

Kaspersky Anti-Virus 6.0 per Windows Servers MP4

MANUALE DELL'UTENTE

VERSIONE DELL'APPLICAZIONE: 6.0 MAINTENANCE PACK 4, CRITICAL FIX

1



KASPERSKY lab

Gentile utente di Kaspersky Anti-Virus,

grazie per aver scelto il nostro prodotto. Ci auguriamo che questa documentazione sia utile e fornisca le risposte necessarie.

Qualsiasi tipo di riproduzione o distribuzione di qualsiasi materiale, incluse le traduzioni, è consentito solo previa autorizzazione scritta concessa da Kaspersky Lab.

Il presente documento e le immagini grafiche in esso contenute possono essere utilizzati a scopo esclusivamente informativo, non commerciale o personale.

Il presente documento è soggetto a modifica senza preavviso. Per la versione più recente del presente documento, visitare il sito Web di Kaspersky Lab all'indirizzo <http://www.kaspersky.com/it/docs>.

Kaspersky Lab non si assume responsabilità riguardo al contenuto, la qualità, la rilevanza o l'accuratezza dei materiali utilizzati in questo documento i cui diritti appartengono a terzi, o per possibili danni associati all'uso di tali documenti.

Il presente documento include marchi depositati e di servizio appartenenti ai rispettivi proprietari.

Data di revisione: 25.02.2010

© 1997-2010 Kaspersky Lab ZAO. Tutti i diritti riservati.

<http://www.kaspersky.it>
<http://support.kaspersky.it>

SOMMARIO

INTRODUZIONE	8
Kit di distribuzione	8
Contratto di licenza con l'utente finale (EULA)	8
Servizi offerti agli utenti registrati	8
Requisiti di sistema hardware e software	9
KASPERSKY ANTI-VIRUS 6.0 PER WINDOWS SERVERS MP4	10
Informazioni sull'applicazione	10
Fonti di informazione per l'esecuzione di ricerche	10
Come contattare l'ufficio vendite	11
Come contattare il servizio di Assistenza tecnica	11
Discussioni sulle applicazioni Kaspersky Lab nel forum Web	12
Novità di Kaspersky Anti-Virus 6.0 per Windows Servers MP4	12
Difesa di Kaspersky Anti-Virus: le basi	13
Anti-Virus File	13
Attività di scansione anti-virus	14
Aggiornamento	14
Funzioni di assistenza dell'applicazione	14
INSTALLAZIONE DI KASPERSKY ANTI-VIRUS 6.0	16
Installazione tramite procedura guidata	16
Passaggio 1. Verifica dei requisiti di installazione del sistema	17
Passaggio 2. Finestra di avvio dell'installazione	17
Passaggio 3. Visualizzazione del Contratto di licenza	17
Passaggio 4. Selezione della cartella di installazione	17
Passaggio 5. Utilizzo delle impostazioni dell'applicazione salvate dopo un'installazione precedente	18
Passaggio 6. Selezione del tipo di installazione	18
Passaggio 7. Selezione dei componenti dell'applicazione per l'installazione	18
Passaggio 9. Ricerca di altre applicazioni anti-virus	19
Passaggio 10. Preparazione finale per l'installazione	19
Passaggio 11. Completamento dell'installazione	19
Installazione dell'applicazione da riga di comando	19
Installazione dall'editor Oggetti criteri di gruppo	20
Installazione dell'applicazione	20
Descrizione delle impostazioni del file setup.ini	21
Aggiornamento della versione dell'applicazione	21
Rimozione dell'applicazione	22
GUIDA INTRODUTTIVA	23
Configurazione guidata iniziale	23
Utilizzo degli oggetti salvati dalla versione precedente	24
Attivazione dell'applicazione	24
Configurazione delle impostazioni di aggiornamento	26
Configurazione della pianificazione della scansione anti-virus	26
Limitazione dell'accesso all'applicazione	27
Completamento della configurazione guidata	27
Scansione anti-virus del computer	27

Aggiornamento dell'applicazione	28
Gestione delle licenze.....	28
Gestione della protezione	29
Sospensione della protezione.....	30
Eliminazione dei problemi. Assistenza tecnica utente	31
Creazione di un file di traccia.....	31
Configurazione delle impostazioni dell'applicazione	32
Rapporti sul funzionamento dell'applicazione. File di dati.....	32
INTERFACCIA DELL'APPLICAZIONE	33
Icona dell'area di notifica della barra delle applicazioni	33
Menu di scelta rapida.....	34
Finestra principale dell'applicazione	35
Notifiche.....	36
Finestra delle impostazioni dell'applicazione	37
ANTI-VIRUS FILE.....	38
Algoritmo di funzionamento del componente	39
Modifica del livello di protezione	40
Modifica delle azioni da eseguire sugli oggetti rilevati	40
Creazione di un ambito di protezione	41
Utilizzo dell'analisi euristica.....	42
Ottimizzazione della scansione.....	43
Scansione dei file composti.....	43
Scansione di file composti di grandi dimensioni.....	44
Modifica della modalità di scansione.....	44
Tecnologia di scansione	45
Sospensione del componente: creazione di una pianificazione.....	45
Sospensione del componente: creazione di un elenco di applicazioni	46
Ripristino delle impostazioni di protezione predefinite	46
Statistiche di Anti-Virus File	47
Trattamento posticipato degli oggetti	47
SCANSIONE ANTI-VIRUS SERVER	49
Avvio della scansione anti-virus	50
Creazione di un elenco di oggetti da esaminare	51
Modifica del livello di protezione	52
Modifica delle azioni da eseguire sugli oggetti rilevati	53
Modifica del tipo di oggetti da esaminare.....	54
Ottimizzazione della scansione.....	54
Scansione dei file composti.....	55
Modifica del metodo di scansione.....	55
Tecnologia di scansione	56
Prestazioni del computer durante l'esecuzione delle attività	57
Sospensione dell'attività: creazione di una pianificazione.....	57
Sospensione del componente: creazione di un elenco di applicazioni	58
Modalità di esecuzione: specifica di un account	58
Modalità di esecuzione: creazione di una pianificazione	58
Funzioni dell'avvio pianificato delle attività.....	59
Statistiche della scansione anti-virus	59
Assegnazione delle impostazioni di scansione comuni per tutte le attività	60

Ripristino delle impostazioni di scansione predefinite	60
AGGIORNAMENTO DELL'APPLICAZIONE.....	61
Avvio dell'aggiornamento.....	62
Rollback dell'ultimo aggiornamento	63
Origine degli aggiornamenti	63
Impostazioni internazionali.....	64
Utilizzo di un server proxy.....	64
Modalità di esecuzione: specifica di un account	65
Modalità di esecuzione: creazione di una pianificazione	65
Selezione degli oggetti da aggiornare.....	66
Modifica della modalità di esecuzione dell'attività di aggiornamento	66
Aggiornamento da una cartella locale.....	67
Statistiche di aggiornamento.....	68
Problemi possibili durante l'aggiornamento	68
CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE	72
Protezione.....	73
Abilitazione/disabilitazione della protezione del computer.....	73
Avvio dell'applicazione all'avvio del sistema operativo	74
Selezione delle categorie di minacce rilevabili	74
Creazione di un'area attendibile	74
Esportazione / importazione delle impostazioni di Kaspersky Anti-Virus	79
Ripristino delle impostazioni predefinite	79
Anti-Virus File	80
Scansione	80
Aggiornamento	81
Opzioni.....	81
Auto-difesa dell'applicazione	82
Restrizione dell'accesso all'applicazione.....	82
Limitazione delle dimensioni dei file iSwift.....	83
Configurazione server multiprocessore.....	83
Notifiche degli eventi di Kaspersky Anti-Virus	84
Elementi attivi dell'interfaccia	86
Rapporti e archiviazioni.....	86
Principi di gestione dei rapporti	87
Configurazione dei rapporti	88
Quarantena per oggetti potenzialmente infetti.....	88
Azioni sugli oggetti in quarantena	89
Copie di backup degli oggetti pericolosi	89
Utilizzo delle copie di backup	90
Configurazione della quarantena e del backup	90
DISCO DI RIPRISTINO	90
Creazione del Disco di Ripristino	91
Passaggio 1. Selezione dell'origine dell'immagine del disco	92
Passaggio 2. Copia dell'immagine ISO	92
Passaggio 3. Aggiornamento dell'immagine ISO	92
Passaggio 4. Avvio remoto.....	93
Passaggio 5. Chiusura della procedura guidata.....	93
Avvio del computer attraverso il Disco di Ripristino	93

Utilizzo del Disco di Ripristino di Kaspersky dal prompt dei comandi	94
Scansione anti-virus	95
Aggiornamento di Kaspersky Anti-Virus	97
Rollback dell'ultimo aggiornamento	97
Visualizzazione della Guida	98
VERIFICA DEL FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS	99
"Virus" di prova EICAR e sue varianti	99
Verifica del funzionamento di Anti-Virus File	100
Verifica del funzionamento dell'attività di scansione anti-virus	101
TIPI DI NOTIFICHE	102
Rilevamento di un oggetto dannoso	102
Impossibile disinfettare l'oggetto	103
Rilevamento di un oggetto sospetto	103
UTILIZZO DELL'APPLICAZIONE DALLA RIGA DI COMANDO	105
Visualizzazione della Guida	106
Scansione anti-virus	106
Aggiornamento dell'applicazione	108
Rollback dell'ultimo aggiornamento	109
Avvio / interruzione delle operazioni di Anti-Virus File o di un'attività	109
Statistiche sul funzionamento di un componente o di un'attività	110
Esportazione delle impostazioni di protezione	111
Importazione delle impostazioni di protezione	111
Attivazione dell'applicazione	111
Ripristino di un file dalla quarantena	112
Chiusura dell'applicazione	112
Come ottenere un file di traccia	112
Codici restituiti della riga di comando	113
MODIFICA, RIPARAZIONE E RIMOZIONE DELL'APPLICAZIONE	114
Modifica, riparazione e rimozione dell'applicazione tramite l'installazione guidata	114
Passaggio 1. Finestra iniziale dell'installazione	114
Passaggio 2. Selezione di un'operazione	114
Passaggio 3. Completamento della modifica, riparazione o rimozione dell'applicazione	115
Rimozione dell'applicazione dalla riga di comando	116
GESTIONE DELL'APPLICAZIONE TRAMITE KASPERSKY ADMINISTRATION KIT	117
Gestione dell'applicazione	120
Avvio e arresto dell'applicazione	121
Configurazione delle impostazioni dell'applicazione	122
Configurazione di impostazioni specifiche	123
Gestione delle attività	125
Avvio e arresto delle attività	126
Creazione di attività	126
Creazione guidata attività locale	127
Configurazione delle attività	128
Gestione dei criteri	130
Creazione di criteri	130
Creazione guidata criterio	131
Configurazione del criterio	133

UTILIZZO DI CODICE DI TERZE PARTI	135
Libreria Boost 1.30.0.....	136
Libreria LZMA SDK 4.40, 4.43.....	136
Libreria Windows Template 7.5	136
Libreria Windows Installer XML (WiX) 2.0.....	137
Libreria ZIP-2.31	140
Libreria ZLIB-1.0.4, ZLIB-1.0., ZLIB-1.1.3, ZLIB-1.2.3	141
Libreria UNZIP-5.51.....	141
Libreria LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12	142
Libreria LIBJPEG-6B.....	144
Libreria LIBUNGIF-4.1.4	146
Libreria MD5 MESSAGE-DIGEST ALGORITHM-REV. 2	146
Libreria MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004	146
Libreria INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999.....	146
Libreria CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004.....	147
Libreria COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum.....	147
Libreria PLATFORM INDEPENDENT IMAGE CLASS.....	147
Libreria FLEX PARSER (FLEXLEXER)-V. 1993.....	148
Libreria ENSURECLEANUP, SWMRG, LAYOUT-V. 2000	148
Libreria STDSTRING- V. 1999.....	149
Libreria T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006	149
Libreria NTSERVICE- V. 1997.....	150
Libreria SHA-1-1.2	150
Libreria COCOA SAMPLE CODE- V. 18.07.2007	151
Libreria PUTTY SOURCES-25.09.2008.	151
Altre informazioni	152
GLOSSARIO	153
KASPERSKY LAB	160
CONTRATTO DI LICENZA	161
INDICE	167

INTRODUZIONE

IN QUESTA SEZIONE

Kit di distribuzione	8
Servizi offerti agli utenti registrati.....	8
Requisiti di sistema hardware e software	9

KIT DI DISTRIBUZIONE

Kaspersky Anti-Virus può essere acquistato presso i nostri rivenditori oppure online dai negozi su Internet, ad esempio nella sezione **Compra Online** del sito <http://www.kaspersky.it>.

Il pacchetto della versione in scatola del prodotto include:

- Una busta sigillata con il CD di installazione contenente i file del programma e la documentazione in formato PDF.
- La Guida dell'utente stampata (se è stata inclusa nell'ordine) oppure la Guida del prodotto.
- File di chiave dell'applicazione allegato alla busta del CD di installazione.
- Scheda di registrazione (con numero di serie del prodotto).
- Contratto di licenza con l'utente finale (EULA).

Si consiglia di leggere attentamente le condizioni dell'EULA prima di aprire la busta del CD di installazione.

L'acquisto di Kaspersky Anti-Virus presso il negozio online comporta il download del prodotto dal sito Web di Kaspersky Lab. Il presente Manuale dell'utente è incluso nel pacchetto di installazione. Alla ricezione del pagamento, l'utente riceverà un messaggio di posta elettronica con il file di chiave.

CONTRATTO DI LICENZA CON L'UTENTE FINALE (EULA)

Il Contratto di licenza con l'utente finale (EULA) è un contratto legale che intercorre tra l'utente e Kaspersky Lab, in cui si specificano le condizioni di utilizzo del software acquistato.

L'EULA deve essere letto con molta attenzione.

Se non si accettano le condizioni dell'EULA, è possibile restituire la confezione del prodotto al rivenditore presso il quale è stata acquistata e ottenere il rimborso corrispondente all'importo pagato, a condizione che la busta contenente il disco di installazione sia ancora sigillata.

L'apertura della busta sigillata con il CD di installazione implica l'accettazione delle condizioni dell'EULA.

SERVIZI OFFERTI AGLI UTENTI REGISTRATI

Kaspersky Lab offre un pacchetto completo di servizi a tutti gli utenti legalmente registrati, consentendo loro di potenziare le prestazioni dell'applicazione.

Con l'acquisto di una licenza si diventa utente registrato e si può usufruire durante tutto il periodo di durata della licenza dei servizi seguenti:

- aggiornamenti orari dei database dell'applicazione e aggiornamento al pacchetto software;
- supporto per i problemi correlati all'installazione, alla configurazione e all'utilizzo del prodotto software acquistato. I servizi vengono forniti tramite telefono o posta elettronica;
- notifiche relative ai nuovi prodotti Kaspersky Lab e ai nuovi virus che si diffondono in tutto il mondo. Questo servizio è disponibile per gli utenti che hanno effettuato la sottoscrizione alla mailing list delle news di Kaspersky Lab nelsito Web del servizio di Assistenza tecnica (<http://support.kaspersky.com/it/subscribe/>).

Non viene fornito supporto per i problemi correlati alle prestazioni e all'utilizzo dei sistemi operativi, altro software di terzi o altre tecnologie.

REQUISITI DI SISTEMA HARDWARE E SOFTWARE

Per il corretto funzionamento di Kaspersky Anti-Virus 6.0, il computer deve soddisfare i requisiti minimi seguenti:

Requisiti generali:

- 300 MB di spazio libero su disco rigido.
- Microsoft Internet Explorer 6.0 o versione successiva (per l'aggiornamento dei database dell'applicazione e dei moduli del programma via Internet).
- Microsoft Windows Installer 2.0 o superiore.

Windows 2000 Server / Advanced Server (Service Pack 4 Rollup1), Windows Server 2003 Standard / Enterprise (Service Pack 2), Windows Server 2003 x64 Standard / Enterprise (Service Pack 2), Windows Small Business Server 2003:

- Processore Intel Pentium da 400 MHz 32 bit (x86) / 64-bit (x64) o superiore (o un equivalente compatibile).
- 512 MB di RAM libera.

Windows Server 2003 R2 Standard / Enterprise Edition, Windows Server 2003 R2 x64 Standard / Enterprise Edition, Windows Server 2008 Standard / Enterprise (Service Pack 1 o superiore), Windows Server 2008 x64 Standard / Enterprise (Service Pack 1 o superiore), Windows Small Business Server 2008, Windows Essential Business Server 2008, Windows Server 2008 R2 x64 Standard / Enterprise:

- Processore Intel Pentium da 1 GHz a 32 bit (x86) / 1,4 GHz a 64 bit (x64) o superiore (o un equivalente compatibile).
- 1 GB di RAM libera.

KASPERSKY ANTI-VIRUS 6.0 PER WINDOWS SERVERS MP4

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 rappresenta una nuova generazione di prodotti per la sicurezza dei dati.

IN QUESTA SEZIONE

Informazioni sull'applicazione	10
Novità di Kaspersky Anti-Virus 6.0 per Windows Servers MP4	12
Difesa di Kaspersky Anti-Virus: le basi	13

INFORMAZIONI SULL'APPLICAZIONE

Per tutte le domande relative all'acquisto, all'installazione o all'utilizzo di Kaspersky Anti-Virus sono state predisposte le risposte più appropriate.

Kaspersky Lab offre diverse fonti di informazioni sull'applicazione. È possibile scegliere la più adatta in base all'urgenza e all'importanza del quesito.

IN QUESTA SEZIONE

Fonti di informazione per l'esecuzione di ricerche	10
Come contattare l'ufficio vendite	11
Come contattare il servizio di Assistenza tecnica	11
Discussioni sulle applicazioni Kaspersky Lab nel forum Web	12

FONTI DI INFORMAZIONE PER L'ESECUZIONE DI RICERCHE

È possibile fare riferimento alle fonti di informazioni sull'applicazione seguenti:

- pagina dell'applicazione nel sito Web di Kaspersky Lab;
- pagina dell'applicazione nel sito Web del servizio di assistenza tecnica (nella Knowledge Base);
- guida in linea;
- documentazione.

Pagina dell'applicazione nel sito Web di Kaspersky Lab

http://www.kaspersky.com/it/anti-virus_windows_server

In questa pagina vengono fornite informazioni generali sull'applicazione, nonché sulle relative funzioni e opzioni.

Pagina dell'applicazione nel sito Web del servizio di assistenza tecnica (nella Knowledge Base)

http://support.kaspersky.com/windows_file_server

In questa pagina sono presenti articoli creati dagli esperti del servizio di assistenza tecnica.

Tali articoli contengono informazioni utili, consigli e FAQ sull'acquisto, sull'installazione e sull'utilizzo dell'applicazione. Sono organizzati in base all'argomento, ad esempio gestione dei file chiave, impostazione degli aggiornamenti dei database o eliminazione degli errori di funzionamento. Gli articoli possono fornire risposte a domande relative non solo all'applicazione specifica, ma anche ad altri prodotti di Kaspersky Lab. Possono inoltre contenere notizie fornite dal servizio di assistenza tecnica.

Guida in linea

Il pacchetto di installazione dell'applicazione include il file della Guida sensibile al contesto e della Guida completa contenente informazioni sulla modalità di gestione della protezione del computer (visualizzazione dello stato di protezione, scansione anti-virus di diverse aree del computer, esecuzione di altre attività), nonché informazioni su ogni finestra dell'applicazione, quali l'elenco delle relative impostazioni con descrizione associata e l'elenco delle attività da eseguire.

Per aprire il file della Guida, fare clic sul pulsante **Guida** nella finestra desiderata o premere <F1>.

Documentazione

Il pacchetto di installazione di Kaspersky Anti-Virus include il documento **Manuale dell'utente** (in formato PDF). Questo documento contiene descrizioni delle funzioni e delle opzioni dell'applicazione, nonché dei principali algoritmi di funzionamento.

COME CONTATTARE L'UFFICIO VENDITE

In caso di domande riguardanti la selezione o l'acquisto dell'applicazione o l'estensione del periodo di utilizzo, è possibile telefonare agli specialisti dell'ufficio vendite nella Sede centrale di Mosca, ai numeri:

+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00

Il servizio è disponibile in russo o in inglese.

È possibile inviare le proprie domande agli specialisti dell'ufficio vendite via e-mail all'indirizzo: sales@kaspersky.com.

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

Una volta acquistato Kaspersky Anti-Virus, è possibile ottenere tutte le informazioni desiderate dal servizio di assistenza tecnica telefonicamente o tramite Internet.

Gli specialisti del servizio di Assistenza tecnica saranno lieti di rispondere a qualsiasi domanda relativa all'installazione e all'utilizzo dell'applicazione, e forniranno consigli preziosi per risolvere i problemi causati dalle attività del malware qualora il computer sia stato infettato.

Prima di contattare il servizio di assistenza tecnica, leggere la sezione Termini e condizioni dell'assistenza tecnica (<http://support.kaspersky.com/it/support/rules>).

Richiesta al servizio di assistenza tecnica via posta elettronica

Per inviare le domande agli specialisti del servizio di assistenza tecnica, compilare il modulo Web Helpdesk (<http://support.kaspersky.com/helpdesk.html?LANG=it>).

La domanda può essere formulata in Italiano, Russo, Inglese, Tedesco, Francese o Spagnolo.

Per inviare una richiesta via e-mail, è necessario indicare l'**ID cliente** ricevuto durante la registrazione al sito Web del servizio di assistenza tecnica insieme alla **password**.

Se non si è ancora un utente registrato delle applicazioni di Kaspersky Lab, è possibile compilare il modulo di registrazione all'indirizzo <https://support.kaspersky.com/it/personalcabinet/registration/form/>. Durante la registrazione, sarà necessario immettere il *codice di attivazione* o il *nome del file di chiave della licenza*.

La risposta del servizio di assistenza tecnica alla richiesta sarà inviata all'account Kaspersky dell'utente (<https://support.kaspersky.com/en/personalcabinet?LANG=it>) e all'indirizzo e-mail specificato nella richiesta.

Descrivere il più dettagliatamente possibile il problema riscontrato nel modulo di richiesta Web. Compilare i seguenti campi obbligatori:

- **Tipo di richiesta.** Selezionare l'argomento che si avvicina di più al problema, ad esempio: problema con l'installazione o la disinstallazione oppure problema con la ricerca o l'eliminazione di virus. Se l'argomento desiderato non è disponibile, selezionare "Domanda di carattere generale".
- **Nome e numero di versione dell'applicazione.**
- **Tipo di richiesta.** Descrivere il problema rilevato il più dettagliatamente possibile.
- **ID cliente e password.** Specificare il numero cliente e la password ricevuti durante la registrazione nel sito Web del servizio di assistenza tecnica.
- **Indirizzo e-mail.** Il servizio di assistenza tecnica invierà una risposta alle domande formulate all'indirizzo specificato.

Assistenza tecnica telefonica

Per sottoporre un problema urgente, è possibile contattare telefonicamente il servizio di assistenza tecnica locale. Prima di contattare gli specialisti del servizio di Assistenza tecnica russo (http://support.kaspersky.ru/support/support_local) o internazionale (<http://support.kaspersky.com/it/support/international>) raccogliere le informazioni (<http://support.kaspersky.com/it/support/details>) sul computer e sull'applicazione anti-virus installata. Ciò consentirà agli esperti di fornire assistenza più rapidamente.

DISCUSSIONI SULLE APPLICAZIONI KASPERSKY LAB NEL FORUM WEB

Se la propria domanda non richiede una risposta urgente, è possibile discuterne con gli specialisti di Kaspersky Lab e altri utenti nel nostro forum all'indirizzo <http://forum.kaspersky.com>.

In questo forum è possibile visualizzare gli argomenti esistenti, lasciare commenti, creare nuovi argomenti e utilizzare il motore di ricerca.

NOVITÀ DI KASPERSKY ANTI-VIRUS 6.0 PER WINDOWS SERVERS MP4

Kaspersky Anti-Virus 6.0 è uno strumento completo di protezione dei dati. Di seguito vengono descritte in modo dettagliato le nuove funzionalità di Kaspersky Anti-Virus 6.0.

Nuova protezione:

- Il nuovo kernel anti-virus utilizzato da Kaspersky Anti-Virus rileva i programmi dannosi in maniera più efficace. Inoltre, consente una scansione anti-virus del sistema molto più rapida. È il risultato di una elaborazione degli oggetti migliorata e di un utilizzo ottimizzato delle risorse del computer (in particolare per i processori dual o quad core).

- È stata implementata una nuova analisi euristica, che fornisce maggiore accuratezza nel rilevamento e nel blocco di programmi dannosi sconosciuti in precedenza. Se la firma di un programma non viene trovata nei database dell'anti-virus, l'analisi euristica simula l'avvio del programma in un ambiente virtuale isolato. Si tratta di un metodo protetto che consente l'analisi di tutti gli effetti di un programma prima del suo avvio in un ambiente reale.
- È stata migliorata la procedura di aggiornamento dell'applicazione. Adesso, non è più sempre necessario riavviare il computer.

Funzioni della nuova interfaccia:

- L'interfaccia rende le funzioni del programma di semplice e facile accesso.
- È stata ridisegnata in base alle esigenze degli amministratori di reti piccole e medie, nonché di reti di grandi aziende.

Nuove funzioni di Kaspersky Administration Kit:

- Kaspersky Administration Kit agevola la gestione di un sistema di protezione anti-virus aziendale. Gli amministratori possono utilizzare l'applicazione per gestire in maniera centralizzata la protezione di una rete aziendale di qualsiasi dimensione, contenente decine di migliaia di nodi, inclusi utenti remoti e mobili.
- È stata aggiunta una funzione che abilita l'installazione remota dell'applicazione con la versione più recente dei database dell'applicazione.
- È stata migliorata la gestione dell'applicazione installata su un computer remoto (è stata ridisegnata la struttura dei criteri).
- È stata aggiunta una funzione che consente di utilizzare la configurazione di un'applicazione esistente durante la creazione di un criterio.
- È stata realizzata un'altra funzione importante che consente per gli utenti mobili di creare configurazioni specifiche per la configurazione delle attività di aggiornamento dei gruppi.
- È inoltre stata implementata una funzione per la disabilitazione temporanea delle azioni relative ai criteri e delle attività dei gruppi per i computer client in cui è installata l'applicazione (dopo l'immissione della password corretta).

DIFESA DI KASPERSKY ANTI-VIRUS: LE BASI

La protezione di Kaspersky Anti-Virus for Windows Servers include:

- Anti-Virus File (vedere a pag. [13](#)) che monitora il file system del computer in modalità tempo reale.
- Attività di scansione anti-virus (a pag. [14](#)) utilizzate per eseguire scansioni anti-virus di tutto il computer oppure di file, cartelle, dischi o aree separati.
- Aggiornamento (vedere a pag. [14](#)) garantisce che i moduli interni e i database dell'applicazione, utilizzati per ricercare i programmi dannosi, siano aggiornati.
- Funzioni di assistenza (vedere la sezione "Funzioni di assistenza dell'applicazione" a pag. [14](#)) forniscono supporto informativo per l'utilizzo dell'applicazione e l'espansione delle relative funzionalità.

ANTI-VIRUS FILE

Mediante Anti-Virus File il server è protetto in tempo reale.

Un file system può contenere virus e altri programmi dannosi. I programmi dannosi possono rimanere memorizzati nel file system per anni senza assolutamente manifestarsi dopo essersi infiltrati tramite un'unità rimovibile o da Internet. È sufficiente, invece, aprire il file infetto per attivare immediatamente il virus.

Anti-Virus File è il componente che monitora il file system del computer. Esegue la scansione di tutti i file aperti, eseguiti o salvati nel computer e di tutte le unità disco connesse. Kaspersky Anti-Virus intercetta ogni tentativo di accedere a un file e ne esegue la scansione allo scopo di individuare virus noti. Il file può essere ulteriormente elaborato solo se non è infetto o se non determina errori nell'applicazione. Se per qualsiasi motivo un file non può essere disinfettato, verrà eliminato e ne verrà salvata una copia nel backup oppure verrà spostato in quarantena.

ATTIVITÀ DI SCANSIONE ANTI-VIRUS

Oltre alla protezione di Anti-Virus File, è estremamente importante eseguire di tanto in tanto la scansione anti-virus del server. Questa pratica è necessaria per eliminare la possibilità che si diffondano programmi dannosi non rilevati da Anti-Virus File, ad esempio, perché è impostato un livello di protezione basso per altri motivi.

In Kaspersky Anti-Virus sono incluse le attività di scansione anti-virus seguenti:

Scansione

Esame degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.

Scansione Completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete.

Scansione Rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo.

AGGIORNAMENTO

Per bloccare eventuali attacchi di rete, eliminare un virus o un altro programma dannoso, è necessario che Kaspersky Anti-Virus venga aggiornato regolarmente. Il componente **Aggiornamenti** è progettato per questo scopo. Consente infatti di gestire l'aggiornamento dei moduli e dei database utilizzati dall'applicazione.

Il servizio di distribuzione degli aggiornamenti consente di salvare gli aggiornamenti dei moduli di programma e dei database scaricati dai server di Kaspersky Lab in una cartella locale in modo da consentire ad altri computer della rete l'accesso agli aggiornamenti e ridurre quindi il traffico di rete.

FUNZIONI DI ASSISTENZA DELL'APPLICAZIONE

Kaspersky Anti-Virus comprende un insieme di funzionalità di assistenza Progettate. Progettate per mantenere aggiornata la protezione del computer, espandere le funzionalità dell'applicazione e fornire un supporto per il relativo utilizzo.

File di dati

Durante l'utilizzo dell'applicazione viene creato un rapporto da ogni componente della protezione, attività di scansione anti-virus e aggiornamento dell'applicazione. Tale rapporto contiene informazioni sulle attività eseguite e i relativi risultati. I dati forniti consentono di conoscere nei dettagli il funzionamento dei singoli componenti di Kaspersky Anti-Virus. In caso di problemi, è possibile inviare i rapporti a Kaspersky Lab. Gli specialisti potranno approfondire la situazione e trovare una soluzione in tempi più brevi.

Kaspersky Anti-Virus sposta tutti i file sospetti in un'area di archiviazione speciale denominata *Quarantena*. I file vengono memorizzati in forma crittografata per evitare di infettare il computer. È possibile eseguire la scansione anti-virus di questi oggetti, ripristinarli nella posizione precedente, eliminarli oppure aggiungere file all'area della

quarantena. Tutti i file che il completamento della scansione anti-virus dimostra essere non infetti vengono automaticamente ripristinati nella posizione precedente.

La cartella *Backup* include le copie dei file disinfettati ed eliminati da Kaspersky Anti-Virus. Tali copie vengono create al fine di ripristinare, se necessario, i file o un'immagine da un'infezione. Le copie di backup dei file vengono inoltre archiviate in forma crittografata per evitare ulteriori infezioni.

È possibile ripristinare un file dalla copia di backup nella posizione originale ed eliminare la copia.

Disco di Ripristino

Disco di Ripristino è stato progettato per eseguire la scansione dei computer compatibili con le piattaforme x86 e per disinfettarli. È consigliabile utilizzare l'applicazione quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione di malware.

Licenza

Quando si acquista Kaspersky Anti-Virus, si stipula un contratto di licenza con Kaspersky Lab che regola l'utilizzo dell'applicazione, l'accesso agli aggiornamenti dei database dell'applicazione e l'assistenza tecnica per un periodo di tempo specificato. I termini di utilizzo e le altre informazioni necessarie per la piena funzionalità dell'applicazione vengono forniti nella licenza.

Utilizzando la funzione **Licenza**, è possibile ottenere informazioni dettagliate sulla propria licenza e acquistare una nuova licenza o rinnovare quella corrente.

Assistenza tecnica

Tutti gli utenti registrati di Kaspersky Anti-Virus possono avvalersi del servizio di assistenza tecnica. Per visualizzare le informazioni sui centri in cui ricevere assistenza tecnica, utilizzare la funzione **Supporto**.

Mediante i collegamenti disponibili, è possibile visitare il forum utenti di Kaspersky Lab ed eseguire una ricerca nelle domande ricorrenti che potrebbero fornire una soluzione al problema. Inoltre, è possibile riempire il modulo speciale che si trova nel sito e inviare all'Assistenza tecnica un messaggio relativo a un errore o un commento sul funzionamento di un programma.

È, inoltre, possibile accedere al Servizio di assistenza tecnica, dove, naturalmente, il nostro personale sarà sempre pronto a fornire assistenza telefonica su Kaspersky Anti-Virus.

INSTALLAZIONE DI KASPERSKY ANTI-VIRUS 6.0

È possibile installare Kaspersky Anti-Virus 6.0 for Windows Servers MP4 su un computer in diversi modi:

- installazione locale – installazione dell'applicazione su un unico computer. Per eseguire e completare l'installazione è necessario l'accesso diretto a quel determinato computer. L'installazione locale può essere eseguita in una delle modalità indicate di seguito:
- modalità interattiva, tramite l'installazione guidata dell'applicazione (vedere la sezione "Installazione mediante procedura guidata" a pag. [16](#)). Tale modalità richiede la partecipazione dell'utente durante l'installazione;
- modalità non-interattiva in cui l'installazione dell'applicazione viene avviata da riga di comando e non richiede la partecipazione dell'utente durante l'installazione (vedere la sezione "Installazione dell'applicazione da riga di comando" a pag. [19](#)).
- installazione remota – l'installazione dell'applicazione su computer in rete gestiti in remoto dalla workstation dell'amministratore mediante:
 - il set di programmi di Kaspersky Administration Kit (vedere il manuale Kaspersky Administration Kit Deployment Guide);
 - criteri del dominio di gruppo di Microsoft Windows Server 2000/2003 (vedere la sezione "Installazione dall'editor Oggetti criteri di gruppo" a pag. [20](#)).

Prima dell'avvio dell'installazione di Kaspersky Anti-Virus (inclusa quella remota), si raccomanda di chiudere tutte le applicazioni attive.

IN QUESTA SEZIONE

Installazione tramite procedura guidata.....	16
Installazione dell'applicazione da riga di comando	19
Installazione dall'editor Oggetti criteri di gruppo	20

INSTALLAZIONE TRAMITE PROCEDURA GUIDATA

Per installare Kaspersky Anti-Virus sul computer, eseguire il file di installazione che si trova nel CD del prodotto.

L'installazione dell'applicazione dal file di installazione scaricato da Internet è identica a quella da CD.

Il programma di installazione viene implementato come una procedura guidata standard di Windows. In ogni finestra è disponibile presente un insieme di pulsanti per il controllo del processo di installazione. Di seguito vengono descritte in breve le funzioni di ciascun pulsante:

- **Avanti** – accetta l'azione e passa al punto successivo della procedura di installazione.
- **Indietro** – torna al punto precedente della procedura di installazione.
- **Annulla** – annulla l'installazione.

- **Fine** – completa la procedura di installazione dell'applicazione.

Di seguito è fornita una descrizione dettagliata di ciascun punto dell'installazione del pacchetto.

PASSAGGIO 1. VERIFICA DEI REQUISITI DI INSTALLAZIONE DEL SISTEMA

Prima di installare Kaspersky Anti-Virus, la procedura guidata verificherà che il computer soddisfi i requisiti minimi. Inoltre, verificherà anche le autorizzazioni necessarie per l'installazione del software.

Se uno dei requisiti non viene soddisfatto, sullo schermo verrà visualizzato il messaggio corrispondente. Si raccomanda di installare gli aggiornamenti e i programmi necessari mediante il servizio **Windows Update**, prima di avviare nuovamente l'installazione di Kaspersky Anti-Virus.

PASSAGGIO 2. FINESTRA DI AVVIO DELL'INSTALLAZIONE

Se il sistema soddisfa totalmente i requisiti di base, subito dopo l'esecuzione del file di installazione verrà visualizzata la finestra di avvio contenente le informazioni sull'avvio dell'installazione di Kaspersky Anti-Virus.

Per procedere con l'installazione, fare clic sul pulsante **Avanti**. Per annullare l'installazione, fare clic sul pulsante **Annulla**.

PASSAGGIO 3. VISUALIZZAZIONE DEL CONTRATTO DI LICENZA

La finestra di dialogo successiva dell'applicazione contiene il contratto di licenza tra l'utente e Kaspersky Lab. Si raccomanda di leggerlo con attenzione e, se si accettano tutti i termini e le condizioni del contratto, selezionare l'opzione  **Accetto i termini del contratto di licenza**, quindi fare clic sul pulsante **Avanti**. L'installazione continua.

Per annullare l'installazione, fare clic sul pulsante **Annulla**.

PASSAGGIO 4. SELEZIONE DELLA CARTELLA DI INSTALLAZIONE

Nel passaggio successivo dell'installazione di Kaspersky Anti-Virus viene definita la cartella di installazione dell'applicazione. Il percorso predefinito è il seguente:

- **<Unità> → Tutti i programmi → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Servers MP4** – per i sistemi a 32 bit.
- **<Unità> → Programmi (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Servers MP4** – per i sistemi a 64 bit.

È possibile specificare una cartella diversa scegliendo il pulsante **Sfoglia** e selezionando una cartella nella finestra di selezione standard oppure immettendo il percorso della cartella nel relativo campo di immissione.

Se si inserisce manualmente il percorso completo della cartella di installazione, la cui lunghezza non deve superare i 200 caratteri e non deve contenere caratteri speciali.

Per procedere con l'installazione, fare clic sul pulsante **Avanti**.

PASSAGGIO 5. UTILIZZO DELLE IMPOSTAZIONI DELL'APPLICAZIONE SALVATE DOPO UN'INSTALLAZIONE PRECEDENTE

In questo passaggio, è possibile specificare se, per il funzionamento dell'applicazione, si desidera utilizzare le impostazioni di protezione e i database dell'applicazione, se tali oggetti sono stati salvati sul computer dopo la rimozione della versione precedente di Kaspersky Anti-Virus 6.0.

Verrà ora illustrato in dettaglio come abilitare le funzionalità descritte prima.

Se sono stati salvati i database dopo la rimozione di una versione precedente (build) di Kaspersky Anti-Virus, è possibile integrarli nella versione che si sta installando. Per eseguire questa operazione, selezionare la casella ☒ **Database dell'applicazione**. I database inclusi nel pacchetto di installazione non verranno copiati sul server.

Per utilizzare le impostazioni di protezione modificate in una versione precedente e salvate sul computer, selezionare la casella

☒ **Impostazioni applicazione**.

PASSAGGIO 6. SELEZIONE DEL TIPO DI INSTALLAZIONE

In questo passaggio, è necessario specificare la completezza dell'installazione dell'applicazione. È possibile scegliere tra due opzioni di installazione:

Completa. In questo caso, tutti i componenti di Kaspersky Anti-Virus verranno installati sul server. Per conoscere i passaggi seguenti dell'installazione, fare riferimento al Passaggio 8.

Personalizzato. In questo caso, è possibile selezionare i componenti dell'applicazione che si desidera installare. Per ulteriori dettagli, vedere il Passaggio 7.

Per selezionare la modalità di installazione, fare clic sul pulsante corrispondente.

PASSAGGIO 7. SELEZIONE DEI COMPONENTI DELL'APPLICAZIONE PER L'INSTALLAZIONE

Questo passaggio verrà eseguito esclusivamente se è stata selezionata l'opzione di installazione **Personalizzato**.

Prima dell'avvio dell'installazione personalizzata, è necessario selezionare i componenti di Kaspersky Anti-Virus che si desidera installare. Per impostazione predefinita, sono selezionati per l'installazione il componente Anti-Virus File, il componente per la scansione anti-virus e il connettore Network Agent per la gestione remota dell'applicazione tramite Kaspersky Administration Kit.

Per selezionare un componente per una installazione successiva, è necessario aprire il menu facendo clic sull'icona che si trova accanto al nome del componente e scegliere la voce **La funzionalità specificata sarà installata sull'unità disco fisso locale**. Nella parte inferiore della finestra del programma di installazione sono contenute le informazioni sul tipo di protezione fornite dal componente selezionato e lo spazio di archiviazione necessario per l'installazione.

Per informazioni dettagliate sullo spazio disco disponibile sul computer, premere il pulsante **Volume**. Le informazioni vengono visualizzate nella finestra aperta.

Per annullare l'installazione dei componenti, selezionare l'opzione **La funzionalità specificata diventerà non disponibile** dal menu di scelta rapida. Se si annulla l'installazione di un componente, il computer non sarà protetto contro diversi programmi pericolosi.

Al termine della selezione dei componenti da installare, premere il pulsante **Avanti**. Per tornare all'elenco predefinito dei componenti da installare, premere il pulsante **Reimposta**.

PASSAGGIO 9. RICERCA DI ALTRE APPLICAZIONI ANTI-VIRUS

A questo punto, la procedura guidata cercherà altri programmi anti-virus, inclusi altri programmi di Kaspersky Lab, che potrebbero entrare in conflitto con Kaspersky Anti-Virus.

Se sul server vengono rilevate applicazioni anti-virus, queste ultime verranno elencate sullo schermo. Prima di proseguire con l'installazione, l'utente avrà la possibilità di disinstallarle.

È possibile scegliere di rimuoverle automaticamente o manualmente, mediante i controlli che si trovano sotto l'elenco dei programmi anti-virus rilevati (vengono rimossi automaticamente solo i prodotti Kaspersky Lab).

Per procedere con l'installazione, fare clic sul pulsante **Avanti**.

PASSAGGIO 10. PREPARAZIONE FINALE PER L'INSTALLAZIONE

Questo passaggio completa la preparazione per l'installazione dell'applicazione sul server.

Per l'installazione iniziale di Kaspersky Anti-Virus 6.0, si consiglia di non deselezionare la casella ☒ **Proteggi il processo di installazione**. L'abilitazione della protezione dei moduli consente l'esecuzione della procedura corretta del rollback dell'installazione selezionare nel caso in cui si verificano errori durante l'operazione. Durante un nuovo tentativo di installazione di un'applicazione, si consiglia di non deselezionare questa casella.

Se l'applicazione viene installata in remoto mediante il **Desktop remoto di Windows**, è consigliabile deselezionare la casella ☒ **Proteggi il processo di installazione**. In caso contrario, la procedura di installazione potrebbe essere eseguita in maniera non corretta o non completata affatto.

Se si desidera che le esclusioni consigliate da Microsoft vengano aggiunte automaticamente all'elenco delle esclusioni, selezionare la casella ☒ **Aggiungi esclusioni Microsoft**.

Se si desidera aggiungere il percorso di avp.com alla variabile d'ambiente %Path% al termine dell'installazione, selezionare la casella ☒ **Aggiungi variabili d'ambiente**.

Per procedere con l'installazione, fare clic sul pulsante **Installa**.

Durante l'installazione dei componenti di Kaspersky Anti-Virus che intercettano traffico di rete, vengono terminate le connessioni di rete correnti. La maggior parte delle connessioni terminate viene ripristinata dopo un breve intervallo di tempo.

PASSAGGIO 11. COMPLETAMENTO DELL'INSTALLAZIONE

La finestra **Installazione completa** contiene informazioni sul completamento dell'installazione di Kaspersky Anti-Virus sul computer.

Per eseguire la Configurazione guidata iniziale, premere il pulsante **Avanti**.

Se per completare con successo l'installazione viene richiesto di riavviare il computer, viene visualizzata una notifica speciale.

INSTALLAZIONE DELL'APPLICAZIONE DA RIGA DI COMANDO

► Per installare Kaspersky Anti-Virus 6.0 for Windows Servers MP4, digitare la seguente riga di comando:

```
msiexec /i <nome_pacchetto>
```

Verrà eseguita l'installazione guidata (vedere la sezione "Installazione mediante procedura guidata" a pag. [16](#)). Al termine dell'installazione dell'applicazione, viene richiesto il riavvio del computer.

➤ *Per eseguire l'installazione in modalità non interattiva (senza avviare la procedura guidata), digitare quanto segue:*

```
msiexec /i <nome_pacchetto> /qn
```

In tal caso, il computer deve essere riavviato manualmente al termine dell'installazione dell'applicazione. Per riavviare automaticamente il computer, digitare la seguente riga di comando:

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

È possibile eseguire il riavvio automatico solo nella modalità di installare non interattiva (con il comando /qn).

➤ *Per installare l'applicazione con una password, che conferma l'autorizzazione a rimuovere l'applicazione, digitare quanto segue:*

```
msiexec /i <package_name> KLUNINSTPASSWD=***** – per l'installazione dell'applicazione in modalità interattiva;
```

```
msiexec /i <nome_pacchetto> KLUNINSTPASSWD=***** /qn – per l'installazione dell'applicazione in modalità non interattiva senza riavviare il computer;
```

```
msiexec /i <nome_pacchetto> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn – per l'installazione dell'applicazione in modalità non interattiva con riavvio del computer.
```

Per l'installazione di Kaspersky Anti-Virus in modalità non interattiva, è supportata la lettura del file setup.ini. Tale file contiene impostazioni generali per l'installazione dell'applicazione, il file di configurazione *instal.cfg* (vedere la sezione Importazione delle impostazioni di protezione a pag. [111](#)) e il file della chiave di licenza. Tali file devono trovarsi nella stessa cartella del pacchetto di installazione di Kaspersky Anti-Virus.

INSTALLAZIONE DALL'EDITOR OGGETTI CRITERI DI GRUPPO

Mediante l'**editor Oggetti criteri di gruppo** è possibile installare, aggiornare e rimuovere Kaspersky Anti-Virus su workstation aziendali appartenenti al dominio, senza l'impiego di Kaspersky Administration Kit.

INSTALLAZIONE DELL'APPLICAZIONE

➤ *Per installare Kaspersky Anti-Virus, eseguire le seguenti operazioni:*

1. Creare una cartella di rete condivisa sul computer, che agirà da controller di dominio, e inserirvi il pacchetto di installazione di Kaspersky Anti-Virus in formato MSI.

Inoltre, in tale directory è possibile inserire il file *setup.ini*, contenente l'elenco delle impostazioni dell'installazione di Kaspersky Anti-Virus, il file di configurazione *install.cfg* (vedere la sezione Importazione delle impostazioni di protezione a pag. [111](#)) e il file della chiave di licenza.

