

Kaspersky Anti-Virus 2012

KASPERSKY **Anti-Virus**

Manuale dell'utente

VERSIONE PROGRAMMA: 12.0

Gentile utente,

grazie per aver scelto il nostro prodotto. Ci auguriamo che questa documentazione sia utile e fornisca risposte esaustive a gran parte delle domande relative al prodotto.

Attenzione! Il presente documento è di proprietà di Kaspersky Lab ZAO (di seguito denominata Kaspersky Lab): tutti i diritti relativi al documento sono riservati dalle leggi sui diritti d'autore e dalle disposizioni dei trattati internazionali. La riproduzione e la distribuzione non autorizzate del presente documento, interamente o in parte, possono comportare gravi responsabilità civili, amministrative e penali, in conformità alle leggi applicabili.

Qualsiasi riproduzione o distribuzione del materiale, incluse le traduzioni, è consentita solo previa autorizzazione scritta concessa da Kaspersky Lab.

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

È possibile che vengano apportate modifiche al documento senza notifiche. La versione più recente del documento è disponibile sul sito Kaspersky Lab, all'indirizzo <http://www.kaspersky.com/it/docs>.

Kaspersky Lab non si assume responsabilità per il contenuto, la qualità, la pertinenza o la precisione del materiale utilizzato in questo documento i cui diritti appartengono a terze parti o per eventuali danni potenziali associati al loro utilizzo.

In questo documento sono presenti marchi registrati e marchi di servizi che appartengono ai rispettivi proprietari.

Data di revisione del documento: 4/15/2011

© 1997-2011 Kaspersky Lab ZAO. Tutti i diritti riservati.

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

CONTENUTO

INFORMAZIONI SULLA GUIDA	8
Contenuto della documentazione	8
Convenzioni utilizzate nella documentazione	9
FONTI DI INFORMAZIONI SULL'APPLICAZIONE	11
Fonti di informazioni per le ricerche in autonomia	11
Discussione delle applicazioni Kaspersky Lab nel forum	12
Come contattare l'ufficio vendite	12
Come contattare il team di sviluppo della documentazione tramite posta elettronica	12
KASPERSKY ANTI-VIRUS	13
Novità	13
Kit di distribuzione	13
Servizi per gli utenti registrati	14
Requisiti hardware e software	14
INSTALLAZIONE E RIMOZIONE DELL'APPLICAZIONE	15
Procedura di installazione standard	15
Passaggio 1. Ricerca di una versione più recente dell'applicazione	16
Passaggio 2. Verifica dei requisiti di installazione	16
Passaggio 3. Scelta del tipo di installazione	16
Passaggio 4. Visualizzazione del contratto di licenza	16
Passaggio 5. Informativa sulla raccolta dei dati per Kaspersky Security Network	17
Passaggio 6. Ricerca di applicazioni incompatibili	17
Passaggio 7. Selezione della cartella di destinazione	17
Passaggio 8. Preparazione per l'installazione	18
Passaggio 9. Installazione	18
Passaggio 10. Completamento dell'installazione	18
Passaggio 11. Attivazione dell'applicazione	18
Passaggio 12. Registrazione di un utente	19
Passaggio 13. Completamento dell'attivazione	19
Aggiornamento della versione precedente di Kaspersky Anti-Virus	19
Passaggio 1. Ricerca di una versione più recente dell'applicazione	20
Passaggio 2. Verifica dei requisiti di installazione	20
Passaggio 3. Scelta del tipo di installazione	20
Passaggio 4. Visualizzazione del contratto di licenza	21
Passaggio 5. Informativa sulla raccolta dei dati per Kaspersky Security Network	21
Passaggio 6. Ricerca di applicazioni incompatibili	21
Passaggio 7. Selezione della cartella di destinazione	21
Passaggio 8. Preparazione per l'installazione	22
Passaggio 9. Installazione	22
Passaggio 10. Termine della procedura guidata	22
Scenari di installazione non standard	23
Operazioni preliminari	23
Rimozione dell'applicazione.	23
Passaggio 1. Salvataggio dei dati per il riutilizzo	24
Passaggio 2. Conferma della rimozione dell'applicazione	24
Passaggio 3. Rimozione dell'applicazione. Completamento della rimozione	24
LICENSING DELL'APPLICAZIONE	25
Informazioni sul Contratto di licenza con l'utente finale	25
Informazioni sulla trasmissione dei dati	25
Informazioni sulla licenza	25
Informazioni sul codice di attivazione	26

INTERFACCIA DELL'APPLICAZIONE	27
Icona nell'area di notifica	27
Menu di scelta rapida	28
Finestra principale di Kaspersky Anti-Virus	29
Finestre di notifica e messaggi a comparsa.....	30
Finestra delle impostazioni dell'applicazione	31
Kaspersky Gadget.....	32
News Agent	32
AVVIO E ARRESTO DELL'APPLICAZIONE	34
Abilitazione e disabilitazione dell'avvio automatico.....	34
Avvio e chiusura manuale dell'applicazione	34
GESTIONE DELLA PROTEZIONE DEL COMPUTER.....	35
Diagnostica ed eliminazione dei problemi relativi alla protezione del computer	35
Abilitazione e disabilitazione della protezione.....	35
Sospensione e ripresa della protezione.....	36
ESECUZIONE DELLE ATTIVITÀ PIÙ COMUNI	38
Attivazione dell'applicazione	38
Acquisto o rinnovo della licenza	39
Come procedere quando vengono visualizzate le notifiche dell'applicazione.....	40
Aggiornamento dei database e dei moduli dell'applicazione	40
Esecuzione di una scansione virus delle aree critiche del computer	40
Scansione virus di file, cartelle, dischi o altri oggetti.....	41
Esecuzione di una scansione virus completa del computer.....	42
Ricerca delle vulnerabilità del computer	42
Protezione dei dati personali dal furto	43
Protezione dal phishing.....	43
Protezione dall'intercettazione dei dati immessi tramite la tastiera	43
Come procedere se si sospetta che un oggetto sia infetto	44
Come procedere se si sospetta che il computer sia infetto.....	45
Ripristino di un file eliminato o disinfettato dall'applicazione.....	46
Creazione e utilizzo di un Rescue Disk	46
Creazione di un Rescue Disk.....	47
Avvio del computer dal Rescue Disk.....	48
Visualizzazione del rapporto sull'esecuzione dell'applicazione.....	49
Ripristino delle impostazioni predefinite dell'applicazione	49
Trasferimento delle impostazioni di Kaspersky Anti-Virus in un altro computer.....	50
Passaggio da Kaspersky Anti-Virus a Kaspersky Internet Security	50
Passaggio alla versione commerciale	51
Passaggio temporaneo alla versione di prova	51
Utilizzo di Kaspersky Gadget.....	53
Come ottenere informazioni sulla reputazione di un'applicazione	54
IMPOSTAZIONI AVANZATE DELL'APPLICAZIONE	55
Impostazioni generali di protezione	55
Restrizione dell'accesso a Kaspersky Anti-Virus	56
Selezione di una modalità di protezione	56
Scansione.....	56
Scansione virus.....	57
Scansione Vulnerabilità	63
Gestione delle attività di scansione. Gestione attività	63
Aggiornamento	64
Selezione della sorgente degli aggiornamenti.....	64
Creazione della pianificazione di avvio degli aggiornamenti	66
Rollback dell'ultimo aggiornamento.....	67
Esecuzione di aggiornamenti tramite un altro account utente.....	67
Utilizzo di un server proxy	67

Anti-Virus File	68
Abilitazione e disabilitazione di Anti-Virus File	68
Sospensione automatica di Anti-Virus File.....	69
Creazione dell'ambito di protezione di Anti-Virus File	69
Modifica e ripristino del livello di protezione dei file.....	70
Selezione della modalità di scansione	70
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus File	71
Selezione di una tecnologia di scansione dei file	71
Modifica dell'azione da eseguire sui file infetti	71
Scansione dei file compositi tramite Anti-Virus File.....	72
Ottimizzazione della scansione dei file	72
Anti-Virus Posta.....	73
Abilitazione e disabilitazione di Anti-Virus Posta.....	74
Creazione dell'ambito di protezione di Anti-Virus Posta.....	74
Modifica e ripristino del livello di protezione dei messaggi e-mail	75
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus Posta.....	75
Modifica dell'azione da eseguire sui messaggi e-mail infetti	75
Filtro degli allegati nei messaggi e-mail	76
Scansione dei file compositi tramite Anti-Virus Posta	76
Scansione della posta elettronica in Microsoft Office Outlook	76
Scansione della posta elettronica in The Bat!	77
Anti-Virus Web.....	77
Abilitazione e disabilitazione di Anti-Virus Web.....	78
Modifica e ripristino del livello di protezione del traffico Web	78
Modifica dell'azione da eseguire sugli oggetti pericolosi dal traffico Web	79
Controllo delle URL nelle pagine Web	79
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus Web.....	81
Blocco degli script pericolosi	81
Ottimizzazione della scansione	82
Creazione di un elenco di indirizzi attendibili.....	82
Anti-Virus IM.....	82
Abilitazione e disabilitazione di Anti-Virus IM.....	83
Creazione dell'ambito di protezione di Anti-Virus IM.....	83
Controllo delle URL nei messaggi dai client IM.....	83
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus IM.....	84
Difesa Proattiva	84
Abilitazione e disabilitazione di Difesa Proattiva	84
Creazione di un gruppo di applicazioni attendibili	85
Utilizzo dell'elenco di attività pericolose	85
Modifica dell'azione da eseguire sulle attività pericolose delle applicazioni	85
Controllo sistema.....	86
Abilitazione e disabilitazione di Controllo sistema.....	86
Utilizzo degli schemi di attività pericolose (BSS).....	86
Rollback delle azioni di un programma dannoso.....	87
Protezione della rete.....	87
Scansione delle connessioni crittografate	88
Configurazione del server proxy	90
Creazione di un elenco di porte monitorate	90
Area attendibile.....	91
Creazione di un elenco di applicazioni attendibili.....	92
Creazione di regole di esclusione	92
Prestazioni e compatibilità con altre applicazioni.....	92
Selezione delle categorie di minacce rilevabili	93
Risparmio energetico	93
Disinfezione avanzata	93
Allocazione delle risorse del computer durante la scansione virus	94

Esecuzione di attività in background.....	94
Modalità a schermo intero. Profilo Gioco	95
Auto-Difesa di Kaspersky Anti-Virus.....	95
Abilitazione e disabilitazione dell'auto-difesa	96
Protezione dal controllo esterno.....	96
Quarantena e Backup.....	96
Archiviazione dei file in quarantena e backup	97
Utilizzo dei file in quarantena	97
Utilizzo degli oggetti nell'archivio Backup.....	98
Scansione dei file in quarantena dopo un aggiornamento	99
Strumenti aggiuntivi per una migliore protezione del computer	99
Eliminazione della cronologia delle attività.....	100
Configurazione di un browser in modalità protetta	101
Rollback delle modifiche apportate dalle procedure guidate	102
Rapporti.....	103
Creazione di un rapporto per il componente di protezione selezionato.....	103
Filtro dei dati	104
Ricerca di eventi	104
Salvataggio di un rapporto in un file.....	105
Archiviazione dei rapporti.....	105
Cancellazione dei rapporti dell'applicazione	106
Registrazione degli eventi non critici nel rapporto.....	106
Configurare la notifica della disponibilità dei rapporti	106
Aspetto dell'applicazione. Gestione degli elementi attivi dell'interfaccia	106
Trasparenza delle finestre di notifica	107
Animazione dell'icona dell'applicazione nell'area di notifica	107
Testo nella schermata di accesso di Microsoft Windows	107
Notifiche.....	107
Abilitazione e disabilitazione delle notifiche	108
Configurazione del metodo di notifica	108
Disabilitazione dell'invio delle notizie	109
Kaspersky Security Network.....	109
Abilitazione e disabilitazione della partecipazione a Kaspersky Security Network.....	109
Verifica della connessione a Kaspersky Security Network.....	110
TESTING DEL FUNZIONAMENTO DELL'APPLICAZIONE	111
Informazioni sul file di prova EICAR	111
Testing dell'applicazione tramite il file di prova EICAR.....	111
Informazioni sui tipi di file di prova EICAR	112
COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA.....	114
Come ottenere assistenza tecnica.....	114
Utilizzo del file di traccia e dello script AVZ	114
Creazione di un rapporto sullo stato del sistema	115
Creazione di un file di traccia	115
Invio dei file di dati	115
Esecuzione di uno script con AVZ	116
Assistenza tecnica telefonica.....	116
Come ottenere assistenza tecnica tramite la Pagina personale	116
APPENDICE	118
Utilizzo dell'applicazione dalla riga di comando.....	118
Attivazione dell'applicazione	119
Avvio dell'applicazione	119
Arresto dell'applicazione	119
Gestione dei componenti e delle attività dell'applicazione	120
Scansione virus.....	121
Aggiornamento dell'applicazione.....	123

Rollback dell'ultimo aggiornamento.....	124
Esportazione delle impostazioni di protezione	124
Importazione delle impostazioni di protezione	125
Creazione di un file di traccia	125
Visualizzazione della Guida	126
Codici restituiti della riga di comando.....	126
Elenco delle notifiche di Kaspersky Anti-Virus.....	127
Notifiche in qualsiasi modalità di protezione	127
Notifiche nella modalità di protezione interattiva	131
GLOSSARIO	138
KASPERSKY LAB ZAO	147
INFORMAZIONI SUL CODICE DI TERZE PARTI	148
INDICE	149

INFORMAZIONI SULLA GUIDA

Grazie per avere scelto i prodotti Kaspersky Lab.

La presente documentazione contiene informazioni sull'installazione, la configurazione e l'utilizzo di Kaspersky Anti-Virus. Ci auguriamo che le informazioni disponibili consentano un utilizzo ottimale dell'applicazione.

Gli obiettivi della presente documentazione sono:

- agevolare l'installazione, l'attivazione e l'utilizzo di Kaspersky Anti-Virus;
- consentire di cercare rapidamente informazioni sui problemi relativi all'applicazione;
- descrivere ulteriori fonti di informazioni sull'applicazione e modalità per collaborare con il Servizio di Assistenza tecnica.

Per un utilizzo corretto dell'applicazione, sono necessarie le seguenti competenze informatiche di base: avere familiarità con l'interfaccia del sistema operativo in uso, conoscere le principali procedure relative a tale sistema e conoscere le modalità di utilizzo della posta elettronica e di Internet.

IN QUESTA SEZIONE:

Contenuto della documentazione.....	8
Convenzioni utilizzate nella documentazione.....	9

CONTENUTO DELLA DOCUMENTAZIONE

La presente documentazione comprende le seguenti sezioni.

Fonti di informazioni sull'applicazione

In questa sezione sono descritte le fonti di informazioni sull'applicazione e sono elencati alcuni siti Web che è possibile utilizzare per discutere del funzionamento dell'applicazione.

Kaspersky Anti-Virus

In questa sezione sono descritte le funzionalità dell'applicazione e viene fornita una breve descrizione delle funzioni e dei componenti dell'applicazione. Sono illustrati gli elementi inclusi nel kit di distribuzione e i servizi disponibili per gli utenti registrati dell'applicazione. Vengono inoltre fornite informazioni sui requisiti software e hardware che un computer deve soddisfare per consentire l'installazione dell'applicazione.

Installazione e rimozione dell'applicazione

In questa sezione vengono fornite informazioni sull'installazione e la disinstallazione dell'applicazione.

Licensing dell'applicazione

In questa sezione vengono fornite informazioni sulle condizioni generali relative all'attivazione dell'applicazione. Vengono descritti lo scopo del contratto di licenza, i tipi di licenza, le modalità di attivazione dell'applicazione e il rinnovo della licenza.

Interfaccia dell'applicazione

In questa sezione vengono fornite informazioni sugli elementi di base dell'interfaccia grafica dell'applicazione: icona dell'applicazione e menu di scelta rapida dell'icona dell'applicazione, finestra principale, finestra delle impostazioni e finestre di notifica.

Avvio e arresto dell'applicazione

In questa sezione sono disponibili informazioni sull'avvio e l'arresto dell'applicazione.

Gestione della protezione del computer

In questa sezione sono fornite informazioni sul rilevamento delle minacce per la protezione del computer e sulla configurazione del livello di protezione. Viene descritto come abilitare, disabilitare e sospendere la protezione durante l'utilizzo dell'applicazione.

Esecuzione delle attività più comuni

In questa sezione vengono fornite informazioni sulla risoluzione dei problemi più comuni relativi alla protezione del computer tramite l'applicazione.

Impostazioni avanzate dell'applicazione

In questa sezione vengono fornite informazioni dettagliate sulla configurazione di ognuno dei componenti dell'applicazione.

Testing del funzionamento dell'applicazione

In questa sezione vengono fornite informazioni su come verificare che l'applicazione rilevi i virus e le relative varianti ed esegua le azioni corrette in caso di rilevamento.

Come contattare il Servizio di Assistenza tecnica

In questa sezione vengono fornite informazioni su come contattare il Servizio di Assistenza tecnica di Kaspersky Lab.

Appendice

In questa sezione vengono fornite informazioni che completano il testo della documentazione.

Glossario

In questa sezione sono disponibili un elenco dei termini utilizzati nella documentazione e le relative definizioni.

Kaspersky Lab ZAO

In questa sezione vengono fornite informazioni su Kaspersky Lab.

Informazioni sul codice di terze parti

In questa sezione vengono fornite informazioni sul codice di terze parti utilizzato nell'applicazione.

Indice

Questa sezione consente di trovare rapidamente le informazioni desiderate all'interno della documentazione.

CONVENZIONI UTILIZZATE NELLA DOCUMENTAZIONE

Il testo della presente documentazione contiene elementi semantici a cui è necessario prestare particolare attenzione: avvisi, suggerimenti ed esempi.

Per evidenziare tali elementi semantici vengono utilizzate particolari convenzioni. Le convenzioni utilizzate nella documentazione e i relativi esempi di utilizzo sono riportati nella tabella seguente.

Tabella 1. Convenzioni utilizzate nella documentazione

TESTO DI ESEMPIO	DESCRIZIONE DELLA CONVENZIONE
Si noti che...	Il testo degli avvisi è in rosso e racchiuso da un riquadro. Gli avvisi forniscono informazioni su azioni potenzialmente indesiderate che possono provocare la perdita di dati o un malfunzionamento del computer.
È consigliabile utilizzare...	Il testo delle note è racchiuso da un riquadro. Le note possono contenere suggerimenti utili, raccomandazioni, specifici valori o particolari situazioni relative all'utilizzo dell'applicazione.

TESTO DI ESEMPIO	DESCRIZIONE DELLA CONVENZIONE
<p>Esempio:</p> <p>...</p>	<p>Gli esempi sono riportati su sfondo giallo e sotto l'intestazione "Esempio".</p>
<p><i>Aggiornamento</i> significa...</p> <p>Si verifica l'evento <i>I database non sono aggiornati</i>.</p>	<p>I seguenti elementi semantici sono in corsivo nel testo:</p> <ul style="list-style-type: none"> • nuovi termini; • nomi di stati ed eventi dell'applicazione.
<p>Premere INVIO.</p> <p>Premere ALT+F4.</p>	<p>I nomi dei tasti sono contrassegnati dalla formattazione in grassetto e in lettere maiuscole.</p> <p>I nomi dei tasti uniti da un segno più (+) indicano una combinazione di tasti. Tali tasti devono essere premuti contemporaneamente.</p>
<p>Fare click sul pulsante Abilita.</p>	<p>I nomi degli elementi di interfaccia dell'applicazione, come campi di immissione, voci di menu e pulsanti, sono in grassetto.</p>
<p>➡ <i>Per configurare la pianificazione per un'attività:</i></p>	<p>Le frasi introduttive delle istruzioni sono in corsivo e contrassegnate da una freccia.</p>
<p>Immettere <code>help</code> nella riga di comando.</p> <p>Verrà visualizzato il seguente messaggio:</p> <p><code>Specificare la data nel formato gg:mm:aa.</code></p>	<p>I seguenti tipi di testo sono visualizzati con uno speciale carattere:</p> <ul style="list-style-type: none"> • testo della riga di comando; • testo dei messaggi visualizzati sullo schermo dall'applicazione; • dati che devono essere immessi dall'utente.
<p><code><Indirizzo IP del computer></code></p>	<p>Le variabili sono racchiuse tra parentesi angolari. Al posto di una variabile deve essere immesso il valore corrispondente, senza le parentesi angolari.</p>

FONTI DI INFORMAZIONI SULL'APPLICAZIONE

In questa sezione sono descritte le fonti di informazioni sull'applicazione e sono elencati alcuni siti Web che è possibile utilizzare per discutere del funzionamento dell'applicazione.

È possibile scegliere le risorse più adatte in base all'urgenza e all'importanza del quesito.

IN QUESTA SEZIONE:

Fonti di informazioni per le ricerche in autonomia	11
Discussione delle applicazioni Kaspersky Lab nel forum	12
Come contattare l'ufficio vendite	12
Come contattare il team di sviluppo della documentazione tramite posta elettronica	12

FONTI DI INFORMAZIONI PER LE RICERCHE IN AUTONOMIA

È possibile utilizzare le seguenti risorse per trovare informazioni sull'applicazione:

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

Se non è possibile risolvere autonomamente un problema, è consigliabile contattare il Servizio di Assistenza tecnica di Kaspersky Lab (vedere la sezione "Assistenza tecnica telefonica" a pagina [116](#)).

Per utilizzare le fonti di informazioni nel sito Kaspersky Lab, è necessaria una connessione a Internet.

Pagina dell'applicazione nel sito Kaspersky Lab

Il sito Kaspersky Lab contiene una singola pagina per ogni applicazione.

In tale pagina (http://www.kaspersky.com/it/kaspersky_anti-virus) è possibile visualizzare informazioni generali su un'applicazione e le relative funzioni e caratteristiche.

La pagina <http://www.kaspersky.com/it/> include un link Compra online per l'accesso al negozio online. Tramite il negozio online è possibile acquistare o rinnovare la licenza dell'applicazione.

Pagina dell'applicazione nel sito Web del Servizio di Assistenza tecnica (Knowledge Base)

La Knowledge Base è una sezione del sito Web del Servizio di Assistenza tecnica che fornisce raccomandazioni sull'utilizzo delle applicazioni Kaspersky Lab. La Knowledge Base comprende articoli di riferimento raggruppati per argomento.

Nella pagina dell'applicazione nella Knowledge Base (<http://support.kaspersky.com/kav2012>) è possibile leggere articoli che forniscono informazioni utili, raccomandazioni e risposte alle domande frequenti sull'acquisto, l'installazione e l'utilizzo dell'applicazione.

Gli articoli possono fornire risposte a domande non solo su Anti-Virus, ma anche correlate ad altre applicazioni Kaspersky Lab. Possono inoltre essere disponibili notizie dal Servizio di Assistenza tecnica.

Guida in linea

La guida in linea dell'applicazione comprende diversi file.

La guida sensibile al contesto fornisce informazioni su ogni finestra dell'applicazione, con un elenco e una descrizione delle relative impostazioni e attività.

La guida completa fornisce informazioni dettagliate sulla gestione della protezione del computer tramite l'applicazione.

Documentazione

Il manuale dell'utente fornisce informazioni sull'installazione, l'attivazione e la configurazione dell'applicazione, nonché sui dati operativi dell'applicazione. Vengono inoltre descritti l'interfaccia dell'applicazione e i metodi di esecuzione delle attività più frequenti da parte dell'utente durante l'utilizzo dell'applicazione.

DISCUSSIONE DELLE APPLICAZIONI KASPERSKY LAB NEL FORUM

Se la domanda non richiede una risposta urgente, è possibile sottoporla agli specialisti di Kaspersky Lab e ad altri utenti nei Forum Kaspersky all'indirizzo <http://forum.kaspersky.com/index.php?showforum=63>.

In questo forum è possibile visualizzare gli argomenti esistenti, lasciare i propri commenti e creare nuovi argomenti.

COME CONTATTARE L'UFFICIO VENDITE

In caso di domande sulla scelta, l'acquisto o il rinnovo dell'applicazione, è possibile contattare gli specialisti del reparto vendite di Kaspersky Lab in uno dei seguenti modi:

- Telefonicamente (<http://www.kaspersky.com/it/contacts>).
- Inviando un messaggio con la propria domanda tramite e-mail a sales.consumer@it.kaspersky.com.

COME CONTATTARE IL TEAM DI SVILUPPO DELLA DOCUMENTAZIONE TRAMITE POSTA ELETTRONICA

Per contattare il team di sviluppo della documentazione, è possibile inviare un e-mail: docfeedback@kaspersky.com. Specificare "Kaspersky Help Feedback: Kaspersky Anti-Virus" come oggetto del messaggio.

KASPERSKY ANTI-VIRUS

In questa sezione sono descritte le funzionalità dell'applicazione e viene fornita una breve descrizione delle funzioni e dei componenti dell'applicazione. Sono illustrati gli elementi inclusi nel kit di distribuzione e i servizi disponibili per gli utenti registrati dell'applicazione. Vengono inoltre fornite informazioni sui requisiti software e hardware che un computer deve soddisfare per consentire l'installazione dell'applicazione.

IN QUESTA SEZIONE:

Novità	13
Kit di distribuzione	13
Servizi per gli utenti registrati	14
Requisiti hardware e software	14

NOVITÀ

Kaspersky Anti-Virus fornisce le seguenti nuove funzionalità:

- L'interfaccia migliorata della finestra principale di Kaspersky Anti-Virus consente di accedere rapidamente alle funzioni dell'applicazione.
- Sono stati apportati miglioramenti alla logica delle funzionalità Quarantena e Backup (vedere pagina [96](#)): ora le funzionalità sono disponibili in due schede separate, ognuna con un ambito specifico.
- È stata aggiunta la funzione Gestione attività, che semplifica la gestione delle attività in Kaspersky Anti-Virus (vedere la sezione "Gestione delle attività di scansione. Gestione attività" a pagina [63](#)).
- La partecipazione a Kaspersky Security Network (vedere pagina [109](#)) consente a Kaspersky Lab di identificare la reputazione delle applicazioni e dei siti Web in base ai dati ricevuti da utenti di tutto il mondo.
- Quando Anti-Virus Web è abilitato, è possibile abilitare separatamente l'analisi euristica per il controllo delle URL di phishing nelle pagine Web (vedere la sezione "Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus Web" a pagina [81](#)). Durante il controllo delle URL di phishing nelle pagine Web, verrà applicata l'analisi euristica indipendentemente dal fatto che sia stata abilitata per Anti-Virus Web.
- L'aspetto del Kaspersky Gadget è stato riprogettato (vedere pagina [32](#)).

KIT DI DISTRIBUZIONE

È possibile acquistare l'applicazione in uno dei seguenti modi:

- **Nella versione in scatola.** Distribuito tramite i negozi dei partner di Kaspersky Lab.
- **Dal negozio online.** Distribuito dai negozi online di Kaspersky Lab (ad esempio, <http://www.kaspersky.com/it>, sezione **Compra online**) o da aziende partner.

Se si acquista la versione in scatola dell'applicazione, il kit di distribuzione contiene i seguenti elementi:

- busta sigillata con il CD di installazione che include i file dell'applicazione e della documentazione;
- manuale dell'utente con il codice di attivazione;
- Contratto di licenza, in cui sono specificate le condizioni per l'utilizzo dell'applicazione.

Il contenuto del kit di distribuzione può variare a seconda dell'area geografica in cui viene distribuita l'applicazione.

In caso di acquisto di Kaspersky Anti-Virus da un negozio online, l'applicazione viene scaricata dal sito Web del negozio. Le informazioni necessarie per l'attivazione dell'applicazione verranno inviate tramite e-mail una volta effettuato il pagamento.

Per ulteriori informazioni sulle modalità di acquisto e sul kit di distribuzione, contattare il reparto vendite.

SERVIZI PER GLI UTENTI REGISTRATI

Acquistando una licenza per l'applicazione, si diventa utenti registrati delle applicazioni Kaspersky Lab ed è possibile usufruire dei seguenti servizi per il periodo di validità della licenza:

- aggiornamento dei database e disponibilità delle nuove versioni dell'applicazione;
- assistenza telefonica e tramite e-mail per i problemi relativi all'installazione, la configurazione e l'utilizzo dell'applicazione;
- ricezione di notifiche relative al rilascio di nuove applicazioni Kaspersky Lab e ai nuovi virus. Per utilizzare questo servizio, è necessario eseguire la sottoscrizione alle notizie inviate da Kaspersky Lab sul sito Web del Servizio di Assistenza tecnica.

Non vengono forniti servizi di consulenza per i problemi relativi al funzionamento dei sistemi operativi o al software e le tecnologie di terze parti.

REQUISITI HARDWARE E SOFTWARE

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

Requisiti generali:

- 480 MB di spazio libero sul disco rigido (inclusi 380 MB nell'unità di sistema).
- Unità CD/DVD-ROM (per installare Kaspersky Anti-Virus dal CD di distribuzione).
- Accesso a Internet (per l'attivazione dell'applicazione e per l'aggiornamento dei database e dei moduli software).
- Microsoft Internet Explorer 6.0 o versione successiva.
- Microsoft Windows Installer 2.0.

Requisiti per Microsoft Windows XP Home Edition (Service Pack 2 o versione successiva), Microsoft Windows XP Professional (Service Pack 2 o versione successiva) e Microsoft Windows XP Professional x64 Edition (Service Pack 2 o versione successiva):

- processore Intel Pentium da 800 MHz a 32 bit (x86) / a 64 bit (x64) o superiore (o un processore equivalente compatibile);
- 512 MB di RAM disponibile.

Requisiti per Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional e Microsoft Windows 7 Ultimate:

- processore Intel Pentium da 1 GHz a 32 bit (x86) / a 64 bit (x64) o superiore (o un processore equivalente compatibile).
- 1 GB di RAM disponibile (per i sistemi operativi a 32 bit); 2 GB di RAM disponibile (per i sistemi operativi a 64 bit).

Requisiti per i netbook:

- Processore Intel Atom da 1,6 GHz o un processore equivalente compatibile.
- Scheda video Intel GMA950 con almeno 64 MB di RAM video (o scheda equivalente compatibile).
- Dimensione dello schermo non inferiore a 10,1 pollici.

INSTALLAZIONE E RIMOZIONE DELL'APPLICAZIONE

In questa sezione vengono fornite informazioni sull'installazione e la disinstallazione dell'applicazione.

IN QUESTA SEZIONE:

Procedura di installazione standard	15
Aggiornamento della versione precedente di Kaspersky Anti-Virus	19
Scenari di installazione non standard.....	23
Operazioni preliminari	23
Rimozione dell'applicazione.	23

PROCEDURA DI INSTALLAZIONE STANDARD

Kaspersky Anti-Virus viene installato nel computer in modalità interattiva tramite l'Installazione guidata.

La procedura guidata comprende una serie di schermate (passaggi), tra cui è possibile spostarsi utilizzando i pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, fare click sul pulsante **Annulla**.

Se l'applicazione protegge più di un computer (il numero massimo di computer dipende dalla licenza), verrà installata nello stesso modo in tutti i computer. In questo caso, in base al contratto di licenza, il periodo di validità della licenza ha inizio dalla data della prima attivazione. Quando si attiva l'applicazione su un secondo computer, il periodo di validità della licenza viene ridotto della quantità di tempo trascorso dalla prima attivazione. Di conseguenza, il periodo di validità della licenza scade contemporaneamente per tutte le copie installate dell'applicazione.

► *Per installare Kaspersky Anti-Virus nel computer:*

Eseguire il file di installazione (con estensione *EXE) dal CD del prodotto.

Il processo per l'installazione di Kaspersky Anti-Virus da un file di installazione scaricato da Internet è identico a quello per l'installazione da CD.

IN QUESTA SEZIONE:

Passaggio 1. Ricerca di una versione più recente dell'applicazione	16
Passaggio 2. Verifica dei requisiti di installazione	16
Passaggio 3. Scelta del tipo di installazione.....	16
Passaggio 4. Visualizzazione del contratto di licenza	16
Passaggio 5. Informativa sulla raccolta dei dati per Kaspersky Security Network.....	17
Passaggio 6. Ricerca di applicazioni incompatibili	17
Passaggio 7. Selezione della cartella di destinazione	17
Passaggio 8. Preparazione per l'installazione	18
Passaggio 9. Installazione.....	18
Passaggio 10. Completamento dell'installazione	18
Passaggio 11. Attivazione dell'applicazione.....	18
Passaggio 12. Registrazione di un utente	19
Passaggio 13. Completamento dell'attivazione.....	19

PASSAGGIO 1. RICERCA DI UNA VERSIONE PIÙ RECENTE DELL'APPLICAZIONE

Prima dell'installazione, il programma di installazione controlla se nei server degli aggiornamenti di Kaspersky Lab è disponibile una nuova versione di Kaspersky Anti-Virus.

Se non vengono trovate nuove versioni nei server degli aggiornamenti di Kaspersky Lab, verrà avviata l'installazione guidata per la versione corrente.

Se nei server degli aggiornamenti è disponibile una nuova versione di Kaspersky Anti-Virus, verrà richiesto se scaricarla e installarla nel computer. È consigliabile installare la nuova versione dell'applicazione, perché le versioni più recenti includono miglioramenti che assicurano una protezione più affidabile del computer. Se si annulla il download della nuova versione, verrà avviata l'installazione guidata per la versione corrente. Se si sceglie di installare la nuova versione, i file di distribuzione del prodotto verranno scaricati nel computer e verrà avviata automaticamente l'installazione guidata per la nuova versione. Per una descrizione della procedura di installazione per la nuova versione, fare riferimento alla documentazione corrispondente.

PASSAGGIO 2. VERIFICA DEI REQUISITI DI INSTALLAZIONE

Prima dell'installazione di Kaspersky Anti-Virus nel computer, il programma di installazione esamina il sistema operativo e i service pack installati per verificare che soddisfino i requisiti software per l'installazione del prodotto (vedere la sezione "Requisiti hardware e software" a pagina [14](#)). Inoltre, il programma di installazione verifica la presenza del software richiesto e delle credenziali necessarie per l'installazione delle applicazioni. Se uno dei requisiti elencati in precedenza non è soddisfatto, verrà visualizzata una notifica.

Se il computer soddisfa tutti i requisiti, la procedura guidata esegue una ricerca delle applicazioni Kaspersky Lab che possono determinare conflitti con Kaspersky Anti-Virus. Se vengono rilevate applicazioni di questo tipo, viene offerta la possibilità di rimuoverle manualmente.

Se viene rilevata una versione precedente di Kaspersky Anti-Virus o Kaspersky Internet Security, tutti i dati utilizzabili in Kaspersky Anti-Virus 2012 (ad esempio, informazioni di attivazione o impostazioni dell'applicazione) verranno salvati e utilizzati per l'installazione della nuova applicazione, mentre quella installata in precedenza sarà automaticamente rimossa.

PASSAGGIO 3. SCELTA DEL TIPO DI INSTALLAZIONE

In questa fase è possibile scegliere il tipo di installazione di Kaspersky Anti-Virus più adatto per le proprie esigenze:

- *Installazione standard.* Se si seleziona questa opzione (la casella **Modifica impostazioni di installazione** è deselezionata), l'applicazione verrà installata nel computer con le impostazioni di protezione consigliate dagli esperti di Kaspersky Lab.
- *Installazione personalizzata.* In questo caso (la casella **Modifica impostazioni di installazione** è selezionata), verrà richiesto di specificare la cartella di destinazione in cui installare l'applicazione (vedere la sezione "Passaggio 7. Selezione della cartella di destinazione" a pagina [17](#)) e disabilitare la protezione del processo di installazione, se necessario (vedere la sezione "Passaggio 8. Preparazione dell'installazione" a pagina [18](#)).

Per continuare l'installazione, fare click sul pulsante **Avanti**.

PASSAGGIO 4. VISUALIZZAZIONE DEL CONTRATTO DI LICENZA

In questa fase è necessario esaminare il contratto di licenza tra l'utente e Kaspersky Lab.

Leggere attentamente il contratto di licenza e, se si accettano tutte le condizioni, fare click sul pulsante **Accetto**. L'installazione proseguirà.

Se non si desidera accettare il contratto di licenza, annullare l'installazione dell'applicazione facendo click sul pulsante **Annulla**.

PASSAGGIO 5. INFORMATIVA SULLA RACCOLTA DEI DATI PER KASPERSKY SECURITY NETWORK

In questa fase, viene offerta la possibilità di partecipare a Kaspersky Security Network. La partecipazione al programma implica l'invio a Kaspersky Lab di informazioni sul sistema in uso e di dati sulle nuove minacce rilevate nel computer, sulle applicazioni in esecuzione o sulle applicazioni con firma digitale scaricate. Le informazioni trasmesse non includono dati personali.

Leggere l'Informativa sulla raccolta dei dati di Kaspersky Security Network. Per leggere la versione completa dell'informativa, fare click sul pulsante **Contratto completo KSN**. Se si accettano tutte le condizioni dell'informativa, selezionare la casella **Accetto le condizioni di adesione al programma Kaspersky Security Network** nella finestra della procedura guidata.

Fare click sul pulsante **Avanti** se è stata eseguita l'installazione personalizzata (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)). Per eseguire l'installazione standard, fare click sul pulsante **Installa**. L'installazione proseguirà.

PASSAGGIO 6. RICERCA DI APPLICAZIONI INCOMPATIBILI

Durante questo passaggio, viene verificato se nel computer sono installate applicazioni incompatibili con Kaspersky Anti-Virus.

Se non vengono rilevate applicazioni di questo tipo, la procedura guidata procede automaticamente al passaggio successivo.

Se vengono rilevate applicazioni incompatibili, queste sono visualizzate in un elenco e viene richiesto all'utente se desidera rimuoverle. Le applicazioni che non vengono rimosse automaticamente da Kaspersky Anti-Virus devono essere rimosse manualmente. Durante la rimozione delle applicazioni incompatibili, sarà necessario riavviare il sistema. Dopo il riavvio, l'installazione di Kaspersky Anti-Virus continuerà automaticamente.

Per continuare l'installazione, fare click sul pulsante **Avanti**.

PASSAGGIO 7. SELEZIONE DELLA CARTELLA DI DESTINAZIONE

Questo passaggio dell'installazione guidata è disponibile solo se è stata selezionata l'installazione personalizzata (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)). Durante l'installazione standard, il passaggio viene saltato e l'applicazione è installata nella cartella predefinita.

In questa fase viene richiesto di scegliere la cartella in cui installare Kaspersky Anti-Virus. Per impostazione predefinita, viene utilizzato il seguente percorso:

- <unità>\Programmi\Kaspersky Lab\Kaspersky Anti-Virus 2012 – per i sistemi a 32 bit;
- <unità>\Programmi (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012 – per i sistemi a 64 bit;

Per installare Kaspersky Anti-Virus in una cartella differente, specificare il percorso desiderato nel campo di immissione o fare click su **Sfogli** e scegliere la cartella nella finestra visualizzata.

