un'unità di rete).

Prefisso	Stato del virus di prova	Azione corrispondente quando l'applicazione elabora l'oggetto
CURE–	Il file contiene un virus di prova. Può essere disinfettato. L'oggetto può essere disinfettato, ed il testo del corpo del virus di prova viene modificato in CURE.	L'oggetto contiene un virus che può essere trattato. L'applicazione esamina l'oggetto alla ricerca di virus, quindi lo disinfetta completamente.
DELE–	Il file contiene un virus di prova. Non è possibile disinfettare l'oggetto.	L'oggetto contiene un virus che non può essere trattato, oppure è un trojan. Il programma elimina questi oggetti.

La prima colonna di questa tabella contiene i prefissi che devono essere aggiunti all'inizio della stringa per un virus di prova standard. La seconda colonna descrive lo stato e la reazione di Kaspersky Anti-Virus a diversi tipi di virus di prova. La terza colonna contiene informazioni sugli oggetti che hanno lo stesso stato trattati dall'applicazione.

I valori nelle impostazioni di scansione anti-virus determinano l'azione effettuata da ciascuno degli oggetti.

9.2. Testare File Anti-Virus

Per testare la funzionalità di File Anti-Virus:

1. Creare una cartella su un disco e copiare in essa il virus di prova scaricato dal sito Web ufficiale dell'organizzazione (vedere 9.1 a pag. 100), nonché le modifiche del virus di prova create dall'utente.
2. Lasciare che tutti gli eventi vengano registrati, in modo che il file rapporto conservi i dati sugli oggetti corrotti e quelli non esaminati a causa di errori. A tal fine, selezionare ☑ **Registra eventi non critici** nella finestra di impostazione dei rapporti (vedere11.3.1 a pag. 129).
3. Lanciare il virus di prova o una sua variante.

File Anti-Virus blocca il tentativo di accesso al file, lo esamina e lo elimina.

Quando si selezionano le diverse opzioni prestabilite di configurazione per trattare gli oggetti rilevati, è possibile testare la reazione di File Anti-Virus al rilevamento di diversi tipi di oggetti.

È possibile visualizzare dettagli sulle prestazioni di File Anti-Virus nel rapporto sul componente.

9.3. Testare le attività di scansione anti-virus

Per testare le attività di scansione anti-virus:

1. Creare una cartella su un disco e copiare in essa il virus di prova scaricato dal sito Web ufficiale dell'organizzazione (vedere 9.1 a pag. 100), nonché le modifiche del virus di prova create dall'utente.
2. Creare una nuova attività di scansione anti-virus (vedere 8.3 a pag. 88) e selezionare la cartella contenente il gruppo di virus di prova quale oggetto da esaminare (vedere 9.1 a pag. 100).
3. Lasciare che tutti gli eventi vengano registrati, in modo che il file rapporto conservi i dati sugli oggetti corrotti e quelli non esaminati a causa di errori. A tal fine, selezionare **Registra eventi non critici** nella finestra di impostazione dei rapporti.
4. Programmare una serie di scansioni antivirus (vedere 8.1 a pag. 86).

Quando si esegue una scansione, se vengono rilevati oggetti sospetti o pericolosi lo schermo visualizza notifiche informative sugli oggetti, richiedendo l'intervento dell'utente per quanto riguarda l'azione da intraprendere:

Figura 29. Rilevato oggetto pericoloso

In questo modo, selezionando come azioni diverse opzioni prestabilite di configurazione per trattare gli oggetti rilevati, è possibile testare le reazioni di Kaspersky Anti-Virus al rilevamento di diversi tipi di oggetti.

È possibile visualizzare dettagli sulle prestazioni dell'attività di scansione anti-virus nel rapporto sul componente.

CAPITOLO 10. AGGIORNAMENTI DEL PROGRAMMA

Mantenere aggiornato il software antivirus costituisce un investimento in termini di sicurezza. Poiché ogni giorno nascono nuovi virus, trojan e altri software dannosi, per proteggere costantemente le proprie informazioni è fondamentale aggiornare regolarmente l'applicazione.

L'aggiornamento dell'applicazione implica lo scaricamento e l'installazione, sul proprio computer, dei seguenti componenti:

- **Elenchi di minacce**

  Per proteggere le informazioni presenti sul computer l'applicazione utilizza gli elenchi di minacce, che vengono utilizzati dai componenti del programma che forniscono la protezione per rilevare e disinfettare oggetti dannosi eventualmente presenti. Le firme vengono aggiunte di ora in ora con la registrazione di nuove minacce e dei metodi per debellarle, Pertanto, si raccomanda di aggiornarli regolarmente.

  Le precedenti versioni delle applicazioni Kaspersky Lab supportavano database antivirus sia *standard* che *estesi*. Ogni database proteggeva il computer da diversi tipi di oggetti pericolosi. Con Kaspersky Anti-Virus for Windows Servers non è più necessario selezionare il database antivirus appropriato, poiché quelle impiegate da questo prodotto garantiscono la protezione sia dai tipi di oggetti pericolosi o potenzialmente tali, che dagli attacchi da parte di hacker.

- **Moduli applicazione**

  Oltre all'elenco dei virus, è possibile aggiornare i moduli di Kaspersky Anti-Virus for Windows Servers. Nuovi aggiornamenti dell'applicazione vengono elaborati con regolarità.

La principale fonte di aggiornamenti per Kaspersky Anti-Virus for Windows Servers è rappresentata dai server di Kaspersky Lab.

Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet.

Se non è possibile accedere ai server di aggiornamento di Kaspersky Lab (ad esempio perchè il computer non è connesso a Internet), chiamare l'ufficio centrale di Kaspersky Lab al numero +7 (495) 797-87-00, +7 (495) 645-79-39 o +7 (495) 956-70-00 per richiedere informazioni sui partner di Kaspersky Lab che possono fornire aggiornamenti in formato compresso su dischetti o CD-ROM.

Gli aggiornamenti possono essere scaricati secondo una delle seguenti modalità:

- *Automaticamente*. Kaspersky Anti-Virus verifica ad intervalli specificati la disponibilità di nuovi pacchetti di aggiornamento presso la relativa sorgente. Le scansioni possono essere impostate in modo da essere più frequenti durante le epidemie di virus e meno frequenti quando sono passate. Quando Anti-Virus rileva nuovi aggiornamenti, li scarica e li installa sul computer. È la modalità predefinita.
- *Come pianificato*. L'avvio dell'aggiornamento è pianificato ad una certa ora.
- *Manualmente*. Con questa opzione, la procedura di aggiornamento viene avviata manualmente.

Durante l'aggiornamento, l'applicazione confronta gli elenchi delle minacce ed i moduli di programma presenti sul computer con le versioni disponibili sul server. Se il server dispone della versione più recente degli elenchi dei virus e dei moduli, verrà visualizzata la relativa notifica nella finestra dell'applicazione. Se le versioni presenti sul computer non corrispondono a quelle disponibili sul server di aggiornamento, il programma scaricherà le sole parti mancanti. Non verranno invece scaricate gli elenchi dei virus e i moduli già presenti sulla macchina, permettendo in tal modo un significativo aumento nella velocità del processo ed una corrispondente riduzione del traffico in rete.

Prima di aggiornare gli elenchi dei virus, Kaspersky Anti-Virus for Windows Servers ne crea una copia di backup, che può essere utilizzata se fosse necessario tornare alla versione precedente (vedere 10.2 a pag. 107). Se, per esempio, il processo di aggiornamento corrompe gli elenchi delle minacce rendendoli inutilizzabili, è possibile tornare con facilità alla versione precedente e ritentare l'aggiornamento in seguito.

È possibile distribuire gli aggiornamenti ad una sorgente locale contemporaneamente all'aggiornamento dell'applicazione (vedere 10.4.4 a pag. 116). Questa funzione consente di aggiornare i database ed i moduli utilizzati dalle applicazioni della versione 6.0 su computer collegati in rete, in modo da risparmiare larghezza di banda.

10.1. Avvio della procedura di aggiornamento

È possibile iniziare l'aggiornamento in qualsiasi momento. Il processo opererà dall'origine dell'aggiornamento selezionata dall'utente (vedere 10.4.1 a pag. 109).

La procedura di aggiornamento può essere avviata da:

- il menù contestuale (vedere 4.2 a pag. 38);
- dalla finestra principale del programma (vedere 4.3 a pag. 39).

Per avviare la procedura di aggiornamento dal menu di scelta rapida:

1. Fare clic col tasto destro del mouse sull'icona dell'applicazione nell'area di notifica per aprire il menu di scelta rapida.
2. Selezionare **Aggiornamento**.

Per avviare la procedura di aggiornamento dalla finestra principale del programma:

1. Selezionare **Aggiornamento** nella sezione **Servizio**.
2. Fare clic sul pulsante **Aggiorna ora!** nel pannello di destra della finestra principale, o utilizzare il pulsante nella barra di stato.

Lo stato dell'aggiornamento verrà visualizzato in una speciale finestra, che può essere nascosta facendo clic su **Chiudi**. L-aggiornamento prosegue a finestra chiusa.

Si noti che gli aggiornamenti vengono distribuiti alla sorgente locale durante il processo di aggiornamento, sempre che il servizio sia abilitato (vedere 10.4.4 a pag. 116).

10.2. Ripristino dell'aggiornamento precedente

Ogni volta che si avvia la procedura di aggiornamento, Kaspersky Anti-Virus for Windows Servers crea una copia degli elenchi delle minacce correnti prima di iniziare a scaricarne le nuove versioni. In tal modo, qualora l'aggiornamento non vada a buon fine, è possibile tornare ad utilizzare gli elenchi delle minacce precedenti.

Per ripristinare la versione precedente degli elenchi delle minacce:

1. Selezionare il componente **Aggiornamento** nella sezione **Servizio** della finestra principale del programma.
2. Fare clic sul pulsante **Rollback** nel pannello di destra della finestra principale dell'applicazione.

10.3. Creazione delle attività di aggiornamento

Kaspersky Anti-Virus presenta un'attività incorporata di aggiornamento per aggiornare i moduli di programma e l'elenco dei virus. L'utente può inoltre creare attività di aggiornamento personalizzate con varie impostazioni e pianificarne l'avvio.

Per esempio, Kaspersky Anti-Virus è installato su un laptop che l'utente usa sia a casa che in ufficio. A casa, l'utente aggiorna il programma dai server di aggiornamento di Kaspersky Lab, mentre in ufficio lo aggiorna da una cartella locale che contiene gli aggiornamenti necessari. E' possibile in questo caso utilizzare due attività diverse per evitare di dover modificare le impostazioni di aggiornamento ogni volta che si passa da casa all'ufficio.

Per creare un'attività di aggiornamento avanzata:

1. Selezionare **Aggiornamento** dalla sezione **Servizio** della finestra principale del programma, aprire il menu di scelta rapida facendo clic col pulsante destro del mouse e selezionare **Salva con nome**.
2. Immettere il nome della nuova attività nella finestra che si apre e fare clic su **OK**. Compare un'operazione con quel nome nella sezione **Servizio** della finestra principale del programma.

Attenzione!

Il numero di attività di aggiornamento che l'utente può creare è limitato in Kaspersky Anti-Virus. Numero massimo: due attività.

La nuova attività eredita tutte le proprietà di quella sulla quale è basata, tranne per le impostazioni di pianificazione. L'impostazione di scansione automatica predefinita per la nuova attività è disabilitata. Sarà necessario continuare l'impostazione specificando la sorgente dell'aggiornamento (vedere 10.4.1 a pag. 109), le impostazioni di rete (vedere 10.4.3 a pag. 114), e se necessario abilitare l'attività con privilegi (vedere 6.4 a pag. 65) e configurare una pianificazione (vedere 6.5 a pag. 66).

Per cambiare nome a un'attività:

Selezionare l'attività dalla sezione **Servizio** della finestra principale del programma, aprire il menu di scelta rapida facendo clic sul pulsante destro del mouse e selezionare **Rinomina**.

Immettere il nome della nuova attività finestra che si apre e fare clic su **OK**. Il nome dell'operazione risulta quindi modificato nella sezione **Servizio**.

Per eliminare un'attività:

Selezionare l'attività dalla sezione **Servizio** della finestra principale del programma, aprire il menu di scelta rapida facendo clic sul pulsante destro del mouse e selezionare **Elimina**.

Confermare la decisione di eliminare l'attività nella finestra di conferma. L'operazione risulta quindi eliminata dalla lista di operazioni nella sezione **Servizio**.

Attenzione!

Solo le attività definite dall'utente possono essere rinominate ed eliminate.

10.4. Configurazione delle impostazioni di aggiornamento

Le impostazioni di aggiornamento specificano i seguenti parametri:

- La sorgente da cui l'aggiornamento viene scaricato e installato (vedere 10.4.1 a pag. 109);
- La modalità di esecuzione dell'aggiornamento dell'applicazione e i specifici componenti aggiornati (vedere 10.4.2 a pag. 112);
- Frequenza degli aggiornamento se gli aggiornamento vengono eseguiti puntualmente (vedere 6.5 a pag. 66);
- Account sotto il quale l'aggiornamento verrà eseguito (vedere 6.4 a pag. 65);
- Il requisito di copiare gli aggiornamenti scaricati in una directory locale (vedere 10.4.4 a pag. 116);
- Le azioni da compiere al termine dell'aggiornamento (vedere 10.4.5 a pag. 117).

Le seguenti sezioni esaminano in dettaglio questi aspetti.

10.4.1. Selezione di un'origine per l'aggiornamento

Le *origini degli aggiornamenti* sono le risorse contenenti gli aggiornamenti degli elenchi delle minacce e dei moduli delle applicazioni di Kaspersky Anti-Virus.

È possibile utilizzare quanto segue come origini degli aggiornamenti:

- *Server di amministrazione* – si tratta di una memoria centralizzata per gli aggiornamenti, ubicata presso il Server di amministrazione di Kaspersky Administration Kit (per ulteriori dettagli, vedere la Guida d'uso per gli amministratori di Kaspersky Administration Kit 6,0).
- *Server degli aggiornamenti di Kaspersky Lab* – si tratta di speciali siti web contenenti gli aggiornamenti disponibili per gli elenchi delle minacce ed i moduli delle applicazioni per tutti i prodotti Kaspersky Lab.
- *Server FTP o HTTP o cartelle locali o di rete* – server o cartella locale contenente gli aggiornamenti più recenti.

Se non si riesce ad accedere ai server di aggiornamento di Kaspersky Lab (se per esempio il computer non è connesso a Internet), chiamare l'ufficio centrale di Kaspersky Lab al numero 7 (495) 797-87-00, +7 (495) 645-79-39 o +7 (495) 956-70-00 per richiedere informazioni sui partner di Kaspersky Lab che possono fornire aggiornamenti in formato compresso su dischetti o CD-ROM.

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 la sorgente di aggiornamento dalla scheda **Origine aggiornamento** (vedere Figura 30).

Per impostazione predefinita, gli aggiornamenti vengono scaricati dai server di aggiornamento di Kaspersky Lab. L'elenco di indirizzi bloccati rappresentato da questo elemento non può essere modificato. Durante l'aggiornamento, Kaspersky Anti-Virus for Windows Servers consulta l'elenco, seleziona l'indirizzo del primo server e cerca di scaricare i file da quest'ultimo. Se non è possibile scaricare gli aggiornamenti dal primo server, l'applicazione cerca di connettersi e di recuperare gli aggiornamenti dal server successivo, finché non riesce.

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 il sito FTP o HTTP a cui si desidera connettersi, oppure specificare l'indirizzo IP, o l'URL del sito nel campo **Origine**. Quando si seleziona un sito ftp come sorgente di aggiornamento, è necessario inserire le impostazioni di autenticazione nell'URL del server in formato ftp://<user_name>:<password>@<host>:<port>.

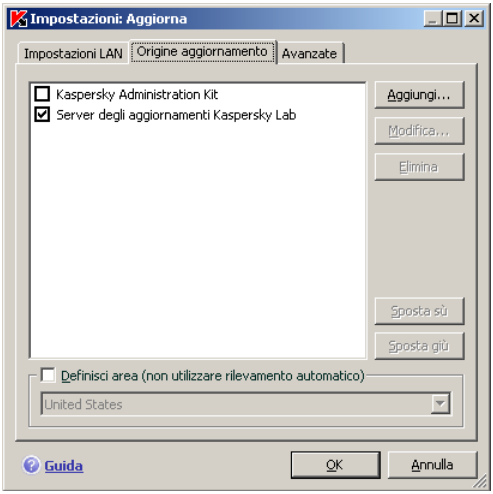


Figura 30. Selezione di una sorgente d'aggiornamento

Attenzione!

Se si seleziona una risorsa esterna alla LAN come sorgente di aggiornamento, è necessario disporre di una connessione Internet per poter aggiornare.

Per scaricare l'aggiornamento da una cartella locale:

1. Fare clic su **Aggiungi.**
2. Nella finestra di dialogo **Seleziona una sorgente di aggiornamento**, selezionare una cartella o specificare il percorso completo di questa cartella nel campo **Origine**.

Kaspersky Anti-Virus for Windows Servers aggiunge nuove sorgenti di aggiornamento in cima alla lista e abilita automaticamente la sorgente come abilitata selezionando la casella accanto al nome della sorgente.

Se sono state selezionate più risorse per l'aggiornamento, 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 sorgenti nell'elenco tramite i pulsanti **Sposta su** e **Sposta giù**.

Per modificare la lista, utilizzare i pulsanti **Aggiungi**, **Modifica** e **Rimuovi**. Non è possibile modificare od eliminare i server di aggiornamento di Kaspersky Lab o Kaspersky Administration Kit.

Se si prelevano gli aggiornamenti dai server di Kaspersky Lab, 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 si seleziona questa casella, gli aggiornamenti verranno eseguiti tenendo conto della regione selezionata nell'elenco. Questa casella di controllo è deselezionata per impostazione predefinita, e vengono utilizzate le informazioni sulla regione corrente tratte dal registro di sistema.

10.4.2. Selezione di un metodo di aggiornamento e degli oggetti da aggiornare

Durante la configurazione delle impostazioni di aggiornamento è importante definire cosa sarà aggiornato e con quale metodo.

Gli oggetti dell'aggiornamento (vedere Figura 31) sono i componenti che verranno aggiornati:

- elenco delle minacce
- moduli del programma

L'elenco delle minacce viene sempre aggiornato, mentre i moduli dell'applicazione vengono aggiornati solo se ciò è previsto nelle impostazioni.

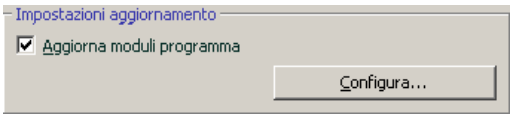


Figura 31. Selezione di un oggetto da aggiornare

Se si desidera scaricare e installare gli aggiornamenti dei moduli del programma:

Selezionare **Aggiorna moduli programma** nella finestra **Impostazioni: Kaspersky Anti-Virus** del servizio **Aggiornamento**.

Se la sorgente di aggiornamento contiene un aggiornamento ad un modulo del programma, l'applicazione scarica gli aggiornamenti richiesti e li applica una volta riavviato il sistema. Gli aggiornamenti scaricati per i moduli saranno installati solo dopo il riavvio del computer.

Se il successivo aggiornamento del programma si verifica prima del riavvio del computer e dell'installazione dei moduli dell'applicazione precedentemente scaricati, verranno aggiornati solo gli elenchi dei virus.

Il Metodo di aggiornamento (vedere Figura 32) definisce le modalità di avvio del programma di aggiornamento. In **Modalità esecuzione** è possibile selezionare una delle seguenti opzioni:

Automaticamente. Kaspersky Anti-Virus verifica ad intervalli specificati la disponibilità di nuovi pacchetti di aggiornamento presso la relativa sorgente (vedere 10.4.1 a pag. 109). Quando Anti-Virus rileva nuovi aggiornamenti, li scarica e li installa sul computer.

Se è specificata una risorsa di rete come origine di aggiornamento, Kaspersky Anti-Virus cerca di avviare il programma di aggiornamento dopo un certo periodo, secondo quanto 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 nel precedente 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 tempestivamente gli aggiornamenti più recenti degli elenchi delle minacce, del database degli attacchi di rete e dei moduli del software, impedendo ai programmi nocivi di penetrare nel server.

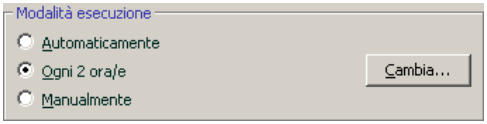


Figura 32. Selezione di una modalità di esecuzione degli aggiornamenti

Come pianificato. L'avvio dell'aggiornamento è pianificato ad una certa ora. Per impostazione predefinita, gli aggiornamenti pianificati hanno cadenza di 2 ore. Per modificare la pianificazione predefinita, fare clic sul pulsante **Cambia...** accanto al nome della modalità e apportare le modifiche necessarie nella finestra che si apre (per ulteriori dettagli, vedere 6.5 a pag. 66). Questa modalità è selezionata per impostazione predefinita.

Manualmente. Questa opzione consente di avviare Updater manualmente. Kaspersky Anti-Virus for Windows Servers notifica quando è necessario un aggiornamento:

- Sopra all'icona dell'applicazione nell'area di notifica compare un messaggio pop-up che informa l'utente che è il momento di effettuare l'aggiornamento (se le notifiche sono abilitate; vedere 11.8.1 a pag. 141)
- Il secondo indicatore nella finestra principale del programma informa che il computer non è aggiornato (vedere 5.1.1 a pag. 44)

- Nella sezione messaggi dell finestra principale del programma viene visualizzata la raccomandazione di aggiornare l'applicazione (vedere 4.3 a pag. 39)

10.4.3. Configurazione delle impostazioni di connessione

Se si imposta il programma in modo da scaricare gli aggiornamenti dai server di Kaspersky Lab o da altri siti FTP o HTTP, si consiglia di controllare prima le impostazioni di connessione.

Tutte le impostazioni sono raggruppate in una scheda particolare – **Impostazioni LAN** (vedere Figura 33).

Selezionare la casella **Usa modalità FTP passiva se possibile** se si scaricano gli aggiornamenti da un server FTP in modalità passiva (per esempio attraverso un firewall). Se si lavora in modalità FTP attiva, deselezionare questa casella.