2. Dalla console standard MMC, aprire l'**editor Oggetti criteri di gruppo** (per informazioni dettagliate sul funzionamento di questo editor fare riferimento al sistema di Guida di Microsoft Windows).
3. Creare un nuovo pacchetto. Per eseguire questa operazione, selezionare **Oggetti criteri di gruppo / Configurazione del computer/ Configurazione dell'applicazione / Installazione del software** dalla struttura ad albero della console e utilizzare il comando **Crea / Pacchetto** dal menu di scelta rapida.

Nella finestra visualizzata, specificare il percorso della cartella di rete condivisa in cui si trova il pacchetto di installazione di Kaspersky Anti-Virus. Nella finestra di dialogo **Distribuzione dell'applicazione**, selezionare l'impostazione **Assegnata**, quindi premere il pulsante **OK**.

I criteri di gruppo verranno applicati a ciascuna workstation alla successiva registrazione di computer nel dominio. Di conseguenza, Kaspersky Anti-Virus verrà installato su tutti i computer.

DESCRIZIONE DELLE IMPOSTAZIONI DEL FILE SETUP.INI

Il file *setup.ini*, che si trova nella directory del pacchetto di installazione di Kaspersky Anti-Virus, viene utilizzato per l'installazione dell'applicazione in modalità non interattiva da riga di comando o dall'editor Oggetti criteri di gruppo. Tale file contiene le impostazioni indicate di seguito:

[Setup] – impostazioni generali per l'installazione dell'applicazione.

- **InstallDir**=<percorso della cartella di installazione dell'applicazione>.
- **Reboot**=yes|no – definisce se il computer deve riavviarsi al termine dell'installazione dell'applicazione (il riavvio non viene eseguito per impostazione predefinita).
- **SelfProtection**=yes|no – definisce se la funzione di Auto-difesa di Kaspersky Anti-Virus deve essere abilitata durante l'installazione (la funzione è abilitata per impostazione predefinita).

[Components] – selezione di componenti dell'applicazione da installare. Se in tale gruppo non sono contenuti componenti, l'applicazione verrà installata integralmente.

- **FileMonitor**=yes|no – installazione del componente Anti-Virus File.

[Tasks] – abilitazione attività di Kaspersky Anti-Virus. Se non è specificata alcuna attività, al termine dell'installazione verranno abilitate tutte le attività. Se è specificata almeno un'attività, quelle non presenti in elenco non verranno installate.

- **ScanMyComputer**=yes|no – attività di scansione completa.
- **ScanStartup**=yes|no – attività di scansione rapida.
- **Scan**=yes|no – attività di scansione.
- **Updater**=yes|no – attività di aggiornamento per i database e i moduli del programma.

È possibile utilizzare i valori 1, on, enable, enabled anziché il valore **yes** e il valore 0, off, disable, disabled anziché il valore **no**.

AGGIORNAMENTO DELLA VERSIONE DELL'APPLICAZIONE

➡ Per aggiornare la versione di Kaspersky Anti-Virus, eseguire le seguenti operazioni:

1. Inserire in una cartella di rete condivisa il pacchetto di installazione contenente gli aggiornamenti di Kaspersky Anti-Virus in formato .msi.
2. Aprire l'**editor Oggetti criteri di gruppo** e creare un nuovo pacchetto mediante la procedura descritta in precedenza.
3. Selezionare il nuovo pacchetto dall'elenco e utilizzare il comando **Proprietà** dal menu di scelta rapida. Selezionare la scheda **Aggiornamenti** nella finestra delle proprietà del pacchetto e specificare il pacchetto contenente il pacchetto di installazione della versione precedente di Kaspersky Anti-Virus. Per installare una versione aggiornata di Kaspersky Anti-Virus salvando le impostazioni di protezione, selezionare l'opzione di installazione con sovrascrittura del pacchetto esistente.

I criteri di gruppo verranno applicati a ciascuna workstation alla successiva registrazione di computer nel dominio.

I computer che eseguono Microsoft Windows 2000 Server non supportano l'aggiornamento di Kaspersky Anti-Virus

tramite l'editor **Oggetti criteri di gruppo**.

RIMOZIONE DELL'APPLICAZIONE

➡ Per rimuovere Kaspersky Anti-Virus, eseguire le seguenti operazioni:

1. Aprire nella **editor Oggetti criteri di gruppo**.
2. Selezionare **Oggetti criteri di gruppo / Configurazione del computer/ Configurazione dell'applicazione / Installazione del software** nella struttura ad albero della console.

Selezionare il pacchetto di Kaspersky Anti-Virus dall'elenco, aprire il menu di scelta rapida ed eseguire il comando **Tutte le attività/ Rimuovi**.

Nella finestra di dialogo **Rimozione applicazioni in corso**, selezionare **Rimuovere immediatamente l'applicazione dai computer di tutti gli utenti**, di modo che Kaspersky Anti-Virus verrà rimosso al riavvio successivo.

GUIDA INTRODUTTIVA

Durante la creazione di Kaspersky Anti-Virus, gli specialisti di Lab si sono posti l'obiettivo, tra gli altri, di fornire la configurazione ottimale dell'applicazione.

Per agevolare l'utente, le fasi di configurazione preliminari sono state combinate nell'interfaccia unificata della Configurazione guidata iniziale che si avvia subito dopo il completamento della procedura di installazione dell'applicazione. Seguendo le istruzioni della procedura guidata, è possibile attivare il programma, configurare le impostazioni per gli aggiornamenti e l'avvio delle attività di scansione anti-virus, nonché configurare la protezione mediante password dell'accesso all'applicazione.

Al termine dell'installazione e dopo il riavvio del programma, si consiglia di eseguire la procedura indicata di seguito:

- Valutare lo stato di protezione corrente (vedere la sezione "Gestione della protezione" a pag. [29](#)) per assicurare l'impostazione del livello di protezione appropriato da parte di Kaspersky Anti-Virus.
- Aggiornare l'applicazione (vedere la sezione Aggiornamento dell'applicazione a pag. [28](#)) (a meno che tale operazione non sia stata già eseguita mediante la configurazione guidata o automaticamente subito dopo l'installazione dell'applicazione).
- Eseguire la scansione anti-virus del server (vedere la sezione "Scansione anti-virus del computer" a pag. [27](#)).

IN QUESTA SEZIONE

Configurazione guidata iniziale.....	23
Scansione anti-virus del computer	27
Aggiornamento dell'applicazione	28
Gestione delle licenze	28
Gestione della protezione.....	29
Sospendi protezione.....	30
Eliminazione dei problemi. Assistenza tecnica utente	31
Creazione di un file di traccia	31
Configurazione delle impostazioni dell'applicazione	32
Rapporti sul funzionamento dell'applicazione. File di dati	32

CONFIGURAZIONE GUIDATA INIZIALE

La configurazione guidata di Kaspersky Anti-Virus viene avviata al termine dell'installazione dell'applicazione. È progettata per consentire la configurazione delle impostazioni iniziali dell'applicazione, in base alle funzioni e alle attività del computer.

L'interfaccia della configurazione guidata riprende quella standard della procedura guidata di Microsoft Windows e consiste in una serie di passaggi che è possibile visualizzare mediante i pulsanti **Indietro** e **Avanti** o terminare mediante il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per terminare l'installazione dell'applicazione nel computer, è necessario eseguire tutti i passaggi della procedura guidata. Se le operazioni della procedura guidata vengono interrotte per qualche motivo, i valori delle impostazioni già

specificati non verranno salvati. Al successivo tentativo di esecuzione dell'applicazione, viene riavviata la configurazione guidata iniziale per modificare nuovamente le impostazioni.

UTILIZZO DEGLI OGGETTI SALVATI DALLA VERSIONE PRECEDENTE

Questa finestra della procedura guidata viene visualizzata quando si installa l'applicazione su una versione precedente di Kaspersky Anti-Virus. È possibile scegliere quali dati utilizzati nella versione precedente devono essere importati nella nuova versione. Tali dati possono essere oggetti in quarantena o del backup oppure impostazioni di protezione.

Per utilizzare quei dati nella nuova versione dell'applicazione, selezionare tutte le caselle necessarie.

ATTIVAZIONE DELL'APPLICAZIONE

La procedura di attivazione dell'applicazione consiste nella registrazione di una licenza mediante l'installazione di un file chiave. A seconda della licenza in uso, l'applicazione determinerà i privilegi esistenti e ne calcolerà le condizioni di utilizzo.

Il file chiave contiene informazioni di servizio necessarie per fare in modo che Kaspersky Anti-Virus sia completamente funzionale, nonché dati aggiuntivi:

- informazioni di assistenza, ovvero chi fornisce assistenza e dove può essere ottenuta;
- nome e numero della chiave e data di scadenza della licenza.

In base alla presenza di un file chiave o meno (nel caso in cui il file debba essere ricevuto dal server di Kaspersky Lab), saranno disponibili le seguenti opzioni per l'attivazione di Kaspersky Anti-Virus:

- Attivazione online (vedere a pag. [25](#)). Selezionare questa opzione se è stata acquistata una versione in commercio dell'applicazione ed è stato ottenuto un codice di attivazione. È possibile utilizzare tale codice per ottenere un file chiave per l'accesso alle funzionalità complete dell'applicazione per tutto il periodo di validità della licenza.
- Attivazione della versione di prova (vedere a pag. [25](#)). Utilizzare questa opzione di attivazione se si desidera installare la versione di prova dell'applicazione prima di procedere all'acquisto di una versione in commercio. Verrà fornito un file chiave gratuito valido per un periodo specificato nel contratto di licenza della versione di prova.
- Attivazione mediante un file chiave di licenza ottenuto in precedenza (vedere la sezione "Attivazione tramite un file chiave" a pag. [25](#)). Attivare l'applicazione mediante il file chiave di Kaspersky Anti-Virus 6.0 ottenuto in precedenza.
- Attivare successivamente. Se si sceglie questa opzione, la fase di attivazione verrà ignorata. L'applicazione sarà installata sul computer e sarà possibile accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (sarà disponibile un solo aggiornamento dell'applicazione subito dopo l'installazione). L'opzione **Attivare successivamente** è disponibile solo al primo avvio dell'Attivazione guidata. Agli avvii successivi della procedura guidata, se l'applicazione risulta già attivata, sarà disponibile l'opzione **Elimina file di chiave** per eseguire la rimozione.

Se le prime due opzioni di attivazione dell'applicazione sono entrambe selezionate, l'applicazione verrà attivata tramite il server Web di Kaspersky Lab. Tale operazione richiede la connessione a Internet. Prima di avviare l'attivazione, verificare e modificare, se necessario, le impostazioni di connessione alla rete nella finestra che verrà visualizzata premendo il pulsante **Impostazioni LAN**. Per ulteriori dettagli sulle impostazioni di rete, contattare l'amministratore di rete o il provider Internet.

Se, al momento dell'installazione non è disponibile una connessione Internet, è possibile eseguire l'attivazione successivamente, tramite l'interfaccia dell'applicazione oppure mediante connessione a Internet da un computer diverso per ottenere una chiave, utilizzando un codice di attivazione ricevuto mediante registrazione al sito Web del servizio di assistenza tecnica di Kaspersky Lab.

È inoltre possibile attivare l'applicazione tramite il Kaspersky Administration Kit. Per effettuare questa operazione, è necessario creare un'attività di installazione del file chiave (vedere pag. [126](#)). Per ulteriori dettagli fare riferimento alla guida di Kaspersky Administration Kit.

VEDERE ANCHE

Attivazione online	25
Come ottenere un file chiave	25
Attivazione tramite un file chiave	25
Completamento dell'attivazione	26

ATTIVAZIONE ONLINE

L'attivazione online viene eseguita immettendo un codice di attivazione inviato tramite e-mail per l'acquisto di Kaspersky Anti-Virus tramite Internet. Se si acquista l'applicazione in confezione presso un rivenditore, il codice di attivazione è stampato sulla custodia cartacea del disco di installazione.

IMMISSIONE DEL CODICE DI ATTIVAZIONE

A questo punto, è necessario immettere il codice di attivazione. Tale codice è una sequenza di numeri e lettere divisi da trattini in quattro gruppi di cinque simboli senza spazi. Ad esempio, 11111-11111-11111-11111. Il codice deve essere immesso in caratteri dell'alfabeto latino.

Immettere le informazioni personali nella parte inferiore della finestra: nome completo, indirizzo e-mail, stato e città di residenza. Queste informazioni potrebbero essere necessarie per identificare un utente registrato se, ad esempio, la licenza è stata smarrita o rubata. In tal caso, è possibile ottenere un altro codice di attivazione tramite le informazioni personali.

COME OTTENERE UN FILE CHIAVE

La configurazione guidata esegue la connessione ai server Internet di Kaspersky Lab e invia i dati di registrazione, tra cui il codice di attivazione e le informazioni di contatto. Una volta stabilita la connessione, il codice di attivazione e le informazioni di contatto vengono verificate. Se il codice di attivazione viene accettato, si riceve un file chiave della licenza che verrà quindi installato automaticamente. Al termine dell'attivazione, viene visualizzata la finestra contenente le informazioni dettagliate sulla licenza ottenuta.

Se il codice di attivazione non viene accettato, viene visualizzato il relativo avviso. In questo caso, contattare il rivenditore del software presso il quale è stato effettuato l'acquisto per le informazioni del caso.

Se viene superato il numero consentito di attivazioni con il codice di attivazione specifico, viene visualizzato il relativo avviso. Il processo di attivazione viene interrotto e l'applicazione consente di contattare il servizio Assistenza tecnica di Kaspersky Lab.

ATTIVAZIONE DELLA VERSIONE DI PROVA

Utilizzare questa opzione di attivazione se si desidera installare una versione di prova di Kaspersky Anti-Virus prima di procedere all'acquisto di una versione commerciale. Verrà fornita una licenza gratuita che sarà valida per il periodo specificato nel contratto di licenza della versione di prova. Alla scadenza della licenza, non sarà possibile attivare nuovamente la versione di prova.

ATTIVAZIONE TRAMITE UN FILE CHIAVE

Se si dispone di file chiave, è possibile utilizzarlo per attivare Kaspersky Anti-Virus. Per effettuare questa operazione, premere il pulsante **Sfoglia** e selezionare il percorso del file con estensione .key.

Dopo aver installato la chiave, nella parte inferiore della finestra verranno visualizzate le informazioni sulla licenza: numero della licenza, tipo di licenza (commerciale, beta, di prova e così via), data di scadenza della licenza e numero di host.

COMPLETAMENTO DELL'ATTIVAZIONE

La configurazione guidata informa l'utente che Kaspersky Anti-Virus è stato attivato correttamente. Vengono inoltre fornite informazioni sulla licenza: numero della licenza, tipo di licenza (commerciale, beta, di prova e così via), data di scadenza e numero di host.

CONFIGURAZIONE DELLE IMPOSTAZIONI DI AGGIORNAMENTO

L'efficacia della protezione del computer è strettamente collegata all'esecuzione di aggiornamenti periodici dei database e dei moduli del programma. In questa finestra della procedura guidata viene chiesto di selezionare la modalità di aggiornamento dell'applicazione e di modificare le impostazioni di pianificazione:

-  **Automaticamente.** Kaspersky Anti-Virus verifica a intervalli specificati la disponibilità di pacchetti di aggiornamento nell'origine degli aggiornamenti. La frequenza della scansione può essere aumentata quando si verificano periodi di attacchi frequenti e ridotta nei periodi più tranquilli. Se vengono rilevati nuovi aggiornamenti, questi vengono scaricati e installati nel computer. Questa è la modalità predefinita.
-  **Ogni 2 ore** (la frequenza può variare in base alle impostazioni di pianificazione). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione. È possibile modificare le impostazioni di pianificazione in un'altra finestra mediante il pulsante **Cambia**.
-  **Manualmente.** Se si seleziona questa opzione, gli aggiornamenti verranno eseguiti manualmente.

I database e i moduli dell'applicazione in dotazione con il pacchetto di installazione potrebbero essere obsoleti al momento dell'installazione dell'applicazione. Per questo motivo, si consiglia di procurarsi gli aggiornamenti più recenti dell'applicazione. A tal fine, cliccare su **Aggiorna ora**. A questo punto, dai siti di aggiornamento verranno scaricati gli aggiornamenti necessari e installati sul computer.

Se si desidera passare alla configurazione degli aggiornamenti (specificare le impostazioni di rete, selezionare un'origine di aggiornamento, eseguire un aggiornamento da un account utente specifico o abilitare il download degli aggiornamenti in un'origine locale), premere il pulsante **Impostazioni**.

CONFIGURAZIONE DELLA PIANIFICAZIONE DELLA SCANSIONE ANTI-VIRUS

La scansione delle aree selezionate alla ricerca di oggetti dannosi è una delle attività chiave nella protezione del computer.

Nell'installazione di Kaspersky Anti-Virus, vengono create tre attività di scansione anti-virus predefinite. In questa finestra della configurazione guidata viene chiesto di selezionare una modalità di esecuzione dell'attività di scansione:

Scansione Completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete. È possibile modificare le impostazioni di pianificazione nella finestra visualizzata premendo il pulsante **Cambia**.

Scansione Rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo. È possibile modificare le impostazioni di pianificazione nella finestra visualizzata premendo il pulsante **Cambia**.

LIMITAZIONE DELL'ACCESSO ALL'APPLICAZIONE

Un server può essere utilizzato da più persone con diversi livelli di conoscenza informatica, inoltre esiste malware in grado di disabilitare la protezione del computer. Per questo motivo è possibile accedere a Kaspersky Anti-Virus mediante password. L'utilizzo di una password consente di proteggere l'applicazione da tentativi non autorizzati di disabilitare la protezione, modificare le impostazioni o disinstallare l'applicazione.

Per abilitare la protezione tramite password, selezionare la casella ☒ **Abilita la protezione tramite password** e compilare i campi **Password** e **Conferma password**.

Specificare l'area alla quale si intende applicare la protezione tramite password selezionando una delle opzioni seguenti:

- ☒ **Tutte le operazioni (ad eccezione delle notifiche di eventi pericolosi).** La password verrà richiesta per qualsiasi azione relativa all'applicazione, eccetto che per le risposte alle notifiche di rilevamento di oggetti pericolosi.
- ☒ **Operazioni selezionate:**
 - ☒ **Configurazione delle impostazioni dell'applicazione** – la password viene richiesta per modificare le impostazioni di Kaspersky Anti-Virus.
 - ☒ **Chiusura applicazione in corso** – la password viene richiesta per chiudere l'applicazione.
 - ☒ **Disabilitazione componenti della protezione e arresto delle attività di scansione** – la password viene richiesta per disabilitare Anti-Virus File o interrompere un'attività di scansione anti-virus.
 - ☒ **Disabilitazione del criterio Kaspersky Administration Kit** – la password viene richiesta per rimuovere il computer dall'ambito dei criteri e delle attività di gruppo (quando si utilizza Kaspersky Administration Kit).
 - ☒ **Durante la disinstallazione dell'applicazione** – la password viene richiesta per rimuovere l'applicazione dal computer.

COMPLETAMENTO DELLA CONFIGURAZIONE GUIDATA

Nell'ultima finestra della procedura guidata, verrà visualizzato un messaggio che conferma l'avvenuta installazione e configurazione di Kaspersky Anti-Virus. È possibile avviare l'applicazione immediatamente selezionando ☒ **Avvia applicazione**.

Se durante l'installazione si è verificato un problema, ad esempio un'incompatibilità con altre applicazioni anti-virus, verrà richiesto di riavviare il computer.

SCANSIONE ANTI-VIRUS DEL COMPUTER

Poiché gli sviluppatori di malware fanno tutto il possibile per nascondere le azioni dei loro programmi, è facile non accorgersi della presenza di tali applicazioni nocive nel computer.

Una volta installato nel computer, Kaspersky Anti-Virus esegue automaticamente l'attività **Scansione Rapida**. Questa attività consiste nel cercare e neutralizzare i programmi nocivi negli oggetti caricati all'avvio del sistema.

Gli specialisti di Kaspersky Lab consigliano inoltre di eseguire l'attività di **Scansione Completa**.

➡ *Per avviare / interrompere un'attività di scansione anti-virus, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.

3. Premere il pulsante **Avvia scansione** per avviare la scansione. Se, durante l'avanzamento dell'attività, è necessario interromperne l'esecuzione, premere il pulsante **Interrompi scansione**.

AGGIORNAMENTO DELL'APPLICAZIONE

Per aggiornare Kaspersky Anti-Virus, è necessario disporre di una connessione a Internet.

Il pacchetto di installazione di Kaspersky Anti-Virus include i database che contengono firme delle minacce. Tali database potrebbero risultare già obsoleti al momento dell'installazione dell'applicazione, poiché Kaspersky Lab aggiorna regolarmente sia i database, che i moduli dell'applicazione.

Quando la configurazione guidata iniziale è attiva, è possibile selezionare la modalità di esecuzione dell'aggiornamento. Per impostazione predefinita, Kaspersky Anti-Virus verifica automaticamente la presenza di nuovi aggiornamenti sui server di Kaspersky Lab. Se il server contiene un nuovo insieme di aggiornamenti, Kaspersky Anti-Virus li scaricherà e li installerà automaticamente.

Per garantire una protezione completa del computer, si consiglia di aggiornare Kaspersky Anti-Virus immediatamente dopo l'installazione.

➡ Per aggiornare Kaspersky Anti-Virus autonomamente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Premere il pulsante **Avvia aggiornamento**.

GESTIONE DELLE LICENZE

Per poter funzionare, Kaspersky Anti-Virus richiede una licenza che viene fornita all'acquisto del prodotto. Tale licenza consente di utilizzare il prodotto non appena questo viene attivato.

A meno che non sia stata attivata una versione di prova, senza una licenza Kaspersky Anti-Virus viene eseguito nella modalità che consente di scaricare un solo aggiornamento. Al termine del periodo di prova, la versione di prova di Kaspersky Anti-Virus attivata non funziona più.

Se è stata attivata una versione di prova dell'applicazione, alla sua scadenza Kaspersky Anti-Virus non verrà avviato.

Quando la licenza commerciale scade, l'applicazione continua a funzionare, ma non sarà possibile aggiornare i database. Resta comunque possibile eseguire la scansione del computer per identificare la presenza di eventuali virus e utilizzare i componenti di protezione, ma solo attraverso i database aggiornati fino alla scadenza della licenza. Ciò significa che la protezione dai virus diffusi dopo la scadenza della licenza del programma non può essere garantita.

Per evitare di infettare il computer con nuovi virus, si consiglia di rinnovare la licenza di Kaspersky Anti-Virus. Due settimane prima della scadenza della licenza, verrà visualizzato un avviso. Durante un determinato periodo, a ogni avvio del programma verrà visualizzato un messaggio corrispondente.

Nella sezione **Licenza** della finestra principale di Kaspersky Anti-Virus sono contenute informazioni generali sulla licenza attualmente in uso (la licenza attiva e quelle aggiuntive, se installate): tipo di licenza (completa, di prova, beta), numero massimo di host, data di scadenza della licenza e numero di giorni mancanti alla data di scadenza. Per ulteriori dettagli sulla licenza, fare clic sul collegamento con il tipo di licenza attualmente in uso.

Per visualizzare il contratto di licenza dell'applicazione, fare clic sul pulsante **Visualizza il Contratto di licenza con l'utente finale**.

Per rimuovere la licenza, fare clic sul pulsante **Aggiungi / Elimina** e seguire tutte le istruzioni della procedura guidata successivamente visualizzata.

Kaspersky Lab propone offerte speciali per il rinnovo della licenza dei prodotti. Verificare sul sito Web di Kaspersky Lab la presenza di eventuali offerte speciali.

➡ Per acquistare o rinnovare una licenza, eseguire le seguenti operazioni:

1. Acquistare un nuovo file chiave o un codice di attivazione. Premere il pulsante **Acquista la licenza** (se l'applicazione non è stata attivata) oppure il pulsante **Rinnova la licenza**. Nella pagina Web visualizzata sono contenute informazioni dettagliate sui termini di acquisto della chiave dall'eStore di Kaspersky Lab o da distributori autorizzati. Se si effettua un acquisto online, una volta eseguito il pagamento verrà inviato un file chiave o un codice di attivazione via e-mail all'indirizzo specificato nel modulo d'ordine.
2. Attivare l'applicazione. Utilizzare il pulsante **Aggiungi /Elimina** nella sezione **Licenza** della finestra principale dell'applicazione oppure usare il comando **Attiva** dal menu di scelta rapida. Verrà eseguita l'attivazione guidata.

GESTIONE DELLA PROTEZIONE

I problemi nella protezione del computer vengono indicati dallo stato della protezione del computer (vedere la sezione "Finestra principale dell'applicazione³⁵" a pag.), che viene visualizzato dai cambiamenti dei colori dell'icona di stato della protezione e del pannello in cui si trova. Se il sistema di protezione presenta problemi, si consiglia di risolverli.



Fig. 1. Stato attuale della protezione del computer

È possibile visualizzare l'elenco dei problemi che si sono verificati, la descrizione e le soluzioni possibili, mediante l'impostazione guidata protezione (vedere figura in basso) che è possibile attivare facendo clic sul collegamento [Ripara](#) (vedere figura in alto).

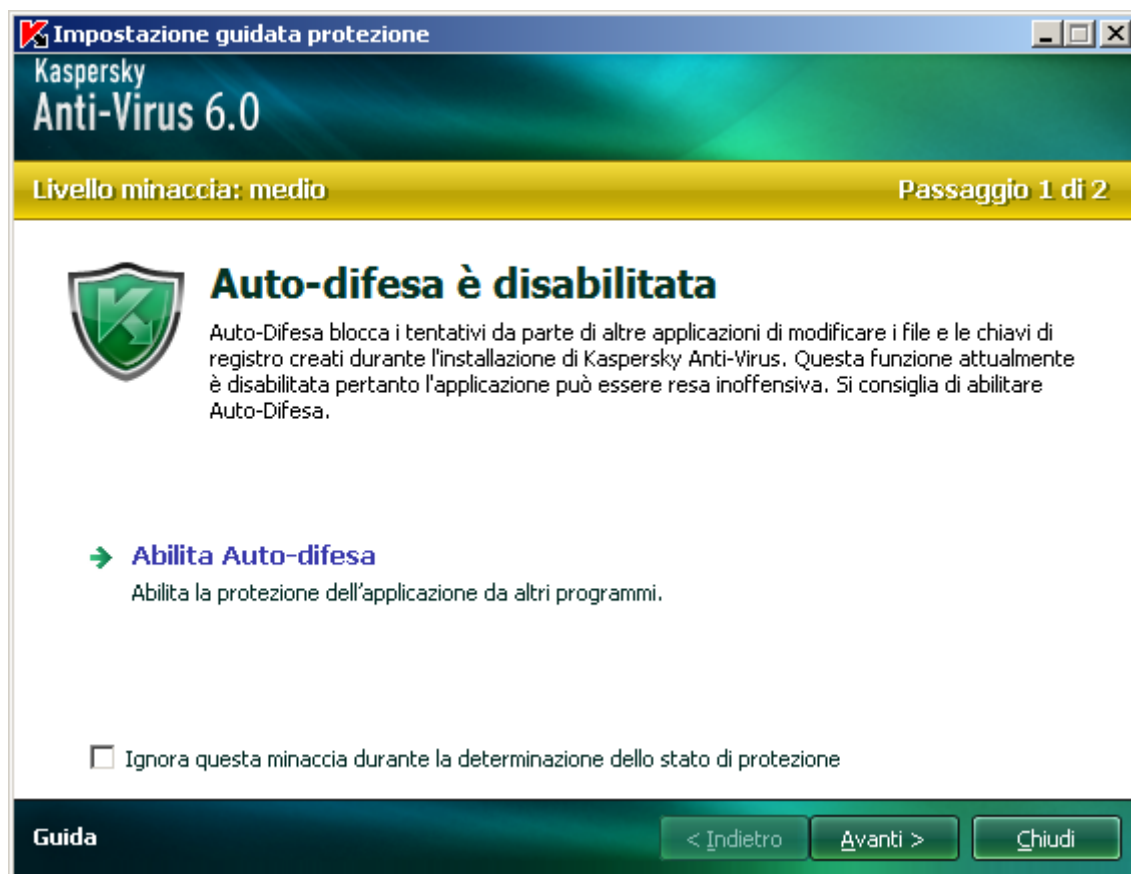


Fig. 2. Risoluzione dei problemi di protezione

Viene visualizzato l'elenco dei problemi correnti. I problemi vengono ordinati in base al livello di criticità: innanzitutto, i problemi più critici, ovvero quelli visualizzati con l'icona di stato rossa, quindi quelli meno importanti, ovvero con l'icona di stato gialla, infine i messaggi informativi. Per ciascun problema viene fornita una descrizione dettagliata e sono disponibili le azioni seguenti:

- *Eliminazione immediata.* Utilizzando i collegamenti appropriati, è possibile passare alla risoluzione del problema, ovvero l'azione consigliata.
- *Rimanda l'eliminazione.* Se non si riesce a eliminare il problema immediatamente, è possibile rimandare questa azione. Selezionare la casella ☒ **Ignora questa minaccia durante la determinazione dello stato di protezione** affinché la minaccia non abbia conseguenze sullo stato di protezione corrente.

Si noti che questa opzione non è disponibile per i problemi più seri. Tali problemi comprendono ad esempio gli oggetti dannosi non disinfettati, il blocco di uno o più componenti o il danneggiamento dei file dell'applicazione. Tale tipo di problemi devono essere eliminati nella maniera più rapida possibile.

SOSPENSIONE DELLA PROTEZIONE

La sospensione della protezione consiste nella disabilitazione temporanea di Anti-Virus File.

➤ *Per sospendere Kaspersky Anti-Virus, eseguire le seguenti operazioni:*

1. Nel Menu di scelta rapida dell'applicazione, selezionare la voce **Sospendi della protezione**.
2. Nella finestra **Sospendi protezione** visualizzata, dalle opzioni suggerite selezionare il periodo di tempo in cui si desidera che la protezione sia attivata.

ELIMINAZIONE DEI PROBLEMI. ASSISTENZA TECNICA UTENTE

Se i problemi si verificano durante il funzionamento di Kaspersky Anti-Virus, per trovare la soluzione al problema si consiglia in primo luogo di consultare la Guida in linea. In secondo luogo, si consiglia di consultare la Knowledge Base di Kaspersky Lab (<http://support.kaspersky.com>). La *Knowledge Base* è una sezione apposita del sito Web dell'Assistenza tecnica di Kaspersky Lab che contiene i consigli per i prodotti Kaspersky Lab e le risposte alle domande più frequenti. Si può provare a trovare una risposta alla propria domanda o una soluzione al proprio problema utilizzando questa risorsa.

➤ *Per utilizzare la Knowledge Base, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Servizio di supporto tecnico**.

Un'altra risorsa per ottenere informazioni sull'uso dell'applicazione è il forum degli utenti di Kaspersky Lab. Si tratta anche in questo caso di una sezione distinta del sito Web dell'Assistenza tecnica che contiene domande, feedback e richieste degli utenti. È possibile visualizzare gli argomenti principali, lasciare un proprio feedback o trovare risposte alle proprie domande.

➤ *Per aprire il forum degli utenti, eseguire le seguenti operazioni:*

1. Aprire nella finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Forum utenti**.

Se non si trova una soluzione al problema nella Guida, nella Knowledge Base o nel Forum degli utenti, si consiglia di contattare l'Assistenza tecnica di Kaspersky Lab.

CREAZIONE DI UN FILE DI TRACCIA

Dopo l'installazione di Kaspersky Anti-Virus, possono verificarsi problemi nel sistema operativo o nel funzionamento di singole applicazioni. La causa più probabile è un conflitto tra l'applicazione e il software installato nel computer o con i driver dei componenti del computer. Per consentire agli specialisti di Kaspersky Lab di risolvere il problema, potrebbe essere necessario creare un file di traccia.

➤ *Per creare il file di traccia:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Tracce**.
4. Nella finestra **Informazioni per il servizio di Assistenza tecnica** visualizzata, utilizzare l'elenco a discesa della sezione **Tracce** per selezionare il livello di traccia. Tale livello deve essere impostato in base alle indicazioni

dello specialista dell'Assistenza tecnica. In assenza di istruzioni da parte dell'Assistenza tecnica, si consiglia di utilizzare il livello di traccia **500**.

5. Per iniziare il processo di creazione di una traccia, fare clic sul pulsante **Attiva**.
6. Riprodurre la situazione che ha causato il problema.
7. Per arrestare il processo di creazione della traccia, cliccare sul bottone **Disattiva**.

CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

La finestra delle impostazioni dell'applicazione (vedere a pag. [72](#)), accessibile dalla finestra principale premendo il pulsante **Impostazioni**, consente di accedere rapidamente alle impostazioni i Kaspersky Anti-Virus 6.0.

RAPPORTI SUL FUNZIONAMENTO DELL'APPLICAZIONE. FILE DI DATI

Il funzionamento di Anti-Virus File e l'esecuzione di ciascuna scansione anti-virus e attività di aggiornamento vengono registrati in un rapporto (vedere a pag. [87](#)). Per visualizzare i rapporti, utilizzare il pulsante **Rapporto** che si trova in basso a destra nella finestra principale.

Gli oggetti messi in quarantena (vedere a pag. [88](#)) o posizionati nel backup (vedere a pag. [89](#)) da Kaspersky Anti-Virus, sono denominati *file dati dell'applicazione*. Premendo il pulsante **Rilevati**, viene aperta la finestra **Archiviazione** in cui è possibile eseguire qualsiasi operazione desiderata su tali oggetti.

INTERFACCIA DELL'APPLICAZIONE

Kaspersky Anti-Virus presenta un'interfaccia di facile utilizzo. In questo capitolo vengono messe in risalto le funzioni di base:

- icona dell'area di notifica;
- menu di scelta rapida;
- finestra principale;
- notifiche;
- Finestra delle impostazioni di Kaspersky Anti-Virus.

IN QUESTA SEZIONE

Icona dell'area di notifica della barra delle applicazioni	33
Menu di scelta rapida	34
Finestra principale dell'applicazione	35
Notifiche	36
Finestra delle impostazioni dell'applicazione	37

ICONA DELL'AREA DI NOTIFICA DELLA BARRA DELLE APPLICAZIONI

Immediatamente dopo l'installazione di Kaspersky Anti-Virus, nell'area di notifica viene visualizzata l'icona corrispondente.

L'icona è una sorta di indicatore delle operazioni di Kaspersky Anti-Virus. Riflette inoltre lo stato della protezione e visualizza numerose funzioni di base eseguite dall'applicazione.

Se l'icona è attiva  (è colorata), significa che la protezione è abilitata del server. If the icon is inactive  (black and white), this means that protection is disabled.

L'icona di Kaspersky Anti-Virus cambia in funzione dell'operazione eseguita:

-  – scansione in corso di un file aperto, salvato o eseguito dall'utente o da un programma.
-  – aggiornamento in corso del database e del modulo di Kaspersky Anti-Virus.
-  – si è verificato un errore nel funzionamento di alcuni componenti di Kaspersky Anti-Virus.

L'icona consente inoltre di accedere ai componenti di base dell'interfaccia dell'applicazione: il menu di scelta rapida e la finestra principale.

Per aprire il menu di scelta rapida, fare clic con il pulsante destro del mouse sull'icona dell'applicazione.

Per aprire la finestra principale di Kaspersky Anti-Virus, fare clic sull'icona dell'applicazione.

MENU DI SCELTA RAPIDA

Il menu di scelta rapida consente di eseguire le attività di protezione di base e contiene le seguenti voci:

- **Scansione completa** – avvia una scansione completa del computer per individuare eventuali oggetti dannosi. Durante l'operazione vengono esaminati gli oggetti di tutte le unità, inclusi i supporti rimovibili.
- **Scansione** – consente di selezionare gli oggetti e avviare la scansione anti-virus. Per impostazione predefinita, l'elenco contiene diversi oggetti, quali la memoria di sistema, gli oggetti di avvio, i database della posta elettronica, tutte le unità del server e così via. È possibile ingrandire l'elenco, selezionare altri oggetti e avviare la scansione anti-virus.
- **Aggiornamento** – avvia gli aggiornamenti dei moduli e i database di Kaspersky Anti-Virus e li installa sul computer.
- **Attiva** – attiva l'applicazione. Per diventare un utente registrato con accesso alle piene funzionalità dell'applicazione e all'assistenza tecnica, è necessario attivare la propria versione di Kaspersky Anti-Virus. Questa voce di menu è disponibile solo se l'applicazione non è attivata.
- **Impostazioni** – consente di visualizzare e modificare le impostazioni di Kaspersky Anti-Virus.
- **Kaspersky Anti-Virus** – apre la finestra principale dell'applicazione.
- **Sospendi protezione / Riprendi protezione** – disabilita o abilita temporaneamente Anti-Virus File. Questa voce di menu non ha effetto sull'esecuzione della scansione anti-virus o sugli aggiornamenti dell'applicazione.
- **Disabilita criteri / Abilita criteri** - disabilita o abilita temporaneamente i criteri mediante il Kaspersky Administration Kit, durante il funzionamento dell'applicazione. Questa voce di menu consente la rimozione del computer dall'ambito operativo di criteri e attività di gruppo. Questa opzione viene gestita mediante password (vedere la sezione "Restrizione dell'accesso all'applicazione" a pag. [82](#)). La voce di menu viene visualizzata solo se è stata impostata una password.
- **Informazioni su** – visualizza la finestra contenente le informazioni sull'applicazione.
- **Esci** – chiude Kaspersky Anti-Virus (se questa opzione è selezionata, l'applicazione viene rimossa dalla RAM del computer).

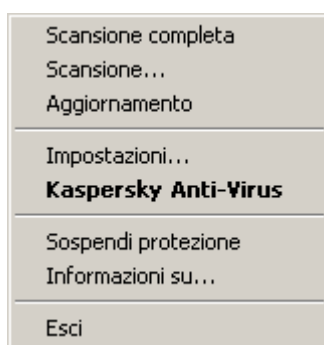


Fig. 3. Menu di scelta rapida

Se è in esecuzione un'attività di scansione anti-virus, il nome di quest'ultima verrà visualizzato nel menu di scelta rapida con l'indicazione dell'avanzamento in percentuale. Dopo la selezione di un'attività, nella finestra dei rapporti è possibile visualizzare i risultati delle prestazioni correnti.

FINESTRA PRINCIPALE DELL'APPLICAZIONE

La finestra principale dell'applicazione può essere divisa in tre parti:

- La parte superiore della finestra indica l'attuale stato di protezione del computer.



Fig. 4. Stato attuale della protezione del computer

Vi sono tre valori possibili dello stato di protezione: ciascuno di essi viene indicato da un determinato colore, analogamente a un semaforo. Il verde indica che la protezione del computer è di livello adeguato, il giallo ed il rosso evidenziano la presenza di minacce alla protezione nella configurazione del sistema o nel funzionamento di Kaspersky Anti-Virus. Oltre ai programmi dannosi, vengono considerati minacce, ad esempio, anche i database dell'applicazione obsoleti.

Le minacce alla protezione devono essere eliminate non appena compaiono. Per ottenere informazioni dettagliate su di esse ed eliminarle rapidamente, utilizzare il collegamento **Ripara** (vedere figura in alto).

- La parte sinistra della finestra consente di accedere rapidamente a qualsiasi funzione dell'applicazione, incluse le attività di scansione anti-virus, di aggiornamento e così via.



Fig. 5. Parte sinistra della finestra principale

- La parte destra della finestra contiene informazioni sulla funzione dell'applicazione selezionata nella parte sinistra, consente di configurare tali funzioni e offre strumenti per eseguire attività di scansione anti-virus, scaricare aggiornamenti e così via.



Fig. 6. Parte destra della finestra principale

È inoltre possibile utilizzare le opzioni seguenti:

- Il pulsante **Impostazioni** – per aprire la finestra delle impostazioni (vedere a pag. [72](#)).
- Il collegamento **Guida** – per aprire la Guida di Kaspersky Anti-Virus.
- Il pulsante **Rilevati** – per utilizzare i file di dati dell'applicazione (vedere a pag. [86](#)).
- Il pulsante **Rapporto** – per aprire i rapporti sul funzionamento dei componenti dell'applicazione (vedere a pag. [87](#)).
- Il collegamento **Supporto** – per aprire la finestra contenente le informazioni sul sistema e i collegamenti alle risorse informative di Kaspersky Lab (vedere a pag. [31](#)) (sito del servizio dell'assistenza tecnica, forum).

NOTIFICHE

Se durante l'esecuzione di Kaspersky Anti-Virus si verificano degli eventi, sullo schermo vengono visualizzate notifiche speciali sotto forma di messaggi a comparsa al di sopra dell'icona dell'applicazione sulla barra delle applicazioni di Microsoft Windows.

A seconda della criticità dell'evento per la protezione del computer, potrebbero essere visualizzati i tipi di notifica seguenti:

- **Allarme.** Si è verificato un evento di importanza critica, come il rilevamento di un virus. È necessario decidere subito come affrontare la minaccia. Questo tipo di notifica è visualizzata in rosso.

- **Attenzione.** Si è verificato un evento potenzialmente pericoloso, come il rilevamento di un oggetto potenzialmente pericoloso. È necessario stabilire quanto è pericoloso l'evento in questione. Questo tipo di notifica è visualizzata in giallo.
- **Informazioni.** Questa notifica fornisce informazioni su eventi non critici. Le notifiche di priorità minore hanno il codice colore verde.

VEDERE ANCHE

Tipi di notifiche [102](#)

FINESTRA DELLE IMPOSTAZIONI DELL'APPLICAZIONE

Dalla finestra principale è possibile aprire la finestra delle impostazioni di Kaspersky Anti-Virus. A tale scopo, cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.

La finestra delle impostazioni riprende la finestra principale:

- la parte sinistra della finestra consente di accedere in maniera rapida e facile alle impostazioni di Anti-Virus File, attività di scansione anti-virus e di aggiornamento e le opzioni del programma;
- la parte destra della finestra contiene un elenco di impostazioni del componente Anti-Virus File o di un'attività selezionati nella parte sinistra della finestra.

VEDERE ANCHE

Configurazione delle impostazioni dell'applicazione [72](#)

ANTI-VIRUS FILE

Anti-Virus File impedisce l'infezione del file system del computer. Tale strumento viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer. Esamina tutti i file che vengono aperti, salvati o eseguiti.

Per impostazione predefinita, mediante il componente Anti-Virus File esegue solo la scansione dei file nuovi o modificati. Una serie di impostazioni, denominata livello di protezione, determina la modalità di scansione dei file. Se il componente Anti-Virus File rileva una minaccia, eseguirà l'azione preimpostata.

Il livello di protezione dei file e della memoria sul computer è determinato dalle combinazioni di impostazioni seguenti:

- impostazioni dell'ambito di protezione;
- impostazioni che definiscono il metodo di scansione utilizzato;
- impostazioni che definiscono la scansione di file composti (così come la scansione di file composti di grandi dimensioni);
- impostazioni che definiscono la modalità di scansione;
- impostazioni utilizzate per sospendere il funzionamento del componente (in base alla pianificazione, durante il funzionamento di applicazioni selezionate).

➡ *Per modificare le impostazioni di Anti-Virus File:*

1. Aprire la finestra principale dell'applicazione e premere il pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Algoritmo di funzionamento del componente.....	39
Modifica del livello di protezione	40
Modifica delle azioni da eseguire sugli oggetti rilevati	40
Creazione di un ambito di protezione	41
Utilizzo dell'analisi euristica	42
Ottimizzazione della scansione	43
Scansione dei file composti	43
Scansione di file composti di grandi dimensioni	44
Modifica della modalità di scansione	44
Tecnologia di scansione	45
Sospensione del componente: creazione di una pianificazione	45
Sospensione del componente: creazione di un elenco di applicazioni	46
Ripristino delle impostazioni di protezione predefinite	46
Statistiche di Anti-Virus File	47
Trattamento posticipato degli oggetti.....	47

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Il componente *Anti-Virus File* viene caricato all'avvio del sistema operativo, viene eseguito nella memoria del computer ed esamina tutti i file che vengono aperti, salvati o eseguiti.

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

1. Il componente intercetta gli accessi a ciascun file da parte dell'utente o di qualsiasi programma.
2. Anti-Virus File esegue la scansione dei database iChecker e iSwift alla ricerca di informazioni sul file individuato e determina se è necessario eseguire la scansione del file, in base alle informazioni recuperate.

La scansione include i seguenti passaggi:

- Il file viene esaminato alla ricerca di virus. Gli oggetti vengono rilevati mediante comparazione con i database dell'applicazione. Il database contiene le descrizioni di tutti i programmi dannosi e le minacce attualmente noti, nonché i metodi per elaborarli.
- Al termine dell'analisi, è possibile eseguire una delle azioni di Kaspersky Anti-Virus seguenti:
 - a. Se nel file viene rilevato codice dannoso, File Anti-Virus blocca il file, ne crea una copia di *backup* e tenta di disinfettarlo. Al termine della disinfezione del file, quest'ultimo diventa utilizzabile da parte dell'utente. Se la disinfezione non riesce, il file viene eliminato.

- b. Se viene rilevato codice potenzialmente dannoso, senza alcuna garanzia dell'effettiva pericolosità, il file viene comunque disinfettato e quindi inviato in un'area di archiviazione speciale denominata *Quarantena*.
- c. Se nel file non viene rilevato codice dannoso, esso viene immediatamente ripristinato.

Se viene rilevato un file infetto o potenzialmente infetto, verrà visualizzata una notifica. È necessario reagire alla notifica sottoponendo il file a ulteriore elaborazione:

- mettere in quarantena l'oggetto, in modo da poter esaminare ed elaborare successivamente la nuova minaccia con i database aggiornati;
- eliminare l'oggetto;
- ignorare la situazione, se si ritiene che l'oggetto non sia dannoso.

VEDERE ANCHE

Anti-Virus File [38](#)

MODIFICA DEL LIVELLO DI PROTEZIONE

Il livello di protezione è definito come configurazione preimpostata delle impostazioni del componente Anti-Virus File. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. Per decidere quale livello selezionare, l'utente deve considerare le condizioni operative e la situazione corrente.

- Se il computer ha una grande possibilità di infettarsi, è necessario selezionare il livello di protezione alto.
- Il livello consigliato garantisce un equilibrio ottimale tra efficienza e protezione ed è adatto nella maggior parte dei casi.
- Se si lavora in un ambiente protetto, ad esempio in una rete aziendale con una gestione della protezione centralizzata, o con applicazioni dall'alto consumo di risorse, si consiglia di selezionare il livello di protezione basso.