Tenere presente le seguenti limitazioni:

- L'applicazione non può essere installata in unità di rete o rimovibili oppure in unità virtuali (create attraverso il comando `SUBST`).
- È consigliabile evitare di installare l'applicazione in una cartella che contiene già file o altre cartelle, perché la cartella risulterà inaccessibile per la modifica.
- Il percorso della cartella di installazione non può avere una lunghezza superiore a 160 caratteri o contenere i caratteri speciali `/, ?, :, *, ", >, < o |`

Per controllare lo spazio libero su disco per l'installazione dell'applicazione, fare click sul pulsante **Utilizzo disco**. Nella finestra visualizzata sono riportate le informazioni sullo spazio su disco. Per chiudere la finestra, fare click su **OK**.

Per procedere con l'installazione, fare click su **Avanti** nella finestra della procedura guidata.

PASSAGGIO 8. PREPARAZIONE PER L'INSTALLAZIONE

Questo passaggio dell'installazione guidata è disponibile solo se è stata selezionata l'installazione personalizzata (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)). Nel caso dell'installazione standard, il passaggio viene saltato.

Poiché il computer potrebbe essere infetto da programmi dannosi che possono influire sull'installazione di Kaspersky Anti-Virus, è necessario proteggere il processo di installazione.

Per impostazione predefinita, la protezione del processo di installazione è abilitata: la casella **Proteggi il processo di installazione** nella finestra della procedura guidata è selezionata.

È consigliabile deselezionare questa casella se non è possibile installare l'applicazione, ad esempio durante l'esecuzione dell'installazione remota tramite Desktop remoto di Windows. Il problema potrebbe essere causato dall'abilitazione della protezione.

In questo caso, interrompere l'installazione, riavviarla, selezionare la casella **Modifica impostazioni di installazione** nel passaggio Scelta del tipo di installazione (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)) e, durante il passaggio Preparazione dell'installazione, deselezionare la casella **Proteggi il processo di installazione**.

Per proseguire con la procedura guidata, fare click sul pulsante **Installa**.

Durante l'installazione dell'applicazione in un computer con sistema operativo Microsoft Windows XP, le connessioni di rete attive vengono terminate. La maggior parte delle connessioni terminate viene ripristinata dopo un breve intervallo di tempo.

PASSAGGIO 9. INSTALLAZIONE

L'installazione dell'applicazione può richiedere alcuni minuti. Attenderne il completamento.

Al termine dell'installazione, la procedura guidata passerà automaticamente al passaggio successivo.

Se si verifica un errore durante l'installazione causato da programmi dannosi che impediscono l'installazione di applicazioni anti-virus nel computer, l'installazione guidata offre la possibilità di scaricare *Kaspersky Virus Removal Tool*, una speciale utilità per la neutralizzazione dell'infezione.

Se si sceglie di installare l'utilità, l'installazione guidata la scarica dai server di Kaspersky Lab e ne avvia automaticamente l'installazione. Se non è possibile eseguire automaticamente il download dell'utilità, viene offerta la possibilità di scaricarla manualmente facendo click sul collegamento fornito.

Al termine dell'utilizzo, è necessario eliminarla e riavviare l'installazione di Kaspersky Anti-Virus.

PASSAGGIO 10. COMPLETAMENTO DELL'INSTALLAZIONE

Questa finestra della procedura guidata segnala il completamento dell'installazione dell'applicazione. Per eseguire Kaspersky Anti-Virus, verificare che la casella **Esegui Kaspersky Anti-Virus** sia selezionata e fare click sul pulsante **Fine**.

In alcuni casi, può essere necessario riavviare il sistema operativo. Se la casella **Esegui Kaspersky Anti-Virus 2012** è selezionata, l'applicazione verrà eseguita automaticamente dopo il riavvio del sistema operativo.

Se la casella è deselezionata e si chiude la procedura guidata, sarà necessario avviare l'applicazione manualmente (vedere la sezione "Avvio e chiusura manuale dell'applicazione" a pagina [34](#)).

PASSAGGIO 11. ATTIVAZIONE DELL'APPLICAZIONE

L'*attivazione* è una procedura di attivazione di una licenza che consente di utilizzare una versione completa dell'applicazione fino alla scadenza della licenza.

Per attivare l'applicazione occorre una connessione a Internet.

Per l'attivazione di Kaspersky Anti-Virus sono disponibili le opzioni seguenti:

- **Attivare la versione commerciale.** Selezionare questa opzione e immettere il codice di attivazione se è stata acquistata una versione commerciale dell'applicazione.

Se si specifica un codice di attivazione di Kaspersky Internet Security nel campo di immissione, al termine dell'attivazione viene avviata la procedura per il passaggio a Kaspersky Internet Security.

- **Attivare la versione di prova.** Utilizzare questa opzione di attivazione se si desidera installare la versione di prova dell'applicazione prima di procedere all'acquisto di una versione commerciale. Sarà possibile usufruire di tutte le funzionalità dell'applicazione per il periodo definito dalla licenza per la versione di prova dell'applicazione. Una volta scaduta, la licenza di prova non può essere riattivata.

PASSAGGIO 12. REGISTRAZIONE DI UN UTENTE

Questo passaggio è disponibile solo durante l'attivazione della versione commerciale dell'applicazione. Nel corso dell'attivazione della versione di prova, questo passaggio viene saltato.

È necessario eseguire la registrazione per poter contattare il Servizio di Assistenza tecnica di Kaspersky Lab.

Se si sceglie di eseguire la registrazione, specificare i dati di registrazione nei campi corrispondenti e fare click sul pulsante **Avanti**.

PASSAGGIO 13. COMPLETAMENTO DELL'ATTIVAZIONE

La procedura guidata informa l'utente che Kaspersky Anti-Virus è stato attivato correttamente. Vengono inoltre fornite informazioni sulla licenza: tipo di licenza (commerciale o di prova), data di scadenza e numero di host per la licenza.

Se è stato attivato un abbonamento, al posto della data di scadenza della licenza sono disponibili informazioni sullo stato dell'abbonamento.

Fare click sul pulsante **Fine** per chiudere la procedura guidata.

AGGIORNAMENTO DELLA VERSIONE PRECEDENTE DI KASPERSKY ANTI-VIRUS

Se Kaspersky Anti-Virus 2010 o 2011 è già installato nel computer, è consigliabile aggiornare l'applicazione a Kaspersky Anti-Virus 2012. Se si dispone di una licenza attiva per Kaspersky Anti-Virus 2010 o 2011, non sarà necessario attivare l'applicazione: le informazioni sulla licenza per Kaspersky Anti-Virus 2010 o 2011 verranno rilevate automaticamente dall'installazione guidata e saranno utilizzate durante il processo di installazione.

Kaspersky Anti-Virus viene installato nel computer in modalità interattiva tramite l'installazione guidata.

La procedura guidata comprende una serie di schermate (passaggi), tra cui è possibile spostarsi utilizzando i pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, fare click sul pulsante **Annulla**.

Se l'applicazione protegge più di un computer (il numero massimo di computer dipende dalla licenza), verrà installata nello stesso modo in tutti i computer. In questo caso, in base al contratto di licenza, il periodo di validità della licenza ha inizio dalla data della prima attivazione. Quando si attiva l'applicazione su un secondo computer, il periodo di validità della licenza viene ridotto della quantità di tempo trascorso dalla prima attivazione. Di conseguenza, il periodo di validità della licenza scade contemporaneamente per tutte le copie installate dell'applicazione.

► *Per installare Kaspersky Anti-Virus nel computer:*

Eseguire il file di installazione (con estensione *.EXE) dal CD del prodotto.

Il processo per l'installazione di Kaspersky Anti-Virus da un file di installazione scaricato da Internet è identico a quello per l'installazione da CD.

IN QUESTA SEZIONE:

Passaggio 1. Ricerca di una versione più recente dell'applicazione	20
Passaggio 2. Verifica dei requisiti di installazione	20
Passaggio 3. Scelta del tipo di installazione.....	20
Passaggio 4. Visualizzazione del contratto di licenza	21
Passaggio 5. Informativa sulla raccolta dei dati per Kaspersky Security Network.....	21
Passaggio 6. Ricerca di applicazioni incompatibili	21
Passaggio 7. Selezione della cartella di destinazione	21
Passaggio 8. Preparazione per l'installazione	22
Passaggio 9. Installazione.....	22
Passaggio 10. Termine della procedura guidata	22

PASSAGGIO 1. RICERCA DI UNA VERSIONE PIÙ RECENTE DELL'APPLICAZIONE

Prima dell'installazione, il programma di installazione controlla se nei server degli aggiornamenti di Kaspersky Lab è disponibile una nuova versione di Kaspersky Anti-Virus.

Se non vengono trovate nuove versioni nei server degli aggiornamenti di Kaspersky Lab, verrà avviata l'Installazione guidata per la versione corrente.

Se nei server degli aggiornamenti è disponibile una nuova versione di Kaspersky Anti-Virus, verrà richiesto se scaricarla e installarla nel computer. È consigliabile installare la nuova versione dell'applicazione, perché le versioni più recenti includono miglioramenti che assicurano una protezione più affidabile del computer. Se si annulla il download della nuova versione, verrà avviata l'Installazione guidata per la versione corrente. Se si sceglie di installare la nuova versione, i file di distribuzione del prodotto verranno scaricati nel computer e verrà avviata automaticamente l'Installazione guidata per la nuova versione. Per una descrizione della procedura di installazione per la nuova versione, fare riferimento alla documentazione corrispondente.

PASSAGGIO 2. VERIFICA DEI REQUISITI DI INSTALLAZIONE

Prima dell'installazione di Kaspersky Anti-Virus nel computer, il programma di installazione esamina il sistema operativo e i service pack installati per verificare che soddisfino i requisiti software per l'installazione del prodotto (vedere la sezione "Requisiti hardware e software" a pagina [14](#)). Inoltre, il programma di installazione verifica la presenza del software richiesto e delle credenziali necessarie per l'installazione delle applicazioni. Se uno dei requisiti elencati in precedenza non è soddisfatto, verrà visualizzata una notifica.

Se il computer soddisfa tutti i requisiti, la procedura guidata esegue una ricerca delle applicazioni Kaspersky Lab che possono determinare conflitti con Kaspersky Anti-Virus. Se vengono rilevate applicazioni di questo tipo, viene offerta la possibilità di rimuoverle manualmente.

Se viene rilevata una versione precedente di Kaspersky Anti-Virus o Kaspersky Internet Security, tutti i dati utilizzabili in Kaspersky Anti-Virus 2012 (ad esempio, informazioni di attivazione o impostazioni dell'applicazione) verranno salvati e utilizzati per l'installazione della nuova applicazione, mentre quella installata in precedenza sarà automaticamente rimossa.

PASSAGGIO 3. SCELTA DEL TIPO DI INSTALLAZIONE

In questa fase è possibile scegliere il tipo di installazione di Kaspersky Anti-Virus più adatto per le proprie esigenze:

- *Installazione standard.* Se si seleziona questa opzione (la casella **Modifica impostazioni di installazione** è deselezionata), l'applicazione verrà installata nel computer con le impostazioni di protezione consigliate dagli esperti di Kaspersky Lab.
- *Installazione personalizzata.* In questo caso (la casella **Modifica impostazioni di installazione** è selezionata), verrà richiesto di specificare la cartella di destinazione in cui installare l'applicazione (vedere la sezione

"Passaggio 7. Selezione della cartella di destinazione" a pagina [17](#)) e disabilitare la protezione del processo di installazione, se necessario (vedere la sezione "Passaggio 8. Preparazione dell'installazione" a pagina [18](#)).

Per continuare l'installazione, fare click sul pulsante **Avanti**.

PASSAGGIO 4. VISUALIZZAZIONE DEL CONTRATTO DI LICENZA

In questa fase è necessario esaminare il contratto di licenza tra l'utente e Kaspersky Lab.

Leggere attentamente il contratto di licenza e, se si accettano tutte le condizioni, fare click sul pulsante **Accetto**. L'installazione proseguirà.

Se non si desidera accettare il contratto di licenza, annullare l'installazione dell'applicazione facendo click sul pulsante **Annulla**.

PASSAGGIO 5. INFORMATIVA SULLA RACCOLTA DEI DATI PER KASPERSKY SECURITY NETWORK

In questa fase, viene offerta la possibilità di partecipare a Kaspersky Security Network. La partecipazione al programma implica l'invio a Kaspersky Lab di informazioni sul sistema in uso e di dati sulle nuove minacce rilevate nel computer, sulle applicazioni in esecuzione o sulle applicazioni con firma digitale scaricate. Le informazioni trasmesse non includono dati personali.

Leggere l'Informativa sulla raccolta dei dati di Kaspersky Security Network. Per leggere la versione completa dell'informativa, fare click sul pulsante **Contratto completo KSN**. Se si accettano tutte le condizioni dell'informativa, selezionare la casella **Accetto le condizioni di adesione al programma Kaspersky Security Network** nella finestra della procedura guidata.

Fare click sul pulsante **Avanti** se è stata eseguita l'installazione personalizzata (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)). Per eseguire l'installazione standard, fare click sul pulsante **Installa**. L'installazione proseguirà.

PASSAGGIO 6. RICERCA DI APPLICAZIONI INCOMPATIBILI

Durante questo passaggio, viene verificato se nel computer sono installate applicazioni incompatibili con Kaspersky Anti-Virus.

Se non vengono rilevate applicazioni di questo tipo, la procedura guidata procede automaticamente al passaggio successivo.

Se vengono rilevate applicazioni incompatibili, queste sono visualizzate in un elenco e viene richiesto all'utente se desidera rimuoverle. Le applicazioni che non vengono rimosse automaticamente da Kaspersky Anti-Virus devono essere rimosse manualmente. Durante la rimozione delle applicazioni incompatibili, sarà necessario riavviare il sistema. Dopo il riavvio, l'installazione di Kaspersky Anti-Virus continuerà automaticamente.

Per continuare l'installazione, fare click sul pulsante **Avanti**.

PASSAGGIO 7. SELEZIONE DELLA CARTELLA DI DESTINAZIONE

Questo passaggio dell'installazione guidata è disponibile solo se è stata selezionata l'installazione personalizzata (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)). Durante l'installazione standard, il passaggio viene saltato e l'applicazione è installata nella cartella predefinita.

In questa fase viene richiesto di scegliere la cartella in cui installare Kaspersky Anti-Virus. Per impostazione predefinita, viene utilizzato il seguente percorso:

- <unità>\Programmi\Kaspersky Lab\Kaspersky Anti-Virus 2012 – per i sistemi a 32 bit;
- <unità>\Programmi (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012 – per i sistemi a 64 bit;

Per installare Kaspersky Anti-Virus in una cartella differente, specificare il percorso desiderato nel campo di immissione o fare click su **Sfogli** e scegliere la cartella nella finestra visualizzata.

Tenere presente le seguenti limitazioni:

- L'applicazione non può essere installata in unità di rete o rimovibili oppure in unità virtuali (create attraverso il comando `SUBST`).
- È consigliabile evitare di installare l'applicazione in una cartella che contiene già file o altre cartelle, perché la cartella risulterà inaccessibile per la modifica.
- Il percorso della cartella di installazione non può avere una lunghezza superiore a 160 caratteri o contenere i caratteri speciali `/, ?, :, *, ", >, < o |`

Per controllare lo spazio libero su disco per l'installazione dell'applicazione, fare click sul pulsante **Utilizzo disco**. Nella finestra visualizzata sono riportate le informazioni sullo spazio su disco. Per chiudere la finestra, fare click su **OK**.

Per procedere con l'installazione, fare click su **Avanti** nella finestra della procedura guidata.

PASSAGGIO 8. PREPARAZIONE PER L'INSTALLAZIONE

Questo passaggio dell'Installazione guidata è disponibile solo se è stata selezionata l'installazione personalizzata (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)). Nel caso dell'installazione standard, il passaggio viene saltato.

Poiché il computer potrebbe essere infetto da programmi dannosi che possono influire sull'installazione di Kaspersky Anti-Virus, è necessario proteggere il processo di installazione.

Per impostazione predefinita, la protezione del processo di installazione è abilitata: la casella **Proteggi il processo di installazione** nella finestra della procedura guidata è selezionata.

È consigliabile deselezionare questa casella se non è possibile installare l'applicazione, ad esempio durante l'esecuzione dell'installazione remota tramite Desktop remoto di Windows. Il problema potrebbe essere causato dall'abilitazione della protezione.

In questo caso, interrompere l'installazione, riavviarla, selezionare la casella **Modifica impostazioni di installazione** nel passaggio Scelta del tipo di installazione (vedere la sezione "Passaggio 3. Scelta del tipo di installazione" a pagina [16](#)) e, durante il passaggio Preparazione dell'installazione, deselezionare la casella **Proteggi il processo di installazione**.

Per procedere con la procedura guidata, fare click sul pulsante **Installa**.

Durante l'installazione dell'applicazione in un computer con sistema operativo Microsoft Windows XP, le connessioni di rete attive vengono terminate. La maggior parte delle connessioni terminate viene ripristinata dopo un breve intervallo di tempo.

PASSAGGIO 9. INSTALLAZIONE

L'installazione dell'applicazione può richiedere alcuni minuti. Attenderne il completamento.

Al termine dell'installazione, la procedura guidata passerà automaticamente al passaggio successivo.

Se si verifica un errore durante l'installazione causato da programmi dannosi che impediscono l'installazione di applicazioni anti-virus nel computer, l'Installazione guidata offre la possibilità di scaricare *Kaspersky Virus Removal Tool*, una speciale utilità per la neutralizzazione dell'infezione.

Se si sceglie di installare l'utilità, l'Installazione guidata la scarica dai server di Kaspersky Lab e ne avvia automaticamente l'installazione. Se non è possibile eseguire automaticamente il download dell'utilità, viene offerta la possibilità di scaricarla manualmente facendo click sul collegamento fornito.

Al termine dell'utilizzo, è necessario eliminarla e riavviare l'installazione di Kaspersky Anti-Virus.

PASSAGGIO 10. TERMINE DELLA PROCEDURA GUIDATA

Questa finestra della procedura guidata segnala il completamento dell'installazione dell'applicazione. Per eseguire Kaspersky Anti-Virus, verificare che la casella **Esegui Kaspersky Anti-Virus** sia selezionata e fare click sul pulsante **Fine**.

In alcuni casi, può essere necessario riavviare il sistema operativo. Se la casella **Esegui Kaspersky Anti-Virus 2012** è selezionata, l'applicazione verrà eseguita automaticamente dopo il riavvio del sistema operativo.

Se la casella è deselezionata e si chiude la procedura guidata, sarà necessario avviare l'applicazione manualmente (vedere la sezione "Avvio e arresto manuale dell'applicazione" a pagina [34](#)).

SCENARI DI INSTALLAZIONE NON STANDARD

In questa sezione sono descritti scenari di installazione dell'applicazione differenti da quelli dell'installazione standard o dell'aggiornamento dalla versione precedente.

Installazione di Kaspersky Anti-Virus e successiva attivazione tramite un codice di attivazione di Kaspersky Internet Security

Se durante l'installazione di Kaspersky Anti-Virus, al momento di attivare l'applicazione, viene inserito un codice di attivazione per Kaspersky Internet Security, viene avviato il processo di aggiornamento di prodotto che modifica Kaspersky Anti-Virus in Kaspersky Internet Security.

Se durante l'installazione di Kaspersky Anti-Virus, al momento di attivare l'applicazione, si sceglie l'opzione **Attiva successivamente** e successivamente si attiva l'applicazione installata con un codice per Kaspersky Internet Security, viene comunque avviato il processo di aggiornamento di prodotto che modifica Kaspersky Anti-Virus in Kaspersky Internet Security.

Installazione di Kaspersky Anti-Virus 2012 su Kaspersky Internet Security 2010 o 2011

Se si esegue l'installazione di Kaspersky Anti-Virus 2012 in un computer in cui è già installato Kaspersky Internet Security 2010 o 2011 con una licenza attiva, l'installazione guidata rileva le informazioni sulla licenza e offre all'utente la possibilità di selezionare una delle seguenti azioni:

- Utilizzare la licenza corrente di Kaspersky Internet Security 2010 o 2011. In questo caso, viene avviato il processo di upgrade, che esegue l'installazione di Kaspersky Internet Security 2012 nel computer. Sarà possibile utilizzare Kaspersky Internet Security 2012 finché la licenza di Kaspersky Internet Security 2010 o 2011 rimane valida.
- Procedere con l'installazione di Kaspersky Anti-Virus 2012. In questo caso, la procedura di installazione continua in base allo scenario standard, a partire dal passaggio Attivazione dell'applicazione.

OPERAZIONI PRELIMINARI

Al termine dell'installazione, l'applicazione è pronta per l'utilizzo. Per assicurare una protezione adeguata del computer, è consigliabile eseguire le seguenti operazioni immediatamente dopo l'installazione e la configurazione:

- Aggiornare i database dell'applicazione (vedere la sezione "Aggiornamento dei database e dei moduli dell'applicazione" a pagina [40](#)).
- Eseguire una scansione del computer alla ricerca di virus (vedere la sezione "Esecuzione di una scansione virus completa del computer" a pagina [42](#)) e vulnerabilità (vedere la sezione "Ricerca delle vulnerabilità del computer" a pagina [42](#)).
- Controllare lo stato della protezione del computer ed eliminare i problemi di protezione, se necessario.

RIMOZIONE DELL'APPLICAZIONE.

Dopo la disinstallazione di Kaspersky Anti-Virus, il computer e i dati personali saranno senza protezione.

Kaspersky Anti-Virus viene disinstallato tramite l'installazione guidata.

➡ Per avviare la procedura guidata:

nel menu **Start** scegliere **Programmi** → **Kaspersky Anti-Virus 2012** → **Rimuovi Kaspersky Anti-Virus 2012**.

IN QUESTA SEZIONE:

Passaggio 1. Salvataggio dei dati per il riutilizzo.....	24
Passaggio 2. Conferma della rimozione dell'applicazione.....	24
Passaggio 3. Rimozione dell'applicazione. Completamento della rimozione	24

PASSAGGIO 1. SALVATAGGIO DEI DATI PER IL RIUTILIZZO

In questa fase è possibile specificare i dati utilizzati dall'applicazione che si desidera mantenere tramite un'installazione successiva, ad esempio di una nuova versione dell'applicazione.

Per impostazione predefinita, l'applicazione viene rimossa interamente dal computer.

► *Per salvare i dati per il riutilizzo:*

1. Scegliere l'opzione **Salva oggetti applicazione**.
2. Selezionare le caselle accanto ai tipi di dati da salvare:
 - **Dati di attivazione** – dati che eliminano l'esigenza di attivare l'applicazione in future, utilizzando automaticamente la licenza corrente, a condizione che questa non scada prima della successiva installazione.
 - **File di backup e in quarantena** – file esaminati dall'applicazione e spostati nell'archivio di backup o in quarantena.
 - **Impostazioni di funzionamento dell'applicazione** – valori delle impostazioni dell'applicazione selezionati durante la configurazione.
 - **Dati di iChecker** – file che contengono informazioni sugli oggetti già sottoposti a scansione virus.

PASSAGGIO 2. CONFERMA DELLA RIMOZIONE DELL'APPLICAZIONE

Dal momento che la rimozione dell'applicazione mette a rischio la protezione del computer e dei dati personali, verrà richiesto di confermare la rimozione. A tale scopo, fare click sul pulsante **Rimuovi**.

Per interrompere la rimozione dell'applicazione in qualsiasi momento, fare click sul pulsante **Annulla**.

PASSAGGIO 3. RIMOZIONE DELL'APPLICAZIONE. COMPLETAMENTO DELLA RIMOZIONE

In questo passaggio la procedura guidata rimuove l'applicazione dal computer. Attendere il completamento della rimozione.

Durante la rimozione dell'applicazione, può essere necessario riavviare il sistema. Se il riavvio non viene eseguito immediatamente, la procedura di rimozione resterà incompleta finché il sistema operativo non verrà riavviato o il computer non verrà spento e riacceso.

LICENSING DELL'APPLICAZIONE

In questa sezione vengono fornite informazioni sulle condizioni generali relative all'attivazione dell'applicazione. Vengono descritti lo scopo del contratto di licenza, i tipi di licenza, le modalità di attivazione dell'applicazione e il rinnovo della licenza.

IN QUESTA SEZIONE:

Informazioni sul Contratto di licenza con l'utente finale.....	25
Informazioni sulla trasmissione dei dati.....	25
Informazioni sulla licenza	25
Informazioni sul codice di attivazione	26

INFORMAZIONI SUL CONTRATTO DI LICENZA CON L'UTENTE FINALE

Il Contratto di licenza è un contratto legale che intercorre tra l'utente e Kaspersky Lab ZAO, in cui sono specificate le condizioni per l'utilizzo dell'applicazione.

Leggere attentamente le condizioni del Contratto di licenza prima di iniziare a utilizzare l'applicazione.

È possibile leggere le condizioni del Contratto di licenza durante l'installazione dell'applicazione Kaspersky Lab.

Le condizioni del Contratto di licenza vengono considerate accettate nei seguenti casi:

- In seguito all'apertura della confezione che contiene il CD di installazione (solo se l'applicazione è stata acquistata nella versione in scatola o presso il negozio di uno dei partner di Kaspersky Lab).
- In seguito alla conferma dell'accettazione del testo del Contratto di licenza durante l'installazione dell'applicazione.

Se non si accettano le condizioni del Contratto di licenza, è necessario interrompere l'installazione dell'applicazione.

INFORMAZIONI SULLA TRASMISSIONE DEI DATI

Allo scopo di aumentare il livello della protezione in tempo reale, l'accettazione delle condizioni del contratto di licenza implica il consenso a inviare le informazioni sui checksum degli oggetti elaborati (MD5), le informazioni necessarie per determinare la reputazione delle URL e i dati statistici per la protezione anti-spam, in modalità automatica. Le informazioni recuperate non contengono dati personali o altri tipi di informazioni riservate. Le informazioni recuperate vengono protette da Kaspersky Lab in base ai requisiti previsti dalla legislazione in vigore. È possibile ottenere maggiori informazioni sul sito Web: <http://support.kaspersky.it>.

INFORMAZIONI SULLA LICENZA

La *licenza* concede per un determinato periodo di tempo il diritto di utilizzare l'applicazione, in conformità con il Contratto di licenza. La licenza contiene un codice univoco per l'attivazione della propria copia di Kaspersky Anti-Virus.

La licenza concede il diritto di usufruire dei seguenti servizi:

- Utilizzo dell'applicazione in uno o più dispositivi.

Il numero di dispositivi in cui è possibile utilizzare l'applicazione è specificato nel Contratto di licenza.

- Possibilità di contattare il Servizio di Assistenza tecnica di Kaspersky Lab.

- Possibilità di utilizzare tutti i servizi forniti da Kaspersky Lab o dai relativi partner durante il periodo di validità della licenza (vedere la sezione "Servizi per gli utenti registrati" a pagina [14](#)).

L'ambito dei servizi forniti e il periodo di validità per l'utilizzo dell'applicazione dipendono dal tipo di licenza utilizzato per attivare l'applicazione.

Sono disponibili i seguenti tipi di licenza:

- *Di prova* – una licenza gratuita con un periodo di validità limitato, offerta per consentire di acquisire familiarità con l'applicazione.

Se si scarica l'applicazione dal sito Web <http://www.kaspersky.it>, si ottiene automaticamente una licenza di prova. Alla scadenza della licenza, tutte le funzionalità di Kaspersky Anti-Virus vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario acquistare la licenza commerciale.

- *Commerciale* – una licenza a pagamento con un periodo di validità limitato, fornita con l'acquisto dell'applicazione.

Dopo la scadenza della licenza commerciale, l'applicazione continua a essere eseguita in modalità con funzionalità limitate. È ancora possibile eseguire una scansione anti-virus del computer e utilizzare gli altri componenti dell'applicazione, ma solo con i database installati prima della scadenza della licenza. Per continuare a utilizzare Kaspersky Anti-Virus, è necessario rinnovare la licenza commerciale.

È consigliabile rinnovare la licenza il giorno della scadenza della licenza corrente, allo scopo di assicurare una protezione anti-virus completa del computer.

INFORMAZIONI SUL CODICE DI ATTIVAZIONE

Il *codice di attivazione* è un codice ricevuto al momento dell'acquisto della licenza commerciale per Kaspersky Anti-Virus. Questo codice è necessario per l'attivazione dell'applicazione.

Il codice di attivazione è una stringa alfanumerica di caratteri dell'alfabeto latino nel formato xxxxx-xxxxx-xxxxx-xxxxx.

Il codice di attivazione viene fornito in una delle seguenti forme, a seconda della modalità di acquisto dell'applicazione:

- Se è stata acquistata la versione in scatola di Kaspersky Anti-Virus, il codice di attivazione è specificato nella documentazione o nella confezione che contiene il CD di installazione.
- Se Kaspersky Anti-Virus è stato acquistato da un negozio online, il codice di attivazione viene inviato all'indirizzo e-mail specificato al momento dell'ordine del prodotto.

Il periodo di validità della licenza ha inizio dal momento in cui si attiva l'applicazione. Se è stata acquistata una licenza che consente l'utilizzo di Kaspersky Anti-Virus in diversi dispositivi, il periodo di validità della licenza ha inizio dal momento in cui si immette il codice nel primo di tali dispositivi.

Se il codice di attivazione è stato smarrito o eliminato accidentalmente dopo l'attivazione, è necessario inviare una richiesta al Servizio di Assistenza tecnica di Kaspersky Lab dalla Pagina personale (vedere la sezione "Come ottenere assistenza tecnica tramite la Pagina personale" a pagina [116](#)).

Al termine dell'attivazione dell'applicazione tramite un codice, viene assegnato un *ID cliente*. L'ID cliente è un ID personale dell'utente necessario per ricevere assistenza tecnica tramite la Pagina personale (vedere la sezione "Come ottenere assistenza tecnica tramite la Pagina personale" a pagina [116](#)).

INTERFACCIA DELL'APPLICAZIONE

In questa sezione vengono fornite informazioni sugli elementi di base dell'interfaccia grafica dell'applicazione: icona dell'applicazione e menu di scelta rapida dell'icona dell'applicazione, finestra principale, finestra delle impostazioni e finestre di notifica.

IN QUESTA SEZIONE:

Icona nell'area di notifica	27
Menu di scelta rapida	28
Finestra principale di Kaspersky Anti-Virus	29
Finestre di notifica e messaggi a comparsa	30
Finestra delle impostazioni dell'applicazione.....	31
Kaspersky Gadget.....	32
News Agent.....	32

ICONA NELL'AREA DI NOTIFICA

Al termine dell'installazione dell'applicazione, la relativa icona viene visualizzata nell'area di notifica della barra delle applicazioni di Microsoft Windows.






Nel sistema operativo Microsoft Windows 7 l'icona dell'applicazione è nascosta per impostazione predefinita, ma è possibile visualizzarla per accedere più facilmente all'applicazione (vedere la documentazione del sistema operativo).

L'icona ha le seguenti funzioni:

- È un indicatore del funzionamento dell'applicazione.
- Consente di accedere al menu di scelta rapida, alla finestra principale dell'applicazione e alla finestra delle notizie.



Indicazione del funzionamento dell'applicazione

Questa icona è un indicatore del funzionamento dell'applicazione. Segnala inoltre lo stato della protezione e visualizza le funzioni di base eseguite dall'applicazione:

-  – scansione di messaggi e-mail;
-  – scansione del traffico Web;
-  – aggiornamento di database e moduli dell'applicazione;
-  – per applicare gli aggiornamenti è necessario riavviare il computer;
-  – si è verificato un errore nel funzionamento di un componente dell'applicazione.


Per impostazione predefinita, l'icona è animata. Ad esempio, durante la scansione dei messaggi e-mail sull'icona dell'applicazione viene visualizzato il simbolo di una lettera, mentre durante un aggiornamento viene visualizzato il simbolo di un globo che ruota. L'animazione può essere disabilitata (vedere la sezione "Trasparenza delle finestre di notifica" a pagina [107](#)).

Quando l'applicazione è disabilitata, l'icona può assumere il seguente aspetto:

-  (simbolo colorato) – alcuni o tutti i componenti di protezione sono abilitati;
-  (simbolo in bianco e nero) – tutti i componenti di protezione sono disabilitati.

Accesso al menu di scelta rapida e alla finestra dell'applicazione

Utilizzando l'icona è possibile aprire il menu di scelta rapida (a pagina [28](#)) (facendo click con il pulsante destro del mouse) e la finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [29](#)) (facendo click con il pulsante sinistro del mouse).

Se sono disponibili notizie da Kaspersky Lab, verrà visualizzata l'icona  nell'area di notifica della barra delle applicazioni di Microsoft Windows. Fare doppio click sull'icona per aprire News Agent (vedere la sezione "News Agent" a pagina [32](#)).

MENU DI SCELTA RAPIDA

Utilizzando il menu di scelta rapida è possibile eseguire rapidamente varie azioni sull'applicazione.

Il menu di Kaspersky Anti-Virus contiene le voci seguenti:

- **Gestione attività** – apre la finestra **Gestione attività**.
- **Aggiornamento** – esegue l'aggiornamento dei database e dei moduli dell'applicazione.
- **Tastiera Virtuale** – visualizza la Tastiera Virtuale.
- **Kaspersky Anti-Virus** – apre la finestra principale dell'applicazione.
- **Sospendi la protezione / Riprendi la protezione** – abilita o disabilita temporaneamente i componenti di protezione in tempo reale. Questo comando non ha effetto sull'esecuzione della scansione virus o sugli aggiornamenti dell'applicazione.
- **Impostazioni** – apre la finestra delle impostazioni dell'applicazione.
- **Informazioni su** – apre una finestra contenente le informazioni sul programma.
- **Notizie** – apre la finestra News Agent (vedere la sezione "News Agent" a pagina [32](#)). Questa voce è visualizzata se sono presenti notizie non lette.
- **Esci** – chiude Kaspersky Anti-Virus (quando viene selezionato questo comando, l'applicazione viene scaricata dalla RAM del computer).



Figura 1. Menu di scelta rapida

Se è in corso un'attività di scansione virus o di aggiornamento quando si apre il menu di scelta rapida, quest'ultimo ne visualizza il nome e lo stato di avanzamento (percentuale completata). Selezionando il comando di menu con il nome di un'attività, è possibile visualizzare la finestra principale con un rapporto sui risultati dell'esecuzione dell'attività corrente.

◆ Per aprire il menu di scelta rapida:

Posizionare il puntatore sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni e fare click con il pulsante destro del mouse.

Nel sistema operativo Microsoft Windows 7 l'icona dell'applicazione è nascosta per impostazione predefinita, ma è possibile visualizzarla per accedere più facilmente all'applicazione (vedere la documentazione del sistema operativo).

FINESTRA PRINCIPALE DI KASPERSKY ANTI-VIRUS

La finestra principale dell'applicazione contiene gli elementi di interfaccia che permettono di accedere a tutte le funzionalità principali dell'applicazione.

Tale finestra può essere suddivisa in due parti:

- La parte superiore della finestra fornisce informazioni sullo stato di protezione del computer.



Figura 2. Parte superiore della finestra principale

- La parte inferiore della finestra consente di passare rapidamente alle principali funzionalità dell'applicazione, come ad esempio l'esecuzione di attività di scansione virus o l'aggiornamento di database e moduli dell'applicazione.

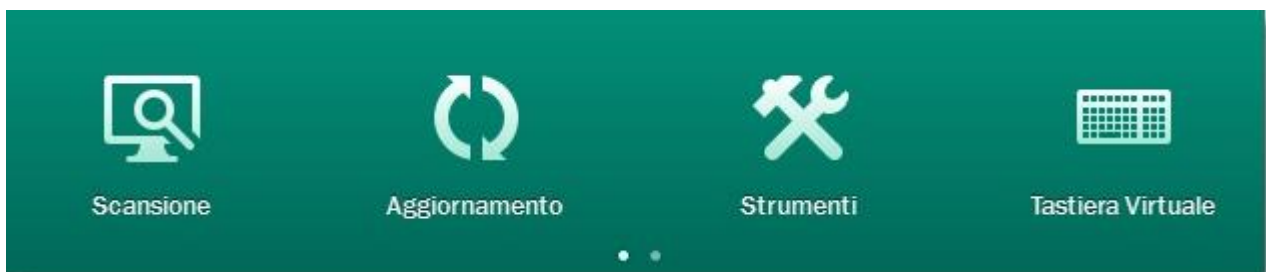


Figura 3. Parte inferiore della finestra principale

Selezionando le sezioni nella parte inferiore della finestra, verrà aperta la finestra della funzione corrispondente. È possibile tornare alla selezione delle funzioni facendo click sul pulsante **Indietro** nell'angolo superiore sinistro della finestra.

È inoltre possibile utilizzare i seguenti pulsanti e collegamenti:

- **Protezione Cloud** – consente di visualizzare le informazioni su Kaspersky Security Network (a pagina [109](#)).
- **Impostazioni** – consente di aprire la finestra delle impostazioni dell'applicazione (vedere la sezione "Finestra delle impostazioni dell'applicazione" a pagina [31](#)).
- **Rapporti** – consente di passare ai rapporti sul funzionamento dell'applicazione.
- **Notizie** – passa alla visualizzazione delle notizie nella finestra News Agent (vedere la sezione "News Agent" a pagina [32](#)). Il collegamento è visualizzato quando l'applicazione riceve una notizia.
- **Guida** – consente di visualizzare la Guida di Kaspersky Anti-Virus.
- **Pagina personale** – consente di accedere alla pagina personale dell'utente nel sito Web del Servizio di Assistenza tecnica.
- **Assistenza** – consente di aprire la finestra contenente informazioni sul sistema e collegamenti alle risorse informative di Kaspersky Lab (sito Web del Servizio di Assistenza tecnica, forum).
- **Gestione licenze** – consente di passare alle opzioni per l'attivazione e il rinnovo della licenza di Kaspersky Anti-Virus.

➔ È possibile aprire la finestra principale dell'applicazione utilizzando uno dei seguenti metodi:

- Facendo click sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni.

Nel sistema operativo Microsoft Windows 7 l'icona dell'applicazione è nascosta per impostazione predefinita, ma è possibile visualizzarla per accedere più facilmente all'applicazione (vedere la documentazione del sistema operativo).

- Selezionando **Kaspersky Anti-Virus** dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina [28](#)).
- Facendo click sull'icona Kaspersky Anti-Virus al centro di Kaspersky Gadget (solo per Microsoft Windows Vista e Microsoft Windows 7).

FINESTRE DI NOTIFICA E MESSAGGI A COMPARSA

Kaspersky Anti-Virus notifica gli eventi importanti che si verificano durante l'esecuzione tramite *finestre di notifica* e *messaggi a comparsa* visualizzati sopra l'icona dell'applicazione nell'area di notifica della barra delle applicazioni.

Le *finestre di notifica* sono visualizzate da Kaspersky Anti-Virus quando è possibile eseguire varie azioni in relazione a un evento: ad esempio, se viene rilevato un oggetto dannoso, è possibile bloccare l'accesso all'oggetto, eliminarlo o tentare di disinfettarlo. Viene offerta la possibilità di selezionare una delle azioni disponibili. Una finestra di notifica scompare dallo schermo solo se si seleziona una delle azioni.