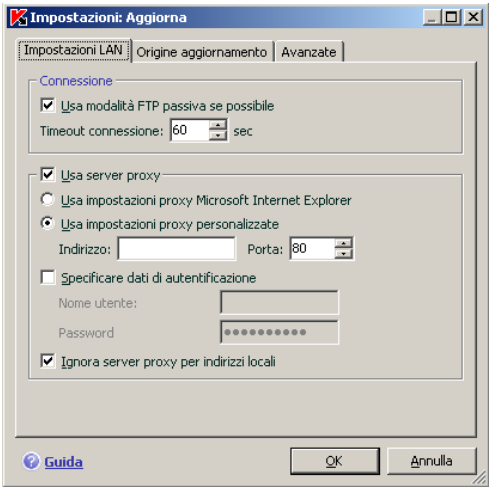


Figura 33. Configurazione delle impostazioni di aggiornamento

Assegnare il tempo allocato per la connessione al server di aggiornamento (in secondi) nel campo **Time-out connessione (sec.)**. Se la connessione non riesce, una volta scaduto questo intervallo il programma tenta la connessione al server di aggiornamento successivo. Ciò continua finché non viene stabilita una connessione valida, o finche non è stata tentata la connessione a tutti i server di aggiornamento.

Selezionare **Usa server proxy** se si accede a Internet attraverso un server proxy e, se necessario, selezionare le seguenti impostazioni:

- Selezionare le impostazioni del server proxy da utilizzare durante l'aggiornamento:

  Usa impostazioni proxy Microsoft Internet Explorer. Se si seleziona questa opzione, le impostazioni del server proxy vengono rilevate automaticamente utilizzando il protocollo WPAD (Web Proxy Auto Discovery Protocol). Se questo protocollo non è in grado di rilevare l'indirizzo, Kaspersky Anti-Virus utilizzerà le impostazioni del server proxy utilizzate in Microsoft Internet Explorer.

  Usa impostazioni proxy personalizzate – per utilizzare un proxy diverso da quello specificato nelle impostazioni di connessione del browser. Nel campo **Indirizzo**, immettere l'indirizzo IP o il nome simbolico del server proxy e specificare il numero di porta proxy nel campo **Porta**.

- Specificare se è richiesta l'autenticazione sul server proxy. L'*autenticazione* è il processo di verifica dei dati di registrazione dell'utente ai fini di controllo dell'accesso.

  Se la connessione al server proxy richiede l'autenticazione, selezionare **Specificare dati di autenticazione** e specificare il nome utente e la password nei campi sotto. In tal caso, verranno tentate prima l'autenticazione NTLM, quindi quella BASIC.

  Se questa casella di controllo non è selezionata o se i dati non vengono immessi, l'autenticazione NLTM verrà tentata utilizzando l'account utente per avviare l'aggiornamento (vedere 6.4 a pag. 65).

  Se il server proxy richiede l'**autenticazione** e non sono stati inseriti nome utente e **password**, oppure i dati inseriti non sono stati accettati dal server proxy per qualsiasi ragione, quando inizia l'aggiornamento verrà visualizzata una finestra che richiede un nome utente ed una password per l'autenticazione. Se l'autenticazione riesce, il nome utente e la password specificati verranno utilizzati per il prossimo aggiornamento dell'applicazione. In caso contrario, verranno nuovamente richiesti i dati di autenticazione.

Per evitare l'uso di un proxy quando l'origine degli aggiornamenti è una cartella locale, selezionare la casella **Ignora server proxy per indirizzi locali**.

10.4.4. Aggiorna mento della cartella di distribuzione

La funzione di copia degli aggiornamento consente di ottimizzare il carico sulla rete aziendale. Gli aggiornamenti vengono copiati in due fasi:

1. Uno dei computer della rete recupera un pacchetto di aggiornamento dell'applicazione e degli elenchi dei virus dai server Web di Kaspersky Lab, oppure da un'altra risorsa di rete che ospita un insieme di aggiornamenti. Gli aggiornamenti 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, selezionare la casella di controllo **Aggiornare cartella di distribuzione** nella scheda **Avanzate** (vedere Figura 34), quindi specificare la cartella condivisa dove verranno salvati gli aggiornamenti nel campo sottostante. È possibile immettere il percorso manualmente o selezionarlo nella finestra che si apre facendo clic su **Sfoglia**. Se la casella di controllo è selezionata, gli aggiornamenti verranno copiati in questa cartella quando vengono recuperati.

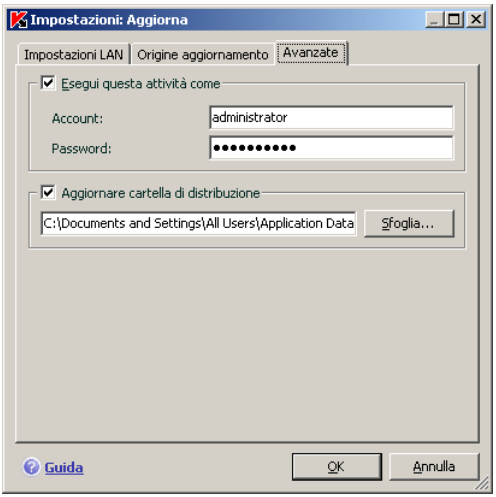


Figura 34. Impostazioni dello strumento di copia degli aggiornamenti

È inoltre possibile specificare il metodo per la funzione Aggiorna distribuzione:

- *completo*, che copia gli aggiornamenti all'elenco dei virus ed ai componenti per tutte le applicazioni Kaspersky Lab 6.0. Per selezionare aggiornamenti completi, selezionare la casella di controllo ☑ **Copia aggiornamenti per tutte le applicazioni**.
- *personalizzato*, che copia gli aggiornamenti all'elenco dei virus ed ai componenti per le sole applicazioni Kaspersky Lab 6,0 installate. Per selezionare questo metodo di aggiornamento, deselezionare la casella di controllo ☑ **Copia aggiornamenti per tutte le applicazioni**.

Se si desidera che altri computer nella rete si aggiornino dalla cartella contenente gli aggiornamenti copiati da Internet, attenersi alla seguente procedura:

1. Consentire l'accesso pubblico alla cartella.
2. Specificare la cartella condivisa quale sorgente degli aggiornamenti per i computer della rete nelle impostazioni di aggiornamento.

10.4.5. Azioni successive all'aggiornamento del programma

Ogni aggiornamento degli elenchi delle minacce contiene nuove voci che proteggono il computer dalle minacce più recenti.

Kaspersky Lab raccomanda di esaminare gli *oggetti in quarantena* e gli *oggetti di avvio* dopo ogni aggiornamento del database.

Perché è necessario esaminare questi oggetti?

L'area di quarantena contiene oggetti che il programma ha catalogato come sospetti o potenzialmente infetti (vedere 11.1 a pag. 120). Utilizzando la versione più recente degli elenchi dei virus, Kaspersky Anti-Virus for Windows Servers può 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 consiglia inoltre di controllare periodicamente gli oggetti in questa cartella in quanto il loro stato può cambiare dopo varie scansioni. Alcuni oggetti possono quindi essere ripristinati nelle loro posizioni originarie per continuare ad utilizzarli.

Per disabilitare la scansione degli oggetti in quarantena, deselezionare la casella ☑ **Ripeti scansione quarantena** nella sezione **Azione post-aggiornamento**.

Gli oggetti di 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 (vedere Capitolo 8 a pag. 85). Si raccomanda di pianificare un calendario di esecuzione per questa attività in modo da avviarlo automaticamente ad ogni aggiornamento degli elenchi delle minacce (vedere 6.5 a pag. 66).

CAPITOLO 11. OPZIONI AVANZATE

Kaspersky Anti-Virus for Windows Servers 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 for Windows Servers (vedere 11.2 a pag. 124). 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 (vedere 11.1 a pag. 120).

Si raccomanda di esaminare periodicamente l'elenco di oggetti archiviati. Alcuni di essi infatti possono essere già obsoleti e altri possono essere stati ripristinati.

Le opzioni avanzate comprendono diverse utili funzioni. Per esempio:

- Il servizio di supporto tecnico offre un'assistenza completa per Kaspersky Anti-Virus for Windows Servers (vedere 11.6 a pag. 137). Kaspersky offre diversi canali di supporto, tra cui il supporto on-line ed un forum di domande e risposte per gli utenti del programma.
- La funzione di Notifica serve per configurare le notifiche agli utenti relative a eventi chiave di Kaspersky Anti-Virus for Windows Servers (vedere 11.8.1 a pag. 141). Può trattarsi di eventi di natura informativa, o di errori critici che devono essere risolti immediatamente.
- 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 limita i diritti dell'amministratore del server sul computer in uso in relazione all'esecuzione di certe azioni in Kaspersky Anti-Virus for Windows Servers (vedere 11.8.2 a pag. 145). Per esempio, la modifica del livello di protezione può influire considerevolmente sulla sicurezza del computer.
- La Gestione chiavi di licenza è in grado di ottenere informazioni dettagliate sulla licenza utilizzata, attivare la copia del programma, e gestire i file delle chiavi di licenza (vedere 11.5 a pag. 135).

Il programma offre anche una sezione di Guida (vedere 11.4 a pag. 134) e rapporti dettagliati (vedere 11.3 a pag. 126) sul funzionamento di File Anti-Virus e le attività di scansione antivirus ed aggiornamento.

È possibile inoltre modificare l'aspetto di Kaspersky Anti-Virus for Windows Servers e personalizzare l'interfaccia del programma (vedere 11.7 a pag. 138).

Le seguenti sezioni esaminano in dettaglio queste funzioni.

11.1. 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 di cui si sospetta l'infezione da virus o virus modificati.

Perché *potenzialmente infetti*? Ci sono diverse ragioni per cui non sempre è possibile stabilire con certezza se un oggetto sia infetto oppure no.

- Il codice dell'oggetto esaminato somiglia a una minaccia nota ma appare parzialmente modificato.

  Gli elenchi delle minacce contengono minacce già studiate da Kaspersky Lab. Se un programma nocivo è stato modificato da un pirata informatico ma le variazioni non sono ancora state registrate negli elenchi delle minacce, Kaspersky Anti-Virus for Windows Servers classifica l'oggetto infettato con il programma nocivo modificato come potenzialmente infetto e indica la minaccia a cui il codice somiglia.

- Il codice dell'oggetto rilevato ricorda, nella struttura, un programma nocivo, nonostante l'elenco dei virus non contenga niente di simile.

  È possibile che si tratti di un nuovo tipo di minaccia, perciò Kaspersky Anti-Virus for Windows Servers classifica l'oggetto come potenzialmente infetto.

L'analizzatore a *codice è euristico* rileva i possibili virus. Si tratta di un meccanismo piuttosto efficace che raramente produce falsi positivi.

Un oggetto potenzialmente infetto può essere rilevato e messo in quarantena da File Anti-Virus, oppure durante una scansione antivirus.

Per mettere un oggetto in quarantena è sufficiente fare clic sul pulsante **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 eliminato dal disco o dall'e-mail e salvato nella cartella di Quarantena. I file in Quarantena vengono salvati in uno speciale formato e pertanto non sono pericolosi.

11.1.1. Azioni da eseguire sugli oggetti in Quarantena

Il numero totale degli oggetti messi in quarantena è visualizzato in **File di dati** nell'area **Servizio** della finestra principale dell'applicazione. Nella parte destra della schermata la sezione *Quarantena* visualizza:

- il numero di oggetti potenzialmente infetti rilevati durante il funzionamento di Kaspersky Anti-Virus for Windows Servers;
- le dimensioni correnti della cartella Quarantena.

Qui è possibile eliminare tutti gli oggetti nella cartella di Quarantena con il pulsante **Cancella**. Osservare che così facendo si eliminano anche i file presenti nella cartella Backup e i rapporti.

Per accedere agli oggetti in Quarantena:

fare clic in qualsiasi punto della sezione **Quarantena**.

La scheda **Quarantena** consente di eseguire le seguenti azioni (vedere Figura 35):

- Trasferire in Quarantena un file sospettato di contenere un'infezione che il programma non ha rilevato A tal fine, fare clic sul pulsante **Aggiungi** e scegliere il file nella finestra standard di selezione. Il file viene aggiunto all'elenco con lo status *aggiunto dall'utente*.
- Esaminare e disinfettare tutti gli oggetti potenzialmente infetti in Quarantena per mezzo di elenchi delle minacce correnti facendo clic su **Scansione completa**.

  Dopo la scansione e l'eventuale riparazione di oggetti in Quarantena, lo status può diventare *infetto, probabilmente infetto, falso positivo, OK,* ecc.

  Lo stato *infetto* significa che l'oggetto è stato identificato come infetto ma non è stato possibile trattarlo. Si consiglia di eliminare tali oggetti.

  Tutti gli oggetti classificati come *falso positivo* possono essere ripristinati poiché il precedente status di *probabilmente infetto* non è stato confermato dal programma in seguito alla nuova scansione.

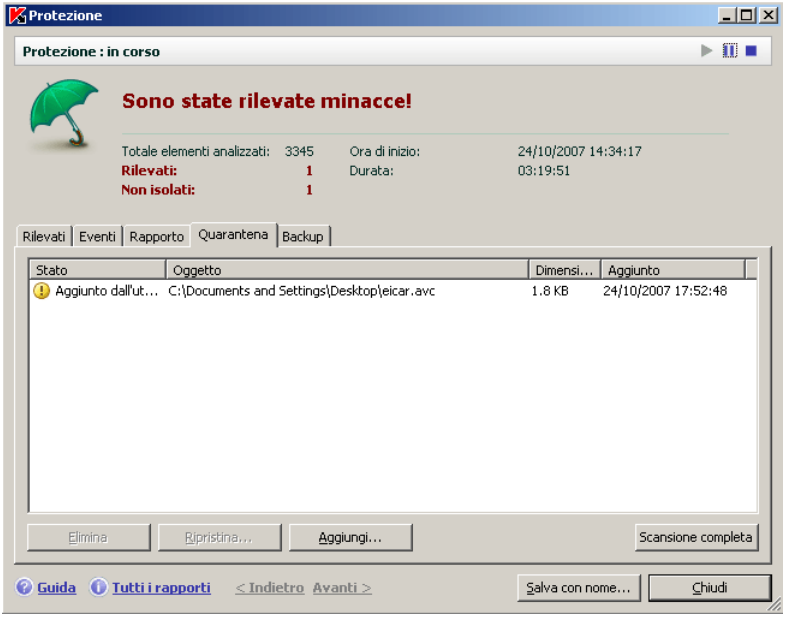


Figura 35. Elenco degli oggetti in quarantena

- Ripristinare i file in una cartella selezionata o nella cartella originale (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.

  Suggerimento:

  Si consiglia di ripristinare solo gli oggetti classificati con lo stato di *falso positivo, OK*, e *disinfettato* poiché il ripristino di altri oggetti può provocare l'infezione del computer.

- Eliminare oggetti o gruppi selezionati di oggetti in Quarantena. Eliminare solo gli oggetti che non possono essere riparati. Per eliminare gli oggetti, selezionarli nella lista e fare clic su **Elimina**.

11.1.2. 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, vedere 10.4.4 a pag. 116).

  > Attenzione!
  >
  > Il programma non è in grado di esaminare gli oggetti messi in quarantena subito dopo l'aggiornamento degli elenchi delle minacce se la quarantena è in uso.

- 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 ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Servers facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
3. Nella sezione **Cartella di Quarantena e Backup** (vedere Figura 36), digitare il tempo massimo allo scadere del quale gli oggetti in quarantena saranno automaticamente eliminati. In alternativa, deselezionare la casella di controllo per disabilitare la cancellazione automatica.

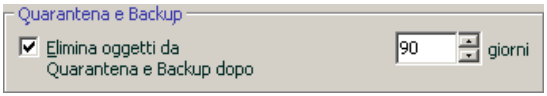


Figura 36. Configurazione del periodo di conservazione degli oggetti in Quarantena

11.2. 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 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.

Backup è un'area di memoria speciale contenente copie di backup degli oggetti pericolosi trattati o eliminati. I file in backup vengono salvati in uno speciale formato e pertanto non sono pericolosi.

11.2.1. Azioni da eseguire sulle copie di backup

Il numero totale delle copie di backup è visualizzato nei **File dati** nell'area **Servizio** della finestra principale dell'applicazione. Nella parte destra della schermata la sezione *Backup* visualizza:

- Il numero di copie di backup degli oggetti create da Kaspersky Anti-Virus for Windows Servers.
- Le dimensioni correnti della cartella di Backup.

Qui è possibile eliminare tutti gli oggetti nella cartella di backup con il pulsante **Cancella**. Osservare che così facendo si eliminano anche i file presenti nella cartella Quarantena e i rapporti.

Per accedere alle copie di oggetti pericolosi:

fare clic con il pulsante sinistro del mouse in qualsiasi punto della sezione **Backup**.

Nella scheda **Backup** viene visualizzato un elenco delle copie di backup (vedere Figura 37). Per ogni copia sono fornite le seguenti informazioni: il nome ed il percorso dell'oggetto lo stato dell'oggetto assegnato dalla scansione e le sue dimensioni.

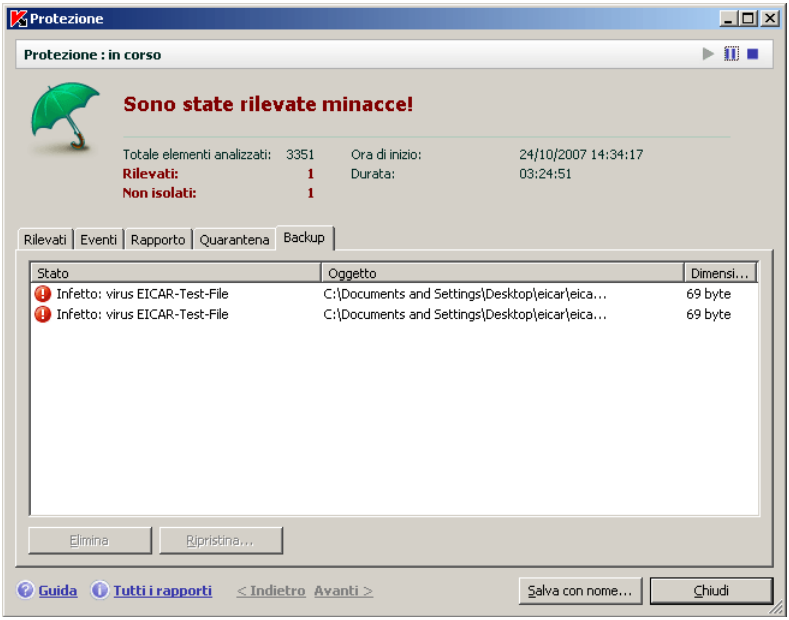


Figura 37. Copie di backup di oggetti eliminati o riparati

Le copie selezionate possono essere ripristinate tramite il 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 disinfezione è stata creata una copia dell'oggetto che si desidera ripristinare), viene visualizzato un apposito messaggio. È possibile cambiare posizione all'oggetto ripristinato oppure rinominarlo.

Si consiglia di effettuare la scansione anti-virus dell'oggetto di backup immediatamente dopo averlo ripristinato. È possibile che gli elenchi aggiornati delle minacce consentano di disinfettarlo senza perdere l'integrità del file.

Si consiglia di **non** ripristinare le copie di backup degli oggetti se non strettamente necessario. Ciò potrebbe provocare l'infezione del computer.

Si consiglia di esaminare periodicamente l'area di backup e di svuotarla tramite il pulsante **Elimina**. È possibile inoltre configurare il programma in modo da eliminare automaticamente dal Backup le copie di più vecchia data (vedere 11.2.2 a pag. 126).

11.2.2. Configurazione delle impostazioni del Backup

È possibile definire il periodo massimo di conservazione delle copie nell'area di backup.

La durata predefinita è di 90 giorni, allo scadere dei quali le copie di backup vengono eliminate. È possibile inoltre modificare la durata di conservazione o disabilitare del tutto questa limitazione procedendo come segue: Per fare ciò:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Servers facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
3. Impostare la durata della conservazione delle copie di backup nella sezione **Quarantena e Backup** (vedere Figura 36) nella parte destra della finestra. In alternativa, deselezionare la casella di controllo per disabilitare la cancellazione automatica.

11.3. Rapporti

Le attività di File Anti-Virus, le scansioni antivirus e le attività di aggiornamento sono tutte registrate in appositi rapporti.

Il numero totale dei rapporti creati dal programma e le loro dimensioni totali sono visualizzati facendo clic su **File dati** nella sezione **Servizio** della finestra principale del programma. Queste informazioni sono indicate nel riquadro *Rapporto*.

Per visualizzare i rapporti:

Fare clic ovunque nel riquadro *Rapporto* per aprire la finestra Protezione, che riassume la protezione offerta dall'applicazione. Si apre una finestra contenente, tra le altre, la scheda **Rapporto** (vedere Figura 38).

La scheda Rapporto elenca gli ultimi rapporti su File Anti-Virus e le attività di scansione anti-virus ed aggiornamento eseguite durante la sessione corrente di Kaspersky Anti-Virus for Windows Servers. Lo stato viene elencato accanto a File Anti-Virus o all'attività, ad esempio *fermato* o *completato*. Per vedere la cronologia completa della creazione dei rapporti per la sessione corrente del programma, selezionare ☑ **Mostra cronologia rapporto**.

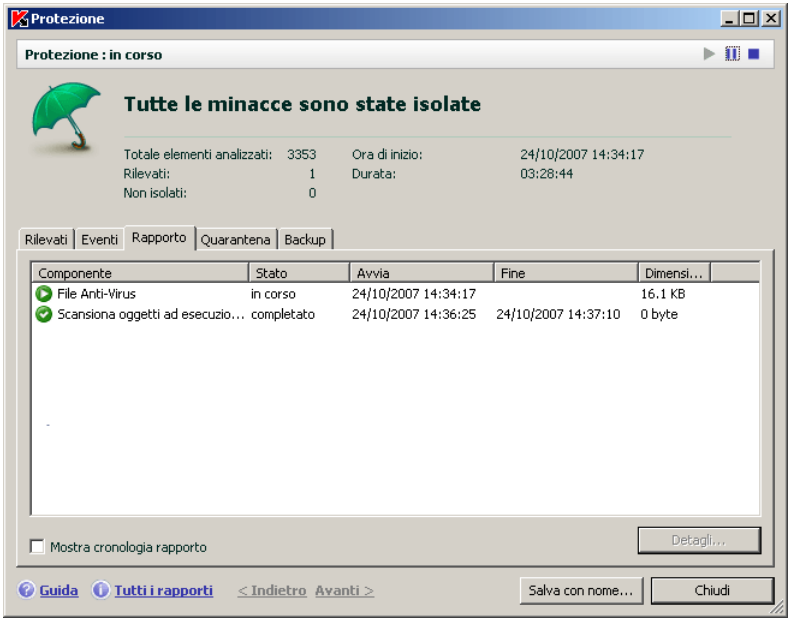


Figura 38. Rapporto sul funzionamento dei componenti

Per consultare tutti gli eventi registrati nel rapporto di File Anti-Virus o dell'attività:

Selezionare File Anti-Virus o l'attività nella scheda **Rapporto** e fare clic sul pulsante **Dettagli**.