Prima di abilitarlo, è consigliabile eseguire la scansione completa del computer con un livello di protezione alto.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare manualmente le impostazioni di Anti-Virus File. Di conseguenza, il nome del livello di protezione cambierà in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

► Per modificare il livello di protezione selezionato del componente Anti-Virus File, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Selezionare il livello di protezione desiderato nella finestra visualizzata.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Come risultato della scansione, Anti-Virus File assegna uno degli stati seguenti agli oggetti rilevati:

- stato programma dannoso (ad esempio *virus*, *Trojan*);

- *potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che l'applicazione ha rilevato nel file una sequenza di codice di un virus sconosciuto o un codice modificato di un virus conosciuto.

Se, durante la scansione anti-virus di un file, Kaspersky Anti-Virus individua oggetti infetti o potenzialmente infetti, le azioni successive eseguite da Anti-Virus File dipendono dallo stato degli oggetti e dall'azione selezionata.

Per impostazione predefinita, tutti i file infetti sono sottoposti a disinfezione e tutti quelli potenzialmente infetti vengono messi in quarantena.

Tutte le azioni possibili sono mostrate nella tabella seguente.

SE L'AZIONE SCELTA È	SE VIENE RILEVATO UN OGGETTO PERICOLOSO
☒ Disinfetta ☐ Elimina se la disinfezione non riesce	L'accesso all'oggetto è bloccato e viene eseguito un tentativo di disinfezione. Una copia dell'oggetto viene archiviata nel Backup. Se la disinfezione riesce, viene restituito all'utente per l'uso normale. Se non è possibile disinfettare l'oggetto, viene messo in quarantena. Le informazioni rilevanti vengono registrate nel rapporto. In un secondo momento sarà possibile provare a disinfettare l'oggetto.
☒ Disinfetta ☒ Elimina se la disinfezione non riesce	L'accesso all'oggetto è bloccato e viene eseguito un tentativo di disinfezione. Una copia dell'oggetto viene archiviata nel Backup. Se la disinfezione riesce, viene restituito all'utente per l'uso normale. Se la disinfezione non riesce, l'oggetto viene eliminato.
☐ Disinfetta ☒ Elimina	Anti-Virus File blocca l'accesso all'oggetto e lo elimina.
☒ Blocca utente infetto per ... ore.	Blocca la connessione al server dell'utente corrente se vengono eseguiti tentativi di copiare un oggetto infetto o potenzialmente infetto. Questa azione può essere inoltre applicata alle azioni correlate all'elaborazione del file (disinfezione o eliminazione). Si noti che se l'utente esce da una sessione e accede nuovamente al sistema, Kaspersky Anti-Virus la considererà una connessione diversa e rimuoverà il blocco.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup e la archivia nel Backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se a un oggetto è assegnato lo stato di *potenzialmente infetto* tale oggetto viene messo in quarantena senza tentare la disinfezione.

➡ Per modificare l'azione da eseguire sugli oggetti rilevati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della sezione **Azione** selezionare l'azione necessaria.

CREAZIONE DI UN AMBITO DI PROTEZIONE

che definisce, oltre alla posizione degli oggetti da esaminare, anche il tipo di file da esaminare. Per impostazione predefinita, Kaspersky Anti-Virus esegue solo la scansione dei aperti file potenzialmente infettabili in qualsiasi disco rigido, unità di rete o unità rimovibile.

È possibile espandere o restringere l'ambito di protezione aggiungendo / rimuovendo gli oggetti da esaminare oppure modificando i tipi di file da esaminare. Ad esempio, si desidera eseguire solo la scansione dei file .exe contenuti nelle unità di rete. È necessario agire con cautela per far sì che il computer non venga esposto alla minaccia di infezioni causate dalla limitazione dell'ambito di protezione.

Quando si selezionano i tipi di file, si tenga presente quanto segue:

- Esistono diversi formati di file con un livello di rischio discretamente basso di contenere codice dannoso che potrebbe essere attivato in seguito (ad esempio i file .txt). Altri formati, al contrario, contengono o possono contenere codice eseguibile, ad esempio i formati .exe, .dll, .doc. e il rischio di attivazione di codice dannoso al loro interno è estremamente alto.
- È importante ricordare che un utente malintenzionato può inviare un virus al computer in un file con estensione *txt* che in realtà è un file eseguibile rinominato come *txt*. Selezionando l'opzione **Scansione file per estensione**, tale file viene escluso dalla scansione. Selezionando l'impostazione **Scansione file per formato**, Anti-Virus File analizza l'intestazione del file indipendentemente dall'estensione, rileva se si tratta di un file .exe, quindi esegue la scansione anti-virus.

Quando si specificano i tipi di file da esaminare, vengono definiti il formato e le dimensioni dei file e le unità su cui verrà eseguita la scansione anti-virus per l'apertura, l'esecuzione o il salvataggio di tali file.

Per facilitare la configurazione, tutti i file vengono suddivisi in due gruppi: *semplici* e *composti*. I file semplici non contengono oggetti (ad esempio i file .txt). I file composti possono contenere diversi oggetti, ciascuno dei quali, a sua volta, può presentare diversi livelli nidificati. Tali oggetti possono essere archivi, file contenenti macro, fogli di calcolo, e-mail con allegati e così via.

È opportuno ricordare che Anti-Virus File eseguirà solo la scansione dei file inclusi nell'ambito di protezione creato. I file che non sono inclusi risulteranno disponibili all'uso senza scansione. Ciò aumenta il rischio di infezione del computer.

➡ Per modificare l'elenco di scansione degli oggetti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Generale**, nella sezione **Ambito della protezione**, premere il pulsante **Aggiungi**.
4. Nella finestra **Selezionare oggetto da analizzare**, selezionare un oggetto, quindi premere il pulsante **Aggiungi**. Premere il pulsante **OK** dopo aver aggiunto tutti gli oggetti necessari.
5. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

➡ Per modificare il tipo di oggetto esaminato:

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
3. Nella finestra visualizzata, selezionare le impostazioni necessarie all'interno della scheda **Generale**, nella sezione **Tipi di file**.

UTILIZZO DELL'ANALISI EURISTICA

Gli oggetti vengono esaminati utilizzando database che contengono le descrizioni di tutti i malware noti e i metodi di disinfezione corrispondenti. Kaspersky Anti-Virus confronta ogni oggetto esaminato con le voci del database per determinare se si tratta di un oggetto dannoso e, in tal caso, identifica la classe di malware cui appartiene. Questo approccio è noto come *analisi della firma* e viene sempre utilizzato per impostazione predefinita.

Ogni giorno vengono creati nuovi oggetti dannosi. Non tutti sono descritti nei database e possono quindi essere rilevati solo attraverso l'analisi euristica. Questo metodo presuppone l'analisi delle azioni eseguite da un oggetto all'interno del sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima ancora che queste vengano studiate dagli analisti anti-virus.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni. Questo livello definisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e il tempo richiesto per la scansione. Maggiore è il livello di dettaglio, più risorse saranno necessarie e maggiore sarà la durata della scansione.

► *Per utilizzare l'analisi euristica e impostare il livello di dettaglio delle scansioni:*

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Metodi di scansione**, selezionare la casella ☒ **Analisi euristica** e impostare il livello di dettaglio della scansione.

OTTIMIZZAZIONE DELLA SCANSIONE

Per ridurre la durata delle scansioni e per aumentare la velocità di Kaspersky Anti-Virus, è possibile scegliere di sottoporre a scansione solo i file nuovi e i file modificati dopo l'ultima analisi. Questa modalità si estende ai file semplici e a quelli composti.

► *Per sottoporre a scansione solo i file nuovi e quelli modificati dall'ultima scansione:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Prestazioni** selezionare la casella ☒ **Esamina solo file nuovi e modificati**.

SCANSIONE DEI FILE COMPOSITI

Un metodo comune di nascondere i virus è quello di incorporarli nei file composti, come gli archivi, i database e così via. Per rilevare i virus nascosti in questa maniera, il file composto deve essere decompresso e ciò può diminuire in maniera significativa la velocità della scansione.

I pacchetti di installazione e i file contenenti oggetti OLE vengono eseguiti all'apertura, risultando quindi più pericolosi degli archivi. Per proteggere il computer contro l'esecuzione di codice dannoso e, allo stesso tempo, aumentare la velocità di scansione, è necessario disabilitare le scansioni degli archivi e abilitare le scansioni per questo tipo di file.

Se un file contenente un oggetto OLE è un archivio, verrà sottoposto a scansione durante la decompressione. È possibile abilitare la scansione di archivi per analizzare file contenenti oggetti OLE incorporati prima della loro decompressione. Tuttavia, questa operazione comporterà una significativa diminuzione della velocità di scansione.

Per impostazione predefinita, Kaspersky Anti-Virus esamina esclusivamente gli oggetti OLE incorporati.

► *Per modificare l'elenco dei file composti esaminati:*

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.

3. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Scansione di file composti**, selezionare le caselle dei tipi di file composti da esaminare.

SCANSIONE DI FILE COMPOSTI DI GRANDI DIMENSIONI

Durante la scansione di file composti di grandi dimensioni, la decompressione preliminare può richiedere molto tempo. È possibile ridurre questo tempo solo se si esegue la scansione dei file in background. Se durante l'utilizzo di questi file è stato rilevato un oggetto dannoso, viene visualizzato un messaggio di notifica.

Per accedere più rapidamente ai file composti, disabilitare la decompressione dei file di dimensioni superiori a quelle specificate. Quando i file vengono estratti da un archivio, vengono sempre sottoposti a scansione.

➡ *Se si desidera abilitare la decompressione in background di file di grandi dimensioni, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Scansione di file composti**, premere il pulsante **Avanzate**.
4. Nella finestra **File composti**, selezionare la casella ☒ **Estrai i file composti in background**, quindi specificare il valore minimo delle dimensioni del file nel campo sottostante.

➡ *Se non si desidera abilitare la decompressione in background di file di grandi dimensioni, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Scansione di file composti**, premere il pulsante **Avanzate**.
4. Nella finestra **File composti**, selezionare la casella ☒ **Non decomprimere file composti di grandi dimensioni**, quindi specificare il valore massimo delle dimensioni del file nel campo sottostante.

MODIFICA DELLA MODALITÀ DI SCANSIONE

Per modalità di scansione si intende la condizione che attiva il funzionamento del componente Anti-Virus File. Per impostazione predefinita, l'applicazione utilizza la modalità Smart che determina se l'oggetto debba essere esaminato sulla base delle azioni eseguite su di esso. Ad esempio, quando si lavora con un documento Microsoft Office, il file viene sottoposto a scansione quando viene aperto per la prima e chiuso per l'ultima volta. Le operazioni intermedie che lo sovrascrivono non determinano la scansione del file.

La modalità di scansione degli oggetti può essere modificata. La selezione della modalità dipende dai file con i quali si lavora più spesso.

➡ *Per modificare la modalità di scansione degli oggetti:*

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.

3. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Modalità di scansione**, selezionare la modalità desiderata.

TECNOLOGIA DI SCANSIONE

È inoltre possibile specificare le tecnologie che verranno utilizzate dal componente Anti-Virus File:

- **Tecnologia iChecker.** Questa tecnologia è in grado di aumentare 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 dei database del programma, la data dell'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

Ad esempio, si dispone di un file archivio analizzato dall'applicazione che gli ha assegnato lo stato di *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata mediante aggiunta di un nuovo oggetto, oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

La tecnologia iChecker presenta alcuni limiti: non funziona con file di grandi dimensioni e si applica solo agli oggetti con una struttura riconosciuta dall'applicazione (ad esempio, .exe, .dll, .lnk, .tff, .inf, .sys, .com, .chm, .zip, .rar).

- **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 associata a un percorso di file specifico nel file system e può essere applicata solo a oggetti in NTFS.

➡ *Per cambiare tecnologia di scansione degli oggetti:*

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Tecnologie di scansione**, selezionare il valore necessario.

SOSPENSIONE DEL COMPONENTE: CREAZIONE DI UNA PIANIFICAZIONE

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File, consentendo un accesso più rapido agli oggetti. Per ridurre il carico e garantire un accesso rapido agli oggetti, è possibile impostare una pianificazione per la disabilitazione del componente.

➡ *Per configurare una pianificazione per sospendere l'attività del componente:*

1. Aprire la finestra dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Sospendi attività**, selezionare la casella ☒ **Programmata**, quindi premere il pulsante **Pianifica**.
4. Nella finestra **Sospendi attività**, specificare l'ora (nel formato 24 ore OO:MM) in cui la protezione verrà sospesa (nei campi **Sospendi l'attività alle** e **Riprendi l'attività alle**).

SOSPENSIONE DEL COMPONENTE: CREAZIONE DI UN ELENCO DI APPLICAZIONI

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File, consentendo un accesso più rapido agli oggetti. Per diminuire il carico e garantire un rapido accesso agli oggetti, è possibile configurare le impostazioni per la disabilitazione del componente quando si utilizzano determinate applicazioni.

La configurazione della disabilitazione del componente Anti-Virus File in caso di conflitti con determinate applicazioni rappresenta una misura drastica. In caso di conflitti con il funzionamento del componente, contattare il servizio di assistenza tecnica di Kaspersky Lab (<http://support.kaspersky.com>). Gli specialisti dell'Assistenza tecnica sono in grado di aiutare l'utente a risolvere i problemi di funzionamento di Kaspersky Anti-Virus in contemporanea con il software presente nel computer.

➡ Per configurare la sospensione del componente mentre sono in uso le applicazioni specificate, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Personalizza**.
3. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Sospendi attività**, selezionare la casella ☒ **All'avvio dell'applicazione**, quindi premere il pulsante **Seleziona**.
4. Nella finestra **Applicazioni**, creare un elenco di applicazioni la cui esecuzione metterà in sospensione il componente.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE PREDEFINITE

Quando si configura Anti-Virus File, è sempre possibile ripristinarne le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

Se, durante la configurazione delle impostazioni di Anti-Virus File, è stato modificato l'elenco di oggetti inclusi nell'area protetta, verrà chiesto se si desidera salvare tale elenco per un utilizzo successivo nel caso di ripristino delle impostazioni iniziali.

➡ Per ripristinare le impostazioni di protezione predefinite e salvare l'elenco modificato degli oggetti inclusi nell'area protetta, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione e fare clic sul pulsante **Impostazioni** nella parte superiore della finestra.
2. Nella finestra visualizzata, selezionare il componente **Anti-Virus File**, quindi premere il pulsante **Livello predefinito**.
3. Nella finestra **Ripristino delle impostazioni** visualizzata, selezionare la casella ☒ **Ambito di protezione**.

STATISTICHE DI ANTI-VIRUS FILE

Tutte le operazioni eseguite da Anti-Virus File vengono registrate in un rapporto speciale. Per visualizzare le informazioni sul funzionamento del componente, fare clic sul collegamento **Statistiche**. Verrà visualizzato un rapporto dettagliato sul funzionamento del componente, raggruppato in schede:

- Tutti gli oggetti pericolosi rilevati durante il processo di protezione del file system sono riportati in un elenco contenuto nella scheda *Rilevati*. In tale elenco sono riportati il percorso completo di ciascun oggetto e lo stato assegnatogli da Anti-Virus File: se viene individuato il programma dannoso che ha infettato l'oggetto, a quest'ultimo verrà assegnato lo stato appropriato. Nel caso di virus, Trojan e così via, se non è possibile stabilire esattamente il tipo di effetto dannoso, all'oggetto viene assegnato lo stato di *sospetto*. Accanto allo stato viene visualizzata anche l'azione applicata all'oggetto (rilevato, non trovato, disinfettato).

Per non visualizzare nella scheda le informazioni sugli oggetti disinfettati, deselezionare la casella ☒ **Mostra oggetti disinfettati**.

- L'elenco completo degli eventi verificatisi durante l'uso di Anti-Virus File è riportato nella scheda *Eventi*. Gli eventi possono essere dei seguenti tipi:
 - *Informativo* (ad esempio oggetti non elaborati, ignorati in base al tipo).
 - *Avviso* (ad esempio se viene rilevato un virus).
 - *Commento* (ad esempio se un archivio è protetto da password).

Solitamente, i messaggi informativi sono esclusivamente di riferimento e non rivestono particolare interesse. È possibile disabilitare la visualizzazione dei messaggi informativi. Per effettuare questa operazione, deselezionare la casella ☒ **Mostra tutti gli eventi**.

- Le *statistiche* di scansione vengono visualizzate nella scheda relativa. In questa scheda sarà riportato il numero totale di oggetti analizzati, quindi, suddivisi in colonne, verranno visualizzati: il numero di archivi presenti sul numero totale di oggetti analizzati, il numero di oggetti pericolosi, il numero di oggetti disinfettati, il numero di oggetti in quarantena e così via.
- Le impostazioni attive in Anti-Virus File vengono visualizzate nella scheda *Impostazioni*. Utilizzare il collegamento **Modifica impostazioni** per configurare rapidamente il componente.
- La scheda *Utenti bloccati* contiene un elenco di utenti i cui computer sono stati bloccati nel tentativo di copiare nel server file infetti o potenzialmente infetti.

TRATTAMENTO POSTICIPATO DEGLI OGGETTI

In Kaspersky Anti-Virus for Windows Servers, viene bloccato l'accesso ai file infetti se questi ultimi sono in corso di disinfezione e eliminazione, nel caso in cui tali operazioni non riuscissero.

Per ripristinare l'accesso agli oggetti bloccati, è necessario prima effettuare un tentativo di disinfezione. Se un oggetto viene disinfettato con successo, verrà ripristinato per l'uso regolare. Se non è possibile disinfettare l'oggetto, viene offerta la possibilità di *eliminarlo o ignorarlo*. In quest'ultimo caso, verrà ripristinato l'accesso al file. Tuttavia, ciò aumenta in maniera significativa il rischio di infezione del server. Si consiglia vivamente di non ignorare gli oggetti dannosi.

➡ Per accedere agli oggetti bloccati al fine di disinfettarli, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Rilevati**.
2. Nella finestra visualizzata, all'interno della scheda **Minacce attive**, selezionare gli oggetti necessari, quindi fare clic sul collegamento **Isola tutto**.

VEDERE ANCHE

Modifica delle azioni da eseguire sugli oggetti rilevati[40](#)

SCANSIONE ANTI-VIRUS SERVER

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 è in grado di eseguire la scansione anti-virus di elementi separati (file, cartelle, dischi, supporti rimovibili) oppure dell'intero computer. La scansione anti-virus esclude la possibilità di diffusione di codice dannoso non rilevato da Anti-Virus File per un motivo qualsiasi.

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 è dotato delle seguenti funzioni di scansione anti-virus:

Scansione

Esame degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.

Scansione Completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete.

Scansione Rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo.

Per impostazione predefinita, le seguenti attività vengono eseguite con le impostazioni consigliate. È possibile modificare tali impostazioni e pianificare l'esecuzione delle attività.

Inoltre, è possibile eseguire la scansione anti-virus di qualsiasi oggetto senza creare un'attività di scansione speciale. È possibile selezionare un oggetto da esaminare mediante l'interfaccia di Kaspersky Anti-Virus o gli strumenti standard di Microsoft Windows Server (ad esempio **Esplora risorse**, **Desktop** ecc.). Posizionare il cursore sul nome dell'oggetto desiderato, cliccare con il pulsante destro del mouse per aprire il menu di scelta rapida di Microsoft Windows e scegliere l'opzione **Scansione Anti-Virus**.



Fig. 7. Menu di scelta rapida di Microsoft Windows

In seguito a una scansione, inoltre, è possibile visualizzarne il rapporto, che contiene informazioni complete sugli eventi verificatisi durante l'esecuzione delle attività.

► Per modificare le impostazioni delle attività di scansione anti-virus, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.

3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, apportare le modifiche necessarie alle impostazioni dell'attività selezionata.

➡ *Per passare al rapporto della scansione anti-virus, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Cliccare sul bottone **Rapporto**.

IN QUESTA SEZIONE

Avvio della scansione anti-virus	50
Creazione di un elenco di oggetti da esaminare.....	51
Modifica del livello di protezione	52
Modifica delle azioni da eseguire sugli oggetti rilevati	53
Modifica del tipo di oggetti da esaminare	54
Ottimizzazione della scansione	54
Scansione dei file composti	55
Modifica del metodo di scansione	55
Tecnologia di scansione	56
Prestazioni del computer durante l'esecuzione delle attività.....	57
Sospensione dell'attività: creazione di una pianificazione	57
Sospensione del componente: creazione di un elenco di applicazioni	58
Modalità di esecuzione: specifica di un account.....	58
Modalità di esecuzione: creazione di una pianificazione	58
Funzioni dell'avvio pianificato delle attività	59
Statistiche della scansione anti-virus.....	59
Assegnazione delle impostazioni di scansione comuni per tutte le attività	60
Ripristino delle impostazioni di scansione predefinite	60

AVVIO DELLA SCANSIONE ANTI-VIRUS

È possibile avviare un'attività di scansione anti-virus con una delle due modalità seguenti:

- dal menu di scelta rapida di Kaspersky Anti-Virus;
- dalla finestra principale di Kaspersky Anti-Virus.

Le informazioni sull'esecuzione dell'attività verranno visualizzate nella finestra principale di Kaspersky Anti-Virus.

È inoltre possibile selezionare l'oggetto da esaminare utilizzando gli strumenti standard del sistema operativo Microsoft Windows, ad esempio dalla finestra di **Esplora risorse**, dal **Desktop** e così via.



Fig. 8. Menu di scelta rapida di Microsoft Windows

➤ Per avviare un'attività di scansione anti-virus dal menu di scelta rapida, eseguire le seguenti operazioni:

1. Cliccare con il pulsante destro del mouse sull'icona nell'area di notifica della barra delle applicazioni.
2. Selezionare la voce **Scansione** dal menu a discesa. Nella finestra principale dell'applicazione visualizzata, selezionare l'attività **Scansione (Scansione completa, Scansione rapida)** necessaria. Se necessario, configurare l'attività selezionata e cliccare sul pulsante **Avvia scansione**.
3. In alternativa, è possibile selezionare la voce **Scansione completa** dal menu di scelta rapida. Verrà avviata una scansione completa del computer. L'avanzamento dell'attività verrà visualizzato nella finestra principale di Kaspersky Anti-Virus.

➤ Per avviare l'attività di scansione anti-virus dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Premere il pulsante **Avvia scansione** per la sezione selezionata. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale dell'applicazione.

➤ Per avviare una scansione anti-virus di un oggetto selezionato dal menu di scelta rapida di Windows:

1. Cliccare con il pulsante destro del mouse sul nome dell'oggetto selezionato.
2. Selezionare la voce **Scansione Anti-Virus** nel menu di scelta rapida visualizzato. L'avanzamento e i risultati dell'esecuzione dell'attività verranno visualizzati nella finestra delle statistiche.

CREAZIONE DI UN ELENCO DI OGGETTI DA ESAMINARE

Ogni scansione anti-virus comprende il relativo elenco predefinito di oggetti. Per visualizzare un elenco di oggetti, selezionare il nome dell'attività (ad esempio **Scansione completa**) nella sezione **Scansione** della finestra principale dell'applicazione. L'elenco di oggetti verrà visualizzato nella parte destra della finestra.

Gli elenchi degli oggetti da esaminare sono già generati per le attività predefinite create durante l'installazione dell'applicazione.

Per agevolare l'utente, è possibile aggiungere categorie all'ambito della scansione, ad esempio caselle di posta, RAM, oggetti di avvio, backup del sistema operativo e file della cartella Quarantena di Kaspersky Anti-Virus.

Inoltre, quando si aggiunge una cartella che contiene oggetti incorporati nell'ambito della scansione, è possibile modificare la ricorsività. A tale scopo, selezionare l'oggetto desiderato dall'elenco di oggetti da esaminare, aprire il menu di scelta rapida e utilizzare l'opzione **Includi sottocartelle**.

► Per creare un elenco di oggetti da esaminare, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Fare clic sul collegamento **Aggiungi** per la sezione selezionata.
4. Nella finestra **Selezionare oggetto da analizzare** visualizzata, selezionare un oggetto e cliccare sul bottone **Aggiungi**. Premere il pulsante **OK** dopo aver aggiunto tutti gli oggetti necessari. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella. Per rimuovere un oggetto dall'elenco, selezionarlo e cliccare sul collegamento **Elimina**.

MODIFICA DEL LIVELLO DI PROTEZIONE

Il livello di protezione è una raccolta preimpostata delle impostazioni della scansione. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. La decisione sul livello da selezionare si basa sulle preferenze personali:

- Se si sospetta che la possibilità che il computer venga infettato sia alta, selezionare un livello di protezione alto.
- Si tratta del livello più appropriato nella maggior parte dei casi e in genere consigliato dagli specialisti Kaspersky Lab.
- Se si utilizzano applicazioni che richiedono quantità notevoli di risorse RAM, selezionare il livello di protezione basso in quanto in questa modalità l'applicazione impiega una quantità inferiore di risorse di sistema.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile configurare la scansione manualmente. Di conseguenza, il nome del livello di protezione cambierà in **Personalizzato**. Per ripristinare le impostazioni predefinite di scansione, selezionare uno dei livelli di protezione preimpostati. Per impostazione predefinita, il livello di scansione impostato è **Consigliato**.

► Per modificare il livello di protezione definito, eseguire le operazioni seguenti:

1. Aprire.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, regolare il dispositivo di scorrimento sulla scala. La regolazione del livello di protezione consente di definire la velocità di scansione e il numero totale di file esaminato: minore è il numero di file sottoposti a scansione anti-virus, maggiore sarà la velocità di scansione. È inoltre possibile cliccare sul bottone **Personalizza** e modificare le impostazioni nella finestra visualizzata secondo necessità. Il livello di protezione verrà modificato in **Personalizzato**.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Se in seguito a una scansione anti-virus viene rilevato un oggetto infetto o sospetto, l'elaborazione successiva dell'applicazione varia in base allo stato dell'oggetto e all'azione selezionata.

In base ai risultati della scansione, è possibile che a un oggetto venga assegnato uno dei seguenti stati:

- stato programma dannoso (ad esempio *virus*, *Trojan*);
- *potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Il dubbio sorge quando l'applicazione rileva nel file una sequenza di codice di un virus sconosciuto o il codice modificato di un virus conosciuto.

Per impostazione predefinita, tutti i file infetti sono sottoposti a disinfezione e tutti quelli potenzialmente infetti vengono messi in quarantena.

SE L'AZIONE SCELTA È	SE VIENE RILEVATO UN OGGETTO PERICOLOSO O POTENZIALMENTE INFETTO
☒ Richiedi intervento utente al termine della scansione	L'applicazione rimanda l'elaborazione degli oggetti fino al termine della scansione. Al termine della scansione, all'utente verrà richiesto di eseguire alcune azioni per ciascun file.
☒ Richiedi intervento utente durante la scansione	Anti-Virus File mostra un messaggio di avviso contenente informazioni su quale programma dannoso abbia infettato o possa infettare il file e offre una serie di possibili azioni.
☒ Non richiedere intervento utente	L'applicazione crea un rapporto con le informazioni relative agli oggetti rilevati senza elaborarli o segnalarli all'utente. Questa modalità dell'applicazione non è consigliata, in quanto lascia gli oggetti infetti o potenzialmente infetti nel computer, rendendo pressoché inevitabile la diffusione dell'infezione.
☒ Non richiedere intervento utente ☒ Disinfetta	L'applicazione crea un rapporto con le informazioni relative agli oggetti rilevati senza elaborarli o segnalarli all'utente. Questa modalità dell'applicazione non è consigliata, in quanto lascia gli oggetti infetti o potenzialmente infetti nel computer, rendendo pressoché inevitabile la diffusione dell'infezione.
☒ Non richiedere intervento utente ☒ Disinfetta ☒ Elimina se la disinfezione non riesce	L'applicazione tenta di disinfettare l'oggetto senza richiedere una conferma dall'utente. Se la disinfezione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene salvata nel Backup.
☒ Non richiedere intervento utente ☐ Disinfetta ☒ Elimina	L'applicazione elimina automaticamente l'oggetto.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup e la archivia nel Backup per consentirne il ripristino o la disinfezione in un secondo momento.

Se a un oggetto è assegnato lo stato di *potenzialmente infetto* tale oggetto viene messo in quarantena senza tentare la disinfezione.

➡ Per modificare l'azione da eseguire sugli oggetti rilevati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.

4. Nella sezione **Azione**, immettere le modifiche desiderate nella finestra visualizzata.

MODIFICA DEL TIPO DI OGGETTI DA ESAMINARE

Quando si specificano i tipi di oggetti da esaminare, vengono definiti il formato e le dimensioni dei file su cui verrà eseguita l'attività di scansione anti-virus selezionata.

Quando si selezionano i tipi di file, si tenga presente quanto segue:

- Alcuni formati di file (ad esempio `.txt`) presentano un rischio alquanto basso di contenere codice dannoso attivabile. Altri formati, al contrario, contengono o possono contenere codice eseguibile (`exe`, `dll`, `doc`). Il rischio di penetrazione ed attivazione di codice nocivo in tali file è piuttosto alto.
- È importante ricordare che un utente malintenzionato può inviare un virus al computer in un file con estensione `txt` che in realtà è un file eseguibile rinominato come `txt`. Selezionando l'opzione  **Scansione file per estensione**, tale file viene ignorato dalla scansione. Se è stata selezionata l'opzione  **Scansione file per formato**, indipendentemente dall'estensione, la protezione del file analizza l'intestazione del file e può determinare se si tratta di un file `.exe`. Tale file sarà sottoposto ad una scansione anti-virus approfondita.

➡ Per modificare il tipo di oggetto esaminato:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Ambito**, sezione **Tipi di file**, selezionare le impostazioni necessarie.

OTTIMIZZAZIONE DELLA SCANSIONE

È possibile ridurre il tempo di scansione e velocizzare Kaspersky Anti-Virus. Per ottenere questo risultato, è necessario eseguire la scansione solo dei file nuovi e dei file stati modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che composti.

Inoltre, è possibile imporre una limitazione alla lunghezza di scansione. Una volta trascorso l'intervallo di tempo specificato, la scansione del file viene interrotta. È inoltre possibile limitare la dimensione del file da esaminare. Il file verrà ignorato in caso di dimensione superiore al valore impostato.

➡ Per esaminare soltanto i file nuovi e modificati, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Ambito**, nella sezione **Ottimizzazione della scansione**, selezionare la casella ☒ **Esamina solo file nuovi e modificati**.

➡ Per imporre una restrizione temporale alla durata della scansione:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Ambito**, nella sezione **Ottimizzazione della scansione**, selezionare la casella ☒ **Esamina solo file nuovi e modificati** e specificare la durata della scansione nel campo corrispondente.

➡ *Per limitare la dimensione del file da esaminare, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, scheda **Ambito**, cliccare sul bottone **Avanzate**.
6. Nella finestra **File compositi** visualizzata, ☒ selezionare la casella **Non decomprimere i file compositi di grandi dimensioni** e specificare la dimensione di file nel campo adiacente.

SCANSIONE DEI FILE COMPOSITI

Un metodo comune per nascondere i virus consiste nell'incorporarli in file compositi: archivi, database e così via. Per rilevare i virus nascosti in questo modo, è necessario decomprimere un file composito e questa operazione può ridurre significativamente la velocità di scansione.

Per ogni tipo di file composito, è possibile scegliere di analizzare tutti i file oppure solo quelli nuovi. Per farlo, utilizzare il collegamento accanto al nome dell'oggetto. Il relativo valore verrà modificato quando si clicca con il bottone sinistro del mouse su di esso. Se si seleziona la modalità di scansione dei soli file nuovi e modificati, non sarà possibile selezionare il tipo di file compositi da sottoporre a scansione.

➡ *Per modificare l'elenco dei file compositi esaminati:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Ambito**, sezione **Scansione dei file compositi**, selezionare il tipo di file compositi richiesto da esaminare.

MODIFICA DEL METODO DI SCANSIONE

È possibile utilizzare l'*analisi euristica* come metodo di scansione, che analizza le azioni eseguite da un oggetto sul sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto.

È inoltre possibile impostare il livello di dettaglio per l'analisi euristica spostando il cursore in una delle seguenti posizioni: **Superficiale**, **Medio** o **Approfondito**.

Oltre a questo metodo, è possibile utilizzare la scansione Rootkit. Il *rootkit* è una serie di strumenti in grado di nascondere applicazioni dannose nel sistema operativo. Queste utilità vengono inserite nel sistema, nascondendo la loro presenza e quella dei processi, delle cartelle e delle chiavi di registro di altri programmi dannosi installati con il rootkit. Se la scansione è abilitata, è possibile specificare il livello di dettaglio (analisi avanzata) per rilevare i rootkit, che esegue una scansione accurata di tali programmi attraverso l'analisi di un gran numero di oggetti di vario tipo.

➡ *Per specificare il metodo di scansione da utilizzare:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Metodi di scansione**, selezionare le tecnologie di scansione desiderate.

TECNOLOGIA DI SCANSIONE

È inoltre possibile specificare la tecnologia da utilizzare durante la scansione:

- **Tecnologia iChecker.** Questa tecnologia è in grado di aumentare 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 del database del programma, la data dell'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

Ad esempio, si dispone di un file di archivio esaminato da Kaspersky Anti-Virus a cui è stato assegnato lo stato *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata mediante aggiunta di un nuovo oggetto, oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

iChecker presenta tuttavia delle limitazioni: non risulta efficace con file di grandi dimensioni e si applica solo ad oggetti con una struttura riconoscibile dall'applicazione, ad esempio file di tipo exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar.

- **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 associata a un percorso di file specifico nel file system e può essere applicata solo ad oggetti in NTFS.

➡ *Per utilizzare la tecnologia di scansione degli oggetti, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Tecnologie di scansione**, abilitare la tecnologia desiderata.

PRESTAZIONI DEL COMPUTER DURANTE L'ESECUZIONE DELLE ATTIVITÀ

È possibile posticipare le attività di scansione anti-virus per limitare il carico sulla CPU (Central Processing Unit) e sui sottosistemi di archiviazione su disco.

L'esecuzione di attività di scansione aumenta il carico sulla CPU e sui sottosistemi del disco, con conseguente rallentamento dell'esecuzione delle altre applicazioni. In questi casi, per impostazione predefinita Kaspersky Anti-Virus sospende l'esecuzione delle attività anti-virus e libera le risorse di sistema per le applicazioni dell'utente.

Alcune applicazioni, tuttavia, verranno avviate immediatamente dopo il rilascio delle risorse della CPU e verranno eseguite in background. Per fare in modo che la scansione non dipenda dalle prestazioni di tali applicazioni, è consigliabile evitare di assegnare loro risorse del sistema.

Si noti che questa impostazione può essere configurata singolarmente per ciascuna attività di scansione anti-virus. In questo caso, la configurazione di un'attività specifica ha una priorità più alta.

➡ *Per posticipare l'esecuzione delle attività di scansione anti-virus quando rallentano altre applicazioni, eseguire le seguenti operazioni:*

1. Aprire nella finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Metodi di scansione**, selezionare la casella ☒ **Concedi risorse ad altre applicazioni**.

SOSPENSIONE DELL'ATTIVITÀ: CREAZIONE DI UNA PIANIFICAZIONE

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File. Per ridurre il carico e garantire un accesso rapido agli oggetti, è possibile impostare una pianificazione per la disabilitazione del componente.

➡ *Per configurare la pianificazione della sospensione dell'attività, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Selezionare la voce **Personalizza** dal menu a discesa.
5. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Sospendi attività**, selezionare la casella ☒ **Programmata**, quindi premere il pulsante **Pianifica**.
6. Nella finestra **Sospendi attività**, specificare l'ora (nel formato 24 ore OO:MM) in cui la protezione verrà sospesa (nei campi **Sospendi l'attività alle** e **Riprendi l'attività alle**).

SOSPENSIONE DEL COMPONENTE: CREAZIONE DI UN ELENCO DI APPLICAZIONI

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File. Per ridurre il carico e garantire un accesso rapido agli oggetti, è possibile impostare un elenco di applicazioni specifiche per la disabilitazione del componente.

► *Per configurare la sospensione del componente mentre sono in uso le applicazioni specificate, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Selezionare la voce **Personalizza** dal menu a discesa.
5. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Sospendi attività**, selezionare la casella ☒ **All'avvio dell'applicazione**, quindi premere il pulsante **Seleziona**.
6. Nella finestra **Applicazioni**, creare un elenco di applicazioni la cui esecuzione metterà in sospensione il componente.

MODALITÀ DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

È possibile specificare un account utilizzato dall'applicazione durante l'esecuzione di una scansione anti-virus.

► *Per avviare l'attività con i privilegi di un altro account utente:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Modalità esecuzione**, sezione **Utente**, selezionare la casella ☒ **Esegui l'attività come**. Specificare il nome utente e la password.

MODALITÀ DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

Tutte le attività di scansione anti-virus possono essere avviate manualmente o in base a una pianificazione.

L'impostazione di pianificazione predefinita per le attività create durante l'installazione del programma è disattivata. L'eccezione è l'attività di scansione rapida, che viene avviata a ogni avvio del computer.

Quando si crea una pianificazione all'avvio delle attività, è necessario impostare l'intervallo delle scansioni.

Se per qualsiasi motivo non è possibile avviare l'attività, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che venga avviata automaticamente non appena possibile.

➤ *Per modificare una pianificazione per le attività di scansione:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, premere il bottone **Cambia** nella sezione **Modalità esecuzione**.
5. Apportare le modifiche necessarie nella finestra **Pianifica** visualizzata.

➤ *Per configurare l'avvio automatico delle attività ignorate:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, premere il bottone **Cambia** nella sezione **Modalità esecuzione**.
5. Nella finestra **Pianifica** visualizzata, sezione **Impostazioni di pianificazione**, selezionare la casella ☒ **Esegui attività se saltata**.

FUNZIONI DELL'AVVIO PIANIFICATO DELLE ATTIVITÀ

Tutte le attività di scansione anti-virus possono essere avviate manualmente o in base a una pianificazione.

Le attività pianificate includono funzionalità aggiuntive, ad esempio è possibile selezionare la casella *Sospendi la scansione pianificata se lo screensaver non è attivo o il computer non è bloccato*. Questa funzionalità consente di rimandare l'avvio dell'attività finché l'utente non avrà terminato di lavorare al computer. Pertanto, l'attività di scansione non richiederà l'utilizzo delle risorse del sistema durante le ore lavorative.

➤ *Per avviare le attività di scansione solo quando il computer non è più in uso, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione completa, Scansione rapida**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Modalità esecuzione**, selezionare la casella ☒ **Sospendi la scansione se lo screensaver non è attivo e il computer non è bloccato**.

STATISTICHE DELLA SCANSIONE ANTI-VIRUS

Le informazioni generali su ciascuna attività di scansione anti-virus sono disponibili nella finestra delle statistiche, in cui è possibile verificare la quantità di oggetti sottoposti a scansione nonché la quantità di oggetti pericolosi e sospetti soggetti a elaborazione. Questa finestra, inoltre, consente di trovare informazioni sull'ora di avvio e di completamento dell'ultima attività di scansione eseguita e sulla durata della scansione.

Le informazioni generali sui risultati della scansione vengono raggruppati nelle schede seguenti:

- Nella scheda *Rilevati* vengono elencati tutti gli oggetti pericolosi rilevati durante l'esecuzione di un'attività.
- Nella scheda *Eventi* vengono elencati tutti gli eventi verificatisi durante l'esecuzione di un'attività.
- Nella scheda *Statistiche* sono disponibili dati statistici sugli oggetti esaminati.

- Nella scheda *Impostazioni* sono disponibili le impostazioni, che determinano le modalità di esecuzione di un'attività.

Se durante la scansione si sono verificati errori, provare a eseguirla di nuovo. Se in seguito a questo tentativo viene restituito un errore, si consiglia di salvare il rapporto sui risultati dell'attività in un file mediante il pulsante **Salva con nome**. Quindi, contattare il Servizio di supporto tecnico e inviare il file di rapporto. Gli specialisti di Kaspersky Lab saranno in grado di offrire assistenza appropriata.

➡ *Per visualizzare le statistiche di un'attività di scansione anti-virus, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**, creare un'attività di scansione e avviarla. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale. Cliccare sul collegamento **Dettagli** per passare alla finestra delle statistiche.

ASSEGNAZIONE DELLE IMPOSTAZIONI DI SCANSIONE COMUNI PER TUTTE LE ATTIVITÀ

Ciascuna attività di scansione viene eseguita in base alle impostazioni a essa associate. Per impostazione predefinita, le attività create al momento dell'installazione dell'applicazione vengono eseguite con le impostazioni consigliate dagli esperti di Kaspersky Lab.

È possibile configurare impostazioni di scansione globali per tutte le attività. Verrà utilizzato un set di proprietà per eseguire la scansione anti-virus di un singolo oggetto come punto iniziale.

➡ *Per assegnare impostazioni di scansione globali a tutte le attività, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Nella parte destra della finestra visualizzata, sezione **Altre impostazioni attività**, cliccare sul pulsante **Applica**. Confermare le impostazioni globali selezionate nella finestra di dialogo a comparsa.

RIPRISTINO DELLE IMPOSTAZIONI DI SCANSIONE PREDEFINITE

Quando si modificano le impostazioni delle attività, è sempre possibile ripristinare quelle consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

➡ *Per ripristinare le impostazioni di scansione dei file predefinite, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, premere il pulsante **Livello predefinito** nella sezione **Livello di sicurezza**.

AGGIORNAMENTO DELL'APPLICAZIONE

L'aggiornamento continuo della protezione è un prerequisito di una protezione affidabile. Poiché ogni giorno nascono nuovi virus, Trojan e software dannosi, è importante aggiornare regolarmente l'applicazione per proteggere costantemente i dati personali.

Il componente di aggiornamento dell'applicazione esegue il download e l'installazione dei seguenti aggiornamenti sul server:

- **Database dell'applicazione**

La protezione delle informazioni viene garantita dai database dell'applicazione. Anti-Virus File li utilizza per la ricerca e la disinfezione di oggetti nocivi sul server. I database vengono aggiornati ogni ora con nuove voci relative alle nuove minacce. È pertanto consigliabile aggiornarli regolarmente.

- **Moduli dell'applicazione**

Oltre ai database dell'applicazione, è inoltre possibile aggiornare i moduli dell'applicazione. I pacchetti di aggiornamento risolvono le vulnerabilità dell'applicazione e aggiungono o migliorano le funzionalità esistenti.

I server di aggiornamento di Kaspersky Lab costituiscono l'origine principale degli aggiornamenti di Kaspersky Anti-Virus.

Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet. Per impostazione predefinita, le impostazioni di connessione a Internet vengono determinate automaticamente. Se le impostazioni del server proxy non vengono configurate automaticamente, è possibile configurare le impostazioni di connessione manualmente.

Durante un aggiornamento, i moduli e i database dell'applicazione nel computer vengono confrontati con quelli dell'origine degli aggiornamenti. Se il computer dispone dell'ultima versione dei database e dei moduli dell'applicazione, viene visualizzata una finestra di notifica che conferma che la protezione del computer è aggiornata. Se i database e i moduli sul computer e sul server di aggiornamento sono diversi, l'applicazione scarica solo la parte incrementale degli aggiornamenti. Il fatto che non vengano scaricati tutti i database e i moduli determina un aumento significativo della velocità di copia dei file e una riduzione del traffico Internet.

Prima di aggiornare i database, in Kaspersky Anti-Virus vengono create copie di backup di questi, affinché sia possibile riutilizzarli in futuro.

Potrebbe essere necessario utilizzare l'opzione di rollback se, ad esempio, i database vengono danneggiati durante il processo di aggiornamento. È possibile eseguire facilmente il rollback alla versione precedente e cercare di aggiornare nuovamente i database.

È possibile copiare gli aggiornamenti recuperati in un'origine locale durante l'aggiornamento dell'applicazione. Tale servizio consente di aggiornare i database e i moduli dell'applicazione sui computer in rete per non intasare il traffico Internet.

È inoltre possibile configurare l'avvio degli aggiornamenti automatici.

Nella sezione **Aggiornamento** viene visualizzato lo stato corrente dei database dell'applicazione.

È possibile visualizzare il rapporto di aggiornamento, che contiene informazioni complete sugli eventi verificatisi durante l'aggiornamento. Una panoramica sull'attività dei virus è disponibile nel sito Web www.kaspersky.com cliccando sul collegamento relativo all'**analisi dell'attività dei virus**.

► *Per modificare le impostazioni delle attività di aggiornamento, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.

3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, apportare le modifiche necessarie alle impostazioni dell'attività selezionata.

➡ *Per passare al rapporto degli aggiornamenti, eseguire le seguenti operazioni:*

1. Aprire la finestra principale.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Cliccare sul bottone **Rapporto**.

IN QUESTA SEZIONE

Avvio dell'aggiornamento	62
Rollback dell'ultimo aggiornamento	63
Origine degli aggiornamenti	63
Impostazioni internazionali	64
Utilizzo di un server proxy	64
Modalità di esecuzione: specifica di un account	65
Modalità di esecuzione: creazione di una pianificazione	65
Selezione degli oggetti da aggiornare	66
Modifica della modalità di esecuzione dell'attività di aggiornamento	66
Aggiornamento da una cartella locale	67
Statistiche di aggiornamento	68
Problemi possibili durante l'aggiornamento	68

AVVIO DELL'AGGIORNAMENTO

È possibile avviare l'aggiornamento dell'applicazione in qualsiasi momento. Gli aggiornamenti vengono scaricati dall'origine degli aggiornamenti selezionata.

È possibile aggiornare Kaspersky Anti-Virus utilizzando uno dei due metodi supportati:

- Dal menu di scelta rapida.
- Dalla finestra principale dell'applicazione.

Le informazioni sull'aggiornamento verranno visualizzate nella finestra principale dell'applicazione.

Si noti che gli aggiornamenti vengono distribuiti su un'origine locale durante il processo di aggiornamento, a condizione che tale servizio sia abilitato.

➡ *Per avviare l'aggiornamento di Kaspersky Anti-Virus dal menu di scelta rapida:*

1. Cliccare con il pulsante destro del mouse sull'icona nell'area di notifica della barra delle applicazioni.

2. Selezionare la voce **Aggiornamento** dal menu a discesa.

➡ *Per avviare l'aggiornamento di Kaspersky Anti-Virus dalla finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Premere il pulsante **Avvia aggiornamento**. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale dell'applicazione.