Figura 4. Finestra di notifica

I *messaggi a comparsa* sono visualizzati da Kaspersky Anti-Virus per segnalare all'utente eventi che non richiedono la selezione di un'azione. Alcuni messaggi a comparsa contengono collegamenti utilizzabili per eseguire un'azione, come ad esempio l'aggiornamento dei database o l'attivazione dell'applicazione. I messaggi a comparsa scompaiono automaticamente dopo pochi secondi.



Figura 5. Messaggio a comparsa

A seconda dell'importanza di un evento dal punto di vista della protezione del computer, le notifiche e i messaggi a comparsa possono essere di tre tipi:

- **Notifiche critiche** – segnalano eventi di importanza critica per la protezione del computer, come ad esempio il rilevamento di un oggetto dannoso o di un'attività pericolosa nel sistema. Le finestre di notifica e i messaggi a comparsa di questo tipo sono in rosso.
- **Notifiche importanti** – segnalano eventi potenzialmente importanti per la protezione del computer, come ad esempio il rilevamento di un oggetto potenzialmente infetto o di un'attività sospetta nel sistema. Le finestre di notifica e i messaggi a comparsa di questo tipo sono in giallo.
- **Notifiche informative** – segnalano eventi che non sono di importanza critica per la protezione del computer. Le finestre di notifica e i messaggi a comparsa di questo tipo sono in verde.

FINESTRA DELLE IMPOSTAZIONI DELL'APPLICAZIONE

La finestra delle impostazioni di Kaspersky Anti-Virus (anche denominata "finestra delle impostazioni") è progettata per la configurazione dell'intera applicazione, dei singoli componenti di protezione, delle attività di scansione e aggiornamento e per l'esecuzione di altre attività di configurazione avanzata (vedere la sezione "Impostazioni avanzate dell'applicazione" a pagina [55](#)).

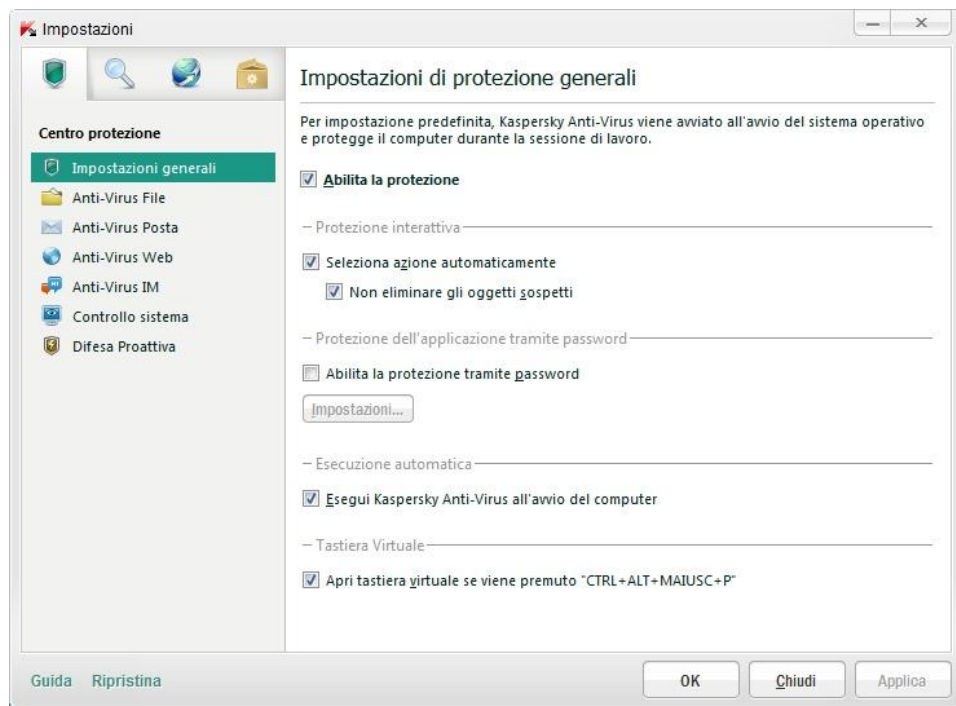


Figura 6. Finestra delle impostazioni dell'applicazione

La finestra delle impostazioni si compone di due parti:

- nella parte sinistra della finestra è possibile selezionare il componente dell'applicazione, l'attività o l'elemento da configurare;
- nella parte destra della finestra sono disponibili i controlli utilizzabili per configurare l'elemento selezionato nella parte sinistra della finestra.

I componenti, le attività e gli altri elementi nella parte sinistra della finestra sono raggruppati nelle seguenti sezioni:



– **Centro protezione;**



– **Scansione;**




– **Aggiornamento;**



– **Impostazioni avanzate.**

È possibile aprire la finestra delle impostazioni utilizzando uno dei seguenti metodi:

- facendo click sul collegamento **Impostazioni** nella parte superiore della finestra dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [29](#));
- selezionando **Impostazioni** dal menu di scelta rapida (vedere la sezione "Menu di scelta rapida" a pagina [28](#)).
- facendo click sul pulsante con l'icona  **Impostazioni** nell'interfaccia di Kaspersky Gadget (solo per i sistemi operativi Microsoft Windows Vista e Microsoft Windows 7). Al pulsante deve essere assegnata la funzione per l'apertura della finestra delle impostazioni (vedere la sezione "Utilizzo di Kaspersky Gadget" a pagina [53](#)).

KASPERSKY GADGET

Quando si utilizza Kaspersky Anti-Virus in un computer che esegue Microsoft Windows Vista o Microsoft Windows 7, è anche possibile utilizzare Kaspersky Gadget (di seguito denominato *gadget*). Kaspersky Gadget consente di accedere rapidamente alle principali funzionalità dell'applicazione, come ad esempio l'indicatore dello stato della protezione, la scansione virus degli oggetti o i rapporti sul funzionamento dell'applicazione.

Al termine dell'installazione di Kaspersky Anti-Virus in un computer con sistema operativo Microsoft Windows 7, il gadget viene visualizzato automaticamente sul desktop. Al termine dell'installazione dell'applicazione in un computer con sistema operativo Microsoft Windows Vista, è necessario aggiungere manualmente il gadget a Windows Sidebar (vedere la documentazione del sistema operativo).





Figura 7. Kaspersky Gadget

NEWS AGENT

Tramite *News Agent*, Kaspersky Lab informa l'utente di tutti gli eventi importanti relativi a Kaspersky Anti-Virus e alla protezione dalle minacce.

L'applicazione notifica le notizie visualizzando una speciale icona nell'area di notifica della barra delle applicazioni (vedere di seguito) e un messaggio a comparsa. Le informazioni sul numero di notizie non lette vengono inoltre visualizzate nella finestra principale dell'applicazione. Viene visualizzata un'icona della notizia nell'interfaccia del gadget di Kaspersky Anti-Virus.

È possibile leggere le notizie in uno dei seguenti modi:

- facendo click sull'icona  nell'area di notifica della barra delle applicazioni;
- facendo click sul collegamento **Leggi notizia** nel messaggio a comparsa;
- facendo click sul collegamento **Notizie** nella finestra principale dell'applicazione;
- facendo click sull'icona  visualizzata al centro del gadget quando è disponibile una nuova notizia (solo per Microsoft Windows Vista e Microsoft Windows 7).

I metodi elencati in precedenza per l'apertura della finestra di News Agent possono essere utilizzati solo se sono disponibili notizie non lette.

Se non si desidera ricevere notizie, è possibile disabilitarne l'invio.

AVVIO E ARRESTO DELL'APPLICAZIONE

In questa sezione sono disponibili informazioni sull'avvio e l'arresto dell'applicazione.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione dell'avvio automatico	34
Avvio e chiusura manuale dell'applicazione	34

ABILITAZIONE E DISABILITAZIONE DELL'AVVIO AUTOMATICO

In modalità di avvio automatico, Kaspersky Anti-Virus viene avviato all'avvio del sistema operativo. Questa è la modalità di avvio predefinita.

► *Per disabilitare o abilitare l'avvio automatico dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare **Impostazioni generali**.
3. Per disabilitare l'avvio automatico dell'applicazione, deselezionare la casella **Esegui Kaspersky Anti-Virus all'avvio del computer** nella sezione Esecuzione automatica nella parte destra della finestra. Per abilitare l'avvio automatico dell'applicazione, selezionare la casella.

AVVIO E CHIUSURA MANUALE DELL'APPLICAZIONE

Gli specialisti di Kaspersky Lab consigliano di non chiudere Kaspersky Anti-Virus, perché questo può mettere a rischio il computer e i dati personali dell'utente. È preferibile sospendere temporaneamente la protezione del computer, senza chiudere l'applicazione.

Se è stato disabilitato l'avvio automatico dell'applicazione, Kaspersky Anti-Virus deve essere avviato manualmente (vedere la sezione "Abilitazione e disabilitazione dell'avvio automatico" a pagina [34](#)).

► *Per avviare l'applicazione manualmente:*

nel menu **Start** scegliere **Programmi** → **Kaspersky Anti-Virus 2012** → **Kaspersky Anti-Virus 2012**.

► *Per chiudere l'applicazione:*

Fare click con il pulsante destro del mouse per aprire il menu di scelta rapida dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni, quindi scegliere **Esci**.

Nel sistema operativo Microsoft Windows 7 l'icona dell'applicazione è nascosta per impostazione predefinita, ma è possibile visualizzarla per accedere più facilmente all'applicazione (vedere la documentazione del sistema operativo).

GESTIONE DELLA PROTEZIONE DEL COMPUTER

In questa sezione sono fornite informazioni sul rilevamento delle minacce per la protezione del computer e sulla configurazione del livello di protezione. Viene descritto come abilitare, disabilitare e sospendere la protezione durante l'utilizzo dell'applicazione.

IN QUESTA SEZIONE:

Diagnostica ed eliminazione dei problemi relativi alla protezione del computer	35
Abilitazione e disabilitazione della protezione	35
Sospensione e ripresa della protezione	36

DIAGNOSTICA ED ELIMINAZIONE DEI PROBLEMI RELATIVI ALLA PROTEZIONE DEL COMPUTER

I problemi relativi alla protezione del computer sono segnalati dall'indicatore nella parte sinistra della finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [29](#)). L'indicatore è un'icona a forma di monitor, che cambia colore a seconda dello stato della protezione del computer: il verde indica che il computer è protetto, il giallo indica problemi correlati alla protezione e il rosso indica gravi minacce per la protezione del computer.



Figura 8. Indicatore dello stato della protezione

È consigliabile risolvere immediatamente i problemi ed eliminare le minacce per la protezione.

Facendo click sull'indicatore nella finestra principale dell'applicazione, è possibile aprire la finestra **Problemi di protezione** (vedere la figura seguente), che contiene informazioni dettagliate sullo stato della protezione del computer e suggerimenti per la risoluzione dei problemi e l'eliminazione delle minacce rilevate.

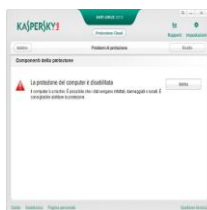


Figura 9. Finestra Problemi di protezione

I problemi di protezione sono raggruppati per categorie. Per ogni problema sono elencate le azioni che è possibile eseguire per la risoluzione.

ABILITAZIONE E DISABILITAZIONE DELLA PROTEZIONE

Per impostazione predefinita, Kaspersky Anti-Virus viene avviato durante il caricamento del sistema operativo e protegge il computer finché non viene spento. Tutti i componenti di protezione sono in esecuzione.

La protezione offerta da Kaspersky Anti-Virus può essere disabilitata completamente o parzialmente.

Gli esperti di Kaspersky Lab consigliano di non disabilitare la protezione, in quanto questo può portare all'infezione del computer e alla perdita di dati. È consigliabile sospendere la protezione per l'intervallo di tempo richiesto (vedere la sezione "Sospensione e ripresa della protezione" a pagina 36).

I seguenti indicatori segnalano che la protezione è sospesa o disabilitata:

- icona dell'applicazione inattiva (grigia) nell'area di notifica della barra delle applicazioni (vedere la sezione "Icona dell'area di notifica" a pagina 27);
- indicatore di protezione di colore rosso nella parte superiore della finestra principale dell'applicazione.

In questo caso, la protezione è considerata come l'insieme dei componenti di protezione. La disabilitazione o la sospensione dei componenti di protezione non influisce sull'esecuzione delle attività di scansione virus e degli aggiornamenti di Kaspersky Anti-Virus.

È possibile abilitare o disabilitare la protezione o singoli componenti dell'applicazione dalla finestra delle impostazioni dell'applicazione (vedere la sezione "Finestra delle impostazioni dell'applicazione" a pagina 31).

➤ *Per abilitare o disabilitare completamente la protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare **Impostazioni generali**.
3. Deselezionare la casella **Abilita la protezione** per disabilitare la protezione. Selezionare la casella per abilitare la protezione.

➤ *Per disabilitare o abilitare un componente di protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente da abilitare o disabilitare.
3. Nella parte destra della finestra deselezionare la casella **Abilita <nome del componente>** per disabilitare il componente. Selezionare la casella per abilitare il componente.

SOSPENSIONE E RIPRESA DELLA PROTEZIONE

Sospendere la protezione significa disabilitare temporaneamente tutti i componenti di protezione per un determinato periodo di tempo.

I seguenti indicatori segnalano che la protezione è sospesa o disabilitata:


- icona dell'applicazione inattiva (grigia) nell'area di notifica della barra delle applicazioni (vedere la sezione "Icona dell'area di notifica" a pagina 27);
- indicatore di protezione di colore rosso nella parte superiore della finestra principale dell'applicazione.

In questo caso, la protezione è considerata come l'insieme dei componenti di protezione. La disabilitazione o la sospensione dei componenti di protezione non influisce sull'esecuzione delle attività di scansione virus e degli aggiornamenti di Kaspersky Anti-Virus.

Se sono state stabilite connessioni di rete al momento della sospensione della protezione, verrà visualizzata una notifica relativa all'interruzione di tali connessioni.

Se si utilizza un computer con sistema operativo Microsoft Windows Vista o Microsoft Windows 7, è possibile sospendere la protezione tramite Kaspersky Gadget. A tale scopo, è necessario assegnare la funzione di sospensione della protezione a uno dei pulsanti del gadget (vedere la sezione "Utilizzo di Kaspersky Gadget" a pagina 53).

➤ *Per sospendere la protezione del computer:*

1. Aprire la finestra **Sospendi la protezione** utilizzando uno dei seguenti metodi:
 - selezionare **Sospendi la protezione** dal menu di scelta rapida dell'icona dell'applicazione (vedere la sezione "Menu di scelta rapida" a pagina 28);
 - fare click sul pulsante con l'icona  **Sospendi la protezione** nell'interfaccia di Kaspersky Gadget (solo per i sistemi operativi Microsoft Windows Vista e Microsoft Windows 7).

2. Nella finestra **Sospendi la protezione** selezionare l'intervallo di tempo dopo il quale riprendere la protezione:

- **Sospendi per il periodo di tempo specificato** – la protezione verrà abilitata al termine dell'intervallo di tempo selezionato dall'elenco a discesa sottostante.
- **Sospendi fino al riavvio** – la protezione verrà abilitata dopo il riavvio dell'applicazione o del sistema operativo, a condizione che l'avvio automatico dell'applicazione sia abilitato (vedere la sezione "Abilitazione e disabilitazione dell'avvio automatico" a pagina [34](#)).
- **Sospendi** – la protezione verrà abilitata quando si decide di riprenderla (vedere di seguito).

► *Per riprendere la protezione del computer:*

Selezionare **Riprendi la protezione** dal menu di scelta rapida dell'icona dell'applicazione (vedere la sezione "Menu di scelta rapida" a pagina [28](#)).

È possibile utilizzare questo metodo per riprendere la protezione del computer se è stata selezionata l'opzione **Sospendi**, **Sospendi per il periodo di tempo specificato** o **Sospendi fino al riavvio**.

ESECUZIONE DELLE ATTIVITÀ PIÙ COMUNI

In questa sezione vengono fornite informazioni sulla risoluzione dei problemi più comuni relativi alla protezione del computer tramite l'applicazione.

IN QUESTA SEZIONE:

Attivazione dell'applicazione	38
Acquisto o rinnovo della licenza	39
Come procedere quando vengono visualizzate le notifiche dell'applicazione	40
Aggiornamento dei database e dei moduli dell'applicazione	40
Esecuzione di una scansione virus delle aree critiche del computer	40
Scansione virus di file, cartelle, dischi o altri oggetti	41
Esecuzione di una scansione virus completa del computer	42
Ricerca delle vulnerabilità del computer	42
Protezione dei dati personali dal furto	43
Come procedere se si sospetta che un oggetto sia infetto	44
Come procedere se si sospetta che il computer sia infetto	45
Ripristino di un file eliminato o disinfettato dall'applicazione	46
Creazione e utilizzo di un Rescue Disk	46
Visualizzazione del rapporto sull'esecuzione dell'applicazione	49
Ripristino delle impostazioni predefinite dell'applicazione	49
Trasferimento delle impostazioni di Kaspersky Anti-Virus in un altro computer	50
Passaggio da Kaspersky Anti-Virus a Kaspersky Internet Security	50
Utilizzo di Kaspersky Gadget	53
Come ottenere informazioni sulla reputazione di un'applicazione	54

ATTIVAZIONE DELL'APPLICAZIONE

L'*attivazione* è una procedura di attivazione di una licenza che consente di utilizzare una versione completa dell'applicazione fino alla scadenza della licenza.

Se si è scelto di non attivare l'applicazione durante l'installazione, è possibile eseguire tale operazione in seguito. Nell'area di notifica della barra delle applicazioni verranno visualizzati messaggi di Kaspersky Anti-Virus come promemoria per l'attivazione.

► Per avviare l'Attivazione guidata di Kaspersky Anti-Virus, eseguire una delle operazioni seguenti:

- Fare click sul collegamento **Attiva** nella finestra dei messaggi di Kaspersky Anti-Virus visualizzata nell'area di notifica.
- Fare click sul collegamento **Inserire qui il codice di attivazione** nella parte inferiore della finestra principale dell'applicazione. Nella finestra **Gestione licenze** visualizzata fare click sul pulsante **Attivare l'applicazione**.

Durante l'utilizzo della configurazione guidata dell'applicazione, è necessario specificare i valori per alcune impostazioni.

Passaggio 1. Immettere il codice di attivazione

Immettere il codice di attivazione nel campo corrispondente, quindi fare click sul pulsante **Avanti**.

Passaggio 2. Richiesta dell'attivazione

Se la richiesta di attivazione viene inviata correttamente, la procedura guidata procede automaticamente al passaggio successivo.

Passaggio 3. Immissione dei dati di registrazione

La registrazione dell'utente è necessaria per poter contattare il Servizio di Assistenza tecnica. Gli utenti non registrati possono ricevere solo un livello di assistenza minimo.

Specificare i dati di registrazione e fare click sul pulsante **Avanti**.

Passaggio 4. Attivazione

Se l'attivazione dell'applicazione è stata eseguita correttamente, la procedura guidata procede automaticamente al passaggio successivo.

Passaggio 5. Termine della procedura guidata

In questa finestra sono visualizzate informazioni sui risultati dell'attivazione: tipo di licenza in uso e data di scadenza della licenza.

Fare click sul pulsante **Fine** per chiudere la procedura guidata.

ACQUISTO O RINNOVO DELLA LICENZA

Se Kaspersky Anti-Virus è stato installato senza una licenza, è possibile acquistarne una dopo l'installazione. Al momento dell'acquisto di una licenza, l'utente riceve un codice di attivazione da utilizzare per attivare l'applicazione (vedere la sezione "Attivazione dell'applicazione" a pagina [38](#)).

Alla scadenza della licenza, è possibile rinnovarla. È possibile acquistare una nuova licenza prima della scadenza del periodo di validità del codice di attivazione corrente. A tale scopo, è necessario aggiungere il nuovo codice come codice di attivazione di riserva. Al termine del periodo di validità della licenza corrente, Kaspersky Anti-Virus verrà attivato automaticamente utilizzando il codice di attivazione di riserva.

► *Per acquistare una licenza:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Gestione licenze** nella parte inferiore della finestra principale per aprire la finestra **Gestione licenze**.
3. Nella finestra visualizzata fare click sul pulsante **Acquista codice di attivazione**.
Verrà visualizzata la pagina Web del negozio online, in cui è possibile acquistare una licenza.

► *Per aggiungere un codice di attivazione di riserva:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Gestione licenze** nella parte inferiore della finestra principale per aprire la finestra **Gestione licenze**.
Verrà visualizzata la finestra **Gestione licenze**.
3. Nella finestra visualizzata, nella sezione **Nuovo codice di attivazione**, fare click sul pulsante **Immettere il codice di attivazione**.
Verrà avviata la procedura guidata Attivazione dell'applicazione.
4. Immettere il codice di attivazione nei campi corrispondenti, quindi fare click sul pulsante **Avanti**.
Kaspersky Anti-Virus invierà i dati al server di attivazione per la verifica. Se la verifica ha esito positivo, la procedura guidata procede automaticamente al passaggio successivo.
5. Selezionare **Nuovo codice**, quindi fare click sul pulsante **Avanti**.
6. Al termine della procedura guidata, fare click sul pulsante **Fine**.

COME PROCEDERE QUANDO VENGONO VISUALIZZATE LE NOTIFICHE DELL'APPLICAZIONE

Le notifiche visualizzate nell'area di notifica della barra delle applicazioni segnalano gli eventi che si verificano durante l'esecuzione dell'applicazione e richiedono l'attenzione dell'utente. A seconda della criticità dell'evento, potrebbero essere visualizzati i seguenti tipi di notifica:

- **Notifiche critiche** – segnalano eventi di importanza critica per la protezione del computer, come ad esempio il rilevamento di un oggetto dannoso o di un'attività pericolosa nel sistema. Le finestre di notifica e i messaggi a comparsa di questo tipo sono in rosso.
- **Notifiche importanti** – segnalano eventi potenzialmente importanti per la protezione del computer, come ad esempio il rilevamento di un oggetto potenzialmente infetto o di un'attività sospetta nel sistema. Le finestre di notifica e i messaggi a comparsa di questo tipo sono in giallo.
- **Notifiche informative** – segnalano eventi che non sono di importanza critica per la protezione del computer. Le finestre di notifica e i messaggi a comparsa di questo tipo sono in verde.

Se viene visualizzata una notifica di questo tipo, è necessario selezionare una delle opzioni suggerite. L'opzione ottimale è quella consigliata come predefinita dagli specialisti di Kaspersky Lab.

AGGIORNAMENTO DEI DATABASE E DEI MODULI DELL'APPLICAZIONE

Per impostazione predefinita, Kaspersky Anti-Virus controlla automaticamente la presenza di nuovi aggiornamenti sui server degli aggiornamenti di Kaspersky Lab. Se il server contiene un nuovo set di aggiornamenti, questi vengono scaricati e installati in background. È possibile avviare manualmente l'aggiornamento di Kaspersky Anti-Virus in qualsiasi momento.

Per scaricare gli aggiornamenti dai server di Kaspersky Lab, è necessario avere stabilito una connessione a Internet.

➔ *Per avviare un aggiornamento dal menu di scelta rapida:*

Selezionare **Aggiornamento** dal menu di scelta rapida dell'icona dell'applicazione.

➔ *Per avviare un aggiornamento dalla finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Aggiornamento** nella parte inferiore della finestra.
2. Nella finestra **Aggiornamento** visualizzata fare click sul pulsante **Esegui aggiornamento**.

ESECUZIONE DI UNA SCANSIONE VIRUS DELLE AREE CRITICHE DEL COMPUTER

Durante la scansione delle aree critiche vengono esaminati i seguenti oggetti:

- oggetti caricati all'avvio del sistema operativo;
- memoria del sistema;
- settori di avvio del disco;
- oggetti aggiunti dall'utente (vedere la sezione "Creazione di un elenco di oggetti da esaminare" a pagina [59](#)).

È possibile avviare una scansione delle aree critiche utilizzando uno dei seguenti metodi:


- utilizzando un collegamento creato precedentemente (vedere pagina [63](#)).
- dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [29](#)).

► Per avviare la scansione utilizzando un collegamento:

1. Aprire Esplora risorse di Microsoft Windows e passare alla cartella in cui è stato creato il collegamento.
2. Fare doppio click sul collegamento per avviare la scansione.

► Per avviare la scansione dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Scansione** nella parte inferiore della finestra.

2. Nella sezione **Scansione delle aree critiche** della finestra **Scansione** visualizzata fare click sul pulsante .

SCANSIONE VIRUS DI FILE, CARTELLE, DISCHI O ALTRI OGGETTI

È possibile eseguire la scansione virus di un oggetto:

- utilizzando il menu di scelta rapida dell'oggetto;
- dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [29](#));
- utilizzando Kaspersky Gadget (solo per i sistemi operativi Microsoft Windows Vista e Microsoft Windows 7).

► Per avviare un'attività anti-virus dal menu di scelta rapida dell'oggetto:

1. Aprire Esplora risorse di Microsoft Windows e passare alla cartella che contiene l'oggetto da esaminare.
2. Fare click con il pulsante destro del mouse per aprire il menu di scelta rapida dell'oggetto (vedere la figura seguente), quindi selezionare **Ricerca virus**.

Nella finestra **Gestione attività** verranno indicati lo stato di avanzamento e i risultati dell'attività.

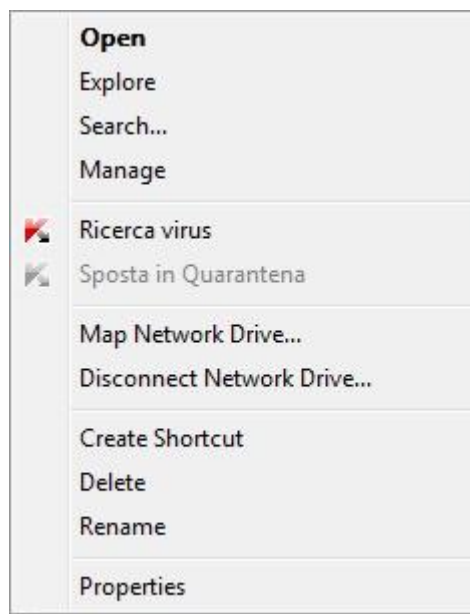


Figura 10. Menu di scelta rapida di un oggetto in Microsoft Windows

► Per avviare la scansione di un oggetto dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Scansione** nella parte inferiore della finestra.
2. Specificare l'oggetto da esaminare utilizzando uno dei seguenti metodi:
 - Fare click sul collegamento **specificare** nell'angolo inferiore destro della finestra per aprire la finestra **Scansione Personalizzata**, quindi selezionare le caselle accanto alle cartelle e alle unità che si desidera esaminare.

Se nella finestra non viene visualizzato alcun oggetto per la scansione:

- a. Fare click sul pulsante **Aggiungi**.
 - b. Nella finestra **Scelta degli oggetti da esaminare** visualizzata selezionare un oggetto da esaminare.
- Trascinare un oggetto da esaminare nell'apposita area della finestra principale (vedere la figura seguente).
- Lo stato di avanzamento dell'attività verrà visualizzato nella finestra **Gestione attività**.

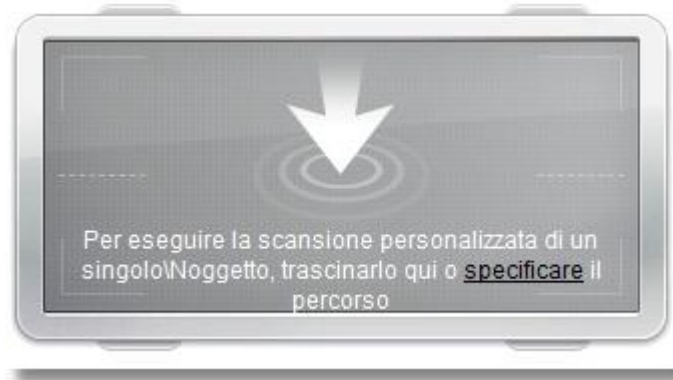


Figura 11. Area della finestra Scansione in cui è necessario trascinare un oggetto per eseguirne la scansione

- Per eseguire la scansione antivirus di un oggetto utilizzando il gadget:

trascinare l'oggetto da esaminare nel gadget.

Lo stato di avanzamento dell'attività verrà visualizzato nella finestra **Gestione attività**.

ESECUZIONE DI UNA SCANSIONE VIRUS COMPLETA DEL COMPUTER


È possibile avviare una scansione virus completa:

- utilizzando un collegamento creato precedentemente (vedere pagina [63](#));
- dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [29](#)).

- Per avviare una scansione completa utilizzando un collegamento:

1. Aprire Esplora risorse di Microsoft Windows e passare alla cartella in cui è stato creato il collegamento.
2. Fare doppio click sul collegamento per avviare la scansione.

- Per avviare la scansione completa dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Scansione** nella parte inferiore della finestra.
2. Nella sezione **Scansione Completa** della finestra **Scansione** visualizzata fare click sul pulsante .

RICERCA DELLE VULNERABILITÀ DEL COMPUTER

Le *vulnerabilità* sono parti non protette del codice del software che un utente malintenzionato può deliberatamente utilizzare per i propri scopi, ad esempio per copiare dati utilizzati in programmi non protetti. La ricerca delle vulnerabilità del computer consente di identificare questi punti deboli. È consigliabile eliminare le vulnerabilità rilevate.


È possibile eseguire la ricerca delle vulnerabilità del sistema:

- dalla finestra principale dell'applicazione (vedere la sezione "Finestra principale di Kaspersky Anti-Virus" a pagina [29](#));
- utilizzando un collegamento creato precedentemente (vedere pagina [63](#)).

➤ *Per avviare l'attività utilizzando un collegamento:*

1. Aprire Esplora risorse di Microsoft Windows e passare alla cartella in cui è stato creato il collegamento.
2. Fare doppio click sul collegamento per avviare la ricerca delle vulnerabilità del sistema.

➤ *Per avviare l'attività dalla finestra principale dell'applicazione:*

1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Scansione** nella parte inferiore della finestra.
2. Nella sezione **Scansione Vulnerabilità** della finestra **Scansione** visualizzata fare click sul pulsante .

PROTEZIONE DEI DATI PERSONALI DAL FURTO

Kaspersky Anti-Virus consente di proteggere dal furto i dati personali come:

- password, nomi utente e altri dati di registrazione;
- numeri di conti e di carte di credito.

Kaspersky Anti-Virus include i seguenti componenti e strumenti che contribuiscono alla protezione dei dati personali:

- Anti-Phishing. Assicura la protezione dal furto di dati attraverso tecniche di phishing.
- Tastiera Virtuale. Impedisce l'intercettazione dei dati immessi tramite la tastiera.

IN QUESTA SEZIONE:

Protezione dal phishing	43
Protezione dall'intercettazione dei dati immessi tramite la tastiera.....	43

PROTEZIONE DAL PHISHING

La protezione dal phishing viene assicurata da Anti-Phishing, implementato nei componenti Anti-Virus Web e Anti-Virus IM. Kaspersky Lab consiglia di abilitare il controllo del phishing per tutti i componenti di protezione.

➤ *Per abilitare la protezione dal phishing quando Anti-Virus Web è in esecuzione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Viene visualizzata la finestra **Anti-Virus Web**.
5. Nella finestra visualizzata, nella sezione **Controllo URL Kaspersky** della scheda **Generale**, selezionare la casella **Controllare le pagine Web di phishing**.

➤ *Per abilitare la protezione dal phishing quando Anti-Virus IM è in esecuzione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella parte destra della finestra, nella sezione **Metodi di scansione**, selezionare la casella **Controllare se le URL sono elencate nel database delle URL di phishing**.

PROTEZIONE DALL'INTERCETTAZIONE DEI DATI IMMESSI TRAMITE LA TASTIERA

Durante l'utilizzo di Internet, spesso è necessario immettere dati personali o nomi utente e password. Questo accade ad esempio durante la registrazione di account nei siti Web, gli acquisti online o l'utilizzo di servizi di online banking.

In tal caso, esiste il rischio che le informazioni personali siano intercettate tramite intercettori di eventi tastiera o keylogger, ovvero programmi che memorizzano le sequenze di tasti.

Lo strumento Tastiera Virtuale previene l'intercettazione dei dati immessi tramite la tastiera.

La Tastiera Virtuale non può proteggere i dati riservati se il sito che richiede l'immissione dei dati è stato violato da un hacker: in tal caso le informazioni vengono ottenute direttamente dagli utenti malintenzionati.

Molte delle applicazioni classificate come spyware hanno la funzione di creare schermate che vengono quindi trasferite a un utente malintenzionato che le analizzerà per sottrarre i dati personali dell'utente. La Tastiera Virtuale impedisce l'utilizzo delle schermate per l'intercettazione dei dati immessi.

È possibile impedire l'intercettazione dei dati personali solo se si utilizzano i browser Microsoft Internet Explorer, Mozilla Firefox e Google Chrome.

La Tastiera Virtuale dispone delle seguenti funzionalità:

- È possibile premere i tasti della Tastiera Virtuale utilizzando il mouse.
- A differenza delle tastiere reali, la Tastiera Virtuale non consente di premere più tasti contemporaneamente. Pertanto, per utilizzare le combinazioni di tasti (ad esempio, **ALT+F4**), è necessario premere il primo tasto (ad esempio, **ALT**), quindi il secondo tasto (ad esempio, **F4**) e infine nuovamente il primo tasto. Il secondo click sul tasto equivale al rilascio del tasto in una tastiera reale.
- Per modificare la lingua di input nella Tastiera Virtuale, utilizzare la combinazione di tasti **CTRL+MAIUSC** (è necessario premere il tasto **MAIUSC** utilizzando il pulsante destro del mouse) o **CTRL+ALT di sinistra** (è necessario premere il tasto **ALT di sinistra** utilizzando il pulsante destro del mouse) a seconda delle impostazioni specificate.

È possibile aprire la Tastiera Virtuale nei modi seguenti:

- dal menu di scelta rapida dell'icona dell'applicazione;
- dalla finestra principale dell'applicazione;
- dalle finestre dei browser Microsoft Internet Explorer, Mozilla Firefox o Google Chrome;
- utilizzando combinazioni di tasti.


➔ *Per aprire la Tastiera Virtuale dal menu di scelta rapida dell'icona dell'applicazione:*

Selezionare **Tastiera Virtuale** dal menu di scelta rapida dell'icona dell'applicazione.

➔ *Per aprire la Tastiera Virtuale dalla finestra principale dell'applicazione:*

Nella parte inferiore della finestra selezionare la sezione **Tastiera Virtuale**.

➔ *Per aprire la Tastiera Virtuale dalla finestra principale del browser:*

Fare click sul pulsante  **Tastiera Virtuale** sulla barra degli strumenti di Microsoft Internet Explorer, Mozilla Firefox o Google Chrome.

➔ *Per aprire la Tastiera Virtuale utilizzando una combinazione di tasti:*

Premere **CTRL+ALT+MAIUSC+P**.

COME PROCEDERE SE SI SOSPETTA CHE UN OGGETTO SIA INFETTO

Se si sospetta che un oggetto sia infetto, eseguirne la scansione tramite Kaspersky Anti-Virus (vedere la sezione "Scansione virus di file, cartelle, dischi o altri oggetti" a pagina [41](#)).

Se l'applicazione esamina un oggetto e quindi lo classifica come non infetto, ma si sospetta che non sia tale, è possibile eseguire una delle seguenti operazioni:

- Spostare l'oggetto in *Quarantena*. Gli oggetti spostati in quarantena non costituiscono una minaccia per il computer. Dopo l'aggiornamento dei database, Kaspersky Anti-Virus potrebbe essere in grado di identificare chiaramente ed eliminare la minaccia.
- Inviare l'oggetto al *Virus Lab*. Gli specialisti del Virus Lab esamineranno l'oggetto. Se l'oggetto risulta infetto da un virus, la descrizione del nuovo virus è aggiunta nei database che verranno scaricati dall'applicazione con un aggiornamento (vedere la sezione "Aggiornamento dei database dell'applicazione" a pagina [40](#)).

È possibile spostare un file in quarantena utilizzando due metodi:

- facendo click sul pulsante **Sposta in Quarantena** nella finestra **Quarantena**;
 - utilizzando il menu di scelta rapida del file.
- ➔ *Per spostare un oggetto in quarantena dalla finestra Quarantena:*
1. Aprire la finestra principale dell'applicazione.
 2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
 3. Nella scheda **Quarantena** fare click sul pulsante **Sposta in Quarantena**.
 4. Nella finestra visualizzata selezionare il file da spostare in quarantena.
- ➔ *Per spostare un file in quarantena utilizzando il menu di scelta rapida:*
1. Aprire Esplora risorse di Microsoft Windows e passare alla cartella che contiene il file da spostare in quarantena.
 2. Fare click con il pulsante destro del mouse per aprire il menu di scelta rapida del file e selezionare **Sposta in Quarantena**.
- ➔ *Per inviare un file al Virus Lab:*
1. Visitare la pagina per l'invio di richieste al Virus Lab (<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=it>).
 2. Attenersi alle istruzioni in questa pagina per inviare la richiesta.

COME PROCEDERE SE SI SOSPETTA CHE IL COMPUTER SIA INFETTO

Se si sospetta che il sistema operativo sia stato danneggiato a causa dell'attività del malware o di errori di sistema, è possibile utilizzare *Risoluzione dei problemi di Microsoft Windows*, che consente di rimuovere qualsiasi traccia di oggetti dannosi dal sistema. Gli esperti di Kaspersky Lab consigliano di eseguire la procedura guidata dopo aver disinfettato il computer per verificare che tutte le minacce e i danni causati dall'infezione siano stati risolti.

Risoluzione dei problemi di Microsoft Windows controlla il sistema alla ricerca di modifiche ed errori, come ad esempio modifiche di estensioni di file o il blocco dell'ambiente di rete e del Pannello di controllo. Le modifiche e gli errori possono essere causati da attività del malware, configurazioni errate, problemi del sistema o l'errato funzionamento delle applicazioni di ottimizzazione del sistema.

Al termine dell'analisi, la procedura guidata analizza le informazioni raccolte per verificare la presenza di danni del sistema che richiedono attenzione immediata. In base ai risultati dell'analisi, viene generato un elenco di azioni necessarie per eliminare i problemi. Tali azioni sono raggruppate per categorie in base alla gravità dei problemi rilevati.

- ➔ *Per avviare la Correzione guidata delle impostazioni di Windows:*
1. Aprire la finestra principale dell'applicazione (vedere pagina [29](#)).
 2. Nella parte inferiore della finestra selezionare la sezione **Strumenti**.
 3. Nella sezione **Risoluzione dei problemi di Microsoft Windows** della finestra visualizzata fare click sul pulsante **Avvio**.

Verrà visualizzata la finestra Risoluzione dei problemi di Microsoft Windows.

La procedura guidata comprende una serie di schermate (passaggi), tra cui è possibile spostarsi utilizzando i pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, fare click sul pulsante **Annulla**.

Passaggio 1. Avvio del ripristino del sistema

Assicurarsi che l'opzione **Cerca i problemi causati dall'attività del malware** sia selezionata, quindi fare click su **Avanti**.

Passaggio 2. Ricerca dei problemi

Verrà eseguita una ricerca dei problemi da risolvere. Al termine della ricerca, la procedura guidata passerà automaticamente al passaggio successivo.