Si apre una finestra contenente informazioni dettagliate sulle prestazioni di File Anti-Virus o dell'attività. Le statistiche sulle prestazioni sono visualizzate nella parte superiore della finestra, mentre le informazioni dettagliate sono riportate nelle schede.

- La scheda **Rilevati** contiene un elenco di oggetti pericolosi individuati da File Anti-Virus o un'attività di scansione antivirus eseguita.
- La scheda **Eventi** visualizza gli eventi relativi a File Anti-Virus o all'attività.
- La scheda **Statistiche** contiene statistiche dettagliate per tutti gli oggetti esaminati.
- La scheda **Impostazioni** visualizza una serie di impostazioni utilizzate da File Anti-Virus, dalle scansioni anti-virus o dagli aggiornamenti all'elenco dei virus.

- La scheda **Utenti bloccati** visualizza un elenco di utenti i cui computer sono stati temporaneamente banditi durante un tentativo di copiare un file infetto o potenzialmente tale sul server.

I rapporti possono essere interamente esportati in formato testo. Questa funzione è utile quando si è verificato un errore impossibile da eliminare autonomamente in File Anti-Virus, per il quale si necessita di assistenza tecnica. In tali casi è necessario inviare il rapporto 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 rapporto in formato testo:

fare clic su **Salva con nome** e specificare dove si intende salvare il file del rapporto.

Una volta completate le operazioni sul rapporto, 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 di scelta rapida con alcune di queste voci 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. Se la riparazione non va a buon fine, è possibile lasciare l'oggetto nell'elenco per esaminarlo in seguito con gli elenchi delle minacce aggiornati oppure eliminarlo. È possibile applicare questa azione ad un singolo oggetto dell'elenco oppure a diversi oggetti selezionati.

Elimina – elimina la voce relativa all'oggetto rilevato dal rapporto.

Aggiungi a zona attendibile – esclude l'oggetto 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 Windows Explorer.

Disinfetta tutti – tutti gli oggetti presenti nell'elenco vengono disinfettati. Kaspersky Anti-Virus for Windows Servers tenta di elaborare gli oggetti utilizzando l'elenco dei virus.

Elimina tutti – il rapporto sugli oggetti rilevati viene azzerato. Con questa funzione, tutti gli oggetti pericolosi rilevati restano nel computer.

Cerca www.viruslist.com – viene visualizzata una descrizione dell'oggetto nella Virus Encyclopedia sul sito web di Kaspersky Lab.

Cerca www.google.com – trova informazioni sull'oggetto utilizzando questo motore di ricerca.

Cerca – immettere i termini di ricerca per gli oggetti nella lista secondo il nome o lo stato.

Inoltre è possibile organizzare le informazioni visualizzate nella finestra in ordine crescente o decrescente per ciascuna colonna, facendo clic sull'intestazione della stessa.

Gli oggetti pericolosi rilevati da Kaspersky Anti-Virus vengono elaborati tramite il pulsante **Disinfetta** (per un oggetto o un gruppo di oggetti selezionati) o **Disinfetta tutti** (per trattare tutti gli oggetti nell'elenco). Una volta elaborato ciascun oggetto, viene visualizzata una notifica sullo schermo, che richiede di decidere le azioni successive.

Se si seleziona **Applica a tutti** nella finestra di notifica, l'azione selezionata verrà applicata a tutti gli oggetti nello stato selezionato dall'elenco prima del trattamento.

11.3.1. Configurazione delle impostazioni dei rapporti

Per configurare le impostazioni per la creazione e il salvataggio dei rapporti:

Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Servers facendo clic su Impostazioni nella finestra principale del programma.

1. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
2. Modificare le impostazioni del riquadro **Rapporto** (vedere Figura 39) 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 rapporto solo gli eventi verificatisi successivamente all'ultima esecuzione dell'attività. Questa impostazione consente di salvare spazio su disco riducendo le dimensioni del rapporto. Se è selezionata l'opzione **Mantieni solo eventi recenti**, le informazioni nel rapporto vengono aggiornate ogni volta che si riavvia l'attività. Tuttavia saranno sovrascritte solo le informazioni non critiche.
   - Impostare la durata della conservazione dei rapporti. La durata predefinita è di 90 giorni, allo scadere dei quali i rapporti vengono eliminati. È possibile modificare la durata massima di conservazione o disabilitare del tutto questa limitazione.

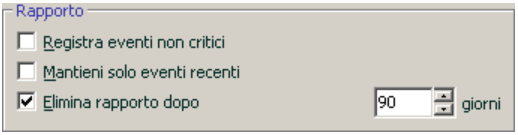


Figura 39. Configurazione delle impostazioni del rapporto

11.3.2. La scheda *Rilevati*

Questa scheda (vedere Figura 40) contiene un elenco di oggetti pericolosi rilevati da Kaspersky Anti-Virus for Windows Servers. Per ogni oggetto è indicato il nome ed il percorso completi, accompagnato dallo stato assegnato ad esso 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 isolati**.

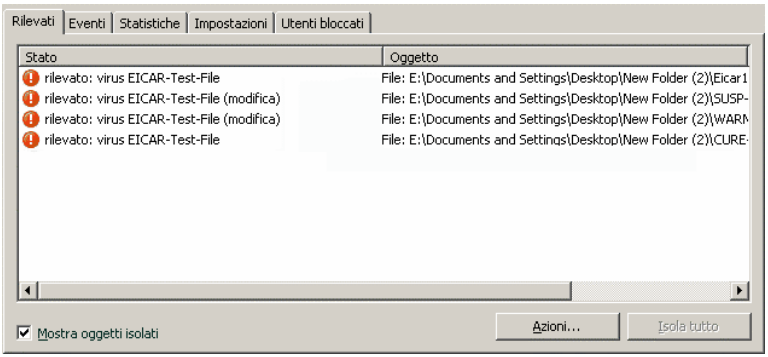


Figura 40. Elenco degli oggetti pericolosi rilevati

Gli oggetti pericolosi rilevati da Kaspersky Anti-Virus vengono elaborati tramite il pulsante **Isola** (per un oggetto o un gruppo di oggetti selezionati) o **Isola tutto** (per trattare tutti gli oggetti nell'elenco). Una volta elaborato ciascun oggetto, viene visualizzata una notifica sullo schermo, che richiede di decidere le azioni successive.

Se si seleziona **Applica a tutti** nella finestra di notifica, l'azione selezionata verrà applicata a tutti gli oggetti nello stato selezionato dall'elenco prima del trattamento.

11.3.3. La scheda *Eventi*

Questa scheda (vedere Figura 41) visualizza un elenco completo di tutti gli eventi importanti verificatisi durante il funzionamento di File Anti-Virus, le scansione anti-virus e gli aggiornamenti all'elenco dei virus.

Questi eventi possono essere:

Gli **Eventi critici** sono eventi di importanza critica che segnalano problemi di funzionamento del programma o vulnerabilità del computer. Per esempio *rilevato virus*, *errore di funzionamento*.

Gli **Eventi importanti** sono eventi da approfondire poiché riflettono situazioni importanti nel funzionamento del programma. Per esempio,*arrestato*

I **Messaggi informativi** sono messaggi di riferimento che di solito non contengono informazioni rilevanti. Per esempio *OK, non elaborato*. Questi eventi sono riportati nel registro eventi se è selezionata l'opzione **Mostra tutti gli eventi**.

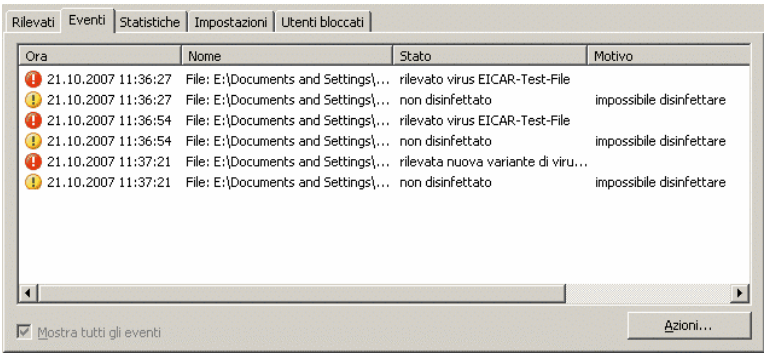


Figura 41. Eventi elaborati dal componente

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 status assegnatogli in seguito alla scansione/elaborazione.

11.3.4. La scheda Statistiche

Questa scheda (vedere Figura 42) contiene le statistiche dettagliate su File Anti-Virus e le attività di scansione antivirus. Da questa finestra risulta:

- Quanti oggetti sono stati esaminati in cerca di caratteristiche pericolose nella sessione corrente di File Anti-Virus, 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 disinfettati, eliminati o trasferiti in Quarantena.

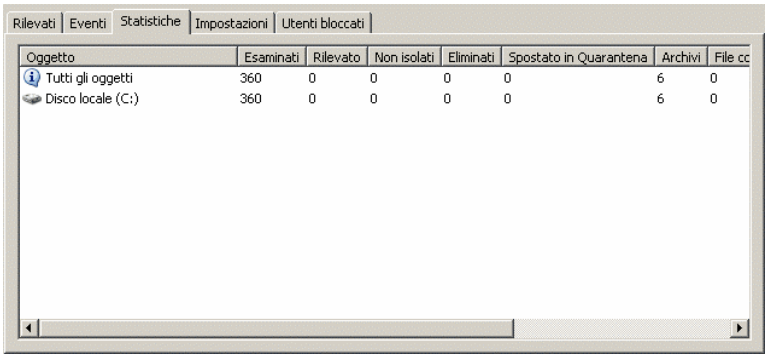


Figura 42. Statistiche dei componenti

11.3.5. La scheda Impostazioni

La scheda **Impostazioni** (vedere Figura 43) visualizza l'elenco completo delle impostazioni di File Anti-Virus, delle scansioni antivirus e degli aggiornamenti del programma. È possibile vedere il livello di protezione di File Anti-Virus o di una scansione antivirus, le azioni compiute sugli oggetti pericolosi o le impostazioni in uso per gli aggiornamenti del programma. Utilizzare il collegamento 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. La casella ☑ **Concedi risorse ad altre applicazioni** è selezionata per impostazione predefinita. Con questa funzione, il

programma individua il carico sul processore e sui sottosistemi 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 aumenta la durata della scansione ma si liberano risorse per le applicazioni dell'utente.

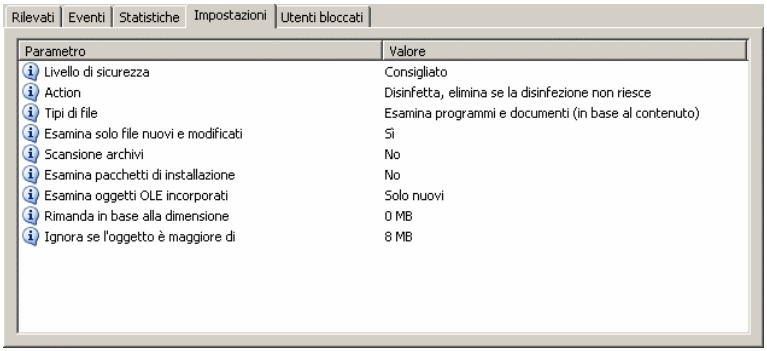


Figura 43. Impostazioni dei componenti

- Impostare la modalità operativa del computer per il periodo successivo al completamento della scansione antivirus. È possibile impostare il computer in modo che si spenga, si riavvii, o entri in modalità standby o basso consumo. Per selezionare un'opzione, fare clic con il pulsante sinistro del mouse sul collegamento fino a visualizzare l'opzione desiderata.

11.3.6. La scheda *Utenti bloccati*

Ciascun computer che abbia tentato di copiare un file infetto o potenzialmente infetto sul server viene bloccato (vedere Figura 44). Tale azione può inoltre essere applicata alle azioni relative all'elaborazione del file (disinfezione o eliminazione).

Questa scheda mostra i computer che sono stati banditi, unitamente alla data ed all'ora in cui ciò si è verificato, e quante ore restano fino all'eliminazione del blocco.

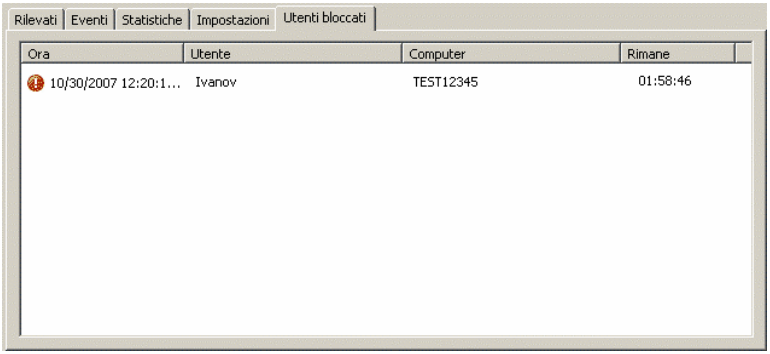


Figura 44. Elenco di utenti bloccati

11.4. Informazioni generali sul programma

Le informazioni generali sul programma sono riportate nella sezione **Servizio** della finestra principale (vedere Figura 45).

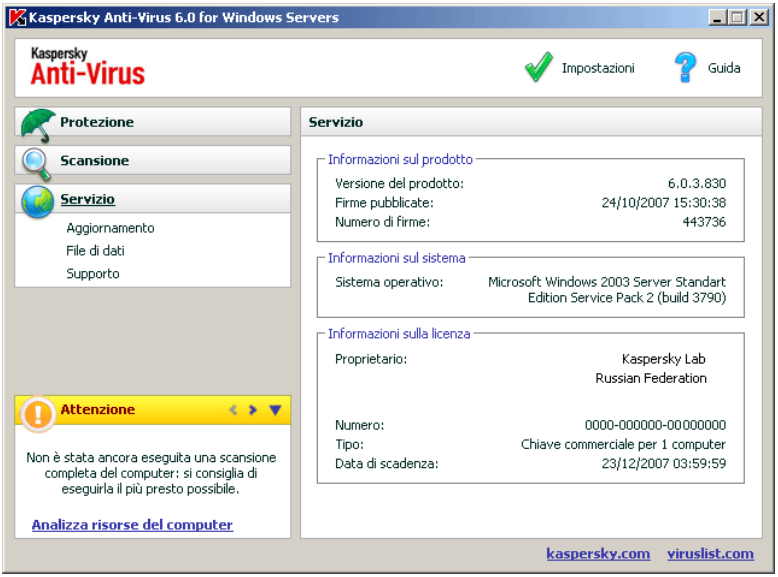


Figura 45. Informazioni sul programma, la licenza ed il sistema sul quale è installato.

Tutte le informazioni sono suddivise in tre sezioni:

- La versione del programma, la data dell'ultimo aggiornamento e il numero delle minacce note fino ad ora sono visualizzati nel riquadro **Informazioni sul prodotto**.
- Le informazioni di base sul funzionamento del sistema installato sul computer sono illustrate nella casella **Informazioni sul sistema**.
- Le informazioni basilari sulla licenza acquistata per Kaspersky Anti-Virus sono contenute nel riquadro **Informazioni sulla licenza**.

Tutte queste informazioni sono necessarie qualora ci si rivolga al servizio di assistenza tecnica di Kaspersky Lab (vedere 11.6 a pag. 137).

11.5. Gestione delle licenze

Per funzionare, Kaspersky Anti-Virus for Windows Server richiede una *chiave di licenza*. All'acquisto del programma viene fornita una chiave di licenza. Essa conferisce all'utente il diritto di utilizzare il programma dal giorno in cui si installa la chiave.

Senza chiave di licenza, Kaspersky Anti-Virus eseguirà l'aggiornamento una sola volta, a meno che non sia stata attivata una licenza di prova. Il programma non scaricherà nuovi aggiornamenti.

Se è stata attivata una versione di prova del programma, una volta scaduto il periodo di prova Kaspersky Anti-Virus non funziona.

Alla scadenza della chiave di licenza commerciale, il programma continua a funzionare ma non è in grado di aggiornare gli elenchi delle minacce. Come in precedenza, è possibile continuare a esaminare il computer e a usare i componenti di protezione, ma utilizzando solo gli elenchi delle minacce installati al momento della scadenza della chiave. Pertanto non è possibile garantire la protezione del computer dai virus diffusi successivamente alla scadenza della licenza d'uso del programma.

Per evitare di infettare il computer con nuovi virus, si consiglia di estendere la licenza di Kaspersky Anti-Virus for Windows Servers. Due settimane prima della scadenza della licenza, il programma visualizza un apposito messaggio e continuerà a visualizzarlo per due settimane ogni volta che lo si avvia.

Per rinnovare la licenza è necessario acquistare e installare una nuova chiave di licenza o inserire un nuovo codice di attivazione per l'applicazione. Per fare ciò:

Contattare il rivenditore del programma ed acquistare una chiave di licenza o un codice di attivazione per l'applicazione.

oppure:

Ottenere una chiave di licenza o un codice di attivazione direttamente da Kaspersky Lab facendo clic sul collegamento Acquista licenza nella finestra delle chiavi di licenza (vedere Figura 46). Compilare quindi il modulo sul nostro sito web. Dopo il pagamento, verrà inviato all'indirizzo di posta elettronica specificato nel modulo d'ordine un collegamento. Esso consentirà di scaricare una chiave di licenza o di ottenere un codice di attivazione per l'applicazione.

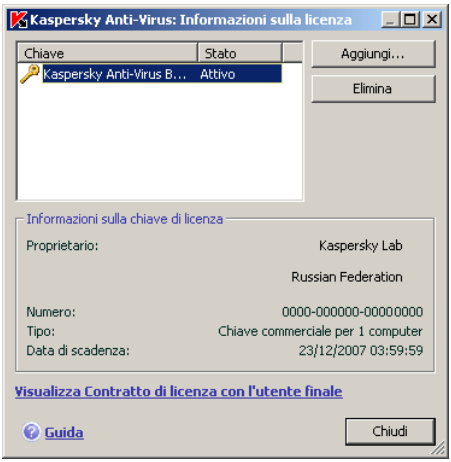


Figura 46. Informazioni sulla licenza

Kaspersky Lab offre regolarmente speciali tariffe per il rinnovo delle licenze sui nostri prodotti. Cercare le offerte speciali sul sito web Kaspersky Lab nell'area **Products→ Sales and special offers**.

Le informazioni sulla chiave di licenza utilizzata sono disponibili nel riquadro **Informazioni sulla licenza** nella sezione **Servizio** della finestra principale del programma. Per aprire la finestra di gestione delle licenze, fare clic ovunque nel riquadro. La finestra che si apre (vedere Figura 46) consente di visualizzare le informazioni sulla chiave di licenza corrente, nonché di aggiungerne una nuova o di eliminarla.

Quando si seleziona una chiave dall'elenco in **Informazioni sulla licenza**, verranno visualizzate informazioni sul numero di licenza, il tipo e la data di scadenza. Per aggiungere una nuova chiave di licenza, fare clic su **Aggiungi** ed attivare l'applicazione tramite la procedura guidata di attivazione (vedere 11.5 a pag. (vedere 11.6 a pag. 137)). Per eliminare una chiave dall'elenco, fare clic sul pulsante **Elimina**.

Per rivedere le disposizioni dell'accordo di licenza, fare clic su Visualizza Contratto di licenza con l'utente finale. Per acquistare una licenza tramite il modulo on-line del sito Web di Kaspersky Lab, fare clic su Acquista licenza.

11.6. Supporto tecnico

Kaspersky Anti-Virus for Windows Servers offre una vasta gamma di opzioni per porgere domande e risolvere problemi relativi al funzionamento del programma. Queste risposte sono fornite sotto **Supporto** (vedere Figura 47) nella sezione **Servizio**.

A seconda del problema riscontrato, siamo in grado di offrire diversi servizi di assistenza tecnica:

Forum utenti. A questa risorsa è dedicata un'apposita sezione del sito web Kaspersky Lab con domande, commenti e suggerimenti da parte degli utenti del programma. È possibile consultare i principali argomenti del forum ed eventualmente lasciare un commento. Il sito potrebbe contenere anche la soluzione del problema dell'utente.

Per accedere a questa risorsa, utilizzare il collegamento Forum utenti.

Knowledge Base . Anche a questa risorsa è dedicata una sezione apposita del sito web Kaspersky Lab; essa contiene i consigli dei tecnici dell'assistenza sull'uso del software Kaspersky Lab e le risposte alle domande più comuni. È una valida risorsa per trovare la risposta a una domanda o la soluzione a un problema.

Per avvalersi dell'assistenza tecnica online, fare clic sul collegamento Domande frequenti (FAQ).

Commenti sul funzionamento del programma. Questo servizio è concepito per l'invio di commenti o la descrizione di problemi presentatisi durante l'uso del programma. Per avvalersi di questo servizio è necessario compilare un apposito modulo sul sito web dell'azienda e descrivere in dettaglio la situazione. Per affrontare il problema in maniera efficiente, Kaspersky Lab necessita di alcune informazioni sul sistema. A tal fine è possibile descrivere la configurazione del sistema o usare l'applicazione studiata appositamente per raccogliere automaticamente le informazioni richieste.

Per andare al modulo dei commenti, utilizzare il collegamento Inviare un rapporto sugli errori o un suggerimento.

Assistenza tecnica. Se si necessita di assistenza tecnica durante l'utilizzo di Kaspersky Anti-Virus, fare clic sul collegamento ubicato nel riquadro

Servizio di assistenza locale. Si aprirà il sito Web di Kaspersky Anti-Virus con informazioni su come contattare i nostri esperti.