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

All'inizio del processo di aggiornamento, Kaspersky Anti-Virus crea una copia di backup dei moduli dell'applicazione e dei database correnti. In questo modo, se l'aggiornamento non riesce, il programma può continuare a funzionare utilizzando i database precedenti.

L'opzione di rollback è utile, ad esempio, se una parte dei database è stata danneggiata. I database locali possono essere danneggiati dall'utente o da un programma nocivo. Ciò è possibile solo se l'Auto-Difesa dell'applicazione è disabilitata. È possibile riportare i database allo stato precedente e ritentare l'aggiornamento in un secondo momento.

➡ *Per eseguire il rollback alla versione precedente del database:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Cliccare sul collegamento **Rollback ai database precedenti**.

ORIGINE DEGLI AGGIORNAMENTI

Per *origine degli aggiornamenti* si intende una risorsa contenente gli aggiornamenti per i database e i moduli di applicazione di Kaspersky Anti-Virus.

È possibile utilizzare le seguenti origini di aggiornamento:

- *Server di amministrazione* è un repository di aggiornamento centralizzato presente nel server di amministrazione di Kaspersky Administration Kit (per ulteriori informazioni consultare il Manuale dell'amministratore per Kaspersky Administration Kit).
- *I server degli aggiornamenti di Kaspersky Lab* sono siti Web speciali che contengono gli aggiornamenti disponibili per i database e i moduli dell'applicazione per tutti i prodotti Kaspersky Lab.
- *I server FTP o HTTP, le cartelle locali o di rete* sono server o cartelle locali che contengono gli aggiornamenti più recenti.

Se non è possibile accedere ai server degli aggiornamenti di Kaspersky Lab, ad esempio in assenza di una connessione a Internet, chiamare l'ufficio centrale di Kaspersky Lab al numero +7 (495) 797-87-00 o +7 (495) 645-79-39 per richiedere informazioni sui partner di Kaspersky Lab che possono fornire aggiornamenti in formato compresso su floppy o dischi ZIP.

È possibile copiare gli aggiornamenti da un disco rimovibile e caricarli su un sito FTP o HTTP oppure salvarli in una cartella locale o di rete.

Quando si richiedono aggiornamenti su supporti rimovibili, specificare se si desidera ricevere anche gli aggiornamenti per i moduli dell'applicazione.

Se si seleziona una risorsa esterna alla LAN come sorgente degli aggiornamenti, è necessario disporre di una connessione a Internet per poter eseguire l'aggiornamento.

Se sono state selezionate più risorse come origini dell'aggiornamento, l'applicazione cerca di connettersi a esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco e recupera gli aggiornamenti dalla prima disponibile.

➡ Per scegliere una sorgente degli aggiornamenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul bottone **Configura**.
5. Nella finestra visualizzata, sulla scheda **Origine aggiornamento**, cliccare sul bottone **Aggiungi**.
6. Selezionare un sito FTP o HTTP oppure immetterne l'indirizzo IP, il nome simbolico o l'URL nella finestra **Seleziona origine aggiornamento** visualizzata.

IMPOSTAZIONI INTERNAZIONALI

Se si utilizzano i server degli aggiornamenti di Kaspersky Lab come origine degli aggiornamenti, è possibile selezionare la posizione ottimale del server da cui scaricare i file. I server Kaspersky Lab sono dislocati in più paesi. La scelta del server più vicino consente di risparmiare tempo e accelerare il download degli aggiornamenti.

➡ Per scegliere il server più vicino:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul bottone **Configura**.
5. Nella finestra visualizzata, sulla scheda **Origine aggiornamento**, sezione **Impostazioni internazionali**, selezionare l'opzione  **Seleziona dall'elenco**, quindi scegliere il paese più vicino alla propria posizione geografica dall'elenco a discesa.

Se si seleziona la casella  **Autorileva**, le informazioni sulla posizione verranno copiate dal registro del sistema operativo durante l'esecuzione dell'aggiornamento.

UTILIZZO DI UN SERVER PROXY

Se si utilizza un server proxy per connettersi a Internet, è necessario configurarne le impostazioni.

➡ Per configurare il server proxy, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul bottone **Configura**.

5. Nella finestra visualizzata, modificare le impostazioni del server proxy sulla scheda **Impostazioni proxy**.

MODALITÀ DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

Kaspersky Anti-Virus è dotato di una funzione che consente di avviare gli aggiornamenti del programma da un altro profilo. Per impostazione predefinita, il servizio è disabilitato e le attività vengono avviate tramite l'account con il quale si è registrati nel sistema.

Poiché l'applicazione può essere aggiornata da un'origine a cui non è possibile accedere (ad esempio la directory degli aggiornamenti di rete) o di cui non si dispone delle autorizzazioni necessarie per accedere al server proxy, è possibile utilizzare tale funzione per eseguire gli aggiornamenti dell'applicazione mediante le credenziali di accesso di un utente che dispone di tali privilegi.

Si noti che se non si esegue l'attività con i privilegi, l'aggiornamento pianificato verrà eseguito con i privilegi dell'account utente corrente. Se al momento non sono registrati utenti sul computer, l'esecuzione degli aggiornamenti con un altro account utente non è stato configurato e gli aggiornamenti eseguiti automaticamente verranno eseguiti con i privilegi di SISTEMA.

➡ *Per avviare l'attività con i privilegi di un altro account utente:*

1. Aprire nella finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul bottone **Configura**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Modalità esecuzione**, selezionare la casella ☒ **Esegui attività come**. Inserire i dati di accesso del profilo con cui si desidera avviare l'attività, ovvero nome utente e password.

MODALITÀ DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

Tutte le attività di scansione anti-virus possono essere avviate manualmente o in base a una pianificazione.

Quando si crea una pianificazione relativa alle attività da avviare, è necessario impostare l'intervallo delle attività di aggiornamento.

Se per qualsiasi motivo non è possibile avviare l'attività, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che venga avviata automaticamente non appena possibile.

➡ *Per modificare una pianificazione per le attività di scansione:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, premere il bottone **Cambia** nella sezione **Modalità esecuzione**.
5. Apportare le modifiche necessarie nella finestra **Pianifica** visualizzata.

➤ *Per configurare l'avvio automatico delle attività ignorate:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, premere il bottone **Cambia** nella sezione **Modalità esecuzione**.
5. Nella finestra **Pianifica** visualizzata, sezione **Impostazioni di pianificazione**, selezionare la casella ☒ **Esegui attività se saltata**.

SELEZIONE DEGLI OGGETTI DA AGGIORNARE

Gli oggetti da aggiornare sono i componenti che verranno aggiornati:

- database dell'applicazione;
- moduli dell'applicazione.

I database dell'applicazione vengono sempre aggiornati mentre i moduli delle applicazioni vengono aggiornati solo se si seleziona una modalità appropriata.

Se è disponibile un set di moduli dell'applicazione nell'origine degli aggiornamenti durante l'aggiornamento, Kaspersky Anti-Virus li scaricherà e installerà al riavvio del computer. Gli aggiornamenti dei moduli scaricati non verranno installati fino al riavvio del computer.

Se il successivo aggiornamento dell'applicazione viene eseguito prima del riavvio del computer e, quindi, prima dell'installazione dei precedenti aggiornamenti per il modulo dell'applicazione, verranno aggiornate solo le firme delle minacce.

➤ *Per scaricare e installare gli aggiornamenti per i moduli dell'applicazione, eseguire le seguenti operazioni:*

1. Aprire l'area principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, selezionare la casella ☒ **Aggiorna moduli programma**.

MODIFICA DELLA MODALITÀ DI ESECUZIONE DELL'ATTIVITÀ DI AGGIORNAMENTO

È possibile selezionare la modalità di esecuzione dell'attività di aggiornamento di Kaspersky Anti-Virus mediante la configurazione guidata dell'applicazione (per ulteriori informazioni, consultare la sezione "Configurazione delle impostazioni di aggiornamento" a pagina [26](#)). È possibile modificare la modalità di esecuzione selezionata.

L'attività di aggiornamento può essere avviata tramite una delle seguenti modalità:

-  **Automaticamente**. Kaspersky Anti-Virus verifica a intervalli specificati la disponibilità di pacchetti di aggiornamento nell'origine degli aggiornamenti. Se vengono rilevati nuovi aggiornamenti, questi vengono scaricati e installati nel computer. Questa è la modalità predefinita.

Kaspersky Anti-Virus tenterà di eseguire gli aggiornamenti in base agli intervalli specificati nel pacchetto di aggiornamenti precedente. Tale opzione consente a Kaspersky Lab di regolare la frequenza degli

aggiornamenti in caso di attacchi da virus e altre situazioni potenzialmente pericolose. L'applicazione riceverà tempestivamente gli ultimi aggiornamenti per i database, gli attacchi di rete e i moduli software, escludendo la possibilità che il malware penetri nel computer.

-  **Programmata** (l'intervallo di tempo cambia in base alle impostazioni). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione.
-  **Manualmente**. Se si seleziona questa opzione, gli aggiornamenti verranno eseguiti manualmente. Kaspersky Anti-Virus informerà immediatamente l'utente in caso di aggiornamenti necessari.

➡ *Per configurare la pianificazione di avvio dell'attività di aggiornamento:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, selezionare la modalità di avvio dell'attività di aggiornamento nella sezione **Modalità esecuzione**. Se l'opzione relativa all'aggiornamento pianificato è selezionata, creare la pianificazione.

AGGIORNAMENTO DA UNA CARTELLA LOCALE

La procedura di recupero degli aggiornamenti da una cartella locale viene organizzata nel modo seguente:

1. Uno dei computer della rete recupera un pacchetto di aggiornamento di Kaspersky Anti-Virus da un server di Kaspersky Lab o da un server mirror che ospita un insieme corrente di aggiornamenti. Gli aggiornamenti recuperati vengono salvati in una cartella condivisa.
2. Gli altri computer della rete accedono alla cartella condivisa per recuperare gli aggiornamenti.

Kaspersky Anti-Virus 6.0 è in grado di recuperare esclusivamente i pacchetti di aggiornamento dai server di Kaspersky Lab. È consigliabile distribuire gli aggiornamenti per le altre applicazioni di Kaspersky Lab tramite il Kaspersky Administration Kit.

➡ *Per abilitare la modalità di aggiornamento, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Aggiorna distribuzione**, selezionare la casella ☒ **Copia aggiornamenti nella cartella** e nel campo sottostante specificare il percorso di una cartella condivisa in cui verranno copiati gli aggiornamenti scaricati. È inoltre possibile selezionare il percorso nella finestra visualizzata cliccando sul bottone **Sfoglia**.

➡ *Se si desidera che gli aggiornamenti dell'applicazione vengano eseguiti dalla cartella condivisa selezionata, eseguire le seguenti operazioni su tutti i computer della rete:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, sulla scheda **Origine aggiornamento**, cliccare sul bottone **Aggiungi**.
6. Nella finestra **Seleziona origine aggiornamento** visualizzata, selezionare la cartella oppure immettere il percorso completo della cartella nel campo **Origine**.
7. Deselezionare la casella ☒ **Server degli aggiornamenti Kaspersky Lab** nella scheda **Origine aggiornamento**.

STATISTICHE DI AGGIORNAMENTO

Nella finestra delle statistiche sono disponibili informazioni generali sulle attività di aggiornamento. In questa finestra, è inoltre possibile visualizzare gli eventi verificatisi durante l'esecuzione di un'attività (scheda *Eventi*) e visualizzare l'elenco di impostazioni che determinano l'esecuzione dell'attività (scheda *Impostazioni*).

Se durante la scansione si sono verificati errori, provare a eseguirla di nuovo. Se in seguito a questo tentativo viene restituito un errore, si consiglia di salvare il rapporto sui risultati dell'attività in un file mediante il bottone **Salva con nome**. Quindi, contattare il Servizio di supporto tecnico e inviare il file di rapporto. Gli specialisti di Kaspersky Lab saranno in grado di offrire assistenza appropriata.

Un breve riepilogo delle statistiche di aggiornamento è disponibile nella parte superiore della finestra delle statistiche. Include la dimensione degli aggiornamenti scaricati e installati, la velocità e la durata dell'aggiornamento, e ulteriori informazioni.

➡ *Per visualizzare le statistiche di un'attività di scansione anti-virus, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiorna**, creare un'attività di aggiornamento e avviarla. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale. Cliccare sul collegamento **Dettagli** per passare alla finestra delle statistiche.

PROBLEMI POSSIBILI DURANTE L'AGGIORNAMENTO

Quando si aggiornano i moduli dell'applicazione o le firme delle minacce di Kaspersky Anti-Virus, è possibile che si verifichino errori associati a configurazioni di aggiornamento non valide, problemi di connessione ecc. In questa sezione della Guida viene elencata la maggior parte degli errori e vengono indicate le possibili soluzioni per eliminarli. Se si riscontrano errori non descritti nella Guida o si desidera ricevere suggerimenti dettagliati per eliminarli, è possibile trovare ulteriori informazioni nella Knowledge Base disponibile nel portale Web di assistenza tecnica nella sezione "Se un programma ha generato un errore...". Se i suggerimenti descritti in questa sezione non risolvono l'errore o in assenza di informazioni nella Knowledge Base, inviare una richiesta al team di assistenza tecnica.

ERRORI DI CONFIGURAZIONE

Gli errori appartenenti a questa categoria si verificano nella maggior parte dei casi a causa di un'installazione non corretta dell'applicazione oppure a causa di modifiche apportate alla configurazione dell'applicazione, che ha provocato una perdita di funzionalità.

Suggerimenti generali:

Se vengono generati errori di questo tipo, si consiglia di riavviare gli aggiornamenti. Se l'errore persiste, contattare l'assistenza tecnica.

Se il problema è causato da un'installazione non appropriata dell'applicazione, si consiglia di reinstallarla.

Nessuna origine aggiornamenti specificata

Le origini specificate non contengono file di aggiornamento. È possibile che non siano state specificate origini degli aggiornamenti nelle impostazioni di aggiornamento. Verificare che le impostazioni di aggiornamento siano configurate correttamente e riprovare.

<i>Errore nella verifica della licenza</i> Tale errore viene generato se la chiave di licenza utilizzata dall'applicazione è bloccata e posizionata nell'elenco di licenze bloccate.
<i>Errore nel recupero delle impostazioni di aggiornamento</i> Errore interno durante il recupero delle impostazioni dell'attività di aggiornamento. Verificare che le impostazioni di aggiornamento siano configurate correttamente e riprovare.
<i>Privilegi insufficienti per aggiornare</i> In genere, tale errore si verifica quando l'account utente utilizzato per avviare l'aggiornamento non dispone di privilegi di accesso all'origine degli aggiornamenti. Si consiglia di verificare che l'account utente disponga dei privilegi necessari. Tale errore può essere generato anche quando si tenta di copiare i file di aggiornamento in una cartella che non è possibile creare.
<i>Errore interno</i> Errore logico interno durante l'attività di aggiornamento. Verificare che le impostazioni di aggiornamento siano configurate correttamente e riprovare.
<i>Errore nella verifica degli aggiornamenti</i> Tale errore viene generato se i file scaricati dall'origine degli aggiornamenti non superano la verifica interna. Ritentare l'aggiornamento in un secondo momento.
ERRORI CHE SI VERIFICANO QUANDO SI LAVORA CON FILE E CARTELLE Questo tipo di errori si verifica quando l'account utente utilizzato per eseguire gli aggiornamenti dispone di diritti limitati o di nessun diritto ad accedere all'origine degli aggiornamenti o alla cartella in cui sono ubicati gli aggiornamenti. <u>Suggerimenti generali:</u> Se si verificano errori di questo tipo, si consiglia di verificare che l'account utente disponga di diritti di accesso sufficienti a tali file e cartelle.
<i>Impossibile creare cartella</i> Tale errore viene generato se non è possibile creare una cartella durante la procedura di aggiornamento.
<i>Privilegi insufficienti per eseguire le operazioni con i file</i> Tale errore verifica se l'account utente utilizzato per eseguire l'aggiornamento non dispone di privilegi sufficienti per eseguire operazioni con i file.
<i>File o cartella non trovati</i> Tale errore si verifica se un file o una cartella necessario negli aggiornamenti è inesistente. Si consiglia di verificare l'esistenza e la disponibilità del file o della cartella specificati.
<i>Errore nelle operazioni con i file</i> Si tratta di un errore logico interno del modulo di aggiornamento durante l'esecuzione delle operazioni con i file.
ERRORI DI RETE Gli errori che rientrano in questa categoria si verificano in caso di problemi di connessione o quando una connessione di rete non è configurata correttamente. <u>Suggerimenti generali:</u> Se si verificano errori di questo tipo, si consiglia di verificare che il computer sia connesso a Internet, le impostazioni di connessione siano configurate correttamente e l'origine degli aggiornamenti sia disponibile. Quindi, ritentare l'aggiornamento. Se il problema persiste, contattare l'assistenza tecnica.
<i>Errore di rete</i> Si è verificato un errore nel recupero dei file di aggiornamento. Se si riscontra questo errore, verificare la connessione di rete del computer.

<i>Connessione interrotta</i> Tale errore si verifica quando l'origine degli aggiornamenti viene interrotta dal server di aggiornamento per qualsiasi motivo.
<i>Timeout operazione rete</i> Timeout della connessione all'origine degli aggiornamenti. Quando si configurano le impostazioni di aggiornamento del programma, è possibile che sia stato impostato un valore di timeout breve per la connessione all'origine degli aggiornamenti. Se il computer non è in grado di stabilire la connessione con il server o con la cartella di aggiornamento durante il periodo specificato, viene restituito questo errore. In tal caso, si consiglia di verificare che le impostazioni del Programma di aggiornamento siano corrette e che l'origine degli aggiornamenti sia disponibile.
<i>Errore di autorizzazione sul server FTP</i> Tale errore si verifica se le impostazioni di autorizzazione del server FTP utilizzate come origine degli aggiornamenti non sono state immesse correttamente. Accertarsi che le impostazioni del server FTP effettivo consentano all'account utente di scaricare file.
<i>Errore di autorizzazione sul server proxy</i> Tale errore viene generato se le impostazioni di aggiornamento mediante un server proxy indicano erroneamente il nome e la password oppure se l'account utente in cui vengono eseguiti tali aggiornamenti non dispone di privilegi di accesso all'origine degli aggiornamenti. Modificare le impostazioni di autorizzazione e ritentare l'aggiornamento.
<i>Errore nella risoluzione del nome DNS</i> Tale errore viene generato se non si rilevano origini degli aggiornamenti. È possibile che l'indirizzo dell'origine degli aggiornamenti non sia indicato correttamente, le impostazioni di rete non siano valide o che il server DNS non sia disponibile. Si consiglia di verificare le impostazioni di aggiornamento e la disponibilità delle origini degli aggiornamenti, quindi riprovare.
<i>Impossibile stabilire la connessione con l'origine degli aggiornamenti</i> Tale errore si verifica in assenza di connessione con l'origine degli aggiornamenti. Verificare che le impostazioni dell'origine degli aggiornamenti siano configurate correttamente e riprovare.
<i>Impossibile stabilire la connessione con il server proxy</i> Tale errore viene generato se le impostazioni di connessione al server proxy non sono indicate correttamente. Per risolvere il problema, si consiglia di verificare che le impostazioni siano configurate correttamente, il server proxy sia disponibile e la connessione Internet sia disponibile, quindi eseguire di nuovo l'aggiornamento.
<i>Errore nella risoluzione del nome DNS del server proxy</i> Tale errore viene generato se non si rileva il server proxy. Si consiglia di verificare che le impostazioni del server proxy siano valide e che il server DNS sia disponibile.
ERRORI CORRELATI AI DATABASE DANNEGGIATI Tali errori vengono generati in caso di file danneggiati nell'origine degli aggiornamenti. <u>Suggerimenti generali:</u> Se si esegue l'aggiornamento dai server Web di Kaspersky Lab, ritentare l'aggiornamento. Se il problema persiste, contattare l'assistenza tecnica. Se si esegue l'aggiornamento da un'altra origine, ad esempio una cartella locale, si consiglia di eseguire l'aggiornamento dai server Web di Kaspersky Lab. Se l'errore si verifica di nuovo, contattare l'assistenza tecnica di Kaspersky Lab.
<i>File inesistente nell'origine degli aggiornamenti</i> Tutti i file scaricati e installati sul computer durante il processo di aggiornamento vengono elencati in un file speciale incluso nell'aggiornamento. Tale errore si verifica in presenza di eventuali file nell'elenco di aggiornamenti non disponibile nell'origine degli aggiornamenti.
<i>Errore nella verifica della firma</i> È possibile che venga restituito questo errore se la firma elettronica digitale del pacchetto di aggiornamento scaricato è danneggiata o non corrisponde alla firma di Kaspersky Lab.

<i>File di indice danneggiato o mancante</i> Tale errore viene generato se il file di indice in formato .xml utilizzato dall'aggiornamento non esiste nell'origine degli aggiornamenti oppure è danneggiato.
ERRORI CORRELATI ALL'AGGIORNAMENTO CON IL COMPONENTE ADMINISTRATION SERVER DI KASPERSKY ADMINISTRATION KIT Tali errori sono generati in caso di problemi di aggiornamento dell'applicazione mediante il componente Administration Server di Kaspersky Administration Kit. <u>Suggerimenti generali:</u> Innanzitutto, verificare che Kaspersky Administration Kit e i relativi componenti (Administration Server e Network Agent) siano installati e in esecuzione. Ritentare l'aggiornamento. Se l'aggiornamento non riesce, riavviare Network Agent e Administration Server, quindi ritentare l'aggiornamento. Se il problema persiste, contattare l'assistenza tecnica.
<i>Errore di connessione ad Administration Server</i> Tale errore viene generato se non è possibile stabilire la connessione con il componente Administration Server di Kaspersky Administration Kit. Si consiglia di verificare che il componente NAgent sia installato e in esecuzione.
<i>Errore di registrazione in NAgent</i> Se si verifica tale errore, attenersi ai suggerimenti generali per la risoluzione di questo tipo di errore. Se l'errore si verifica di nuovo, inviare il file di rapporto dettagliato per l'aggiornamento e Network Agent sul computer al servizio di assistenza servendosi del modulo online. Descrivere la situazione dettagliatamente.
<i>Impossibile stabilire la connessione. Administration Server è occupato e non è in grado di elaborare la richiesta</i> In tal caso, è necessario tentare l'aggiornamento in un secondo momento.
<i>Impossibile stabilire la connessione con Administration Server / Main Administration Server / NAgent, errore fisico / errore sconosciuto</i> Se si riscontrano questo tipo di errori, si consiglia di tentare l'aggiornamento in un secondo momento. Se il problema persiste, contattare l'assistenza tecnica.
<i>Errore nel recupero del file da Administration Server, argomento di trasporto non valido</i> Se l'errore persiste, contattare l'assistenza tecnica.
<i>Errore nel recupero del file da Administration Server</i> Se si riscontrano questo tipo di errori, si consiglia di tentare l'aggiornamento in un secondo momento. Se il problema persiste, contattare l'assistenza tecnica.
CODICI VARI Tale categoria comprende gli errori che non è possibile includere nelle categorie precedentemente descritte.
<i>File per l'operazione di rollback mancanti</i> Tale errore si verifica se è stato eseguito un altro tentativo di rollback dopo aver completato il rollback degli aggiornamenti senza installare nessun aggiornamento. Non è possibile ripetere la procedura di rollback fino al completamento di un aggiornamento riuscito che ripristini un set di file sottoposti a backup.

CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

La finestra delle impostazioni dell'applicazione consente di accedere rapidamente alle principali impostazioni di Kaspersky Anti-Virus 6.0.

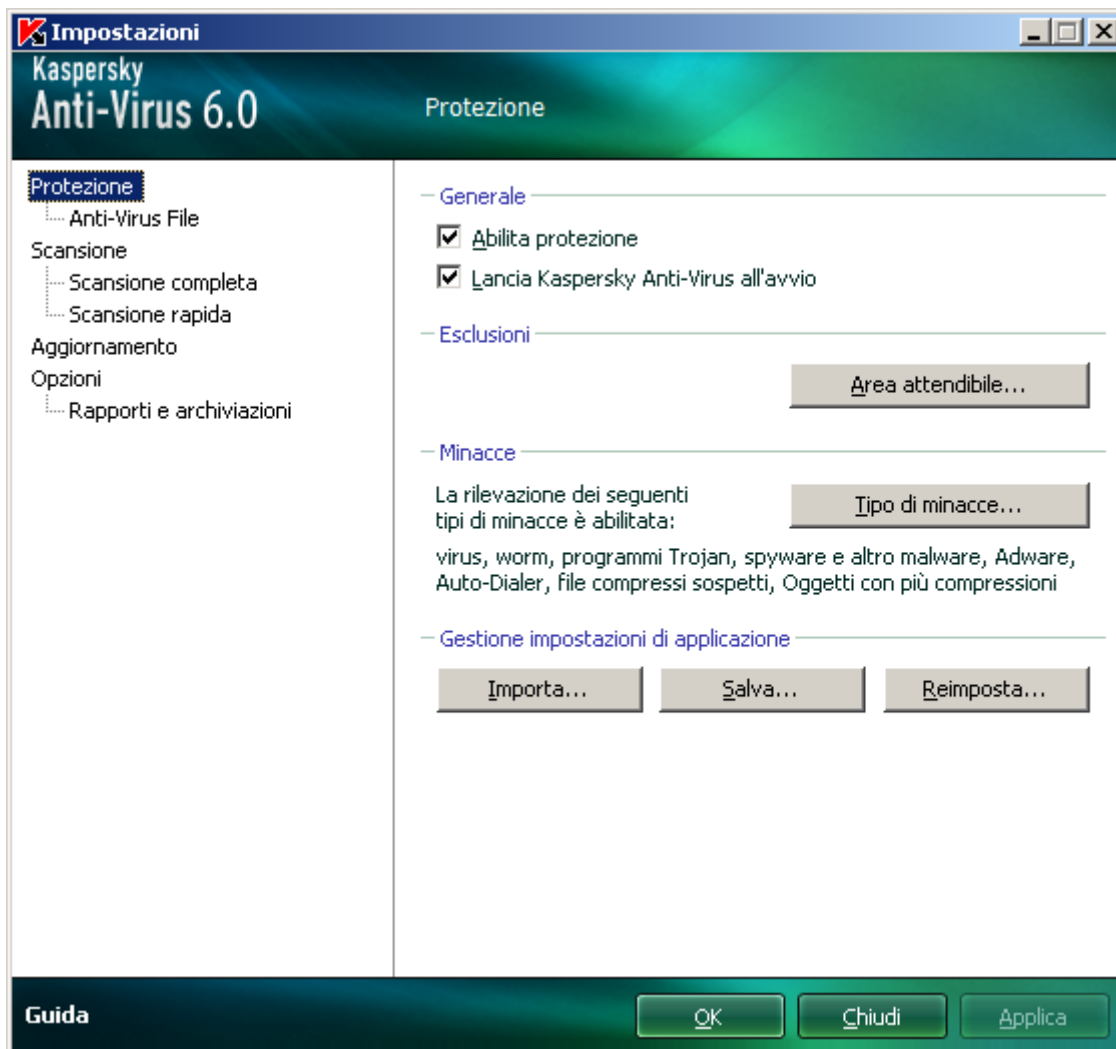


Fig. 9. Finestra di configurazione delle impostazioni dell'applicazione

La finestra è composta da due parti:

- la parte sinistra consente di accedere ai componenti di Anti-Virus File, alle attività di scansione anti-virus, alle attività di aggiornamento e così via.
- la parte destra della finestra contiene un elenco di impostazioni relative, ad esempio, al componente e all'attività selezionati nella parte sinistra della finestra.

È possibile aprire questa finestra:

- Dalla finestra principale dell'applicazione. A tale scopo, cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.

- Dal menu di scelta rapida. A tale scopo, selezionare la voce **Impostazioni** dal menu di scelta rapida.

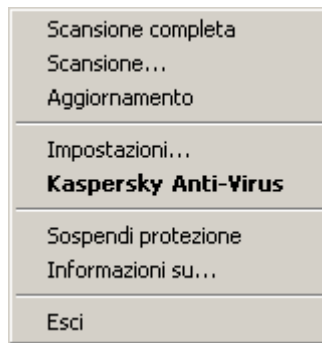


Fig. 10. Menu di scelta rapida

IN QUESTA SEZIONE

Protezione	73
Anti-Virus File	80
Scansione.....	80
Aggiornamento	81
Impostazioni	81
Rapporti e archiviazioni	86

PROTEZIONE

Nella finestra **Protezione** è possibile utilizzare le funzioni avanzate di Kaspersky Anti-Virus elencate di seguito:

- Abilitazione / disabilitazione della protezione dell'applicazione (vedere pagina [73](#)).
- Avvio dell'applicazione all'avvio del sistema operativo (vedere pagina [74](#)).
- Selezione delle categorie di minacce rilevabili (vedere pagina [74](#)).
- Creazione di un'area attendibile (vedere pagina [74](#)):
 - creazione di una regola di esclusione (vedere pagina [75](#));
 - creazione di un elenco di applicazioni attendibili (vedere pagina [77](#));
 - esportazione / importazione dei componenti dell'area attendibile (vedere pagina [78](#)).
- Esportazione / importazione delle impostazioni dell'applicazione (vedere pagina [79](#)).
- Ripristino delle impostazioni predefinite dell'applicazione (vedere pagina [79](#)).

ABILITAZIONE/DISABILITAZIONE DELLA PROTEZIONE DEL COMPUTER

Per impostazione predefinita, Kaspersky Anti-Virus viene avviato durante il caricamento del sistema operativo e protegge il computer finché non viene spento. File Anti-Virus è in esecuzione.

È possibile disabilitare tutti i tipi di protezione disponibili in Anti-Virus File.

Kaspersky Lab consiglia di **non disabilitare la protezione**, in quanto tale operazione può provocare un'infezione del server e la perdita di dati.

La disabilitazione della protezione provoca l'interruzione di Anti-Virus File. La disabilitazione dei componenti non altera l'esecuzione delle attività di scansione anti-virus e di aggiornamento di Kaspersky Anti-Virus.

➤ *Per disabilitare completamente la protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Deselezionare la casella ☒ **Abilita la protezione**.

AVVIO DELL'APPLICAZIONE ALL'AVVIO DEL SISTEMA OPERATIVO

Se per qualsiasi motivo è necessario arrestare completamente Kaspersky Anti-Virus, selezionare la voce **Esci** dal menu di scelta rapida dell'applicazione. In questo modo, l'applicazione verrà rimossa dalla memoria RAM, causando l'esecuzione del computer in uno stato non protetto.

Per abilitare la protezione del computer, avviare l'applicazione dal menu **Avvia** → **Programmi** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0**.

La protezione può essere anche ripresa automaticamente dopo aver riavviato il sistema operativo.

➤ *Per avviare la modalità di avvio dell'applicazione all'avvio del sistema operativo, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la casella ☒ **Lancia Kaspersky Anti-Virus all'avvio**.

SELEZIONE DELLE CATEGORIE DI MINACCE RILEVABILI

Kaspersky Anti-Virus protegge da diversi tipi di programmi pericolosi. A prescindere dalle impostazioni selezionate, viene sempre eseguita la scansione e la disinfezione per eliminare virus e Trojan. Questi programmi infatti possono danneggiare gravemente il computer. Per offrire una maggiore protezione, è possibile ampliare l'elenco di minacce da rilevare, abilitando il controllo di vari programmi potenzialmente pericolosi.

➤ *Per selezionare le categorie di minacce rilevabili, eseguire le operazioni seguenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Minacce**, cliccare sul bottone **Tipi di minacce**.
4. Nella finestra **Tipi di minacce** visualizzata, selezionare le ☒ caselle relative alle categorie di minacce da cui si desidera proteggere il computer.

CREAZIONE DI UN'AREA ATTENDIBILE

L'*area attendibile* è un elenco di oggetti creati dall'utente non esaminati da Kaspersky Anti-Virus. In altre parole, si tratta di una serie di programmi esclusi dall'ambito di protezione dell'applicazione.

L'utente crea un'area attendibile sulla base delle caratteristiche degli oggetti che utilizza e delle applicazioni installate nel computer. Questo elenco di esclusioni può tornare utile, ad esempio, se Kaspersky Anti-Virus blocca l'accesso a un oggetto o un'applicazione della cui sicurezza l'utente è assolutamente certo.

È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file oppure escludere un'area specifica (ad esempio una cartella o un'applicazione), processi di programmi oppure oggetti in base alla classificazione dell'Enciclopedia di virus (stato assegnato da Kaspersky Anti-Virus durante una scansione).

Un oggetto di esclusione viene escluso dalla scansione quando il disco o la cartella in cui è ubicato è sottoposto a scansione. Tuttavia, se si seleziona specificamente tale oggetto, la regola di esclusione non verrà applicata a questo.

► Per creare un elenco di esclusioni dalla scansione, eseguire le seguenti operazioni:

1. Aprire nella finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul bottone **Area attendibile**.
4. Nella finestra visualizzata, configurare le regole di esclusione per gli oggetti (vedere pagina [75](#)) e creare l'elenco di applicazioni attendibili (vedere pagina [77](#)).

VEDERE ANCHE

Creazione di una regola di esclusione.....	75
Maschere di esclusione file consentite	76
Maschere di esclusione consentite secondo la Virus Encyclopedia	77
Creazione dell'elenco di applicazioni attendibili.....	77
Esportazione/importazione di componenti di area attendibile.....	78

CREAZIONE DI UNA REGOLA DI ESCLUSIONE

Le *regole di esclusione* sono insiemi di condizioni utilizzati da Kaspersky Anti-Virus per verificare se sia possibile evitare la scansione di un oggetto.

È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file o escludere una determinata area, ad esempio una cartella o un'applicazione, processi di programmi o oggetti in base alla classificazione dell'Enciclopedia di virus.

Il *tipo di minaccia* è lo stato assegnato da Kaspersky Anti-Virus a un oggetto durante la scansione. Tale stato viene assegnato in base alla classificazione di malware e riskware individuata nell'Enciclopedia di virus di Kaspersky Lab.

Il software potenzialmente pericoloso non svolge una funzione dannosa vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice nocivo in quanto contiene errori e vulnerabilità. Tale categoria comprende, ad esempio, applicazioni di amministrazione remota, client IRC, server FTP, utilità di vario genere per interrompere o nascondere processi, keylogger, macro di password, autodialer e così via. Tali applicazioni software non vengono considerate come virus ma possono essere suddivise in diversi tipi, ad esempio Adware, Joke, Riskware ecc. (per ulteriori informazioni sulle applicazioni software potenzialmente pericolose rilevate da Kaspersky Anti-Virus, consultare l'Enciclopedia di virus disponibile all'indirizzo www.viruslist.com (<http://www.viruslist.com/en/viruses/encyclopedia>)). Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di questi programmi vengono sfruttati ampiamente dagli utenti, è possibile escluderli dalla scansione. A tale scopo, è necessario aggiungere il nome della minaccia oppure la maschera del nome della minaccia (in base alla classificazione dell'Enciclopedia di virus) all'area attendibile.

È ad esempio possibile che si utilizzi frequentemente un programma di amministrazione remota, si tratta di un sistema di accesso remoto che consente di utilizzare le risorse da un computer remoto. Kaspersky Anti-Virus rileva questo tipo di

attività come potenzialmente pericolose e potrebbe bloccarle. Per evitare di bloccare l'applicazione, è necessario creare una regola di esclusione per specificare Remote Admin come verdetto.

L'aggiunta di un'esclusione crea un criterio, che in seguito può essere utilizzato da Anti-Virus File e durante l'esecuzione di attività anti-virus.

► Per creare una regola di esclusione, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul bottone **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Regole di esclusione**, cliccare sul bottone **Aggiungi**.
5. Nella finestra **Maschera di esclusione** visualizzata, sezione **Proprietà**, selezionare un tipo di esclusione. Quindi, nella sezione **Descrizione della regola**, assegnare i valori ai tipi di esclusione selezionati e scegliere i componenti da includere nella regola.

► Per creare una regola di esclusione dalla finestra dei rapporti, eseguire le seguenti operazioni:

1. Selezionare l'oggetto nel rapporto da aggiungere alle esclusioni.
2. Selezionare la voce **Aggiungi a zona attendibile** dal menu di scelta rapida dell'oggetto specificato.
3. Nella finestra visualizzata **Maschera di esclusione** assicurarsi che le impostazioni dei criteri di esclusione siano quelli desiderate. I campi relativi al nome dell'oggetto e al tipo di minaccia pertinente vengono compilati automaticamente in base ai dati del rapporto. Per creare la regola, cliccare sul bottone **OK**.

MASCHERE DI ESCLUSIONE FILE CONSENTITE

Di seguito vengono illustrati in modo dettagliato alcuni esempi di maschere consentite che è possibile utilizzare per la creazione dell'elenco di file da escludere dalla scansione:

1. Maschere senza percorsi file:
 - ***.exe** – tutti i file con l'estensione .exe;
 - ***.ex?** – tutti i file con l'estensione ex? , in cui? può rappresentare un qualsiasi carattere singolo;
 - **test** – tutti i file con il nome test.
2. Maschere con percorsi file assoluti:
 - **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file contenuti nella cartella C:\dir\;
 - **C:\dir*.exe** – tutti i file con l'estensione .exe contenuti nella cartella C:\dir\;
 - **C:\dir*.ex?** – tutti i file con l'estensione ex? contenuti nella cartella C:\dir\, dove ? può rappresentare qualsiasi carattere;
 - **C:\dir\test** – solo il file con il nome C:\dir\test.

Se non si desidera che l'applicazione esegua la scansione dei file in tutte le sottocartelle nidificate della cartella specificata,

☒ selezionare la casella **Includi sottocartelle** durante la creazione della maschera.

3. Maschere con percorsi file:
 - **dir*.*** o **dir*** o **dir** – tutti i file contenuti in tutte le cartelle dir\;

- **dir\test** – tutti i file *test* contenuti nelle cartelle *dir*;
- **dir*.exe** – tutti i file con l'estensione *.exe* contenuti in tutte le cartelle *dir*;
- **dir*.ex?** – tutti i file con l'estensione *ex?* in tutte le cartelle *dir*, in cui *?* può rappresentare qualsiasi carattere.

Se non si desidera che l'applicazione esegua la scansione dei file in tutte le sottocartelle nidificate della cartella specificata,

☒ selezionare la casella **Includi sottocartelle** durante la creazione della maschera.

Le maschere di esclusione **.** e *** possono essere utilizzate solo se si specifica il tipo di classificazione della minaccia indicato nella Virus Encyclopedia. In questo caso la minaccia specificata non verrà rilevata in alcun oggetto. L'uso di queste maschere senza specificare una classificazione in sostanza disabilita il monitoraggio. Inoltre, durante l'impostazione di un'esclusione, non è consigliabile selezionare un percorso relativo a un disco di rete creato in base a una cartella del file system attraverso il comando *subst*, nonché a un disco che rispecchia una cartella di rete. Potrebbe accadere infatti che a risorse diverse venga assegnato lo stesso nome del disco per utenti diversi, con l'inevitabile conseguenza di attivare in modo errato le regole di esclusione.

VEDERE ANCHE

Maschere di esclusione consentite secondo la Virus Encyclopedia [77](#)

MASCHERE DI ESCLUSIONE CONSENTITE SECONDO LA VIRUS ENCYCLOPEDIA

Quando si aggiungono maschere per escludere determinate minacce in base alla relativa classificazione in Virus Encyclopedia, è possibile specificare le impostazioni seguenti:

- Il nome completo della minaccia come indicato nell'Enciclopedia di virus all'indirizzo www.viruslist.com (<http://www.viruslist.com>), ad esempio **not-a-virus:RiskWare.RemoteAdmin.RA.311** o **Flooder.Win32.Fuxx**.
- Il nome della minaccia in base alla maschera, ad esempio:
 - **not-a-virus*** – esclude i programmi legittimi ma potenzialmente pericolosi dalla scansione, oltre ai programmi joke;
 - ***Riskware.*** – esclude il riskware dalla scansione;
 - ***RemoteAdmin.*** – esclude tutti i programmi di amministrazione remota dalla scansione.

VEDERE ANCHE

Maschere di esclusione file consentite [76](#)

CREAZIONE DELL'ELENCO DI APPLICAZIONI ATTENDIBILI

È possibile creare un elenco di applicazioni attendibili. L'attività di tali programmi (inclusi l'attività sospetta, l'attività dei file, l'attività di rete e i tentativi di accesso al registro di sistema) non verrà controllata.

È ad esempio possibile ritenere che gli oggetti utilizzati in **Blocco note** di Microsoft Windows siano sicuri e non necessitino di scansione. In altre parole, si considera affidabile quest'applicazione. Per escludere dalla scansione gli oggetti utilizzati da questo processo, aggiungere l'applicazione **Blocco note** all'elenco delle applicazioni attendibili. Il file eseguibile e il processo dell'applicazione attendibile saranno contemporaneamente sottoposti a scansione anti-virus

come in precedenza. Per escludere completamente un'applicazione dalla scansione, è consigliabile utilizzare le regole di esclusione.

Inoltre, determinate azioni classificate come pericolose potrebbero essere ritenute normali da diverse applicazioni. Le applicazioni che ad esempio commutano automaticamente le tastiere, come Punto Switcher, intercettano regolarmente il testo immesso sulla tastiera. Per tenere conto delle caratteristiche specifiche di tali applicazioni e disabilitare il monitoraggio delle relative attività, è consigliabile aggiungerle all'elenco delle applicazioni attendibili.

L'utilizzo dell'elenco di esclusione delle applicazioni attendibili consente inoltre di risolvere i potenziali conflitti di compatibilità tra Kaspersky Anti-Virus e altre applicazioni (ad esempio, traffico di rete da un altro computer già esaminato dall'applicazione anti-virus) e di potenziare la produttività del computer, particolarmente importante quando si utilizzano applicazioni server.

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

➡ *Per aggiungere un'applicazione all'elenco delle applicazioni attendibili, eseguire le operazioni seguenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul bottone **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Applicazioni attendibili**, cliccare sul bottone **Aggiungi**.
5. Nella finestra **Applicazione attendibile** visualizzata, selezionare il programma cliccando sul bottone **Sfoglia**. Viene aperto un menu di scelta rapida dal quale, cliccando su **Sfoglia**, si accede alla finestra standard di selezione file per selezionare il percorso del file eseguibile; oppure cliccando su **Applicazioni**, è possibile passare all'elenco delle applicazioni attualmente in esecuzione e selezionarne una o più, secondo necessità. Specificare le impostazioni necessarie per l'applicazione selezionata.

ESPORTAZIONE/IMPORTAZIONE DI COMPONENTI DI AREA ATTENDIBILE

Con le funzioni di importazione ed esportazione, è possibile trasferire le regole di esclusione e gli elenchi di applicazioni attendibili su altri computer.

➡ *Per copiare le regole di esclusione, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul bottone **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Regole di esclusione**, cliccare sui bottoni **Esporta** o **Importa** per copiare le regole.

➡ *Per copiare l'elenco di applicazioni attendibili, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul bottone **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Applicazioni attendibili**, cliccare sui bottoni **Esporta** o **Importa** per copiare l'elenco.

ESPORTAZIONE / IMPORTAZIONE DELLE IMPOSTAZIONI DI KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus consente di importare ed esportare le proprie impostazioni.

Questa funzione è utile, ad esempio, quando l'applicazione è installata sia nel computer di casa che in quello dell'ufficio. È possibile configurare le impostazioni preferite del programma sul computer di casa, esportarle sotto forma di file su un disco e, servendosi della funzione di importazione, caricarle sul computer in ufficio. Le impostazioni vengono salvate in uno speciale file di configurazione.

➡ *Per esportare le impostazioni correnti dell'applicazione, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Gestione impostazioni di applicazione** cliccare sul bottone **Salva**.
4. Nella finestra visualizzata, immettere il nome del file di configurazione e il percorso in cui salvarlo.

➡ *Per importare le impostazioni dell'applicazione da un file di configurazione salvato, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Gestione impostazioni di applicazione** cliccare sul bottone **Importa**.
4. Nella finestra visualizzata, selezionare il file da cui importare le impostazioni di Kaspersky Anti-Virus.

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE

È sempre possibile ripristinare le impostazioni predefinite o consigliate di Kaspersky Anti-Virus. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Configurazione guidata dell'applicazione consente di ripristinare le impostazioni predefinite.

Nella finestra visualizzata, all'utente verrà richiesto di specificare quali impostazioni salvare durante il ripristino del livello di protezione necessario.

Al termine della procedura guidata, verrà impostato il livello di protezione **Consigliato** per Anti-Virus File, tenendo in considerazione le impostazioni che si è deciso di mantenere inalterate durante il ripristino. Verranno inoltre applicate le impostazioni specificate durante l'esecuzione della procedura guidata.

➡ *Per ripristinare le impostazioni relative alla protezione, eseguire le operazioni seguenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Gestione impostazioni di applicazione**, cliccare sul bottone **Reimposta**.
4. Nella finestra visualizzata, selezionare le caselle relative alle impostazioni da salvare. Cliccare sul bottone **Avanti**. Verrà avviata la configurazione guidata iniziale di cui sarà necessario seguire le indicazioni.

ANTI-VIRUS FILE

Le impostazioni del componente **Anti-Virus File** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Protezione anti-virus del file system del computer" a pag. [38](#)). Modificando le impostazioni dell'applicazione, è possibile:

- modificare il livello di sicurezza (vedere a pag. [40](#));
- modificare l'azione intrapresa in caso di rilevamento di oggetti (vedere pagina [40](#));
- creare un ambito di protezione (vedere a pag. [41](#));
- ottimizzare la scansione (vedere a pag. [43](#));
- configurare la scansione di file compositi (vedere a pag. [43](#));
- modificare la modalità di scansione (vedere a pag. [44](#));
- utilizzare l'analisi euristica (vedere a pag. [42](#));
- sospendere il componente (vedere a pag. [45](#));
- selezionare una tecnologia di scansione (vedere a pag. [45](#));
- ripristinare le impostazioni di protezione predefinite (vedere a pag. [46](#)) nel caso fossero state modificate.

➡ *Per passare alle impostazioni di Anti-Virus File, eseguire le operazioni seguenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Virus File**.
3. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Cliccare sul bottone **Personalizza** per visualizzare le altre impostazioni di Anti-Virus File.