Passaggio 3. Selezione delle azioni per la risoluzione dei problemi

Tutti i danni rilevati durante il passaggio precedente vengono raggruppati in base al tipo di rischio che costituiscono. Per ogni gruppo di danni viene consigliata la sequenza di azioni correttive più appropriate. Sono disponibili tre gruppi di azioni:

- Le *azioni fortemente consigliate* eliminano i problemi che costituiscono una grave minaccia per la protezione. È consigliabile eseguire tutte le azioni appartenenti a questo gruppo.
- Le *azioni consigliate* eliminano i problemi che costituiscono una potenziale minaccia. È consigliabile eseguire anche tutte le azioni appartenenti a questo gruppo.
- Le *azioni aggiuntive* riparano i danni del sistema che al momento non costituiscono una minaccia, ma possono rappresentare un pericolo per il computer in futuro.

Per visualizzare le azioni di un gruppo, fare click sull'icona **+** a sinistra del nome del gruppo.

Per eseguire una determinata azione, selezionare la casella a sinistra della descrizione dell'azione corrispondente. Per impostazione predefinita, la procedura guidata esegue tutte le azioni consigliate e fortemente consigliate. Se non si desidera eseguire una determinata azione, deselegionare la casella corrispondente.

Deselegionare le caselle selezionate per impostazione predefinita è fortemente sconsigliato, perché tale operazione lascia il computer vulnerabile alle minacce.

Una volta definito il set di azioni da eseguire, fare click su **Avanti**.

Passaggio 4. Eliminazione dei problemi

La procedura guidata eseguirà le azioni selezionate durante il passaggio precedente. L'eliminazione può richiedere un certo tempo. Al termine della risoluzione dei problemi, la procedura guidata passerà automaticamente al passaggio successivo.

Passaggio 5. Termine della procedura guidata

Fare click sul pulsante **Fine** per chiudere la procedura guidata.

RIPRISTINO DI UN FILE ELIMINATO O DISINFETTATO DALL'APPLICAZIONE

Kaspersky Lab consiglia di evitare di ripristinare i file eliminati e disinfettati, perché costituiscono una minaccia per il computer.

Se si desidera ripristinare un file eliminato o disinfettato, è possibile utilizzare una copia di backup creata dall'applicazione durante la scansione.

➤ *Per ripristinare un file eliminato o disinfettato dall'applicazione*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Archivio** selezionare il file desiderato dall'elenco, quindi fare click sul pulsante **Ripristina**.

CREAZIONE E UTILIZZO DI UN RESCUE DISK

Dopo avere installato Kaspersky Anti-Virus ed eseguito la prima scansione del computer, è consigliabile creare il Rescue Disk.

Il Rescue Disk è un'applicazione denominata Kaspersky Rescue Disk e registrata in un supporto rimovibile (CD o unità flash USB).

Sarà quindi possibile utilizzare il Kaspersky Rescue Disk per la scansione e la disinfezione dei computer infetti che non possono essere disinfettati in altro modo, ad esempio tramite le applicazioni anti-virus.

IN QUESTA SEZIONE:

Creazione di un Rescue Disk	47
Avvio del computer dal Rescue Disk	48

CREAZIONE DI UN RESCUE DISK

La creazione di un Rescue Disk consiste nella creazione di un'immagine del disco (file ISO) con la versione aggiornata di Kaspersky Rescue Disk e la relativa registrazione su un supporto rimovibile.

È possibile scaricare l'immagine del disco originale dal server di Kaspersky Lab o copiarla da un'origine locale.

Il Rescue Disk viene creato tramite la *Creazione guidata Kaspersky Rescue Disk*. Il file *rescuecd.iso* creato dalla procedura guidata viene salvato sul disco rigido del computer:

- in Microsoft Windows XP – nella seguente cartella: Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Data\Rdisk\;
- nei sistemi operativi Microsoft Windows Vista e Microsoft Windows 7 – nella seguente cartella: ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

➔ *Per creare un Rescue Disk:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Strumenti**.
3. Nella sezione **Kaspersky Rescue Disk** della finestra visualizzata fare click sul pulsante **Crea**.

Verrà visualizzata la finestra **Creazione guidata Kaspersky Rescue Disk**.

La procedura guidata comprende una serie di schermate (passaggi), tra cui è possibile spostarsi utilizzando i pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, fare click sul pulsante **Annulla**.

Di seguito sono descritti in dettaglio i vari passaggi della procedura guidata.

Passaggio 1. Avvio della procedura guidata. Ricerca di un'immagine del disco esistente

La prima finestra della procedura guidata contiene informazioni su Kaspersky Rescue Disk.

Se viene rilevato un file ISO di un Rescue Disk esistente nell'apposita cartella (vedere paragrafo precedente), nella prima finestra della procedura guidata verrà visualizzata la casella **Usa immagine ISO esistente**. Selezionare la casella per utilizzare il file rilevato come immagine ISO originale e andare direttamente al passaggio **Aggiornamento dell'immagine del disco** (vedere di seguito). Se non si desidera utilizzare l'immagine del disco rilevata, deselezionare la casella. La procedura guidata passerà alla finestra **Selezionare la sorgente dell'immagine del disco**.

Passaggio 2. Selezione dell'origine dell'immagine del disco

Se è stata selezionata la casella **Usa immagine ISO esistente** nella prima finestra della procedura guidata, questo passaggio verrà ignorato.

Durante questo passaggio, è necessario selezionare l'origine del file di immagine dalle opzioni disponibili:

- Se si dispone già di una copia registrata del Rescue Disk o di un'immagine ISO salvata nel computer o in una risorsa di rete locale, selezionare **Copia immagine ISO da unità locale o di rete**.
- Se non è stato creato alcun file di immagine ISO per il Rescue Disk e si desidera scaricarlo dal server di Kaspersky Lab (la dimensione del file è di circa 175 MB), selezionare **Scaricare l'immagine ISO dal server di Kaspersky Lab**.

Passaggio 3. Copia (download) dell'immagine del disco

Se è stata selezionata la casella **Usa immagine ISO esistente** nella prima finestra della procedura guidata, questo passaggio verrà ignorato.

Se nel passaggio precedente è stata selezionata l'opzione **Copia immagine ISO da unità locale o di rete**, fare click sul pulsante **Sfoglia**. Dopo avere specificato il percorso del file, fare click sul pulsante **Avanti**. Nella finestra della procedura guidata viene visualizzato lo stato di avanzamento della copia dell'immagine del disco.

Se nel passaggio precedente è stata selezionata l'opzione **Scaricare l'immagine ISO dal server di Kaspersky Lab**, viene visualizzato immediatamente lo stato di avanzamento del download dell'immagine del disco.

Al termine della copia o del download dell'immagine ISO, la procedura guidata procede automaticamente al passaggio successivo.

Passaggio 4. Aggiornamento del file immagine ISO

La procedura di aggiornamento del file immagine ISO comprende le seguenti operazioni:

- aggiornamento dei database anti-virus;
- aggiornamento dei file di configurazione.

I file di configurazione determinano se il computer può essere avviato da un supporto rimovibile (ad esempio un CD/DVD o un'unità flash USB con Kaspersky Rescue Disk) creato dalla procedura guidata.

Per l'aggiornamento dei database anti-virus vengono utilizzati i database distribuiti durante l'ultimo aggiornamento di Kaspersky Anti-Virus. Se i database non sono aggiornati, è consigliabile eseguire l'attività di aggiornamento e avviare nuovamente la Creazione guidata Kaspersky Rescue Disk.

Per avviare l'aggiornamento del file ISO, fare click sul pulsante **Avanti**. Nella finestra della procedura guidata verrà visualizzato lo stato di avanzamento dell'aggiornamento.

Passaggio 5. Registrazione dell'immagine del disco su un supporto

Durante questo passaggio, viene segnalato il completamento della creazione dell'immagine del disco e viene offerta la possibilità di registrarla su un supporto.

Specificare un supporto dati per la registrazione del Kaspersky Rescue Disk:

- Per registrare l'immagine del disco su un CD/DVD, selezionare **Registra su CD/DVD** e specificare il supporto in cui si desidera registrare l'immagine del disco.
- Per registrare l'immagine del disco in un'unità flash USB, selezionare **Registra in unità flash USB** e specificare un dispositivo in cui si desidera registrare l'immagine del disco.

Kaspersky Lab consiglia di evitare di registrare l'immagine ISO in dispositivi che non sono appositamente progettati per l'archiviazione di dati, come ad esempio smartphone, telefoni cellulari, PDA e lettori MP3. La registrazione di immagini ISO in questi dispositivi può provocare problemi di malfunzionamento.

- Per registrare l'immagine del disco nel disco rigido del proprio computer o nel disco rigido di un altro computer accessibile in rete, selezionare **Salvare l'immagine disco in un file in un'unità locale o di rete**, quindi specificare la cartella in cui registrare l'immagine del disco e il nome del file ISO.

Passaggio 6. Termine della procedura guidata

Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**. È possibile utilizzare il Rescue Disk creato per avviare il computer (vedere pagina [48](#)) quando non è possibile avviarlo ed eseguire Kaspersky Anti-Virus in modalità normale a causa dell'azione dannosa di virus o malware.

AVVIO DEL COMPUTER DAL RESCUE DISK

Se non è possibile eseguire l'avvio del sistema operativo a causa dell'attacco di un virus, utilizzare il Rescue Disk.

Per avviare il sistema operativo, è necessario utilizzare un CD/DVD o un'unità flash USB contenenti il Kaspersky Rescue Disk (vedere la sezione "Creazione di un Rescue Disk" a pagina [47](#)).

Non sempre è possibile avviare un computer da un supporto rimovibile. In particolare, questa modalità non è supportata da alcuni modelli di computer obsoleti. Prima di arrestare il computer per avviarlo da un supporto rimovibile, verificare che sia possibile eseguire questa operazione.

► Per avviare il computer dal Rescue Disk:

1. Nelle impostazioni del BIOS abilitare l'avvio da CD/DVD o da un dispositivo USB. Per informazioni dettagliate, fare riferimento alla documentazione relativa alla scheda madre installata nel computer.
2. Inserire un CD/DVD nell'unità CD/DVD del computer infetto o collegare un dispositivo flash USB in cui è stato copiato il Kaspersky Rescue Disk.
3. Riavviare il computer.


Per informazioni dettagliate sull'utilizzo del Rescue Disk, fare riferimento al manuale dell'utente di Kaspersky Rescue Disk.

VISUALIZZAZIONE DEL RAPPORTO SULL'ESECUZIONE DELL'APPLICAZIONE

Kaspersky Anti-Virus crea rapporti sul funzionamento di ogni componente. Utilizzando un rapporto è possibile ottenere informazioni statistiche sul funzionamento dell'applicazione, ad esempio quanti oggetti dannosi sono stati rilevati e neutralizzati durante il periodo specificato, quante volte l'applicazione è stata aggiornata durante lo stesso periodo, quanti messaggi di spam sono stati rilevati e così via.

Se si utilizza un computer con sistema operativo Microsoft Windows Vista o Microsoft Windows 7, è possibile aprire i rapporti tramite Kaspersky Gadget. A tale scopo, è necessario configurare Kaspersky Gadget assegnando l'opzione per l'apertura della finestra dei rapporti a uno dei pulsanti (vedere la sezione "Utilizzo di Kaspersky Gadget" a pagina [53](#)).

► Per visualizzare il rapporto sul funzionamento dell'applicazione:

1. Aprire la finestra **Rapporti** utilizzando uno dei seguenti metodi:
 - fare click sul collegamento **Rapporti** nella parte superiore della finestra principale dell'applicazione;
 - fare click sul pulsante con l'icona  **Rapporti** nell'interfaccia di Kaspersky Gadget (solo per i sistemi operativi Microsoft Windows Vista e Microsoft Windows 7).

Nella finestra **Rapporti** vengono visualizzati i rapporti sul funzionamento dell'applicazione tramite diagrammi.

2. Se si desidera visualizzare un rapporto dettagliato sul funzionamento dell'applicazione (ad esempio, un rapporto sul funzionamento di ogni componente), fare click sul pulsante **Rapporto dettagliato** nella parte inferiore della finestra **Rapporti**.

Verrà visualizzata la finestra **Rapporto dettagliato**, in cui i dati sono rappresentati in una tabella. Per agevolare la visualizzazione dei rapporti, è possibile selezionare varie opzioni per l'ordinamento delle voci.

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE DELL'APPLICAZIONE

È possibile ripristinare in qualsiasi momento le impostazioni predefinite dell'applicazione consigliate da Kaspersky Lab per Kaspersky Anti-Virus. Le impostazioni possono essere ripristinate tramite la *Configurazione guidata dell'applicazione*.

Al termine della procedura guidata, viene impostato il livello di protezione **Consigliato** per tutti i componenti di protezione. Durante il ripristino del livello di protezione consigliato, è possibile salvare i valori specificati in precedenza per alcune impostazioni dei componenti dell'applicazione.

► Per ripristinare le impostazioni predefinite dell'applicazione:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. È possibile eseguire la Configurazione guidata dell'applicazione utilizzando uno dei seguenti metodi:
 - Fare click sul collegamento **Ripristina** nella parte inferiore della finestra.
 - Nella parte sinistra della finestra selezionare **Gestione impostazioni** nella sezione **Impostazioni avanzate**, quindi fare click sul pulsante **Ripristina** nella sezione **Ripristina impostazioni predefinite**.

Di seguito sono descritti in dettaglio i vari passaggi della procedura guidata.

Passaggio 1. Avvio della procedura guidata

Fare click sul pulsante **Avanti** per continuare con la procedura guidata.

Passaggio 2. Ripristina impostazioni

Questa finestra della procedura guidata mostra i componenti di Kaspersky Anti-Virus le cui impostazioni sono diverse da quelle predefinite perché modificate dall'utente. Se sono state create impostazioni speciali per uno o più componenti, anche queste verranno visualizzate nella finestra.

Selezionare le caselle relative alle impostazioni da salvare e fare click sul pulsante **Avanti**.

Passaggio 3. Completamento del ripristino

Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**.

TRASFERIMENTO DELLE IMPOSTAZIONI DI KASPERSKY ANTI-VIRUS IN UN ALTRO COMPUTER

Dopo avere configurato il prodotto, è possibile applicarne le impostazioni a una nuova installazione di Kaspersky Anti-Virus in un altro computer. Come risultato, l'applicazione sarà configurata in modo identico in entrambi i computer. Questa funzione è ad esempio utile quando Kaspersky Anti-Virus è installato sia nel computer di casa che in quello dell'ufficio.

Le impostazioni dell'applicazione sono memorizzate in uno speciale file di configurazione, che è possibile trasferire in un altro computer.

Le impostazioni di Kaspersky Anti-Virus possono essere trasferite in un altro computer eseguendo tre passaggi:

1. Salvare le impostazioni dell'applicazione in un file di configurazione.
2. Trasferire un file di configurazione in un altro computer, ad esempio tramite posta elettronica o su un supporto rimovibile.
3. Applicare le impostazioni di un file di configurazione all'applicazione installata in un altro computer.

➔ *Per esportare le impostazioni correnti di Kaspersky Anti-Virus:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Gestione impostazioni**.
3. Fare click sul pulsante **Salva** nella parte destra della finestra.
4. Nella finestra visualizzata immettere il nome del file di configurazione e il percorso in cui salvarlo.
5. Fare click sul pulsante **OK**.

➔ *Per importare le impostazioni dell'applicazione da un file di configurazione salvato:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Gestione impostazioni**.
3. Fare click sul pulsante **Importa** nella parte destra della finestra.
4. Nella finestra visualizzata selezionare il file da cui importare le impostazioni di Kaspersky Anti-Virus.
5. Fare click sul pulsante **OK**.

PASSAGGIO DA KASPERSKY ANTI-VIRUS A KASPERSKY INTERNET SECURITY

Kaspersky Anti-Virus consente di passare a Kaspersky Internet Security senza eseguire il download e l'installazione di ulteriore software.

Kaspersky Internet Security è un'applicazione progettata per assicurare una protezione completa del computer. Offre una gamma completa di funzionalità avanzate implementate attraverso i seguenti moduli e funzioni:

- Controllo Applicazioni;
- Parental Control;
- Firewall;
- Prevenzione Intrusioni;
- Filtro Geografico;
- Blocco dell'accesso ai siti Web pericolosi;
- Monitor di Rete;
- Anti-Spam;
- Anti-Banner;
- Eliminazione della cronologia delle attività;
- Modalità Protetta.

È possibile passare temporaneamente alla versione di prova di *Kaspersky Internet Security* in modo da valutarne le funzionalità o iniziare immediatamente a utilizzare la versione commerciale dell'applicazione.

Se si utilizza la licenza con abbonamento o in particolari aree geografiche, la copia di *Kaspersky Internet Security* non consente di passare temporaneamente alla versione di prova.

IN QUESTA SEZIONE:

Passaggio alla versione commerciale	51
Passaggio temporaneo alla versione di prova.....	51

PASSAGGIO ALLA VERSIONE COMMERCIALE

Se si desidera passare alla versione commerciale di *Kaspersky Internet Security*, è necessario un codice di attivazione per la versione commerciale dell'applicazione utilizzabile per attivarla (vedere la sezione "Attivazione dell'applicazione" a pagina [38](#)).

➤ *Per acquistare un codice di attivazione per Kaspersky Internet Security:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Upgrade**.
3. Nella finestra visualizzata fare click sul pulsante **Acquista codice di attivazione**.

Verrà visualizzata la pagina Web del negozio online, in cui è possibile acquistare un codice di attivazione per *Kaspersky Internet Security*.

Se si acquista l'applicazione in particolari aree geografiche o si utilizza la licenza con abbonamento, la sezione **Upgrade** non è disponibile nella finestra principale dell'applicazione.

PASSAGGIO TEMPORANEO ALLA VERSIONE DI PROVA

È possibile passare temporaneamente alla versione di prova di *Kaspersky Internet Security* in modo da valutarne le funzionalità. Successivamente, sarà possibile scegliere di acquistare una licenza per continuare a utilizzare l'applicazione.

➤ *Per passare temporaneamente a Kaspersky Internet Security:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Upgrade**.
3. Nella finestra visualizzata fare click sul pulsante **Versione di prova**.
Verrà avviata la Configurazione guidata dell'applicazione.

Se si acquista l'applicazione in particolari aree geografiche o si utilizza la licenza con abbonamento, la sezione **Upgrade** non è disponibile nella finestra principale dell'applicazione.

Durante l'utilizzo della Configurazione guidata dell'applicazione, è necessario specificare i valori per alcune impostazioni.

Passaggio 1. Richiesta di attivazione della versione di prova di Kaspersky Internet Security

Se la richiesta di attivazione di Kaspersky Internet Security viene inviata correttamente, la procedura guidata procede automaticamente al passaggio successivo.

Passaggio 2. Avvio dell'upgrade

Durante questo passaggio, la procedura guidata visualizza un messaggio che segnala che tutti i prerequisiti per l'upgrade sono stati soddisfatti. Per procedere con la procedura guidata, fare click sul pulsante **Avanti**.

Passaggio 3. Rimozione delle applicazioni incompatibili

Durante questo passaggio, viene verificato se nel computer sono installate applicazioni incompatibili con Kaspersky Internet Security. Se non vengono rilevate applicazioni di questo tipo, la procedura guidata procede automaticamente al passaggio successivo. Se vengono rilevate applicazioni incompatibili, queste sono visualizzate in un elenco e viene offerta la possibilità di rimuoverle.

Una volta disinstallate le applicazioni incompatibili, può essere necessario riavviare il sistema operativo. Dopo il riavvio del sistema operativo, la procedura guidata riprende automaticamente il processo di upgrade.

Passaggio 4. Upgrade

Durante questo passaggio, la procedura guidata esegue la connessione dei moduli dell'upgrade. L'operazione potrebbe richiedere alcuni minuti. Al termine, la procedura passa automaticamente al passaggio successivo.

Passaggio 5. Riavvio dell'applicazione

Durante il passaggio finale dell'upgrade, è necessario riavviare l'applicazione. A tale scopo, fare click sul pulsante **Fine** nella finestra della procedura guidata.

Passaggio 6. Completamento dell'attivazione

Dopo il riavvio dell'applicazione, la procedura guidata viene aperta automaticamente. Una volta completata l'attivazione della versione di prova di Kaspersky Internet Security, la finestra della procedura guidata visualizza informazioni sul periodo di tempo per cui è possibile utilizzare la versione di prova.

Passaggio 7. Analisi del sistema

Durante questa fase vengono raccolte informazioni sulle applicazioni di Microsoft Windows. Tali applicazioni vengono aggiunte all'elenco di applicazioni attendibili, alle quali non vengono imposte restrizioni relativamente alle azioni eseguibili nel sistema.

Al termine dell'analisi, la procedura guidata passerà automaticamente al passaggio successivo.

Passaggio 8. Completamento dell'upgrade

Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**.

Non è possibile eseguire una seconda volta il passaggio alla versione di prova di Kaspersky Internet Security.

UTILIZZO DI KASPERSKY GADGET

Quando si utilizza Kaspersky Anti-Virus in un computer che esegue Microsoft Windows Vista o Microsoft Windows 7, è anche possibile utilizzare Kaspersky Gadget (di seguito denominato *gadget*). Al termine dell'installazione di Kaspersky Anti-Virus in un computer con sistema operativo Microsoft Windows 7, il gadget viene visualizzato automaticamente sul desktop. Al termine dell'installazione dell'applicazione in un computer con sistema operativo Microsoft Windows Vista, è necessario aggiungere manualmente il gadget a Windows Sidebar (vedere la documentazione del sistema operativo).

L'indicatore colorato del gadget visualizza lo stato della protezione del computer nello stesso modo dell'indicatore nella finestra principale dell'applicazione (vedere la sezione "Diagnostica ed eliminazione dei problemi relativi alla protezione del computer" a pagina 35). Il colore verde indica che il computer è protetto in modo adeguato, il giallo indica che vi sono problemi di protezione e il rosso indica che la protezione del computer è a rischio. Il colore grigio indica che l'applicazione è stata arrestata.

Durante l'aggiornamento dei database dell'applicazione e dei moduli software, viene visualizzata l'icona di un globo che ruota al centro del gadget.

È possibile utilizzare il gadget per eseguire le seguenti azioni:

- riprendere l'esecuzione dell'applicazione se è stata sospesa in precedenza;
- aprire la finestra principale dell'applicazione;
- eseguire la scansione virus degli oggetti specificati;
- aprire la finestra delle notizie.

È inoltre possibile configurare i pulsanti del gadget in modo da avviare ulteriori azioni:

- eseguire un aggiornamento;
- modificare le impostazioni dell'applicazione;
- visualizzare i rapporti dell'applicazione;
- sospendere la protezione;
- aprire la Tastiera Virtuale;
- aprire la finestra Gestione attività.

➤ *Per avviare l'applicazione utilizzando il gadget:*

Fare click sull'icona  **Abilita** al centro del gadget.

➤ *Per aprire la finestra principale dell'applicazione utilizzando il gadget:*


Fare click sull'icona del monitor al centro del gadget.

➤ *Per eseguire la scansione antivirus di un oggetto utilizzando il gadget:*


trascinare l'oggetto da esaminare nel gadget.

Lo stato di avanzamento dell'attività verrà visualizzato nella finestra **Gestione attività**.

➤ *Per aprire la finestra delle notizie utilizzando il gadget:*

Fare click sull'icona  visualizzata al centro del gadget quando è disponibile una notizia.

➤ *Per configurare il gadget:*

1. Aprire la finestra delle impostazioni del gadget facendo click sull'icona  visualizzata nell'angolo superiore destro del gadget quando si posiziona il puntatore del mouse su di esso.
2. Dagli elenchi a discesa corrispondenti ai pulsanti del gadget, selezionare le azioni da eseguire quando si fa click su tali pulsanti.
3. Fare click sul pulsante **OK**.

COME OTTENERE INFORMAZIONI SULLA REPUTAZIONE DI UN'APPLICAZIONE

Kaspersky Anti-Virus consente di ottenere informazioni sulla reputazione delle applicazioni da utenti di tutto il mondo. La reputazione di un'applicazione comprende i seguenti criteri:

- nome del produttore;
- informazioni sulla firma digitale (disponibili se è presente una firma digitale);
- informazioni sul gruppo in cui l'applicazione è stata inclusa dalla maggior parte degli utenti di Kaspersky Security Network;
- numero di utenti di Kaspersky Security Network che utilizzano l'applicazione (disponibile se l'applicazione è stata inclusa nel gruppo Attendibili nel database di Kaspersky Security Network);
- ora in cui l'applicazione è diventata nota in Kaspersky Security Network;
- paesi in cui l'applicazione è più diffusa.

Per verificare la reputazione di un'applicazione, è necessario accettare di partecipare a Kaspersky Security Network (vedere pagina [109](#)) durante l'installazione di Kaspersky Anti-Virus.

◆ *Per ottenere informazioni sulla reputazione di un'applicazione:*

Aprire il menu di scelta rapida del file eseguibile dell'applicazione, quindi selezionare **Controlla reputazione in KSN**.

VEDERE ANCHE:

Kaspersky Security Network [109](#)

IMPOSTAZIONI AVANZATE DELL'APPLICAZIONE

In questa sezione vengono fornite informazioni dettagliate sulla configurazione di ognuno dei componenti dell'applicazione.

IN QUESTA SEZIONE:

Impostazioni generali di protezione	55
Scansione	56
Aggiornamento	64
Anti-Virus File	68
Anti-Virus Posta	73
Anti-Virus Web	77
Anti-Virus IM	82
Difesa Proattiva	84
Controllo sistema	86
Protezione della rete	87
Area attendibile	91
Prestazioni e compatibilità con altre applicazioni	92
Auto-Difesa di Kaspersky Anti-Virus	95
Quarantena e Backup	96
Strumenti aggiuntivi per una migliore protezione del computer	99
Rapporti	103
Aspetto dell'applicazione. Gestione degli elementi attivi dell'interfaccia	106
Notifiche	107
Kaspersky Security Network	109

IMPOSTAZIONI GENERALI DI PROTEZIONE

Nella finestra delle impostazioni dell'applicazione, nell'area **Impostazioni generali** della sezione **Centro protezione**, è possibile:

- disabilitare tutti i componenti di protezione (vedere la sezione "Abilitazione e disabilitazione della protezione" a pagina [35](#));
- selezionare la modalità di protezione interattiva o automatica (vedere la sezione "Selezione della modalità di protezione" a pagina [56](#));
- limitare l'accesso degli utenti all'applicazione impostando una password (vedere la sezione "Restrizione dell'accesso a Kaspersky Anti-Virus" a pagina [56](#));
- disabilitare o abilitare l'esecuzione automatica dell'applicazione all'avvio del sistema operativo (vedere la sezione "Abilitazione e disabilitazione dell'avvio automatico" a pagina [34](#));
- abilitare una combinazione di tasti personalizzata per visualizzare la Tastiera Virtuale (vedere la sezione "Protezione dall'intercettazione dei dati immessi tramite la tastiera" a pagina [43](#)).

IN QUESTA SEZIONE:

Restrizione dell'accesso a Kaspersky Anti-Virus.....	56
Selezione di una modalità di protezione.....	56

RESTRIZIONE DELL'ACCESSO A KASPERSKY ANTI-VIRUS

Un computer può essere utilizzato da diversi utenti, con differenti livelli di esperienza. Concedere agli utenti un accesso senza limitazioni a Kaspersky Anti-Virus e alle relative impostazioni può ridurre il livello di protezione del computer.

Per limitare l'accesso all'applicazione, è possibile impostare una password e specificare le azioni che richiedono l'immissione della password:

- modifica delle impostazioni dell'applicazione;
- chiusura dell'applicazione;
- rimozione dell'applicazione.

Prestare attenzione durante l'utilizzo di una password per limitare l'accesso alla rimozione dell'applicazione. Se si dimentica la password, sarà difficile rimuovere l'applicazione dal computer.

► *Per limitare l'accesso a Kaspersky Anti-Virus tramite una password:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare **Impostazioni generali**.
3. Nella parte destra della finestra, nella sezione **Protezione dell'applicazione tramite password**, selezionare la casella **Abilita la protezione tramite password** e fare click sul pulsante **Impostazioni**.
4. Nella finestra **Protezione dell'applicazione tramite password** visualizzata immettere la password e specificare l'area a cui applicare la limitazione dell'accesso.

SELEZIONE DI UNA MODALITÀ DI PROTEZIONE

Per impostazione predefinita, Kaspersky Anti-Virus viene eseguito in *modalità di protezione automatica*. In questa modalità, l'applicazione applica automaticamente le azioni consigliate da Kaspersky Lab in risposta agli eventi pericolosi. Se si desidera che Kaspersky Anti-Virus invii notifiche di tutti gli eventi pericolosi e sospetti nel sistema e consenta all'utente di decidere quali azioni applicare, è possibile abilitare la *modalità di protezione interattiva*.

► *Per selezionare la modalità di protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare **Impostazioni generali**.
3. Nella sezione **Protezione interattiva** selezionare o deselezionare le caselle a seconda della modalità di protezione desiderata:
 - per abilitare la modalità di protezione interattiva, deselezionare la casella **Seleziona azione automaticamente**;
 - per abilitare la modalità di protezione automatica, selezionare la casella **Seleziona azione automaticamente**.

Se non si desidera che Kaspersky Anti-Virus elimini gli oggetti sospetti quando viene eseguito in modalità automatica, selezionare la casella **Non eliminare gli oggetti sospetti**.

SCANSIONE

La scansione del computer per la verifica della presenza di vulnerabilità, virus e altro riskware è una delle attività più importanti per garantire la sicurezza del computer.

È necessario eseguire periodicamente una scansione anti-virus e del riskware per eliminare la possibilità che si diffondano programmi dannosi non rilevati dai componenti di protezione, ad esempio perché è stato impostato un livello di protezione basso o per altri motivi.

La ricerca delle vulnerabilità esegue la diagnostica del sistema operativo e consente di rilevare le vulnerabilità software che possono essere utilizzate da utenti malintenzionati per diffondere oggetti dannosi e ottenere l'accesso a informazioni personali.

In questa sezione sono disponibili informazioni su funzionalità e configurazione delle attività di scansione, livelli di protezione, metodi di scansione e tecnologie di scansione.

IN QUESTA SEZIONE:

Scansione virus.....	57
Scansione Vulnerabilità.....	63
Gestione delle attività di scansione. Gestione attività	63

SCANSIONE VIRUS

Per il rilevamento di virus e altri riskware, Kaspersky Anti-Virus include le seguenti attività:

- **Scansione Completa.** Scansione dell'intero sistema. Per impostazione predefinita, Kaspersky Anti-Virus esamina i seguenti oggetti:
 - memoria del sistema;
 - oggetti caricati all'avvio del sistema operativo;
 - backup del sistema;
 - database di posta elettronica;
 - supporti di archiviazione rimovibili, dischi rigidi e unità di rete.
- **Scansione delle aree critiche.** Per impostazione predefinita, Kaspersky Anti-Virus esamina gli oggetti caricati all'avvio del sistema operativo.
- **Scansione Personalizzata.** Kaspersky Anti-Virus esegue la scansione degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi dei seguenti oggetti:
 - memoria del sistema;
 - oggetti caricati all'avvio del sistema operativo;
 - backup del sistema;
 - database di posta elettronica;
 - supporti di archiviazione rimovibili, dischi rigidi e unità di rete;
 - qualsiasi file o cartella selezionata dall'utente.

Le attività Scansione Completa e Scansione delle aree critiche presentano alcune particolarità. Per queste attività, non è consigliabile modificare gli elenchi degli oggetti da esaminare.

Ogni attività di scansione viene eseguita in un'area specificata e può essere avviata in base a una pianificazione creata precedentemente. Ogni attività di scansione è inoltre caratterizzata da un livello di protezione (una combinazione di impostazioni che influiscono sul livello di approfondimento della scansione). Per impostazione predefinita, la *modalità firma* (in cui vengono utilizzati i record dei database dell'applicazione per la ricerca delle minacce) è sempre abilitata. È inoltre possibile applicare diversi metodi e tecnologie di scansione.

Dopo l'avvio dell'attività di scansione completa o di scansione delle aree critiche, lo stato di avanzamento della scansione viene visualizzato nella finestra **Scansione**, nella sezione con il nome dell'attività in esecuzione, e in Gestione attività (vedere la sezione "Gestione delle attività di scansione" Gestione attività" a pagina [63](#)).

Se vengono rilevate minacce, Kaspersky Anti-Virus assegna uno degli stati seguenti all'oggetto rilevato:

- Programma dannoso, ad esempio nel caso di un *virus* o di un *Trojan*.
- *Potenzialmente infetto* (sospetto), se non è possibile stabilire se l'oggetto è infetto o meno. Il file può contenere una sequenza di codice caratteristica dei virus o un codice modificato di un virus conosciuto.

L'applicazione visualizza una notifica (vedere pagina [107](#)) della minaccia rilevata e ed esegue l'azione impostata. È possibile modificare le azioni da eseguire quando viene rilevata una minaccia.

Se si utilizza la modalità automatica (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)), quando vengono rilevati oggetti pericolosi, Kaspersky Anti-Virus applica automaticamente l'azione raccomandata dagli specialisti di Kaspersky Lab. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce e Sposta in Quarantena** per gli oggetti sospetti. Se vengono rilevati oggetti pericolosi durante l'utilizzo della modalità interattiva (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)), l'applicazione visualizza una notifica che è possibile utilizzare per selezionare l'azione desiderata dall'elenco delle azioni disponibili.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento. Gli oggetti sospetti (potenzialmente infetti) sono messi in quarantena. È possibile abilitare la scansione automatica degli oggetti in quarantena dopo ogni aggiornamento.

Le informazioni sui risultati della scansione e sugli eventi che si sono verificati durante l'esecuzione dell'attività vengono registrate in un rapporto di Kaspersky Anti-Virus (vedere pagina [103](#)).

IN QUESTA SEZIONE:

Modifica e ripristino del livello di protezione	58
Creazione della pianificazione di avvio della scansione	59
Creazione di un elenco di oggetti da esaminare	59
Selezione di un metodo di scansione	60
Selezione della tecnologia di scansione	60
Modifica delle azioni da eseguire quando viene rilevata una minaccia	61
Esecuzione di una scansione tramite un altro account utente	61
Modifica del tipo di oggetti da esaminare	61
Scansione dei file composti	61
Ottimizzazione della scansione	62
Scansione delle unità rimovibili alla connessione	62
Creazione di un collegamento per un'attività	63

MODIFICA E RIPRISTINO DEL LIVELLO DI PROTEZIONE

A seconda delle proprie esigenze, è possibile selezionare uno dei livelli di protezione preimpostati o modificare le attività di scansione manualmente.

Durante la configurazione delle impostazioni delle attività di scansione, è sempre possibile ripristinare quelle consigliate. Tali impostazioni, che consentono di ottenere una configurazione ottimale e sono consigliate da Kaspersky Lab, sono raggruppate nel livello di protezione **Consigliato**.

► Per modificare il livello di protezione impostato:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** impostare il livello di protezione desiderato per l'attività selezionata o fare click sul pulsante **Impostazioni** per modificare manualmente le impostazioni di scansione.

Se si modificano manualmente le impostazioni, il nome del livello di protezione diventerà **Personalizzato**.

➤ *Per ripristinare le impostazioni predefinite di scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Livello predefinito** per l'attività selezionata.

CREAZIONE DELLA PIANIFICAZIONE DI AVVIO DELLA SCANSIONE

È possibile creare una pianificazione per avviare automaticamente le attività di scansione virus, specificando la frequenza di esecuzione dell'attività, l'ora di avvio (se necessario) e le impostazioni avanzate.

Se per qualsiasi motivo non è possibile avviare l'attività, ad esempio perché all'ora prevista il computer è spento, è possibile configurare l'attività non eseguita in modo che venga avviata automaticamente non appena possibile. È possibile sospendere automaticamente la scansione quando 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. L'attività di scansione non richiederà pertanto l'utilizzo delle risorse del sistema durante le ore lavorative.

La speciale modalità di scansione a PC inattivo (vedere la sezione "Esecuzione di attività in background" a pagina [94](#)) consente di avviare l'aggiornamento automatico mentre il PC è inattivo.

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

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Vulnerabilità**).
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Pianificazione** della scheda **Modalità di esecuzione**, selezionare **In base alla pianificazione** e configurare la modalità di esecuzione della scansione specificando i valori desiderati per l'impostazione **Frequenza**.

➤ *Per abilitare l'avvio automatico di un'attività non eseguita:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Vulnerabilità**).
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Pianificazione** della scheda **Modalità di esecuzione**, selezionare **In base alla pianificazione** e selezionare la casella **Esegui attività ignorate**.

➤ *Per avviare le scansioni solo quando il computer non è in uso:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Vulnerabilità**).
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Pianificazione** della scheda **Modalità di esecuzione**, selezionare **In base alla pianificazione**, quindi selezionare la casella **Esegui scansione quando lo screensaver è attivo o il computer è bloccato**.

CREAZIONE DI UN ELENCO DI OGGETTI DA ESAMINARE

Ogni scansione virus comprende un elenco predefinito di oggetti. Tali oggetti possono includere elementi del file system del computer, quali le unità logiche e i database di posta elettronica, o altri tipi di oggetti quali le unità di rete. L'elenco può essere modificato.

Se l'ambito della scansione è vuoto o non contiene oggetti selezionati, non è possibile avviare l'attività di scansione.

➤ *Per creare un elenco di oggetti per un'attività di scansione personalizzata:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Scansione**.
3. Nella parte inferiore della finestra visualizzata fare click sul collegamento **specificare** per aprire un elenco degli oggetti da esaminare.
4. Nella finestra **Scansione Personalizzata** visualizzata fare click sul pulsante **Aggiungi**.
5. Nella finestra **Scelta degli oggetti da esaminare** visualizzata selezionare l'oggetto desiderato e fare click sul pulsante **Aggiungi**. Fare click sul pulsante **OK** dopo aver aggiunto tutti gli oggetti desiderati. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselegionare la relativa casella.

È inoltre possibile trascinare i file da esaminare direttamente nell'apposita area nella sezione **Scansione**.

➤ *Per creare un elenco di oggetti per le attività Scansione Completa, Scansione delle aree critiche o Scansione Vulnerabilità:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività di scansione desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Vulnerabilità**).
3. Nella parte destra della finestra fare click sul pulsante **Ambito della scansione**.
4. Nella finestra **Ambito della scansione** visualizzata utilizzare i pulsanti **Aggiungi**, **Modifica** ed **Elimina** per creare un elenco. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselegionare la relativa casella.

Gli oggetti che appaiono nell'elenco per impostazione predefinita non possono essere modificati né eliminati.

SELEZIONE DI UN METODO DI SCANSIONE

Durante la scansione anti-virus viene sempre utilizzata l'*analisi delle firme*; Kaspersky Anti-Virus confronta l'oggetto rilevato con i record nel relativo database.

È possibile utilizzare ulteriori metodi di scansione per incrementare l'efficienza della scansione: l'*analisi euristica* (analisi delle azioni eseguite da un oggetto all'interno del sistema) e la *ricerca di rootkit* (ricerca di strumenti in grado di nascondere programmi dannosi nel sistema operativo).