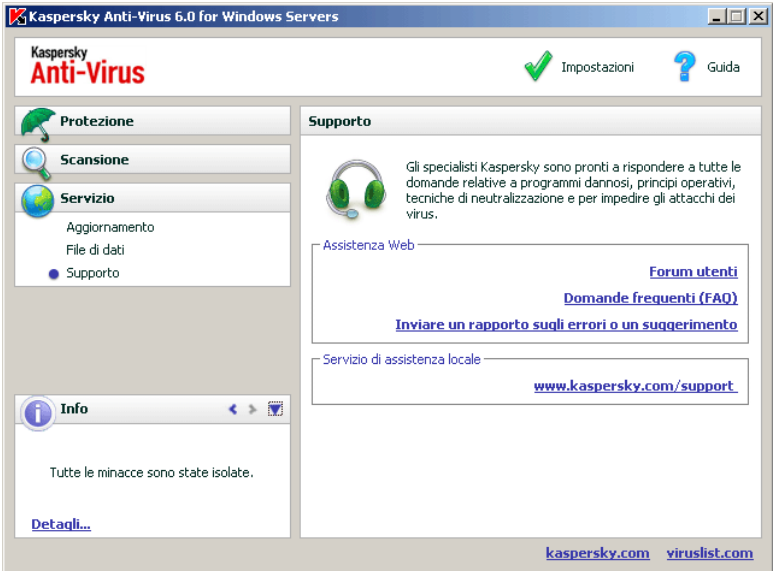


Figura 47. Informazioni sul servizio di assistenza tecnica

11.7. Configurazione dell'interfaccia di Kaspersky Anti-Virus for Windows Servers

Kaspersky Anti-Virus for Windows Servers 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 pop-up.

Per configurare l'interfaccia del programma procedere come segue:

1. Aprire la finestra delle impostazioni di Kaspersky Anti-Virus for Windows Servers facendo clic sul collegamento Impostazioni nella finestra principale.
2. Selezionare **Aspetto** nella sezione **Servizio** della struttura ad albero delle impostazioni del programma (vedere Figura 48).

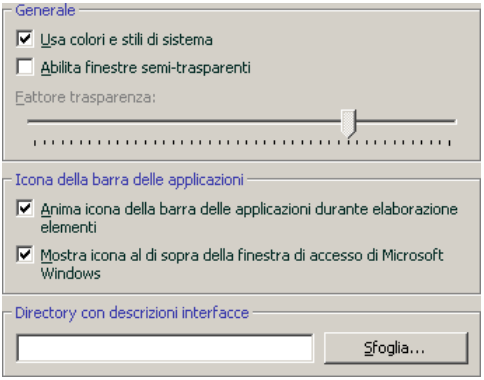


Figura 48. Configurazione dell'aspetto dell'interfaccia del programma

Nella parte destra della finestra delle impostazioni, è possibile determinare i seguenti elementi.

- Se visualizzare l'indicatore di protezione di Kaspersky Anti-Virus for Windows Servers all'avvio del sistema operativo.

  Per impostazione predefinita, questo indicatore è visualizzato nell'angolo superiore destro dello schermo al caricamento del programma. Esso informa che il computer è protetto da tutti i tipi di minaccia. Per non visualizzare l'indicatore di protezione, deselezionare ☑ **Mostra icona al di sopra della finestra di accesso di Microsoft Windows**.

- Se abilitare l'animazione nell'icona dell'area di notifica.

  A seconda dell'operazione eseguita dal programma, l'icona dell'area di notifica cambia. L'animazione dell'icona è abilitata per impostazione predefinita. Per disabilitare l'animazione, deselezionare ☑ **Anima icona della barra delle applicazioni durante elaborazione elementi**. 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 sospesa o disabilitata l'icona diventa grigia.

- Grado di trasparenza dei messaggi a comparsa.

  Tutte le operazioni di Kaspersky Anti-Virus for Windows Servers che richiedono una decisione dell'utente o il suo intervento immediato sono comunicate in un messaggio a comparsa sopra l'icona dell'area di notifica. Le finestre del messaggio sono trasparenti in modo da non interferire con altre operazioni. Se si muove il cursore sul messaggio, la trasparenza svanisce. Il grado di trasparenza di questi messaggi può essere modificato A tal fine, regolare il **Fattore di trasparenza** sul livello

desiderato. Per eliminare la trasparenza dei messaggi, deselezionare **Abilita finestre semi-trasparenti**.

- Applicare stili personalizzati all'interfaccia del programma.

  Tutti i colori, i font, le icone e i testi utilizzati nell'interfaccia di Kaspersky Anti-Virus for Windows Servers possono essere modificati. È possibile creare elementi grafici personalizzati per il programma o tradurli in un'altra lingua. Per utilizzare uno stile di visualizzazione delle pagine, specificare la directory con le relative impostazioni nel campo **Directory con descrizione degli stili**. Selezionare la directory con il pulsante **Sfoglia**.

  Per impostazione predefinita, lo stile del programma applica i colori e gli stili del sistema. È possibile rimuoverli deselezionando **Usa colori e stili di sistema**. Saranno quindi applicati gli stili specificati nelle impostazioni del tema dello schermo.

SI noti che le modifiche alle impostazioni dell'interfaccia di Kaspersky Anti-Virus non vengono salvate se si ripristinano le impostazioni predefinite o se si disinstalla il programma.

11.8. Uso delle opzioni avanzate

Kaspersky Anti-Virus for Windows Servers offre le seguenti funzioni avanzate:

- Notifiche di determinati eventi che si verificano nel programma.
- Autodifesa di Kaspersky Anti-Virus for Windows Servers dalla disattivazione, eliminazione o modifica dei moduli, nonché protezione del programma tramite password.
- Risoluzione dei conflitti tra Kaspersky Anti-Virus e altri programmi.

Per configurare queste funzioni:

1. Aprire la finestra delle impostazioni del programma con il collegamento Impostazioni nella finestra principale.
2. Selezionare **Servizio** dalla struttura ad albero delle impostazioni.

Nella parte destra dello schermo è possibile specificare se abilitare le funzioni supplementari durante l'uso del programma.

11.8.1. Notifica eventi di Kaspersky Anti-Virus for Windows Servers

Durante l'uso di Kaspersky Anti-Virus for Windows Servers si verificano diversi tipi di eventi. 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 da risolvere immediatamente.

Per ricevere gli aggiornamenti sul funzionamento di Kaspersky for Windows Servers è possibile utilizzare la funzione di notifica.

Le notifiche possono essere trasmesse in vari modi:

- In forma di messaggi a comparsa sopra l'icona del programma nella barra delle applicazioni.
- Con segnali acustici.
- Messaggi di posta elettronica.
- Registra evento.

Per usare questa funzione procedere come segue:

1. Selezionare **Abilita notifiche** nella casella **Interazione con l'utente** (vedere Figura 49).

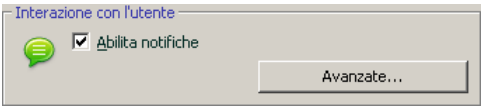


Figura 49. Abilitazione delle notifiche

2. Definire i tipi di eventi di Kaspersky Anti-Virus for Windows Servers per i quali si desidera essere informati e il metodo di notifica (vedere 11.8.1.1 a pag. 141).
3. Configurare le impostazioni di consegna delle notifiche via posta elettronica, se questo è il metodo utilizzato (vedere 11.8.1.2 a pag. 143).

11.8.1.1. Tipi di eventi e metodo di notifica

Durante il funzionamento di Kaspersky Anti-Virus for Windows Servers, si possono verificare i seguenti tipi di eventi:

Notifiche critiche – 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,*il danneggiamento dell'elenco dei virus* o *il fatto che la licenza è scaduta*.

Notifiche errori – eventi che determinano il mancato funzionamento dell'applicazione. Per esempio, l'assenza della licenza o degli elenchi delle minacce.

Notifiche importanti – eventi da approfondire poiché riflettono situazioni importanti nel funzionamento del programma. Per esempio, il fatto che *la protezione è disabilitata* o *la scansione anti-virus del computer non è stata eseguita da tempo.*

Notifiche minori - messaggi di riferimento che in linea generale non contengono informazioni importanti. Per esempio, *comunicano quali sono tutti gli oggetti pericolosi puliti*.

Per specificare gli eventi da comunicare e le modalità di notifica:

1. Fare clic sul collegamento Impostazioni nella finestra principale del programma.
2. Nella finestra delle impostazioni del programma, selezionare **Servizio**, quindi **Abilita notifiche**, e modificare le impostazioni dettagliate facendo clic sul pulsante **Avanzate**.

È possibile configurare i seguenti metodi di notifica per gli eventi sopra elencati nella finestra **Impostazioni notifica** della finestra che si apre (vedere Figura 50):

- *Messaggi a comparsa* sopra l'icona del programma nella barra delle applicazioni, contenenti informazioni sull'evento verificatosi.

  Per usare questo tipo di notifica, selezionare nella sezione **Area commenti** accanto all'evento del quale si desidera essere informati.

- *Segnale acustico*

  Se si desidera che questo avviso sia accompagnato da un suono, selezionare **Suono** nelle impostazioni dell'evento.

- *Notifica via posta elettronica*

  Per utilizzare questo tipo di notifica, selezionare la colonna **Email** opposta all'evento di cui si desidera essere informati e configurare le impostazioni per l'invio delle notifiche (vedere 11.8.1.2 a pag. 143).

- *Registra evento*

  Per registrare nel log le informazioni su qualsiasi evento verificatosi, selezionare nella colonna **Registro** e configurare le impostazioni del registro eventi (vedere 11.8.1.3 a pag. 144).

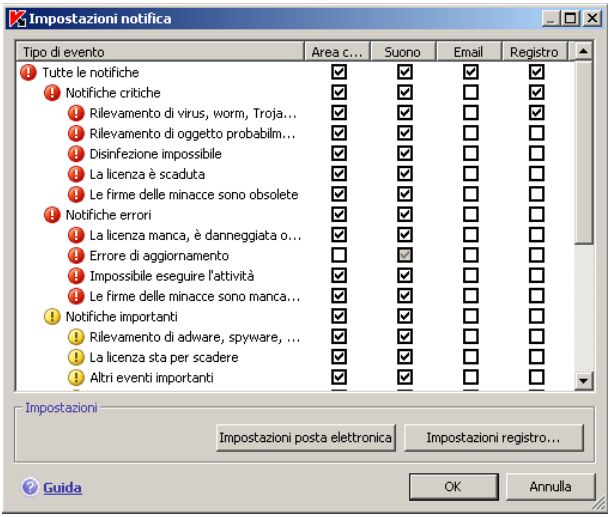


Figura 50. Eventi del programma e metodi di notifica eventi

11.8.1.2. Configurazione delle notifiche via posta elettronica

Dopo aver selezionato gli eventi (vedere 11.8.1.1 a pag. 141) dei quali si desidera essere informati per e-mail, è necessario configurare la consegna dell'avviso. Per fare ciò:

1. Aprire la finestra delle impostazioni del programma con il collegamento Impostazioni nella finestra principale.
2. Selezionare **Servizio** dalla struttura ad albero delle impostazioni.
3. Fare clic su **Avanzate** nella sezione **Interazione con l'utente**nella parte destra dello schermo.
4. Nella finestra **Impostazioni di notifica**, selezionare la casella di controllo ☑ nella colonna **E-mail** per gli eventi che prevedono l'invio di un messaggio di posta elettronica.
5. Nella finestra che si apre facendo clic su **Impostazioni posta elettronica**, configurare le seguenti impostazioni per l'invio di notifiche via posta elettronica:
    - Impostare la notifica di invio in **Da - Indirizzo e-mail**.

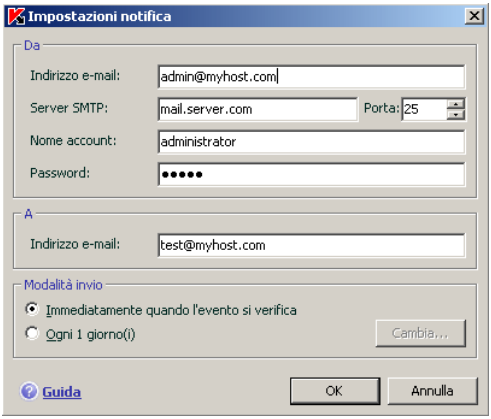


Figura 51. Configurazione delle notifiche via posta elettronica

- Specificare l'indirizzo e-mail a cui inviare gli avvisi in **A - Indirizzo e-mail**.
- Impostare il metodo di avviso 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.

11.8.1.3. Configurazione delle impostazioni del registro eventi

Configurare le impostazioni del registro eventi:

1. Aprire la finestra delle impostazioni dell'applicazione tramite il collegamento Impostazioni della finestra principale.
2. Selezionare **Servizio** dalla struttura ad albero delle impostazioni.
3. Fare clic su **Avanzate** nella sezione **Interazione con l'utente**nella parte destra dello schermo.

Nella finestra **Impostazioni di notifica**, selezionare l'opzione che prevede la registrazione delle informazioni per un evento e fare clic sul pulsante **Impostazioni registro**.

Kaspersky Anti-Virus offre l'opzione di registrare le informazioni sugli eventi che si verificano mentre il programma è in esecuzione, sia nel registro eventi

generale di MS Windows (**Applicazione**) che nel registro eventi dedicato di Kaspersky Anti-Virus (**Registro eventi Kaspersky**).

I registri possono essere visualizzati nel **Visualizzatore eventi** di Microsoft Windows, che si apre selezionando **Start → Impostazioni → Pannello di controllo → Strumenti di amministrazione → Visualizzatore eventi**.

11.8.2. Protezione automatica e limitazioni d'accesso

Kaspersky Anti-Virus for Windows Servers garantisce la sicurezza del computer contro i programmi nocivi e in virtù di questo, può essere esso stesso il bersaglio di programmi nocivi che cercano di bloccarlo o di cancellarlo dal computer.

Inoltre è possibile che più utenti si servano dello stesso PC, con diversi gradi di competenza nel suo utilizzo. 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.

Per abilitare la protezione automatica:

1. Aprire la finestra delle impostazioni del programma tramite il collegamento Impostazioni della finestra principale.
2. Selezionare **Servizio** dalla struttura ad albero delle impostazioni.

Effettuare le seguenti configurazioni nella sezione **Autodifesa** (vedere Figura 52):

- ☑ **Abilita Auto-Difesa**. Se questa casella è selezionata, il programma protegge i propri file, processi di 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.

In presenza di qualsiasi azione tra quelle sopra elencate, viene visualizzato un messaggio sopra l'icona del programma nella barra delle applicazioni (sempre che l'utente non abbia disabilitato le notifiche).

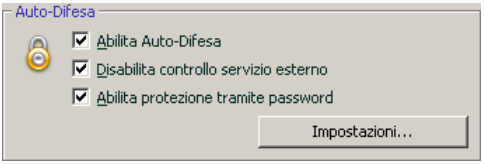


Figura 52. Configurazione della protezione automatica

Per proteggere il programma mediante password, selezionare la casella **Abilita protezione tramite password**. Fare clic sul pulsante **Impostazioni** per aprire la finestra **Protezione tramite password** ed immettere la password e l'area coperta dalla restrizione di accesso (vedere Figura 53).

Figura 53. Impostazioni di protezione del programma tramite password

È possibile 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 del programma
- Chiusura di Kaspersky Anti-Virus for Windows Servers
- Disattivazione o sospensione della protezione del computer

Ciascuna di queste azioni diminuisce il livello di protezione del computer, quindi è necessario stabilire quali persone lavoreranno col server.

Ora, ogni volta che un utente cerca di eseguire tali azioni sul server selezionato, il programma richiede una password.

11.8.3. Risoluzione dei conflitti con altre applicazioni

Ci sono casi in cui Kaspersky Anti-Virus può determinare conflitti con altre applicazioni installate sul computer. Ciò succede perché quei programmi hanno meccanismi di autodifesa interni, che si attivano quando Kaspersky Anti-Virus cerca di ispezionarli. Queste applicazioni comprendono il plug-in Authentica per Acrobat Reader, che verifica l'accesso ai file .pdf, Oxygen Phone Manager II, ed alcuni giochi per PC dotati di strumenti per la gestione dei diritti in digitale.

Per risolvere il problema, selezionare la casella **Modalità compatibilità con programmi che utilizzano metodi di auto-protezione** nella sezione **Servizio** del riquadro delle impostazioni dell'applicazione. È necessario riavviare il sistema operativo perché tale modifica abbia effetto.

11.9. Importazione ed esportazione delle impostazioni di Kaspersky Anti-Virus for Windows Servers

Kaspersky Anti-Virus for Windows Servers include l'opzione di importare ed esportare le sue impostazioni.

Le impostazioni vengono salvate in uno speciale file di configurazione.

Per esportare le impostazioni correnti del programma:

1. Aprire la finestra principale di Kaspersky Anti-Virus for Windows Servers.
2. Selezionare la selezione **Servizio** e fare clic su Impostazioni.
3. Fare clic sul pulsante **Salva** nella sezione **Gestione configurazione**.
4. Digitare un nome per il file di configurazione e selezionare una destinazione in cui salvarlo.

Per importare le impostazioni da un file di configurazione:

1. Aprire la finestra principale di Kaspersky Anti-Virus for Windows Servers.
2. Selezionare la selezione **Servizio** e fare clic su Impostazioni.
3. Fare clic sul pulsante **Importa** e selezionare il file da cui si desidera importare le impostazioni di Kaspersky Anti-Virus.

11.10. Ripristino delle impostazioni predefinite

È sempre possibile tornare alle impostazioni predefinite del programma, che sono considerate le migliori, nonché quelle consigliate da Kaspersky Lab. A tal fine, servirsi della procedura di configurazione guidata.

Per ripristinare le impostazioni di protezione:

1. Selezionare la sezione **Servizio** e fare clic su Impostazioni per andare alla finestra di configurazione del programma.
2. Fare clic sul pulsante **Reimposta** nella sezione **Gestione configurazione**.

La finestra che si apre richiede di definite quali impostazioni devono essere riportate ai valori predefiniti.

Il programma salva per impostazione predefinita tutte le impostazioni personalizzate dell'elenco (se deselezionate). Se non si desidera salvare una delle impostazioni, selezionare la casella corrispondente.

Dopo aver configurato le impostazioni, fare clic sul pulsante **Avanti** (vedere 3.2 a pag. 27). Si apre la procedura di configurazione guidata. Seguire le istruzioni.

Una volta completata la procedura guidata, viene impostato il livello di sicurezza **Consigliato** per File Anti-Virus, fatta eccezione per le impostazioni che si è deciso di conservare. Vengono applicate inoltre le impostazioni configurate con la procedura di configurazione guidata.

CAPITOLO 12. GESTIONE DELL'APPLICAZIONE PER MEZZO DI KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit è un sistema che consente di gestire le principali attività amministrative nell'utilizzo di un sistema di sicurezza per una rete aziendale, basato sulle applicazioni incluse in Kaspersky Anti-Virus Business Optimal e Kaspersky Corporate Suite.

Kaspersky Anti-Virus 6.0 for Windows Servers è uno dei prodotti di Kaspersky Lab che può essere amministrato tramite la sua interfaccia, tramite riga di comando (questi metodi sono descritti sopra nella presente documentazione) oppure utilizzando Kaspersky Administration Kit (se il computer fa parte del sistema centralizzato di amministrazione remota).

Per gestire Kaspersky Anti-Virus 6.0 for Windows Servers tramite Kaspersky Administration Kit, seguire i seguenti passaggi:

- Implementare *Administration Server* nella rete; installare la Console *di amministrazione* presso la stazione del lavoro dell'amministratore (per ulteriori istruzioni, vedere la Guida d'uso per gli amministratori di Kaspersky Administration Kit 6.0);
- Sui file server della rete, implementare Kaspersky Anti-Virus 6.0 for Windows Servers e *NAgent* (incluso con Kaspersky Administration Kit) sui computer della rete. Per ulteriori dettagli sull'installazione remota di Kaspersky Anti-Virus sui computer della rete, vedere la Guida dell'amministratore all'implementazione di Kaspersky Administration Kit 6.0.

Una volta eseguito l'upgrade del plug-in di amministrazione di Kaspersky Lab tramite Kaspersky Administration Kit, chiudere la Console di amministrazione.

La *Console di amministrazione* (vedere Figura 54) consente di amministrare l'applicazione tramite Kaspersky Administration Kit. Si tratta di un'**interfaccia standard integrata nell'MMC** (Microsoft Management Console), che consente all'amministratore di eseguire le seguenti operazioni:

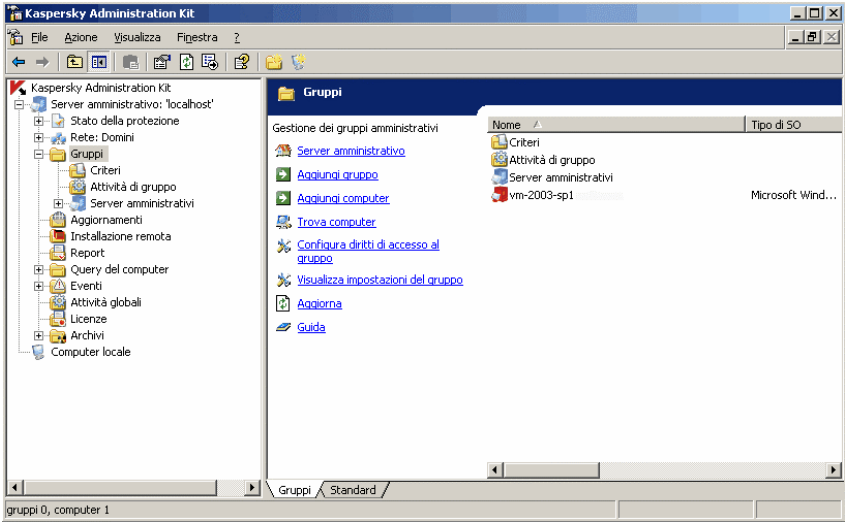


Figura 54. Console di amministrazione di Kaspersky Administration Kit

- Installare Kaspersky Anti-Virus for Windows Servers 6.0 e *NAgent* sui computer della rete
- Configurare in remoto Kaspersky Anti-Virus sui computer della rete
- Aggiornare l'elenco delle minacce ed i moduli di Kaspersky Anti-Virus
- Gestire le licenze per l'applicazione sui computer della rete
- Visualizzare le informazioni sul funzionamento del programma sui computer client

Quando si utilizza Kaspersky Administration Kit, il programma viene amministrato tramite le impostazioni delle regole, le impostazioni delle attività e le impostazioni dell'applicazione stabilite dall'amministratore.

Le **Impostazioni dell'applicazione** sono un insieme di impostazioni per il funzionamento del programma che comprendono le impostazioni di protezione generale, quelle di backup e quarantena, quelle per la generazione dei rapporti, ecc.