SCANSIONE

La selezione del metodo da utilizzare per la scansione degli oggetti presenti nel computer viene determinata da un set di proprietà assegnato a ogni attività.

Gli specialisti di Kaspersky Lab distinguono diverse attività di scansione anti-virus. Le più comuni sono le seguenti:

Scansione

Esame degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.

Scansione Completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete.

Scansione Rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo.

La finestra delle impostazioni di ciascun attività consente di eseguire le seguenti operazioni:

- selezionare il livello di sicurezza (vedere pagina [52](#)) con le impostazioni che verranno utilizzate dall'attività;
- selezionare un'azione (vedere pagina [53](#)) applicata quando si rileva un oggetto infetto / potenzialmente infetto;
- creare una pianificazione (vedere pagina [58](#)) per l'esecuzione automatica delle attività;
- specificare i tipi di file (vedere pagina [54](#)) da sottoporre a scansione anti-virus;
- specificare le impostazioni di scansione dei file compositi (vedere pagina [55](#));
- selezionare i metodi di scansione e le tecnologie di scansione (vedere pagina [56](#));
- assegnare impostazioni di scansione comuni a tutte le attività (vedere pagina [60](#)).

➡ *Per modificare le impostazioni dell'attività, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione (Scansione completa, Scansione rapida)**.
3. Nella parte destra della finestra, selezionare il livello di sicurezza necessario, la risposta alla minaccia, quindi configurare la modalità di esecuzione. Cliccare sul bottone **Personalizza** per visualizzare le altre impostazioni dell'attività. Per ripristinare le impostazioni predefinite, cliccare sul bottone **Livello predefinito**.

AGGIORNAMENTO

L'aggiornamento di Kaspersky Anti-Virus viene eseguito mediante le impostazioni che determinano quanto segue:

- l'origine (vedere pagina [63](#)) da cui verranno scaricati e installati gli aggiornamenti;
- la modalità di esecuzione dell'aggiornamento dell'applicazione (vedere a pag. [66](#)) e i componenti specifici da aggiornare (vedere a pag.);
- la frequenza di avvio degli aggiornamenti in caso di avvio pianificato configurato (vedere pagina [65](#));
- l'account (vedere pagina [65](#)) con cui avviare l'aggiornamento;
- se gli aggiornamenti devono essere copiati in un'origine locale (vedere pagina [67](#));
- l'utilizzo di un server proxy (vedere pagina [64](#)).

➡ *Per procedere con la configurazione dell'aggiornamento, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Selezionare la modalità di esecuzione necessaria nella parte destra della finestra. Cliccare sul bottone **Configura** per passare alla configurazione di altre attività.

OPZIONI

Nella finestra **Opzioni** è possibile utilizzare le funzioni avanzate di Kaspersky Anti-Virus elencate di seguito:

- Auto-difesa dell'applicazione (vedere pagina [82](#)).

- Limitazione dell'accesso all'applicazione (vedere pagina [82](#)).
- Limitazione delle dimensioni dei file iSwift (vedere pagina [83](#)).
- Prestazioni del server per l'utilizzo di una configurazione multiprocessore (vedere a pag. [83](#)).
- Notifiche sugli eventi Kaspersky Anti-Virus (vedere pagina [84](#)):
 - selezione del tipo di eventi e modalità di invio delle notifiche (vedere pagina [85](#));
 - configurazione della notifica di posta elettronica (vedere pagina [85](#));
 - configurazione del registro di eventi (vedere pagina [86](#)).
- Elementi attivi dell'interfaccia (vedere pagina [86](#)).

AUTO-DIFESA DELL'APPLICAZIONE

Kaspersky Anti-Virus garantisce la protezione del computer da programmi malware e, proprio per questo, può essere essa stessa oggetto di attacchi da parte di tali programmi che cercano di bloccare l'attività o eliminarla.

Per garantire la stabilità del sistema di protezione del computer, l'applicazione dispone di propri meccanismi di auto-difesa e di protezione dall'accesso remoto.

Nei computer che utilizzano sistemi operativi Microsoft Windows Server 2008 e Windows Server 2003 a 64 bit (senza Service Packs installati), l'auto-difesa è disponibile solo per impedire la modifica o l'eliminazione dei file di Kaspersky Anti-Virus sui dischi locali e delle relative voci del Registro di sistema.

Quando la protezione da accessi remoti è abilitata, in alcuni casi è possibile che sia necessario consentire i programmi di amministrazione remota (ad esempio RemoteAdmin) per gestire l'applicazione. A tale scopo, è necessario aggiungere tali programmi all'elenco di applicazioni attendibili e abilitare l'impostazione **Consenti interazione con interfaccia applicazione** per questi.

➡ Per abilitare il meccanismo di auto-difesa di Kaspersky Anti-Virus, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Auto-Difesa**, selezionare la casella ☒ **Abilita Auto-Difesa** per distribuire il meccanismo di protezione di Kaspersky Anti-Virus dalle modifiche o dall'eliminazione dei file del disco rigido, dei processi della RAM e delle voci del Registro di sistema.

Nella sezione **Auto-Difesa**, selezionare la casella ☒ **Disabilita controllo esterno del servizio di sistema** per bloccare qualsiasi tentativo di gestire i servizi dell'applicazione in remoto.

Se si tenta di eseguire una delle azioni elencate, verrà visualizzato un messaggio sopra l'icona dell'applicazione nell'area di notifica della barra delle applicazioni (sempre che il servizio di notifica non sia stato disabilitato dall'utente).

RESTRIZIONE DELL'ACCESSO ALL'APPLICAZIONE

Un personal computer può essere utilizzato da diversi utenti, con differenti livelli di esperienza in ambito informatico. Pertanto, lasciare libero accesso a Kaspersky Anti-Virus e alle relative impostazioni potrebbe ridurre notevolmente il livello di protezione del computer nel suo insieme.

Per aumentare il livello di protezione del computer, utilizzare una password per accedere a Kaspersky Anti-Virus. In questo modo, è possibile che vengano bloccate tutte le operazioni, ad eccezione delle notifiche di rilevamento di oggetti pericolosi e viene impedita l'esecuzione delle seguenti azioni:

- modifica delle impostazioni dell'applicazione;
- chiusura dell'applicazione;
- disabilitazione di Anti-Virus File e delle attività di scansione;
- disabilitazione dei criteri (quando l'applicazione viene eseguita mediante Kaspersky Administration Kit);
- rimozione dell'applicazione.

Ognuna delle azioni sopra descritte comporta un abbassamento del livello di protezione del computer, quindi tentare di stabilire gli utenti del computer autorizzati a intraprendere tali azioni.

➡ *Per proteggere l'accesso all'applicazione con una password, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Protezione tramite password**, selezionare la casella ☒ **Abilita protezione tramite password** e cliccare sul bottone **Impostazioni**.
4. Nella finestra **Protezione tramite password** visualizzata, immettere la password e specificare l'area da includere nella limitazione di accesso. In questo modo, ogni volta che un utente del computer cercherà di eseguire le azioni selezionate dovrà immettere una password.

LIMITAZIONE DELLE DIMENSIONI DEI FILE iSWIFT

I file *iSwift* contengono informazioni sugli oggetti NTFS già sottoposti a una scansione anti-virus (con tecnologia *iSwift*). L'utilizzo di tali file consente di velocizzare la scansione, poiché Kaspersky Anti-Virus esamina soltanto gli oggetti modificati dall'ultima scansione. Col tempo, le dimensioni dei file *iSwift* aumentano. Si consiglia di limitare le dimensioni di tali file. Una volta raggiunto il valore specificato, il file *iSwift* verrà cancellato.

➡ *Per limitare le dimensioni dei file iSwift, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Risorse**, selezionare la casella ☒ **Reimposta database iSwift quando raggiunge** e specificare la dimensione del database in MB.

CONFIGURAZIONE SERVER MULTIPROCESSORE

Se si utilizza una configurazione di server multiprocessore, è possibile gestire le prestazioni del server nei modi seguenti:

- Impostare il numero di copie del kernel anti-virus da caricare per l'esecuzione di Kaspersky Anti-Virus sul server (es. il numero dei processi anti-virus in esecuzione in parallelo sul server).

Maggiore è il numero di copie del kernel anti-virus in esecuzione, più veloce sarà l'elaborazione dei oggetti da parte dell'anti-virus. Tuttavia, ciò influisce sulle prestazioni globali del server. Se il volume della RAM non è sufficiente o il numero di copie del kernel anti-virus in esecuzione è alto, potrebbero verificarsi errori nel funzionamento di Anti-Virus File.

Inoltre, l'esecuzione contemporanea di diversi processi anti-virus sul server garantisce la protezione continua del server in caso di errore del kernel.

- Controllare il carico del server: ad esempio, riservare una parte dei processori per l'elaborazione anti-virus degli oggetti e un'altra parte per le attività primarie del server.

Kaspersky Lab consiglia di riservare almeno un processore per le attività del server quando il programma è in esecuzione su un server multiprocessore.

➡ *Per impostare il numero di copie del kernel anti-virus, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Configurazione multi-CPU**, premere il pulsante **Dettagli**.
4. Nella finestra visualizzata **Configurazione multi-CPU**, nella sezione **Parametri**, specificare il numero di copie dell'anti-virus.

➡ *Per equilibrare il carico del server, eseguire le operazioni seguenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Configurazione multi-CPU**, premere il pulsante **Dettagli**.
4. Nella finestra visualizzata **Configurazione multi-CPU**, nella sezione **Processori utilizzati**, deselezionare le caselle ☒ dei processori riservati rigorosamente per il funzionamento del server.

NOTIFICHE DEGLI EVENTI DI KASPERSKY ANTI-VIRUS

Durante il funzionamento di Kaspersky Anti-Virus, si verificano diversi tipi di eventi, che possono essere di riferimento o contenere dati importanti. Un evento può ad esempio informare l'utente del completamento con esito positivo di un aggiornamento dell'applicazione o registrare un errore nel funzionamento di un determinato componente che deve essere eliminato immediatamente.

Per essere aggiornati sugli eventi più recenti che si verificano durante il funzionamento di Kaspersky Anti-Virus, utilizzare la funzione di notifica.

Le notifiche possono essere inviate in uno dei seguenti modi:

- messaggi a comparsa che vengono visualizzati sopra l'icona dell'applicazione nell'area di notifica;
- notifica acustica;
- messaggi di posta elettronica;
- registrazione di informazioni nel registro eventi.

➡ *Per utilizzare il servizio di notifica, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella ☒ **Abilita notifiche** e cliccare sul bottone **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, specificare i tipi di eventi Kaspersky Anti-Virus di cui si desidera ricevere notifiche e i tipi di notifiche.

VEDERE ANCHE

Selezione del tipo di evento e della modalità di invio delle notifiche.....	85
Configurazione della notifica tramite posta elettronica	85
Configurazione del registro eventi	86

SELEZIONE DEL TIPO DI EVENTO E DELLA MODALITÀ DI INVIO DELLE NOTIFICHE

Durante il funzionamento di Kaspersky Anti-Virus, si verificano i tipi di eventi seguenti:

- Le **notifiche critiche** sono eventi di una certa rilevanza. Si consiglia vivamente di segnalarle con le notifiche poiché fanno riferimento a problemi di funzionamento dell'applicazione o vulnerabilità della protezione del computer, ad esempio *database obsoleti* o *periodo di validità della licenza scaduto*.
- Le **notifiche di errori** sono eventi che causano l'interruzione del funzionamento dell'applicazione, ad esempio *database mancanti o danneggiati*.
- Le **notifiche importanti** sono eventi cui l'utente deve prestare attenzione poiché riflettono situazioni importanti nel funzionamento dell'applicazione, ad esempio *database obsoleti* o *prossima scadenza della licenza*.
- Le **notifiche minori** sono messaggi di riferimento che in linea generale non contengono informazioni importanti, ad esempio *oggetti in quarantena*.

➡ Per specificare quali eventi notificare all'utente e le modalità di notifica, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella ☒ **Abilita notifiche** e cliccare sul bottone **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, selezionare le ☒ caselle relative agli eventi di cui si desidera ricevere notifiche e le modalità di invio delle notifiche.

CONFIGURAZIONE DELLA NOTIFICA TRAMITE POSTA ELETTRONICA

Dopo aver selezionato gli eventi (per ulteriori informazioni, consultare la sezione "Selezione del tipo di evento e della modalità di invio delle notifiche" a pagina [85](#)) di cui si desidera ricevere una notifica tramite posta elettronica, è necessario impostare le notifiche.

➡ Per configurare le notifiche tramite posta elettronica, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella ☒ **Abilita notifiche** e cliccare sul bottone **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, selezionare le ☒ caselle relative agli eventi desiderati nel campo **Email** e cliccare sul bottone **Impostazioni posta elettronica**.
5. Nella finestra **Impostazioni di notifica e-mail** visualizzata, specificare i valori necessari per le impostazioni. Per inviare notifiche sugli eventi a orari stabiliti, creare una pianificazione per l'invio del messaggio informativo cliccando sul bottone **Cambia**. Apportare le modifiche necessarie nella finestra **Pianifica** visualizzata.

CONFIGURAZIONE DEL REGISTRO EVENTI

Kaspersky Anti-Virus offre la possibilità di registrare le informazioni relative agli eventi che si verificano mentre l'applicazione è in esecuzione, nel registro eventi generale di Microsoft Windows (**Applicazione**) o in un registro eventi specifico per Kaspersky Anti-Virus (**Registro Eventi Kaspersky**).

È possibile visualizzare gli eventi in **Visualizzatore eventi** di Microsoft Windows, selezionabile da **Avvia/Impostazioni/Pannello di controllo/Strumenti di amministrazione/Visualizza i registri eventi**.

► Per configurare il registro eventi, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella ☒ **Abilita notifiche** e cliccare sul bottone **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, selezionare le ☒ caselle relative agli eventi desiderati nel campo **Registro** e cliccare sul bottone **Impostazioni registro**.
5. Nella finestra **Impostazioni registro eventi** visualizzata, selezionare il registro in cui verranno registrate le informazioni sugli eventi.

ELEMENTI ATTIVI DELL'INTERFACCIA

Gli elementi attivi dell'interfaccia includono le seguenti opzioni di Kaspersky Anti-Virus:

Anima icona area di notifica della barra delle applicazioni.

L'icona dell'applicazione nell'area di notifica cambia in base all'operazione eseguita dall'applicazione. Ad esempio, durante la scansione dei messaggi di posta elettronica, viene visualizzata un'icona di lettera di piccole dimensioni di fronte all'icona dell'applicazione. Per impostazione predefinita, l'icona dell'applicazione è animata. In questo caso, l'icona mostra solo lo stato di protezione del computer: se la protezione è abilitata, l'icona è colorata, mentre se la protezione è sospesa o disabilitata, l'icona diventa grigia.

Mostra "Protected by Kaspersky Lab" nella schermata di accesso a Microsoft Windows.

Per impostazione predefinita, questo indicatore viene visualizzato nell'angolo superiore destro della schermata all'avvio di Kaspersky Anti-Virus e informa l'utente che il computer è protetto da qualsiasi tipo di minaccia.

► Per configurare gli elementi attivi dell'interfaccia, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Selezionare le caselle necessarie nella sezione **Aspetto**.

RAPPORTI E ARCHIVIAZIONI

La sezione contiene le impostazioni che consentono di controllare le operazioni con i file di dati dell'applicazione.

I file di dati dell'applicazione sono oggetti messi in quarantena da Kaspersky Anti-Virus o spostati nella cartella Backup, nonché file contenenti rapporti sul funzionamento dei componenti dell'applicazione.

In questa sezione, è possibile:

- configurare la creazione e l'archiviazione dei rapporti (vedere pagina [88](#));

- configurare la quarantena e il backup (vedere pagina [90](#));
- svuotare l'archivio dei rapporti, la quarantena e il backup.

➡ *Per svuotare le aree di archiviazione, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rapporti e archiviazioni**.
3. Nella finestra visualizzata, cliccare sul bottone **Cancella**.
4. Nella finestra **File di dati** visualizzata, specificare le aree di archiviazione da cui rimuovere tutti gli oggetti.

VEDERE ANCHE

Principi di gestione dei rapporti	87
Configurazione dei rapporti	88
Quarantena per oggetti potenzialmente infetti	88
Azioni sugli oggetti in quarantena.....	89
Copie di backup degli oggetti pericolosi	89
Utilizzo delle copie di backup	90
Configurazione della quarantena e del backup	90

PRINCIPI DI GESTIONE DEI RAPPORTI

Il funzionamento di Anti-Virus File e l'esecuzione di tutte le attività di scansione anti-virus e di aggiornamento vengono registrati in un rapporto.

➡ *Per visualizzare i rapporti, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul bottone **Rapporto**.

➡ *Per esaminare tutti gli eventi relativi alle prestazioni di un componente o di un'attività registrati nel rapporto, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione e premere il pulsante **Rapporto**.
2. Nella finestra visualizzata, sulla scheda **Rapporto**, selezionare il nome di un componente o di un'attività, quindi cliccare sul collegamento **Dettagli**. Di conseguenza, viene visualizzata una finestra contenente informazioni dettagliate sul funzionamento di Anti-Virus File o delle attività. Le statistiche relative alle prestazioni vengono visualizzate nella parte superiore della finestra; nelle varie schede poste nella parte centrale sono disponibili informazioni dettagliate. La struttura delle schede può variare in base al tipo di rapporto selezionato (per Anti-Virus File o per un'attività).

➡ *Per importare il rapporto in un file di testo, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone **Rapporto**.
2. Nella finestra visualizzata, sulla scheda **Rapporto**, selezionare il nome di un componente o di un'attività, quindi cliccare sul collegamento **Dettagli**.

3. Nella finestra visualizzata saranno disponibili le informazioni sulle prestazioni del componente o dell'attività selezionati. Premere il pulsante **Salva con nome** e specificare se si desidera salvare il file di rapporto.

CONFIGURAZIONE DEI RAPPORTI

È possibile modificare le seguenti impostazioni di creazione e salvataggio dei rapporti:

- Consentire o bloccare la registrazione degli eventi informativi. Solitamente, questi eventi non sono critici per la protezione (casella ☒ **Registra eventi non critici**).
- Consentire il salvataggio nel rapporto solo degli eventi che si sono verificati dall'ultimo avvio dell'attività. In questo modo è possibile limitare l'uso di spazio del disco riducendo le dimensioni del rapporto (casella ☒ **Mantieni solo eventi recenti**). Se la casella è selezionata, le informazioni verranno aggiornate ogni volta che l'attività viene riavviata. Tuttavia, verranno sovrascritte solo le informazioni non critiche.
- Impostare il termini di archiviazione per i rapporti (casella ☒ **Non memorizzare rapporti di oltre**). Per impostazione predefinita, la durata di archiviazione degli oggetti è di 30 giorni. Una volta trascorso questo periodo, gli oggetti vengono eliminati. È possibile modificare la durata massima di archiviazione o persino rimuovere eventuali limiti imposti su tale valore.
- Specificare le dimensioni massime del rapporto (casella ☒ **Dimensione massima**). Per impostazione predefinita, la dimensione massima è di 250 MB. È possibile annullare eventuali restrizioni impostate sulla dimensione del rapporto o immettere un altro valore.

➡ Per modificare le impostazioni di creazione e archiviazione, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rapporti e archiviazioni**.
3. Nella sezione **Rapporto**, selezionare tutte le caselle necessarie, quindi impostare il termine di archiviazione e la dimensione massima del rapporto, secondo necessità.

QUARANTENA PER OGGETTI POTENZIALMENTE INFETTI

Quarantena è uno speciale repository in cui vengono memorizzati gli oggetti che potrebbero essere stati infettati da virus.

Gli **oggetti potenzialmente infetti** sono oggetti sospettati di essere stati infettati da virus o relative varianti.

Perché *potenzialmente infetto*? Non è sempre possibile determinare esattamente se un oggetto è infetto, per i seguenti probabili motivi:

- *Il codice dell'oggetto analizzato ricorda quello di una minaccia nota ma è in parte modificato.*

I database dell'applicazione contengono informazioni sulle minacce al momento esaminate dagli specialisti di Kaspersky Lab. Se un programma dannoso è stato modificato e le modifiche non sono state ancora inserite nei database, Kaspersky Anti-Virus classifica l'oggetto infetto con il programma dannoso modificato come oggetto potenzialmente infetto e indica con esattezza la minaccia alla quale somiglia questa infezione.

- *La struttura del codice dell'oggetto rilevato ricorda un programma dannoso; tuttavia nei database dell'applicazione non è stato registrato nulla di simile.*

È abbastanza probabile che si tratti di un nuovo tipo di minaccia, pertanto Kaspersky Anti-Virus classifica l'oggetto come oggetto potenzialmente infetto.

I file vengono identificati come potenzialmente infettati da un virus dall'*analisi euristica di codice*. Questo meccanismo è estremamente efficace e determina falsi positivi molto raramente.

Un oggetto potenzialmente infetto può essere rilevato e messo in quarantena mediante una scansione anti-virus oppure da Anti-Virus File.

Quando un oggetto viene messo in Quarantena, viene spostato, non copiato. Esso viene eliminato dal disco o dalla posta elettronica e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

VEDERE ANCHE

Azioni sugli oggetti in quarantena.....	89
Configurazione della quarantena e del backup	90

AZIONI SUGLI OGGETTI IN QUARANTENA

È possibile eseguire le seguenti operazioni con gli oggetti in quarantena:

- mettere in quarantena i file sospettati di essere infetti;
- esaminare e disinfettare tutti gli oggetti potenzialmente infetti in quarantena utilizzando i database dell'applicazione correnti;
- ripristinare i file nelle cartelle da cui sono stati spostati per essere messi in quarantena oppure nelle cartelle selezionate dall'utente;
- eliminare tutti gli oggetti in quarantena oppure un gruppo di oggetti selezionati.

➡ *Per intraprendere azioni sugli oggetti in quarantena, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione e cliccare sul bottone pulsante **Rilevati**.
2. Nella finestra visualizzata, sulla scheda **Quarantena**, eseguire le azioni necessarie.

COPIE DI BACKUP DEGLI OGGETTI PERICOLOSI

In alcuni casi non è possibile mantenere l'integrità degli oggetti durante la disinfezione. Se il file disinfettato contiene informazioni importanti, e dopo la disinfezione diventa in parte o del tutto inaccessibile, è possibile provare a ripristinare l'oggetto originale dalla copia di backup.

La **copia di backup** è una copia dell'oggetto pericoloso originale creata quando l'oggetto è stato disinfettato o eliminato per la prima volta e salvata sotto forma di backup.

Backup è uno repository speciale che contiene copie di backup degli oggetti pericolosi dopo l'elaborazione o l'eliminazione. La principale funzione del backup è la possibilità di ripristinare in qualsiasi momento l'oggetto originale. I file del backup vengono salvati in un formato speciale e non costituiscono un pericolo.

VEDERE ANCHE

Utilizzo delle copie di backup	90
Configurazione della quarantena e del backup	90

UTILIZZO DELLE COPIE DI BACKUP

È possibile eseguire le seguenti operazioni con gli oggetti archiviati nel backup:

- ripristinare le copie selezionate;
- eliminare gli oggetti.

➡ Per intraprendere azioni sugli oggetti del backup, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione e cliccare sul pulsante **Rilevati**.
2. Nella finestra visualizzata, sulla scheda **Backup**, eseguire le azioni necessarie.

CONFIGURAZIONE DELLA QUARANTENA E DEL BACKUP

È possibile modificare le impostazioni seguenti per la quarantena e il backup:

- Abilitare la modalità Scansione automatica per gli oggetti in quarantena dopo ogni aggiornamento dei database dell'applicazione (casella ☒ **Scansiona file nella quarantena dopo l'aggiornamento**).

Kaspersky Anti-Virus non è in grado di eseguire la scansione degli oggetti in quarantena subito dopo l'aggiornamento dei database dell'applicazione se tali oggetti sono in uso.

- Determinare la durata massima di archiviazione per gli oggetti in quarantena e le copie degli oggetti nel backup (casella ☒ **Memorizza oggetti non più di**). Per impostazione predefinita, la durata di memorizzazione degli oggetti è di 90 giorni. Una volta trascorso questo periodo, gli oggetti vengono eliminati. È possibile modificare la durata massima di archiviazione o persino rimuovere eventuali limiti imposti su tale valore.
- Specificare la dimensione massima dell'area di archiviazione dei dati (casella ☒ **Dimensione massima**). Per impostazione predefinita, la dimensione massima è di 1000 MB. È possibile annullare eventuali restrizioni imposte sulla dimensione del rapporto o immettere un altro valore.

➡ Per configurare le impostazioni della quarantena e del backup:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rapporti e archiviazioni**.
3. Nella sezione **Quarantena e Backup**, selezionare le caselle desiderate e specificare la dimensione massima dell'area di memorizzazione dei dati in base alle esigenze.

DISCO DI RIPRISTINO

Kaspersky Anti-Virus comprende un servizio che consente di creare un Disco di Ripristino.

Disco di Ripristino è stato progettato per eseguire la scansione dei computer compatibili con le piattaforme x86 e per disinfettarli. È consigliabile utilizzarlo quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione di malware, ad esempio Kaspersky AVPTool, del sistema operativo. In questo caso, è possibile ottenere un livello di efficacia della disinfezione superiore, in quanto i programmi malware non ottengono il controllo quando viene caricato il sistema operativo.

Disco di Ripristino è un file con estensione iso basato sulla piattaforma Linux che include gli elementi seguenti:

- file di sistema e file Linux di configurazione;
- una serie di utilità diagnostiche per il sistema operativo;
- una serie di strumenti aggiuntivi (gestione file e così via);
- file di Disco di Ripristino Kaspersky;
- file contenenti i database dell'applicazione.

È possibile avviare un computer con un sistema operativo danneggiato in uno dei due modi seguenti:

- *in locale*, da un CD/DVD. A tale scopo, è necessario che il computer sia dotato di un dispositivo appropriato.
- *in remoto*, dalla stazione di lavoro dell'amministratore o da un altro computer sulla rete.

È possibile eseguire l'avvio remoto solo se il computer da avviare supporta la tecnologia Intel® vPro™ o Intel® Active Management.

➡ Per creare un Disco di Ripristino, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul pulsante **Disco di Ripristino** per eseguire la creazione guidata del Disco di Ripristino (vedere pagina [91](#)).
3. Seguire le istruzioni della procedura guidata.
4. Utilizzando il file fornito con la procedura guidata, creare un CD/DVD di avvio. A tale scopo, è possibile utilizzare un'applicazione di masterizzazione di CD/DVD, come Nero.

VEDERE ANCHE

Creazione del Disco di Ripristino.....	91
Avvio del computer attraverso il Disco di Ripristino	93

CREAZIONE DEL DISCO DI RIPRISTINO

La creazione del Disco di Ripristino comporta la creazione di un'immagine del disco (file ISO) con database e file di configurazione anti-virus aggiornati.

L'immagine del disco di origine da utilizzare come base per la creazione del nuovo file può essere scaricata dal server Kaspersky Lab o copiata da un'origine locale.

Il file di immagine creato mediante la procedura guidata verrà salvato nella cartella "*Documents and Settings\All Users\Dati applicazioni\Kaspersky Lab\AVP80\Data\Rdisk*" o "*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk*" per Microsoft Vista e verrà denominato *rescuecd.iso*. Se la procedura guidata rileva un file ISO creato in precedenza nella cartella specificata, è possibile utilizzarlo come immagine del disco originale selezionando la casella ☒ **Usa immagine esistente** e andare al passaggio 3 in cui viene eseguito l'aggiornamento dell'immagine (vedere pagina [92](#)). Se la procedura guidata non rileva alcun file di immagine, questa casella non sarà disponibile.

Il Disco di Ripristino viene creato con una procedura guidata composta da una serie di caselle (passaggi). È possibile selezionare le diverse caselle con i pulsanti **Indietro** e **Avanti**; per completare la procedura guidata, cliccare sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

DESCRIZIONE DETTAGLIATA DEI PASSAGGI DELLA PROCEDURA GUIDATA

Passaggio 1. Selezione dell'origine dell'immagine del disco	92
Passaggio 2. Copia dell'immagine ISO	92
Passaggio 3. Aggiornamento dell'immagine ISO.....	92
Passaggio 4. Avvio remoto.....	93
Passaggio 5. Chiusura della procedura guidata	93

PASSAGGIO 1. SELEZIONE DELL'ORIGINE DELL'IMMAGINE DEL DISCO

Se è stata selezionata la casella ☒ **Usa file ISO esistente** nella finestra della procedura guidata precedente, questo passaggio verrà ignorato.

Durante questo passaggio, è necessario selezionare l'origine del file di immagine nell'elenco di opzioni:

- Selezionare  **Copiare l'immagine ISO da un CD/DVD o dalla rete locale** se si dispone già di un Disco di Ripristino su CD/DVD o di un'immagine preparata per il disco e memorizzata nel computer o in una risorsa di rete locale.
- Selezionare l'opzione  **Scaricare l'immagine ISO dal server Kaspersky Lab** se non si dispone di un file di immagine esistente. Questa opzione consente di scaricare il file dal server Kaspersky Lab (la dimensione del file è di circa 100 MB).

PASSAGGIO 2. COPIA DELL'IMMAGINE ISO

Se nel passaggio precedente è stata selezionata l'opzione di copia dell'immagine da un'origine locale, ovvero  **Copiare l'immagine ISO dal CD/DVD o dalla rete locale**, è necessario specificare il percorso dell'immagine nel passaggio corrente. A questo scopo, utilizzare il pulsante **Sfogli**. Verrà quindi visualizzato lo stato di avanzamento della copia.

Se è stata selezionata l'opzione  **Scaricare l'immagine ISO dal server Kaspersky Lab**, lo stato di avanzamento del download del file verrà visualizzato immediatamente.

PASSAGGIO 3. AGGIORNAMENTO DELL'IMMAGINE ISO

La procedura di aggiornamento dei file include:

- aggiornamento dei database dell'applicazione;
- aggiornamento dei file di configurazione.

I file di configurazione determinano le modalità di utilizzo del Disco di Ripristino: su un computer locale o remoto; pertanto, è necessario selezionare un'opzione prima di aggiornare il file ISO:

-  **Avvio remoto** se si intende caricare un computer remoto.

Se è selezionato l'avvio di un computer remoto, questo deve supportare la tecnologia Intel® vPro™ o Intel® Active Management.

Se l'accesso a Internet da un computer remoto viene garantito da un proxy, non sarà possibile eseguire

l'aggiornamento mediante il Disco di Ripristino. In tal caso, si consiglia di aggiornare prima Kaspersky Anti-Virus.

-  **Avvio dal disco CD/DVD** se l'immagine del disco creata è destinata ad essere registrata su un CD/DVD.

Una volta selezionata l'opzione, cliccare sul bottone **Avanti**. Nella finestra successiva della procedura guidata verrà visualizzato lo stato di avanzamento dell'aggiornamento.

Se è stata selezionata l'opzione **Avvio remoto**, non sarà possibile utilizzare l'immagine creata né per masterizzare un CD/DVD, né per caricare il computer. Per caricare il computer da un CD/DVD, è necessario avviare di nuovo la procedura guidata e selezionare l'opzione **Avvio dal disco CD/DVD** durante questo passaggio.

PASSAGGIO 4. AVVIO REMOTO

Questo passaggio della procedura guidata viene visualizzato solo se è stata selezionata l'opzione  **Avvio remoto** durante il passaggio precedente.

Immettere le informazioni sul computer:

- **Indirizzo IP o nome computer** sulla rete;
- I dati dell'account utente con diritti di amministratore del sistema: **Nome utente** e **Password**.

La finestra successiva della procedura guidata è una console iAMT in cui è possibile controllare il processo di caricamento del computer (vedere pagina [93](#)).

PASSAGGIO 5. CHIUSURA DELLA PROCEDURA GUIDATA

In questa finestra della procedura guidata viene visualizzato un messaggio che indica che un Disco di Ripristino è stato creato correttamente.

AVVIO DEL COMPUTER ATTRAVERSO IL DISCO DI RIPRISTINO

Se non è possibile eseguire l'avvio del sistema operativo a causa dell'attacco di un virus, utilizzare il Disco di Ripristino.

Per caricare il sistema operativo, sarà necessario il file di immagine del disco di avvio (con estensione iso). È possibile scaricare (vedere pagina [92](#)) il file da un server di Kaspersky Lab oppure aggiornare (vedere pagina [92](#)) quello esistente.

Di seguito viene illustrato in modo dettagliato il funzionamento del Disco di Ripristino. Durante il caricamento del disco, vengono eseguite le operazioni seguenti:

1. Rilevamento automatico dell'hardware del computer.
2. Ricerca dei file system nei dischi rigidi. Ai file system rilevati verranno assegnati nomi che iniziano con "C".

È possibile che ai dischi rigidi e ai dispositivi rimovibili vengano assegnati nomi che non corrispondono a quelli assegnati dal sistema operativo.

Se il sistema operativo del computer caricato è in modalità di sospensione o se il relativo file system presenta lo stato *infecto* a causa di una chiusura non corretta, l'utente potrà scegliere se installare il file system o riavviare il computer.

L'installazione del file system potrebbe comportarne il danneggiamento.

3. Ricerca del file swap di Microsoft Windows *pagefile.sys*. Se tale file è assente, il volume della memoria virtuale sarà limitato dalla dimensione della RAM.
4. Selezione della lingua di localizzazione. Se la selezione non viene effettuata dopo un determinato intervallo di tempo, per impostazione predefinita verrà impostata la lingua inglese.

Quando si carica un computer remoto, tale passaggio viene ignorato.

5. Ricerca (creazione) nelle cartelle di database anti-virus, rapporti, memoria di quarantena e file aggiuntivi. Per impostazione predefinita, verranno utilizzate le cartelle dell'applicazione di Kaspersky Lab, installate nel computer infetto (*ProgramData/Kaspersky Lab/AVP8* – per Microsoft Windows Vista, *Documents and Settings/All Users/Dati applicazioni/Kaspersky Lab/AVP8* – per le versioni precedenti di Microsoft Windows). Se non è possibile individuare tali cartelle, verrà effettuato il tentativo di crearle. Se non è possibile trovare le cartelle né crearle, la cartella *kl.files* verrà creata in un disco di sistema.
6. Tentativo di configurazione delle connessioni di rete in base ai dati rilevati nei system file del computer di cui è in corso il caricamento.
7. Caricamento di un sottosistema grafico e avvio del Disco di Ripristino di Kaspersky (in caso di caricamento del computer da un CD/DVD).

Se un computer remoto viene caricato nella console iAMT, verrà caricato il prompt dei comandi. È possibile utilizzare i comandi per l'utilizzo del Disco di Ripristino di Kaspersky dalla riga di comando per gestire le attività (vedere pagina [94](#)).

Nella modalità di ripristino del sistema sono disponibili solo le attività di scansione anti-virus e di aggiornamento dei database da un'origine locale, nonché il rollback degli aggiornamenti e la visualizzazione delle statistiche.

► Per caricare il sistema operativo di un computer infetto da un CD/DVD, eseguire le seguenti operazioni:

1. Nelle impostazioni del BIOS, abilitare l'avvio dall'unità CD/DVD-ROM. Per informazioni dettagliate, fare riferimento alla documentazione relativa alla scheda madre installata nel computer.
2. Inserire il CD/DVD con l'immagine del Disco di Ripristino nell'unità CD/DVD di un computer infetto.
3. Riavviare il computer.
4. Le operazioni di avvio successive verranno eseguite in base all'algoritmo descritto prima.

► Per caricare il sistema operativo di un computer remoto, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul pulsante **Disco di Ripristino** per eseguire la creazione guidata del Disco di Ripristino (vedere pagina [91](#)). Seguire le istruzioni della procedura guidata.

È necessario selezionare l'opzione  **Avvio remoto** durante la fase di aggiornamento dell'immagine del disco (vedere pagina [92](#)).

Le operazioni di avvio successive verranno eseguite in base all'algoritmo descritto prima.

UTILIZZO DEL DISCO DI RIPRISTINO DI KASPERSKY DAL PROMPT DEI COMANDI

È possibile utilizzare il Disco di Ripristino di Kaspersky dal prompt dei comandi. In tal caso sono consentite le operazioni seguenti:

- scansione di oggetti selezionati;
- aggiornamento dei database e dei moduli dell'applicazione;
- rollback dell'ultimo aggiornamento
- richiamo della Guida nella sintassi della riga di comando;
- richiamo della Guida nella sintassi dei comandi.

Sintassi della riga di comando:

```
<comando> [impostazioni]
```

È possibile utilizzare i seguenti comandi:

HELP	fornisce indicazioni sulla sintassi dei comandi e sull'elenco dei comandi
SCAN	esegue la scansione anti-virus degli oggetti
UPDATE	aggiorna l'avvio dell'attività
ROLLBACK	ultimo rollback di aggiornamento
EXIT	consente di uscire dal Disco di Ripristino di Kaspersky

IN QUESTA SEZIONE

Scansione anti-virus	95
Aggiornamento di Kaspersky Anti-Virus	97
Rollback dell'ultimo aggiornamento	97
Visualizzazione della Guida.....	98

SCANSIONE ANTI-VIRUS

L'avvio della scansione anti-virus di una determinata area e l'elaborazione degli oggetti dannosi dalla riga di comando generalmente presenta la sintassi seguente:

```
SCAN [<oggetto esaminato>] [<azione>] [<tipi di file>] [<esclusioni>] [<impostazioni  
rapporto>]
```

Descrizione delle impostazioni:

<oggetto esaminato>: questo parametro fornisce l'elenco di oggetti che verranno esaminati per rilevare eventuale codice dannoso.

Può includere diversi valori dell'elenco fornito separati da spazi.

<file>	Elenco di percorsi dei file e/o delle cartelle da esaminare. È possibile indicare un percorso assoluto o relativo. Gli elementi dell'elenco devono essere separati da uno spazio. Commenti: - Se il nome dell'oggetto contiene uno spazio, esso deve essere incluso tra virgolette. - Se viene fatto riferimento a una directory specifica, verranno esaminati tutti i file in essa contenuti.
/discs/	Scansione di tutte le unità.
/discs/<nome_disco>:/<cartella>	Scansione dell'unità selezionata, in cui <nome_disco> corrisponde al nome dell'unità, mentre <cartella> rappresenta il percorso della cartella da esaminare.
<azione> : questo parametro determina le azioni che verranno eseguite sugli oggetti dannosi rilevati durante la scansione. Se non è definito, l'azione predefinita è quella con il valore -i8.	
-i0	Nessuna azione sull'oggetto; solo registrazione delle informazioni nel rapporto.
-i1	Gli oggetti infetti vengono elaborati e, se la disinfezione è impossibile, vengono ignorati.
-i2	Gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Non vengono eliminati gli oggetti infetti appartenenti a oggetti composti. Per impostazione predefinita, vengono eliminati gli oggetti composti con intestazione eseguibile (archivi .sfx).
-i3	Gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
-i4	Vengono eliminati gli oggetti infetti. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
-i8	Viene richiesto l'intervento dell'utente se viene rilevato un oggetto infetto.
-i9	Viene richiesto l'intervento dell'utente al termine della scansione.
<tipi file> : questo parametro definisce i tipi di file che saranno sottoposti alla scansione anti-virus. Per impostazione predefinita, questo parametro non è specificato e sono sottoposti a scansione solo i file infetti in base al contenuto.	
-fe	Vengono esaminati solo i file infetti in base all'estensione.
-fi	Vengono esaminati solo i file infetti in base al contenuto.
-fa	Vengono esaminati tutti i file.
<esclusioni> : questo parametro definisce gli oggetti esclusi dalla scansione. Può includere diversi valori dell'elenco fornito separati da spazi.	
-e:a	Non vengono esaminati gli archivi.
-e:b	Non vengono esaminati i database della posta.
-e:m	Non vengono esaminati i messaggi di posta con testo semplice.

-e:<mascherafile>	Non vengono esaminati gli oggetti corrispondenti alla maschera.
-e:<secondi>	Vengono ignorati gli oggetti la cui scansione richiede un intervallo di tempo superiore a quello specificato nel parametro <secondi> .
-es:<dimensione>	Vengono ignorati gli oggetti di dimensioni (in MB) superiori a quelle specificate nel parametro <dimensione> .

Esempi:

➡ *Avvio della scansione della cartella Documents and Settings e dell'unità <D>:*

```
SCAN /discs/D: "/discs/C:/Documents and Settings"
```

AGGIORNAMENTO DI KASPERSKY ANTI-VIRUS

La sintassi del comando per l'aggiornamento dei database e dei moduli del programma di Kaspersky Anti-Virus è la seguente:

```
UPDATE [<origine_aggiornamenti>] [-R[A]:<file_rapporto>]
```

Descrizione delle impostazioni:

<sorgente_aggiornamenti>	Server HTTP o FTP o cartella di rete per il download degli aggiornamenti. Il valore dell'impostazione può essere nel formato di un percorso completo di un URL o di un'origine degli aggiornamenti. Se non si seleziona il percorso, l'origine degli aggiornamenti verrà desunta dalle impostazioni del servizio di aggiornamento di Kaspersky Anti-Virus.
-R[A]:<file_rapporti>	-R:<file_rapporti>: registra solo eventi importanti nel rapporto. -RA:<file_rapporti>: registra tutti gli eventi nel rapporto. È possibile utilizzare un percorso assoluto al file. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

Esempi:

➡ *Aggiornamento dei database e registrazione di tutti gli eventi in un rapporto:*

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

Sintassi del comando:

```
ROLLBACK [-R[A]:<file_rapporti>]
```

Descrizione delle impostazioni:

-R[A]:<file_rapporti>	-R:<file_rapporti>: registra solo eventi importanti nel rapporto. -RA:<file_rapporti>: registra tutti gli eventi nel rapporto. È possibile utilizzare un percorso assoluto al file. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.
------------------------------------	---

Esempio:

```
ROLLBACK -RA:/discs/C:/rollback.txt
```

VISUALIZZAZIONE DELLA GUIDA

Questo comando consente di visualizzare la sintassi della riga di comando dell'applicazione:

```
[ -? | HELP ]
```

Per visualizzare la Guida per la sintassi di un comando specifico, è possibile utilizzare uno dei comandi seguenti:

```
<comando> -?
```

```
HELP <comando>
```

VERIFICA DEL FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS

Dopo aver installato e configurato Kaspersky Anti-Virus, è possibile verificare la correttezza della configurazione tramite un virus di "prova" e le sue varianti. Per ciascun protocollo / componente di protezione è necessario eseguire un test separato.

IN QUESTA SEZIONE

"Virus" di prova EICAR e sue varianti.....	99
Verifica del funzionamento di Anti-Virus File	100
Verifica del funzionamento dell'attività di scansione anti-virus	101

"VIRUS" DI PROVA EICAR E SUE VARIANTI

Questo "virus" di prova è stato progettato specificamente da **eicar** (European Institute for Computer Antivirus Research) per il collaudo dei prodotti anti-virus.

Il "virus" di prova NON È UN VIRUS, poiché non contiene codice in grado di danneggiare il computer. Tuttavia, la maggior parte dei prodotti anti-virus lo identifica come tale.

Si raccomanda di non utilizzare mai virus autentici per verificare il corretto funzionamento di un programma anti-virus.

È possibile scaricare il "virus" di prova dal sito Web ufficiale di **EICAR** all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.

Prima di scaricare il file, è necessario disabilitare la protezione anti-virus del computer perché altrimenti l'applicazione identificherà ed elaborerà il file *anti_virus_test_file.htm* come oggetto infetto trasferito tramite il protocollo HTTP. Riattivare la protezione anti-virus subito dopo aver scaricato il "virus" di prova.

L'applicazione identifica il file scaricato dal sito **EICAR** come oggetto infetto contenente un virus che **non può essere disinfettato** ed esegue le azioni specificate per questo tipo di oggetto.

È possibile inoltre utilizzare varianti del "virus" di prova standard per verificare il funzionamento dell'applicazione. A tal fine, modificare il contenuto del "virus" standard aggiungendo uno dei prefissi elencati nella tabella di seguito. Per modificare il "virus" di prova, è possibile utilizzare qualsiasi editor di testo o di ipertesto, ad esempio **Blocco note Microsoft**, **UltraEdit32** e così via.

È possibile verificare il corretto funzionamento dell'applicazione anti-virus tramite il "virus" modificato EICAR solo se i database anti-virus sono aggiornati almeno al 24 ottobre 2003 (Ottobre 2003, aggiornamenti cumulativi).

Nella tabella seguente la prima colonna contiene i prefissi che devono essere aggiunti all'inizio della stringa del "virus" di prova standard. La seconda colonna elenca tutti i valori possibili dello stato che l'applicazione Anti-Virus può assegnare all'oggetto in base ai risultati della scansione. La terza colonna indica come vengono elaborati gli oggetti che presentano lo stato specificato. Si noti che le azioni eseguite sugli oggetti sono determinate dalle impostazioni dell'applicazione.

Dopo aver aggiunto un prefisso al "virus" di prova, salvare il nuovo file con un nome diverso, ad esempio: *ecar_dele.com*. Assegnare nomi simili a tutti i "virus" modificati.