➤ *Per selezionare il metodo di scansione da utilizzare:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella sezione **Metodi di scansione** della scheda **Avanzate**, selezionare i metodi di scansione desiderati.

SELEZIONE DELLA TECNOLOGIA DI SCANSIONE

Oltre ai metodi di scansione, è possibile utilizzare speciali tecnologie di scansione degli oggetti che consentono di incrementare la velocità di scansione anti-virus escludendo i file che non sono stati modificati dall'ultima scansione.

➤ *Per specificare le tecnologie di scansione degli oggetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella sezione **Tecnologie di scansione** della scheda **Avanzate**, selezionare i valori desiderati.

MODIFICA DELLE AZIONI DA ESEGUIRE QUANDO VIENE RILEVATA UNA MINACCIA

Se vengono rilevati oggetti infetti, l'applicazione esegue l'azione selezionata.

➤ *Per modificare l'azione da eseguire quando viene rilevata una minaccia:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella parte destra della finestra selezionare l'opzione desiderata nella sezione **Azione se viene rilevata una minaccia**.

ESECUZIONE DI UNA SCANSIONE TRAMITE UN ALTRO ACCOUNT UTENTE

Per impostazione predefinita, le attività di scansione vengono eseguite utilizzando il proprio account utente. Può essere tuttavia necessario eseguire un'attività tramite un altro account utente. È possibile specificare un account utilizzato dall'applicazione durante l'esecuzione di un'attività di scansione.

➤ *Per avviare una scansione tramite un altro account utente:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Vulnerabilità**).
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Account utente** della scheda **Modalità di esecuzione**, selezionare la casella **Esegui l'attività come**. Specificare il nome utente e la password.

MODIFICA DEL TIPO DI OGGETTI DA ESAMINARE

Quando si specificano i tipi di oggetti da esaminare, vengono definiti i formati dei file su cui verrà eseguita l'attività di scansione virus selezionata.

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

- La probabilità di penetrazione di codice dannoso in alcuni formati di file (ad esempio TXT) e la successiva attivazione è piuttosto bassa. Altri formati, al contrario, contengono o possono contenere codice eseguibile (EXE, DLL, DOC). Il rischio di penetrazione ed attivazione di codice dannoso in tali file è piuttosto alto.
- Un utente malintenzionato potrebbe inviare al computer un virus in un file eseguibile rinominato come TXT. Se è stata selezionata la scansione dei file in base all'estensione, tale file verrà ignorato dalla scansione. Se è stata selezionata la scansione dei file in base al formato, indipendentemente dall'estensione, Anti-Virus File analizzerà l'intestazione del file e rivelerà che si tratta di un file EXE. Tale file sarà sottoposto a una scansione virus approfondita.

➤ *Per modificare il tipo di oggetti da esaminare:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella sezione **Tipi di file** della scheda **Ambito**, selezionare l'opzione desiderata.

SCANSIONE DEI FILE COMPOSITI

Un metodo comune per nascondere i virus è incorporarli in file compositi: archivi, pacchetti di installazione, oggetti OLE incorporati e formati di file di posta. Per rilevare i virus nascosti in questo modo, è necessario decomprimere i file compositi, cosa che può ridurre significativamente la velocità di scansione.

Per ogni tipo di file composito, è possibile scegliere di esaminare tutti i file oppure solo quelli nuovi. Per effettuare la selezione, fare click sul collegamento accanto al nome dell'oggetto. Il relativo valore verrà modificato quando si fa click con il pulsante sinistro del mouse su di esso. Se si seleziona la modalità di scansione dei soli file nuovi e modificati (vedere pagina [62](#)), non saranno disponibili i collegamenti che consentono di esaminare tutti i file o solo quelli nuovi.

È possibile limitare la dimensione massima di un file composto da esaminare. I file composti di dimensioni maggiori di quelle specificate non saranno esaminati.

I file di grandi dimensioni estratti dagli archivi verranno esaminati anche se la casella **Non decomprimere i file composti molto grandi** è selezionata.

➤ *Per modificare l'elenco dei file composti da esaminare:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella sezione **Scansione dei file composti** della scheda **Ambito**, selezionare i tipi di file composti che si desidera esaminare.

➤ *Per impostare la dimensione massima dei file composti da esaminare:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella sezione **Scansione dei file composti** della scheda **Ambito**, fare click sul pulsante **Avanzate**.
5. Nella finestra **File composti** visualizzata selezionare la casella **Non decomprimere i file composti molto grandi** e specificare la dimensione massima del file.

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 modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che composti.

È anche possibile limitare la durata della scansione di un oggetto. Al termine dell'intervallo di tempo specificato, l'oggetto verrà escluso dalla scansione corrente (ad eccezione degli archivi e dei file composti da più oggetti).

➤ *Per eseguire la scansione solo dei file nuovi e modificati:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella sezione **Ottimizzazione della scansione** della scheda **Ambito**, selezionare la casella **Esamina solo i file nuovi e modificati**.

➤ *Per limitare la durata della scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare l'attività desiderata (**Scansione Completa**, **Scansione delle aree critiche** o **Scansione Personalizzata**).
3. Nella sezione **Livello di protezione** fare click sul pulsante **Impostazioni** per l'attività selezionata.
4. Nella finestra visualizzata, nella sezione **Ottimizzazione della scansione** della scheda **Ambito**, selezionare la casella **Ignora gli oggetti analizzati per più di** e specificare la durata della scansione di un singolo file.

SCANSIONE DELLE UNITÀ RIMOVIBILI ALLA CONNESSIONE

Gli oggetti dannosi che utilizzano le vulnerabilità del sistema operativo per replicarsi tramite reti e supporti rimovibili si stanno diffondendo sempre di più. Kaspersky Anti-Virus consente di eseguire la scansione delle unità rimovibili quando vengono connesse al computer.

► *Per configurare la scansione delle unità rimovibili al momento della connessione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare **Impostazioni generali**.
3. Nella sezione **Scansione automatica delle unità rimovibili** selezionare l'azione e, se necessario, definire la dimensione massima dell'unità da esaminare nel campo sottostante.

CREAZIONE DI UN COLLEGAMENTO PER UN'ATTIVITÀ

L'applicazione offre la possibilità di creare collegamenti per avviare le attività di scansione completa, di scansione rapida e di ricerca delle vulnerabilità. In questo modo è possibile avviare la scansione desiderata senza aprire la finestra principale dell'applicazione o un menu di scelta rapida.

► *Per creare un collegamento per l'avvio di una scansione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare **Impostazioni generali**.
3. Nella parte destra della finestra, nella sezione **Esecuzione rapida delle attività di scansione**, fare click sul pulsante **Crea collegamento** accanto al nome dell'attività desiderata (**Scansione delle aree critiche**, **Scansione Completa** o **Scansione Vulnerabilità**).
4. Nella finestra visualizzata specificare il nome del collegamento e il percorso in cui salvarlo. Per impostazione predefinita, il collegamento viene creato con il nome di un'attività nella cartella Risorse del computer dell'utente corrente.

SCANSIONE VULNERABILITÀ

Le vulnerabilità possono comparire nel sistema operativo per diversi motivi, ad esempio a causa di errori di programmazione, password non sicure o azioni di programmi dannosi. Durante l'esecuzione della scansione delle vulnerabilità, l'applicazione esegue varie procedure di protezione, ad esempio l'analisi del sistema, l'analisi delle impostazioni del sistema operativo e del browser e la ricerca di servizi vulnerabili.

La diagnostica può richiedere alcuni minuti. Al termine, i problemi rilevati vengono analizzati dal punto di vista della loro pericolosità per il sistema.

Dopo l'avvio dell'attività di scansione delle vulnerabilità (vedere pagina [42](#)), lo stato di avanzamento viene visualizzato nella finestra **Scansione** (nella sezione **Scansione Vulnerabilità**) e in Gestione attività (vedere la sezione "Gestione delle attività di scansione. Gestione attività" a pagina [63](#)).

Le informazioni sui risultati di un'attività di scansione delle vulnerabilità vengono registrate in un rapporto di Kaspersky Anti-Virus (vedere pagina [103](#)).

Come nel caso delle attività di scansione virus, è possibile impostare una pianificazione per l'avvio delle attività di ricerca delle vulnerabilità, creare un elenco di oggetti da esaminare (vedere pagina [59](#)), specificare un account (vedere la sezione "Esecuzione di una scansione tramite un altro account utente" a pagina [61](#)) e creare un collegamento per avviare rapidamente l'attività. Per impostazione predefinita, le applicazioni già installate nel computer vengono selezionate come oggetti da esaminare.

GESTIONE DELLE ATTIVITÀ DI SCANSIONE. GESTIONE ATTIVITÀ

Visualizza informazioni sulle attività di scansione eseguite più di recente o attualmente in esecuzione (ad esempio, scansione virus, scansione vulnerabilità, ricerca di rootkit o disinfezione avanzata).

È possibile utilizzare Gestione attività per visualizzare lo stato di avanzamento e i risultati di un'attività di scansione oppure per interrompere l'attività. Per alcune attività sono inoltre disponibili ulteriori azioni (ad esempio, al termine di una scansione vulnerabilità, è possibile aprire l'elenco delle vulnerabilità rilevate e correggerle).

► *Per aprire Gestione attività:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Scansione**.
3. Nella finestra **Scansione** visualizzata fare click sul pulsante **Gestione attività** nell'angolo superiore destro.

AGGIORNAMENTO

L'aggiornamento dei database e dei moduli del programma di Kaspersky Anti-Virus assicura il massimo livello di protezione per il computer. In tutto il mondo appaiono quotidianamente nuovi virus, Trojan e altri tipi di malware. Le informazioni sulle minacce e sui metodi che consentono di neutralizzarle sono contenute nei database di Kaspersky Anti-Virus. Per un rilevamento tempestivo delle nuove minacce, è necessario aggiornare periodicamente i database e i moduli dell'applicazione.

Per gli aggiornamenti periodici è necessaria una licenza attiva per l'utilizzo dell'applicazione. Se non è installata alcuna licenza, è possibile eseguire un aggiornamento una sola volta.

Quando si esegue un aggiornamento, l'applicazione scarica e installa i seguenti oggetti nel computer:

- Database di Kaspersky Anti-Virus.

La protezione delle informazioni è assicurata da database che contengono firme delle minacce, descrizioni degli attacchi di rete e informazioni per contrastarli. I componenti di protezione utilizzano queste informazioni per rilevare e disinfettare gli oggetti pericolosi nel computer. I database vengono aggiornati ogni ora con nuovi record relativi alle nuove minacce e ai metodi per neutralizzarle. È pertanto consigliabile aggiornare i database regolarmente.

Oltre ai database di Kaspersky Anti-Virus, vengono aggiornati i driver di rete che consentono ai componenti dell'applicazione di intercettare il traffico di rete.

- Moduli dell'applicazione.

Oltre ai database di Kaspersky Anti-Virus, è anche possibile aggiornare i moduli del programma. Gli aggiornamenti dei moduli dell'applicazione risolvono le vulnerabilità di Kaspersky Anti-Virus e arricchiscono o migliorano le funzionalità esistenti.

Durante un aggiornamento, i moduli dell'applicazione e i database nel computer vengono confrontati con la versione aggiornata disponibile nella sorgente degli aggiornamenti. Se i database e i moduli dell'applicazione correnti sono differenti da quelli della versione più recente dell'applicazione, la parte mancante di aggiornamenti verrà installata nel computer.

Se i database sono obsoleti, il pacchetto di aggiornamento può essere di grandi dimensioni, causando traffico Internet aggiuntivo (fino a decine di MB).

Prima di procedere all'aggiornamento dei database, Kaspersky Anti-Virus ne crea delle copie di backup, qualora si decida di eseguire il rollback alla versione precedente (vedere la sezione "Rollback dell'ultimo aggiornamento" a pagina [67](#)).

Le informazioni sulla condizione corrente dei database di Kaspersky Anti-Virus sono visualizzate nella sezione **Aggiornamento** della finestra principale dell'applicazione.

Le informazioni sui risultati dell'aggiornamento e sugli eventi che si sono verificati durante l'esecuzione dell'attività vengono registrate in un rapporto di Kaspersky Anti-Virus (vedere pagina [103](#)).

È possibile selezionare una sorgente degli aggiornamenti (vedere la sezione "Selezione della sorgente degli aggiornamenti" a pagina [64](#)) e configurare l'avvio automatico dell'aggiornamento.

IN QUESTA SEZIONE:

Selezione della sorgente degli aggiornamenti.....	64
Creazione della pianificazione di avvio degli aggiornamenti	66
Rollback dell'ultimo aggiornamento.....	67
Esecuzione di aggiornamenti tramite un altro account utente	67
Utilizzo di un server proxy	67

SELEZIONE DELLA SORGENTE DEGLI AGGIORNAMENTI

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

Le principali sorgenti degli aggiornamenti sono i server degli aggiornamenti di Kaspersky Lab, in cui sono memorizzati gli aggiornamenti dei database e dei moduli dell'applicazione per tutti i prodotti Kaspersky Lab.

Il computer deve essere connesso a Internet per il download degli aggiornamenti dai server di Kaspersky Lab. Per impostazione predefinita, le impostazioni di connessione a Internet vengono determinate automaticamente. Se si utilizza un server proxy, può essere necessario regolare le impostazioni di connessione (vedere la sezione "Configurazione del server proxy" a pagina [90](#)).

Durante l'aggiornamento di Kaspersky Anti-Virus, è possibile copiare gli aggiornamenti dei database e dei moduli del programma ricevuti dai server di Kaspersky Lab in una cartella locale (vedere la sezione "Aggiornamento dell'applicazione da una cartella condivisa" a pagina [65](#)); e quindi fornire l'accesso agli altri computer della rete. Questo consente di ridurre il traffico Internet.

Se non è possibile accedere ai server degli aggiornamenti di Kaspersky Lab, ad esempio in assenza di una connessione a Internet, chiamare la sede centrale (<http://www.kaspersky.com/contacts>) di Kaspersky Lab per richiedere informazioni sui partner Kaspersky Lab che possono fornire aggiornamenti su supporti rimovibili.

Quando si ordinano aggiornamenti su un supporto rimovibile, specificare se si desiderano anche gli aggiornamenti dei moduli dell'applicazione.

AGGIUNTA DI UNA SORGENTE DEGLI AGGIORNAMENTI

Per impostazione predefinita, l'elenco contiene solo i server degli aggiornamenti di Kaspersky Lab. È possibile aggiungere una cartella locale o un server differente come sorgente degli aggiornamenti. Se sono state selezionate più risorse come sorgenti degli aggiornamenti, Kaspersky Anti-Virus tenta 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 aggiungere una sorgente degli aggiornamenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Sorgente degli aggiornamenti** nella parte destra della finestra.
4. Nella finestra visualizzata, nella scheda **Sorgente**, aprire la finestra di selezione facendo click sul pulsante **Aggiungi**.
5. Nella finestra **Sorgente degli aggiornamenti** visualizzata selezionare la cartella che contiene gli aggiornamenti o immettere un indirizzo nel campo **Sorgente** per specificare il server da cui scaricare gli aggiornamenti.

SELEZIONE DELLA NAZIONE DEL SERVER DEGLI AGGIORNAMENTI

Se si utilizzano i server di Kaspersky Lab come sorgente degli aggiornamenti, è possibile selezionare la posizione ottimale del server da cui scaricare i file. I server Kaspersky Lab sono dislocati in più paesi.

Utilizzando il server degli aggiornamenti Kaspersky Lab più vicino, è possibile ridurre il tempo necessario per la ricezione degli aggiornamenti e aumentare le prestazioni. Per impostazione predefinita, l'applicazione utilizza le informazioni sulla nazione corrente dal registro del sistema operativo. È possibile selezionare la nazione manualmente.

◆ Per selezionare la nazione del server:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Sorgente degli aggiornamenti** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Impostazioni internazionali** della scheda **Sorgente**, selezionare l'opzione **Seleziona dall'elenco**, quindi scegliere il paese più vicino alla propria posizione corrente nell'elenco a discesa.

AGGIORNAMENTO DELL'APPLICAZIONE DA UNA CARTELLA CONDIVISA

Per ridurre il traffico Internet, è possibile configurare l'aggiornamento di Kaspersky Anti-Virus da una cartella condivisa quando si aggiorna l'applicazione nei computer della rete. In questo caso uno dei computer della rete riceve un pacchetto di aggiornamento dai server di Kaspersky Lab o da un'altra risorsa Web che contiene il set di aggiornamenti

desiderato. Gli aggiornamenti ricevuti vengono copiati in una cartella condivisa. Gli altri computer della rete accedono a questa cartella per ricevere gli aggiornamenti per Kaspersky Anti-Virus.

Se si esegue l'accesso con un account guest in Microsoft Windows 7, gli aggiornamenti non vengono copiati nella cartella condivisa. È consigliabile eseguire l'accesso con un account differente per consentire la copia degli aggiornamenti.

➤ *Per abilitare la modalità di distribuzione degli aggiornamenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Selezionare la casella **Copia aggiornamenti nella cartella** nella sezione **Avanzate** e specificare nel campo sottostante il percorso di una cartella pubblica in cui verranno copiati tutti gli aggiornamenti scaricati. È anche possibile selezionare una cartella facendo click sul pulsante **Sfoggia**.

➤ *Per scaricare gli aggiornamenti per il computer da una cartella condivisa specificata:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Sorgente degli aggiornamenti** nella parte destra della finestra.
4. Nella finestra visualizzata, nella scheda **Sorgente**, aprire la finestra di selezione facendo click sul pulsante **Aggiungi**.
5. Nella finestra **Sorgente degli aggiornamenti** visualizzata selezionare la cartella contenente gli aggiornamenti o immetterne il percorso completo nel campo **Sorgente**.
6. Nella scheda **Sorgente** deselezionare la casella **Server degli aggiornamenti Kaspersky Lab**.

CREAZIONE DELLA PIANIFICAZIONE DI AVVIO DEGLI AGGIORNAMENTI

È possibile creare una pianificazione per avviare automaticamente le attività di aggiornamento, specificando la frequenza, l'ora di avvio (se necessario) e le impostazioni avanzate.

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

È anche possibile rimandare l'esecuzione automatica dell'attività dopo l'avvio dell'applicazione. Tutte le attività pianificate verranno eseguite solo dopo il periodo di tempo specificato dall'avvio di Kaspersky Anti-Virus.

La speciale modalità di scansione a PC inattivo (vedere la sezione "Esecuzione di attività in background" a pagina [94](#)) consente di avviare l'aggiornamento automatico mentre il PC è inattivo.

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

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Pianificazione** della scheda **Modalità di esecuzione**, selezionare **In base alla pianificazione** e configurare la modalità di esecuzione dell'aggiornamento.

➤ *Per abilitare l'avvio automatico di un'attività non eseguita:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Pianificazione** della scheda **Modalità di esecuzione**, selezionare **In base alla pianificazione** e selezionare la casella **Esegui attività ignorate**.

➤ *Per rimandare l'esecuzione di un'attività dopo l'avvio dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Pianificazione** della scheda **Modalità di esecuzione**, selezionare **In base alla pianificazione** e specificare il tempo per cui rimandare l'esecuzione dell'attività nel campo **Rimanda l'esecuzione dopo l'avvio dell'applicazione per**.


ROLLBACK DELL'ULTIMO AGGIORNAMENTO

Dopo il primo aggiornamento di Kaspersky Anti-Virus, diventa disponibile l'opzione per il rollback ai database precedenti.

La funzionalità di rollback degli aggiornamenti è utile quando una nuova versione dei database contiene una firma non valida che determina il blocco di un'applicazione sicura da parte di Kaspersky Anti-Virus.

In caso di danneggiamento dei database di Kaspersky Anti-Virus, è consigliabile eseguire l'attività di aggiornamento per scaricare un set di database aggiornato.

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

1. Aprire la finestra principale dell'applicazione.
2. Selezionare la sezione **Aggiornamento** nella parte inferiore della finestra.
3. Nella finestra **Aggiornamento** visualizzata fare click sul pulsante , quindi selezionare **Rollback ai database precedenti** dal menu visualizzato.

ESECUZIONE DI AGGIORNAMENTI TRAMITE UN ALTRO ACCOUNT

UTENTE

Per impostazione predefinita, la procedura di aggiornamento viene eseguita utilizzando il proprio account utente. Kaspersky Anti-Virus può tuttavia eseguire l'aggiornamento da un'origine per la quale non si dispone di diritti di accesso, ad esempio una cartella di rete contenente aggiornamenti, o di credenziali utente di un proxy autorizzato. È possibile eseguire gli aggiornamenti di Kaspersky Anti-Virus per conto di un account utente che dispone di tali diritti.

➤ *Per avviare l'aggiornamento utilizzando un altro account utente:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Modalità di esecuzione** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Account utente** della scheda **Modalità di esecuzione**, selezionare la casella **Esegui l'attività come**. Specificare il nome utente e la password.

UTILIZZO DI UN SERVER PROXY

Se si utilizza un server proxy per la connessione a Internet, è necessario impostare i parametri di connessione per il corretto aggiornamento di Kaspersky Anti-Virus.

➤ *Per configurare il server proxy:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Fare click sul pulsante **Sorgente degli aggiornamenti** nella parte destra della finestra.
4. Nella finestra visualizzata, nella scheda **Sorgente**, fare click sul pulsante **Server proxy**.
5. Configurare le impostazioni del server proxy nella finestra **Impostazioni del server proxy** visualizzata.

ANTI-VIRUS FILE

Anti-Virus File impedisce l'infezione del file system del computer. Il componente viene avviato all'avvio del sistema operativo, rimane nella RAM del computer ed esamina tutti i file aperti, salvati o eseguiti nel computer e in tutte le unità connesse alla ricerca di virus e altri riskware.

È possibile creare un ambito di protezione e impostare il livello di protezione (un insieme di impostazioni che determinano l'accuratezza della scansione).

Quando l'utente o un programma tenta di accedere a un file protetto, Anti-Virus File controlla se i database di iChecker e iSwift contengono informazioni su tale file e determina se sottoporre o meno a scansione il file.

Per impostazione predefinita, *l'analisi della firma* (una modalità in cui vengono utilizzati i record dei database dell'applicazione per la ricerca delle minacce) è sempre abilitata. È inoltre possibile abilitare l'analisi euristica e varie tecnologie di scansione.

Se vengono rilevate minacce in un file, Kaspersky Anti-Virus assegna al file uno degli stati seguenti:

- Stato che indica il tipo di programma dannoso rilevato (ad esempio, *virus* o *Trojan*).
- *Potenzialmente infetto* (sospetto), se non è possibile stabilire se il file è infetto o meno. Il file può contenere una sequenza di codice tipica dei virus o di altro malware oppure un codice modificato di un virus conosciuto.

L'applicazione visualizza quindi una notifica (vedere pagina [107](#)) della minaccia rilevata ed esegue l'azione specificata nelle impostazioni di Anti-Virus File. È possibile modificare l'azione (vedere pagina [71](#)) che deve essere eseguita dall'applicazione se viene rilevata una minaccia.

Se si utilizza la modalità automatica (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)), quando vengono rilevati oggetti pericolosi, Kaspersky Anti-Virus applica automaticamente l'azione raccomandata dagli specialisti di Kaspersky Lab. Per gli oggetti dannosi, tale azione sarà **Disinfetta. Elimina se la disinfezione fallisce** e **Sposta in Quarantena** per gli oggetti sospetti. Se vengono rilevati oggetti pericolosi durante l'utilizzo della modalità interattiva (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)), l'applicazione visualizza una notifica che è possibile utilizzare per selezionare l'azione desiderata dall'elenco delle azioni disponibili.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento. Gli oggetti sospetti (potenzialmente infetti) sono messi in quarantena. È possibile abilitare la scansione automatica degli oggetti in quarantena dopo ogni aggiornamento.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione di Anti-Virus File	68
Sospensione automatica di Anti-Virus File	69
Creazione dell'ambito di protezione di Anti-Virus File	69
Modifica e ripristino del livello di protezione dei file	70
Selezione della modalità di scansione	70
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus File	71
Selezione di una tecnologia di scansione dei file	71
Modifica dell'azione da eseguire sui file infetti.....	71
Scansione dei file composti tramite Anti-Virus File.....	72
Ottimizzazione della scansione dei file.....	72

ABILITAZIONE E DISABILITAZIONE DI ANTI-VIRUS FILE

Per impostazione predefinita, Anti-Virus File è abilitato ed eseguito nella modalità consigliata dagli specialisti di Kaspersky Lab. Se necessario, è possibile disabilitare Anti-Virus File.

◆ *Per disabilitare Anti-Virus File:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella parte destra della finestra deselezionare la casella **Abilita Anti-Virus File**.

SOSPENSIONE AUTOMATICA DI ANTI-VIRUS FILE

Quando si eseguono attività che richiedono un utilizzo intensivo delle risorse, è possibile sospendere Anti-Virus File. Per ridurre il carico di lavoro e assicurare un accesso rapido agli oggetti, è possibile configurare la sospensione automatica del componente a un orario specificato o durante l'esecuzione di programmi specificati.

La sospensione di Anti-Virus File in caso di conflitti con altre applicazioni rappresenta una misura di emergenza. In caso di conflitti durante l'utilizzo del componente, contattare l'Assistenza tecnica Kaspersky Lab (<http://www.kaspersky.com/it/service>). Gli specialisti dell'Assistenza tecnica aiuteranno a risolvere i problemi di funzionamento di Kaspersky Anti-Virus con le altre applicazioni presenti nel computer.

➤ *Per sospendere il componente a un orario specificato:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Sospendi l'attività** della scheda **Avanzate**, selezionare la casella **In base alla pianificazione** e fare click sul pulsante **Pianifica**.
5. Nella finestra **Sospendi l'attività** specificare la durata (nel formato a 24 ore hh:mm) della sospensione della protezione (campi **Sospendi l'attività alle** e **Riprendi l'attività alle**).

➤ *Per sospendere il componente durante l'esecuzione di applicazioni specificate:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Sospendi l'attività** della scheda **Avanzate**, selezionare la casella **All'avvio dell'applicazione** e fare click sul pulsante **Seleziona**.
5. Nella finestra **Applicazioni** creare un elenco di applicazioni la cui esecuzione comporta la sospensione del componente.

CREAZIONE DELL'AMBITO DI PROTEZIONE DI ANTI-VIRUS FILE

L'ambito di protezione è costituito dal percorso e dai tipi di file di cui eseguire la scansione. Per impostazione predefinita, Kaspersky Anti-Virus esamina solo i file potenzialmente infettabili archiviati in qualsiasi disco rigido, unità di rete o supporto rimovibile.

➤ *Per creare l'ambito di protezione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Tipi di file** della scheda **Generale**, specificare il tipo di file che si desidera esaminare tramite Anti-Virus File:
 - Per esaminare tutti i file, selezionare **Esamina tutti i file**.
 - Per esaminare i file nei formati che presentano la maggiore vulnerabilità alle infezioni, selezionare **Esamina i file per formato**.
 - Per esaminare i file con le estensioni che presentano la maggiore vulnerabilità alle infezioni, selezionare **Esamina i file per estensione**.

Durante la selezione dei tipi di file da esaminare, tenere presente quanto segue:

- La probabilità di penetrazione di codice dannoso in alcuni formati di file (ad esempio TXT) e la successiva attivazione è piuttosto bassa. Altri formati, al contrario, contengono o possono contenere codice eseguibile (EXE, DLL, DOC). Il rischio di penetrazione ed attivazione di codice dannoso in tali file è piuttosto alto.
- Un hacker potrebbe inviare un virus o altro riskware al computer dell'utente in un file eseguibile rinominato con estensione TXT. Se è stata selezionata la scansione dei file in base all'estensione, tale file verrà ignorato dalla scansione. Se è stata selezionata la scansione dei file in base al formato, indipendentemente dall'estensione, Anti-Virus File analizzerà l'intestazione del file e rivelerà che si tratta di un file EXE. Un file di questo tipo viene esaminato in modo approfondito alla ricerca di virus e altro riskware.

5. Nell'elenco **Ambito della protezione** eseguire una delle seguenti operazioni:
 - Per aggiungere un nuovo oggetto all'elenco degli oggetti da esaminare, fare click sul collegamento **Aggiungi**.
 - Per modificare il percorso di un oggetto, selezionare l'oggetto desiderato dall'elenco e fare click sul collegamento **Modifica**.

Verrà aperta la finestra **Scelta degli oggetti da esaminare**.

- Per eliminare un oggetto dall'elenco degli oggetti da esaminare, selezionare l'oggetto desiderato dall'elenco e fare click sul collegamento **Elimina**.
Verrà aperta una finestra di conferma dell'eliminazione.
6. Eseguire una delle seguenti operazioni:
 - Per aggiungere un nuovo oggetto all'elenco degli oggetti da esaminare, selezionare l'oggetto desiderato nella finestra **Scelta degli oggetti da esaminare** e fare click sul pulsante **OK**.
 - Per modificare il percorso di un oggetto, modificare il percorso nel campo **Oggetto** nella finestra **Scelta degli oggetti da esaminare**, quindi fare click sul pulsante **OK**.
 - Per eliminare un oggetto dall'elenco degli oggetti da esaminare, fare click sul pulsante **Sì** nella finestra di conferma dell'eliminazione.
 7. Se necessario, ripetere i passaggi 6 – 7 per aggiungere, spostare o eliminare oggetti dall'elenco degli oggetti da esaminare.
 8. Per escludere un oggetto dall'elenco degli oggetti da esaminare, deselegionare la casella accanto all'oggetto desiderato nell'elenco **Ambito della protezione**. L'oggetto rimane nell'elenco degli oggetti da esaminare, ma viene escluso dalla scansione da parte di Anti-Virus File.

MODIFICA E RIPRISTINO DEL LIVELLO DI PROTEZIONE DEI FILE

A seconda delle specifiche esigenze, è possibile selezionare uno dei livelli di protezione preimpostati per i file e la memoria o configurare Anti-Virus File autonomamente.

Durante la configurazione di Anti-Virus File, è sempre possibile ripristinare i valori consigliati. Tali impostazioni, che consentono di ottenere una configurazione ottimale e sono consigliate da Kaspersky Lab, sono raggruppate nel livello di protezione **Consigliato**.

➤ *Per modificare il livello di protezione dei file:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella parte destra della finestra, nella sezione **Livello di protezione**, impostare il livello di protezione desiderato o fare click sul pulsante **Impostazioni** per modificare manualmente le impostazioni.

Se si modificano manualmente le impostazioni, il nome del livello di protezione diventerà **Personalizzato**.

➤ *Per ripristinare il livello di protezione dei file predefinito:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Fare click sul pulsante **Livello predefinito** nella sezione **Livello di protezione** nella parte destra della finestra.

SELEZIONE DELLA MODALITÀ DI SCANSIONE

Una *modalità di scansione* rappresenta una condizione per cui Anti-Virus File avvia la scansione dei file. Per impostazione predefinita, Kaspersky Anti-Virus viene eseguito in modalità smart. Quando viene eseguito in questa modalità di scansione dei file, Anti-Virus File prende decisioni sulla scansione dei file in base all'analisi delle azioni eseguite dall'utente sui file e in base al tipo di file. Ad esempio, quando si lavora con un documento Microsoft Office, il file viene sottoposto a scansione quando viene aperto per la prima volta e chiuso per l'ultima volta. Le operazioni intermedie di sovrascrittura del file non ne determinano la scansione.

➤ *Per modificare la modalità di scansione dei file:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Modalità di scansione** della scheda **Avanzate**, selezionare la modalità desiderata.

Durante la selezione della modalità di scansione, è necessario tenere conto dei tipi di file con cui si lavora la maggior parte del tempo.

UTILIZZO DELL'ANALISI EURISTICA DURANTE L'UTILIZZO DI ANTI-VIRUS FILE

Durante l'esecuzione di Anti-Virus File viene sempre utilizzata l'*analisi delle firme*; Kaspersky Anti-Virus confronta l'oggetto rilevato con i record nel relativo database.

Per aumentare l'efficienza della protezione, è possibile utilizzare l'*analisi euristica*, ovvero l'analisi delle attività eseguite da un oggetto nel sistema. Questa analisi consente di rilevare nuovi oggetti dannosi non ancora descritti nei database.

➤ *Per abilitare l'analisi euristica:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Metodi di scansione** della scheda **Prestazioni**, selezionare la casella **Analisi euristica** e specificare il livello di dettaglio per la scansione.

SELEZIONE DI UNA TECNOLOGIA DI SCANSIONE DEI FILE

Oltre all'analisi euristica, è possibile utilizzare speciali tecnologie che consentono di ottimizzare le prestazioni di scansione dei file escludendo i file che non sono stati modificati dall'ultima scansione.

➤ *Per specificare le tecnologie di scansione degli oggetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Tecnologie di scansione** della scheda **Avanzate**, selezionare i valori desiderati.

MODIFICA DELL'AZIONE DA ESEGUIRE SUI FILE INFETTI

Se vengono rilevati oggetti infetti, l'applicazione esegue l'azione selezionata.

➤ *Per modificare l'azione da eseguire sugli oggetti infetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella parte destra della finestra selezionare l'opzione desiderata nella sezione **Azione se viene rilevata una minaccia**.

SCANSIONE DEI FILE COMPOSITI TRAMITE ANTI-VIRUS FILE

Un metodo comune per nascondere i virus è incorporarli in file compositi: archivi, pacchetti di installazione, oggetti OLE incorporati e formati di file di posta. Per rilevare i virus nascosti in questo modo, è necessario decomprimere i file compositi, cosa che può ridurre significativamente la velocità di scansione.

Per ogni tipo di file composito, è possibile scegliere di esaminare tutti i file oppure solo quelli nuovi. Per effettuare la selezione, fare click sul collegamento accanto al nome dell'oggetto. Il relativo valore verrà modificato quando si fa click con il pulsante sinistro del mouse su di esso. Se si seleziona la modalità di scansione dei soli file nuovi e modificati, non saranno disponibili i collegamenti che consentono di esaminare tutti i file o solo quelli nuovi.

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

Durante la scansione di file compositi di grandi dimensioni, la decompressione preliminare può richiedere molto tempo. Questo periodo di tempo può essere ridotto abilitando la decompressione dei file compositi in background se superano le dimensioni specificate. Se durante l'utilizzo di questi file è stato rilevato un oggetto dannoso, viene visualizzato un messaggio di notifica.

È possibile limitare la dimensione massima di un file composito da esaminare. I file compositi di dimensioni maggiori di quelle specificate non saranno esaminati.

I file di grandi dimensioni estratti dagli archivi verranno esaminati anche se la casella **Non decomprimere i file compositi molto grandi è selezionata.**

➤ *Per modificare l'elenco dei file compositi da esaminare:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Scansione dei file compositi** della scheda **Prestazioni**, selezionare il tipo di file compositi che si desidera esaminare.

➤ *Per impostare la dimensione massima dei file compositi da esaminare:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Scansione dei file compositi** della scheda **Prestazioni**, fare click sul pulsante **Avanzate**.
5. Nella finestra **File compositi** selezionare la casella **Non decomprimere i file compositi molto grandi** e specificare la dimensione massima del file.

➤ *Per decomprimere i file compositi di grandi dimensioni in background:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Scansione dei file compositi** della scheda **Prestazioni**, fare click sul pulsante **Avanzate**.
5. Nella finestra **File compositi** selezionare la casella **Estrai i file compositi in background** e specificare la dimensione minima dei file.

OTTIMIZZAZIONE DELLA SCANSIONE DEI FILE


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 modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che compositi.

➤ Per eseguire la scansione solo dei file nuovi e modificati:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus File**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Ottimizzazione della scansione** della scheda **Prestazioni**, selezionare la casella **Esamina solo i file nuovi e modificati**.

ANTI-VIRUS POSTA

Anti-Virus Posta esamina i messaggi di posta elettronica in entrata e in uscita per verificare la presenza di oggetti dannosi. Questo componente viene avviato all'avvio del sistema operativo ed è sempre in esecuzione per esaminare tutta la posta elettronica inviata o ricevuta tramite i protocolli POP3, SMTP, IMAP, MAPI e NNTP, nonché le connessioni crittografate (SSL) per POP3 e IMAP (vedere la sezione "Scansione delle connessioni crittografate" a pagina [88](#)).

L'indicatore di funzionamento del componente è l'icona dell'applicazione nell'area di notifica della barra delle applicazioni  che appare ogni volta che viene esaminato un messaggio e-mail.

Anti-Virus Posta intercetta e analizza ogni messaggio e-mail inviato o ricevuto dall'utente. Se non vengono individuate minacce in un messaggio, questo viene reso disponibile per l'utente.

È possibile specificare i tipi di messaggi da esaminare e selezionare il livello di protezione (vedere pagina [75](#)) (impostazioni di configurazione che influenzano il livello di approfondimento della scansione).

Per impostazione predefinita, *l'analisi delle firme* (una modalità in cui vengono utilizzati i record dei database dell'applicazione per la ricerca delle minacce) è sempre abilitata. È possibile abilitare l'analisi euristica. È inoltre possibile abilitare il filtraggio degli allegati (vedere pagina [76](#)), che consente di rinominare o eliminare automaticamente i tipi di file specificati.

Se vengono rilevate minacce in un file, Kaspersky Anti-Virus assegna al file uno degli stati seguenti:

- Stato che indica il tipo di programma dannoso rilevato (ad esempio, *virus* o *Trojan*).
- *Potenzialmente infetto* (sospetto), se non è possibile stabilire se il file è infetto o meno. Il file può contenere una sequenza di codice tipica dei virus o di altro malware oppure un codice modificato di un virus conosciuto.

L'applicazione blocca il messaggio e-mail, visualizza una notifica (vedere pagina [107](#)) della minaccia rilevata ed esegue l'azione specificata nelle impostazioni di Anti-Virus Posta. È possibile modificare le azioni da eseguire quando viene rilevata una minaccia (vedere la sezione "Modifica dell'azione da eseguire sui messaggi e-mail infetti" a pagina [75](#)).

Se si utilizza la modalità automatica (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)), quando vengono rilevati oggetti pericolosi, Kaspersky Anti-Virus applica automaticamente l'azione raccomandata dagli specialisti di Kaspersky Lab. Per gli oggetti dannosi, tale azione sarà **Disinfezza. Elimina se la disinfezione fallisce** e **Sposta in Quarantena** per gli oggetti sospetti. Se vengono rilevati oggetti pericolosi durante l'utilizzo della modalità interattiva (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)), l'applicazione visualizza una notifica che è possibile utilizzare per selezionare l'azione desiderata dall'elenco delle azioni disponibili.

Prima di provare a disinfectare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup per consentirne il ripristino o la disinfezione in un secondo momento. Gli oggetti sospetti (potenzialmente infetti) sono messi in quarantena. È possibile abilitare la scansione automatica degli oggetti in quarantena dopo ogni aggiornamento.

Se la disinfezione viene eseguita correttamente, il messaggio e-mail diventa disponibile. Se la disinfezione ha esito negativo, l'oggetto infetto viene eliminato dal messaggio. Anti-Virus Posta modifica l'oggetto del messaggio e-mail aggiungendo del testo che indica all'utente che il messaggio è stato elaborato da Kaspersky Anti-Virus.