Un'**Attività** è un'azione specifica eseguita dall'applicazione. Le attività di Kaspersky Anti-Virus for Windows Servers sono suddivise per tipo secondo la funzione (attività di scansione antivirus, attività di aggiornamento del programma, rollback di un aggiornamento precedente, attività di installazione di una chiave di licenza). Ciascuna attività specifica prevede un insieme di impostazioni di Kaspersky Anti-Virus che vengono utilizzate per la sua esecuzione *(impostazioni dell'attività)*.

La funzione chiave dell'amministrazione centralizzata è il raggruppamento dei computer e la gestione delle loro impostazioni creando e configurando regole di gruppo.

Una **Regola** è un gruppo di impostazioni per il funzionamento del programma sui computer nei gruppi di lavoro della rete, nonchè un gruppo di restrizioni sulla riconfigurazione di tali impostazioni quando si imposta l'applicazione o le attività su un computer client singolo.

Una regola include le impostazioni per la configurazione di tutte le funzioni del programma. Di conseguenza, le regole comprendono le impostazioni del programma e le impostazioni per tutti tipi di attività, tranne le impostazioni specifiche per un certo tipo di attività

12.1. Amministrazione dell'applicazione

Kaspersky Administration Kit consente di avviare e sospendere Kaspersky Anti-Virus in remoto sui computer client singoli, come anche di configurare le impostazioni generali dell'applicazione, ad esempio l'abilitazione o disabilitazione della protezione del computer, le impostazioni di backup e quarantena, e le impostazioni per la creazione dei rapporti.

Per gestire le impostazioni dell'applicazione:

1. Selezionare la cartella del gruppo che contiene il computer client nella cartella **Gruppi** (vedere Figura 54).
2. Nel riquadro dei risultati, selezionare il computer per il quale si desidera modificare le impostazioni dell'applicazione. Nel menù contestuale o in quello **Azioni**, selezionare il comando **Proprietà**.
3. La scheda **Applicazioni** sulla finestra delle proprietà del computer client (vedere Figura 55) visualizza un elenco completo delle applicazioni di Kaspersky Lab installate sul computer client.

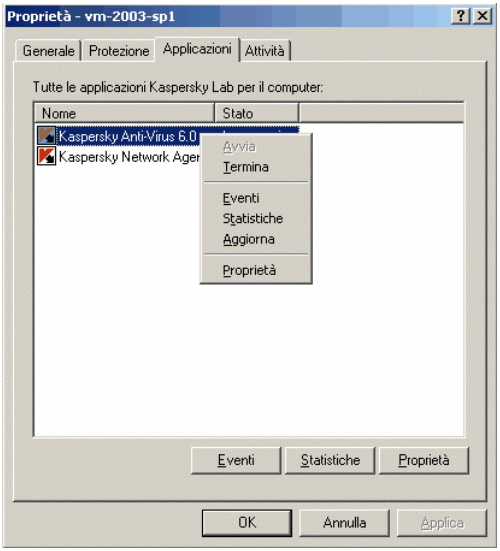


Figura 55. Elenco di applicazioni di Kaspersky Lab

I pulsanti di controllo sotto l'elenco dei programmi possono essere utilizzati per:

- Visualizzare un elenco di eventi nel funzionamento dell'applicazione che si sono verificati sul client e sono stati registrati sul server di amministrazione
- Visualizzare le statistiche correnti sul funzionamento del programma
- Configurare le impostazione del programma (vedere 12.1.2 a pag. 153)

12.1.1. Avvio/arresto dell'applicazione

È possibile avviare o sospendere Kaspersky Anti-Virus su un computer remoto tramite i comandi del menù contestuale nella finestra delle proprietà del computer (vedere Figura 55).

È possibile eseguire le stesse azioni utilizzando i pulsanti **Avvia/Arresta** della finestra delle impostazioni sulla scheda **Generale** (vedere Figura 56).

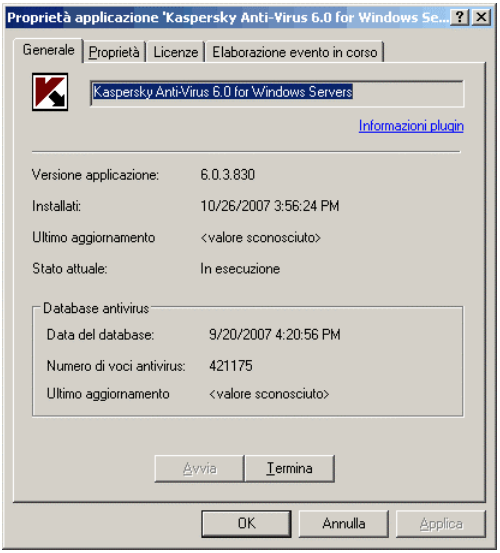


Figura 56. Configurazione delle impostazioni di Kaspersky Anti-Virus. Scheda **Generale**

La sezione superiore della finestra visualizza il nome dell'applicazione installata, la versione, la data dell'installazione, lo stato (se l'applicazione è in esecuzione oppure no sul computer locale) nonché le informazioni relative alle condizioni del database antivirus.

12.1.2. Configurazione delle impostazioni dell'applicazione

Per visualizzare o modificare le impostazioni dell'applicazione:

1. Aprire la finestra delle proprietà per il computer client sulla scheda **Applicazione** (vedere Figura 54).
2. Selezionare **Kaspersky Anti-Virus for Windows Servers 6.0**. Fare clic sul pulsante **Proprietà** nella finestra delle impostazioni dell'applicazione.

Tutte le schede (ad eccezione di **Proprietà**) sono standard di Kaspersky Administration Kit. Per ulteriori informazioni sulle schede standard, vedere la Guida dell'amministratore.

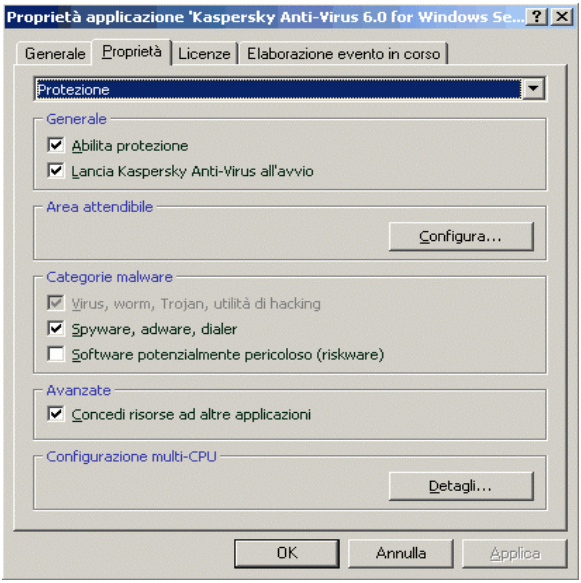


Figura 57. Configurazione delle impostazioni di Kaspersky Anti-Virus. La scheda **Proprietà**

Se è stata creata una regola per l'applicazione (vedere 12.3.1 a pag. 163) che impedisce la riconfigurazione di alcune impostazioni, esse non saranno modificabili quando si configura l'applicazione.

La scheda **Proprietà** consente di configurare le impostazioni generali e di servizio per la protezione di Kaspersky Anti-Virus, le impostazioni di backup e quarantena, e le impostazioni di creazione dei rapporti. A tal fine, selezionare il valore desiderato dall'elenco a discesa nella parte superiore della finestra e configurare le impostazioni:

Protezione
Questa finestra consente di: • Abilitare/disabilitare la protezione di un computer (vedere 6.1 a pag. 53) • Configurare l'avvio automatico dell'applicazione all'accensione del computer (vedere 6.1.5 a pag. 57) • Creare una zona affidabile o un elenco di esclusioni (vedere 6.3 a pag. 58)

- Selezionare il tipo di programmi nocivi che verranno monitorati dall'applicazione (vedere 6.2 a pag. 57)
- Configurare le impostazioni di produttività per l'applicazione e quelle per una configurazione multiprocessore (vedere 6.7 a pag. 69)

Servizio

La configurazione delle impostazioni di servizio comprende:

- Configurare le notifiche per gli eventi che si verificano (vedere 11.8.1 a pag. 141)
- Gestire la funzione di autodifesa e le impostazioni di protezione con password dell'applicazione (vedere 11.8.2 a pag. 145)
- Configurare l'aspetto dell'applicazione (vedere 12.3.1 a pag. 163)
- Configurare le impostazioni di compatibilità tra Kaspersky Anti-Virus e altri programmi (vedere 11.8.3 a pag. 147)

File di dati

Questa finestra consente di configurare le impostazioni per la generazione dei rapporti statistici sul funzionamento del programma (vedere 11.3.1 a pag. 129) e di specificare per quanto tempo i file vengono conservati nell'area di backup (vedere 11.2.2 a pag. 124) ed in quella di quarantena (vedere 11.1.2 a pag. 121).

12.1.3. Configurazione delle impostazioni specifiche

Durante l'amministrazione di Kaspersky Anti-Virus tramite Kaspersky Administration Kit, è possibile abilitare o disabilitare l'interattività e modificare le informazioni di assistenza tecnica. Per fare ciò:

1. Aprire la finestra delle proprietà per il computer client sulla scheda **Applicazione** (vedere Figura 55).
2. Selezionare **Kaspersky Anti-Virus for Windows Servers 6.0** ed utilizzare il pulsante **Proprietà**. Si aprirà una finestra di impostazione dell'applicazione (vedere Figura 57). Selezionare **Servizio** dal menù a discesa nella parte superiore della finestra.

La scheda **Servizio** della sezione **Aspetto** consente di abilitare o disabilitare l'interattività di Kaspersky Anti-Virus su un computer remoto: la visualizzazione dell'icona di Kaspersky Anti-Virus nell'area di notifica, l'invio di notifiche sugli

eventi che si verificano nell'applicazione (ad esempio il rilevamento di un oggetto pericoloso).

Se è selezionato **Consenti interattività**, un utente che lavori su un computer remoto potrà vedere l'icona di Anti-Virus ed i messaggi a comparsa, e sarà in grado di prendere decisioni sull'azione successiva nelle finestre di notifica riguardanti gli eventi che si verificano. Per disabilitare l'interattività dell'applicazione, deselezionare la casella di controllo.

La scheda **Informazioni di assistenza personali** nella finestra che si apre facendo clic sul pulsante **Impostazioni** consente di modificare le informazioni di assistenza tecnica utente che vengono visualizzate nella sezione **Servizio** della voce **Assistenza** (vedere Figura 47) di Kaspersky Anti-Virus.

Per modificare le informazioni del caso superiore, immettere il testo corrente nell'assistenza fornita. Nel campo sottostante, è possibile modificare i collegamenti ipertestuali che vengono visualizzati nella casella **Assistenza tecnica on-line**, che appare selezionando **Assistenza** nella sezione **Servizio**.

Per modificare l'elenco di fonti, utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. Kaspersky Anti-Virus aggiungerà un nuovo collegamento sulla parte superiore dell'elenco. Per modificare l'ordine dei collegamenti nell'elenco, utilizzare i pulsanti **Su** e **Giù**.

Se la finestra non contiene dati, le informazioni predefinite sull'assistenza tecnica non sono modificabili.

12.2. Gestione delle attività

Questa sezione include informazioni sulla gestione delle attività di Kaspersky Anti-Virus for Windows Servers 6.0 Per ulteriori dettagli sul concetto di gestione delle attività tramite Kaspersky Administration Kit 6.0, si veda la Guida dell'amministratore per il programma.

Un insieme di attività di sistema viene creato per ciascun computer all'installazione dell'applicazione. Questo elenco (vedere Figura 58) comprende le attività di protezione in tempo reale (File Anti-Virus), le attività di scansione antivirus (Risorse del computer, Oggetti di avvio, Aree critiche), nonché le attività di aggiornamento (aggiornamento all'elenco dei virus ed ai moduli dell'applicazione, rollback di un aggiornamento, e distribuzione degli aggiornamenti).

È possibile avviare le attività di sistema, configurarne le impostazioni e pianificarle, ma non possono essere eliminate.

Inoltre, è possibile creare le proprie attività, ad esempio scansioni antivirus, aggiornamenti dell'applicazione e rollback dell'aggiornamento precedente, attività di installazione di una chiave di licenza.

Per visualizzare un elenco delle attività create per un computer client:

1. Selezionare la cartella del gruppo che contiene il computer client nella cartella **Gruppi** (vedere Figura 54).
2. Nel riquadro dei risultati, selezionare il computer per il quale si desidera creare un'attività locale, quindi utilizzare il comando **Attività** nel menu di scelta rapida o nel menu **Azioni**. Nella finestra principale si aprirà un'altra finestra che visualizza le proprietà del computer client.
3. La scheda **Attività** (vedere Figura 58) visualizza un elenco completo di attività create per quel computer client.

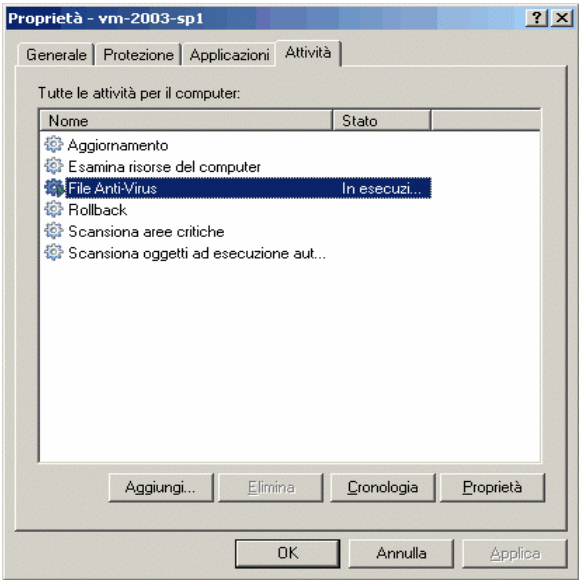


Figura 58. Elenco di attività dell'applicazione

12.2.1. Avvio e arresto delle attività

Le attività possono essere avviate sui computer client solo se la corrispondente applicazione è in esecuzione (vedere 12.1.1 a pag. 152). Se l'applicazione viene arrestata, tutte le attività avviate verranno arrestate.

Le attività vengono avviate e sospese automaticamente, in base ad una pianificazione, oppure manualmente utilizzando i comandi dal menù contestuale e dalla finestra di visualizzazione delle impostazioni dell'attività. È inoltre possibile sospendere un'attività e riavviarla.

Per avviare/arrestare/sospendere/riprendere manualmente un'attività:

Selezionare l'attività desiderata dal riquadro dei risultati, aprire il menu di scelta rapida e selezionare **Avvia/Arresta/Sospendi/Riprendi** nel menu stesso o nel menu **Azione**.

È possibile eseguire operazioni analoghe dalla finestra di impostazione delle attività sulla scheda **Generale** (vedere Figura 59) utilizzando i pulsanti corrispondenti.

12.2.2. Creazione delle attività

Quando si lavora con l'applicazione tramite Kaspersky Administration Kit, è possibile creare:

- Attività locali, configurate per i singoli computer
- Attività di gruppo, configurate per i computer uniti in un gruppo di rete
- Attività globali, configurate per qualsiasi insieme di computer da qualsiasi gruppo di rete

È possibile modificare le impostazioni delle attività, controllarne l'esecuzione, copiare e spostare attività da un gruppo all'altro, ed eliminarle tramite i comandi standard del menu di scelta rapida, come **Copia/Incolla**, **Taglia/Incolla** e **Cancella**, o tramite comandi analoghi nel menu **Azione**.

12.2.2.1. Creazione delle attività locali

Per creare un'attività locale, procedere come segue:

1. Aprire la finestra delle proprietà per il computer client sulla scheda **Attività** (vedere Figura 58).
2. Fare clic su **Aggiungi** per creare una nuova attività. Si aprirà una nuova finestra Crea nuova attività, che è progettata come una procedura guidata di Windows standard e consiste in una serie di passaggi tra i quali è possibile navigare utilizzando i pulsanti **Indietro** e **Avanti**; per completare la procedura, fare clic sul pulsante **Fine.** Per uscire dalla procedura in qualsiasi momento, fare clic su **Annulla**.

Passaggio 1. Immissione delle informazioni generali sull'attività

La prima finestra principale ha una funzione introduttiva: digitare qui il nome dell'attività (campo **Nome**).

Passaggio 2. Selezionare l'applicazione ed il tipo di attività

Durante questo passaggio, è necessario specificare l'applicazione per la quale viene creata l'attività (Kaspersky Anti-Virus for Windows Servers 6.0). È inoltre necessario selezionare il tipo di attività. Le attività possibili per Kaspersky Anti-Virus 6.0 sono:

- *Scansione antivirus* – analizza l'area specificata dall'utente alla ricerca di virus
- *Aggiornamento* – recupera ed applica i pacchetti di aggiornamento per il programma
- *Rollback dell'aggiornamento* – ripristina l'aggiornamento precedente del programma
- *Installazione della chiave di licenza* – aggiunge una nuova chiave di licenza per l'utilizzo dell'applicazione

Passaggio 3. Configurazione delle impostazioni per il tipo di attività selezionato

In funzione del tipo di attività selezionato durante il passo precedente, i contenuti delle seguenti finestre possono variare:

SCANSIONE ANTIVIRUS

La finestra di configurazione dell'attività di scansione antivirus richiede la creazione di un elenco di oggetti da esaminare (vedere 8.2 a pag.86), nonché di specificare l'azione che dovrà essere eseguita da Kaspersky Anti-Virus alla rilevamento di un oggetto pericoloso (vedere 8.4.4 a pag. 95).

UPDATE

Per le attività di aggiornamento dell'elenco delle minacce e dei moduli dell'applicazione, è necessario specificare la sorgente che verrà utilizzata per scaricare gli aggiornamenti (vedere 10.4.1 a pag. 109). L'origine di aggiornamento predefinita è costituita dal server di aggiornamento di Kaspersky Administration Kit.

ROLLABACK DELL'AGGIORNAMENTO PRECEDENTE

L'attività di rollback degli aggiornamenti più recenti non prevede impostazioni specifiche.

INSTALLAZIONE DELLA CHIAVE DI LICENZA

Per le attività di installazione delle chiavi di licenza, specificare il percorso al file chiave col pulsante **Sfoglia**. Per utilizzare una chiave aggiunta quale backup, selezionare **Aggiungi come chiave di backup**. Essa sarà attivata alla scadenza della chiave corrente.

Le informazioni sulla chiave aggiunta (numero di licenza, tipo e data di scadenza) vengono visualizzate nel campo sottostante.

Passaggio 4. Configurazione dell'avvio di un'attività utilizzando un diverso account utente

In questa fase, viene richiesto di configurare le attività per l'avvio tramite un account utente con privilegi sufficienti a garantire l'accesso all'oggetto che viene esaminato, o all'origine degli aggiornamenti (vedere 6.4 a pag. 65).

Passaggio 5. Pianificazione degli aggiornamenti

Dopo avere configurato le impostazioni dell'attività, verrà richiesto di pianificare l'esecuzione automatica dell'attività.

A tal fine, selezionare la frequenza desiderata per l'esecuzione dell'attività dal menù a discesa, è regolare le impostazioni di pianificazione nella parte inferiore della finestra.

Passaggio 6. Completare la creazione di un'attività

L'ultima finestra di dialogo della procedura guidata comunica all'utente che l'attività è stata creata con successo.

12.2.2.2. Creazione delle attività di gruppo

Per creare un'attività di gruppo, procedere come segue:

1. Selezionare il gruppo per il quale si desidera creare un'attività dall'albero della consolle.
2. Selezionare la cartella **Attività di gruppo**, aprire il menù contestuale e selezionare il comando **Crea→attività**, oppure utilizzare lo stesso comando dal menù **Azione**. Partirà quindi la procedura di creazione

guidata dell'attività, simile alla procedura guidata per la creazione delle attività locali12.2.2.1 158). Seguire le istruzioni.

Una volta terminata la procedura guidata, l'attività verrà aggiunta alla cartella **Attività di gruppo** di quel gruppo e di tutti i suoi sottogruppi, e visualizzata nel riquadro dei risultati.

12.2.2.3. Creazione delle attività globali

Per creare un'attività globale, procedere come segue:

1. Selezionare il nodo **Attività globali** dall'albero della console, aprire il menù contestuale e selezionare il comando **Crea→attività**, oppure utilizzare lo stesso comando dal menù **Azione**.
2. Partirà quindi la procedura di creazione guidata dell'attività, simile alla procedura guidata per la creazione delle attività locali12.2.2.1 158). La differenza è che previsto il passaggio per la creazione di un elenco di computer client della rete per per i quali viene creata l'attività globale.
3. E selezionare dalla rete i computer che eseguiranno l'attività. È possibile selezionare computer da più cartelle o selezionare un'intera cartella (per ulteriori dettagli, consultare la guida dell'amministratore di Kaspersky Administration Kit 6.0).

Le attività globali vengono eseguite esclusivamente sui computer specificati. Se vengono aggiunti nuovi computer ad un gruppo contenente computer per i quali è stata creata un'attività di installazione remota, l'attività non verrà eseguita per essi. A tal fine sarà necessario creare una nuova attività o modificare di conseguenza quella esistente.

Una volta terminata la procedura guidata, una nuova attività globale sarà giunta al nodo **Attività globali** della struttura ad albero della console, e visualizzata nel riquadro dei risultati.

12.2.3. Configurazione delle impostazioni dell'attività

Per visualizzare o modificare le impostazioni dell'attività del computer client:

1. Aprire la finestra delle proprietà per il computer client sulla scheda **Attività** (vedere Figura 58).

2. Selezionare l'attività desiderata dall'elenco e fare clic sul pulsante **Proprietà**. Si aprirà una finestra di impostazione dell'attività (vedere Figura 60).

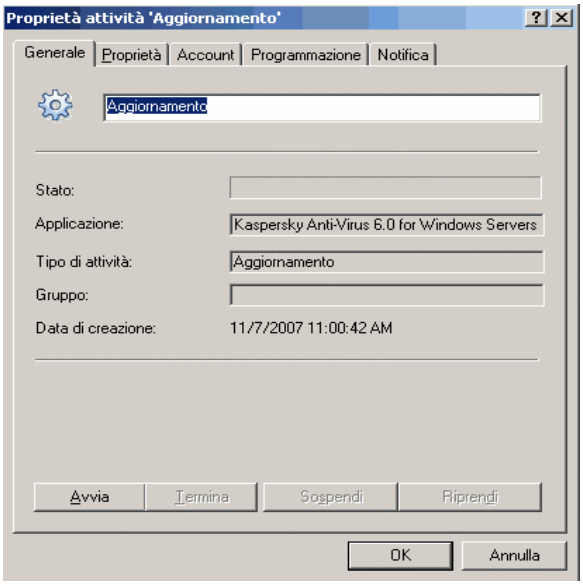


Figura 59. Configurazione delle impostazioni dell'attività

Tutte le schede (ad eccezione di **Impostazioni**) sono quelle standard di Kaspersky Administration Kit 6.0. Vengono trattate con maggiore dettaglio nella guida dell'amministratore. La scheda **Impostazioni** contiene impostazioni specifiche per Kaspersky Anti-Virus. I contenuti di questa scheda variano in funzione del tipo di attività selezionata.