Table 1. Varianti del "virus" di prova

Prefisso	Stato dell'oggetto	Informazioni di elaborazione dell'oggetto
Nessun prefisso, "virus" di prova standard.	Infetto. L'oggetto contiene codice di un virus noto e non può essere disinfettato.	L'applicazione identifica l'oggetto come virus non disinfettabile. Si verifica un errore nel tentativo di disinfettare l'oggetto; verrà eseguita l'azione specificata per gli oggetti non disinfettabili.
CORR–	Danneggiato.	L'applicazione ha potuto accedere all'oggetto ma non ha potuto esaminarlo, poiché l'oggetto è danneggiato, ad esempio la struttura del file è danneggiata o il formato file non è valido. Informazioni sull'elaborazione dell'oggetto sono disponibili nel rapporto sul funzionamento dell'applicazione.
WARN–	Sospetto. L'oggetto contiene codice di un virus sconosciuto e non può essere disinfettato.	L'oggetto è stato ritenuto sospetto dall'analizzatore euristico di codice. Al momento del rilevamento, i database delle firme delle minacce dell'Anti-Virus non contengono alcuna descrizione della procedura per il trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.
SUSP–	Sospetto. L'oggetto contiene codice modificato di un virus noto e non può essere disinfettato.	L'applicazione ha rilevato una corrispondenza parziale tra una sezione di codice dell'oggetto e una sezione di codice di un virus noto. Al momento del rilevamento, i database delle firme delle minacce dell'Anti-Virus non contengono alcuna descrizione della procedura per il trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.
ERRO–	Errore di scansione.	Si è verificato un errore durante la scansione di un oggetto. L'applicazione non ha potuto eseguire l'accesso all'oggetto, in quanto l'integrità dell'oggetto è stata compromessa, ad esempio a causa di un archivio in più volumi, o non è stata stabilita una connessione a esso, ad esempio se l'oggetto viene esaminato in una risorsa di rete. Informazioni sull'elaborazione dell'oggetto sono disponibili nel rapporto sul funzionamento dell'applicazione.
CURE–	Infetto. L'oggetto contiene codice di un virus noto disinfettato.	L'oggetto contiene un virus che può essere disinfettato. L'applicazione disinfetterà l'oggetto; il testo del corpo del "virus" verrà sostituito dalla parola CURE. Il rilevamento di un oggetto di questo tipo viene notificato.
DELE–	Infetto. L'oggetto contiene codice di un virus noto e non può essere disinfettato.	L'applicazione identifica l'oggetto come virus non disinfettabile. Si verifica un errore nel tentativo di disinfettare l'oggetto; verrà eseguita l'azione specificata per gli oggetti non disinfettabili. Il rilevamento di un oggetto di questo tipo viene notificato.

VERIFICA DEL FUNZIONAMENTO DI ANTI-VIRUS FILE

➡ Per verificare che Anti-Virus File sia configurato correttamente, eseguire le seguenti operazioni:

1. Creare una cartella su un disco, copiare al suo interno il "virus" di prova scaricato dal sito Web ufficiale di EICAR all'indirizzo (http://www.eicar.org/anti_virus_test_file.htm), nonché tutte le varianti create.
2. Lasciare che tutti gli eventi vengano registrati, in modo che il file del rapporto conservi i dati sugli oggetti danneggiati o su quelli non esaminati a causa di errori.
3. Eseguire il virus "di prova" o una delle relative versioni modificate.

Anti-Virus File intercetta il tentativo di eseguire il file, lo esamina ed esegue l'azione specificata nelle impostazioni per gli oggetti che presentano quello stato. Selezionando diverse azioni da eseguire sull'oggetto rilevato, è possibile effettuare un controllo completo del funzionamento del componente.

Il rapporto sul funzionamento del componente include informazioni sui risultati dell'operazione eseguita da Anti-Virus File.

VERIFICA DEL FUNZIONAMENTO DELL'ATTIVITÀ DI SCANSIONE ANTI-VIRUS

➡ *Per verificare che l'attività di scansione anti-virus funzioni correttamente:*

1. Creare una cartella su un disco, copiare al suo interno il "virus" di prova scaricato dal sito Web ufficiale di EICAR all'indirizzo (http://www.eicar.org/anti_virus_test_file.htm), nonché tutte le varianti create.
2. Creare una nuova attività di scansione anti-virus e selezionare la cartella contenente il gruppo di "virus" di prova come oggetto da esaminare.
3. Lasciare che tutti gli eventi vengano registrati, in modo che il file del rapporto conservi i dati sugli oggetti danneggiati e su quelli non esaminati a causa di errori.
4. Eseguire l'attività di scansione anti-virus.

Quando l'attività di scansione è in esecuzione, le azioni specificate nelle impostazioni verranno eseguite al rilevamento di oggetti infetti o sospetti. Selezionando diverse azioni da eseguire sull'oggetto rilevato, è possibile effettuare un controllo completo del funzionamento del componente.

È possibile visualizzare tutte le informazioni sulle azioni dell'attività di scansione anti-virus nel rapporto sul funzionamento del componente.

TIPI DI NOTIFICHE

Quando si verificano eventi di Kaspersky Anti-Virus, vengono visualizzati messaggi di notifica speciali. A seconda della criticità dell'evento per la protezione del computer, potrebbero essere visualizzati i tipi di notifica seguenti:

- **Allarme.** Si è verificato un evento critico, ad esempio è stato rilevato un oggetto dannoso o un'attività pericolosa nel sistema. È necessario decidere subito come affrontare la minaccia. Questo tipo di notifica è visualizzata in rosso.
- **Attenzione.** Si è verificato un evento potenzialmente pericoloso. Ad esempio, nel sistema sono stati rilevati file potenzialmente infetti o un'attività sospetta. È necessario stabilire quanto è pericoloso l'evento in questione. Questo tipo di notifica è visualizzata in giallo.
- **Informazioni.** Questa notifica fornisce informazioni su eventi non critici. Le notifiche informative sono visualizzate in blu.

IN QUESTA SEZIONE

Rilevamento di un oggetto dannoso	102
Impossibile disinfettare l'oggetto	103
Rilevamento di un oggetto sospetto	103

RILEVAMENTO DI UN OGGETTO DANNOSO

Se Anti-Virus File o una scansione anti-virus rileva un codice dannoso, viene visualizzata una notifica speciale.

La notifica contiene le informazioni seguenti:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nella Virus Encyclopedia di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Disinfetta:** viene eseguito un tentativo di disinfezione dell'oggetto dannoso. Prima del trattamento, viene eseguita una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Elimina:** l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Salta:** l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di un'attività di scansione anti-virus fino al relativo completamento.

IMPOSSIBILE DISINFETTARE L'OGGETTO

In alcuni casi può risultare impossibile disinfettare un oggetto dannoso. Questo può succedere se un file è talmente danneggiato che diventa impossibile eliminarne il codice dannoso e ripristinarne l'integrità. La procedura di disinfezione di questi casi non può essere eseguita su diversi tipi di oggetti pericolosi, ad esempio i Trojan.

In queste situazioni verrà visualizzata una notifica speciale con le informazioni seguenti:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nella Virus Encyclopedia di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Elimina:** l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Salta:** l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di un'attività di scansione anti-virus fino al relativo completamento.

RILEVAMENTO DI UN OGGETTO SOSPETTO

Se Anti-Virus File o una scansione anti-virus rilevano un oggetto contenente il codice di un virus sconosciuto o il codice modificato di un virus noto, viene visualizzata una notifica speciale.

La notifica contiene le informazioni seguenti:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto così come è elencato nella Virus Encyclopedia di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Quarantena:** l'oggetto viene messo in quarantena. Quando un oggetto viene messo in Quarantena, viene spostato, non copiato. Esso viene eliminato dal disco o dalla posta elettronica e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

Successivamente, quando si esegue la scansione della cartella Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

- **Elimina:** l'oggetto viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Salta:** l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

Successivamente sarà possibile tornare agli oggetti ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☒ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di un'attività di scansione anti-virus fino al relativo completamento.

Se si è certi che l'oggetto rilevato non sia dannoso, si consiglia di aggiungerlo alla zona attendibile per evitare che l'applicazione rilevi falsi positivi ripetuti durante l'utilizzo dell'oggetto.

UTILIZZO DELL'APPLICAZIONE DALLA RIGA DI COMANDO

Kaspersky Anti-Virus può essere utilizzato anche dalla riga di comando.

Sintassi della riga di comando:

```
avp.com <comando> [opzioni]
```

È necessario accedere all'applicazione dalla riga di comando dalla cartella di installazione Kaspersky Anti-Virus o specificando il percorso completo di avp.com.

È possibile utilizzare i seguenti comandi come <comando>:

- **HELP** – per indicazioni sulla sintassi dei comandi e sull'elenco dei comandi.
- **SCAN** – per la ricerca di malware negli oggetti.
- **UPDATE** – per avviare l'aggiornamento dell'applicazione.
- **ROLLBACK** – esegue il rollback dell'ultimo aggiornamento di Kaspersky Anti-Virus (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione).
- **START** – per avviare un componente o un'attività.
- **STOP** – per interrompere un componente o un'attività (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia di Kaspersky Anti-Virus).
- **STATUS** – per visualizzare lo stato del componente o dell'attività corrente.
- **STATISTICS** – per visualizzare le statistiche del componente o dell'attività corrente.
- **EXPORT** – per esportare le impostazioni di protezione dell'applicazione.
- **IMPORT** – per importare le impostazioni di protezione di un componente o un'attività (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia di Kaspersky Anti-Virus).
- **ACTIVATE** – per attivare Kaspersky Anti-Virus via Internet utilizzando il codice di attivazione.
- **ADDKEY** – per attivare l'applicazione utilizzando un file di chiave (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione).
- **RESTORE** – per ripristinare un file dalla quarantena.
- **EXIT** – per chiudere l'applicazione (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione).
- **TRACE** – per ottenere un file di traccia.

Ogni comando richiede un insieme specifico di parametri.

IN QUESTA SEZIONE

Visualizzazione della Guida.....	106
Scansione anti-virus	106
Aggiornamento dell'applicazione	108
Rollback dell'ultimo aggiornamento	109
Avvio / interruzione delle operazioni di Anti-Virus File o di un'attività	109
Statistiche sul funzionamento di un componente o di un'attività	110
Esportazione delle impostazioni di protezione.....	111
Importazione delle impostazioni di protezione.....	111
Attivazione dell'applicazione.....	111
Ripristino di un file dalla quarantena	112
Chiusura dell'applicazione.....	112
Come ottenere un file di traccia.....	112
Codici restituiti della riga di comando	113

VISUALIZZAZIONE DELLA GUIDA

Questo comando consente di visualizzare la sintassi della riga di comando dell'applicazione:

```
avp.com [ /? | HELP ]
```

Per visualizzare la Guida per la sintassi di un comando specifico, è possibile utilizzare uno dei comandi seguenti:

```
avp.com <comando> /?
```

```
avp.com HELP <comando>
```

SCANSIONE ANTI-VIRUS

L'avvio della scansione anti-virus di una determinata area e l'elaborazione degli oggetti dannosi dalla riga di comando generalmente presenta la sintassi seguente:

```
avp.com SCAN [<oggetto esaminato>] [<azione>] [<tipi file>] [<esclusioni>]
[<impostazioni rapporti>] [<impostazioni avanzate>]
```

Per esaminare gli oggetti, è inoltre possibile utilizzare le attività create nell'applicazione avviando quella richiesta dalla riga di comando. L'attività viene eseguita con le impostazioni specificate nell'interfaccia di Kaspersky Anti-Virus.

Descrizione delle impostazioni:

<oggetto esaminato>: questo parametro fornisce l'elenco di oggetti che verranno esaminati per rilevare eventuale codice dannoso. Può includere diversi valori dell'elenco fornito separati da spazi:

- **<file>** – elenco di percorsi dei file e/o delle cartelle da esaminare. È possibile indicare un percorso assoluto o relativo. Gli elementi dell'elenco devono essere separati da uno spazio. Commenti:
 - se il nome dell'oggetto contiene uno spazio, deve essere incluso tra virgolette;
 - se viene fatto riferimento a una cartella specifica, verranno esaminati tutti i file in essa contenuti.
- **/ALL** – scansione completa del computer.
- **/MEMORY** – oggetti della RAM.
- **/STARTUP** – oggetti di avvio.
- **/MAIL** – database di posta elettronica.
- **/REMDRIVES** – tutte le unità rimovibili.
- **/FIXDRIVES** – tutte le unità locali.
- **/NETDRIVES** – tutte le unità di rete.
- **/QUARANTINE** – oggetti in quarantena.
- **/@:<filelist.lst>** – percorso del file contenente un elenco di oggetti e cataloghi da esaminare. Il file deve essere in formato testo e ogni oggetto della scansione deve essere elencato in una riga separata. È possibile indicare un percorso assoluto o relativo. Il percorso deve essere inserito tra virgolette anche se contiene spazi.

<azione>: questo parametro determina le azioni che verranno eseguite sugli oggetti dannosi rilevati durante la scansione. Se non è definito, l'azione predefinita è quella con il valore **/i2**. Sono possibili i valori seguenti:

- **/i0** – nessuna azione sull'oggetto; solo registrazione delle informazioni nel rapporto.
- **/i1** – gli oggetti infetti vengono elaborati e, se la disinfezione è impossibile, vengono ignorati.
- **/i2** – gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Non vengono eliminati gli oggetti infetti appartenenti a oggetti composti. Vengono eliminati gli oggetti composti con intestazione eseguibile (archivi .sfx). Per impostazione predefinita.
- **/i3** – gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
- **/i4** – gli oggetti infetti vengono eliminati. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
- **/i8** – viene richiesto l'intervento dell'utente se viene rilevato un oggetto infetto.
- **/i9** – viene richiesto l'intervento dell'utente al termine della scansione.

<tipi file>: questo parametro definisce i tipi di file che saranno sottoposti alla scansione anti-virus. Per impostazione predefinita, questo parametro non è specificato e sono sottoposti a scansione solo i file infetti in base al contenuto. Sono possibili i valori seguenti:

- **/fe** – vengono esaminati solo i file infetti in base all'estensione.
- **/fi** – vengono esaminati solo i file infetti in base al contenuto.
- **/fa** – vengono esaminati tutti i file.

<esclusioni>: questo parametro definisce gli oggetti esclusi dalla scansione. Può includere diversi valori dell'elenco fornito separati da spazi.

- **/e:a** – non vengono esaminati gli archivi.
- **/e:b** – non vengono esaminati i database di posta elettronica.
- **/e:m** – non vengono esaminati i messaggi di posta con testo semplice.
- **/e:<maschera>** – non vengono esaminati gli oggetti corrispondenti alla maschera.
- **/e:<secondi>** – vengono ignorati gli oggetti la cui scansione richiede un intervallo di tempo superiore a quello specificato nel parametro **<secondi>**.

<impostazioni rapporti>: questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi.

<impostazioni avanzate> – impostazioni che definiscono l'utilizzo delle tecnologie di scansione anti-virus e del file di configurazione delle impostazioni:

- **/iChecker=<abilitato|disabilitato>** – viene abilitato/disabilitato l'utilizzo della tecnologia iChecker.
- **/iSwift=<abilitato|disabilitato>** – viene abilitato/disabilitato l'utilizzo della tecnologia /iSwift.
- **/C:<nome_file_configurazione>** – definisce il percorso del file di configurazione che contiene le impostazioni di scansione dell'applicazione. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia dell'applicazione.

Esempi:

- *Avviare una scansione di memoria, oggetti di avvio, database di posta elettronica, directory Documenti e Programmi e file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\Documenti"
"C:\Programmi" "C:\Downloads\test.exe"
```

- *Scansione degli oggetti elencati nel file object2scan.txt mediante il file di configurazione scan_setting.txt per l'operazione. Utilizzo del file di configurazione scan_setting.txt. Al termine della scansione, creare un rapporto per registrare tutti gli eventi:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

File di configurazione di esempio:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

AGGIORNAMENTO DELL'APPLICAZIONE

La sintassi per l'aggiornamento dei moduli e dei database di Kaspersky Anti-Virus dalla riga di comando è la seguente:

```
avp.com UPDATE [<sorgente_aggiornamento>] [/APP=<abilitato|disabilitato>]
[<impostazioni_rapporti>] [<impostazioni_avanzate>]
```

Descrizione delle impostazioni:

<sorgente_aggiornamento> – server HTTP o FTP o cartella di rete per il download degli aggiornamenti. Se non viene selezionato un percorso, la sorgente degli aggiornamenti sarà quella delle impostazioni di aggiornamento dell'applicazione.

/APP=<abilitato|disabilitato> – abilita / disabilita l'aggiornamento dei moduli dell'applicazione.

<impostazioni rapporti>: questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi. Sono possibili i valori seguenti:

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi.

<impostazioni avanzate> – impostazioni che definiscono l'utilizzo delle tecnologie di scansione anti-virus.

/C:<nome_file_configurazione> – definisce il percorso del file di configurazione che contiene le impostazioni di scansione dell'applicazione. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia dell'applicazione.

Esempi:

➡ *aggiornamento dei database dell'applicazione e registrazione di tutti gli eventi in un rapporto:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➡ *Aggiornamento dei moduli di Kaspersky Anti-Virus mediante i parametri del file di configurazione updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

Sintassi del comando:

```
avp.com ROLLBACK </password=<password>> [<impostazioni_rapporto>]
```

Descrizione delle impostazioni:

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione. Il comando ROLLBACK non verrà eseguito senza l'immissione di una password.

<impostazioni rapporti> – questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

Esempio:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

AVVIO / INTERRUZIONE DELLE OPERAZIONI DI ANTI-VIRUS FILE O DI UN'ATTIVITÀ

Sintassi del comando START:

```
avp.com START <profilo|nome_attività> [<impostazioni_rapporto>]
```

Sintassi del comando STOP:

```
avp.com STOP <profilo|nome_attività> </password=<password>>
```

Descrizione delle impostazioni:

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione. Il comando STOP non verrà eseguito senza l'immissione di una password.

<impostazioni rapporti> – questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi. Sono possibili i valori seguenti:

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

L'impostazione **<profilo|nome_attività>** può contenere uno dei valori seguenti:

- **Protection (RTP)** – tutti i computer di protezione;
- **File_Monitoring (FM)** – Anti-Virus File;
- **Scan_My_Computer** – attività di scansione completa del computer;
- **Scan_Objects** – scansione di oggetti;
- **Scan_Quarantine** – scansione della quarantena;
- **Scan_Startup (STARTUP)** – scansione degli oggetti di avvio;
- **Updater** – attività di aggiornamento;
- **Rollback** – attività di rollback degli aggiornamenti.

I componenti e le attività avviati dalla riga di comando vengono eseguiti con le impostazioni modificate nell'interfaccia dell'applicazione.

Esempi:

➡ *Per abilitare Anti-Virus File, digitare quanto segue nel prompt dei comandi:*

```
avp.com START FM
```

➡ *Per arrestare l'attività di scansione dal prompt dei comandi, immettere:*

```
avp.com STOP SCAN_MY_COMPUTER /password=<password_utente>
```

STATISTICHE SUL FUNZIONAMENTO DI UN COMPONENTE O DI UN'ATTIVITÀ

Sintassi del comando STATUS:

```
avp.com STATUS <profilo|nome_attività>
```

Sintassi del comando STATISTICS:

```
avp.com STATISTICS <profilo|nome_attività>
```

Descrizione delle impostazioni:

L'impostazione **<profilo|nome_attività>** può contenere uno dei valori specificati nei comandi START / STOP (vedere a pag. [109](#)).

ESPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com EXPORT <profilo|nome_attività> <nome_file>
```

Descrizione delle impostazioni:

L'impostazione **<profilo|nome_attività>** può contenere uno dei valori specificati nei comandi START / STOP (vedere a pag. [109](#)).

<nome_file> – percorso nel quale verranno esportate le impostazioni dell'applicazione. È possibile specificare un percorso assoluto o relativo.

Esempio:

```
avp.com EXPORT RTP RTP_settings.dat - formato binario
avp.com EXPORT FM FM_settings.txt - formato testo
```

IMPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com IMPORT <nome_file> </password=<password_utente>>
```

Descrizione delle impostazioni:

<nome_file> – percorso nel quale verranno importate le impostazioni dell'applicazione. È possibile specificare un percorso assoluto o relativo.

</password=<password_utente>> – password assegnata mediante l'interfaccia dell'applicazione.

Esempio:

```
avp.com IMPORT settings.dat
```

ATTIVAZIONE DELL'APPLICAZIONE

Kaspersky Anti-Virus può essere attivato in due modi:

- tramite Internet utilizzando un codice di attivazione (comando ACTIVATE)
- utilizzando un file di chiave della licenza (comando ADDKEY).

Sintassi del comando:

```
avp.com ACTIVATE <codice_attivazione> </password=<password>>
avp.com ADDKEY <nome_file> </password=<password>>
```

Descrizione delle impostazioni:

<codice_attivazione> – il codice di attivazione: xxxxx-xxxxx-xxxxx-xxxxx.

<nome_file> – file di chiave dell'applicazione con estensione .key: xxxxxxxx.key.

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione.

Esempio:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </password=<password>>
```

RIPRISTINO DI UN FILE DALLA QUARANTENA

Sintassi del comando:

```
avp.com RESTORE [/REPLACE] <nome_file>
```

Descrizione delle impostazioni:

/REPLACE – sostituzione di un file esistente.

<nome_file> – nome del file da ripristinare.

Esempio:

```
avp.com REPLACE C:\eicar.com
```

CHIUSURA DELL'APPLICAZIONE

Sintassi del comando:

```
avp.com EXIT </password=<password>>
```

Descrizione delle impostazioni:

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione. Il comando non verrà eseguito senza l'immissione di una password.

COME OTTENERE UN FILE DI TRACCIA

Se si verificano problemi con Kaspersky Anti-Virus, potrebbe essere necessario creare un file di traccia. I file di traccia sono utili per individuare il problema con maggiore precisione e vengono molto utilizzati dagli esperti dell'Assistenza tecnica.

Sintassi del comando:

```
avp.com TRACE [file] [on|off] [<livello_traccia>]
```

Descrizione delle impostazioni:

[abilitato|disabilitato] – abilita / disabilita la creazione del file di traccia.

[file] – copia la traccia in un file.

<livello_traccia> – questo valore può essere un numero intero compreso tra 100 (livello minimo, solo messaggi critici) e 600 (livello massimo, tutti i messaggi).

Se si contatta il servizio di assistenza tecnica, occorre specificare il livello di traccia necessario. Se non viene specificato alcun livello, si consiglia di impostare il valore su 500.

Esempi:

- ➡ *Per disabilitare la creazione del file di traccia:*

```
avp.com TRACE file off
```

- ➡ *Creare un file di traccia con un livello di 500:*

```
avp.com TRACE file on 500
```

CODICI RESTITUITI DELLA RIGA DI COMANDO

I codici generali possono essere restituiti da qualsiasi comando dalla riga di comando. I codici restituiti comprendono i codici generali nonché quelli relativi a un tipo specifico di attività.

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 annullata.

Codici restituiti dall'attività di scansione anti-virus:

- 101 – tutti gli oggetti pericolosi sono stati elaborati;
- 102 – rilevamento di oggetti pericolosi.

MODIFICA, RIPARAZIONE E RIMOZIONE DELL'APPLICAZIONE

L'applicazione può essere disinstallata nei modi seguenti:

- mediante la configurazione guidata dell'applicazione;
- dalla riga di comando (vedere la sezione "Rimozione dell'applicazione dalla riga di comando" a pagina [116](#));
- tramite Kaspersky Administration Kit (vedere la Guida di distribuzione di Kaspersky Administration Kit);
- tramite i criteri di gruppo di dominio di Microsoft Windows Server 2000/2003 (vedere la sezione "Disinstallazione dell'applicazione" a pagina [22](#)).

IN QUESTA SEZIONE

Modifica, riparazione e rimozione dell'applicazione tramite l'installazione guidata [114](#)

Rimozione dell'applicazione dalla riga di comando [116](#)

MODIFICA, RIPARAZIONE E RIMOZIONE DELL'APPLICAZIONE TRAMITE L'INSTALLAZIONE GUIDATA

In caso di errori di funzionamento dovuti a una configurazione errata o alla corruzione dei file può rendersi necessario riparare l'applicazione.

► *Per riparare o modificare i componenti assenti di Kaspersky Anti-Virus o disinstallare l'applicazione, eseguire le operazioni seguenti:*

1. Inserire il CD di installazione nell'unità CD/DVD-ROM se è stata utilizzata per installare l'applicazione. Se Kaspersky Anti-Virus è stato installato da una fonte diversa (cartella ad accesso pubblico, cartella nel disco fisso, ecc.), verificare che il pacchetto di installazione dell'applicazione si trovi nello stesso percorso e di potervi accedere.
2. Selezionare **Start** → **Tutti i programmi** → **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** → **Modifica, Ripara o Rimuovi**.

Si aprirà l'installazione guidata del programma. Di seguito vengono illustrati in modo dettagliato i passaggi della riparazione, modifica o rimozione dell'applicazione.

PASSAGGIO 1. FINESTRA INIZIALE DELL'INSTALLAZIONE

Dopo aver eseguito tutti i passaggi sopra descritti, necessari per riparare o modificare l'applicazione, si apre la finestra iniziale di installazione di Kaspersky Anti-Virus. Fare clic sul pulsante **Avanti** per continuare.

PASSAGGIO 2. SELEZIONE DI UN'OPERAZIONE

In questa fase viene chiesto di selezionare l'operazione che si desidera eseguire sull'applicazione. È possibile modificare i componenti dell'applicazione, riparare quelli già installati, rimuoverne alcuni o l'intera applicazione. Per eseguire

l'operazione desiderata, fare clic sul pulsante corrispondente. Il programma di installazione si comporterà diversamente in base all'operazione selezionata.

La modifica dell'applicazione è analoga all'installazione personalizzata, in cui è possibile specificare quali componenti si desidera installare e quali eliminare.

La riparazione dell'applicazione dipende dai componenti installati. Saranno riparati i file di tutti i componenti installati e per ciascuno di essi sarà impostato il livello di protezione **Consigliato**.

Se la disinstallazione di Kaspersky Anti-Virus 6.0 viene eseguita in remoto, il server non verrà riavviato automaticamente. Tuttavia, per rimuovere i componenti dell'applicazione e garantire un funzionamento corretto del computer in futuro, si consiglia di riavviare il server manualmente.

Quando si rimuove l'applicazione è possibile selezionare quali dati creati e usati dall'applicazione si desidera salvare nel computer. Per eliminare tutti i dati di Kaspersky Anti-Virus, selezionare l'opzione  **Disinstallazione completa**. Per salvare i dati, selezionare l'opzione  **Salva i dati dell'applicazione** e specificare quali oggetti non devono essere eliminati:

- *Informazioni sull'attivazione* – file chiave necessario per il funzionamento dell'applicazione.
- *Database dell'applicazione* – serie completa delle firme di programmi pericolosi, virus e altre minacce correnti alla data dell'ultimo aggiornamento.
- *Backup oggetti* – copie di backup di oggetti eliminati o disinfettati. Si consiglia di salvare questi oggetti per poterli eventualmente ripristinare in un secondo momento.
- *Oggetti in quarantena* – oggetti potenzialmente infetti da virus o varianti di essi. Questi oggetti contengono codici simili a quelli di virus noti ma è difficile stabilire se siano dannosi. Si consiglia di salvare questi oggetti poiché potrebbero rivelarsi innocui oppure essere disinfettati dopo l'aggiornamento delle firme delle minacce.
- *Impostazioni di protezione* – valori delle impostazioni di tutti i componenti dell'applicazione.
- *Dati iSwift* – database contenente informazioni sugli oggetti esaminati nei file system NTFS. Questi dati possono aumentare la velocità di scansione. Usando questo database, Kaspersky Anti-Virus esamina solo i file che hanno subito delle modifiche dopo l'ultima scansione.

Se trascorre molto tempo tra la disinstallazione di una versione di Kaspersky Anti-Virus e l'installazione di un'altra, si sconsiglia di utilizzare il database iSwift creato da un'installazione precedente dell'applicazione. Un programma dannoso potrebbe infatti 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**. L'applicazione inizierà a copiare i file necessari nel computer o a eliminare i componenti e i dati selezionati.

PASSAGGIO 3. COMPLETAMENTO DELLA MODIFICA, RIPARAZIONE O RIMOZIONE DELL'APPLICAZIONE

L'avanzamento del processo di modifica, riparazione o rimozione dell'applicazione viene visualizzato 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. L'applicazione chiederà quindi se si desidera riavviare il computer. Fare clic sul pulsante **Sì** per riavviarlo subito. Per riavviarlo in un secondo momento, fare clic sul pulsante **No**.

RIMOZIONE DELL'APPLICAZIONE DALLA RIGA DI COMANDO

- *Per disinstallare Kaspersky Anti-Virus 6.0 for Windows Servers MP4 dalla riga di comando, eseguire quanto indicato di seguito:*

```
msiexec /x <package_name>
```

Si aprirà l'installazione guidata, che consente di disinstallare l'applicazione.

- *Per disinstallare l'applicazione in modalità non interattiva senza riavviare il computer (il computer dovrà essere riavviato manualmente dopo la disinstallazione), digitare:*

```
msiexec /x <package_name> /qn
```

- *Per disinstallare l'applicazione in modalità non interattiva e riavviare il computer al termine dell'operazione, digitare:*

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

Se durante l'installazione dell'applicazione si è scelto di proteggerla dalla disinstallazione tramite una password, è necessario confermare tale password quando la si disinstalla. In caso contrario, sarà impossibile disinstallare l'applicazione.

- *Per rimuovere l'applicazione quando è protetta da una password, digitare:*

```
msiexec /x <nome_pacchetto> KLUNINSTPASSWD=***** – per rimuovere l'applicazione in modalità interattiva;
```

```
msiexec /x <package_name> KLUNINSTPASSWD=***** /qn – per rimuovere l'applicazione in modalità non interattiva.
```

GESTIONE DELL'APPLICAZIONE TRAMITE KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit è un sistema che consente di centralizzare la gestione delle principali attività amministrative utilizzate in un sistema di protezione per una rete aziendale, basato sulle applicazioni incluse in Kaspersky Anti-Virus Open Space Security. Kaspersky Administration Kit supporta tutte le configurazioni di rete basate sul protocollo TCP/IP.

L'applicazione è destinata agli amministratori di reti aziendali e ai dipendenti responsabili della protezione anti-virus nelle rispettive aziende.

Kaspersky Anti-Virus 6.0 for Windows Servers MP4 è uno dei prodotti Kaspersky Lab che può essere gestito tramite l'interfaccia dell'applicazione, il prompt dei comandi (questi metodi sono descritti nella presente documentazione) o utilizzando il programma Kaspersky Administration Kit (se il computer è incluso in un sistema di amministrazione remota centralizzato).

Per gestire Kaspersky Anti-Virus tramite Kaspersky Administration Kit, eseguire le seguenti operazioni:

- distribuire il *server di amministrazione* nella rete;
- installare la *console di amministrazione* nella workstation dell'amministratore (per ulteriori informazioni consultare il manuale di distribuzione di Kaspersky Administration Kit);
- installare Kaspersky Anti-Virus e *Network Agent* (fornito con Kaspersky Administration Kit) nei computer della rete. Per ulteriori informazioni sull'installazione remota del pacchetto di installazione di Kaspersky Anti-Virus nei computer in rete, consultare il manuale per la distribuzione di Kaspersky Administration Kit.

Prima di aggiornare il plug-in di amministrazione di Kaspersky Anti-virus tramite Kaspersky Administration Kit, chiudere la console di amministrazione.

La console di amministrazione (vedere la figura seguente) consente di gestire l'applicazione tramite Kaspersky Administration Kit. Costituisce un'interfaccia standard integrata in MMC e consente all'amministratore di eseguire le funzioni seguenti:

- Installazione e disinstallazione remota di Kaspersky Anti-Virus e di *Network Agent* nei computer della rete;
- Configurazione remota di Kaspersky Anti-Virus nei computer della rete;
- Aggiornamento dei database e moduli di Kaspersky Anti-Virus;
- Gestione delle licenze per Kaspersky Anti-Virus nei computer della rete;
- Visualizzazione di informazioni sul funzionamento dell'applicazione nei computer client.



Fig. 11. La console di amministrazione di Kaspersky Administration Kit.

L'aspetto della finestra principale del Kaspersky Administration Kit varia in relazione al sistema operativo del computer in uso.

Quando si utilizza Kaspersky Administration Kit, l'applicazione viene gestita tramite le impostazioni dei criteri, delle attività e dell'applicazione definite dall'amministratore.

Le azioni eseguite dall'applicazione vengono definite *attività*. In base alle funzioni che eseguono, le attività si suddividono in *tipi*: attività di scansione anti-virus, attività di aggiornamento dell'applicazione, rollback degli aggiornamenti e attività di installazione del file di chiave.

Ogni attività prevede una serie di impostazioni per l'applicazione che vengono utilizzate quando viene eseguita. Le impostazioni dell'attività per l'applicazione che sono comuni a tutti i tipi di attività sono definiti *impostazioni dell'applicazione*. Le impostazioni dell'applicazione che sono specifiche per un tipo di attività costituiscono le *impostazioni dell'attività*. Le impostazioni dell'applicazione e le impostazioni di attività non si sovrappongono.

La funzione chiave dell'amministrazione centralizzata consiste nel raggruppare computer remoti nella rete e gestirli creando e configurando criteri di gruppo.

Un *criterio* è una serie di impostazioni dell'applicazione per un gruppo, nonché una serie di restrizioni alla modifica di tali impostazioni durante la configurazione dell'applicazione o delle attività in un singolo computer client. Un criterio include impostazioni per la configurazione di tutte le funzioni, dell'applicazione ad eccezione delle impostazioni personalizzate per istanze specifiche di un'attività. ad esempio le impostazioni di pianificazione.

Di conseguenza, i criteri includono le seguenti impostazioni:

- Impostazioni comuni a tutte le attività (impostazioni dell'applicazione);
- Impostazioni comuni a tutte le istanze di un singolo tipo di attività (impostazioni principali di un'attività).

Di conseguenza, un criterio per Kaspersky Anti-Virus, le cui attività includono la protezione e la scansione anti-virus, include tutte le impostazioni necessarie per configurare l'applicazione quando si eseguono entrambi i tipi di attività, ma non include, ad esempio, una pianificazione per l'esecuzione di tali attività o le impostazioni che definiscono l'ambito della scansione.

IN QUESTA SEZIONE

Gestione dell'applicazione	120
Gestione delle attività	125
Gestione dei criteri.....	130

GESTIONE DELL'APPLICAZIONE

Kaspersky Administration Kit offre l'opportunità di avviare e terminare Kaspersky Anti-Virus in remoto su singoli computer client, nonché di modificare le impostazioni generali per l'applicazione, ad esempio abilitando/disabilitando la protezione del computer, modificando le impostazioni per il backup, la quarantena e la creazione di rapporti.

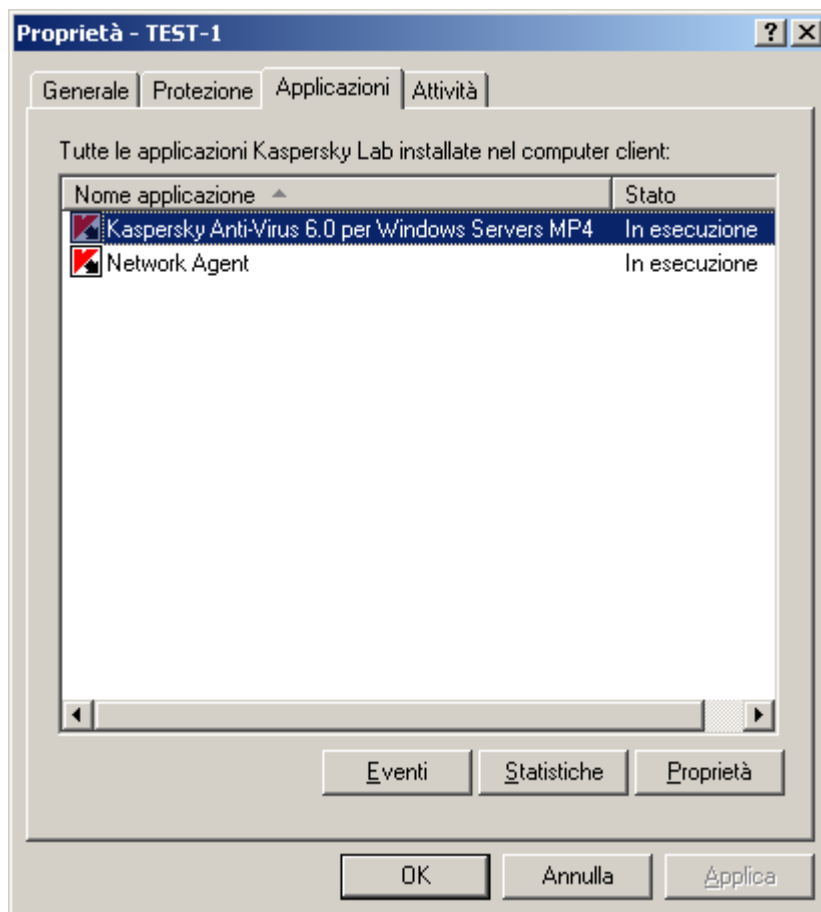


Fig. 12. Finestra delle proprietà del computer client. Scheda **Applicazioni**

➡ Per gestire le impostazioni dell'applicazione, eseguire le seguenti operazioni:

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Selezionare la cartella **Computer gestiti** con il nome del gruppo che include il computer client.
3. Nel gruppo selezionato, aprire la cartella **Computer client** e selezionare il computer per cui modificare le impostazioni dell'applicazione.
4. Selezionare il comando **Proprietà** dal menu di scelta rapida o la voce corrispondente nel menu **Azione** per aprire la finestra delle proprietà del computer client.
5. Nella scheda **Applicazioni** nella finestra delle proprietà del computer client viene visualizzato l'elenco completo delle applicazioni Kaspersky Lab installate nel computer client. Selezionare **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** nell'elenco delle applicazioni.

In questo elenco di applicazioni sono disponibili controlli che consentono di:

- Visualizzare l'elenco di eventi verificatisi durante il funzionamento dell'applicazione nel computer client e registrati nel server di amministrazione;
- Visualizzare le statistiche correnti sul funzionamento dell'applicazione;

- Modificare le impostazioni dell'applicazione (vedere a pag. [122](#)).

AVVIO E ARRESTO DELL'APPLICAZIONE

Kaspersky Anti-Virus 6.0 può essere installato e avviato nei computer clienti dalla finestra delle proprietà dell'applicazione (vedere la figura seguente).

Nella parte superiore della finestra è presente il nome dell'applicazione installata, le informazioni sulla versione, la data di installazione, lo stato (se l'applicazione è in esecuzione o è stata terminata nel computer locale) e informazioni sullo stato del database delle firme delle minacce.

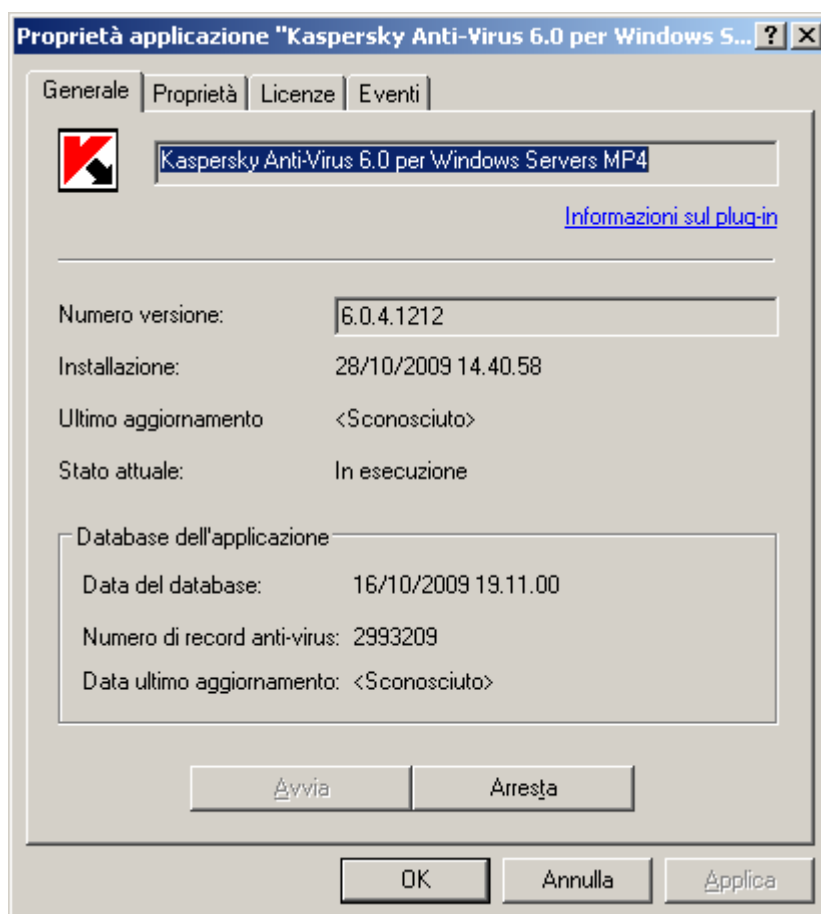


Fig. 13. Finestra delle proprietà dell'applicazione. Scheda **Generale**

► Per terminare o avviare l'applicazione in un computer remoto, eseguire le seguenti operazioni:

1. Aprire la scheda **Applicazioni** nella finestra delle proprietà del computer client (vedere pagina [120](#)).
2. Selezionare **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** nell'elenco delle applicazioni, quindi premere il pulsante **Proprietà**.
3. Nella finestra delle proprietà dell'applicazione che verrà visualizzata cliccare sul bottone **Termina** nella scheda **Generale** per arrestare l'applicazione o il bottone **Avvia** per avviarla.

CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

È possibile visualizzare e modificare le impostazioni dell'applicazione nella scheda **Proprietà** della finestra delle proprietà dell'applicazione (vedere la figura seguente). Le altre schede sono standard per l'applicazione Kaspersky Administration Kit e sono descritte in maggiore dettaglio nel manuale di riferimento.

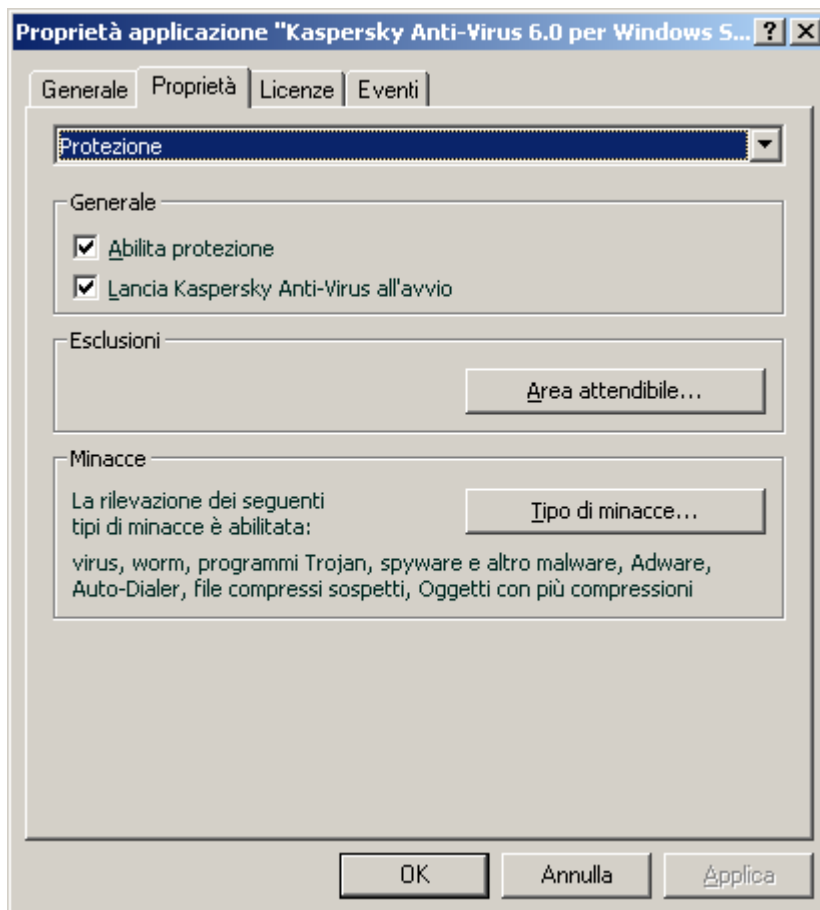


Fig. 14. Finestra delle proprietà dell'applicazione. Scheda **Proprietà**

Se è stato creato un criterio per l'applicazione (vedere pagina [131](#)) che impedisce di modificare alcune impostazioni, non sarà possibile modificarle durante la configurazione dell'applicazione.

➡ Per visualizzare e modificare l'applicazione eseguire le seguenti operazioni:

1. Aprire la scheda **Applicazioni** nella finestra delle proprietà del computer client (vedere pagina [120](#)).
2. Selezionare **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** nell'elenco delle applicazioni, quindi premere il pulsante **Proprietà**.
3. Nella finestra delle proprietà dell'applicazione visualizzata, all'interno della scheda **Proprietà**, è possibile modificare le impostazioni generali di Kaspersky Anti-Virus, le impostazioni di archiviazione e di creazione rapporti, nonché le impostazioni di rete. A tale scopo, selezionare il valore richiesto nel menu a discesa nella parte superiore della finestra e modificare le impostazioni.

VEDERE ANCHE

Avvio dell'applicazione all'avvio del sistema operativo	74
Selezione delle categorie di minacce rilevabili	74
Creazione di un'area attendibile	74
Configurazione della notifica tramite posta elettronica	85
Configurazione dei rapporti	88
Configurazione della quarantena e del backup	90

CONFIGURAZIONE DI IMPOSTAZIONI SPECIFICHE

Quando si gestisce Kaspersky Anti-Virus tramite Kaspersky Administration Kit, è possibile abilitare/disabilitare l'interattività, configurare l'aspetto dell'applicazione e modificare le informazioni relative all'assistenza tecnica. Queste impostazioni possono essere modificate nella finestra delle proprietà dell'applicazione (vedere la figura seguente).