È disponibile un plug-in integrato per Microsoft Office Outlook che consente di ottimizzare la configurazione del client di posta elettronica.

Se si utilizza il client di posta The Bat!, Kaspersky Anti-Virus può essere utilizzato unitamente ad altre applicazioni anti-virus. A tale scopo, le regole di elaborazione del traffico e-mail vengono configurate direttamente in The Bat! e hanno una priorità superiore rispetto alle impostazioni di protezione della posta di Kaspersky Anti-Virus.

Se si utilizzano altri client di posta molto diffusi (inclusi Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora e Incredimail), Anti-Virus Posta esamina i messaggi trasmessi tramite i protocolli SMTP, POP3, IMAP, e NNTP.

Si noti che quando si utilizza il client di posta Thunderbird, i messaggi di posta elettronica trasmessi tramite IMAP non vengono sottoposti a scansione virus se si utilizzano filtri per lo spostamento dei messaggi dalla cartella **Posta in arrivo.**

IN QUESTA SEZIONE:

Abilitazione e disabilitazione di Anti-Virus Posta	74
Creazione dell'ambito di protezione di Anti-Virus Posta	74
Modifica e ripristino del livello di protezione dei messaggi e-mail	75
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus Posta	75
Modifica dell'azione da eseguire sui messaggi e-mail infetti	75
Filtro degli allegati nei messaggi e-mail.....	76
Scansione dei file composti tramite Anti-Virus Posta	76
Scansione della posta elettronica in Microsoft Office Outlook.....	76
Scansione della posta elettronica in The Bat!	77

ABILITAZIONE E DISABILITAZIONE DI ANTI-VIRUS POSTA

Per impostazione predefinita, Anti-Virus Posta è abilitato ed eseguito nella modalità consigliata dagli specialisti di Kaspersky Lab. Se necessario, è possibile disabilitare Anti-Virus Posta.

➤ *Per disabilitare Anti-Virus Posta:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Nella parte destra della finestra deselezionare la casella **Abilita Anti-Virus Posta**.

CREAZIONE DELL'AMBITO DI PROTEZIONE DI ANTI-VIRUS POSTA

L'ambito di protezione comprende il tipo di messaggi e-mail di cui eseguire la scansione, i protocolli con il traffico esaminato da Kaspersky Anti-Virus e le impostazioni per l'integrazione di Anti-Virus Posta nel sistema.

Per impostazione predefinita, Kaspersky Anti-Virus è integrato in Microsoft Office Outlook e The Bat!, esegue la scansione sia dei messaggi e-mail in entrata anche di quelli in uscita ed esamina il traffico dei protocolli POP3, SMTP, NNTP e IMAP.

➤ *Per disabilitare la scansione dei messaggi in uscita:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Nella sezione **Ambito della protezione** della scheda **Generale** della finestra visualizzata selezionare l'opzione **Solo messaggi in entrata**.

Se è stata selezionata solo la scansione dei messaggi in entrata, è consigliabile eseguire la scansione dei messaggi in uscita quando si esegue per la prima volta Kaspersky Anti-Virus, dal momento che il computer potrebbe essere infetto da worm che utilizzano la posta elettronica per diffondersi. La scansione dei messaggi in uscita consente di evitare i problemi associati all'invio incontrollato di messaggi e-mail dal proprio computer.

➤ *Per selezionare i protocolli da esaminare e le impostazioni per l'integrazione di Anti-Virus Posta nel sistema:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Nella finestra visualizzata, nella sezione **Connettività** della scheda **Avanzate**, selezionare le impostazioni desiderate.

MODIFICA E RIPRISTINO DEL LIVELLO DI PROTEZIONE DEI MESSAGGI E-MAIL

A seconda delle specifiche esigenze, è possibile selezionare uno dei livelli di protezione preimpostati per i file e la memoria o configurare Anti-Virus Posta autonomamente.

Kaspersky Lab consiglia di non configurare manualmente le impostazioni di Anti-Virus Posta. Nella maggior parte dei casi è sufficiente selezionare un diverso livello di protezione.

Durante la configurazione di Anti-Virus Posta, è sempre possibile ripristinare i valori consigliati. Tali impostazioni, che consentono di ottenere una configurazione ottimale e sono consigliate da Kaspersky Lab, sono raggruppate nel livello di protezione **Consigliato**.

➔ *Per modificare il livello corrente di protezione della posta elettronica:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Nella parte destra della finestra, nella sezione **Livello di protezione**, impostare il livello di protezione desiderato o fare click sul pulsante **Impostazioni** per modificare manualmente le impostazioni.

Se si modificano manualmente le impostazioni, il nome del livello di protezione diventerà **Personalizzato**.

➔ *Per ripristinare le impostazioni predefinite di protezione della posta:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Fare click sul pulsante **Livello predefinito** nella sezione **Livello di protezione** nella parte destra della finestra.

UTILIZZO DELL'ANALISI EURISTICA DURANTE L'UTILIZZO DI ANTI-VIRUS POSTA

Durante l'esecuzione di Anti-Virus Posta viene sempre utilizzata l'*analisi delle firme*; Kaspersky Anti-Virus confronta l'oggetto rilevato con i record nel relativo database.

Per aumentare l'efficienza della protezione, è possibile utilizzare l'*analisi euristica*, ovvero l'analisi delle attività eseguite da un oggetto nel sistema. Questa analisi consente di rilevare nuovi oggetti dannosi non ancora descritti nei database.

➔ *Per abilitare l'analisi euristica:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Nella sezione **Livello di protezione** nella parte destra della finestra fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella sezione **Metodi di scansione** della scheda **Generale**, selezionare la casella **Analisi euristica** e specificare il livello di dettaglio per la scansione.

MODIFICA DELL'AZIONE DA ESEGUIRE SUI MESSAGGI E-MAIL INFETTI

Se vengono rilevati oggetti infetti, l'applicazione esegue l'azione selezionata.

➔ *Per modificare l'azione da eseguire sui messaggi e-mail infetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Nella parte destra della finestra selezionare l'opzione desiderata nella sezione **Azione se viene rilevata una minaccia**.

FILTRO DEGLI ALLEGATI NEI MESSAGGI E-MAIL

I programmi dannosi possono diffondersi tramite gli allegati dei messaggi e-mail. È possibile configurare il filtro in base ai tipi di allegati dei messaggi e-mail, in modo da rinominare o eliminare automaticamente i file dei tipi specificati.

➤ *Per configurare il filtro degli allegati:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Utilizzare la scheda **Filtro allegati** della finestra visualizzata per selezionare la modalità di filtraggio degli allegati. Quando si seleziona una delle ultime due modalità, l'elenco dei tipi di file (estensioni) verrà abilitato. In tale elenco è possibile selezionare i tipi desiderati o aggiungere una nuova maschera per i tipi di file.

Per aggiungere all'elenco una maschera di tipi di file, fare click sul collegamento **Aggiungi** per aprire la finestra **Maschera per il nome del file** e immettere le informazioni desiderate.

SCANSIONE DEI FILE COMPOSITI TRAMITE ANTI-VIRUS POSTA

Un metodo comune per nascondere i virus è incorporarli in file compositi: archivi, pacchetti di installazione, oggetti OLE incorporati e formati di file di posta. Per rilevare i virus nascosti in questo modo, è necessario decomprimere i file compositi, cosa che può ridurre significativamente la velocità di scansione.

È possibile abilitare o disabilitare la scansione dei file compositi e limitare le dimensioni massime dei file compositi da esaminare.

Se il computer non è protetto da alcun software di rete locale (ovvero se si accede a Internet direttamente senza un server proxy o un firewall), è consigliabile non disabilitare la scansione dei file compositi.

➤ *Per configurare la scansione dei file compositi:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Posta**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Utilizzare la scheda **Generale** della finestra visualizzata per definire le impostazioni desiderate.

SCANSIONE DELLA POSTA ELETTRONICA IN MICROSOFT OFFICE OUTLOOK

Durante l'installazione di Kaspersky Anti-Virus, in Microsoft Office Outlook viene integrato uno speciale plug-in. Questo plug-in consente di passare rapidamente alla configurazione di Anti-Virus Posta da Microsoft Office Outlook e di determinare quando esaminare i messaggi e-mail alla ricerca di virus e altro riskware (al momento della ricezione, dell'apertura o dell'invio di un messaggio).

La configurazione di Anti-Virus Posta da Microsoft Office Outlook è disponibile se questa opzione è selezionata nelle impostazioni dell'ambito di protezione di Anti-Virus Posta.

➤ *Per passare alle impostazioni di scansione dei messaggi e-mail in Microsoft Office Outlook:*

1. Aprire la finestra principale di Microsoft Office Outlook.
2. Selezionare **Strumenti** → **Opzioni** dal menu dell'applicazione.
3. Nella finestra **Impostazioni** visualizzata selezionare la scheda **Anti-Virus Posta**.

SCANSIONE DELLA POSTA ELETTRONICA IN THE BAT!

Le azioni da intraprendere sugli oggetti di posta infetti nel client The Bat! vengono definite mediante gli strumenti del programma stesso.

Le impostazioni di Anti-Virus Posta che determinano se è necessario eseguire la scansione dei messaggi in entrata e in uscita, le azioni da eseguire sugli oggetti pericolosi nella posta elettronica e le esclusioni da applicare vengono ignorate. L'unica azione presa in considerazione da The Bat! è la scansione degli archivi allegati.

Le impostazioni di protezione della posta elettronica si estendono a tutti i componenti anti-virus installati nel computer che supportano The Bat!.

I messaggi e-mail in entrata vengono esaminati prima da Anti-Virus Posta e quindi dal plug-in per The Bat!. Se viene rilevato un oggetto dannoso, Kaspersky Anti-Virus segnala immediatamente l'evento all'utente. Se si seleziona l'azione **Disinfetta (Elimina)** nella finestra di notifica di Anti-Virus Posta, le azioni mirate all'eliminazione della minaccia verranno eseguite da questo componente. Se si seleziona l'opzione **Ignora** nella finestra di notifica, l'oggetto verrà disinfettato dal plug-in per The Bat!. I messaggi e-mail in uscita vengono esaminati prima dal plug-in e quindi da Anti-Virus Posta.

Le impostazioni di Anti-Virus Posta sono disponibili da The Bat! se questa opzione è selezionata nelle impostazioni dell'ambito di protezione di Anti-Virus Posta.

Per configurare la scansione dei messaggi e-mail in The Bat!, è necessario definire i seguenti criteri:

- il flusso di posta (in entrata o in uscita) da esaminare;
- il momento in cui esaminare gli oggetti di posta (all'apertura di un messaggio o prima del salvataggio su disco);
- le azioni che verranno eseguite dal client di posta in caso di identificazione di oggetti pericolosi nei messaggi di posta elettronica. È ad esempio possibile selezionare:
 - **Tenta di disinfettare le parti infette**: se questa opzione è selezionata, viene tentata la disinfezione dell'oggetto infetto. Se non è possibile disinfettarlo, l'oggetto è mantenuto nel messaggio.
 - **Elimina parti infette**: se questa opzione è selezionata, l'oggetto pericoloso presente nel messaggio viene eliminato indipendentemente dal fatto che sia infetto o sospetto.

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

I messaggi e-mail che contengono oggetti pericolosi non vengono contrassegnati nel campo dell'oggetto quando sono esaminati dal plug-in per The Bat!.

► Per passare alle impostazioni di scansione dei messaggi e-mail in The Bat!:

1. Aprire la finestra principale di The Bat!.
2. Dal menu **Properties (Proprietà)** selezionare **Settings (Impostazioni)**.
3. Selezionare **Virus protection (Protezione anti-virus)** nella struttura ad albero delle impostazioni.

ANTI-VIRUS WEB

Ogni volta che ci si connette a Internet, si espongono le informazioni memorizzate nel proprio computer al rischio di infezioni da parte di virus e altro malware. Questi elementi possono penetrare nel computer quando si scaricano applicazioni gratuite o si visualizzano informazioni su siti Web che hanno subito un attacco da parte di hacker. Inoltre, i worm di rete possono penetrare nel computer ancora prima di aprire una pagina Web o di scaricare un file, non appena il computer stabilisce una connessione a Internet.

Anti-Virus Web protegge le informazioni ricevute dal computer e inviate tramite i protocolli HTTP, HTTPS e FTP, oltre a impedire l'esecuzione nel computer di script pericolosi.

Anti-Virus Web monitora solo il traffico Web trasferito tramite le porte specificate nell'elenco delle porte monitorate. Il pacchetto di Kaspersky Anti-Virus comprende un elenco di porte monitorate comunemente utilizzate per il trasferimento di dati. Se si utilizzano porte non incluse nell'elenco delle porte monitorate, è necessario aggiungerle all'elenco delle porte monitorate (vedere la sezione "Creazione di un elenco di porte monitorate" a pagina [90](#)) per assicurare la protezione del traffico Web trasferito tramite tali porte.

Anti-Virus Web esamina il traffico Web in base a uno specifico insieme di impostazioni denominato livello di protezione. Se Anti-Virus Web rileva una minaccia, esegue l'azione impostata. Gli oggetti dannosi vengono rilevati utilizzando i database e l'algoritmo euristico di Kaspersky Anti-Virus.

Kaspersky Lab consiglia di non configurare manualmente le impostazioni di Anti-Virus Web. Nella maggior parte dei casi è sufficiente selezionare un livello di protezione appropriato.

Algoritmo di scansione del traffico Web

Ogni pagina Web o file a cui accede l'utente o un programma attraverso i protocolli HTTP, HTTPS o FTP viene intercettato e analizzato da Anti-Virus Web per escludere la presenza di codice dannoso:

- Se una pagina Web o un file al quale l'utente cerca di accedere contiene codice dannoso, l'accesso a tale file o pagina Web viene bloccato. Viene visualizzata una notifica che segnala che il file o la pagina Web richiesta è infetta.
- Se il file o la pagina Web non contiene codice dannoso, il programma concede immediatamente l'accesso all'utente.

Algoritmo di scansione degli script

Ogni esecuzione di uno script viene intercettata da Anti-Virus Web e analizzata per individuare eventuale codice dannoso:

- Se uno script contiene codice dannoso, Anti-Virus Web lo blocca e visualizza una notifica.
- Se nello script non viene rilevato alcun codice dannoso, lo script viene eseguito.

Anti-Virus Web intercetta solo gli script basati sulla funzionalità Microsoft Windows Script Host.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione di Anti-Virus Web.....	78
Modifica e ripristino del livello di protezione del traffico Web	78
Modifica dell'azione da eseguire sugli oggetti pericolosi dal traffico Web	79
Controllo delle URL nelle pagine Web.....	79
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus Web.....	81
Blocco degli script pericolosi	81
Ottimizzazione della scansione	82
Creazione di un elenco di indirizzi attendibili.....	82

ABILITAZIONE E DISABILITAZIONE DI ANTI-VIRUS WEB

Per impostazione predefinita, Anti-Virus Web è abilitato ed eseguito nella modalità consigliata dagli specialisti di Kaspersky Lab. Se necessario, è possibile disabilitare Anti-Virus Web.

➤ *Per disabilitare Anti-Virus Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella parte destra della finestra deselezionare la casella **Abilita Anti-Virus Web**.

MODIFICA E RIPRISTINO DEL LIVELLO DI PROTEZIONE DEL TRAFFICO WEB

A seconda delle specifiche esigenze, è possibile selezionare uno dei livelli di protezione preimpostati per il traffico Web o configurare Anti-Virus Web autonomamente.

Durante la configurazione di Anti-Virus Web, è sempre possibile ripristinare i valori consigliati. Tali impostazioni, che consentono di ottenere una configurazione ottimale e sono consigliate da Kaspersky Lab, sono raggruppate nel livello di protezione **Consigliato**.

➔ *Per modificare il livello di protezione del traffico Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella parte destra della finestra, nella sezione **Livello di protezione**, impostare il livello di protezione desiderato o fare click sul pulsante **Impostazioni** per modificare manualmente le impostazioni.

Se si modificano manualmente le impostazioni, il nome del livello di protezione diventerà **Personalizzato**.

➔ *Per ripristinare il livello predefinito di protezione del traffico Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Livello predefinito** nella sezione **Livello di protezione** nella parte destra della finestra.

MODIFICA DELL'AZIONE DA ESEGUIRE SUGLI OGGETTI PERICOLOSI DAL TRAFFICO WEB

Se vengono rilevati oggetti infetti, l'applicazione esegue l'azione selezionata.

Anti-Virus Web blocca sempre le azioni eseguite da script pericolosi e visualizza messaggi che comunicano all'utente l'azione intrapresa. Non è possibile modificare l'azione da eseguire su uno script pericoloso. L'unica operazione consentita è la disabilitazione della scansione degli script (vedere la sezione "Blocco degli script pericolosi" a pagina [81](#)).

➔ *Per modificare l'azione da eseguire sugli oggetti rilevati:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Nella parte destra della finestra selezionare l'opzione desiderata nella sezione **Azione se viene rilevata una minaccia**.

CONTROLLO DELLE URL NELLE PAGINE WEB

La scansione delle pagine Web alla ricerca di elementi di phishing consente di impedire gli *attacchi di phishing*. Gli attacchi di phishing generalmente vengono eseguiti tramite messaggi e-mail da presunte organizzazioni finanziarie che contengono URL per l'accesso ai siti Web di tali organizzazioni. Il testo del messaggio e-mail induce il lettore a fare click sulla URL e a immettere informazioni riservate nella finestra visualizzata, ad esempio, un numero di carta di credito o il nome utente e la password usati per collegarsi a un servizio di online banking. Un attacco di phishing può ad esempio presentarsi sotto forma di una comunicazione proveniente dalla propria banca con un collegamento al relativo sito Web ufficiale. Facendo click sul collegamento, si viene indirizzati a una copia identica del sito della banca (che visualizza addirittura l'indirizzo effettivo nel browser), anche se in realtà di tratta di un sito falso. Da questo momento, tutte le operazioni eseguite nel sito vengono registrate e possono essere utilizzate per prelevare denaro dal conto dell'utente.

Poiché i collegamenti ai siti Web di phishing possono essere ricevuti non solo tramite posta elettronica ma anche da altre origini, come ad esempio i messaggi di ICQ, Anti-Virus Web monitora i tentativi di accedere a un sito Web di phishing a livello di traffico Web e blocca l'accesso a tali posizioni.

Oltre ai database di Kaspersky Anti-Virus, è possibile utilizzare l'analisi euristica (vedere pagina [81](#)) per la scansione delle pagine Web alla ricerca di elementi di phishing.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione del controllo delle URL	80
Utilizzo di Controllo URL Kaspersky	80

ABILITAZIONE E DISABILITAZIONE DEL CONTROLLO DELLE URL

► *Per abilitare i controlli delle URL in base ai database di indirizzi Web sospetti e di phishing:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
Viene visualizzata la finestra **Anti-Virus Web**.
4. Nella sezione **Controllo URL Kaspersky** della scheda **Generale** selezionare le caselle **Controllare se le URL sono elencate nel database delle URL sospette** e **Controllare le pagine Web di phishing**.

UTILIZZO DI CONTROLLO URL KASPERSKY

Controllo URL Kaspersky è integrato in Microsoft Internet Explorer, Mozilla Firefox e Google Chrome come plug-in.

Controllo URL Kaspersky verifica tutte le URL in una pagina Web per stabilire se sono incluse nell'elenco delle URL sospette. Viene inoltre verificato se si tratta di URL di phishing, evidenziandole nella finestra del browser.

È possibile creare un elenco di siti Web per cui controllare tutte le URL, controllare le URL in tutti i siti Web tranne quelli inclusi nell'elenco delle esclusioni, controllare solo le URL nei risultati di ricerca o specificare categorie di siti Web di cui controllare le URL.

Controllo URL Kaspersky può essere configurato non solo nella finestra delle impostazioni dell'applicazione, ma anche nella finestra delle impostazioni di Controllo URL Kaspersky, accessibile dal browser Web.

► *Per specificare i siti Web per cui controllare tutte le URL:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Viene visualizzata la finestra **Anti-Virus Web**.
5. Nella sezione **Controllo URL Kaspersky** della scheda **Navigazione sicura** selezionare **Verifica URL**.
6. Selezionare i siti Web in cui è necessario esaminare i collegamenti:
 - a. Se si desidera creare un elenco di siti Web per cui controllare tutte le URL, selezionare **Solo i siti Web nell'elenco** e fare click sul pulsante **Specifica**. Nella finestra **URL controllate** visualizzata creare un elenco di siti Web da controllare.
 - b. Se si desidera controllare le URL in tutti i siti Web tranne quelli specificati, selezionare **Tutti tranne le esclusioni** e fare click sul pulsante **Esclusioni**. Nella finestra **Esclusioni** visualizzata creare un elenco di siti Web di cui non si desidera controllare le URL.

► *Per controllare solo le URL nei risultati di ricerca:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Viene visualizzata la finestra **Anti-Virus Web**.
5. Nella sezione **Controllo URL Kaspersky** della scheda **Navigazione sicura** selezionare **Verifica URL** e fare click sul pulsante **Impostazioni**.
6. Nella finestra **Impostazioni di Controllo URL Kaspersky** visualizzata, nella sezione **Modalità controllo**, selezionare **Solo le URL nei risultati di ricerca**.

► *Per selezionare le categorie di siti Web per cui controllare le URL:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Viene visualizzata la finestra **Anti-Virus Web**.

5. Nella sezione **Controllo URL Kaspersky** della scheda **Navigazione sicura** selezionare **Verifica URL** e fare click sul pulsante **Impostazioni**.
6. Nella finestra **Impostazioni di Controllo URL Kaspersky** visualizzata, nella sezione **Categorie di siti Web**, selezionare la casella **Mostra informazioni sulle categorie di contenuti dei siti Web**.
7. Nell'elenco delle categorie selezionare le caselle accanto alle categorie di siti Web di cui si desidera controllare le URL.

➤ *Per aprire la finestra delle impostazioni di Controllo URL Kaspersky dal browser Web:*

Fare click sul pulsante con l'icona di Kaspersky Anti-Virus sulla barra degli strumenti del browser.

UTILIZZO DELL'ANALISI EURISTICA DURANTE L'UTILIZZO DI ANTI-VIRUS WEB

Per aumentare l'efficienza della protezione, è possibile utilizzare l'*analisi euristica*, ovvero l'analisi delle attività eseguite da un oggetto nel sistema. Questa analisi consente di rilevare nuovi oggetti dannosi non ancora descritti nei database.

Quando Anti-Virus Web è in esecuzione, è possibile abilitare separatamente l'analisi euristica per la scansione del traffico Web e per il controllo delle pagine Web alla ricerca di URL di phishing.

➤ *Per abilitare l'analisi euristica per la scansione del traffico Web:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
Viene visualizzata la finestra **Anti-Virus Web**.
4. Nella sezione **Analisi euristica** della scheda **Generale**, selezionare la casella **Usa l'analisi euristica e impostare il livello di dettaglio per la scansione**.

➤ *Per abilitare l'analisi euristica per il controllo delle pagine Web alla ricerca di URL di phishing:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
Viene visualizzata la finestra **Anti-Virus Web**.
4. Nella sezione **Controllo URL Kaspersky** della scheda **Generale** fare click sul pulsante **Avanzate**.
5. Nella finestra **Impostazioni dell'Anti-Phishing** visualizzata selezionare la casella **Usa l'analisi euristica per controllare le URL di phishing** nelle pagine Web e impostare il livello di dettaglio per la scansione.

BLOCCO DEGLI SCRIPT PERICOLOSI

Anti-Virus Web esamina tutti gli script elaborati in Microsoft Internet Explorer, nonché qualsiasi altro script WSH (ad esempio, JavaScript, Visual Basic Script e così via) avviato durante l'utilizzo del computer da parte dell'utente. Se uno script costituisce una minaccia per il computer, verrà bloccato.

➤ *Per disabilitare il blocco degli script pericolosi:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
Viene visualizzata la finestra **Anti-Virus Web**.
4. Nella sezione **Avanzate** della scheda **Generale** deselezionare la casella **Blocca gli script pericolosi in Microsoft Internet Explorer**.

OTTIMIZZAZIONE DELLA SCANSIONE

Per migliorare l'efficienza di rilevamento del codice dannoso, Anti-Virus Web utilizza la memorizzazione nella cache di frammenti degli oggetti ricevuti da Internet. Utilizzando la memorizzazione nella cache, Anti-Virus Web esamina gli oggetti solo una volta che sono stati interamente ricevuti nel computer.

La memorizzazione nella cache aumenta la quantità di tempo necessario per elaborare gli oggetti e renderli disponibili all'utente per ulteriori operazioni. Questo può causare problemi durante il download e l'elaborazione di oggetti di grandi dimensioni, in quanto è possibile che la connessione al client HTTP raggiunga il timeout.

È possibile risolvere il problema utilizzando l'opzione per limitare la memorizzazione nella cache dei frammenti di oggetti ricevuti da Internet. Alla scadenza di un determinato intervallo di tempo, ogni frammento di un oggetto viene passato all'utente senza essere esaminato. Quando la copia viene completata, l'oggetto viene sottoposto a scansione interamente. Questo consente di ridurre la quantità di tempo necessario per rendere disponibili gli oggetti all'utente e risolvere i problemi relativi all'interruzione della connessione. Il livello di protezione Internet non viene ridotto.

L'aumento delle restrizioni per la durata della memorizzazione nella cache del traffico Web aumenta l'efficienza della scansione virus, ma può rallentare l'accesso agli oggetti.

► *Per impostare o rimuovere un limite di tempo per il buffering dei frammenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
Viene visualizzata la finestra **Anti-Virus Web**.
4. Nella sezione **Avanzate** della scheda **Generale** selezionare la casella **Limita a 1 secondo la memorizzazione nella cache del traffico per ottimizzare la scansione**.

CREAZIONE DI UN ELENCO DI INDIRIZZI ATTENDIBILI

Anti-Virus Web non esegue la scansione del traffico Web alla ricerca di oggetti pericolosi se il traffico è originato da URL attendibili.

► *Per creare un elenco di indirizzi Web attendibili:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus Web**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
Viene visualizzata la finestra **Anti-Virus Web**.
4. Nella scheda **URL attendibili** selezionare la casella **Non esaminare il traffico Web per le URL attendibili**.
5. Creare un elenco di siti Web o di pagine Web di cui si ritengono attendibili i contenuti. A tal fine, procedere nel seguente modo:
 - a. Fare click sul pulsante **Aggiungi**.
Verrà visualizzata la finestra **Maschera per l'indirizzo (URL)**.
 - b. Immettere l'indirizzo di un sito o di una pagina Web o una maschera per l'indirizzo di un sito o di una pagina Web.
 - c. Fare click sul pulsante **OK**.
Verrà visualizzato nuovo record nell'elenco delle URL attendibili.
6. Se necessario, ripetere i passaggi da a a c.

ANTI-VIRUS IM

Anti-Virus IM analizza il traffico dei client IM (*sistemi di messaggistica istantanea*).

I messaggi dei client IM possono contenere collegamenti a siti Web sospetti e a siti utilizzati dagli hacker per organizzare attacchi di phishing. I programmi dannosi utilizzano infatti questo tipo di client per inviare messaggi di spam e collegamenti a programmi (o i programmi stessi) creati per rubare gli ID e le password degli utenti.

Kaspersky Anti-Virus garantisce il funzionamento sicuro di varie applicazioni di messaggistica istantanea, tra cui ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent e IRC.

Alcuni client IM, come Yahoo! Messenger e Google Talk, utilizzano connessioni crittografate. Per esaminare il traffico generato da tali programmi, è necessario abilitare la scansione delle connessioni protette (vedere pagina [88](#)).

Anti-Virus IM intercetta i messaggi e li analizza alla ricerca di oggetti o di URL pericolosi. È possibile selezionare i tipi di messaggi da esaminare e vari metodi di scansione.

Se in un messaggio vengono rilevate minacce, Anti-Virus IM sostituisce il messaggio con un messaggio di avviso per l'utente.

La scansione dei file trasferiti tramite client di messaggistica immediata viene eseguita dal componente Anti-Virus File (a pagina [68](#)) quando si tenta di salvarli.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione di Anti-Virus IM	83
Creazione dell'ambito di protezione di Anti-Virus IM	83
Controllo delle URL nei messaggi dai client IM	83
Utilizzo dell'analisi euristica durante l'utilizzo di Anti-Virus IM	84

ABILITAZIONE E DISABILITAZIONE DI ANTI-VIRUS IM

Per impostazione predefinita, Anti-Virus IM è abilitato e funziona in modalità normale. Se necessario, è possibile disabilitare Anti-Virus IM.

► *Per disabilitare Anti-Virus IM:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella parte destra della finestra deselezionare la casella **Abilita Anti-Virus IM**.

CREAZIONE DELL'AMBITO DI PROTEZIONE DI ANTI-VIRUS IM

Per ambito di protezione si intende il tipo di messaggi da esaminare. Per impostazione predefinita, Kaspersky Anti-Virus esamina sia i messaggi in entrata che quelli in uscita. Se si è certi che i messaggi inviati non contengano oggetti pericolosi, è possibile disabilitare la scansione del traffico in uscita.

► *Per disabilitare la scansione dei messaggi in uscita:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella parte destra della finestra, nella sezione **Ambito della protezione**, selezionare l'opzione **Solo messaggi in entrata**.

CONTROLLO DELLE URL NEI MESSAGGI DAI CLIENT IM

► *Per esaminare i messaggi alla ricerca di URL sospette e di phishing:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella parte destra della finestra, nella sezione **Metodi di scansione**, selezionare le caselle **Controllare se le URL sono elencate nel database delle URL sospette** e **Controllare se le URL sono elencate nel database delle URL di phishing**.

UTILIZZO DELL'ANALISI EURISTICA DURANTE L'UTILIZZO DI ANTI-VIRUS IM

Per aumentare l'efficienza della protezione, è possibile utilizzare l'*analisi euristica*, ovvero l'analisi delle attività eseguite da un oggetto nel sistema. Questa analisi consente di rilevare nuovi oggetti dannosi non ancora descritti nei database.

Quando si utilizza l'analisi euristica, qualsiasi script incluso nei messaggi di un client IM viene eseguito in un ambiente protetto. Se l'attività dello script è tipica di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. L'analisi euristica è abilitata per impostazione predefinita.

► *Per abilitare l'analisi euristica:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Anti-Virus IM**.
3. Nella parte destra della finestra, nella sezione **Metodi di scansione**, selezionare la casella **Analisi euristica**, quindi impostare il livello di approfondimento desiderato per la scansione.

DIFESA PROATTIVA

Difesa Proattiva assicura la protezione dalle minacce che non sono ancora incluse nei database di Kaspersky Anti-Virus.

Il funzionamento di Difesa Proattiva è basato su tecnologie preventive. Le tecnologie di questo tipo consentono di neutralizzare una nuova minaccia prima che possa danneggiare in qualche modo il computer. A differenza delle tecnologie reattive, che analizzano il codice in base ai record contenuti nei database di Kaspersky Anti-Virus, le tecnologie preventive riconoscono una nuova minaccia nel computer tramite una sequenza di azioni eseguite da un programma. Se, come risultato dell'analisi delle attività, la sequenza di azioni dell'applicazione desta sospetti, Kaspersky Anti-Virus blocca l'attività dell'applicazione.

Quando ad esempio vengono rilevate azioni come quelle di un programma che duplica se stesso in risorse di rete, nella cartella di avvio e nel registro di sistema, è molto probabile che tale programma sia un worm.

Le sequenze di azioni pericolose includono i tentativi di modificare il file HOSTS, l'installazione nascosta di driver ed altro ancora. È possibile disattivare il monitoraggio (vedere pagina [85](#)) di qualsiasi attività pericolosa o modificare le regole di monitoraggio (vedere pagina [85](#)).

È possibile creare un gruppo di applicazioni attendibili (vedere pagina [85](#)) per Difesa Proattiva. Non si riceveranno notifiche delle attività di queste applicazioni.

Se il computer in uso dispone del sistema operativo Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 o Microsoft Windows 7 x64, il controllo non verrà applicato a tutti gli eventi. Ciò è dovuto alle specifiche caratteristiche di questi sistemi operativi. Ad esempio, il controllo non verrà applicato in modo completo all'invio di dati tramite le applicazioni attendibili e alle attività di sistema sospette.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione di Difesa Proattiva	84
Creazione di un gruppo di applicazioni attendibili	85
Utilizzo dell'elenco di attività pericolose	85
Modifica dell'azione da eseguire sulle attività pericolose delle applicazioni	85

ABILITAZIONE E DISABILITAZIONE DI DIFESA PROATTIVA

Per impostazione predefinita, Difesa Proattiva è abilitato ed eseguito nella modalità consigliata dagli specialisti di Kaspersky Lab. Se necessario, è possibile disabilitare Difesa Proattiva.

➤ *Per disabilitare Difesa Proattiva:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Difesa Proattiva**.
3. Nella parte destra della finestra deselegionare la casella **Abilita Difesa Proattiva**.

CREAZIONE DI UN GRUPPO DI APPLICAZIONI ATTENDIBILI

È possibile creare un gruppo di applicazioni attendibili, le cui attività non devono essere controllate da Difesa Proattiva. Per impostazione predefinita, l'elenco delle applicazioni attendibili include le applicazioni con firme digitali verificate e le applicazioni classificate come attendibili nel database di Kaspersky Security Network.

➤ *Per modificare le impostazioni delle applicazioni del gruppo Attendibili:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Difesa Proattiva**.
3. Nella parte destra della finestra, nella sezione **Applicazioni attendibili**, eseguire le seguenti operazioni:
 - Se si desidera che le applicazioni dotate di firme digitali verificate vengano incluse nel gruppo delle applicazioni attendibili, selezionare la casella **Applicazioni con firma digitale**.
 - Se si desidera che le applicazioni classificate come attendibili nel database di Kaspersky Security Network vengano incluse nel gruppo delle applicazioni attendibili, selezionare la casella **Attendibile nel database di Kaspersky Security Network**.

UTILIZZO DELL'ELENCO DI ATTIVITÀ PERICOLOSE

L'elenco delle azioni tipiche delle attività pericolose non può essere modificato. È tuttavia possibile evitare il monitoraggio di una specifica attività pericolosa.

➤ *Per disattivare il monitoraggio di un'attività pericolosa:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Difesa Proattiva**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Nella finestra **Difesa Proattiva** visualizzata deselegionare la casella accanto al tipo di attività che non si desidera monitorare.

MODIFICA DELL'AZIONE DA ESEGUIRE SULLE ATTIVITÀ PERICOLOSE DELLE APPLICAZIONI

L'elenco delle azioni tipiche delle attività pericolose non può essere modificato. È tuttavia possibile modificare l'azione eseguita da Kaspersky Anti-Virus quando vengono rilevate attività pericolose delle applicazioni.

➤ *Per modificare l'azione eseguita dall'applicazione Kaspersky Lab sulle attività pericolose delle applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Difesa Proattiva**.
3. Fare click sul pulsante **Impostazioni** nella parte destra della finestra.
4. Nella finestra **Difesa Proattiva** visualizzata, nella colonna **Evento**, selezionare l'evento per cui si desidera modificare la regola.
5. Configurare le impostazioni per l'evento selezionato utilizzando i collegamenti nella sezione **Descrizione della regola**: Ad esempio:
 - a. Fare click sul collegamento con l'azione preimpostata e selezionare l'azione desiderata nella finestra **Seleziona azione** visualizzata.
 - b. Fare click sul collegamento **Attivato / Disattivato** per indicare se creare o meno un rapporto sull'esecuzione dell'operazione.

CONTROLLO SISTEMA

Controllo sistema raccoglie dati sulle azioni delle applicazioni nel computer e fornisce informazioni ad altri componenti per una maggiore protezione.

In base alle informazioni raccolte da Controllo sistema, Kaspersky Anti-Virus può eseguire il rollback delle azioni eseguite dai programmi dannosi.

Il rollback delle azioni eseguite dai programmi dannosi può essere avviato da uno dei seguenti componenti di protezione:

- Controllo sistema - in base agli schemi di attività pericolose;
- Difesa Proattiva;
- Anti-Virus File;
- durante l'esecuzione di una scansione virus.

Se nel sistema vengono rilevati eventi sospetti, i componenti di protezione di Kaspersky Anti-Virus possono richiedere ulteriori informazioni a Controllo sistema. Nella modalità di protezione interattiva di Kaspersky Anti-Virus (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)), è possibile visualizzare i dati raccolti dal componente Controllo sistema, che vengono presentati in un rapporto sulla cronologia delle attività pericolose. Questi dati aiutano a prendere una decisione al momento di selezionare un'azione nella finestra di notifica. Quando viene rilevato un programma dannoso, nella parte superiore della finestra di notifica (vedere pagina [128](#)) viene visualizzato il collegamento al rapporto di Controllo sistema e viene richiesto di scegliere un'azione.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione di Controllo sistema	86
Utilizzo degli schemi di attività pericolose (BSS).....	86
Rollback delle azioni di un programma dannoso.....	87

ABILITAZIONE E DISABILITAZIONE DI CONTROLLO SISTEMA

Per impostazione predefinita, Controllo sistema è abilitato ed eseguito nella modalità consigliata dagli specialisti di Kaspersky Lab. Se necessario, è possibile disabilitare Controllo sistema.

È consigliabile non disabilitare il componente a meno che non sia assolutamente necessario, dal momento che questa operazione riduce inevitabilmente l'efficienza di Difesa Proattiva e di altri componenti di protezione che possono richiedere i dati raccolti da Controllo sistema per identificare la potenziale minaccia rilevata.

► *Per disabilitare Controllo sistema:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Controllo sistema**.
3. Nella parte destra della finestra deselezionare la casella **Abilita Controllo sistema**.

UTILIZZO DEGLI SCHEMI DI ATTIVITÀ PERICOLOSE (BSS)

Gli schemi di attività pericolose, o BSS (Behavior Stream Signatures), contengono sequenze di azioni tipiche di applicazioni classificate come pericolose. Se l'attività di un'applicazione corrisponde a uno schema di attività pericolosa, Kaspersky Anti-Virus esegue l'azione specificata.

Per assicurare un'efficace protezione in tempo reale, Kaspersky Anti-Virus aggiunge gli schemi di attività pericolose, che vengono utilizzati da Controllo sistema, durante gli aggiornamenti dei database.

Per impostazione predefinita, quando Kaspersky Anti-Virus viene eseguito in modalità automatica, se l'attività di un'applicazione corrisponde a uno schema di attività pericolosa, Controllo sistema sposta l'applicazione in Quarantena. Se viene eseguito in modalità interattiva, Controllo sistema richiede all'utente di scegliere un'azione. È possibile

specificare l'azione che il componente deve eseguire quando l'attività di un'applicazione corrisponde a uno schema di attività pericolosa.

Oltre all'esatta corrispondenza tra azioni delle applicazioni e schemi di attività pericolose, Controllo sistema rileva anche le azioni che corrispondono solo parzialmente a schemi di attività pericolose, considerate sospette in base all'analisi euristica. Se viene rilevata un'attività sospetta, Controllo sistema richiede l'intervento dell'utente indipendentemente dalla modalità di esecuzione.