La configurazione delle impostazioni delle attività di programma tramite l'interfaccia di Kaspersky Administration Kit è analoga alla configurazione attraverso l'interfaccia locale di Kaspersky Anti-Virus, tranne per quanto riguarda le impostazioni specifiche per quell'attività. Vedere Capitolo 7 – Capitolo 10 a pag. 71 – 105 di questa guida utente per una descrizione più approfondita della configurazione delle impostazioni di un'attività.

Se è stata creata una regola per l'applicazione (vedere 12.3 a pag. 162) che impedisce la riconfigurazione di alcune impostazioni, esse non saranno modificabili quando si configurano le attività.

12.3. Gestione delle regole

L'impostazione di regole consente di applicare impostazioni universali per l'applicazione e le attività ai computer client appartenenti ad un singolo gruppo di rete.

Questa sezione include informazioni sulla creazione e gestione di regole per Kaspersky Anti-Virus for Windows Servers 6.0 Per ulteriori dettagli sul concetto di gestione delle regole tramite Kaspersky Administration Kit 6.0, si veda la Guida dell'amministratore per il programma.

12.3.1. Creazione di regole

Per creare una regola per Kaspersky Anti-Virus, procedere come segue:

1. Nella cartella **Gruppi** (vedere Figura 54), selezionare il gruppo di computer per il quale si desidera creare una regola.
2. Selezionare la cartella **Regole** appartenente al gruppo selezionato, aprire il menù contestuale ed utilizzare il comando **Crea→ regola**. Verrà visualizzata una finestra Crea nuova regola.

   Questa interfaccia è concepita come una procedura guidata standard di Windows ed è costituita da una serie di passaggi tra i quali è possibile navigare utilizzando i pulsanti **Indietro** e **Avanti**; per completare la procedura, fare clic sul pulsante **Fine.** Per uscire dalla procedura in qualsiasi momento, fare clic su **Annulla**.

Durante ciascuna fase di creazione di una regola, le impostazioni immesse possono essere bloccate con il pulsante  . Se il lucchetto sul pulsante è chiuso, i valori assegnati in futuro dalla regola creata verranno utilizzati quando si utilizza la regola sui computer client.

Passaggio 1. Immissione delle informazioni generali sulla regola

Le prime finestre della procedura guidata hanno funzione introduttiva. Qui è necessario specificare il nome della regola (campo **Nome**) e selezionare **Kaspersky Anti-Virus for Windows Servers 6.0** dal menù a discesa **Nome applicazione**. Se si desidera che le impostazioni della regola abbiano effetto immediato dopo averla creata, selezionare **Attiva regola**.

Passaggio 2. Selezione di uno stato per una regola

Questa finestra richiede di specificare lo stato della regola. A tal fine, selezionare l'opzione desiderata: regola attiva o regola inattiva.

È possibile creare diverse regole in un gruppo per un'applicazione, ma solo una di esse può essere la regola corrente (attiva).

Passaggio 3. Selezione configurazione dei componenti di protezione

Durante questa fase, è possibile abilitare o disabilitare la protezione del computer, nonchè File Anti-Virus. Per impostazione predefinita, la protezione è abilitata e File Anti-Virus è in esecuzione.

Per configurare con maggiore precisione la protezione o File Anti-Virus, selezionarli dall'elenco e fare clic sul pulsante **Impostazioni**.

Passaggio 4. Configurazione delle attività di scansione antivirus

Durante questa fase, viene richiesto di configurare le impostazioni che verranno utilizzate per le attività di scansione antivirus.

Nel riquadro **Livello di sicurezza**, selezionare uno dei tre livelli di sicurezza preimpostati (vedere 7.1 a pag. 72). Per regolare con maggiore precisione il livello selezionato, fare clic sul pulsante **Impostazioni**. Per ripristinare le impostazioni del livello di protezione **Consigliato**, utilizzare il pulsante **Predefinito**.

Nella sezione **Azioni**, specificare l'azione che dev'essere eseguita da Anti-Virus quando viene rilevato un oggetto pericoloso (vedere 8.4.4 a pag. 95).

Passaggio 5. Configurazione delle impostazioni di aggiornamento

In questa finestra, configurare le impostazioni per la funzione di distribuzione degli aggiornamenti di Kaspersky Anti-Virus.

Nella sezione **Impostazioni di aggiornamento**, specificare se i moduli del programma devono essere aggiornati (vedere 10.4.2 a pag. 109). Nella finestra che si apre facendo clic sul pulsante **Impostazioni**, assegnare le impostazioni locali della rete (vedere 10.4.3 a pag. 114) e specificare l'origine di aggiornamento (vedere 10.4.1 a pag. 109).

Nella sezione **Azioni successive all'aggiornamento**, abilitare o disabilitare la scansione della quarantena dopo aver ricevuto un nuovo pacchetto di aggiornamento (vedere 10.4.4 a pag. 116).

Passaggio 6. Applicazione delle regole

Durante questa fase, viene richiesto di selezionare un metodo per distribuire la regola ai client del gruppo (per maggiori dettagli consultare la guida dell'amministratore di Kaspersky Administration Kit 6.0).

Passaggio 7. Determinare un metodo per la prima applicazione di una regola

A questo punto, selezionare un metodo per la prima applicazione di una regola sui computer client del gruppo nella finestra **Applica regola** (per maggiori dettagli vedere la guida dell'amministratore di Kaspersky Administration Kit 6.0).

Passaggio 8. Completare la creazione di una regola

La finestra finale della procedura guidata comunica all'utente che una nuova regola è stata creata con successo.

Al termine della procedura guidata, la regola di che Anti-Virus verrà aggiunta alla cartella **Regole** del gruppo corrispondente, e sarà visualizzata nel pannello dei risultati.

È possibile modificare le impostazioni della regola creata e stabilire delle restrizione alla loro modifica utilizzando il pulsante  per ciascun gruppo di impostazioni. Un utente su un computer client non sarà in grado di modificare le impostazioni se vengono bloccate in questo modo. La regola verrà applicata ai computer client al momento della loro prima sincronizzazione con il server.

È possibile copiare e spostare le regole da un gruppo ad un altro oppure cancellarle, utilizzando i comandi standard del menu di scelta rapida, come **Copia**/**Incolla**, **Taglia**/**Incolla** e **Cancella**, o i comandi analoghi nel menu Azione.

12.3.2. Visualizzazione e modifica delle impostazioni delle regole

In fase di modifica, è possibile modificare la regola e bloccare la modifica delle impostazioni delle regole di gruppo nidificate e di quelle dell'applicazione e delle attività.

Per visualizzare e modificare le impostazioni delle regole:

1. Selezionare il gruppo di computer per il quale si desidera modificare le impostazioni dall'albero della console nella cartella **Gruppi**.
2. Selezionare la cartella **Regole** appartenente a quel gruppo. A questo punto, il riquadro dei risultati visualizza tutte le regole create per il gruppo.
3. Selezionare la regola desiderata dall'elenco di regole per **Kaspersky Anti-Virus for Windows Servers 6.0** (il nome dell'applicazione è specificato nel campo **Applicazione**).
4. Aprire il menu di scelta rapida per la regola selezionata e fare clic sul comando **Proprietà**. Lo schermo visualizza la finestra dell'impostazione della regola per Kaspersky Anti-Virus 6.0 (vedere Figura 60).

Tutte le schede (ad eccezione di **Impostazioni**) sono quelle standard di Kaspersky Administration Kit 6.0. Vengono trattate con maggiore dettaglio nella guida dell'amministratore.

La scheda **Impostazioni** visualizza le impostazioni della regola per Kaspersky Anti-Virus 6.0. Le impostazioni della regola includono le impostazioni del programma (vedere 12.1.2 a pag. 153) e le impostazioni dell'attività (vedere 12.2 a pag. 156).

Per configurare le impostazioni, selezionare il valore richiesto dal menù a discesa nella parte superiore della finestra e configurare le impostazioni.

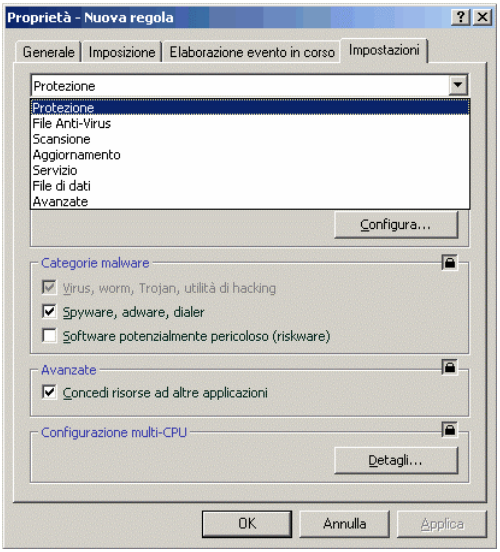


Figura 60. Configurazione delle impostazioni delle regole

CAPITOLO 13. USO DEL PROGRAMMA DA RIGA DI COMANDO

Kaspersky Anti-Virus for Windows Servers può essere utilizzato da riga di comando. eseguendo le seguenti operazioni:

- Avvio, arresto, sospensione e ripristino dell'attività del File Anti-Virus
- Avvio, arresto, pausa e ripristino delle scansioni antivirus
- Ottenimento di informazioni sullo stato corrente di File Anti-Virus e sulle relative statistiche
- Scansione degli oggetti selezionati
- Aggiornamento degli elenchi delle minacce 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 da riga di comando è la seguente:

```
avp.com <command> [settings]
```

È necessario accedere al programma dalla riga di comando dalla cartella d'installazione del programma o specificando il percorso completo a avp.com

Quando segue può essere utilizzato come **<commands>**:

ADDKEY	Attiva l'applicazione utilizzando una chiave di licenza (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)
ACTIVATE	Attiva l'applicazione on-line utilizzando il codice di attivazione.
START	Avvia File Anti-Virus o un'attività
PAUSE	Sospende File Anti-Virus o un'attività (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)

RESUME	Ripristina File Anti-Virus o un'attività
STOP	Arresta File Anti-Virus o un'attività (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)
STATUS	Visualizza lo stato di File Anti-Virus o dell'attività sullo schermo
STATISTICS	Visualizza le statistiche di File Anti-Virus o dell'attività sullo schermo
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	Ripristina la versione precedente dopo un aggiornamento (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)
EXIT	Chiude il programma (è possibile eseguire questo comando solo con la password impostata nell'interfaccia del programma)
IMPORT	Importa le impostazioni di Kaspersky Anti-Virus for Windows Servers (il comando può essere eseguito solo inserendo la password assegnata tramite l'interfaccia del programma)
EXPORT	Esporta le impostazioni di Kaspersky Anti-Virus for Windows Servers

Ogni comando utilizza le proprie impostazioni specifiche per il particolare componente di Kaspersky Anti-Virus for Windows Servers.

13.1. Attivazione dell'applicazione

Due sono i metodi per attivare l'applicazione:

- on-line utilizzando un codice di attivazione (comando ACTIVATE)
- utilizzando un file chiave di licenza (comando ADDKEY).

Sintassi del comando:

```
ACTIVATE <activation_code>
ADDKEY <file_name> /password=<your_password>
```

Parametri:

<file_name>	Nome del file chiave di licenza con l'estensione *.key
<activation_code>	Codice di attivazione dell'applicazione fornito all'acquisto.
<your_password>	Password di Kaspersky Anti-Virus impostata tramite l'interfaccia del programma.
Si noti che questo comando non sarà accettato senza password	

Esempio:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<your_password>
```

13.2. Gestione di File Anti-Virus e delle attività

Sintassi del comando:

```
avp.com <command> <profile|task_name>
[/R[A]:<log_file>]
avp.com STOP|PAUSE <profile|task_name>
/password=<your_password> [/R[A]:<report_file>]
```

Parametri:

<command>	Kaspersky Anti-Virus consente la gestione dell'attività del componente dalla riga di comando utilizzando i seguenti comandi: **START** – avvia un componente o un'attività di protezione in tempo reale. **STOP** – arresta un componente o un'attività di protezione in tempo reale. **PAUSE** – sospende un componente o un'attività di protezione in tempo reale. **RESUME** – ripristina un componente o un'attività di protezione in tempo reale. **STATUS** – visualizza lo stato corrente di un componente o un'attività di protezione in tempo reale. **STATISTICS** – visualizza le statistiche di esecuzione di un componente o un'attività di protezione in tempo reale. Si noti che i comandi PAUSE e STOP sono protetti da password.
<profile|task_name>	Al parametro **<profile>** può essere assegnato come valore qualsiasi componente di protezione dell'applicazione in tempo reale o qualsiasi modulo di componente, come anche qualsiasi attività di scansione manuale o di aggiornamento (i valori standard utilizzati dall'applicazione sono mostrati di seguito). I valori validi per il parametro **<task_name>** possono includere il nome di qualsiasi attività di scansione manuale o di aggiornamento definita dall'utente.
<your_password>	Password di Kaspersky Anti-Virus impostata tramite l'interfaccia del programma.
/R[A]:<report_file>	**R:<report_file>**: registra solo eventi importanti; **/RA:<report_file>**: registra tutti gli eventi. È possibile utilizzare un percorso assoluto o

	relativo ad un file. Se il parametro non è definito, i risultati di scansione vengono visualizzati sullo schermo, insieme a tutti gli eventi.

Uno dei seguenti valori è assegnato a **<profile>**:

RTP	Tutti i componenti della protezione Il comando `avp.com START RTP` avvia File Anti-Virus se era stato sospeso utilizzando il pulsante ❚❚ nell'interfaccia grafica utente, oppure tramite il comando `PAUSE` dalla riga di comando. Se il componente è stato disabilitato tramite il pulsante ■ nell'interfaccia grafica utente o il comando `STOP` dalla riga di comando, è necessario lanciare il comando `avp.com START FM` per riavviarlo.
FM	File Anti-Virus
UPDATER	Aggiornamento
RetranslationCfg	Distribuzione degli aggiornamenti ad una sorgente locale.
Rollback	Ripristina l'aggiornamento precedente del programma
SCAN_OBJECTS	Attività di scansione antivirus
SCAN_MY_COMPUTER	Attività Risorse del computer
SCAN_CRITICAL_AREAS	Attività aree critiche
SCAN_STARTUP	Attività oggetti ad esecuzione automatica
SCAN_QUARANTINE	Attività di scansione degli oggetti in quarantena
I componenti e le attività avviati da riga di comando vengono eseguiti con le impostazioni configurate dall'interfaccia del programma.	

Esempi:

Per abilitare File Anti-Virus, digitare la seguente stringa nella riga di comando*:*

```
avp.com START FM
```

Per terminare un'attività di scansione delle Risorse del computer da riga di comando, digitare*:*

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

13.3. Scansioni antivirus

La sintassi per avviare una scansione anti-virus di una determinata area ed elaborare gli oggetti nocivi dalla riga di comando generalmente ha questo aspetto:

```
avp.com SCAN [<object scanned>] [<action>] [<file
types>] [<exclusions>] [<configuration file>]
[<report settings>] [<advanced settings>]
```

Per eseguire la scansione di oggetti, è possibile anche avviare una delle attività create in Kaspersky Anti-Virus for Windows Servers dalla riga di comando (vedere 13.2 a pag. 170). L'attività viene eseguita con le impostazioni specificate nell'interfaccia del programma.

Descrizione dei parametri:

<object scanned> - questo parametro fornisce l'elenco di oggetti che saranno sottoposti a scansione per evidenziare eventuali codici nocivi. Può includere diversi valori dall'elenco seguente, separati da uno spazio.	
<files>	Lista dei percorsi ai file e/o cartelle da sottoporre a scansione. È possibile inserire percorsi assoluti o relativi. Gli elementi nell'elenco sono 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 antivirus tutti i file in essa contenuti.

/MEMORY	Oggetti della memoria di sistema
/STARTUP	Oggetti di avvio
/MAIL	Database di posta
/REMDRIVES	Tutte le unità estraibili.
/FIXDRIVES	Tutte le unità interne
/NETDRIVES	Tutte le unità di rete
/QUARANTINE	Oggetti in quarantena
/ALL	Scansione completa
/@:<filelist.lst>	Percorso al file contenente un elenco di oggetti e cartelle da includere nella scansione. Il file deve essere in formato testo e ogni oggetto della scansione deve iniziare una nuova riga. È possibile immettere un percorso assoluto o relativo al file. Il percorso deve essere scritto tra virgolette se contiene uno spazio.
<action> - questo parametro imposta le reazioni agli oggetti nocivi rilevati durante la scansione. Se questo parametro non viene definito, il valore predefinito è **/i8**.	
/i0	nessuna azione sull'oggetto; semplice registrazione delle informazioni nel rapporto.
/i1	Trattare gli oggetti infetti e, se la riparazione non riesce, ignorare.
/i2	Trattare gli oggetti infetti e, se la disinfezione non riesce, eliminarli. Eccezioni: non eliminare gli oggetti infetti dagli oggetti compositi; eliminare gli oggetti compositi con intestazioni eseguibili, ad esempio gli archivi .sfx (impostazione predefinita).

/i3	Trattare gli oggetti infetti e, se la disinfezione non riesce, eliminarli. Inoltre, eliminare completamente tutti gli oggetti compositi se i contenuti infetti non possono essere eliminati.
/i4	Disinfettare gli oggetti infetti e, se la disinfezione non riesce, eliminarli. Inoltre, eliminare completamente tutti gli oggetti compositi se i contenuti infetti non possono essere eliminati.
/i8	Richiedere l'intervento dell'utente se viene rilevato un oggetto infetto.
/i9	Richiedere l'intervento dell'utente al termine della scansione.
<file types> - questo parametro definisce quali tipi di file saranno sottoposti alla scansione anti-virus. Se questo parametro non viene definito, il valore predefinito è /i8.	
/fe	Esaminare solo i file potenzialmente infetti in base all'estensione.
/fi	Esaminare solo i file potenzialmente infetti in base ai contenuti (impostazione predefinita).
/fa	Esaminare tutti i file
<exclusions> - questo parametro definisce quali oggetti sono esclusi dalla scansione. Può includere diversi valori dall'elenco fornito, separati da uno spazio.	
-e:a	Non esaminare archivi
-e:b	Non esaminare database di posta
-e : m	Le e-mail con testo semplice non vengono esaminate
-e:<filemask>	Non esaminare oggetti in base alle maschere

-e:<seconds>	Vengono ignorati gli oggetti la cui scansione richiede un intervallo di tempo superiore a quello specificato nel parametro **<secondi>**.
-es:<size>	Ignorare gli oggetti di dimensione (in MB) superiore a quella specificata nel parametro **<size>**
<configuration file> - definisce il percorso al file di configurazione che contiene le impostazioni di scansione del programma. Il file di configurazione viene salvato in formato binario (*.dat*, a meno che non venga specificato un altro formato o il formato non sia assegnato, e può essere utilizzato successivamente per importare le impostazioni dell'applicazione su altri computer. È possibile immettere un percorso assoluto o relativo al file. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia di Kaspersky Anti-Virus for Windows Servers.	
/C:<file_name>	Utilizzare i valori di impostazione assegnati nel file di configurazione **<file_name>**
<report settings> - questo parametro determina il formato del rapporto sui risultati di scansione. È possibile immettere un percorso assoluto o relativo al file. Se il parametro non è definito, i risultati di scansione sono visualizzati sullo schermo, insieme a tutti gli eventi.	
/R:<report_file>	Registrare in questo file solo gli eventi importanti.
/RA:<report_file>	Registrare tutti gli eventi in questo file.
<advanced settings> - Impostazioni che definiscono l'utilizzo delle tecnologie di scansione antivirus.	
/iChecker=<on|off>	Abilita/disabilita iChecker.
/iSwift=<on|off>	Abilita/disabilita iSwift.

Esempi:

*Avviare una scansione di RAM, programmi di avvio, database di posta elettronica, directory **Documenti** e **Programmi** e del 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
```

*Esaminare gli oggetti elencati nel file **object2scan.txt**. Utilizzare il file di configurazione **scan_setting.txt**. Dopo la scansione, creazione di un rapporto con registrazione di tutti gli eventi:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_Impostazioni.txt /RA:scan.log
```

File di configurazione esemplificativo:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

13.4. Aggiornamenti del programma

La sintassi per l'aggiornamento dei moduli di programma di Kaspersky Anti-Virus for Windows Servers e degli elenchi delle minacce dalla riga di comando è la seguente:

```
avp.com UPDATE [<update_source>] [/R[A]:<report_file>]
[/C:<file_name>] [/APP=<on|off>]
```

Descrizione dei parametri:

<update_source>	Server HTTP o FTP o directory di rete per il download degli aggiornamenti. Il valore per il parametro può essere un percorso completo ad un'origine di aggiornamento o ad un URL. Se non viene selezionato un percorso, l'origine degli aggiornamenti sarà quella delle impostazioni di aggiornamento dell'applicazione.

/R[A]:<report_file>	**/R:<report_file>** - registra solo gli eventi importanti nel rapporto. **/R[A]:<file_report>** – registra tutti gli eventi nel rapporto. È possibile immettere un percorso assoluto o relativo al file. Se il parametro non è definito, i risultati di scansione sono visualizzati sullo schermo, insieme a 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 contenente l'insieme di parametri da riga di comando per l'aggiornamento del programma. È possibile immettere un percorso assoluto o relativo al file. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia di Kaspersky Anti-Virus for Windows Servers.
/APP=<on|off>	Abilita/disabilita gli aggiornamenti ai moduli del programma.

Esempi:

Aggiornamento dell'elenco dei virus e registrazione di tutti gli eventi nel rapporto:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Aggiornamento dei moduli di programma di Kaspersky Anti-Virus for Windows Servers applicando le impostazioni nel file di configurazione **updateapp.ini**:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

File di configurazione esemplificativo:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

13.5. Impostazioni di rollback

Sintassi del comando:

```
ROLLBACK [/R[A]:<report_file>]
[/password=<your_password>]
```

/R[A]:<report_file>	**/R:<report_file>** - registra solo gli eventi importanti nel rapporto. **/R[A]:<file_report>** – registra tutti gli eventi nel rapporto. È possibile immettere un percorso assoluto o relativo al file. Se il parametro non è definito, i risultati di scansione sono visualizzati sullo schermo, insieme a tutti gli eventi.
<your_password>	La password di accesso a Kaspersky Anti-Virus assegnata nell'interfaccia del programma.
Osservare che non è possibile eseguire questo comando senza digitare la password.	

Esempi:

```
avp.com ROLLBACK /RA:rollback.txt
[/password=<password>]
```

13.6. Esportazione delle impostazioni

Sintassi del comando:

```
avp.com EXPORT <profile> <file_name>
```

Descrizione dei parametri:

<profile>	File Anti-Virus o attività con le impostazioni da esportare. È possibile utilizzare qualsiasi valore per **<profile>**, elencato 13.2 a pag. 170.

<file_name>	Percorso al file in cui sono esportate le impostazioni di Kaspersky Anti-Virus for Windows Servers. È possibile inserire percorsi assoluti o relativi. Il file di configurazione viene salvato in formato binario (*.dat*, a meno che non venga specificato un altro formato o il formato non sia assegnato, e può essere utilizzato successivamente per importare le impostazioni dell'applicazione su altri computer. Il file di configurazione può essere salvato come file di testo. A tal fine, specificare l'estensione *.txt* nel nome del file. Si noti che non è possibile importare le impostazioni di protezione da un file di testo. Questo file può essere utilizzato solo per specificare le impostazioni principali per il funzionamento del programma.

Esempi:

```
avp.com EXPORT c:\settings.dat
```

13.7. Importazione delle impostazioni

Sintassi del comando:

```
avp.com IMPORT <file_name>
[/password=<your_password>]
```

<file_name>	Percorso verso il file dal quale vengono importate le impostazioni di Kaspersky Anti-Virus for Windows Servers. È possibile inserire percorsi assoluti o relativi. Le impostazioni possono essere importate solo da file binari. Se si installa il programma in modalità nascosta dalla riga di comando o con il l'Editor Oggetti delle Regole di gruppo, il nome del file di configurazione deve essere *install.cfg*. In caso contrario il programma non lo riconoscerà.

<your_password>	La password di Kaspersky Anti-Virus impostata dall'interfaccia del programma.
Si noti che questo comando non sarà accettato senza password	

Esempi:

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

13.8. Avvio del programma

Sintassi del comando:

```
avp.com
```

13.9. Arresto del programma

Sintassi del comando:

```
EXIT /password=<password>
```

<password>	La password di Kaspersky Anti-Virus impostata dall'interfaccia del programma.
Si noti che questo comando non sarà accettato senza password	

Osservare che non è possibile eseguire questo comando senza digitare la password.

13.10. Ottenere un file traccia

Potrebbe essere necessario un file traccia nel caso in cui ci siano problemi di runtime dell'applicazione, per consentire agli specialisti dell'assistenza tecnica di ricercare i problemi con maggiore precisione.

Sintassi del comando:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

[on|off]	Abilita/disabilita la creazione della traccia.
[file]	Ottenere una traccia e salvarla in un file.

<trace_level>	A questo parametro possono essere assegnati valori numerici compresi tra 0 (valore più basso, solo eventi critici) e 700 (valore più alto, tutti gli eventi). Quando viene inviata una richiesta all'assistenza tecnica, un esperto deve definire il livello di traccia richiesto. Se non viene specificato, il livello richiesto è 500.
Prudenza! La generazione del file traccia deve essere abilitata solo per risolvere un determinato problema. Tenere sempre attivata la funzione traccia può ridurre le prestazioni del computer e fare sì che il disco rigidi diventi pieno.	

Esempi:

Disabilitare la traccia:

```
avp.com TRACE file off
```

Generare un file traccia per l'assistenza tecnica con un livello di traccia massimo pari a 500:

avp.com TRACE file on 500

13.11. 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>
```

13.12. Codici restituiti dall'interfaccia a riga di comando

Questa sezione contiene un elenco di codici restituiti dalla riga di comando. I codici generali possono essere restituiti da qualsiasi comando dalla riga di

comando. I codici restituiti comprendono i codici generali e quelli specifici per un'attività di tipo specifico.

Codici restituiti generali:	
0	Operazione completata con successo
1	Valore non valido per l'impostazione
2	Errore sconosciuto
3	Errore di completamento dell'attività
4	Attività cancellata
Codici restituiti dall'attività di scansione anti-virus	
101	Tutti gli oggetti pericolosi sono stati elaborati
102	Rilevati oggetti pericolosi

CAPITOLO 14. MODIFICA, RIPARAZIONE E DISINSTALLAZIONE DEL PROGRAMMA

L'applicazione può essere disinstallata in due modi:

- tramite la procedura guidata d'installazione dell'applicazione (vedere 14.2 a pag. 187);
- dalla riga di comando (vedere 14.2 a pag. 187);
- tramite Kaspersky Administration Kit (vedere la Guida di distribuzione di Kaspersky Administration Kit);
- tramite le regole di dominio di gruppo di Microsoft Windows Server 2000/2003 (vedere 3.4.3 a pag. 35).

14.1. Modifica, riparazione e rimozione del programma tramite la procedura guidata d'installazione

In caso di errori di funzionamento dovuto a un'errata configurazione o alla corruzione dei file può rendersi necessario riparare il programma.

Per riparare o modificare i componenti assenti di Kaspersky Anti-Virus for Windows Servers o disinstallare il programma:

1. Inserire l'eventuale CD di installazione nell'unità CD-ROM (se utilizzato per installare il programma). Se Kaspersky Anti-Virus for Windows Servers è stato installato da una diversa origine (cartella ad accesso pubblico, cartella nel disco fisso, ecc.), verificare che l'origine specificata contenga il pacchetto di installazione e di potervi accedere.
2. Selezionare **Start→ Tutti i programmi→ Kaspersky Anti-Virus for Windows Servers 6.0 → 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. Finestra di avvio dell'installazione

Dopo aver eseguito tutti i passaggi sopra descritti, necessari per riparare o modificare il programma, si apre la finestra iniziale di installazione di Kaspersky Anti-Virus for Windows Servers. Fare clic sul pulsante **Avanti** per continuare.

Passaggio 2. Selezione di un'operazione

In questa fase viene richiesto di selezionare l'operazione che si desidera eseguire. È possibile modificare i componenti del programma, riparare quelli già installati, rimuoverli o disinstallare completamente il 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 personalizzata, in cui è possibile specificare quali componenti si desidera installare (vedere Passaggio 7 a pag. 25) 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 sicurezza Consigliato.

Attenzione!

Se Kaspersky Anti-Virus 6.0 viene installato in remoto, il server non riparte automaticamente. Tuttavia, per rimuovere completamente i componenti dell'applicazione e per fare in modo che il computer operi correttamente in futuro, si raccomanda di riavviare manualmente.

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 for Windows Servers, selezionare ◉ **Disinstallazione completa**. Per salvare i dati, selezionare ◉ **Salva oggetti dell'applicazione** e specificare quali oggetti non eliminare dall'elenco:

- *Dati di attivazione* – informazioni sull'attivazione del programma.
- *Elenchi delle minacce* – serie completa delle firme di programmi pericolosi, virus e altre minacce correnti all'ultimo aggiornamento.
- *File di backup* – copie di backup di oggetti eliminati o disinfettati. Si consiglia di salvarli per poterli eventualmente ripristinare in un secondo momento.

- *File in 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 consiglia di salvare questi file poiché potrebbero non essere effettivamente infetti, oppure essere riparati dopo l'aggiornamento degli elenchi delle minacce.
- *Impostazioni dell'applicazione* - le configurazioni di File Anti-Virus.
- *Dati iSwift* – database con informazioni sugli oggetti esaminati nei file system NTFS, che può aumentare la velocità di scansione. Quando usa questo database, Kaspersky Anti-Virus for Windows Servers esamina solo i file che hanno subito modifiche in seguito all'ultima scansione.

Attenzione!

Se trascorre un lungo periodo di tempo tra la disinstallazione di una versione di Kaspersky Anti-Virus for Windows Servers e l'installazione di un'altra, si sconsiglia di utilizzare il database *iSwift* di un'installazione 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 3. 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**.

14.2. Disinstallazione del programma da riga di comando

Per disinstallare Kaspersky Anti-Virus 6.0 for Windows Servers dalla riga di comando, digitare:

```
msiexec /x <package_name>
```

Si apre la procedura di installazione guidata. Essa consente di disinstallare l'applicazione (vedere la Capitolo 14 a pag. 184).

Per disinstallare l'applicazione in modalità non interattiva senza riavviare il computer, (il computer deve essere riavviato manualmente dopo la disinstallazione), digitare:

```
msiexec /x <package_name> /qn
```

Per disinstallare l'applicazione in background e dopo riavviare il computer, digitare:

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

Se durante l'installazione si è scelto di proteggere il programma dalla disinstallazione tramite una password, è necessario inserire tale password. In caso contrario, sarà impossibile disinstallare il programma.

Per rimuovere l'applicazione inserendo una password come dimostrazione dell'autorizzazione a disinstallare, inserire:

`msiexec /x <package_name> KLUNINSTPASSWD=******` – per rimuovere l'applicazione in modalità interattiva;

`msiexec /x <package_name> KLUNINSTPASSWD=****** /qn` – per rimuovere l'applicazione in modalità non interattiva.

APPENDICE A. INFORMAZIONI DI RIFERIMENTO

Questa appendice contiene materiale di riferimento sui formati dei file e le maschere delle estensioni utilizzate nelle impostazioni di Kaspersky Anti-Virus for Windows Servers.

A.1. Elenco dei file esaminati in base all'estensione

Se si seleziona **Programmi e documenti (per estensione)**, File Anti-Virus sottopone a un'approfondita scansione antivirus i file con le estensioni sotto elencate.

com – file eseguibile per un programma

exe – file eseguibile o archivio autoestraente

sys – driver di sistema

prg – testo programma per un programma dBase, Clipper o Microsoft Visual FoxPro, o WAVmaker

bin – file binario

bat – file batch

cmd – riga di comando per Microsoft Windows NT (simile a un file .bat per DOS), OS/2.

dpl – libreria compressa Borland Delphi

dll – libreria a caricamento dinamico

scr – splash screen di Microsoft Windows

cpl – modulo del pannello di controllo di Microsoft Windows

ocx – oggetto OLE Microsoft (Object Linking and Embedding)

tsp – programma che si esegue in modalità a ripartizione di tempo

drv – driver dispositivo

vxd – driver dispositivo virtuale Microsoft Windows

pif – file di informazione programma

lnk – file di collegamento Microsoft Windows

reg – file della chiave di registro del sistema di Microsoft Windows

ini – file di inizializzazione

cla – classe Java

vbs – script Visual Basic

vbe – estensione video BIOS

js, jse – testo sorgente JavaScript

htm – documento ipertestuale

htt – intestazione ipertesto Microsoft Windows

hta – programma di ipertesto per Microsoft Internet Explorer

asp – script Active Server Pages

chm – file HTML compilato

pht – HTML con script PHP incorporati

php – script incorporato in file HTML

wsh – file di Windows Script Host

wsf – script Microsoft Windows

the – sfondo desktop Microsoft Windows 95

hlp – file della guida di Windows

eml – file di posta elettronica Microsoft Outlook Express

nws – nuovo file di posta elettronica Microsoft Outlook Express

msg – file di posta elettronica Microsoft Mail

plg – posta elettronica

mbx – estensione per messaggi di posta elettronica salvati in Microsoft Office Outlook

*doc** - un documento di Microsoft Word, come: *doc* – un documento di Microsoft Word , *docx* – un documento di Microsoft Word 2007 con supporto XML, *docm* – un documento di Microsoft Word 2007 con supporto alle macro

*dot** – un modello di documento Microsoft Word, come *dot* – un modello di documento Microsoft Word, *dotx* – un modello di documento Microsoft Word 2007, *dotm* – un modello di documento Microsoft Word 2007 con supporto alle macro

fpm – programma di database, file di avvio di Microsoft Visual FoxPro

rtf – documento in Rich Text Format

shs – frammento di gestore di eventi oggetti Shell Scrap

dwg – database blueprint AutoCAD

msi – pacchetto di Microsoft Windows Installer

otm – progetto VBA per Microsoft Office Outlook

pdf – documento di Adobe Acrobat

swf – file di Shockwave Flash

jpg, jpeg, png – formato compresso delle immagini

emf – formato Enhanced Metafile, prossima generazione dei metafile del sistema operativo Microsoft Windows. I file EMF non sono supportati da Microsoft Windows a 16 bit.

ico – file icona

ov? – file eseguibili Microsoft DOC

*xl** - documenti e file di Microsoft Office Excel, come: *xla* - estensione Microsoft Office Excel, *xlc* - diagramma, *xlt* - modelli di documento. *xlsx* – un documento di lavoro Microsoft Excel 2007, *xltm* – un documento di lavoro Microsoft Excel 2007 con supporto alle macro, *xlsb* – un documento Microsoft Excel 2007 in formato binario (non XML), *xltx* – un modello di documento Microsoft Excel 2007, *xlsm* – un modello di documento Microsoft Excel 2007 con supporto alle macro, *xlam* – un plug-in di Microsoft Excel 2007 con supporto alle macro.

*xl** - documenti e file di Microsoft Office Excel, come: *xla* - estensione Microsoft Office Excel, *xlc* - diagramma, *xlt* - modelli di documento. *xlsx* – un documento di lavoro Microsoft Excel 2007, *xltm* – un documento di lavoro Microsoft Excel 2007 con supporto alle macro, *xlsb* – un documento Microsoft Excel 2007 in formato binario (non XML), *xltx* – un modello di documento Microsoft Excel 2007, *xlsm* – un modello di documento Microsoft Excel 2007 con supporto alle macro, *xlam* – un plug-in di Microsoft Excel 2007 con supporto alle macro.

*md** - Documenti e file di Microsoft Office Access, come: *mda* - Gruppo di lavoro, mdb - database, ecc. di Microsoft Office Access

sldx – una diapositiva di Microsoft PowerPoint 2007.

sldm – una diapositiva di Microsoft PowerPoint 2007 con supporto alle macro.

thmx – un tema di Microsoft Office 2007.

Si tenga presente che il formato effettivo di un file può non corrispondere al formato indicato dall'estensione.

A.2. Maschere di esclusione file possibili

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
- **test** – tutti i file con estensione *.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 nella cartella *C:\dir*
  - **C:\dir*.ex?** – tutti i file con estensione .ex? nella cartella *C:\dir\,* dove ? può rappresentare qualsiasi carattere
  - **C:\dir\test** – solo il file *C:\dir\test*
  - Se si desidera che il programma non scansioni i file nelle sottocartelle di questa cartella, deselezionare ☑ **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 *prova* nelle cartelle *dir*
  - **dir*.exe** – tutti i file con estensione *exe* in tutte le cartelle *dir*
  - **dir*.ex?**– tutti i file con estensione .ex? in tutte le cartelle di *C:\dir\,* dove ? rappresenta qualsiasi carattere

  Se si desidera che il programma non esamini i file nelle sottocartelle di questa cartella, deselezionare ☑ **Includi sottocartelle** durante la creazione della maschera.

Suggerimento:

Le maschere di esclusione *.* e * possono essere usate esclusivamente se si assegna ad una minaccia il verdetto previsto dalla Virus Encyclopedia. In caso contrario, la minaccia specificata non sarà rilevata in alcun oggetto. L'uso di queste maschere senza selezionare un verdetto disabilita il monitoraggio.

Si sconsiglia inoltre di selezionare un'unità virtuale creata sulla base di una directory di file system usando il comando *subst* come 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 possibili utilizzando la classificazione della Virus Encyclopedia

Quando si aggiungono come esclusioni le minacce con un determinato stato tratto dalla classificazione dell'enciclopedia dei virus, è possibile specificare:

- il nome completo della minaccia come indicata nella Virus Encyclopedia sul collegamento www.viruslist.com (per esempio, **not-a-virus:RiskWare.RemoteAdmin.RA.311** o **Flooder.Win32.Fuxx**);
- nome della minaccia in base alla maschera. Per esempio:
  - **not-a-virus*** – esclude dalla scansione potenziali programmi pericolosi e joke.
  - ***Riskware.*** - esclude il riskware dalla scansione.
  - ***RemoteAdmin.*** - esclude tutti i programmi di amministrazione remota dalla scansione.

A.4. Panoramica delle impostazioni in *setup.ini*

Il file *setup.ini*, ubicato nella cartella d'installazione di Kaspersky Anti-Virus, viene utilizzato durante l'installazione del programma in modalità non interattiva dalla riga di comando (vedere 3.3 a pag. 33) o tramite l'Editor Oggetti delle Regole di gruppo (vedere 3.4 a pag. 34). Il file contiene le seguenti impostazioni:

[Setup] – impostazioni generali per l'installazione del programma.

InstallDir=<percorso alla cartella d'installazione del programma>.

Reboot=yes|no – stabilisce se riavviare o meno il computer al termine dell'installazione (non viene riavviato per impostazione predefinita).

SelfProtection=yes|no – stabilisce se Kaspersky Anti-Virus deve abilitare l'Autodifesa durante l'installazione (abilitata per impostazione predefinita).

MSExclusions=yes|no – stabilisce se aggiungere o meno le esclusioni consigliate da Microsoft all'elenco di esclusioni di Kaspersky Anti-Virus.

AddPath=yes|no – stabilisce se il percorso a avp.com debba essere aggiunto alla variabile ambientale di sistema %Path%.

[Components] – seleziona i componenti da installare. Se questo gruppo non contiene elementi, verranno installati tutti i componenti.

FileMonitor=yes|no – installa File Anti-Virus.

[Tasks] – abilita le attività di Kaspersky Anti-Virus. Se non vengono specificate attività, dopo l'installazione verranno eseguite tutte. Se vengono specificate attività, tutte quelle non elencate saranno disabilitate.

ScanMyComputer=yes|no – attività che prevede la scansione completa del computer

ScanStartup=yes|no – attività di scansione degli oggetti di avvio

ScanCritical=yes|no – attività di scansione delle aree critiche

Updater=yes|no – attività di aggiornamento dell'elenco delle minacce e dei moduli del programma

Anziché il valore **yes**, è possibile utilizzare i valori **1**, **on**, **enable**, o **enabled**, e invece di **no** è possibile utilizzare – **0**, **off**, **disable**, o **disabled** .

APPENDICE B. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è ormai un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce un'ampia gamma di software per la sicurezza dei dati e fornisce soluzioni complete e ad elevate prestazioni per proteggere computer e reti da tutti i tipi di programmi nocivi, posta elettronica indesiderata e attacchi degli hacker.

Kaspersky Lab è un azienda internazionale, con sede nella Federazione Russa e uffici di rappresentanza nel Regno Unito ed in 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 450 esperti, tutti specializzati in tecnologie antivirus, 10 dei quali in possesso di laurea in amministrazione aziendale, 16 di specializzazione postlaurea, e due appartenenti alla 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 14 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus informatici consente all'azienda di offrire una protezione completa contro le 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 hanno fatto dell'azienda uno dei 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 per la protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, file server, sistemi di posta elettronica, firewall, gateway Internet e palmari. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'azienda. Numerose imprese di grande notorietà utilizzano Kaspersky Anti-Virus, tra cui Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India), BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di un'ampia gamma di servizi supplementari volti a garantire non solo un funzionamento stabile dei prodotti dell'azienda, ma anche 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 24 ore su 24, disponibile in diverse lingue per soddisfare le esigenze di una clientela internazionale.

B.1. Altri prodotti Kaspersky Lab

Kaspersky Lab News Agent

News Agent è progettato per comunicare tempestivamente le notizie pubblicate da Kaspersky Lab, per le notifiche relative allo status corrente dell'attività dei virus e per notizie fresche. Il programma legge l'elenco dei canali di news disponibili ed il loro contenuto dai news server di Kaspersky Lab ad intervalli specificati.

News Agent consente agli utenti di:

- Vedere le previsioni correnti in materia di virus nell'aria di notifica
- Iscriversi ai newsfeed ed annullare l'iscrizione
- Recupera le notizie da ciascun canale selezionato agli intervalli specificati, e notifica la presenza di notizie fresche
- Rivedere le notizie sui canali specificati
- Rivedere l'elenco dei canali ed il loro stato
- Aprire l'intero testo dell'articolo nel browser

News Agent è un'applicazione autonoma di Microsoft Windows, che può essere utilizzata indipendentemente o in congiunzione con diverse 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 viene eseguito direttamente dal browser. In questo modo, l'utente riceve una risposta rapida alle domande riguardanti potenziali infezioni del computer in uso. Questo servizio consente agli utenti di:

- Escludere gli archivi e i database di posta dalla scansione
- Selezionare il database standard/esteso per la scansione
- Salvare un rapporto sui risultati della scansione in formato .txt o .html

Kaspersky® OnLine Scanner Pro

Questo programma è un servizio a pagamento offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer e di disinfettare i file pericolosi. Kaspersky OnLine Scanner Pro viene eseguito direttamente dal browser. Questo servizio consente agli utenti di:

- Escludere gli archivi e i database di posta dalla scansione
- Selezionare il database standard/esteso per la scansione
- Salvare un rapporto sui risultati della scansione in formato .txt o .html

Kaspersky® Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 è progettato per proteggere i personal computer dal software nocivo grazie a una combinazione ottimale di metodi di protezione antivirus convenzionali e nuove tecnologie proattive.

Il programma offre complesse verifiche antivirus, fra cui:

- Scansione antivirus del traffico e-mail al livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in arrivo, e SMTP per quella in uscita) indipendentemente dal client di posta usato, nonché riparazione dei database di posta.
- Scansione antivirus in tempo reale del traffico Internet trasferito mediante HTTP.
- Scansione antivirus di singoli file, cartelle o unità. Inoltre è possibile usare un'attività di scansione preimpostata per iniziare l'analisi antivirus esclusivamente delle aree critiche del sistema operativo e degli oggetti ad esecuzione automatica di Microsoft Windows.

La protezione proattiva offre le seguenti funzioni:

Controlla le modifiche nel file system. Il programma consente agli utenti di creare un elenco di applicazioni che controllerà in base ai componenti. Aiuta a proteggere l'integrità delle applicazioni dall'influsso del software nocivo.

Monitora i processi nella RAM. Kaspersky Anti-Virus 7.0 avvisa tempestivamente gli utenti ogni volta che rileva processi pericolosi, sospetti o nascosti, o nei casi in cui si siano verificate variazioni non autorizzate dei processi attivi.

Monitora le variazioni del registro del SO grazie al controllo interno del registro di sistema.