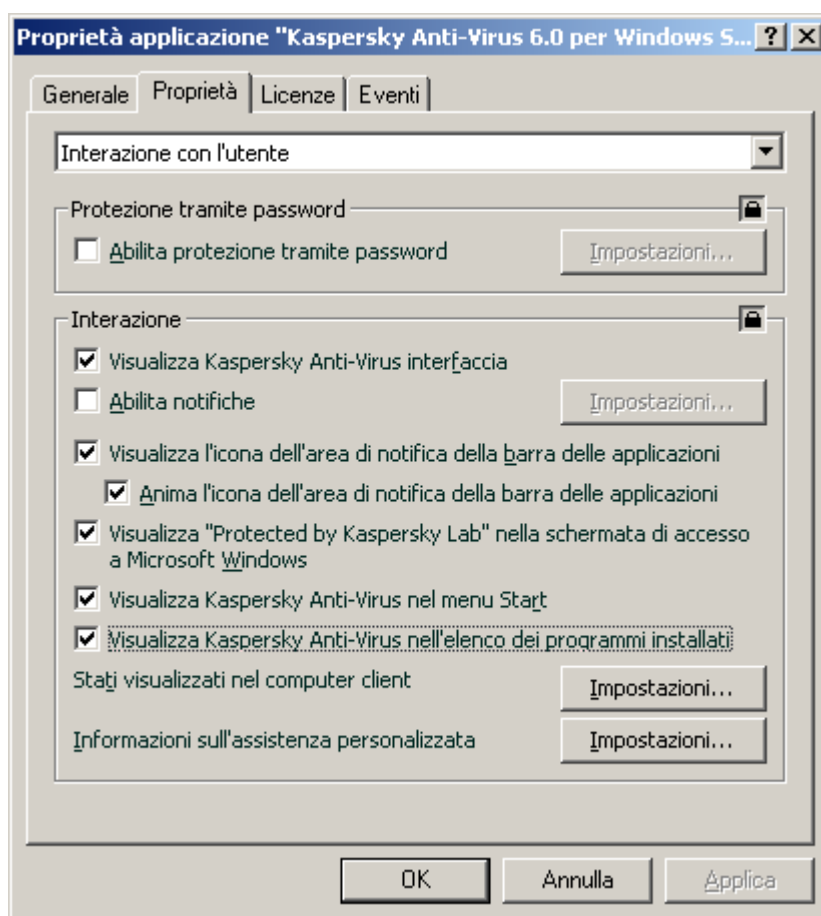


Fig. 15. Finestra delle proprietà dell'applicazione. Configurazione di impostazioni specifiche

Per proteggere tramite password Kaspersky Anti-Virus, selezionare la casella ☒ **Abilita protezione tramite password** nella finestra visualizzata, premendo il pulsante **Impostazioni**, quindi immettere la password e l'area coperta dalla restrizione dell'accesso.

Per garantire protezione contro rimozioni non autorizzate di un'applicazione da un computer locale, selezionare la casella ☒ **Abilita protezione disinstallazione**. Nella finestra visualizzata premendo il pulsante **Impostazioni**, immettere una password per la disinstallazione e confermare.

Per proteggere tramite password Kaspersky Anti-Virus, selezionare la casella ☒ **Abilita protezione tramite password** nella finestra visualizzata, premendo il pulsante **Impostazioni**, quindi immettere la password e l'area coperta dalla restrizione dell'accesso.

Per garantire protezione contro rimozioni non autorizzate di un'applicazione da un computer locale, selezionare la casella ☒ **Abilita protezione disinstallazione**. Nella finestra visualizzata premendo il pulsante **Impostazioni**, immettere una password per la disinstallazione e confermare.

Nella sezione **Interazione** è possibile specificare le impostazioni per l'interazione dell'utente con l'interfaccia di Kaspersky Anti-Virus:

- Se la casella ☐ **Disabilita interazione** non è selezionata, gli utenti che lavorano su un computer remoto vedranno l'icona di Kaspersky Anti-Virus e i messaggi a comparsa. Avranno inoltre la possibilità di decidere le azioni ulteriori nella finestra di notifica in cui vengono segnalati gli eventi. Per disabilitare la modalità interattiva nel funzionamento dell'applicazione, selezionare la casella. Se occorre nascondere la presenza dell'applicazione agli utenti, è necessario selezionare anche la casella ☒ **Nascondi applicazione installata**.
- Nella finestra **Visualizzazione** visualizzata premendo il pulsante **Impostazioni**, è possibile modificare le informazioni sull'assistenza tecnica contenute nella finestra **Supporto** di Kaspersky Anti-Virus.

Per modificare le informazioni, nel campo superiore immettere il testo corrente sull'assistenza fornita. Nel campo sottostante è possibile modificare i collegamenti ipertestuali visualizzati nella sezione **Link utili** della finestra **Supporto** che viene visualizzata cliccando sul collegamento **Supporto** nella finestra principale di Kaspersky Anti-Virus.

È possibile modificare l'elenco mediante i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. Kaspersky Anti-Virus aggiungerà un nuovo collegamento nella parte superiore dell'elenco. Per modificare l'ordine dei collegamenti nell'elenco, utilizzare i bottoni **Sposta su** e **Sposta giù**.

Se la finestra non contiene dati, le informazioni predefinite dell'assistenza tecnica non possono essere modificate.

Nella sezione **Stati applicazione**, è possibile specificare gli stati dell'applicazione che verranno visualizzati nella finestra principale di Kaspersky Anti-Virus. Per effettuare questa operazione, premere il pulsante **Impostazioni** e selezionare le caselle ☒ degli stati in questione nella finestra visualizzata. In questa stessa finestra è possibile specificare anche i periodi di monitoraggio dei database dell'applicazione.

Nella sezione **Visualizza**, è possibile modificare le impostazioni della modalità di funzionamento interattivo di Kaspersky Anti-Virus su un computer remoto: la visualizzazione dell'icona nella finestra di login di Microsoft Windows, l'animazione dell'icona di Kaspersky Anti-Virus nell'area di notifica, la creazione di notifiche per gli eventi che si verificano nell'applicazione (ad esempio il rilevamento di un oggetto pericoloso).

Se è stato creato un criterio per l'applicazione (vedere pagina [131](#)) che impedisce di modificare alcune impostazioni, non sarà possibile modificarle durante la configurazione dell'applicazione.

➡ Per visualizzare e modificare le impostazioni avanzate dell'applicazione, eseguire le seguenti operazioni:

1. Aprire nella finestra delle proprietà del computer client (vedere pagina [120](#)) la scheda **Applicazioni**.
2. Selezionare **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** nell'elenco delle applicazioni, quindi premere il pulsante **Proprietà**.
3. Nella scheda **Proprietà** della finestra dell'applicazione visualizzata selezionare la voce **Interazione con l'utente** nell'elenco a discesa e modificare le impostazioni.

GESTIONE DELLE ATTIVITÀ

In questa sezione sono incluse informazioni sulla gestione delle attività per Kaspersky Anti-Virus. Per maggiori dettagli sulla gestione delle attività tramite Kaspersky Administration Kit, consultare il manuale dell'amministratore per tale prodotto.

Durante l'installazione dell'applicazione viene creato un elenco di attività di sistema per ogni computer della rete. L'elenco riporta le attività di protezione (Anti-Virus File), le attività di scansione anti-virus (scansione completa e rapida) e le attività di aggiornamento (aggiornamenti dei database e dei moduli dell'applicazione, rollback degli aggiornamenti).

È possibile gestire la pianificazione delle attività di sistema e modificare le relative impostazioni. Non è possibile eliminare queste attività.

È anche possibile creare attività personalizzate (vedere pagina [126](#)), quali attività di scansione, aggiornamenti delle applicazioni e rollback degli aggiornamenti, e attività di installazione del file di chiave.

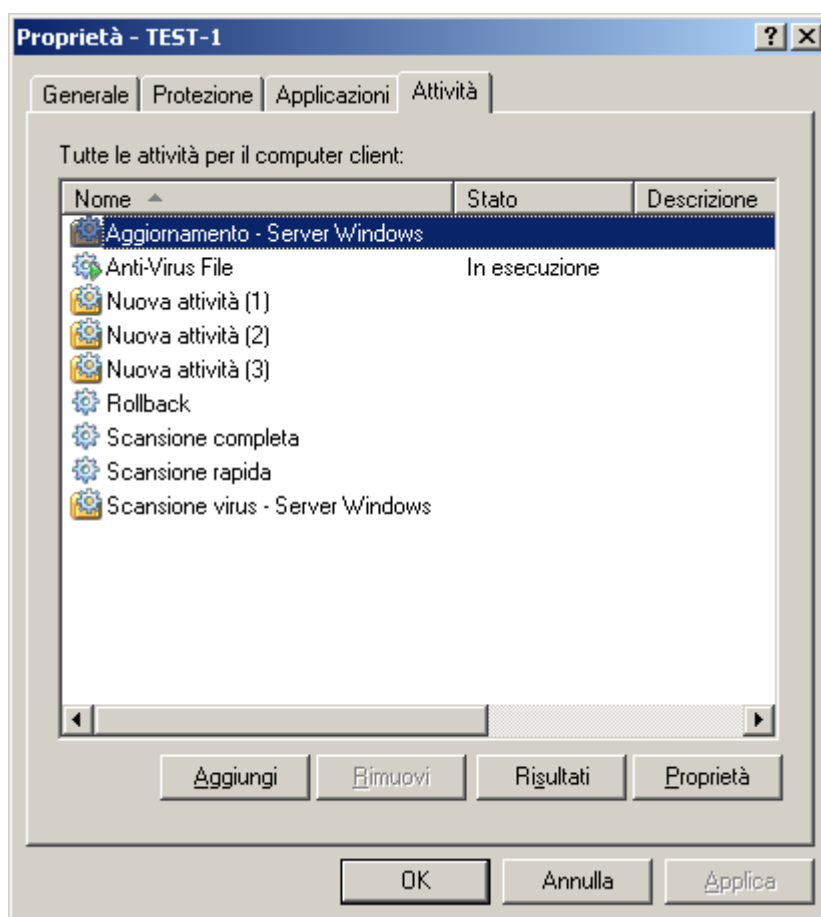


Fig. 16. Finestra delle proprietà del computer client. Scheda **Attività**

► Per aprire l'elenco di attività create per un computer client, eseguire le seguenti operazioni:

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Selezionare la cartella **Computer gestiti** con il nome del gruppo che include il computer client.
3. Nel gruppo selezionato, aprire la cartella **Computer client** e selezionare il computer per cui modificare le impostazioni dell'applicazione.
4. Selezionare il comando **Proprietà** dal menu di scelta rapida o la voce corrispondente nel menu **Azione** per aprire la finestra delle proprietà del computer client.

5. Nella finestra delle proprietà dell'applicazione che viene visualizzata, selezionare la scheda **Attività**. In questa scheda è possibile trovare l'elenco completo di attività create per il computer client.

AVVIO E ARRESTO DELLE ATTIVITÀ

Le attività vengono avviate nel computer client solo se è in esecuzione l'applicazione corrispondente (vedere pagina [121](#)). Se l'applicazione viene chiusa, tutte le attività in esecuzione verranno terminate.

Le attività vengono avviate e arrestate automaticamente in base a una pianificazione o manualmente tramite i comandi del menu di scelta rapida e dalla finestra Visualizza impostazioni attività. È anche possibile sospendere e riprendere le attività.

► Per avviare/arrestare/sospendere/riprendere manualmente un'attività, eseguire le seguenti operazioni:

1. Aprire nella finestradelle proprietà del computer client nella scheda **Attività**.
2. Selezionare l'attività richiesta e aprire il relativo menu di scelta rapida. Selezionare la voce **Avvia** per avviare l'attività oppure la voce **Termina** per terminarla. È inoltre possibile utilizzare le voci corrispondenti del menu **Azione**.

Non è possibile sospendere e riprendere un'attività dal menu di scelta rapida.

oppure

Selezionare l'attività richiesta nell'elenco e cliccare sul bottone **Proprietà**. È possibile utilizzare i bottoni della scheda **Generale** all'interno della finestra delle proprietà dell'attività per avviare, terminare, sospendere o riprendere un'attività.

CREAZIONE DI ATTIVITÀ

Quando si gestisce l'applicazione tramite Kaspersky Administration Kit, è possibile creare i seguenti tipi di attività:

- attività locali definite per singoli computer client;
- attività di gruppo definite per computer che appartengono a gruppi di amministrazione;
- attività per insiemi di computer definiti per computer esterni ai gruppi di amministrazione;
- Le attività di Kaspersky Administration Kit sono specifiche per il server di aggiornamento: attività di download degli aggiornamenti, attività di backup e attività di invio rapporti.

Le attività di gruppo del computer vengono eseguite solo nell'insieme selezionato di computer. Se vengono aggiunti nuovi computer client a un gruppo contenente computer per cui è stata creata un'attività di installazione remota, l'attività non verrà eseguita per tali computer. È necessario creare una nuova attività o apportare le modifiche necessarie alle impostazioni dell'attività esistente.

È possibile eseguire le azioni seguenti in relazione alle attività:

- specificare le impostazioni delle attività;
- monitorare l'esecuzione dell'attività;
- copiare e spostare le attività da un gruppo all'altro, oppure eliminarle utilizzando i comandi standard **Copia/Incolla**, **Taglia/Incolla**, **Elimina** dal menu di scelta rapida oppure i comandi corrispondenti nel menu **Azione**;

- importare ed esportare le attività.

Per ulteriori informazioni sull'utilizzo delle attività, consultare il manuale di riferimento di Kaspersky Administration Kit.

➡ *Per creare un'attività locale, eseguire le seguenti operazioni:*

1. Aprire la finestra principale delle proprietà del computer client in questione nella scheda **Attività**.
2. Cliccare sul bottone **Aggiungi**.
3. Verrà quindi avviata la Creazione guidata nuova attività (vedere pagina [127](#)). Seguirne le istruzioni.

➡ *Per creare un'attività di gruppo, eseguire le seguenti operazioni:*

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.
3. Nel gruppo selezionato, aprire la cartella **Attività di gruppo** in cui è possibile trovare tutte le attività create per tale gruppo.
4. Aprire la Creazione guidata nuova attività cliccando sul collegamento **Crea nuova attività** nella barra delle applicazioni. Le specifiche per la creazione di attività di gruppo sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

➡ *Per creare un'attività per un gruppo di computer (un'attività di Kaspersky Administration Kit), eseguire le seguenti operazioni:*

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Selezionare la cartella **Attività per computer specifici (attività di Kaspersky Administration Kit)**.
3. Aprire la Creazione guidata nuova attività cliccando sul collegamento **Crea nuova attività** nella barra delle applicazioni. Le specifiche per la creazione di attività di Kaspersky Administration Kit e di attività per gruppi di computer sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

CREAZIONE GUIDATA ATTIVITÀ LOCALE

Creazione guidata attività locale viene avviato quando si selezionano i comandi corrispondenti dal menu di scelta rapida per il computer client o nella finestra delle proprietà per tale computer.

La procedura guidata è costituita da una serie di finestre (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** ed **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per annullare la procedura in qualsiasi momento, utilizzare il bottone **Annulla**.

PASSAGGIO 1. IMMISSIONE DI DATI GENERALI NELL'ATTIVITÀ

La prima finestra della procedura guidata è introduttiva e richiede solo l'immissione del nome dell'attività nel campo **Nome**.

PASSAGGIO 2. SELEZIONE DI UN'APPLICAZIONE E DI UN TIPO DI ATTIVITÀ

In questo passaggio è necessario specificare l'applicazione per cui si intende creare l'attività (Kaspersky Anti-Virus 6.0 for Windows Servers MP4 o Administration Agent). È necessario selezionare anche il tipo di attività. Le attività disponibili per Kaspersky Anti-Virus 6.0 sono:

- *File dei virus*: attività di scansione anti-virus delle aree specificate dall'utente.
- *Aggiornamento*: consente di recuperare e implementare pacchetti di aggiornamento per l'applicazione.

- *Aggiorna rollback*: esegue il rollback all'ultimo aggiornamento dell'applicazione.
- *Installazione file di chiave*: installazione di un file di chiave per una nuova licenza, se necessario per utilizzare l'applicazione.

PASSAGGIO 3. CONFIGURAZIONE DEL TIPO DI ATTIVITÀ SELEZIONATO

Il contenuto della finestra delle impostazioni varia in base al tipo di attività selezionato.

Le attività di scansione anti-virus richiedono di specificare l'azione che Kaspersky Anti-Virus eseguirà se rileva un oggetto dannoso (vedere pagina [53](#)) e di creare un elenco di oggetti da sottoporre a scansione (vedere pagina [51](#)).

Per le attività di aggiornamento del database e dei moduli dell'applicazione, è necessario specificare l'origine che verrà utilizzata per scaricare gli aggiornamenti (vedere pagina [63](#)). L'origine di aggiornamento predefinita è il server di aggiornamento di Kaspersky Administration Kit.

Le attività di rollback degli aggiornamenti non presentano impostazioni specifiche.

Per le attività di installazione della chiave di licenza, specificare il percorso del file di chiave mediante il bottone **Sfoglia**. Per aggiungere un file come chiave di licenza per una licenza aggiuntiva, selezionare la casella ☒ corrispondente. La chiave di licenza aggiuntiva verrà attivata alla scadenza della chiave di licenza già attiva.

Nel campo seguente sono visualizzate informazioni sulla licenza specifica (numero, tipo e data di scadenza della licenza).

PASSAGGIO 4. CONFIGURAZIONE DI UNA PIANIFICAZIONE

Dopo aver configurato le attività, viene offerta la possibilità di configurare la pianificazione di esecuzione automatica dell'attività.

A tale scopo, selezionare la frequenza di esecuzione dell'attività dal menu a discesa nella finestra delle impostazioni di pianificazione e modificare tali impostazioni nella parte inferiore della finestra.

PASSAGGIO 5. COMPLETAMENTO DELLA CREAZIONE DELL'ATTIVITÀ

Nell'ultima finestra della procedura guidata viene indicato che la creazione dell'attività è stata completata.

CONFIGURAZIONE DELLE ATTIVITÀ

La configurazione delle attività dell'applicazione tramite l'interfaccia di Kaspersky Administration Kit è simile alla stessa procedura eseguita tramite l'interfaccia locale di Kaspersky Anti-Virus, con la differenza che le impostazioni vengono modificate singolarmente per ogni utente, ad esempio la pianificazione dell'esecuzione delle attività di scansione o le impostazioni specifiche di Kaspersky Administration Kit, quali le impostazioni che consentono/bloccano la gestione delle attività di scansione locale eseguite dagli utenti.

Se è stato creato un criterio per l'applicazione (vedere pagina [131](#)) che impedisce di modificare alcune impostazioni, non sarà possibile modificarle durante la configurazione dell'applicazione.

Tutte le schede presenti nella finestra delle proprietà dell'attività, ad eccezione della scheda **Proprietà** (vedere la figura seguente), sono standard per Kaspersky Administration Kit e sono descritte in maggior dettaglio nel manuale di riferimento. La scheda **Proprietà** contiene impostazioni specifiche per Kaspersky Anti-Virus. Il contenuto di questa scheda varia in base al tipo di attività selezionato.

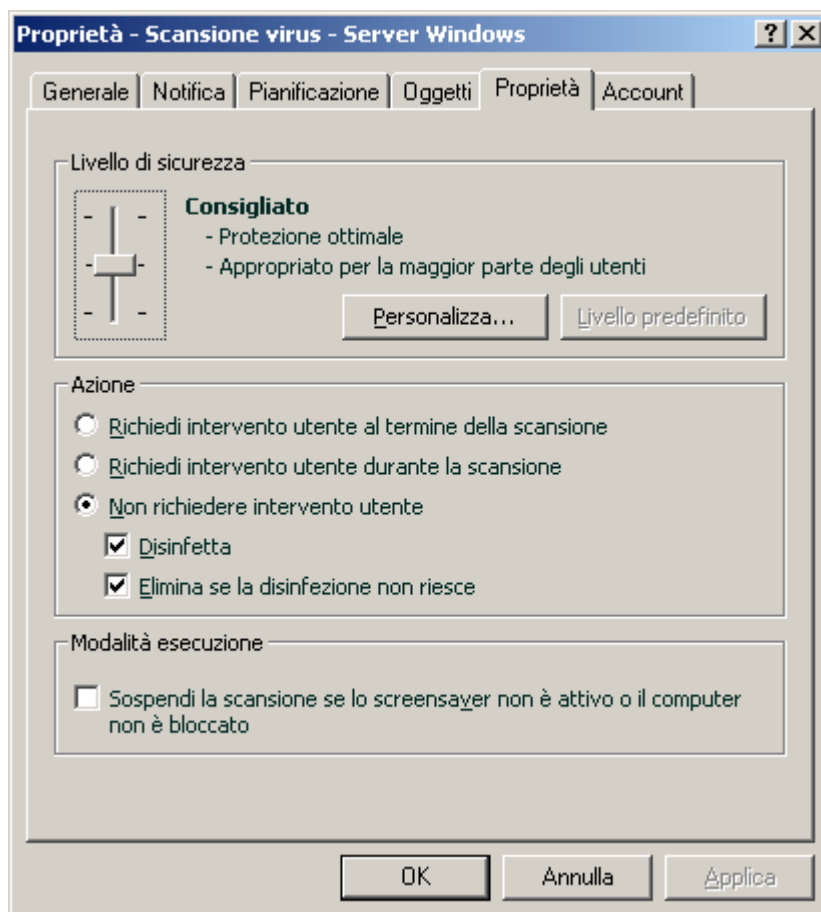


Fig. 17. Finestra delle proprietà dell'attività. Scheda **Proprietà**

➡ Per visualizzare e modificare le attività locali, eseguire le seguenti operazioni:

1. Aprire la finestra delle proprietà del computer client nella scheda **Attività**.
2. Selezionare un'attività nell'elenco e cliccare sul bottone **Proprietà**. Verrà aperta la finestra delle impostazioni dell'attività.

➡ Per visualizzare le attività di gruppo, eseguire le seguenti operazioni:

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.
3. Nel gruppo selezionato, aprire la cartella **Attività di gruppo** in cui è possibile trovare tutte le attività create per tale gruppo.
4. Selezionare l'attività richiesta dalla struttura ad albero della console per visualizzarne e modificarne le proprietà.

Nella barra delle applicazioni verranno visualizzate informazioni complete sull'attività, insieme ai collegamenti per gestire l'esecuzione dell'attività e la modifica delle relative impostazioni. Le specifiche per la creazione di attività di gruppo sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

➤ *Per visualizzare attività per un gruppo di computer (un'attività di Kaspersky Administration Kit), eseguire le seguenti operazioni:*

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Selezionare la cartella **Attività per computer specifici (attività di Kaspersky Administration Kit)**.
3. Selezionare l'attività richiesta dalla struttura ad albero della console per visualizzarne e modificarne le proprietà.

Nella barra delle applicazioni verranno visualizzate informazioni complete sull'attività, insieme ai collegamenti per gestire l'esecuzione dell'attività e la modifica delle relative impostazioni. Le specifiche delle attività di Kaspersky Administration Kit e le attività per gruppi di computer sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

GESTIONE DEI CRITERI

L'impostazione di criteri consente di applicare impostazioni universali dell'applicazione e dell'attività ai computer client che appartengono a un singolo gruppo di amministrazione.

In questa sezione sono incluse informazioni sulla creazione e configurazione dei criteri per Kaspersky Anti-Virus 6.0 for Windows Servers MP4. Per ulteriori informazioni sui concetti legati alla gestione dei criteri tramite Kaspersky Administration Kit, consultare il manuale dell'amministratore per l'applicazione.

Quando si crea e si configura un criterio, è possibile bloccare completamente o in parte la modifica delle impostazioni nei criteri per i gruppi nidificati, le impostazioni delle attività e le impostazioni delle applicazioni. A tale scopo, premere il bottone . Dovrebbe diventare  per le impostazioni bloccate.

➤ *Per aprire l'elenco di criteri per Kaspersky Anti-Virus, eseguire le seguenti operazioni:*

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Selezionare la cartella **Computer gestiti** con il nome del gruppo che include il computer client.
3. Nel gruppo selezionato, aprire la cartella **Criteri** in cui è possibile trovare tutti i criteri creati per tale gruppo.

CREAZIONE DI CRITERI

Quando si utilizza Kaspersky Anti-Virus tramite Kaspersky Administration Kit, è possibile creare i seguenti tipi di criteri:

È possibile eseguire le azioni seguenti in relazione ai criteri:

- configurare i criteri;
- copiare e spostare i criteri da un gruppo all'altro, oppure eliminarli utilizzando i comandi standard **Copia/Incolla**, **Taglia/Incolla**, **Elimina** dal menu di scelta rapida oppure i comandi corrispondenti nel menu **Azione**;
- importare ed esportare le impostazioni dei criteri.

La gestione dei criteri è illustrata in maggior dettaglio nel manuale di riferimento di Kaspersky Administration Kit.

➤ *Per creare un criterio, eseguire le seguenti operazioni:*

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.
3. Nel gruppo selezionato, aprire la cartella **Criteri** in cui è possibile trovare tutti i criteri creati per tale gruppo.

4. Aprire la Creazione guidata nuova attività cliccando sul collegamento **Crea nuovo criterio** nella barra delle applicazioni.
5. Verrà quindi avviata la Creazione guidata nuova attività nella finestra visualizzata (vedere a pag. [131](#)) di cui sarà necessario seguire le indicazioni.

CREAZIONE GUIDATA CRITERIO

È possibile avviare Creazione guidata criterio selezionando l'azione corrispondente dal menu di scelta rapida della cartella **Criteri** del gruppo di amministrazione selezionato oppure cliccando sul collegamento nel riquadro dei risultati (per le cartelle **Criteri**).

La procedura guidata è costituita da una serie di finestre (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** ed **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per annullare la procedura in qualsiasi momento, utilizzare il bottone **Annulla**.

PASSAGGIO 1. IMMISSIONE DI DATI GENERALI NEL CRITERIO

Le prime finestre della procedura guidata sono introduttive. In queste finestre è necessario specificare il nome del criterio nel campo **Nome** e selezionare **Kaspersky Anti-Virus 6.0 for Windows Servers MP4** nel menu a discesa **Nome applicazione**.

Se si esegue la Creazione guidata criterio dal nodo **Criteri** della barra delle applicazioni (utilizzando **Crea nuovo criterio di Kaspersky Anti-Virus for Windows Servers MP4**), non sarà possibile selezionare un'applicazione.

Se si desidera creare un criterio basato sulle impostazioni di un criterio esistente creato per la versione precedente dell'applicazione, selezionare la casella ☒ **Utilizza impostazioni del criterio esistente** e il criterio di cui si desidera utilizzare le impostazioni per il nuovo criterio. Per selezionare un criterio, cliccare sul bottone **Seleziona** che aprirà l'elenco dei criteri esistenti che possono essere utilizzati per crearne uno nuovo.

PASSAGGIO 2. SELEZIONE DELLO STATO DEL CRITERIO

In questa finestra è possibile specificare lo stato del criterio creato, selezionando una delle opzioni seguenti: criterio attivo o criterio inattivo. Per ulteriori informazioni sullo stato dei criteri, consultare il manuale di riferimento di Kaspersky Administration Kit.

È possibile creare vari criteri per una singola applicazione in un gruppo, ma solo uno di essi può essere il criterio attivo.

PASSAGGIO 3. IMPORTAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

Se si dispone di un file con impostazioni dell'applicazione salvate in precedenza, è possibile specificarne il percorso utilizzando il pulsante **Importa**. Nelle finestre della procedura guidata visualizzate da quel momento in poi verranno mostrate le impostazioni importate.

PASSAGGIO 4. CONFIGURAZIONE DELLA PROTEZIONE

In questo passaggio è possibile abilitare/disabilitare o configurare i componenti di protezione che verranno utilizzati nel criterio.

Per impostazione predefinita, tutti i componenti di protezione sono abilitati. Per disabilitare singoli componenti, deselezionare la casella accanto ad essi. Per modificare un componente di protezione, selezionarlo nell'elenco e cliccare sul bottone **Configura**.

PASSAGGIO 5. CONFIGURAZIONE DELLA PROTEZIONE TRAMITE PASSWORD

In questa finestra della procedura guidata, è possibile configurare la protezione mediante password delle operazioni con l'applicazione e della disinstallazione.

PASSAGGIO 6. CONFIGURAZIONE DELL'AREA ATTENDIBILE

In questa finestra della procedura guidata è possibile configurare l'area attendibile, ovvero aggiungere il software utilizzato per l'amministrazione della rete all'elenco di applicazioni attendibili ed escludere vari tipi di file dalla scansione.

PASSAGGIO 7. CONFIGURAZIONE DELL'INTERAZIONE CON L'UTENTE

In questo passaggio è possibile specificare le impostazioni per l'interazione dell'utente con Kaspersky Anti-Virus:

- visualizzazione dell'interfaccia dell'applicazione in un computer remoto;
- invio di notifiche degli eventi agli utenti;
- visualizzazione dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni e della relativa animazione;
- visualizzazione di "Protected by Kaspersky Lab" nella schermata di accesso a Microsoft Windows;
- visualizzazione dell'applicazione nel menu Start;
- visualizzazione dell'applicazione nell'elenco dei programmi installati.

PASSAGGIO 8. COMPLETAMENTO DELLA CREAZIONE DEL CRITERIO

Nell'ultima finestra della procedura guidata viene indicato che la creazione del criterio è stata completata.

Al termine della procedura guidata, il criterio per l'applicazione verrà aggiunto alla cartella **Criteri** del gruppo corrispondente, diventando visibile nella struttura ad albero della console.

È possibile modificare le impostazioni del criterio creato e impostare restrizioni alla modifica delle relative impostazioni utilizzando i bottoni  e  per ogni gruppo di impostazioni. Se viene visualizzata l'icona , l'utente del computer client non potrà modificare le impostazioni. Se viene visualizzata l'icona , l'utente del computer client potrà modificare le impostazioni. Il criterio verrà applicato ai computer client durante la prima sincronizzazione dei client con il server.

CONFIGURAZIONE DEL CRITERIO

Durante la fase di modifica è possibile modificare il criterio e bloccare la modifica delle impostazioni nei criteri dei gruppi nidificati e nelle impostazioni dell'applicazione e dell'attività. Le impostazioni del criterio possono essere modificate nella finestra delle proprietà del criterio (vedere la figura seguente).

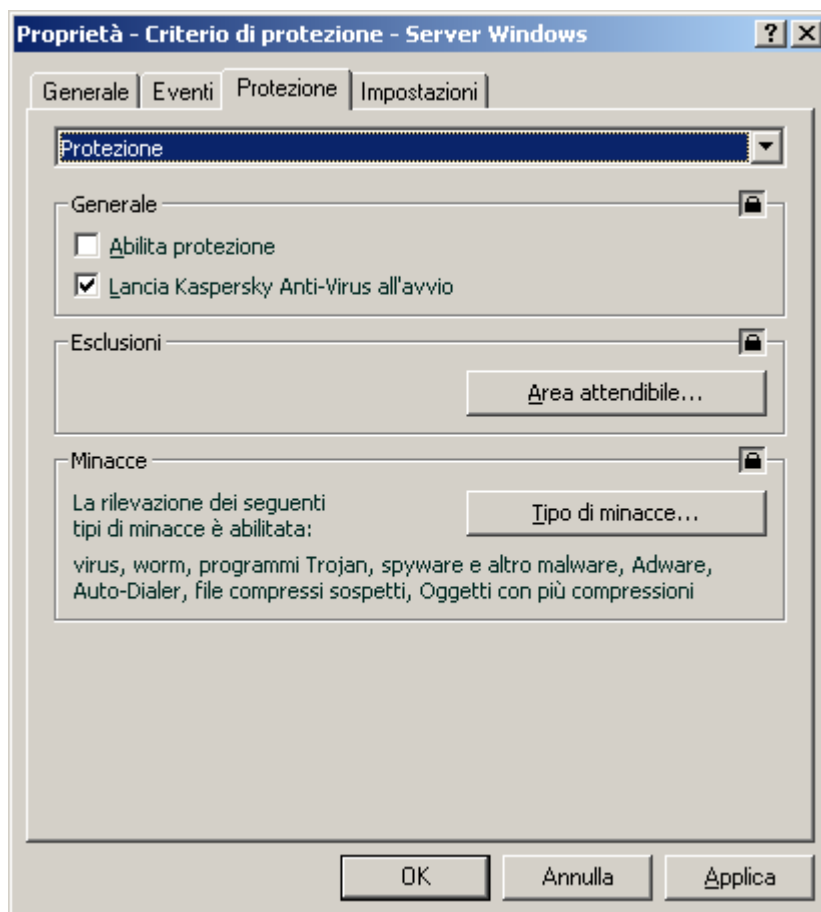


Fig. 18. Finestra delle proprietà dei criteri. Scheda **Protezione**

Tutte le schede, ad eccezione delle schede **Protezione** e **Impostazioni**, sono standard per Kaspersky Administration Kit e sono descritte in maggior dettaglio nel manuale dell'amministratore.

Le impostazioni dei criteri per Kaspersky Anti-Virus 6.0 includono le impostazioni dell'applicazione (vedere a pag. [122](#)) e le impostazioni dell'attività. Nella scheda **Impostazioni** vengono visualizzate le impostazioni dell'applicazione e nella scheda **Protezione** le impostazioni dell'attività.

Per modificare le impostazioni, selezionare il valore richiesto nel menu a discesa nella parte superiore della finestra e impostarlo.

➡ Per visualizzare e modificare le impostazioni dei criteri, eseguire le seguenti operazioni:

1. Aprire la console di amministrazione di Kaspersky Administration Kit.
2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.
3. Nel gruppo selezionato, aprire la cartella **Criteri** in cui è possibile trovare tutti i criteri creati per tale gruppo.
4. Selezionare il criterio richiesto dalla struttura ad albero della console per visualizzarne e modificarne le proprietà.

5. Nella barra delle applicazioni verranno visualizzate informazioni complete sul criterio, insieme ai collegamenti per gestire lo stato del criterio e la modifica delle relative impostazioni.

oppure

Aprire il menu di scelta rapida per il criterio selezionato e utilizzare l'elemento **Proprietà** per aprire la finestra delle impostazioni dei criteri di Kaspersky Anti-Virus.

Le specifiche dell'utilizzo dei criteri sono disponibili nel manuale di riferimento di Kaspersky Administration Kit.

UTILIZZO DI CODICE DI TERZE PARTI

Durante lo sviluppo di Kaspersky Anti-Virus, è stato utilizzato codice di terze parti.

IN QUESTA SEZIONE

Libreria Boost 1.30.0	136
Libreria LZMA SDK 4.40, 4.43.....	136
Libreria Windows Template 7.5	136
Libreria Windows Installer XML (WiX) 2.0	137
Libreria ZIP-2.31.....	140
Libreria ZLIB-1.0.4, ZLIB-1.0., ZLIB-1.1.3, ZLIB-1.2.3.....	141
Libreria UNZIP-5.51.....	141
Libreria LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12.....	142
Libreria LIBJPEG-6B	144
Libreria LIBUNGIF-4.1.4.....	146
Libreria MD5 MESSAGE-DIGEST ALGORITHM-REV. 2	146
Libreria MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004	146
Libreria INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999	146
Libreria CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004	147
Libreria COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum.....	147
Libreria PLATFORM INDEPENDENT IMAGE CLASS	147
Libreria FLEX PARSER (FLEXLEXER)-V. 1993	148
Libreria ENSURECLEANUP, SWMRG, LAYOUT-V. 2000.....	148
Libreria STDSTRING- V. 1999	149
Libreria T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006	149
Libreria NTSERVICE- V. 1997	150
Libreria SHA-1-1.2.....	150
Libreria COCOA SAMPLE CODE- V. 18.07.2007	151
Libreria PUTTY SOURCES-25.09.2008.	151
Altre informazioni.....	152

LIBRERIA BOOST 1.30.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Boost 1.30.0.

Copyright (C) 2003, Christof Meerwald

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA LZMA SDK 4.40, 4.43

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LZMA SDK 4.40, 4.43.

LIBRERIA WINDOWS TEMPLATE 7.5

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Windows Template 7.5.

Copyright (C) 2006, Microsoft Corporation

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce", "reproduction", "derivative works", and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

LIBRERIA WINDOWS INSTALLER XML (WiX) 2.0

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Windows Installer XML (WiX) toolset 2.0.

Copyright (C) 2009, Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

- a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and
- b) in the case of each subsequent Contributor:
 - i) changes to the Program, and
 - ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the

Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBRERIA ZIP-2.31

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria ZIP-2.31.

Copyright (C) 1990-2005, Info-ZIP

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at

<ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBRERIA ZLIB-1.0.4, ZLIB-1.0., ZLIB-1.1.3, ZLIB-1.2.3

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria ZLIB-1.0.4, ZLIB-1.0.8, ZLIB-1.1.3, ZLIB-1.2.3.

Copyright (C) 1995-2005, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

LIBRERIA UNZIP-5.51

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria UNZIP-5.51. Copyright (c) 1990-2004 Info-ZIP.

Copyright (c) 1990-2004, Info-ZIP

This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at <http://ftp.info-zip.org/pub/infozip/license.html> indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as

the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBRERIA LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12.

This copy of the libpng notices is provided for your convenience. In case of any discrepancy between this copy and the notices in the file png.h that is included in the libpng distribution, the latter shall prevail.

COPYRIGHT NOTICE, DISCLAIMER, and LICENSE:

If you modify libpng you may insert additional notices immediately following

this sentence.

This code is released under the libpng license.

libpng versions 1.2.6, 15 agosto 2004, through 1.2.39, 13 agosto 2009, are

Copyright (c) 2004, 2006-2009 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, 01 luglio 2000, through 1.2.5 - 03 ottobre 2002, are Copyright (c) 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfill any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, 20 marzo 2000, are Copyright (c) 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright (c) 1996, 1997 Andreas Dilger Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

```
printf("%s",png_get_copyright(NULL));
```

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg" (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

LIBRERIA LIBJPEG-6B

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LIBJPEG-6B.

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

=====

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

- (1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

- (2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

- (3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium

but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBRERIA LIBUNGIF-4.1.4

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LIBUNGIF-4.1.4.

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA MD5 MESSAGE-DIGEST ALGORITHM-REV. 2

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.

LIBRERIA MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.

LIBRERIA INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999.

Copyright (C) 1991-2, RSA Data Security, Inc.

RSA's MD5 disclaimer

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

LIBRERIA CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004.

Copyright 2001-2004 Unicode, Inc.

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

LIBRERIA COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum.

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware, Shareware, Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

LIBRERIA PLATFORM INDEPENDENT IMAGE CLASS

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria PLATFORM INDEPENDENT IMAGE CLASS.

Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx)

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

LIBRERIA FLEX PARSER (FLEXLEXER)-V. 1993

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria FLEX PARSER (FLEXLEXER)-V. 1993.

Copyright (c) 1993 The Regents of the University of California

This code is derived from software contributed to Berkeley by

Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

LIBRERIA ENSURECLEANUP, SWMRG, LAYOUT-V. 2000

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria ENSURECLEANUP, SWMRG, LAYOUT-V. 2000.

Copyright (C) 2009, Microsoft Corporation

NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software ("License Agreement").

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as "sample" available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License <http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL>.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

LIBRERIA STDSTRING- V. 1999

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria STDSTRING- V. 1999.

Copyright (C) 1999, Joseph M. O'Leary

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes

your \$30 billion dollar satellite explode in orbit. If you redistribute

it in any form, I'd appreciate it if you would leave this notice here.

LIBRERIA T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006.

Copyright (C) 2003-2006, Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

LIBRERIA NTSERVICE- V. 1997

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria NTSERVICE- V. 1997.

Copyright (C) 1997, Joerg Koenig and the ADG mbH, Mannheim, Germany

Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY "///!! TCW MOD"

LIBRERIA SHA-1-1.2

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria SHA-1-1.2.

Copyright (C) 2001, The Internet Society

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

LIBRERIA COCOA SAMPLE CODE- V. 18.07.2007

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Cocoa sample code- v.

Copyright (C) 2007, Apple Inc

Disclaimer: IMPORTANT: This Apple software is supplied to you by Apple Inc. ("Apple")

in consideration of your agreement to the following terms, and your use, installation, modification or redistribution of this Apple software constitutes acceptance of these terms. If you do not agree with these terms, please do not use, install, modify or redistribute this Apple software.

In consideration of your agreement to abide by the following terms, and subject to these terms, Apple grants you a personal, non – exclusive license, under Apple's copyrights in this original Apple software (the "Apple Software"), to use, reproduce, modify and redistribute the Apple Software, with or without modifications, in source and / or binary forms; provided that if you redistribute the Apple Software in its entirety and without modifications, you must retain this notice and the following text and disclaimers in all such redistributions of the Apple Software. Neither the name, trademarks, service marks or logos of Apple Inc. may be used to endorse or promote products derived from the Apple Software without specific prior written permission from Apple. Except as expressly stated in this notice, no other rights or licenses, express or implied, are granted by Apple herein, including but not limited to any patent rights that may be infringed by your derivative works or by other works in which the Apple Software may be incorporated.

The Apple Software is provided by Apple on an "AS IS" basis.

APPLE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON - INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE APPLE SOFTWARE OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH YOUR PRODUCTS.

IN NO EVENT SHALL APPLE BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) ARISING IN ANY WAY OUT OF THE USE, REPRODUCTION, MODIFICATION AND / OR DISTRIBUTION OF THE APPLE SOFTWARE, HOWEVER CAUSED AND WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBRERIA PUTTY SOURCES-25.09.2008.

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria PUTTY SOURCES-25.09.2008. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified <http://www.opensource.org/licenses/> and complies with the Debian Free Software Guidelines http://www.debian.org/social_contract)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

ALTRE INFORMAZIONI

La libreria Crypto C, sviluppato da CryptoEx OOO (<http://www.cryptoex.ru>), è utilizzata per verificare la firma digitale.

La libreria Agava-C, sviluppata da OOO "R-Alpha", è utilizzata per verificare la firma digitale.

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code (Open Source Software). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com.

GLOSSARIO

A

AGGIORNAMENTI CRITICI

Aggiornamenti critici ai moduli dell'applicazione Kaspersky Lab.

AGGIORNAMENTI DEL DATABASE

Elenco di indirizzi Web, definiti come phishing dagli specialisti di Kaspersky Lab. I database vengono scaricati dai server degli aggiornamenti di Kaspersky Lab nel computer e collegati automaticamente all'applicazione.

AGGIORNAMENTI DISPONIBILI

Gruppo di aggiornamenti per i moduli dell'applicazione Kaspersky Lab, inclusi gli aggiornamenti critici accumulati in un periodo di tempo e le modifiche apportate all'architettura dell'applicazione.

AGGIORNAMENTO

Procedura di sostituzione/aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky Lab.

ANALISI EURISTICA

Tecnologia di rilevamento delle minacce che non possono essere identificate dai database Anti-Virus. Consente di rilevare gli oggetti sospettati di essere stati colpiti da un virus sconosciuto o da una variante nuova di virus noti.

L'utilizzo dell'analisi euristica consente di rilevare fino al 92% delle minacce. Questo meccanismo è estremamente efficace e determina falsi positivi molto raramente.

I file rilevati dall'analisi euristica sono considerati sospetti.

APPLICAZIONE NON COMPATIBILE

Applicazione anti-virus di uno sviluppatore di terze parti o applicazione Kaspersky Lab che non supporta la gestione attraverso Kaspersky Administration Kit.

ARCHIVIO

File "contenente" uno o diversi altri oggetti che possono anche essere archivi.

ATTACCO DI VIRUS

Serie di attacchi intenzionali per infettare un computer con un virus.

B

BACKUP

Memoria speciale destinata al salvataggio delle copie di backup di oggetti creati prima della disinfezione o eliminazione iniziale.

BLACKLIST DEI FILE CHIAVE

Modello in base al quale viene generata una notifica di minaccia di attacco di virus. Un elenco di file chiave bloccati è necessario per il funzionamento delle applicazioni di Kaspersky Lab. Il contenuto del file viene aggiornato insieme ai database.

BLOCCO DELL'OGGETTO

Negazione dell'accesso a un oggetto da parte di applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

C**CARTELLA DI DATI**

La cartella contenente le cartelle e i database del servizio necessari per utilizzare l'applicazione. Se la cartella di dati viene spostata, tutte le informazioni in essa incluse devono essere salvate nella nuova posizione.

COPIA DI BACKUP

Creazione di una copia di backup di un file prima di qualsiasi elaborazione. La copia viene archiviata nella memoria di backup e consente di ripristinare il file in seguito, ad esempio per eseguire una scansione con database aggiornati.

D**DATABASE**

Database creati dagli esperti di Kaspersky Lab contenenti una descrizione dettagliata di tutte le minacce alla sicurezza del computer attualmente esistenti nonché dei metodi per rilevarle ed eliminarle. I database vengono costantemente aggiornati da Kaspersky Lab al presentarsi di nuove minacce. Per ottenere una migliore qualità di rilevamento delle minacce, è consigliabile copiare regolarmente i database dai server degli aggiornamenti di Kaspersky Lab.

DISINFEZIONE DEGLI OGGETTI

Metodo utilizzato per elaborare gli oggetti infetti che consente di recuperare completamente o parzialmente i dati; in caso contrario l'oggetto viene considerato non disinfettabile. La disinfezione degli oggetti viene eseguita in base alle voci dei database. Se la disinfezione è l'azione primaria da eseguire sull'oggetto (ovvero la prima azione da eseguire non appena viene rilevato), dell'oggetto viene creata una copia di backup prima di tentare la disinfezione. Durante la disinfezione è possibile che parte dei dati venga persa. Questa copia di backup può essere utilizzata per ripristinare lo stato originario dell'oggetto.

DISINFEZIONE DEGLI OGGETTI AL RIAVVIO

Metodo di elaborazione degli oggetti infetti utilizzati da altre applicazioni al momento della disinfezione. Consiste nel creare una copia dell'oggetto infetto, disinfettare la copia creata e sostituire l'oggetto infetto originale con la copia disinfettata dopo il riavvio successivo del sistema.

E**ELIMINAZIONE DEL MESSAGGIO**

Metodo di elaborazione di un messaggio di posta contenente tracce di spam che consente di eliminare il messaggio fisicamente. L'applicazione di questo metodo è consigliata per i messaggi contenenti inequivocabilmente spam. Prima di eliminare un messaggio, ne viene salvata una copia nella cartella di backup (a meno che questa opzione non sia disabilitata).

ELIMINAZIONE DI UN OGGETTO

Metodo di elaborazione dell'oggetto che implica la sua eliminazione fisica dalla posizione originaria (disco rigido, cartella, risorsa di rete). Si consiglia di applicare questo metodo agli oggetti pericolosi che, per qualsiasi ragione, non possono essere disinfettati.

ESCLUSIONE

Per esclusione si intende un oggetto escluso dalla scansione da parte dell'applicazione Kaspersky Lab. Prima di eliminare un messaggio, ne viene salvata una copia nella cartella di backup (a meno che questa opzione non sia disabilitata). A ogni attività può essere assegnato un insieme di esclusioni.

F**FALSO ALLARME**

Situazione in cui l'applicazione Kaspersky Lab considera un oggetto non infetto come infetto a causa del codice simile a quello di un virus.

FILE CHIAVE

File con l'estensione key, che rappresenta la "chiave" personale che consente di utilizzare l'applicazione Kaspersky Lab. Un file chiave viene incluso nel prodotto acquistato presso i distributori Kaspersky Lab o inviato tramite posta elettronica se l'acquisto avviene online.