► *Per selezionare l'azione che il componente deve eseguire quando l'attività di un'applicazione corrisponde a uno schema di attività pericolosa:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Controllo sistema**.
3. Nella parte destra della finestra, nella sezione **Analisi euristica**, selezionare la casella **Usa schemi aggiornabili di attività pericolose (BSS)**.
4. Fare click su **Seleziona azione** e specificare l'azione desiderata nell'elenco a discesa.

ROLLBACK DELLE AZIONI DI UN PROGRAMMA DANNOSO

È possibile utilizzare l'opzione per il rollback delle operazioni eseguite dal malware nel sistema. Per consentire il rollback, Controllo sistema registra la cronologia delle attività dei programmi. È possibile limitare il volume di informazioni memorizzate da Controllo sistema per il rollback.

Per impostazione predefinita, Kaspersky Anti-Virus esegue automaticamente il rollback delle operazioni appropriate quando i componenti di protezione rilevano attività dannose. Se viene eseguito in modalità interattiva, Controllo sistema richiede all'utente di scegliere un'azione. È possibile specificare l'azione da eseguire se è disponibile il rollback delle azioni eseguite da un programma dannoso.

La procedura di rollback delle operazioni del malware influisce su un set di dati ben definito. Non provoca conseguenze negative per il sistema operativo o l'integrità dei dati nel computer.

► *Per selezionare l'azione da eseguire se è disponibile il rollback delle azioni eseguite da un programma dannoso:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Controllo sistema**.
3. Nella parte destra della finestra, nella sezione **Rollback delle azioni del malware**, selezionare **Seleziona azione**, quindi selezionare l'azione desiderata dall'elenco a discesa.

► *Per limitare il volume di informazioni memorizzate da Controllo sistema per il rollback:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Centro protezione**, selezionare il componente **Controllo sistema**.
3. Nella parte destra della finestra, nella sezione **Rollback delle azioni del malware**, selezionare la casella **Limita i dati da memorizzare per il rollback** e specificare il volume massimo di dati che devono essere memorizzati da Controllo sistema per il rollback.

PROTEZIONE DELLA RETE

Vari strumenti e impostazioni di Kaspersky Anti-Virus garantiscono la sicurezza e il controllo delle attività di rete.

Nelle sezioni seguenti sono disponibili informazioni dettagliate sulla verifica delle connessioni di rete, le impostazioni del server proxy e il monitoraggio delle porte della rete.

IN QUESTA SEZIONE:

Scansione delle connessioni crittografate	88
Configurazione del server proxy	90
Creazione di un elenco di porte monitorate	90

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE

La connessione tramite i protocolli SSL / TLS assicura la protezione del canale di scambio dei dati via Internet. I protocolli SSL / TLS sono in grado di identificare le parti che scambiano dati tramite certificati elettronici, codificare i dati trasferiti e garantirne l'integrità durante il trasferimento.

Queste funzionalità dei protocolli vengono utilizzate dagli hacker per diffondere programmi dannosi, poiché quasi tutti i programmi anti-virus non esaminano il traffico SSL / TLS.

Kaspersky Anti-Virus esegue la scansione delle connessioni crittografate utilizzando un certificato di Kaspersky Lab.

In caso di rilevamento di un certificato non valido durante la connessione al server, ad esempio se il certificato viene sostituito da un utente malintenzionato, verrà visualizzata una notifica che richiede di accettare o rifiutare il certificato.

Se si è certi che la connessione a un sito Web è sicura nonostante l'utilizzo di un certificato non valido, è possibile aggiungere il sito Web all'elenco delle URL attendibili. La connessione crittografata con il sito Web non verrà esaminata da Kaspersky Anti-Virus.

È possibile utilizzare l'Installazione guidata certificato per installare un certificato per la scansione delle connessioni crittografate in modalità semi-interattiva in Microsoft Internet Explorer, Mozilla Firefox (se non è in esecuzione) e Google Chrome, nonché ottenere istruzioni per l'installazione del certificato di Kaspersky Lab per Opera.

► *Per abilitare la scansione delle connessioni crittografate e installare il certificato di Kaspersky Lab:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Rete**.
3. Nella finestra visualizzata selezionare la casella **Scansione delle connessioni crittografate**. Quando si abilita questa impostazione per la prima volta, viene avviata automaticamente l'Installazione guidata certificato.
4. Se la procedura guidata non viene avviata, fare click sul pulsante **Installa certificato**. Verrà avviata una procedura guidata che contiene le istruzioni da seguire per installare correttamente il certificato di Kaspersky Lab.

IN QUESTA SEZIONE:

Scansione delle connessioni crittografate in Mozilla Firefox	88
Scansione delle connessioni crittografate in Opera	89

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE IN MOZILLA FIREFOX

Il browser Mozilla Firefox non utilizza l'archivio certificati di Microsoft Windows. Per eseguire la scansione delle connessioni SSL in Mozilla Firefox, è necessario installare il certificato di Kaspersky Lab manualmente.

È possibile utilizzare l'Installazione guidata certificato se il browser non è in esecuzione.

► *Per installare il certificato di Kaspersky Lab:*

1. Nel menu del browser selezionare **Tools (Strumenti)** → **Settings (Impostazioni)**.
2. Nella finestra visualizzata selezionare la sezione **Additional (Avanzate)**.
3. Nella sezione **Certificates (Certificati)** selezionare la scheda **Security (Protezione)** e fare click sul pulsante **View Certificates (Visualizzazione certificati)**.
4. Nella finestra visualizzata selezionare la scheda **Certification Authorities (Autorità)** e fare click sul pulsante **Restore (Ripristina)**.

5. Nella finestra visualizzata selezionare il file del certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
 6. Nella finestra visualizzata selezionare le caselle relative alle azioni da sottoporre a scansione con il certificato installato. Per visualizzare le informazioni relative al certificato, fare click sul pulsante **View (Visualizza)**.
- *Per installare il certificato di Kaspersky Lab per Mozilla Firefox versione 3.x manualmente:*
1. Nel menu del browser selezionare **Tools (Strumenti)** → **Settings (Impostazioni)**.
 2. Nella finestra visualizzata selezionare la sezione **Additional (Avanzate)**.
 3. Nella scheda **Encryption (Cifratura)** fare click sul pulsante **View Certificates (Visualizzazione certificati)**.
 4. Nella finestra visualizzata selezionare la scheda **Authorities (Autorità)** e fare click sul pulsante **Import (Importa)**.
 5. Nella finestra visualizzata selezionare il file del certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
 6. Nella finestra visualizzata selezionare le caselle relative alle azioni da sottoporre a scansione con il certificato installato. Per visualizzare le informazioni relative al certificato, fare click sul pulsante **View (Visualizza)**.

Se il computer è dotato del sistema operativo Microsoft Windows Vista o Microsoft Windows 7, il percorso del file del certificato di Kaspersky Lab è il seguente: `%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE IN OPERA

Il browser Opera non utilizza l'archivio certificati di Microsoft Windows. Per eseguire la scansione delle connessioni SSL in Opera, è necessario installare il certificato di Kaspersky Lab manualmente.

- *Per installare il certificato di Kaspersky Lab:*
1. Nel menu del browser selezionare **Tools (Strumenti)** → **Settings (Impostazioni)**.
 2. Nella finestra visualizzata selezionare la sezione **Additional (Avanzate)**.
 3. Nella parte sinistra della finestra selezionare la scheda **Security (Protezione)** e fare click sul pulsante **Manage Certificates (Gestisci certificati)**.
 4. Nella finestra visualizzata selezionare la scheda **Vendors (Fornitori)** e fare click sul pulsante **Import (Importa)**.
 5. Nella finestra visualizzata selezionare il file del certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
 6. Nella finestra visualizzata fare click sul pulsante **Installa**. Il certificato di Kaspersky Lab verrà installato. Per visualizzare le informazioni sul certificato e selezionare le azioni per cui verrà utilizzato, selezionare il certificato nell'elenco e fare click sul pulsante **View (Visualizza)**.
- *Per installare il certificato di Kaspersky Lab per Opera versione 9.x:*
1. Nel menu del browser selezionare **Tools (Strumenti)** → **Settings (Impostazioni)**.
 2. Nella finestra visualizzata selezionare la sezione **Additional (Avanzate)**.
 3. Nella parte sinistra della finestra selezionare la scheda **Security (Protezione)** e fare click sul pulsante **Manage Certificates (Gestisci certificati)**.
 4. Nella finestra visualizzata selezionare la scheda **Authorities (Autorità)** e fare click sul pulsante **Import (Importa)**.
 5. Nella finestra visualizzata selezionare il file del certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
`%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\fake\Kaspersky Anti-Virus personal root certificate.cer.`
 6. Nella finestra visualizzata fare click sul pulsante **Installa**. Il certificato di Kaspersky Lab verrà installato.

Se il computer è dotato del sistema operativo Microsoft Windows Vista o Microsoft Windows 7, il percorso del file del certificato di Kaspersky Lab è il seguente: %AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert(fake)Kaspersky Anti-Virus personal root certificate.cer.

CONFIGURAZIONE DEL SERVER PROXY

Se la connessione a Internet del computer viene stabilita tramite un server proxy, potrebbe essere necessario configurarne le impostazioni di connessione. Kaspersky Anti-Virus utilizza tali impostazioni per determinati componenti di protezione, nonché per l'aggiornamento dei moduli di applicazione e dei database.

Se la rete include un server proxy che utilizza una porta non standard, è consigliabile aggiungere il numero di porta all'elenco di porte monitorate (vedere la sezione "Creazione di un elenco di porte monitorate" a pagina [90](#)).

➤ *Per configurare la connessione a un server proxy:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Rete**.
3. Nella sezione **Server proxy** fare click sul pulsante **Impostazioni del server proxy**.
4. Nella finestra **Impostazioni del server proxy** visualizzata specificare le impostazioni desiderate per la connessione a un server proxy.

CREAZIONE DI UN ELENCO DI PORTE MONITORATE

Componenti della protezione come Anti-Virus Posta, Anti-Virus Web e Anti-Virus IM (vedere pagina [77](#)) controllano i flussi di dati trasferiti attraverso protocolli specifici e determinate porte TCP del computer. Anti-Virus Posta, ad esempio, analizza le informazioni trasferite tramite il protocollo SMTP, mentre Anti-Virus Web esamina le informazioni trasferite tramite HTTP, HTTPS e FTP.

È possibile abilitare il monitoraggio tutte le porte di rete o solo delle porte selezionate. Se si configura il prodotto per il monitoraggio delle porte selezionate, è possibile creare un elenco di programmi per cui monitorare tutte le porte. È consigliabile espandere questo elenco includendo le applicazioni che ricevono o trasferiscono dati tramite FTP.

➤ *Per aggiungere una porta all'elenco delle porte monitorate:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rete**.
3. Nella sezione **Porte monitorate** selezionare **Soltanto le porte selezionate** e fare click sul pulsante **Seleziona**.
Verrà visualizzata la finestra **Porte di rete**.
4. Fare click sul collegamento **Aggiungi** sotto l'elenco delle porte nella parte superiore della finestra per aprire la finestra **Porta di rete** e immettere il numero e la descrizione di una porta.

➤ *Per escludere una porta dall'elenco di porte monitorate:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rete**.
3. Nella sezione **Porte monitorate** selezionare **Soltanto le porte selezionate** e fare click sul pulsante **Seleziona**.
Verrà visualizzata la finestra **Porte di rete**.
4. Nell'elenco delle porte nella parte superiore della finestra deselezionare la casella accanto alla descrizione della porta da escludere.

➤ *Per creare un elenco di applicazioni per cui monitorare tutte le porte:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare **Rete**.
3. Nella sezione **Porte monitorate** selezionare **Soltanto le porte selezionate** e fare click sul pulsante **Seleziona**.
Verrà visualizzata la finestra **Porte di rete**.

4. Selezionare la casella **Controlla tutte le porte per le applicazioni specificate** e nell'elenco delle applicazioni sottostante selezionare le caselle accanto ai nomi delle applicazioni per cui controllare tutte le porte.
5. Se l'applicazione desiderata non è inclusa nell'elenco, aggiungerla nel modo seguente:
 - a. Fare click sul collegamento **Aggiungi** sotto l'elenco delle applicazioni per aprire un menu, quindi selezionare un elemento:
 - Per specificare il percorso del file eseguibile di un'applicazione, selezionare **Sfoglia** e specificare il percorso del file nel computer.
 - Per selezionare un'applicazione dall'elenco delle applicazioni in esecuzione, selezionare **Applicazioni**. Nella finestra **Seleziona applicazione** visualizzata selezionare l'applicazione desiderata.
 - b. Nella finestra **Applicazione** immettere una descrizione per l'applicazione selezionata.

AREA ATTENDIBILE

L'*area attendibile* è un elenco degli oggetti che non devono essere monitorati dall'applicazione. In altre parole, si tratta di una serie di programmi esclusi dall'ambito di protezione di Kaspersky Anti-Virus.

L'area attendibile viene creata in base all'elenco delle applicazioni attendibili (vedere la sezione "Creazione di un elenco di applicazioni attendibili" a pagina [92](#)) e alle regole di esclusione (vedere la sezione "Creazione di regole di esclusione" a pagina [92](#)), a seconda delle funzionalità degli oggetti utilizzati e delle applicazioni installate nel computer. L'inclusione di oggetti nell'area attendibile può ad esempio essere necessaria se Kaspersky Anti-Virus blocca l'accesso a un oggetto o un'applicazione, benché si abbia la certezza che l'oggetto o l'applicazione non ponga alcun problema di protezione.

Se ad esempio si ritiene che gli oggetti utilizzati da Blocco note di Microsoft Windows siano sicuri e non richiedano alcuna scansione, è possibile aggiungere Blocco note all'elenco di applicazioni attendibili per escludere dalla scansione gli oggetti utilizzati da questo processo.

Alcune azioni classificate come pericolose possono essere sicure nell'ambito di determinate applicazioni. Ad esempio, le applicazioni che commutano automaticamente i layout di tastiera, come Punto Switcher, intercettano regolarmente il testo immesso con la 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.

Quando si aggiunge un'applicazione all'elenco delle applicazioni attendibili, le relative attività di rete e sui file (incluse quelle sospette) non vengono controllate. Lo stesso vale per i tentativi di accesso al registro di sistema. Il file eseguibile e il processo dell'applicazione attendibile sono comunque sottoposti a scansione virus come in precedenza. Per escludere completamente un'applicazione dalla scansione, è consigliabile utilizzare le regole di esclusione.

L'esclusione delle applicazioni attendibili dalla scansione consente di evitare eventuali problemi di compatibilità dell'applicazione con altri programmi, ad esempio il problema della doppia scansione del traffico di rete di un computer di terze parti da parte di Kaspersky Anti-Virus e di un'altra applicazione anti-virus, nonché di migliorare le prestazioni del computer, aspetto di fondamentale importanza quando si utilizzano applicazioni server.

Le regole di esclusione dell'area attendibile consentono inoltre di utilizzare in modo sicuro le applicazioni legittime potenzialmente utilizzabili da un utente malintenzionato per danneggiare i dati o il computer dell'utente. Queste applicazioni di per sé non includono funzionalità dannose, ma possono essere utilizzate come componenti ausiliari di un programma dannoso. Questa categoria include applicazioni di amministrazione remota, client IRC, server FTP, utilità per arrestare o nascondere processi, keylogger, programmi per l'hackeraggio delle password, dialer e altri software. Tali applicazioni possono essere bloccate da Kaspersky Anti-Virus. Per evitare il blocco, è possibile configurare le regole di esclusione.

Una *regola di esclusione* è un gruppo di condizioni che determinano l'esclusione di un oggetto dalla scansione eseguita da Kaspersky Anti-Virus. In tutti gli altri casi, l'oggetto viene esaminato da tutti i componenti di protezione in base alle relative impostazioni.

Le regole di esclusione dell'area attendibile possono essere utilizzate da diversi componenti dell'applicazione, quali Anti-Virus File (vedere la sezione "Anti-Virus File" a pagina [68](#)), Anti-Virus Posta (vedere la sezione "Anti-Virus Posta" a pagina [73](#)) e Anti-Virus Web (vedere la sezione "Anti-Virus Web" a pagina [77](#)), o durante l'esecuzione delle attività di scansione virus.

IN QUESTA SEZIONE:

Creazione di un elenco di applicazioni attendibili	92
Creazione di regole di esclusione	92

CREAZIONE DI UN ELENCO DI APPLICAZIONI ATTENDIBILI

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. Quando si aggiunge un'applicazione all'elenco di applicazioni attendibili, Kaspersky Anti-Virus la esclude dalla scansione.

➤ *Per aggiungere un'applicazione all'elenco di applicazioni attendibili:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Minacce ed Esclusioni**.
3. Nella sezione **Esclusioni** fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella scheda **Applicazioni attendibili**, fare click sul pulsante **Aggiungi** per aprire il menu di selezione dell'applicazione.
5. Nel menu visualizzato selezionare un'applicazione dall'elenco **Applicazioni** o selezionare **Sfoglia** per specificare il percorso dei file eseguibili dell'applicazione desiderata.
6. Nella finestra **Esclusioni per l'applicazione** visualizzata selezionare le caselle per i tipi di attività dell'applicazione da escludere dalla scansione.

CREAZIONE DI REGOLE DI ESCLUSIONE

Se si utilizzano applicazioni riconosciute da Kaspersky Anti-Virus come legittime ma potenzialmente utilizzabili da un intruso per danneggiare i dati o il computer, è consigliabile configurare regole di esclusione per tali applicazioni.

➤ *Per creare una regola di esclusione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Minacce ed Esclusioni**.
3. Nella sezione **Esclusioni** fare click sul pulsante **Impostazioni**.
4. Nella finestra visualizzata, nella scheda **Regole di esclusione**, fare click sul pulsante **Aggiungi**.
5. Nella finestra **Regola di esclusione** visualizzata modificare le impostazioni della regola di esclusione.

PRESTAZIONI E COMPATIBILITÀ CON ALTRE APPLICAZIONI

Le prestazioni di Kaspersky Anti-Virus dipendono dal numero di minacce rilevabili, ma anche dal consumo di energia e dall'impiego di risorse.

Kaspersky Anti-Virus consente di selezionare le varie categorie di minacce (vedere la sezione "Selezione delle categorie di minacce rilevabili" a pagina [93](#)) che devono essere rilevate dall'applicazione.

Il consumo di energia è particolarmente importante per i computer portatili. La scansione virus dei computer e l'aggiornamento dei database di Kaspersky Anti-Virus spesso richiedono grandi quantità di risorse. La speciale modalità portatile di Kaspersky Anti-Virus (vedere la sezione "Risparmio energetico" a pagina [93](#)) consente di rimandare automaticamente le attività di scansione e aggiornamento pianificate durante l'utilizzo della batteria, riducendo il consumo energetico, mentre la modalità di scansione a PC inattivo (vedere la sezione "Esecuzione di attività in background" a pagina [94](#)) consente di eseguire le attività che richiedono un utilizzo considerevole delle risorse quando il computer non è in uso.

L'impiego delle risorse del computer da parte di Kaspersky Anti-Virus può ridurre le prestazioni di altre applicazioni. Per risolvere i problemi di operazioni simultanee che aumentano il carico sulla CPU e sui dischi, Kaspersky Anti-Virus consente di sospendere le attività di scansione e di cedere risorse alle altre applicazioni (vedere la sezione "Allocazione delle risorse del computer durante la scansione virus" a pagina [94](#)) in esecuzione nel computer.

Nella modalità Profilo Gioco (vedere pagina [95](#)) l'applicazione disabilita automaticamente la visualizzazione delle notifiche di Kaspersky Anti-Virus quando vengono avviate altre applicazioni a schermo intero.

In caso di infezione attiva del sistema, la procedura avanzata di disinfezione richiede il riavvio del computer, con eventuali conseguenze per le prestazioni di altre applicazioni. Se necessario, è possibile disabilitare la tecnologia avanzata di disinfezione (vedere pagina [93](#)) per evitare riavvii indesiderati del computer.

IN QUESTA SEZIONE:

Selezione delle categorie di minacce rilevabili	93
Risparmio energetico	93
Disinfezione avanzata	93
Allocazione delle risorse del computer durante la scansione virus	94
Esecuzione di attività in background	94
Modalità a schermo intero. Profilo Gioco.....	95

SELEZIONE DELLE CATEGORIE DI MINACCE RILEVABILI

Le minacce rilevate da Kaspersky Anti-Virus sono suddivise in categorie in base a vari attributi. L'applicazione esegue sempre la ricerca di virus, programmi Trojan e strumenti dannosi. Questi programmi possono infatti danneggiare gravemente il computer. Per migliorare l'affidabilità della protezione del computer, è possibile estendere l'elenco delle minacce rilevate abilitando il controllo delle azioni eseguite da applicazioni legittime potenzialmente utilizzabili da un utente malintenzionato per danneggiare i dati o il computer dell'utente.

◆ *Per selezionare le categorie di minacce rilevabili:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Minacce ed Esclusioni**.
3. Nella parte destra della finestra, fare click sul pulsante **Impostazioni** sotto l'elenco **È in atto il monitoraggio dei seguenti tipi di minacce**.
4. Nella finestra **Minacce** visualizzata selezionare le caselle per le categorie di minacce da rilevare.

RISPARMIO ENERGETICO

Per risparmiare energia su un computer portatile, è possibile rimandare le attività di scansione virus e di aggiornamento pianificato. Se necessario, è possibile aggiornare Kaspersky Anti-Virus o avviare una scansione virus manuale.

◆ *Per abilitare la modalità di risparmio energetico durante l'alimentazione a batteria:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Risparmio energetico**.
3. Nella parte destra della finestra selezionare la casella **Disabilita le scansioni programmate durante l'alimentazione a batteria**.

DISINFEZIONE AVANZATA

Gli attuali programmi dannosi possono invadere i livelli più bassi di un sistema operativo, rendendone praticamente impossibile l'eliminazione. Se viene rilevata un'attività dannosa all'interno del sistema, Kaspersky Anti-Virus offre la possibilità di applicare la Tecnologia di disinfezione avanzata, che consente di eliminare la minaccia e di rimuoverla dal computer.

Al termine della procedura di disinfezione avanzata, l'applicazione riavvia il computer. Dopo aver riavviato il computer, viene consigliata l'esecuzione di una scansione virus completa (vedere la sezione "Esecuzione di una scansione virus completa del computer" a pagina [42](#)).

◆ *Per consentire a Kaspersky Anti-Virus di utilizzare la tecnologia di disinfezione avanzata:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Compatibilità**.
3. Selezionare la casella **Attiva tecnologia avanzata di disinfezione**.

ALLOCAZIONE DELLE RISORSE DEL COMPUTER DURANTE LA SCANSIONE VIRUS

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

Alcune applicazioni, tuttavia, vengono avviate immediatamente dopo il rilascio delle risorse della CPU e sono 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.

► *Per rimandare le attività di scansione di Kaspersky Anti-Virus quando rallentano altre applicazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Compatibilità**.
3. Selezionare la casella **Concedi risorse alle altre applicazioni**.

ESECUZIONE DI ATTIVITÀ IN BACKGROUND

Per ottimizzare il carico sulle risorse del computer, Kaspersky Anti-Virus esegue la scansione periodica dei rootkit in background ed effettua le attività che richiedono un utilizzo considerevole delle risorse mentre il computer è inattivo.

La scansione periodica dei rootkit viene eseguita mentre l'utente lavora al computer. La scansione richiede al massimo cinque minuti e utilizza una quantità minima di risorse del computer.

Mentre il computer è inattivo possono essere eseguite le seguenti attività:

- aggiornamento automatico dei database anti-virus e dei moduli del programma;
- scansione di memoria del sistema, oggetti di avvio e partizione di sistema.

Le attività di scansione a PC inattivo vengono eseguite se il computer è stato bloccato dall'utente o se lo screensaver viene visualizzato per almeno cinque minuti.

Se il computer è alimentato a batteria, non viene eseguita alcuna attività di scansione o aggiornamento mentre il computer è inattivo.

Quando le attività vengono eseguite in background, il relativo stato di avanzamento è visualizzato in Gestione attività (vedere la sezione "Gestione delle attività di scansione. Gestione attività" a pagina [63](#)).

IN QUESTA SEZIONE:

Ricerca di rootkit in background	94
Scansione a PC inattivo	94

RICERCA DI ROOTKIT IN BACKGROUND

Per impostazione predefinita, Kaspersky Anti-Virus esegue periodicamente la ricerca dei rootkit. Se necessario, è possibile disabilitare la ricerca dei rootkit.

► *Per disabilitare la ricerca periodica dei rootkit:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare **Impostazioni generali**.
3. Nella parte destra della finestra deselezionare la casella **Esegui ricerca periodica di rootkit**.

SCANSIONE A PC INATTIVO

La prima fase della scansione a PC inattivo è il controllo dell'aggiornamento dei database e dei moduli dell'applicazione. Se il controllo rivela che è necessario un aggiornamento, viene avviata l'attività di aggiornamento automatico. Nella seconda fase, l'applicazione verifica la data e lo stato dell'ultima esecuzione della scansione a PC inattivo. Se la

scansione a PC inattivo non è mai stata eseguita, se è stata eseguita da più di sette giorni o se è stata interrotta, l'applicazione esegue l'attività di scansione della memoria del sistema, degli oggetti di avvio e del Registro di sistema.

La scansione a PC inattivo viene eseguita utilizzando il livello di analisi euristica approfondito, che aumenta le probabilità di rilevamento delle minacce.

Quando l'utente riprende il lavoro, l'attività di scansione a PC inattivo viene interrotta automaticamente. L'applicazione memorizza il punto in cui l'attività è stata interrotta, in modo da riprendere la scansione da questo punto in seguito.

Se l'attività di scansione a PC inattivo è stata interrotta durante il download di un pacchetto di aggiornamento, l'aggiornamento verrà ripreso dall'inizio.

➤ *Per disabilitare la modalità di scansione a PC inattivo:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Scansione**, selezionare **Impostazioni generali**.
3. Nella parte destra della finestra deselezionare la casella **Esegui scansione quando il PC non viene utilizzato**.

MODALITÀ A SCHERMO INTERO. PROFILO GIOCO

Determinati programmi eseguiti in modalità a schermo intero, in particolare i giochi per computer, sono scarsamente compatibili con alcune funzionalità di Kaspersky Anti-Virus, come ad esempio le notifiche a comparsa. Spesso queste applicazioni richiedono significative risorse di sistema, di conseguenza l'esecuzione di alcune attività di Kaspersky Anti-Virus potrebbe rallentare le prestazioni.

Per evitare di dover disabilitare manualmente le notifiche e sospendere le attività a ogni avvio di applicazioni a schermo intero, Kaspersky Anti-Virus include la possibilità di modificare temporaneamente le impostazioni mediante Profilo Gioco. Quando Profilo Gioco è attivo, con il passaggio alla modalità a schermo intero vengono modificate automaticamente le impostazioni di tutti i componenti del prodotto per assicurare in funzionamento ottimale. All'uscita dalla modalità a schermo intero, vengono ripristinati i valori originali delle impostazioni del prodotto.

➤ *Per abilitare Profilo Gioco:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Profilo Gioco**.
3. Selezionare la casella **Usa Profilo Gioco** e specificare nella sezione **Opzioni profilo** sottostante le impostazioni desiderate.

AUTO-DIFESA DI KASPERSKY ANTI-VIRUS

Poiché Kaspersky Anti-Virus assicura la protezione del computer dal malware, i programmi dannosi che penetrano nel computer possono tentare di bloccare Kaspersky Anti-Virus o perfino di eliminare l'applicazione dal computer.

La stabilità delle prestazioni del sistema di protezione del computer viene assicurata dalle funzionalità di auto-difesa e protezione dal controllo esterno implementate in Kaspersky Anti-Virus.

La funzionalità di auto-difesa di Kaspersky Anti-Virus impedisce la modifica e l'eliminazione di file sul disco rigido, processi in memoria e voci del registro di sistema. La protezione dal controllo esterno consente di bloccare tutti i tentativi di controllare in remoto i servizi delle applicazioni.

Nei computer con sistemi operativi a 64 bit e Microsoft Windows Vista, l'auto-difesa di Kaspersky Anti-Virus è disponibile solo per impedire la modifica o l'eliminazione dei file del programma nelle unità locali e le relative voci del registro di sistema.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione dell'auto-difesa	96
Protezione dal controllo esterno	96

ABILITAZIONE E DISABILITAZIONE DELL'AUTO-DIFESA

Per impostazione predefinita, la funzionalità Auto-Difesa di Kaspersky Anti-Virus è abilitata. Se necessario, è possibile disabilitare Auto-Difesa.

► *Per disabilitare la funzionalità Auto-Difesa di Kaspersky Anti-Virus:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Auto-Difesa**.
3. Nella parte destra della finestra deselezionare la casella **Abilita l'Auto-Difesa**.

PROTEZIONE DAL CONTROLLO ESTERNO

Per impostazione predefinita, la protezione dal controllo esterno è abilitata. Se necessario, è possibile disabilitarla.

Quando si utilizzano applicazioni di amministrazione remota (come RemoteAdmin), è necessario aggiungere tali applicazioni all'elenco Applicazioni attendibili (vedere la sezione "Area attendibile" a pagina [91](#)) quando il servizio di controllo esterno è attivato e abilitare l'impostazione **Non monitorare l'attività dell'applicazione**.

► *Per disabilitare la protezione dal controllo esterno:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Auto-Difesa**.
3. Nella sezione **Controllo esterno** deselezionare la casella **Disabilita il servizio di controllo esterno**.

QUARANTENA E BACKUP

La *Quarantena* è una speciale area per l'archiviazione dei file potenzialmente infetti da virus e dei file che non è possibile disinfettare al momento del rilevamento.

Un potenzialmente infetto può essere rilevato e messo in quarantena nel corso di una scansione virus o da Anti-Virus File, Anti-Virus Posta o Difesa Proattiva.

I file sono messi in quarantena nei seguenti casi:

- Il codice del file ricorda una minaccia nota ma in parte modificata o ha una struttura simile a quella del malware ma non è registrato nel database. In questo caso, il file viene messo in quarantena dopo l'analisi euristica eseguita da Anti-Virus File e Anti-Virus Posta o durante la scansione virus. In rari casi, l'analisi euristica causa falsi allarmi.
- La sequenza di operazioni eseguita da un oggetto appare sospetta. In questo caso, il file viene messo in quarantena dopo l'analisi del relativo comportamento da parte del componente Difesa Proattiva.

I file in quarantena non costituiscono alcuna minaccia per il computer. Nel corso del tempo diventano disponibili informazioni sulle nuove minacce e sui metodi che consentono di neutralizzarle, pertanto Kaspersky Anti-Virus potrebbe essere in grado di disinfettare un file in quarantena.

L'*archivio di backup* archivia le copie di backup dei file che sono stati eliminati o modificati durante il processo di disinfezione.

IN QUESTA SEZIONE:

Archiviazione dei file in quarantena e backup	97
Utilizzo dei file in quarantena	97
Utilizzo degli oggetti nell'archivio Backup	98
Scansione dei file in quarantena dopo un aggiornamento	99

ARCHIVIAZIONE DEI FILE IN QUARANTENA E BACKUP

Per impostazione predefinita, la durata massima per l'archiviazione degli oggetti è di 30 giorni. Al termine di questo periodo, gli oggetti vengono eliminati. È possibile annullare il limite di tempo o modificare la durata massima per l'archiviazione degli oggetti.

È inoltre possibile specificare la dimensione massima di Quarantena e Backup. Quando viene raggiunta la dimensione massima, il contenuto di Quarantena e Backup viene sostituito da nuovi oggetti. Per impostazione predefinita, il limite per la dimensione massima è disabilitato.

➤ *Per modificare la durata massima per l'archiviazione degli oggetti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Archiviazione degli oggetti di quarantena e backup**, selezionare la casella **Mantieni gli oggetti per non più di** e specificare la durata massima per l'archiviazione degli oggetti in quarantena.

➤ *Per configurare la dimensione massima di Quarantena e Backup:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Archiviazione degli oggetti di quarantena e backup**, selezionare la casella **Dimensione massima** e specificare la dimensione massima della cartella Quarantena e Backup.

UTILIZZO DEI FILE IN QUARANTENA

La quarantena di Kaspersky Anti-Virus consente di eseguire le seguenti operazioni:

- mettere in quarantena i file potenzialmente infetti;
- esaminare i file in quarantena utilizzando la versione corrente dei database di Kaspersky Anti-Virus;
- ripristinare i file nelle cartelle originali da cui sono stati spostati in quarantena;
- eliminare i file selezionati dalla quarantena;
- inviare i file in quarantena a Kaspersky Lab per l'analisi.

È possibile utilizzare i seguenti metodi per spostare un file in quarantena:

- utilizzando il pulsante **Sposta in Quarantena** nella finestra **Quarantena**;
- utilizzando il menu di scelta rapida del file.

➤ *Per spostare un oggetto in quarantena dalla finestra Quarantena:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Quarantena** fare click sul pulsante **Sposta in Quarantena**.
4. Nella finestra visualizzata selezionare il file da spostare in quarantena.

➤ *Per spostare un file in quarantena utilizzando il menu di scelta rapida:*

1. Aprire Esplora risorse di Microsoft Windows e passare alla cartella che contiene il file da spostare in quarantena.
2. Fare click con il pulsante destro del mouse per aprire il menu di scelta rapida del file e selezionare **Sposta in Quarantena**.

➤ *Per eseguire la scansione di un file in quarantena:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Quarantena** selezionare il file che si desidera esaminare.
4. Fare click sul pulsante **Scansione**.

➤ *Per ripristinare un oggetto in quarantena:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Quarantena** selezionare il file che si desidera ripristinare.
4. Fare click sul pulsante **Ripristina**.

➤ *Per eliminare un oggetto in quarantena:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Quarantena** selezionare il file che si desidera eliminare.
4. Fare click con il pulsante destro del mouse sul file per aprire il relativo menu di scelta rapida, quindi selezionare **Elimina**.

➤ *Per inviare un oggetto in quarantena a Kaspersky Lab per l'analisi:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Quarantena** selezionare il file che si desidera inviare per l'analisi.
4. Fare click con il pulsante destro del mouse per aprire il menu di scelta rapida del file, quindi selezionare **Invia per l'analisi**.

UTILIZZO DEGLI OGGETTI NELL'ARCHIVIO BACKUP

L'archivio Backup di Kaspersky Anti-Virus consente di eseguire le seguenti operazioni:

- ripristinare i file in una cartella specificata o nella cartella originale in cui erano contenuti prima dell'elaborazione da parte di Kaspersky Anti-Virus;
- eliminare file selezionati o tutti i file dall'archivio Backup.

➤ *Per ripristinare un oggetto dall'archivio Backup:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Archivio** selezionare il file che si desidera ripristinare.
4. Fare click sul pulsante **Ripristina**.

➤ *Per eliminare un file dall'archivio Backup:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Archivio** selezionare il file che si desidera eliminare.
4. Fare click con il pulsante destro del mouse sul file per aprire il relativo menu di scelta rapida, quindi selezionare **Elimina**.

➤ *Per eliminare tutti i file dall'archivio Backup:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Quarantena**.
3. Nella scheda **Archivio** fare click sul pulsante **Cancella archivio**.

SCANSIONE DEI FILE IN QUARANTENA DOPO UN AGGIORNAMENTO

Se l'applicazione ha esaminato un file e non è stata in grado di identificare esattamente i programmi dannosi che lo hanno infettato, il file viene messo in quarantena. Dopo l'aggiornamento dei database, Kaspersky Anti-Virus potrebbe essere in grado di identificare chiaramente ed eliminare la minaccia. È possibile abilitare la scansione automatica degli oggetti in quarantena dopo ogni aggiornamento.

È consigliabile visualizzare periodicamente i file in quarantena. La scansione potrebbe modificarne lo stato degli oggetti. Alcuni file potrebbero essere ripristinati nelle posizioni precedenti, in modo che l'utente possa continuare a utilizzarli.

► Per abilitare la scansione dei file in quarantena dopo l'aggiornamento:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Aggiornamento**, selezionare il componente **Impostazioni di aggiornamento**.
3. Selezionare la casella **Ripeti la scansione degli oggetti in Quarantena dopo l'aggiornamento** nella sezione **Avanzate**.

STRUMENTI AGGIUNTIVI PER UNA MIGLIORE PROTEZIONE DEL COMPUTER

È possibile utilizzare le seguenti procedure guidate e i seguenti strumenti inclusi in Kaspersky Anti-Virus per risolvere specifici problemi relativi alla protezione del computer:

- Creazione guidata Kaspersky Rescue Disk consente di creare un'immagine del disco ISO e di registrare il Kaspersky Rescue Disk in un supporto rimovibile, in modo da poter ripristinare l'operatività del sistema dopo l'attacco di un virus avviando l'applicazione dal supporto rimovibile. È consigliabile utilizzare il Kaspersky Rescue Disk quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione del malware.
- Eliminazione guidata della cronologia delle attività cerca ed elimina le tracce delle attività di un utente nel sistema e le impostazioni del sistema operativo che consentono di raccogliere informazioni sulle attività dell'utente.
- Correzione guidata delle impostazioni di Windows consente di eliminare le impostazioni di sistema danneggiate e le tracce degli oggetti malware nel sistema.
- Correzione guidata delle impostazioni del browser Internet consente di analizzare e regolare le impostazioni di Microsoft Internet Explorer per eliminarne le potenziali vulnerabilità.

Tutti i problemi rilevati dalle procedure guidate (ad eccezione della Creazione guidata Kaspersky Rescue Disk) sono raggruppati in base al tipo di minaccia che costituiscono per il sistema operativo. Kaspersky Lab offre una serie di azioni per ciascun gruppo di problemi, che aiutano a eliminare le vulnerabilità e i punti deboli nelle impostazioni del sistema. Esistono tre gruppi di problemi distinti e, rispettivamente, tre gruppi di azioni a essi associate:

- Le *azioni fortemente consigliate* aiutano a eliminare i problemi che costituiscono una grave minaccia. È consigliabile eseguire tempestivamente tutte le azioni appartenenti a questo gruppo per eliminare la minaccia.
- Le *azioni consigliate* eliminano i problemi che costituiscono un problema potenziale. È consigliabile eseguire anche tutte le azioni appartenenti a questo gruppo per ottenere il livello di protezione ottimale.
- Le *azioni aggiuntive* riparano i danni che non costituiscono una minaccia al momento, ma che potrebbero minacciare la sicurezza del computer in futuro. L'esecuzione di queste azioni assicura una protezione completa del computer. Tali azioni, tuttavia, in alcuni casi possono comportare l'eliminazione di impostazioni dell'utente, come ad esempio i cookie.

IN QUESTA SEZIONE:

Eliminazione della cronologia delle attività	100
Configurazione di un browser in modalità protetta	101
Rollback delle modifiche apportate dalle procedure guidate	102

ELIMINAZIONE DELLA CRONOLOGIA DELLE ATTIVITÀ

Durante l'utilizzo del computer, le azioni dell'utente vengono registrate nel sistema. I dati salvati includono le query di ricerca eseguite e i siti Web visitati dall'utente, i programmi avviati, i file aperti e salvati, il registro eventi di Microsoft Windows, i file temporanei ed altro ancora.