Il controllo dei processo nascosti favorisce la protezione dai codici nocivi nascosti nel sistema operativo tramite le tecnologie rootkit.

Analizzatore euristico. Durante la scansione di un programma, l'analizzatore ne emula l'esecuzione e registra tutta l'attività sospetta, come l'apertura o la scrittura in un file, l'interruzione di intercettazioni vettoriali, ecc. La reazione viene presa in base a tale procedura in relazione a possibili infezioni del programma con un virus. L'emulazione ha luogo in un ambiente virtuale isolato, che protegge con affidabilità il computer dalle infezioni.

Ripristina il sistema dopo attacchi da parte di software nocivi tenendo traccia di tutte le modifiche al registro ed al file system del computer, e le annulla a discrezione dell'utente.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 è una soluzione integrata per la protezione dei personal computer dalle principali minacce alle informazioni (virus, hacker, spam e spyware). Una singola interfaccia consente agli utenti di configurare e gestire tutti i componenti del programma.

Le funzioni di protezione anivirus includono:

Scansione antivirus del traffico e-mail al livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in arrivo, e SMTP per quella in uscita) indipendentemente dal client di posta usato, nonché riparazione dei database di posta. Il programma include plug-in per i client di posta più utilizzati (come Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail), e TheBat!) e supporta la disinfezione dei loro database di posta.

Scansione antivirus in tempo reale del traffico Internet trasferito mediante HTTP.

Protezione del file system: scansione antivirus di singoli file, cartelle o unità. Inoltre l'applicazione è in grado di eseguire l'analisi antivirus esclusivamente delle aree critiche del sistema operativo e degli oggetti di avvio di Microsoft Windows.

Difesa proattiva: il programma monitora costantemente l'attività delle applicazioni e dei processi in esecuzione nella RAM, impedendo modifiche pericolose al file system ed al registro, e ripristina il sistema dopo gli effetti dei programmi nocivi.

La protezione dalle frodi via Internet è garantita grazie al riconoscimento degli attacchi di phishing, il che previene le perdite di dati riservati (innanzitutto, le password ed i numeri di di numero di conto bancario e di carta di credito) e blocca l'esecuzione di script pericolosi su pagine Web, finestre pop-up e banner pubblicitari. La funzione di **blocco autodialer** aiuta a identificare il software che cerca di utilizzare il modem per connessioni nascoste non autorizzate a servizi telefonici a pagamento ed impedisce tali attività. Il modulo *Privacy Control* protegge i dati riservati da accessi e trasmissioni non autorizzate. *Parental Control* è un componente di Kaspersky Internet Security che monitora l'accesso degli utenti a Internet.

Kaspersky Internet Security 7.0 **registra i tentativi di scansione delle porte del computer**, che spesso precedono gli attacchi di rete, e difende con successo dai tipici attacchi di rete. Il programma utilizza **regole definite come base** per il controllo di tutte le transazioni di rete, controllando **tutti i pacchetti di dati in entrata ed in uscita**. La **modalità Stealth** (basata sulla tecnologia

SmartStealth™) **impedisce il rilevamento del computer dall'esterno**. In modalità Stealth , il sistema blocca tutte le attività di rete tranne le poche transazioni autorizzate nelle regole definite dall'utente.

Il programma utilizza un approccio omnicomprensivo al filtraggio spam dei messaggi e-mail in entrata:

- Verifica a fronte di liste nere e bianche di destinatari (tra cui gli indirizzi dei siti di phishing)
- Ispezione delle frasi nel corpo del messaggio
- Analisi del testo del messaggio tramite un algoritmo ad apprendimento automatico
- Riconoscimento della spam inviata in file immagine

Kaspersky Anti-Virus Mobile

Kaspersky ® Anti-Virus Mobile garantisce la protezione antivirus ai dispositivi mobili che eseguono Symbian OS e Microsoft Windows Mobile. Il programma offre la scansione antivirus completa, che comprende:

- **Scansioni manuali** della memoria del dispositivo mobile, delle memory card e delle singole cartelle, oppure di file specifici; se viene rilevato un file infetto, esso viene spostato in quarantena o eliminato
- **Scansione in tempo reale –** tutti i file in entrata ed in uscita vengono esaminati automaticamente, come anche tutti i file ai quali si cerca di accedere
- **Protezione dallo spam via SMS**

Kaspersky Anti-Virus for File Servers

Questo pacchetto software offre un'affidabile protezione ai file system dei server che utilizzano Microsoft Windows, Novell NetWare, Linux e Samba da tutti i tipi di software nocivo. La suite include le seguenti applicazioni di 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 del server vengono esaminati all'apertura o al salvataggio sul server;
- *Previene le pandemie di virus*;
- *Scansioni manuali* dell'intero file system o di singoli file e singole unità e cartelle;
- *Uso di tecnologie di ottimizzazione* durante la scansione di oggetti nel file system del server;
- *Ripristino del sistema dopo attacchi da parte di virus*;
- *Scalabilità del pacchetto software* nell'ambito delle risorse di sistema disponibili;
- *Monitoraggio dell'equilibrio del carico sul sistema*;
- *Creazione di un elenco di processi attendibili* la cui attività sul server non è soggetta a controllo da parte del pacchetto software;
- *Amministrazione remota* del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;
- *Salvataggio delle copie di backup degli oggetti infetti ed eliminati* per poterli ripristinare;
- *Messa in quarantena degli oggetti sospetti*;
- *Invio di notifiche sugli eventi* che si verificano nel programma all'amministratore;
- *Registrazione di rapporti dettagliati*;
- *Aggiornamento automatico* dei database del programma.

Kaspersky Open Space Security

Kaspersky Open Space Security è un pacchetto software con un approccio nuovo alla sicurezza per le reti aziendali moderne di qualsiasi dimensione, che offre la protezione centralizzata ai sistemi informati ed il supporto per gli uffici remoti e gli utenti mobili.

La suite comprende quattro programmi:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Le specifiche di ciascun programma sono riportate di seguito.

Kaspersky WorkSpace Security è un programma destinato alla protezione centralizzata delle workstation all'interno ed all'esterno di reti aziendali da tutte le attuali minacce di Internet (virus, spyware, attacchi di hacker, spam).

Caratteristiche e funzionalità:

- *Protezione completa da virus, spyware, attacchi degli hacker e spam*;
- *Difesa proattiva da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database;*
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker;*
- *Ripristino del sistema dopo modifiche nocive;*
- *Protezione dagli attacchi di phishing e dalla posta indesiderata;*
- *Distribuzione dinamica delle risorse durante le scansioni complete del sistema;*
- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Supporto per Cisco® NAC (Network Admission Control);*
- *Scansione antivirus della posta elettronica e del traffico Internet in tempo reale;*
- *Blocco delle finestre pop-up e dei banner pubblicitari su Internet;*
- *Funzionamento sicuro in qualsiasi tipo di rete, tra cui il Wi-Fi;*
- *Strumenti di creazione dei dischi di ripristino che consentono di ripristinare il sistema dopo una pandemia di virus;*
- *Sistema di reporting completo sullo stato della protezione;*
- *Aggiornamenti automatici al database;*
- *Supporto completo per sistemi operativi a 64 bit;*
- *Ottimizzazione delle prestazioni del programma per PC portatili (tecnologia Intel® Centrino® Duo);*
- *Capacità di disinfezione remota (Intel® Active Management, Intel® vPro™).*

Kaspersky Business Space Security garantisce la protezione ottimale delle risorse informative dell'azienda dalle minacce attuali su Internet. Kaspersky Business Space Security protegge le workstation ed i file server da tutti i tipi di

minacce, trojan, e worm, previene le pandemie di virus e protegge le informazioni garantendo nel contempo un accesso istantaneo alle risorse di rete per gli utenti.

Caratteristiche e funzionalità:

- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Supporto per Cisco® NAC (Network Admission Control);*
- *Protezione delle workstation e dei server da tutti i tipi di minacce su Internet;*
- *Tecnologia iSwift per evitare di ripetere la scansione dei file nella rete;*
- *Distribuzione del carico tra i processori del server;*
- *Messa in quarantena degli oggetti sospetti dalle workstation;*
- *Ripristino del sistema dopo modifiche nocive;*
- *Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;*
- *Difesa proattiva per le workstation da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database;*
- *Scansione antivirus della posta elettronica e del traffico Internet in tempo reale;*
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker;*
- *Protezione durante l'utilizzo di reti Wi-Fi;*
- *Autodifesa da programmi pericolosi;*
- *Messa in quarantena degli oggetti sospetti;*
- *Aggiornamenti automatici al database.*

Kaspersky Enterprise Space Security

Questo programma include i componenti per la protezione delle workstation e dei server collegati dalle attuali minacce su Internet. Elimina i virus dalla posta elettronica, proteggendo le informazioni e garantendo un accesso sicuro alle risorse di rete per gli utenti.

Caratteristiche e funzionalità:

- *Protezione delle workstation e dei file server da virus, trojan, e worm;*
- *Protezione dei server di posta Sendmail, Qmail, Postfix e Exim;*
- *Scansione dei messaggi di posta elettronica su Microsoft Exchange Server, comprese le cartelle condivise;*
- *Elaborazione di messaggi di posta elettronica ed altri oggetti per server Lotus Domino;*
- *Protezione dagli attacchi di phishing e dalla posta indesiderata;*
- *Prevenzione degli invii in massa e delle pandemie di virus;*
- *Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;*
- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Supporto per Cisco® NAC (Network Admission Control);*
- *Difesa proattiva per le workstation da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database;*
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker;*
- *Funzionamento sicuro durante l'utilizzo di reti Wi-Fi;*
- *Scansione del traffico Internet in tempo reale;*
- *Ripristino del sistema dopo modifiche nocive;*
- *Distribuzione dinamica delle risorse durante le scansioni complete del sistema;*
- *Messa in quarantena degli oggetti sospetti;*
- *Sistema di reporting completo sullo stato della protezione del sistema;*
- *Aggiornamenti automatici al database.*

Kaspersky Total Space Security

Questa soluzione monitora tutti i flussi di dati in entrata ed uscita (posta elettronica, Internet e tutte le interazioni di rete). Include componenti per la protezione di workstation e dispositivi mobili, protegge le informazioni garantendo nel contempo agli utenti un accesso sicuro alle fonti informative dell'azienda ed a Internet, e garantisce comunicazioni di posta elettronica sicure.

Caratteristiche e funzionalità:

- *Protezione completa da virus, spyware, attacchi degli hacker e spam a tutti i livelli della rete aziendale, dalle workstation ai gateway Internet;*
- *Difesa proattiva per le workstation da nuovi programmi pericolosi le cui firme non sono ancora state aggiunte al database;*
- *Protezione dei server di posta e dei servizi correlati;*
- *Scansione del traffico Internet (HTTP/FTP) in entrata nella rete locale in tempo reale;*
- *Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;*
- *Blocco dell'accesso delle workstation infette;*
- *Previene le pandemie di virus;*
- *Reporting centralizzato sullo stato di protezione;*
- *Amministrazione remota del pacchetto software, compresa l'installazione, la configurazione e l'amministrazione centralizzata;*
- *Supporto per Cisco® NAC (Network Admission Control);*
- *Supporto per i server proxy di tipo hardware;*
- *Filtraggio del traffico Internet tramite un elenco di server affidabili, tipi di oggetti e gruppi di utenti;*
- *Tecnologia iSwift per evitare di ripetere la scansione dei file nella rete;*
- *Distribuzione dinamica delle risorse durante le scansioni complete del sistema;*
- *Personal Firewall con sistema di rilevamento delle intrusioni e avvisi per gli attacchi degli hacker;*
- *Funzionamento sicuro per gli utenti in qualsiasi tipo di rete, tra cui il Wi-Fi;*
- *Protezione dagli attacchi di phishing e dalla posta indesiderata;*
- *Capacità di disinfezione remota (Intel® Active Management, Intel® vPro™);*
- *Ripristino del sistema dopo modifiche nocive;*
- *Autodifesa da programmi pericolosi;*
- *Supporto completo per sistemi operativi a 64 bit*;

- *Aggiornamenti automatici al database*.

Kaspersky Security for Mail Servers

Questo programma protegge i server di posta ed i server collegati dai programmi nocivi e dalla posta spam. Il programma comprende le applicazioni in grado di proteggere tutti i server di posta standard (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix ed Exim) e consente di configurare un gateway di posta elettronica dedicato. La soluzione comprende:

- 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 funzioni comprendono:

- *Protezione affidabile dai programmi nocivi o potenzialmente pericolosi*;
- *Filtraggio della posta indesiderata*;
- *La scansione della posta in entrata ed in uscita, nonché degli allegati*;
- *Scansione antivirus dei messaggi di posta elettronica su* Microsoft Exchange Server, comprese le cartelle condivise;
- *Elaborazione di messaggi di posta elettronica, database ed altri oggetti per server Lotus Domino*;
- *Filtraggio* della posta elettronica in base agli allegati;
- *Messa in quarantena* degli oggetti sospetti;
- *Sistema di amministrazione del programma* molto semplice;
- *Previene le pandemie di virus*;
- *Monitoraggio del sistema di protezione* tramite notifiche;
- *Sistema di reporting* per il funzionamento del programma;
- Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;
- *Aggiornamenti automatici al database*.

Kaspersky Security for Internet Gateways

Questo programma garantisce l'accesso sicuro ad Internet per tutti i dipendenti di un'organizzazione, eliminando automaticamente i programmi nocivi e pericolosi dai dati in entrata tramite HTTP/FTP. La soluzione comprende:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Le sue funzioni comprendono:

- *Protezione affidabile dai programmi nocivi o potenzialmente pericolosi*;
- *Scansione del traffico Internet* (HTTP/FTP) in tempo reale;
- *Filtraggio del traffico Internet* tramite un elenco di server affidabili, tipi di oggetti e gruppi di utenti;
- *Messa in quarantena* degli oggetti sospetti;
- *Sistema di amministrazione semplice da utilizzare*;
- *Sistema di reporting per il funzionamento del programma*;
- *Supporto per i server proxy di tipo hardware*;
- Scalabilità del pacchetto software nell'ambito delle risorse di sistema disponibili;
- *Aggiornamenti automatici al 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 la rivoluzionaria tecnologia di analisi linguistica con metodi moderni di filtraggio della posta elettronica, tra cui le liste nere DNS e le caratteristiche delle lettere formali. L'esclusiva combinazione di servizi consente agli utenti di identificare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, Kaspersky® Anti-Spam è una barriera alla posta non desiderata controllando tutta la posta in entrata alla ricerca di spam. Il software è compatibile con qualsiasi sistema di posta già in uso presso il cliente, e può essere installato sia su server mail esistenti sia su server dedicati.

L'elevato grado di efficacia di Kaspersky® Anti-Spam è garantito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i

campioni forniti dagli specialisti del laboratorio linguistico dell'azienda. I database vengono aggiornati ogni 20 minuti.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper garantisce scansioni antivirus ad alta velocità del traffico su server che eseguono Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

Il programma è un plug-in ed esamina in tempo reale i messaggi e-mail in entrata ed in uscita alla ricerca di virus e processi..

B.2. Recapiti

Per domande, commenti e suggerimenti, rivolgetevi a un nostro distributore o direttamente a Kaspersky Lab. Saremo lieti di aiutarvi per qualsiasi questione legata ai nostri prodotti, per telefono o via posta elettronica. Tutte le raccomandazioni e i suggerimenti pervenuti saranno presi in considerazione e valutati con attenzione.

Assistenza tecnica	Per qualsiasi informazione relativa al supporto tecnico, visitare la pagina 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 Posta elettronica: info@kaspersky.com

APPENDICE C. CONTRATTO DI LICENZA

Contratto di licenza standard per 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 FOR WINDOWS SERVERS 6.0 ("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.

CONFORMEMENTE ALLA NORMATIVA RELATIVA AL SOFTWARE KASPERSKY PER SINGOLI UTENTI ACQUISTATO SCARICANDO IL FILE DAL SITO WEB DI KASPERSKY LAB O DEI SUOI PARTNER, IL CLIENTE PUÒ RESTITUIRE IL PRODOTTO AL RIVENDITORE PER LA SOSTITUZIONE O IL RIMBORSO COMPLETO ENTRO QUATTORDICI (14) GIORNI LAVORATIVI DALLA DATA DELL'ACQUISTO, A PATTO CHE LA CONFEZIONE NON SIA STATA APERTA.

IL SOFTWARE KASPERSKY PER UTENTI SINGOLI NON ACQUISTATO ONLINE SU INTERNET NON PUÒ ESSERE RESTITUITO PER IL RIMBORSO NÉ PER LA SOSTITUZIONE SE NON DIVERSAMENTE STABILITO DAL PARTNER CHE RIVENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON È VINCOLATO DALLE CLAUSOLE STABILITE DAL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SPETTA SOLO ALL'ACQUIRENTE ORIGINARIO.

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.

1.1 *Uso*. Il numero di computer dell'utente che può essere protetto dal Software è specificato nel file chiave di licenza ed indicato nella finestra "Servizio". Il software non può essere utilizzato per proteggere reti con un numero di server superiore a tale numero.

1.1.1 Il Software è "in uso" su un computer quando è caricato nella memoria temporanea (vale a dire nella memoria ad accesso casuale o RAM) o è installato nella memoria permanente (per esempio disco fisso, CD-ROM, o altro dispositivo di memoria) 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 backup, 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 i computer dai virus la cui firma sia contenuta nel database degli elenchi delle minacce disponibile presso i server di aggiornamento di Kaspersky Lab.

1.1.3 Qualora l'utente venda il computer su cui è installato il Software, dovrà assicurarsi che tutte le copie del Software siano state cancellate.

1.1.4 All'utente è fatto divieto di decompilare, reingegnerizzare, disassemblare o altrimenti ridurre qualsiasi parte del presente Software a una forma leggibile dall'uomo e di permettere a terzi di compiere tali azioni. Le informazioni di interfaccia necessarie per ottenere l'interoperatività del software con programmi per computer creati indipendentemente sarà fornita da Kaspersky Lab dietro richiesta e dietro pagamento dei ragionevoli costi e delle spese sostenute per procurarsi e fornire tali informazioni. Qualora Kaspersky Lab notificasse al cliente che, per qualsiasi ragione, inclusa senza tuttavia ad essa limitarsi quella dei costi, non intende fornire tali informazioni, l'utente sarà autorizzato a intraprendere le azioni necessarie per ottenere l'interoperatività a condizione di eseguire le operazioni di decompilazione o reverse engineering entro i limiti previsti dalla legge.

1.1.5 L'utente non deve effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software, né creare opere da esso derivate derivate, né permettere a terzi di copiarlo (in modo diverso da quanto espressamente permesso nel presente documento).

1.1.6 All'utente è fatto divieto di affittare, noleggiare o prestare il Software a terzi oltre che di trasferire o di fornire a terzi la licenza in concessione.

1.1.7 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.

1.1.8 Kaspersky Lab può richiedere all'utente di installare la versione più recente del Software (la versione più recente nonché il più recente pacchetto di manutenzione).

1.1.9 Rimozione dei prodotti potenzialmente pericolosi. L'utente riconosce e concorda che, oltre al rilevamento del software dannoso e nocivo, il Prodotto possa anche identificare, rimuovere e/o disabilitare i prodotti potenzialmente pericolosi, tra cui quelli considerati o classificati come Adware, Riskware, Pornware, ecc.

2. *Assistenza*.

(i) Kaspersky Lab fornirà all'utente i servizi di assistenza ("Servizi di assistenza") di seguito definiti per il periodo specificato nel File chiave di licenza e indicato nella finestra "Servizio", a partire dalla data di acquisto, dietro:

  (a) pagamento della tariffa di assistenza corrente; e

  (b) Il Servizio di assistenza di Kaspersky Lab ha inoltre diritto di richiedere all'utente finale ulteriore identificazione per assegnare l'identificatore che dà diritto ai Servizi di Assistenza.

  (c) Fino all'attivazione del software e/o all'ottenimento dell'identificatore dell'utente finale (ID cliente) il servizio di assistenza presterà 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, 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 intende:

  (a) Aggiornamenti orari del database antivirus

  (b) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione

(c) Assistenza tecnica tramite Internet o linea telefonica dedicata forniti dal distributore e/o dal rivenditore;

(d) Aggiornamenti per la rilevazione e la disinfezione dei virus 24 ore su 24.

(v) I servizi di assistenza vengono forniti solo se e quando sul computer dell'utente è installata l'ultima versione del Software come disponibile sul sito Web ufficiale di Kaspersky Lab (www.kaspersky.com).

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 sei (6) mesi a decorrere dal primo download o processo d'installazione, il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzionalità descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione stessa.

(ii) L'utente si assume ogni responsabilità in merito alla scelta del presente Software per le proprie esigenze. 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) (iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente riportare erroneamente un virus in un titolo non infettato da quel virus.

(iv) Kaspersky Lab non garantisce la protezione fornita dal Software dopo la data di scadenza (vedere la sezione.2 (i))

(v) 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.

(vi) 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.

(vii) Le garanzie e le condizioni specificate in questo Contratto sostituiscono qualsiasi altra condizione, garanzia o termine relativi alla fornitura o alla presunta fornitura, all'impossibilità di fornire o al ritardo nella fornitura del Software o della Documentazione che, se non fosse per questo paragrafo (vi), potrebbero verificarsi tra Kaspersky Lab e l'utente o sarebbero altrimenti impliciti o incorporati nel presente Contratto o in qualsiasi altro contratto collaterale, per disposizione statutaria, legislazione vigente o altro, che con ciò sarebbero esclusi (inclusi, senza limitazione, le condizioni implicite, le garanzie o altri termini relativi all'adeguatezza della qualità, all'idoneità allo scopo o all'uso di competenza e cura ragionevoli).

6. *Limitazione di responsabilità*.

(i) Nessun elemento nel presente Contratto deve escludere o limitare la responsabilità di Kaspersky Lab relativamente 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, o (c) da qualsiasi altra responsabilità che non possa essere esclusa per legge..

(ii) Ai sensi del paragrafo (i), 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 attività;

(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 nessun'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 l'utente utilizza la versione di prova del Software, non avrà diritto all'Assistenza tecnica specificata nella Clausola 2 del presente Contratto di licenza, né potrà vendere la copia in suo possesso a terzi.

L'utente avrà diritto ad utilizzare il Software a scopi dimostrativi per il periodo specificato nel file chiave di licenza, a partire dal momento in cui viene attivato (questo periodo può essere visualizzato nelle finestra Servizio dell'interfaccia grafica utente del software).