FILE COMPRESSO

File di archivio contenente un programma di decompressione e istruzioni di esecuzione per il sistema operativo.

I**INTERCETTATORE**

Sottocomponente dell'applicazione responsabile della scansione di tipi specifici di messaggi di posta elettronica. Il set di intercettori specifico dell'installazione dipende dal ruolo o dalla combinazione di ruoli per i quali l'applicazione è stata distribuita.

INTESTAZIONE

Informazioni all'inizio di un file o di un messaggio, composte da dati di basso livello sullo stato e l'elaborazione del file (o del messaggio). In particolare, l'intestazione del messaggio di posta elettronica contiene dati come le informazioni sul mittente e sul destinatario, nonché la data.

L**LICENZA AGGIUNTIVA**

Licenza che è stata aggiunta per il funzionamento dell'applicazione Kaspersky Lab ma non è stata attivata. La licenza aggiuntiva viene attivata alla scadenza della licenza attiva.

LICENZA ATTIVA

La licenza attualmente utilizzata per il funzionamento un'applicazione Kaspersky Lab. La licenza definisce la data di scadenza per le funzionalità complete e i criteri di licenza per l'applicazione. Non è possibile disporre di più di una licenza con lo stato attivo.

LIVELLO CONSIGLIATO

Livello di protezione basato sulle impostazioni dell'applicazione consigliate dagli esperti di Kaspersky Lab per fornire il livello di protezione ottimale del computer. Questo livello viene impostato per essere utilizzato per impostazione predefinita.

LIVELLO DI GRAVITÀ DELL'EVENTO

Descrizione dell'evento, registrato durante il funzionamento dell'applicazione Kaspersky Lab. Esistono quattro livelli di gravità:

Eventi critici.

Errori funzionali.

Attenzione.

Messaggio informativo.

Eventi dello stesso tipo possono avere livelli di gravità diversi, in base alla situazione in cui si sono verificati.

M

MASCHERA DI FILE

Per esclusione si intende un oggetto escluso dalla scansione da parte dell'applicazione Kaspersky Lab. I due caratteri jolly standard utilizzati nelle maschere file sono * e ?, dove * rappresenta una qualsiasi combinazione di caratteri e ? indica un qualsiasi singolo carattere. Utilizzando questi caratteri jolly, è possibile rappresentare qualsiasi file. Notare che il nome e l'estensione sono sempre separati da un punto.

MEMORIA DI BACKUP

Cartella di archiviazione speciale per le copie dei dati di Administration Server creati mediante una utilità di backup.

O

OGGETTI DI AVVIO

Cartella nella quale vengono conservati tutti gli oggetti potenzialmente infetti rilevati durante le scansioni o la protezione in tempo reale. Questi oggetti vengono eseguiti ad ogni avvio del sistema operativo. Esistono virus in grado di infettare questi tipi di oggetti in particolare e bloccare, ad esempio, l'accesso al sistema operativo.

OGGETTO OLE

Un oggetto allegato o un oggetto incorporato in un altro file. L'applicazione Kaspersky Lab consente di eseguire la scansione anti-virus degli oggetti OLE. Se ad esempio si inserisce una tabella di Microsoft Office Excel in un documento di Microsoft Office Word, tale tabella verrà esaminata come oggetto OLE.

OGGETTO INFETTO

Oggetto contenente codice dannoso: viene rilevato quando una sezione del codice dell'oggetto corrisponde in modo preciso a una sezione del codice di una minaccia nota. Kaspersky Lab sconsiglia l'uso di oggetti di questo tipo poiché potrebbero causare un'infezione nel computer.

OGGETTO MONITORATO

File trasferito mediante i protocolli HTTP, FTP o SMTP attraverso il firewall e inviato all'applicazione Kaspersky Lab per essere sottoposto a scansione.

OGGETTO PERICOLOSO

Oggetto contenente un virus. Si sconsiglia di accedere a questi oggetti perché ciò potrebbe determinare un'infezione del computer. Una volta rilevato un oggetto infetto, si consiglia di disinfettarlo tramite una delle applicazioni di Kaspersky Lab o di eliminarlo se non è possibile eseguire l'operazione.

OGGETTO POTENZIALMENTE INFETTABILE

Oggetto che, a causa della sua struttura o formato, può essere utilizzato dagli intrusi come "contenitore" per memorizzare e distribuire un oggetto dannoso. Solitamente, si tratta di file eseguibili, ad esempio file con estensione .com, .exe, .dll e così via. Il rischio di attivare codice dannoso in tali file è estremamente alto.

OGGETTO POTENZIALMENTE INFETTO

Oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. I file potenzialmente infetti vengono rilevati tramite l'analisi euristica.

OGGETTO SEMPLICE

Corpo del messaggio e-mail o semplici allegati, ad esempio, un file eseguibile. Vedere anche oggetti contenitore.

OGGETTO SOSPETTO

Oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. Gli oggetti sospetti vengono rilevati mediante l'analisi euristica.

P**PACCHETTO DI AGGIORNAMENTO**

Pacchetto di file per l'aggiornamento del software. Viene scaricato da Internet e installato nel computer.

PERIODO DI VALIDITÀ DELLA LICENZA

Periodo di tempo durante il quale è possibile utilizzare tutte le funzionalità dell'applicazione Kaspersky Lab. Questo livello viene impostato per essere utilizzato per impostazione predefinita. Livello di gravità dell'evento. Descrizione dell'evento, registrato durante il funzionamento dell'applicazione Kaspersky Lab. Non è possibile aggiornare i database dell'applicazione.

PROCESSO ATTENDIBILE

Processo dell'applicazione le cui operazioni sui file non vengono monitorate dall'applicazione di Kaspersky Lab in modalità di protezione in tempo reale. In altre parole, nessun oggetto eseguito, aperto o salvato dal processo considerato attendibile verrà esaminato.

PROTEZIONE IN TEMPO REALE

Modalità operativa dell'applicazione che consente di eseguire la scansione degli oggetti per verificare la presenza di codice dannoso in tempo reale.

Ogni programma elabora i dati ricevuti attraverso una determinata porta. Talvolta il programma viene definito "in ascolto" sulla porta. Gli oggetti non infetti vengono restituiti all'utente, quelli contenenti minacce o per i quali si sospetta la presenza di una minaccia vengono elaborati in base alle impostazioni dell'attività e quindi disinfettati, eliminati o messi in Quarantena.

PROTEZIONE MASSIMA

Livello di protezione per il computer corrispondente alla protezione più completa che l'applicazione è in grado di offrire. Con questo livello di protezione, tutti i file presenti sul computer, supporti rimovibili e unità di rete vengono sottoposti a una scansione anti-virus se collegati al computer.

Q**QUARANTENA**

Cartella nella quale vengono conservati tutti gli oggetti potenzialmente infetti rilevati durante le scansioni o la protezione in tempo reale.

R**RIPRISTINO**

Spostamento di un oggetto originale dalla sezione Quarantena o Backup alla cartella in cui era stato inizialmente trovato prima di essere disinfettato, eliminato, spostato nella Quarantena o in una cartella diversa specificata dall'utente.

S**SALTARE GLI OGGETTI**

Metodo di elaborazione in base al quale un oggetto viene passato all'utente senza alcuna modifica. Se la registrazione degli eventi è abilitata per questo tipo di evento, le informazioni sull'oggetto rilevato verranno registrate nel rapporto.

SCANSIONE ARCHIVIAZIONE

Scansione dei messaggi e-mail archiviati sul server di posta e il contenuto delle cartelle condivise utilizzando la versione più recente del database. La scansione viene eseguita in background e può essere eseguita utilizzando una pianificazione o su richiesta dell'utente. Vengono esaminate tutte le cartelle condivise e l'archivio delle caselle di posta.

Durante la scansione è possibile che vengano rilevati virus per i quali non erano disponibili informazioni nel database durante le scansioni precedenti.

SCANSIONE DEL TRAFFICO

La subnet mask (nota anche come netmask) e l'indirizzo di rete determinano gli indirizzi dei computer in una rete.

SCANSIONE MANUALE

Modalità operativa dell'applicazione di Kaspersky Lab avviata dall'utente in grado di gestire qualsiasi file presente sul computer.

SERVER DEGLI AGGIORNAMENTI DI KASPERSKY LAB

Elenco dei server HTTP e FTP di Kaspersky Lab da cui l'applicazione scarica database e aggiornamenti dei moduli nel computer.

SETTORE DI AVVIO DEL DISCO

Un settore di avvio è una determinata area sul disco rigido, su floppy o su altri dispositivi di memorizzazione dei dati del computer. Contiene informazioni sul file system del disco e un programma di caricamento responsabile dell'avvio del sistema operativo.

In particolare può anche memorizzare ed elaborare richieste inverse, determinando il nome di un host in base al relativo indirizzo IP (record PTR). L'applicazione Kaspersky Lab consente di esaminare i settori di avvio per verificare la presenza di virus e di disinfettarli se viene rilevata un'infezione.

SOGLIA DI ATTIVITÀ VIRUS

Livello massimo consentito per un tipo specifico di evento in un periodo di tempo limitato che, se superato, verrà considerato come attività eccessiva del virus e minaccia di un attacco di virus. Questa funzionalità è molto importante durante gli attacchi di virus e consente a un amministratore di reagire con tempestività alle minacce di attacchi che si presentano.

SPOSTAMENTO DI OGGETTI IN QUARANTENA

Metodo di elaborazione di un oggetto potenzialmente infetto attraverso il blocco dell'accesso al file e lo spostamento dalla posizione originale alla cartella Quarantena, in cui viene salvato in forma crittografata, in modo da eliminare la minaccia di infezione. Gli oggetti in quarantena possono essere esaminati utilizzando i database Anti-Virus aggiornati, analizzati dall'amministratore o inviati a Kaspersky Lab.

STATO DELLA PROTEZIONE

Stato corrente della protezione che indica il livello di sicurezza del computer.

T

TECNOLOGIA iCHECKER

iChecker è una tecnologia che consente di accelerare la scansione anti-virus escludendo gli oggetti che sono rimasti inalterati dall'ultima scansione, sempre che i parametri di scansione, ovvero le impostazioni e il database anti-virus, non siano stati modificati. Le informazioni di ogni file vengono memorizzate in un database speciale. Questa tecnologia viene utilizzata nelle modalità di protezione in tempo reale e di scansione manuale.

Si supponga, ad esempio, che a un archivio esaminato da Kaspersky Lab sia stato assegnato lo stato non infetto. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se il contenuto dell'archivio è stato modificato aggiungendo un nuovo oggetto, oppure sono state modificate le impostazioni di scansione o è stato aggiornato il database anti-virus, l'archivio verrà esaminato nuovamente.

Limitazioni della tecnologia iChecker:

questa tecnologia non rappresenta la scelta ideale con i file di grandi dimensioni in quanto risulta più veloce esaminare un file che controllare se sia stato modificato dall'ultima scansione;

la tecnologia supporta un numero limitato di formati (.exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

V**VIRUS DI BOOT**

Virus che infetta i settori di avvio dell'unità disco rigido di un computer. Il caricamento del virus all'interno del sistema viene forzato durante il riavvio dal virus stesso e il codice del virus assume il controllo diretto al posto del codice del programma di avvio originale.

VIRUS SCONOSCIUTO

Nuovo virus su cui non sono disponibili informazioni nei database. In genere i virus sconosciuti vengono rilevati dall'applicazione negli oggetti mediante l'analisi euristica e tali oggetti vengono classificati come potenzialmente infetti.

KASPERSKY LAB

Fondata nel 1997 Kaspersky Lab rappresenta oggi una delle aziende leader nello sviluppo di una vasta gamma di prodotti software ad elevate prestazioni destinati alla protezione delle informazioni, tra cui sistemi anti-virus, anti-spam e anti-hacking.

Kaspersky Lab è una società internazionale. La sede centrale si trova nella Federazione russa e gli uffici di rappresentanza sono nel Regno Unito, in Francia, Germania, Giappone, nei paesi del Benelux, in Cina, Polonia, Romania e negli USA (California). Recentemente è stata inaugurata una nuova sede, l'European Anti-Virus Research Centre, in Francia. La rete di partner di Kaspersky Lab è costituita da oltre 500 aziende in tutto il mondo.

Degli oltre 1000 specialisti qualificati che lavorano presso Kaspersky Lab, 10 hanno conseguito un Master di specializzazione post laurea in Business Administration e 16 un dottorato di ricerca. Tutti gli esperti anti-virus Kaspersky Lab senior sono membri dell'organizzazione CARO (Computer Anti-Virus Researchers Organization).

I punti di forza dell'azienda sono la notevole competenza e la significativa esperienza maturata in quattordici di anni di intensa attività di sviluppo di efficaci soluzioni anti-virus. Un'analisi approfondita delle attività dei virus informatici consente agli specialisti dell'azienda di anticipare le tendenze nello sviluppo di malware e di offrire agli utenti una protezione efficace e tempestiva contro nuovi tipi di attacchi. Questo vantaggio sta alla base dei prodotti e dei servizi offerti da Kaspersky Lab. I prodotti dell'azienda sono sempre un passo avanti rispetto a quelli della concorrenza nell'ambito della protezione anti-virus.

L'esperienza maturata in anni di duro lavoro hanno rafforzato nel tempo la posizione dominante raggiunta oggi. Kaspersky Lab è stata la prima azienda a sviluppare molti degli standard per software anti-virus moderni. Il prodotto di punta, Kaspersky Anti-Virus®, protegge in modo efficace tutti i tipi di sistemi dagli attacchi dei virus, incluse le workstation, i file server, i sistemi di posta, i firewall, i gateway Internet e i computer palmari. Gli strumenti di facile gestione di cui è fornito consentono di automatizzare la protezione anti-virus di computer e reti aziendali. Un gran numero di sviluppatori di fama internazionale utilizza il kernel di Kaspersky Anti-Virus nei propri prodotti, inclusi Nokia ICG (USA), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

I clienti di Kaspersky Lab possono usufruire di una vasta gamma di servizi aggiuntivi che garantiscono il funzionamento costante dei prodotti e una compatibilità completa con i propri requisiti specifici. L'azienda progetta, implementa e supporta sistemi anti-virus aziendali. Il database anti-virus di Kaspersky Lab viene aggiornato ogni ora. Il servizio di supporto tecnico offerto ai clienti è disponibile 24 ore su 24, in diverse lingue.

Per porre domande, fare commenti o ricevere consigli, è possibile contattarci tramite i rivenditori o direttamente presso Kaspersky Lab. Tutta l'assistenza necessaria in relazione alle questioni sollevate sui prodotti Kaspersky verrà fornita tramite telefono o posta elettronica. Viene sempre garantita una risposta completa e dettagliata a qualsiasi domanda.

Sito ufficiale di Kaspersky Lab: <http://www.kaspersky.it>

Enciclopedia dei Virus: <http://www.viruslist.com>

Anti-Virus Lab: newvirus@kaspersky.com

(solo per l'invio di archivi di oggetti sospetti)

<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en>

(per domande agli analisti anti-virus)

CONTRATTO DI LICENZA

CONTRATTO DI LICENZA CON L'UTENTE FINALE KASPERSKY LAB

AVVERTENZA LEGALE IMPORTANTE PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO PRIMA DI INIZIARE A USARE IL SOFTWARE.

FACENDO CLIC SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O IMMETTENDO IL/ SIMBOLO/I CORRISPONDENTE/I, LEI ACCETTA DI ESSERE VINCOLATO AL RISPETTO DEI TERMINI E DELLE CONDIZIONI DI QUESTO CONTRATTO. **TALE AZIONE EQUIVALE AD APPORRE LA SUA FIRMA E SIGNIFICA CHE ACCETTA DI ESSERE VINCOLATO E DI DIVENTARE UNA PARTE CONTRAENTE DEL PRESENTE CONTRATTO E CHE ACCETTA LA VALIDITÀ LEGALE DEL PRESENTE CONTRATTO COME QUALSIASI ACCORDO STIPULATO PER ISCRITTO E DA LEI FIRMATO.** SE NON È D'ACCORDO CON TUTTI I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO, ANNULLI L'INSTALLAZIONE DEL SOFTWARE E NON LO INSTALLI.

IL SOFTWARE PUÒ ESSERE ACCOMPAGNATO DA UN CONTRATTO AGGIUNTIVO O DOCUMENTO SIMILARE (IL "CONTRATTO AGGIUNTIVO") CHE PUÒ STABILIRE IL NUMERO DI COMPUTER SUI QUALI IL SOFTWARE PUÒ ESSERE USATO, IL PERIODO DI UTILIZZO DEL SOFTWARE, I TIPI DI OGGETTI PER I QUALI IL SOFTWARE È STATO CREATO E ALTRI TERMINI DI ACQUISTO, ACQUISIZIONE E USO AGGIUNTIVI. TALE CONTRATTO AGGIUNTIVO COSTITUISCE PARTE INTEGRANTE DEL CONTRATTO DI LICENZA.

DOPO AVER CLICCATO IL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O DOPO AVER IMMESSO IL/ SIMBOLO/I CORRISPONDENTE/I LEI HA IL DIRITTO DI USARE IL SOFTWARE SECONDO I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO.

1. Definizioni

- 1.1. **Per Software** si intende il software, compresi gli aggiornamenti e i relativi materiali.
- 1.2. **Per Titolare** (titolare di tutti i diritti, sia esclusivi che non, relativi al Software) si intende Kaspersky Lab ZAO, una società regolarmente costituita ai sensi delle leggi della Federazione Russa.
- 1.3. **Per Computer** si intende l'hardware, ivi compresi i personal computer, i laptop, le postazioni di lavoro, i personal digital assistant, gli "smart phone", i dispositivi palmari o gli altri dispositivi elettronici per cui il Software è stato progettato su cui il Software verrà installato e/o utilizzato.
- 1.4. **Per Utente Finale (Lei/Suo)** si intende il soggetto o i soggetti che installano o utilizzano il Software per proprio conto e che sta/stanno utilizzando legalmente una copia del Software; o, se il Software è stato scaricato o installato per conto di un'organizzazione, ad esempio da un dipendente, "*Lei*" sta a intendere anche l'organizzazione per cui il Software è stato scaricato o installato e si dichiara con il presente che tale organizzazione ha autorizzato quel soggetto ad accettare questo contratto, scaricando e installando il Software per conto dell'organizzazione stessa. Ai fini del presente contratto il termine "*organizzazione*" include, a titolo esemplificativo e non limitativo, qualsiasi società di persone, società a responsabilità limitata, persona giuridica, associazione, società per azioni, trust, joint venture, organizzazione sindacale, organizzazione non registrata o autorità governativa.
- 1.5. **Per Partner** si intendono le organizzazioni o il soggetto/i soggetti che distribuiscono il Software al Titolare sulla base di un contratto e di una licenza.
- 1.6. **Per Aggiornamento/i** si intendono tutti gli aggiornamenti, le revisioni, le patch, i perfezionamenti, le correzioni, le modifiche, le copie, le aggiunte o i pacchetti di manutenzione, ecc.
- 1.7. **Per Manuale dell'Utente** si intende il manuale dell'utente, la guida per l'amministratore, il libro di riferimento e i relativi materiali di tipo illustrativo o di altro tipo.
- 1.8. **Per Acquisizione del Software** si intende l'acquisto del Software o l'acquisizione del Software secondo i termini definiti nel contratto aggiuntivo, ivi compresa l'acquisizione gratuita.

2. Concessione della licenza

- 2.1. Con il presente il Titolare Le concede licenza di uso non esclusivo per la memorizzazione, il caricamento, l'installazione, l'esecuzione e la visualizzazione (l'"uso") del Software su di una quantità specificata di Computer al fine di fornire un supporto per la protezione del Suo Computer, sul quale è installato il Software, contro le minacce descritte nel Manuale dell'Utente, in osservanza di tutti i requisiti tecnici descritti nel Manuale dell'Utente e secondo i termini e le condizioni di questo Contratto (la "Licenza") e Lei accetta questa Licenza:

Versione di prova. Se ha ricevuto, scaricato e/o installato la versione di prova del Software e se ha aderito alla licenza di valutazione del Software, può utilizzare il Software solo a scopo dimostrativo e soltanto per il periodo dimostrativo consentito, salvo laddove diversamente indicato, a partire dalla data della prima installazione. È severamente proibito l'uso del Software per scopi diversi o per un periodo più lungo del periodo di valutazione consentito.

Software per ambiente multiplo; Software a linguaggio multiplo; Software a doppio supporto magnetico; Copie multiple; Servizi aggiuntivi. Qualora Lei utilizzi diverse versioni del Software o edizioni del Software di lingua diversa, o riceva il Software su diversi supporti magnetici, o comunque riceva copie multiple del Software, ovvero qualora in cui Lei abbia acquistato il Software insieme a software aggiuntivi, il numero massimo di Computer su cui il Software può essere installato equivale al numero di computer specificati nelle licenze ricevute dal Titolare *sempre che* ogni licenza acquisita Le dia diritto a installare e utilizzare il Software sulla quantità numero di Computer specificata nei paragrafi 2.2 e 2.3, salvo laddove diversamente stabilito dai termini della licenza.

- 2.2. Se il Software è stato acquisito su un supporto fisico, Lei ha il diritto di utilizzare il Software per proteggere la quantità di Computer specificata nel pacchetto Software o come specificato nel contratto aggiuntivo.
- 2.3. Se il Software è stato acquisito via Internet, Lei ha il diritto di utilizzare il Software per la protezione della quantità di Computer specificata all'atto dell'acquisizione della Licenza del Software o come specificato nel contratto aggiuntivo.
- 2.4. Lei ha diritto di copiare il Software soltanto a scopo di back-up e solo a titolo di sostituzione della copia di Sua legale proprietà, qualora essa vada persa, distrutta o diventi inutilizzabile. Questa copia di back-up non può essere utilizzata per fini diversi e deve essere distrutta quando viene meno il diritto d'uso del Software o alla scadenza della Sua licenza o qualora questa venga meno per qualsiasi altro motivo, ai sensi dalla legislazione in vigore nel principale paese di residenza o nel paese in cui Lei fa uso del Software.
- 2.5. Dal momento in cui si procede all'attivazione del Software o dopo l'installazione del file della chiave di licenza (a eccezione della versione di prova del Software), Lei ha diritto di ricevere i seguenti servizi per il periodo di tempo specificato sul pacchetto Software (se il Software è stato acquisito su supporto fisico) o specificato durante l'acquisizione (se il Software è stato acquisito via Internet):
- Aggiornamenti del Software via Internet quando e nel momento in cui il Titolare li pubblica sul suo sito o attraverso altri servizi online. Qualsiasi Aggiornamento di cui Lei possa essere destinatario costituisce parte del Software e a esso si applicano i termini e le condizioni di questo Contratto;
 - Supporto Tecnico via Internet e Hotline telefonica di Supporto Tecnico.

3. **Attivazione e validità**

- 3.1. Nel caso in cui Lei apportasse modifiche al Suo computer o al software di altri fornitori installato su di esso, il Titolare ha la facoltà di chiederLe di ripetere l'attivazione del Software o l'installazione del file della chiave di licenza. Il Titolare si riserva il diritto di utilizzare qualsiasi mezzo e qualsiasi procedura per verificare la validità della Licenza e/o la validità legale della copia del Software installata e/o utilizzata sul Suo Computer.
- 3.2. Se il Software è stato acquisito su supporto fisico, esso può essere utilizzato previa accettazione del presente Contratto per il periodo specificato sulla confezione a far data dalla data di accettazione del presente Contratto o come specificato nel contratto aggiuntivo.
- 3.3. Se il Software è stato acquisito via Internet, il Software può essere utilizzato previa accettazione del presente Contratto per il periodo specificato durante l'acquisizione o come specificato nel contratto aggiuntivo.
- 3.4. Lei ha diritto di usare la versione di prova del Software secondo quanto disposto dal Paragrafo 2.1 senza alcun addebito unicamente per il periodo di valutazione (30 giorni) concesso dal momento della sua attivazione ai sensi del presente Contratto, *purché* la versione di prova non dia diritto ad Aggiornamenti e a Supporto Tecnico via Internet e tramite Hotline telefonica.

- 3.5. La Sua Licenza d'Uso del Software è limitata al periodo di tempo specificato nei Paragrafi 3.2 o 3.3 (secondo quanto applicabile) e nel periodo restante può essere visionata utilizzando i supporti descritti nel Manuale dell'Utente.
- 3.6. Nel caso in cui Lei abbia acquisito il Software per un utilizzo su più di un Computer, la Sua Licenza d'Uso del Software è limitata al periodo di tempo che ha inizio alla data di attivazione del Software o l'installazione del file della chiave di licenza sul primo Computer.
- 3.7. Fatto salvo qualsiasi altro rimedio previsto dalla legge o basato sui principi di opportunità, giustizia e onesta composizione ("equity") a cui il Titolare possa legittimamente fare ricorso, nel caso di una Sua violazione dei termini e delle condizioni del presente Contratto, il Titolare avrà diritto in ogni momento e senza obbligo di preavviso di rescindere questa Licenza d'uso del Software senza rimborsare il prezzo d'acquisto né parte di esso.
- 3.8. Lei accetta di fare uso del Software e utilizzare qualsiasi rapporto o informazione derivante dall'utilizzo di questo Software in modo conforme a tutte le leggi applicabili internazionali, nazionali, statali, regionali e locali e a qualsiasi normativa, ivi compresa, a titolo esemplificativo e non limitativo, le leggi sulla privacy, sui diritti d'autore, sul controllo delle esportazioni e sulle oscenità.
- 3.9. Fatte salve eventuali disposizioni contrarie specificamente previste in questa sede, Lei non ha la facoltà di trasferire né di assegnare alcuno dei diritti che le sono stati concessi ai sensi del presente Contratto né alcuno degli obblighi che da esso Le derivano.

4. Supporto Tecnico

Il Supporto Tecnico descritto al Paragrafo 2.5 del presente Contratto Le viene fornito quando è stato installato l'Aggiornamento più recente del Software (a eccezione della versione di prova del Software). Servizio di assistenza tecnica: <http://support.kaspersky.com>

5. Restrizioni

- 5.1. Le è fatto divieto di emulare, clonare, locare, dare in prestito, noleggiare, vendere, modificare, decompilare o reingegnerizzare il Software, disassemblarlo o creare opere accessorie basate sul Software o su una porzione di esso con la sola eccezione di diritti non rinunciabili previsti dalla legislazione applicabile, e Le è fatto comunque divieto di ridurre parte del Software in forma decifrabile o trasferire il Software tutelato da licenza o qualsivoglia sottoinsieme dello stesso, o permettere a terzi di fare quanto sopra, salvo nella misura in cui le limitazioni sopra illustrate siano espressamente proibite dal diritto applicabile. È fatto divieto di utilizzare o reingegnerizzare qualsivoglia codice binario o origine del Software allo scopo di ricreare l'algoritmo del programma, che è proprietario. Tutti i diritti non espressamente concessi attraverso il presente Contratto sono riservati al Titolare e/o ai suoi fornitori, secondo quanto applicabile. L'uso non autorizzato del Software produrrà la rescissione immediata e automatica del presente Contratto e della Licenza concessa in virtù dello stesso e può determinare l'apertura di un procedimento legale nei Suoi confronti.
- 5.2. Fatto salvo quanto disposto nel contratto aggiuntivo, Lei non ha diritto di trasferire i diritti d'uso del Software a terzi.
- 5.3. Le è fatto divieto di mettere a conoscenza di terzi il codice di attivazione e/o il file chiave della licenza o di consentire l'accesso al codice di attivazione e/o di licenza, i quali rappresentano dati riservati del Titolare; Lei sarà inoltre tenuta a usare ogni ragionevole cautela per la protezione del codice di attivazione e/o di licenza riservati, qualora Lei abbia la facoltà di trasferire il codice di attivazione e/o di licenza a terzi secondo quanto illustrato nel contratto aggiuntivo.
- 5.4. Non è consentito concedere a noleggio, in locazione o in prestito a terzi il Software.
- 5.5. Non è consentito utilizzare il Software per la creazione di dati o di software che servono a individuare, bloccare o gestire le minacce descritte nel Manuale dell'Utente.
- 5.6. In caso di violazione dei termini e delle condizioni del presente Contratto, il Titolare ha il diritto di bloccare il file di codice o di annullare la Sua licenza d'uso del Software senza obbligo di rimborso.
- 5.7. Se si usa la versione di prova del Software non si ha il diritto di ricevere il Supporto Tecnico specificato al Paragrafo 4 del presente Contratto, né il diritto di trasferire la licenza o i diritti d'uso del software a terzi.

6. Garanzia limitata e clausola di esclusione della responsabilità

- 6.1. Il Titolare garantisce che il Software eseguirà sostanzialmente le prestazioni illustrate nelle specifiche e descritte nel Manuale dell'Utente *fermo restando, tuttavia, che* tale garanzia limitata non si applica a quanto segue: (w) lacune del Suo Computer e relative violazioni per le quali il Titolare declina espressamente qualsiasi responsabilità di garanzia; (x) malfunzionamenti, difetti o guasti conseguenti a cattivo uso, abuso, incidente, negligenza, difetti di installazione, funzionamento o manutenzione, furto, atto vandalico, evento di forza maggiore, atti di terrorismo, interruzione di tensione o momentanea sovratensione, infortunio, alterazione, modifica non consentita o riparazioni eseguite da soggetti diversi dal Titolare o qualsiasi azione o causa, a opera Sua o di qualsiasi altro soggetto terzo, ragionevolmente fuori del controllo del Titolare; (y) qualsiasi difetto da Lei tenuto nascosto al Titolare anche dopo la comparsa della prima anomalia; e (z) incompatibilità provocata da componenti hardware e/o software installati sul Suo computer.
- 6.2. Lei riconosce, accetta e concorda che nessun software è esente da errori e che Lei è stato informato che è necessario fare il back-up del Computer, con la frequenza e secondo le modalità per Lei più indicate.
- 6.3. In caso di violazione dei termini descritti nel Manuale dell'Utente o nel presente Contratto, il Titolare non garantisce il corretto funzionamento del Software.
- 6.4. Il Titolare non garantisce che il Software funzionerà correttamente se Lei non scarica regolarmente gli Aggiornamenti specificati nel Paragrafo 2.5 del presente Contratto.
- 6.5. Il Titolare non garantisce la protezione dalle minacce descritte nel Manuale dell'Utente una volta scaduto il periodo specificato nei Paragrafi 3.2 or 3.3 del presente Contratto o una volta scaduta, per qualsiasi motivo, la Licenza d'uso del Software.
- 6.6. IL SOFTWARE VIENE FORNITO "COSÌ COM'È" E IL TITOLARE NON FA ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA IN QUANTO A USO O PRESTAZIONI. FATTE SALVE LE GARANZIE, LE CONDIZIONI, LE DICHIARAZIONI O I TERMINI CHE NON POSSONO ESSERE ESCLUSI O LIMITATI DAL DIRITTO APPLICABILE, IL TITOLARE E I SUOI PARTNER, NON FORNISCONO ALCUNA GARANZIA, CONDIZIONE, DICHIARAZIONE O TERMINE (NÉ ESPLICITO NÉ IMPLICITI NÉ PREVISTO DALLA LEGGE, DALLA *COMMON LAW*, DALLE CONSUETUDINI O DAGLI USI O ALTRO) IN MERITO A QUALSIVOGLIA QUESTIONE, IVI COMPRESA, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, LA NON VIOLAZIONE DEI DIRITTI DI TERZI, LA COMMERCIALIZZABILITÀ, LA QUALITÀ SODDISFACENTE, L'INTEGRAZIONE O L'APPLICABILITÀ PER UN FINE SPECIFICO. LEI SI ASSUME LA RESPONSABILITÀ DI TUTTI GLI ERRORI E TUTTI I RISCHI RELATIVI ALLE PRESTAZIONI NONCHÉ LA RESPONSABILITÀ DI AVER SCELTO IL SOFTWARE ALLO SCOPO DI RAGGIUNGERE I RISULTATI DESIDERATI NONCHÉ DELL'INSTALLAZIONE DEL SOFTWARE, DEL RELATIVO USO E DEI RISULTATI OTTENUTI DALL'ISTESSO. SENZA LIMITARE LE DISPOSIZIONI DI CUI SOPRA, IL TITOLARE NON FORNISCE ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA CHE IL SOFTWARE SARÀ ESENTE DA ERRORI O ESENTE DA INTERRUZIONI O ALTRI DIFETTI DI FUNZIONAMENTO NÉ CHE IL SOFTWARE SARÀ IN GRADO DI SODDISFARE IN TOTO O IN PARTE LE SUE ESIGENZE, SIANO ESSE STATE COMUNICATE AL TITOLARE O MENO.

7. Esclusione e limite della responsabilità

NELLA MASSIMA MISURA CONSENTITA DAL DIRITTO APPLICABILE, IN NESSUN CASO IL TITOLARE O I SUOI PARTNER SARANNO RESPONSABILI DI DANNI SPECIALI, MARGINALI, PUNITIVI, INDIRETTI O DI DANNI INDIRETTI DI QUALSIASI TIPO (IVI COMPRESI, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, I DANNI PER PERDITA DI UTILI O PER PERDITA DI INFORMAZIONI RISERVATE O DI ALTRE INFORMAZIONI, PER INTERRUZIONE DELL'ATTIVITÀ LAVORATIVA, PER PERDITA DI PRIVACY, PER CORRUZIONE, DANNO E PERDITA DI DATI O DI PROGRAMMI, PER MANCATA OSSERVANZA DI UN OBBLIGO IVI COMPRESO QUALSIASI ONERE IMPOSTO PER LEGGE, DOVERE DI BUONA FEDE O DOVERE DI RAGIONEVOLE DILIGENZA, PER NEGLIGENZA, PER PERDITA ECONOMICA E PER QUALSIASI ALTRA PERDITA PECUNIARIA O ALTRA PERDITA DI SORTA) DERIVANTE DA O IN QUALSIASI MODO COLLEGATO ALL'USO O ALL'IMPOSSIBILITÀ DI USARE IL SOFTWARE, ALLA FORNITURA O MANCATA FORNITURA DEL SERVIZIO DI SUPPORTO O DI ALTRI SERVIZI, INFORMAZIONI, SOFTWARE E RELATIVI CONTENUTI ATTRAVERSO IL SOFTWARE O COMUNQUE DERIVANTI DALL'USO DEL SOFTWARE O COMUNQUE AI SENSI O IN RELAZIONE A QUALSIASI DISPOSIZIONE DEL PRESENTE CONTRATTO, O DERIVANTI DA UNA VIOLAZIONE DEL PRESENTE CONTRATTO O DA QUALSIVOGLIA ILLECITO (IVI COMPRESA LA NEGLIGENZA, LA FALSA TESTIMONIANZA, QUALSIASI OBBLIGO O DOVERE RELATIVI ALLA RESPONSABILITÀ) O DA UNA VIOLAZIONE DI UN OBBLIGO DI LEGGE O DA UNA VIOLAZIONE DELLA GARANZIA DA PARTE DEL TITOLARE O DI UNO DEI SUOI PARTNER, ANCHE QUALORA IL TITOLARE O UNO DEI SUOI PARTNER SIA STATO INFORMATO DELLA POSSIBILITÀ DI TALI DANNI.

LEI ACCETTA CHE NEL CASO IN CUI IL TITOLARE E/O SUOI PARTNER VENISSE TROVATI RESPONSABILI, LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER SI LIMITERÀ AL COSTO DEL SOFTWARE. IN NESSUN CASO LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER POTRÀ SUPERARE LE SOMME VERSATE PER IL SOFTWARE AL TITOLARE O AL PARTNER (SECONDO QUANTO APPLICABILE).

NULLA IN QUESTO CONTRATTO ESCLUDE O LIMITA LA QUALSIVOGLIA RICHIESTA DI DANNI IN CASO DI MORTE E LESIONI PERSONALI. INOLTRE IN CASO IN CUI UNA MANLEVA, ESCLUSIONE O LIMITAZIONE CONTEMPLATE DAL PRESENTE CONTRATTO NON POSSA ESSERE ESCLUSA O LIMITATA AI SENSI DEL DIRITTO APPLICABILE, QUELLA MANLEVA, ESCLUSIONE O LIMITAZIONE NON SARÀ VALIDA NEI SUOI CONFRONTI E LEI DOVRÀ CONTINUARE A OSSERVARE TUTTE LE RESTANTI MANLEVE, ESCLUSIONI E LIMITAZIONI.

8. GNU e altre licenze di Terzi

Il Software può comprendere alcuni programmi software sottoposti a licenza (o a sublicenza) dell'utente ai sensi della GNU Licenza Pubblica Generica (General Public License, GPL) o ad altra licenza software di analoga natura che, tra gli altri, concede all'utente il diritto di copiare, modificare e ridistribuire certi programmi o porzioni di essi e di avere accesso al codice source ("Software Open Source"). Se tali licenze prevedono che per un software distribuito in formato binario eseguibile anche il codice source venga reso disponibile ai suoi utenti, il codice source deve essere reso accessibile inviando la richiesta all'indirizzo source@kaspersky.com, altrimenti il codice source verrà fornito insieme al Software. Se le licenze dei Software Open Source prevedono che il Titolare fornisca diritti d'uso, di copia e modifica del programma Software Open Source più ampi dei diritti concessi in virtù del presente Contratto, tali diritti avranno la priorità sui diritti e sulle restrizioni contemplati da questo documento.

9. Proprietà Intellettuale

- 9.1 Lei accetta che il Software e il fatto di esserne autori, i sistemi, le idee e i metodi operativi, la documentazione e altre informazioni contenute nel Software, sono proprietà intellettuale esclusiva e/o preziosi segreti commerciali del Titolare o dei suoi partner e che il Titolare e i suoi partner, secondo quanto applicabile, sono protetti dal diritto civile e penale e dalla legge sul copyright, sul segreto commerciale, sul marchio di fabbrica e sui brevetti della Federazione Russa, dell'Unione Europea e degli Stati Uniti e da altri trattati internazionali o di altri paesi. Il presente Contratto non Le concede alcun diritto di proprietà intellettuale né alcun diritto sui marchi o sui marchi di servizio del Titolare e/o dei suoi partner ("Marchi di fabbrica"). Lei ha la facoltà di usare i marchi di fabbrica solo nella misura in cui essi permettono di identificare le stampe prodotte dal Software in conformità con la pratica sui marchi generalmente accettata, ivi compresa l'identificazione del nome del proprietario del Marchio di fabbrica. Tale uso di un Marchio di fabbrica non Le conferisce alcun diritto di proprietà sul Marchio stesso. Il Titolare e/o i relativi partner possiedono e conservano ogni diritto, titolo e interesse relativo e collegato al Software, ivi comprese, senza alcuna limitazione, le correzioni d'errore, i perfezionamenti, gli Aggiornamenti o altre modifiche del Software, sia apportate dal Titolare che da Terzi nonché tutti i diritti d'autore, i brevetti, i diritti su segreti commerciali, i marchi di fabbrica e qualsiasi altro diritto di proprietà intellettuale ivi contemplato. Il possesso, l'installazione o l'uso del Software da parte Sua non Le trasferisce alcun titolo nella proprietà intellettuale del Software e Lei non acquisirà alcun diritto sul Software, salvo nella misura espressamente indicata nel presente Contratto. Tutte le copie del Software eseguite ai sensi del presente documento devono contenere le stesse avvertenze proprietarie che compaiono sul e nel Software. Fatto salvo quanto disposto in questo documento, il presente Contratto non Le conferisce alcun diritto di proprietà intellettuale sul Software e Lei riconosce che la Licenza, secondo la definizione data in seguito, concessa ai sensi del presente Contratto Le conferisce soltanto il diritto di uso limitato ai termini e alle condizioni del presente Contratto. Il Titolare si riserva tutti i diritti che non Le sono espressamente concessi ai sensi del presente Contratto.
- 9.2 Lei riconosce che il codice source, il codice di attivazione e/o il file di codice di licenza per il Software sono proprietari del Titolare e che essi costituiscono segreto commerciale del Titolare. Lei accetta di non modificare, adattare, reingegnerizzare, decompilare, disassemblare, né comunque tentare di scoprire il codice source del Software.
- 9.3 Lei accetta di non modificare, né alterare in alcun modo il Software. Lei non ha la facoltà di rimuovere, né di alterare alcuna delle avvertenze in materia di diritti d'autore o altre avvertenze proprietarie sulle copie del Software.

10. Diritto applicabile; Arbitrato

Il presente Contratto sarà regolamentato dalle leggi della Federazione Russa e interpretato conformemente a esse, senza riferimento a conflitti fra stato di diritto e principi. Il presente Contratto non sarà regolamentato dalla Convenzione delle Nazioni Unite sui Contratti per la Vendita Internazionale di Merci, la cui applicazione è espressamente esclusa. Qualsiasi vertenza derivante dall'interpretazione o dall'applicazione dei termini del presente Contratto o dalla sua violazione dovrà essere regolata tramite trattativa diretta oppure dal Tribunale dell'Arbitrato Commerciale Internazionale avente sede presso la Camera di Commercio e dell'Industria della Federazione Russa di Mosca, Federazione Russa. Qualsiasi lodo arbitrale emesso dall'arbitro sarà definitivo e vincolante per le parti e qualsiasi giudizio su tale lodo può essere fatto valere in ogni foro competente. Nulla nel presente Paragrafo 10 può impedire a una delle Parti di ricercare e ottenere equo indennizzo presso un foro competente, sia prima, durante sia dopo il processo d'arbitrato.

11. Periodo di validità per la presentazione di azioni legali

A prescindere dalla forma, nessuna azione derivante dalle transazioni commerciali eseguite ai sensi del presente Contratto può essere presentata dalle due parti contrattuali a più di un (1) anno dal momento in cui è accaduto o si è scoperto che è accaduto l'evento su cui si basa l'azione, tranne in caso di azioni per violazione dei diritti di proprietà intellettuale, che possono essere presentate entro il periodo massimo applicabile secondo i termini di legge.

12. Totalità del Contratto; Clausola salvatoria; Assenza di deroga

Il presente Contratto costituisce l'intero contratto tra Lei e il Titolare e sostituisce ogni altro accordo, proposta, comunicato o comunicato commerciale precedente, sia verbale che scritto, relativo al Software o relativo al presente Contratto. Lei riconosce di aver letto il presente Contratto, lo comprende e accetta di essere vincolato ai suoi termini e condizioni. Se un foro competente giudica una qualsiasi disposizione del presente Contratto non valida, nulla o per qualsiasi motivo non applicabile, *in toto* o in parte, tale disposizione sarà riformulata più precisamente per renderla legittima e applicabile; ciò tuttavia non inficerà il Contratto e le rimanenti disposizioni del Contratto resteranno pienamente valide e in vigore nella massima misura consentita dalla legge diritto o dall'equity, conservando quanto più possibile il loro intento originale. Non varrà alcuna deroga a disposizioni o a condizioni del presente Contratto, a meno che la deroga non sia presentata per iscritto e firmata da Lei e da rappresentante autorizzato del Titolare, purché nessuna deroga a una violazione di una disposizione del presente Contratto valga come una deroga a qualsiasi violazione precedente, concorrente o successiva. La mancata insistenza da parte del Titolare nel richiedere la stretta applicazione di qualsiasi disposizione del presente Contratto o nel far valere un diritto non potrà essere interpretata quale deroga a tale disposizione o rinuncia a tale diritto.

13. Informazioni di contatto del Titolare

Per qualsiasi domanda relativa al presente Contratto, o se si desidera consultare per qualsiasi motivo il Titolare, si prega di contattare il nostro Servizio Clienti presso:

Kaspersky Lab ZAO, 10 edificio 1 1st Volokolamsky Proezd
Mosca, 123060
Federazione Russa

Tel: +7-495-797-8700
Fax: +7-495-645-7939

E-mail: info@kaspersky.com

Sito Web: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Tutti i diritti riservati. Il Software e la documentazione d'accompagnamento sono soggetti a diritto d'autore e sono protetti dalle leggi sul copyright e dai trattati internazionali sul copyright nonché da altre leggi e trattati in materia di proprietà intellettuale.

INDICE

A

Aggiornamento	
da una cartella locale	67
impostazioni internazionali	64
in base alla pianificazione	66
manuale	62
modalità di esecuzione	65, 66
oggetti da aggiornare	66
origine degli aggiornamenti	63
rollback dell'ultimo aggiornamento	63
utilizzo di un server proxy	64
Algoritmo di funzionamento	
Anti-Virus File	39
Ambito di protezione	
Anti-Virus File	41
Analisi euristica	
Anti-Virus File	42
Anti-Virus File	
algoritmo di funzionamento	39
ambito di protezione	41
analisi euristica	42
livello di protezione	40
modalità di scansione	44
ottimizzazione della scansione	43
reazione alle minacce	40
scansione dei file composti	43, 44
sospensione	45, 46
statistiche sul funzionamento del componente	47
tecnologia di scansione	45
Area attendibile	
applicazioni attendibili	74, 77
regole di esclusione	74, 75
Auto-difesa dell'applicazione	82
Avvio attività	
scansione	50, 58, 59
Avvio dell'attività	
aggiornamento	62, 65, 66
Azioni da eseguire sugli oggetti	40

B

Backup	89, 90
--------------	--------

C

Categorie di minacce rilevabili	74
---------------------------------------	----

D

Disco di Ripristino	90, 91, 93
---------------------------	------------

F

File iSwift	83
Finestra principale dell'applicazione	35

I

Icona dell'area di notifica della barra delle applicazioni	33
--	----

Interfaccia dell'applicazione	33
K	
Kaspersky Lab	10
L	
Limitazione dell'accesso all'applicazione	82
Livello di protezione	
Anti-Virus File	40
M	
Menu di scelta rapida	34
N	
Notifiche	84
Q	
Quarantena	88, 89, 90
Quarantena e backup	88, 89
R	
Rapporto	87, 88
Reazione alle minacce	
Anti-Virus File	40
scansione anti-virus	53
Ripristino delle impostazioni predefinite	46
S	
Scansione	
avvio automatico dell'attività ignorata	57, 58
azione da eseguire in caso di oggetto rilevato	53
in base alla pianificazione	58
livello di protezione	52
modalità di esecuzione	58
ottimizzazione della scansione	54
scansione dei file compositi	55
sospensione dell'attività	57, 58
tecnologie di scansione	56
tipo di oggetti da esaminare	54
Statistiche sul funzionamento del componente	
Anti-Virus File	47