Tutte queste fonti di informazioni sulle attività dell'utente possono contenere dati riservati, incluse le password, e possono diventare disponibili per gli utenti malintenzionati che le analizzano. L'utente spesso non dispone di sufficienti conoscenze per evitare il furto di informazioni con questo metodo.

Kaspersky Anti-Virus include l'Eliminazione guidata della cronologia delle attività. Questa procedura guidata ricerca le tracce di attività dell'utente nel sistema e le impostazioni del sistema operativo che contribuiscono alla memorizzazione dei dati sulle attività dell'utente.

È necessario tenere presente che i dati relativi all'attività dell'utente vengono accumulati continuamente. Viene registrato l'avvio di ogni file o l'apertura di qualsiasi documento. Il log di sistema di Microsoft Windows registra molti eventi che si verificano nel sistema. Per questo motivo, un'esecuzione ripetuta di Eliminazione guidata della cronologia delle attività può rilevare tracce di attività non pulite durante la precedente esecuzione della procedura guidata. Alcuni file, ad esempio il file registro di Microsoft Windows, possono risultare in uso nel sistema mentre la procedura guidata cerca di eliminarli. Per eliminare tali file, la procedura guidata richiede di riavviare il sistema. Tuttavia, durante il riavvio tali file potrebbero essere ricreati e rilevati nuovamente come tracce di attività.

La procedura guidata comprende una serie di schermate (passaggi), tra cui è possibile spostarsi utilizzando i pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, fare click sul pulsante **Annulla**.

➔ *Per rimuovere le tracce delle attività dell'utente nel sistema:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Strumenti**.
3. Nella finestra visualizzata, nella sezione **Eliminazione della cronologia delle attività**, fare click sul pulsante **Avvio**.

Di seguito sono descritti in dettaglio i vari passaggi della procedura guidata.

Passaggio 1. Avvio della procedura guidata

Assicurarsi che l'opzione **Eseguire la diagnostica delle tracce di attività dell'utente** sia selezionata, quindi fare click su **Avanti** per avviare la procedura guidata.

Passaggio 2. Ricerca tracce attività utente

La procedura guidata cerca tracce di attività dell'utente nel computer. Tale attività può richiedere un certo tempo. Al termine della ricerca, la procedura guidata passerà automaticamente al passaggio successivo.

Passaggio 3. Selezione delle azioni di Eliminazione della cronologia delle attività

Al termine della ricerca, vengono visualizzate le tracce delle attività rilevate e le azioni suggerite per eliminarle.

Per visualizzare le azioni di un gruppo, fare click sull'icona **+** a sinistra del nome del gruppo.

Per eseguire una determinata azione, selezionare la casella a sinistra della descrizione dell'azione corrispondente. Per impostazione predefinita, la procedura guidata esegue tutte le azioni consigliate e fortemente consigliate. Se non si desidera eseguire una determinata azione, deselegionare la casella corrispondente.

Deselegionare le caselle selezionate per impostazione predefinita è fortemente sconsigliato, perché tale operazione lascia il computer vulnerabile alle minacce.

Una volta definito il set di azioni da eseguire, fare click su **Avanti**.

Passaggio 4. Eliminazione della cronologia delle attività

La procedura guidata eseguirà le azioni selezionate durante il passaggio precedente. L'eliminazione delle tracce di attività può richiedere alcuni minuti. Per l'eliminazione di alcune tracce di attività, può essere necessario il riavvio del computer. In tal caso, questo verrà segnalato nel corso della procedura guidata.

Al termine dell'eliminazione, la procedura guidata passerà automaticamente al passaggio successivo.

Passaggio 5. Termine della procedura guidata

Se si desidera eliminare automaticamente le tracce delle attività dell'utente alla chiusura di Kaspersky Anti-Virus, utilizzare l'ultima schermata della procedura guidata per selezionare la casella **Pulisci le tracce delle attività a ogni chiusura di Kaspersky Anti-Virus**. Se si desidera eliminare manualmente le tracce delle attività utilizzando la procedura guidata, non selezionare la casella.

Fare click sul pulsante **Fine** per chiudere la procedura guidata.

CONFIGURAZIONE DI UN BROWSER IN MODALITÀ PROTETTA

In alcuni casi, il browser Microsoft Internet Explorer richiede una speciale analisi e configurazione, dal momento che i valori delle impostazioni selezionati dall'utente o le impostazioni predefinite possono causare problemi di protezione.

Di seguito sono riportati alcuni esempi degli oggetti e dei parametri utilizzati nel browser, illustrandone la relazione con le potenziali minacce per la protezione:

- **La cache di Microsoft Internet Explorer.** La cache memorizza i dati scaricati da Internet, evitando di eseguirne nuovamente il download agli accessi successivi. Questo velocizza il download delle pagine Web e riduce il traffico Internet. Inoltre, la cache contiene dati riservati e consente di individuare i siti visitati dall'utente. Alcuni oggetti malware esaminano la cache durante la scansione del disco, consentendo ad esempio agli utenti malintenzionati di ottenere l'indirizzo di posta elettronica dell'utente. Per aumentare la protezione, è consigliabile cancellare il contenuto della cache ogni volta che si chiude il browser.
- **Visualizzazione delle estensioni per i tipi di file conosciuti.** Per maggiore praticità, è possibile disattivare la visualizzazione delle estensioni nei nomi dei file. Talvolta, tuttavia, è utile visualizzare l'estensione del file. I nomi di file di numerosi oggetti dannosi contengono combinazioni di simboli che simulano un'estensione aggiuntiva prima di quella reale (ad esempio, example.txt.com). Se l'estensione reale del file non viene visualizzata, gli utenti possono visualizzare solo la parte del nome del file con l'estensione simulata, scambiando un oggetto dannoso per un file innocuo. Per aumentare la protezione, è consigliabile abilitare la visualizzazione delle estensioni per i file di formato conosciuto.
- **Elenco dei siti Web attendibili.** Per il corretto funzionamento di alcuni siti Web, è necessario aggiungerli all'elenco dei siti attendibili. Al tempo stesso, un oggetto dannoso può aggiungere a questo elenco collegamenti a siti Web creati da un hacker.

La configurazione del browser per Modalità Protetta può causare problemi di visualizzazione di determinati siti Web (ad esempio, se utilizzano elementi ActiveX). Questo problema può essere risolto aggiungendo tali siti Web all'area attendibile.

L'analisi e la configurazione del browser vengono eseguite nel corso della Correzione guidata delle impostazioni del browser. La procedura guidata verifica che siano installati gli aggiornamenti più recenti del browser e che le impostazioni correnti del browser non producano vulnerabilità del sistema. Inoltre, una volta completata la procedura guidata, viene generato un rapporto che può essere inviato a Kaspersky Lab per l'analisi.

La procedura guidata comprende una serie di schermate (passaggi), tra cui è possibile spostarsi utilizzando i pulsanti **Indietro** e **Avanti**. Per chiudere la procedura guidata al termine dell'attività, fare click sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, fare click sul pulsante **Annulla**.

Chiudere tutte le finestre di Microsoft Internet Explorer prima di avviare la diagnostica.

► *Per configurare il browser in modalità protetta:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra selezionare la sezione **Strumenti**.
3. Nella sezione **Correzione delle impostazioni del browser** della finestra visualizzata fare click sul pulsante **Avvio**.

Di seguito sono descritti in dettaglio i vari passaggi della procedura guidata.

Passaggio 1. Avvio della procedura guidata

Assicurarsi che l'opzione **Esegui la diagnostica per Microsoft Internet Explorer** sia selezionata, quindi fare click su **Avanti** per avviare la procedura guidata.

Passaggio 2. Analisi delle impostazioni di Microsoft Internet Explorer

La procedura guidata analizza le impostazioni di Microsoft Internet Explorer. La ricerca di problemi nelle impostazioni del browser può richiedere qualche minuto. Al termine della ricerca, la procedura guidata passerà automaticamente al passaggio successivo.

Passaggio 3. Selezione delle azioni per la configurazione del browser

Al termine della ricerca, vengono visualizzati i problemi rilevati e le azioni suggerite per eliminarli.

Per visualizzare le azioni di un gruppo, fare click sull'icona **+** a sinistra del nome del gruppo.

Per eseguire una determinata azione, selezionare la casella a sinistra della descrizione dell'azione corrispondente. Per impostazione predefinita, la procedura guidata esegue tutte le azioni consigliate e fortemente consigliate. Se non si desidera eseguire una determinata azione, deselezionare la casella corrispondente.

Deselezionare le caselle selezionate per impostazione predefinita è fortemente sconsigliato, perché tale operazione lascia il computer vulnerabile alle minacce.

Una volta definito il set di azioni da eseguire, fare click su **Avanti**.

Passaggio 4. Correzione delle impostazioni del browser Internet

La procedura guidata eseguirà le azioni selezionate durante il passaggio precedente. La configurazione del browser può richiedere alcuni minuti. Al termine, la procedura guidata passa automaticamente al passaggio successivo.

Passaggio 5. Termine della procedura guidata

Fare click sul pulsante **Fine** per chiudere la procedura guidata.

ROLLBACK DELLE MODIFICHE APPORTATE DALLE PROCEDURE GUIDATE

Alcune modifiche apportate durante l'esecuzione di Eliminazione guidata della cronologia delle attività (vedere la sezione "Eliminazione della cronologia delle attività" a pagina [100](#)), Correzione guidata delle impostazioni di Windows (vedere la sezione "Come procedere se si sospetta che il computer sia infetto" a pagina [45](#)) e Correzione guidata delle impostazioni del browser (vedere la sezione "Configurazione di un browser in modalità protetta" a pagina [101](#)) possono essere annullate eseguendone il rollback.

➡ *Per eseguire il rollback delle modifiche apportate dalle procedure guidate:*

1. Aprire la finestra principale dell'applicazione e selezionare la sezione **Strumenti** nella parte inferiore della finestra.
2. Nella parte destra della finestra fare click sul pulsante **Avvia** nella sezione con il nome della procedura guidata per cui si desidera eseguire il rollback delle modifiche:
 - **Eliminazione della cronologia delle attività** – per eseguire il rollback delle modifiche apportate da Eliminazione della cronologia delle attività;
 - **Risoluzione dei problemi di Microsoft Windows** – per eseguire il rollback delle modifiche apportate da Risoluzione dei problemi di Microsoft Windows;
 - **Correzione delle impostazioni del browser** – per eseguire il rollback delle modifiche apportate da Correzione guidata delle impostazioni del browser.

Di seguito sono illustrati i passaggi delle procedure guidate in caso di rollback delle modifiche.

Passaggio 1. Avvio della procedura guidata

Selezionare **Rollback delle modifiche**, quindi fare click sul pulsante **Avanti**.

Passaggio 2. Ricerca delle modifiche

La procedura guidata esegue una ricerca delle modifiche apportate in precedenza che è possibile annullare. Al termine della ricerca, la procedura guidata passerà automaticamente al passaggio successivo.

Passaggio 3. Selezione delle modifiche di cui eseguire il rollback

Al termine della ricerca, la procedura guidata segnala le modifiche rilevate.

Per eseguire il rollback di un'azione, selezionare la casella a sinistra del nome dell'azione.

Dopo avere selezionato le azioni di cui si desidera eseguire il rollback, fare click sul pulsante **Avanti**.

Passaggio 4. Rollback delle modifiche

La procedura guidata esegue il rollback delle azioni selezionate durante il passaggio precedente. Al termine del rollback, la procedura passa automaticamente al passaggio successivo.

Passaggio 5. Termine della procedura guidata

Fare click sul pulsante **Fine** per chiudere la procedura guidata.

RAPPORTI

Gli eventi che si verificano durante l'esecuzione dei componenti di protezione o delle attività di Kaspersky Anti-Virus vengono registrati nei rapporti.

IN QUESTA SEZIONE:

Creazione di un rapporto per il componente di protezione selezionato	103
Filtro dei dati.....	104
Ricerca di eventi.....	104
Salvataggio di un rapporto in un file	105
Archiviazione dei rapporti.....	105
Cancellazione dei rapporti dell'applicazione.....	106
Registrazione degli eventi non critici nel rapporto	106
Configurare la notifica della disponibilità dei rapporti	106

CREAZIONE DI UN RAPPORTO PER IL COMPONENTE DI PROTEZIONE SELEZIONATO

È possibile ottenere un rapporto dettagliato sugli eventi che si verificano durante l'esecuzione di qualsiasi componente di protezione di Kaspersky Anti-Virus o delle relative attività.

Per utilizzare al meglio i rapporti, è possibile modificare la modalità di visualizzazione dei dati: raggruppare gli eventi in base a vari parametri, selezionare il periodo del rapporto, ordinare gli eventi in base a una colonna o per importanza e nascondere colonne.

► *Per creare un rapporto relativo a un componente di protezione o un'attività:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare click sul collegamento **Rapporti**.
3. Nella finestra **Rapporti** visualizzata fare click sul pulsante **Rapporto dettagliato**.
4. Nella parte sinistra della finestra **Rapporto dettagliato** visualizzata selezionare il componente o l'attività per cui creare il rapporto. Selezionando **Centro protezione** viene creato un rapporto per tutti i componenti di protezione.

FILTRO DEI DATI

È possibile filtrare gli eventi nei rapporti di Kaspersky Anti-Virus in base a uno o più valori nelle colonne dei rapporti e definire condizioni complesse per il filtro dei dati.

► *Per filtrare gli elenchi in base ai valori:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare click sul collegamento **Rapporti**.
3. Nella finestra **Rapporti** visualizzata fare click sul pulsante **Rapporto dettagliato**.
4. Nella parte destra della finestra **Rapporto dettagliato** visualizzata spostare il puntatore del mouse nell'angolo superiore sinistro dell'intestazione della colonna e fare click per aprire il menu del filtro.
5. Selezionare il valore da utilizzare per filtrare i dati nel menu del filtro.
6. Ripetere la procedura per un'altra colonna, se necessario.

► *Per specificare una condizione complessa per il filtro:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Rapporti** nella parte superiore della finestra per aprire la finestra dei rapporti.
3. Nella finestra visualizzata, nella scheda **Rapporto**, fare click sul pulsante **Rapporto dettagliato**.
4. Nella parte destra della finestra **Rapporto dettagliato** visualizzata fare click con il pulsante destro del mouse sulla colonna del rapporto desiderata per aprire il menu di scelta rapida e selezionare **Personalizzato**.
5. Nella finestra **Filtro personalizzato** visualizzata impostare le condizioni per il filtro:
 - a. Definire i limiti della query nella parte destra della finestra.
 - b. Nella parte sinistra della finestra selezionare dall'elenco a discesa **Condizione** la condizione di query desiderata, ad esempio maggiore o minore, uguale o diverso dal valore specificato come limite della query.
 - c. Se necessario, aggiungere una seconda condizione utilizzando le operazioni di congiunzione logica (AND logico) e disgiunzione logica (OR logico). Se si desidera che la query dati soddisfi entrambe le condizioni specificate, selezionare **E**. Se è richiesta solo una delle due condizioni, selezionare **O**.

RICERCA DI EVENTI

È possibile eseguire una ricerca degli eventi desiderati nei rapporti specificando una parola chiave nella casella di ricerca o nella speciale finestra di ricerca.

► *Per eseguire una ricerca di un evento utilizzando la casella di ricerca:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare click sul collegamento **Rapporti**.
3. Nella finestra **Rapporti** visualizzata fare click sul pulsante **Rapporto dettagliato**.
4. Immettere la parola chiave nella casella di ricerca nella parte destra della finestra **Rapporto dettagliato** visualizzata.

► *Per eseguire una ricerca di un evento utilizzando la finestra di ricerca:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare click sul collegamento **Rapporti**.
3. Nella finestra **Rapporti** visualizzata fare click sul pulsante **Rapporto dettagliato**.

4. Nella parte destra della finestra **Rapporto dettagliato** visualizzata fare click con il pulsante destro del mouse sull'intestazione della colonna desiderata per aprire il menu di scelta rapida e selezionare **Cerca**.
5. Specificare i criteri di ricerca nella finestra **Cerca** visualizzata.
 - a. Nel campo **Stringa** immettere una parola chiave da cercare.
 - b. Selezionare nell'elenco a discesa **Colonna** il nome della colonna in cui cercare la parola chiave specificata.
 - c. Se necessario, selezionare le caselle per ulteriori impostazioni di ricerca.
6. Avviare la ricerca utilizzando uno dei seguenti metodi:
 - Per trovare un evento che soddisfa i criteri di ricerca specificati ed è successivo a quello evidenziato nell'elenco, fare click sul pulsante **Trova successivo**.
 - Per trovare tutti gli eventi che soddisfano i criteri di ricerca specificati, fare click sul pulsante **Evidenzia tutto**.

SALVATAGGIO DI UN RAPPORTO IN UN FILE

Il rapporto ottenuto può essere salvato in un file di testo.

➤ *Per salvare il rapporto in un file:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare click sul collegamento **Rapporti**.
3. Nella finestra **Rapporti** visualizzata fare click sul pulsante **Rapporto dettagliato**.
4. Nella finestra **Rapporto dettagliato** visualizzata creare il rapporto desiderato, quindi fare click sul collegamento **Salva** per selezionare il percorso in cui salvare il file.
5. Nella finestra visualizzata selezionare una cartella in cui salvare il file del rapporto e immettere il nome del file.

ARCHIVIAZIONE DEI RAPPORTI

Per impostazione predefinita, la durata massima per l'archiviazione dei rapporti è di 30 giorni. Al termine di questo periodo, i rapporti vengono eliminati. È possibile annullare il limite di tempo o modificare la durata massima per l'archiviazione dei rapporti.

È inoltre possibile definire la dimensione massima dei file dei rapporti. Per impostazione predefinita, la dimensione massima è di 1024 MB. Una volta raggiunta la dimensione massima, il contenuto del file viene sostituito con nuovi record. È possibile annullare i limiti impostati per la dimensione del rapporto o immettere un altro valore.

➤ *Per modificare la durata massima per l'archiviazione dei rapporti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Archiviazione dei rapporti**, selezionare la casella **Mantieni i rapporti per non più di** e specificare il periodo massimo di archiviazione dei rapporti.

➤ *Per configurare la dimensione massima dei file dei rapporti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Archiviazione dei rapporti**, selezionare la casella **Dimensione massima del file** e specificare la dimensione massima dei file dei rapporti.

CANCELLAZIONE DEI RAPPORTI DELL'APPLICAZIONE

È possibile cancellare i rapporti che contengono dati non più necessari.

➤ *Per cancellare il contenuto dei rapporti dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Rapporti e Backup**.
3. Nella parte destra della finestra, nella sezione **Eliminazione dei rapporti**, fare click sul pulsante **Cancella**.
4. Nella finestra **Eliminazione dei rapporti** visualizzata selezionare le caselle relative ai rapporti da cancellare.

REGISTRAZIONE DEGLI EVENTI NON CRITICI NEL RAPPORTO

Per impostazione predefinita, nei rapporti non vengono inclusi gli eventi non critici e gli eventi relativi al registro di sistema e al file system. È possibile aggiungere il record di tali eventi al rapporto.


➤ *Per aggiungere gli elementi non critici al rapporto:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare la sezione **Rapporti e Backup**.
3. Nella parte destra della finestra selezionare la casella **Registra gli eventi non critici**.

CONFIGURARE LA NOTIFICA DELLA DISPONIBILITÀ DEI RAPPORTI

È possibile creare una pianificazione in base alla quale Kaspersky Anti-Virus notificherà all'utente il completamento del rapporto.

➤ *Per configurare la notifica del completamento di un rapporto:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare click sul collegamento **Rapporti**.
3. Nella finestra **Rapporti** visualizzata fare click sul pulsante .
4. Nella finestra **Notifiche** visualizzata specificare le impostazioni della pianificazione.

ASPETTO DELL'APPLICAZIONE. GESTIONE DEGLI ELEMENTI ATTIVI DELL'INTERFACCIA

Kaspersky Anti-Virus consente di regolare le impostazioni per la visualizzazione del testo nella schermata di accesso di Microsoft Windows e degli elementi attivi dell'interfaccia (icona dell'applicazione nell'area di notifica, finestre di notifica e messaggi a comparsa).

IN QUESTA SEZIONE:

Trasparenza delle finestre di notifica.....	107
Animazione dell'icona dell'applicazione nell'area di notifica	107
Testo nella schermata di accesso di Microsoft Windows	107

TRASPARENZA DELLE FINESTRE DI NOTIFICA

► Per rendere semi-trasparenti le finestre di notifica:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Aspetto**.
3. Nella sezione **Icona nell'area di notifica della barra delle applicazioni** selezionare la casella **Abilita finestre semi-trasparenti**.

ANIMAZIONE DELL'ICONA DELL'APPLICAZIONE NELL'AREA DI NOTIFICA

L'animazione dell'icona dell'applicazione viene visualizzata nell'area di notifica durante l'esecuzione di un aggiornamento o una scansione.

Per impostazione predefinita, l'animazione dell'icona dell'applicazione nell'area di notifica è abilitata.

► Per disabilitare l'animazione dell'icona dell'applicazione:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Aspetto**.
3. Nella sezione **Icona nell'area di notifica della barra delle applicazioni** deselegionare la casella **Anima l'icona sulla barra delle applicazioni durante l'esecuzione delle attività**.

TESTO NELLA SCHERMATA DI ACCESSO DI MICROSOFT WINDOWS

Per impostazione predefinita, se Kaspersky Anti-Virus è abilitato e protegge il computer, viene visualizzato il testo "Protected by Kaspersky Lab" nella schermata di accesso durante il caricamento di Microsoft Windows.

Il testo "Protected by Kaspersky Lab" viene visualizzato solo in Microsoft Windows XP.

► Per abilitare la visualizzazione del testo durante il caricamento di Microsoft Windows:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Aspetto**.
3. Nella sezione **Icona nell'area di notifica della barra delle applicazioni** deselegionare la casella **Mostra "Protected by Kaspersky Lab" nella schermata di accesso a Microsoft Windows**.

NOTIFICHE

Per impostazione predefinita, viene notificato all'utente qualsiasi evento che si verifica durante l'esecuzione di Kaspersky Anti-Virus. Se è richiesta la selezione di un'azione da parte dell'utente, verrà visualizzata una finestra di notifica (vedere la sezione "Finestre di notifica e messaggi a comparsa" a pagina [30](#)). L'applicazione notifica gli eventi che non richiedono la selezione di un'azione con segnali acustici, messaggi e-mail e messaggi a comparsa nell'area di notifica della barra delle applicazioni (vedere la sezione "Finestre di notifica e messaggi a comparsa" a pagina [30](#)).

Kaspersky Anti-Virus comprende News Agent (vedere pagina [32](#)), utilizzato da Kaspersky Lab per notificare all'utente varie notizie. Se non si desidera ricevere notizie, è possibile disabilitarne l'invio.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione delle notifiche.....	108
Configurazione del metodo di notifica	108
Disabilitazione dell'invio delle notizie.....	109

ABILITAZIONE E DISABILITAZIONE DELLE NOTIFICHE

Per impostazione predefinita, in Kaspersky Anti-Virus vengono utilizzati vari metodi per segnalare all'utente tutti gli eventi importanti relativi all'esecuzione dell'applicazione (vedere la sezione "Configurazione del metodo di notifica" a pagina [108](#)). È possibile disabilitare l'invio di notifiche.

Indipendentemente dal fatto che l'invio di notifiche sia abilitato o disabilitato, le informazioni sugli eventi che si verificano durante l'esecuzione di Kaspersky Anti-Virus vengono registrate nel rapporto sul funzionamento dell'applicazione (vedere pagina [103](#)).

La disabilitazione dell'invio di notifiche non influisce sulla visualizzazione delle finestre di notifica. Per ridurre il numero di finestre di notifica visualizzate, utilizzare la modalità di protezione automatica (vedere la sezione "Selezione della modalità di protezione" a pagina [56](#)).

➤ *Per disabilitare l'invio di notifiche:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Notifiche**.
3. Nella parte destra della finestra deselezionare la casella **Attiva le notifiche degli eventi**.

CONFIGURAZIONE DEL METODO DI NOTIFICA

L'applicazione notifica gli eventi utilizzando i seguenti metodi:

- messaggi a comparsa nell'area di notifica della barra delle applicazioni;
- notifiche audio;
- messaggi di posta elettronica.

È possibile configurare un singolo set di metodi di notifica per ciascun tipo di eventi.

Per impostazione predefinita, le notifiche critiche e le notifiche di errori nel funzionamento dell'applicazione sono accompagnate da un segnale acustico. Viene utilizzata la combinazione di suoni Microsoft Windows come origine per gli effetti acustici. È possibile modificare la combinazione corrente o disabilitare i suoni.

Per consentire a Kaspersky Anti-Virus di inviare notifiche degli eventi tramite e-mail, è necessario regolare le impostazioni e-mail per l'invio di notifiche.

➤ *Per selezionare i metodi di notifica per i vari tipi di eventi:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Notifiche**.
3. Nella parte destra della finestra selezionare la casella **Attiva le notifiche degli eventi** e fare click sul pulsante **Impostazioni** sotto la casella.
4. Nella finestra **Notifiche** visualizzata selezionare le caselle relative ai metodi da utilizzare per le notifiche dei vari eventi: tramite e-mail, mediante messaggi a comparsa o con un segnale acustico.

➤ *Per modificare le impostazioni e-mail per l'invio di notifiche:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Notifiche**.
3. Nella parte destra della finestra selezionare la casella **Attiva le notifiche via e-mail** e fare click sul pulsante **Impostazioni**.
4. Nella finestra **Impostazioni delle notifiche via e-mail** visualizzata specificare le impostazioni per l'invio delle notifiche tramite e-mail.

➤ *Per configurare i suoni utilizzati per le notifiche:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Notifiche**.
3. Nella parte destra della finestra deselezionare la casella **Attiva le notifiche audio**.

Se si desidera utilizzare la combinazione di suoni di Microsoft Windows per le notifiche degli eventi di Kaspersky Anti-Virus, selezionare la casella **Usa i suoni standard di Microsoft Windows**. Se la casella è deselezionata, vengono utilizzati i suoni delle versioni precedenti di Kaspersky Anti-Virus.

DISABILITAZIONE DELL'INVIO DELLE NOTIZIE

➤ *Per disabilitare l'invio delle notizie dalla finestra delle impostazioni dell'applicazione:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Aspetto**.
3. Nella parte destra della finestra deselezionare la casella **Attiva le notifiche delle notizie**.

KASPERSKY SECURITY NETWORK

Per aumentare l'efficienza della protezione del computer, Kaspersky Anti-Virus utilizza dati raccolti da utenti di tutto il mondo. La raccolta di questi dati viene eseguita tramite Kaspersky Security Network.

Kaspersky Security Network (KSN) è un'infrastruttura di servizi online che consente di accedere alla Knowledge Base di Kaspersky Lab, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati di Kaspersky Security Network assicura una risposta più rapida da parte di Kaspersky Anti-Virus quando vengono rilevati nuovi tipi di minacce, migliora le prestazioni di alcuni componenti di protezione e riduce il rischio di falsi positivi.

La partecipazione degli utenti a Kaspersky Security Network consente a Kaspersky Lab di raccogliere informazioni in tempo reale sui tipi e le fonti delle nuove minacce, sviluppare metodi per neutralizzarle e ridurre il numero dei falsi positivi.

La partecipazione a Kaspersky Security Network consente inoltre di ricevere informazioni sulla reputazione di varie applicazioni e siti Web.

Quando si partecipa a Kaspersky Security Network, determinate statistiche raccolte durante l'esecuzione di Kaspersky Anti-Virus vengono inviate automaticamente a Kaspersky Lab.

Non vengono raccolti, elaborati o memorizzati dati riservati.

La partecipazione al programma Kaspersky Security Network è facoltativa. È possibile scegliere se partecipare durante l'installazione di Kaspersky Anti-Virus, ma l'impostazione può essere modificata successivamente.

IN QUESTA SEZIONE:

Abilitazione e disabilitazione della partecipazione a Kaspersky Security Network	109
Verifica della connessione a Kaspersky Security Network	110

ABILITAZIONE E DISABILITAZIONE DELLA PARTECIPAZIONE A KASPERSKY SECURITY NETWORK

➤ *Per partecipare a Kaspersky Security Network:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, nella sezione **Impostazioni avanzate**, selezionare il componente **Feedback**.
3. Nella parte destra della finestra selezionare la casella **Accetto di partecipare al programma Kaspersky Security Network**.

VERIFICA DELLA CONNESSIONE A KASPERSKY SECURITY NETWORK

La connessione a Kaspersky Security Network potrebbe interrompersi per uno dei seguenti motivi:

- il computer non è connesso a Internet;
- si è scelto di non partecipare a Kaspersky Security Network;
- la licenza in uso per Kaspersky Anti-Virus è limitata.

➡ *Per verificare la connessione a Kaspersky Security Network:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte superiore della finestra fare click sul pulsante **Protezione Cloud**.
3. Nella parte sinistra della finestra visualizzata viene indicato lo stato di connessione a Kaspersky Security Network.

TESTING DEL FUNZIONAMENTO DELL'APPLICAZIONE

In questa sezione vengono fornite informazioni su come verificare che l'applicazione rilevi i virus e le relative varianti ed esegua le azioni corrette in caso di rilevamento.

IN QUESTA SEZIONE:

Informazioni sul file di prova EICAR	111
Testing dell'applicazione tramite il file di prova EICAR.....	111
Informazioni sui tipi di file di prova EICAR.....	112

INFORMAZIONI SUL FILE DI PROVA EICAR

È possibile verificare che l'applicazione rilevi i virus e disinfetti i file infetti utilizzando un *file di prova EICAR*. Il file di prova EICAR è stato sviluppato da European Institute for Computer Antivirus Research (EICAR) allo scopo di testare le funzionalità delle applicazioni anti-virus.

Il file di prova EICAR non è un virus. Il file di prova EICAR non contiene alcun codice di programma che può danneggiare il computer. Tuttavia, la maggior parte delle applicazioni anti-virus identifica il file di prova EICAR come un virus.

Il file di prova EICAR non è progettato per testare le funzionalità dell'analizzatore euristico o della ricerca del malware a livello di sistema (rootkit).

Non utilizzare virus reali per testare le funzionalità delle applicazioni anti-virus. Questa operazione può danneggiare il computer.

Non dimenticare di abilitare nuovamente la protezione anti-virus del traffico Internet e dei file al termine del test con il file di prova EICAR.

TESTING DELL'APPLICAZIONE TRAMITE IL FILE DI PROVA EICAR

È possibile utilizzare il file di prova EICAR per testare la protezione del traffico Internet, la protezione anti-virus dei file e la funzionalità di scansione dei computer.

Non dimenticare di abilitare nuovamente la protezione anti-virus del traffico Internet e dei file al termine del test con il file di prova EICAR.

◆ *Per testare la protezione del traffico Internet utilizzando il file di prova EICAR:*

1. È possibile scaricare il file di prova dal sito Web ufficiale di EICAR all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.
2. Tentare di salvare il file di prova EICAR in una cartella nel computer.
Kaspersky Anti-Virus segnalerà che è stata rilevata una minaccia nella URL richiesta e bloccherà il tentativo di salvare l'oggetto nel computer.
3. Se necessario, è possibile utilizzare diversi tipi di file di prova EICAR (vedere la sezione "Informazioni sui tipi di file di prova EICAR" a pagina [112](#)).

➤ *Per testare la protezione anti-virus dei file utilizzando il file di prova EICAR o una sua variante:*

1. Sospendere la protezione anti-virus del traffico Internet e la protezione anti-virus dei file nel computer.
Quando la protezione viene sospesa, non è consigliabile connettere il computer a reti locali o utilizzare dispositivi rimovibili, per evitare eventuali danni al computer causati dal malware.
2. È possibile scaricare il file di prova dal sito Web ufficiale di EICAR all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.
3. Salvare il file di prova EICAR in una cartella nel computer.
4. Aggiungere uno dei prefissi all'intestazione del file di prova EICAR (vedere la sezione "Informazioni sui tipi di file di prova EICAR" a pagina [112](#)).
A tale scopo, è possibile utilizzare qualsiasi editor di testo o di ipertesti, come ad esempio Blocco note. Per aprire Blocco note, selezionare **Start** → **Tutti i programmi** → **Accessori** → **Blocco note**.
5. Salvare il file risultante con un nome che descriva la variante del file EICAR; ad esempio, aggiungere il prefisso DELE- e salvare il file come eicar_dele.com.
6. Riprendere la protezione anti-virus del traffico Internet e la protezione anti-virus dei file nel computer.
7. Tentare di eseguire il file salvato.
Kaspersky Anti-Virus segnala che è stata rilevata una minaccia sul disco rigido del computer ed esegue l'azione specificata nelle impostazioni della protezione anti-virus dei file.

➤ *Per testare la funzionalità di scansione virus utilizzando il file di prova EICAR o una sua variante:*

1. Sospendere la protezione anti-virus del traffico Internet e la protezione anti-virus dei file nel computer.
Quando la protezione viene sospesa, non è consigliabile connettere il computer a reti locali o utilizzare dispositivi rimovibili, per evitare eventuali danni al computer causati dal malware.
2. È possibile scaricare il file di prova dal sito Web ufficiale di EICAR all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.
3. Aggiungere uno dei prefissi all'intestazione del virus di prova eicar (vedere la sezione "Tipi e varianti del virus di prova eicar" a pagina [112](#)).
A tale scopo, è possibile utilizzare qualsiasi editor di testo o di ipertesti, come ad esempio Blocco note. Per aprire Blocco note, selezionare **Start** → **Tutti i programmi** → **Accessori** → **Blocco note**.
4. Salvare il file risultante con un nome che descriva la variante del file di prova EICAR; ad esempio, aggiungere il prefisso DELE- e salvare il file come eicar_dele.com.
5. Avviare la scansione del file salvato.
Kaspersky Anti-Virus segnala che è stata rilevata una minaccia sul disco rigido del computer ed esegue l'azione specificata nelle impostazioni della scansione virus.
6. Riprendere la protezione anti-virus del traffico Internet e la protezione anti-virus dei file nel computer.

INFORMAZIONI SUI TIPI DI FILE DI PROVA EICAR

È possibile testare il funzionamento dell'applicazione creando diverse varianti del file di prova EICAR. L'applicazione rileva il file di prova EICAR (o una sua variante) e gli assegna uno stato a seconda del risultato la scansione. L'applicazione esegue le azioni specificate sul file di prova EICAR se sono state selezionate nell'impostazione del componente che ha rilevato il file di prova EICAR.

La prima colonna della tabella (vedere la tabella seguente) contiene i prefissi che è possibile utilizzare durante la creazione delle varianti del file di prova EICAR. La seconda colonna elenca tutti i possibili stati assegnati al file in base ai risultati della scansione dell'applicazione. La terza colonna indica come vengono elaborati i file che presentano lo stato specificato.

Tabella 2. Varianti del file di prova EICAR

Prefisso	Stato del file	Informazioni sull'elaborazione del file
Nessun prefisso, virus di prova standard.	Infetto. Il file contiene il codice di un virus noto. Il file non può essere disinfettato.	L'applicazione identifica il file come contenente un virus che non può essere disinfettato. L'azione impostata per i file infetti viene applicata al file. Per impostazione predefinita, l'applicazione visualizza una notifica che segnala che non è possibile disinfettare il file.
CURE-	Infetto. Il file contiene il codice di un virus noto. Il file può essere disinfettato.	Il file contiene un virus che può essere disinfettato o eliminato. L'applicazione disinfetta il file; il testo del corpo del "virus" viene sostituito dalla parola CURE. L'applicazione visualizza una notifica che segnala che è stato rilevato un file disinfettato.
DELE-	Infetto. Il file contiene il codice di un virus noto. Il file non può essere disinfettato.	L'applicazione identifica il file come un virus che non può essere disinfettato e lo elimina. L'applicazione visualizza una notifica che segnala che il file disinfettato è stato eliminato.
WARN-	Potenzialmente infetto. Il file contiene il codice di un virus sconosciuto. Il file non può essere disinfettato.	Il file è potenzialmente infetto. L'applicazione applica l'azione impostata per i file potenzialmente infetti. Per impostazione predefinita, l'applicazione visualizza una notifica che segnala che è stato rilevato un file potenzialmente infetto.
SUSP-	Potenzialmente infetto. Il file contiene il codice modificato di un virus noto. Il file non può essere disinfettato.	L'applicazione ha rilevato una corrispondenza parziale tra una sezione di codice del file e una sezione di codice di un virus noto. Quando viene rilevato un file potenzialmente infetto, i database dell'applicazione non contengono una descrizione dell'intero codice del virus. L'applicazione applica l'azione impostata per i file potenzialmente infetti. Per impostazione predefinita, l'applicazione visualizza una notifica che segnala che è stato rilevato un file potenzialmente infetto.
CORR-	Danneggiato.	L'applicazione non esegue la scansione di questo tipo di file perché la sua struttura è danneggiata (ad esempio, il formato di file non è valido). Informazioni sull'elaborazione del file sono disponibili nel rapporto sul funzionamento dell'applicazione.
ERRO-	Errore di scansione.	Si è verificato un errore durante la scansione di un file. L'applicazione non ha potuto eseguire l'accesso al file, in quanto l'integrità del file è stata compromessa, ad esempio a causa di un archivio in più volumi, o non è stata stabilita una connessione al file, ad esempio se il file viene esaminato in un'unità di rete. Informazioni sull'elaborazione del file sono disponibili nel rapporto sul funzionamento dell'applicazione.

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

In questa sezione sono disponibili informazioni sulle modalità con cui è possibile ottenere assistenza tecnica e sulle condizioni da soddisfare per ricevere supporto dal Servizio di Assistenza tecnica.

IN QUESTA SEZIONE:

Come ottenere assistenza tecnica	114
Utilizzo del file di traccia e dello script AVZ	114
Assistenza tecnica telefonica	116
Come ottenere assistenza tecnica tramite la Pagina personale	116

COME OTTENERE ASSISTENZA TECNICA

Se non è possibile trovare una soluzione per il proprio problema nella documentazione dell'applicazione o in una delle fonti di informazioni sull'applicazione (vedere la sezione "Fonti di informazioni sull'applicazione" a pagina [11](#)), è consigliabile contattare il Servizio di Assistenza tecnica di Kaspersky Lab. Gli specialisti del Servizio di Assistenza tecnica rispondono a qualunque quesito in merito all'installazione e all'utilizzo dell'applicazione. Se il computer è infetto, gli specialisti forniranno assistenza per la risoluzione di qualsiasi problema causato dal malware.

Prima di contattare il Servizio di Assistenza tecnica, consultare le regole dell'assistenza (<http://support.kaspersky.com/it/support/rules>).

È possibile contattare il Servizio di Assistenza tecnica in uno dei modi seguenti:

- Telefonicamente. Questo metodo consente di consultare gli specialisti del Servizio di Assistenza tecnica in lingua russa o internazionale.
- Inviando una richiesta dalla propria Pagina personale sul sito Web del Servizio di Assistenza tecnica. Questo metodo consente di contattare gli specialisti utilizzando il modulo di richiesta.

Per ottenere assistenza tecnica, è necessario essere un utente registrato di una versione commerciale di Kaspersky Anti-Virus. L'assistenza tecnica non è disponibile per gli utenti di versioni di prova dell'applicazione.

UTILIZZO DEL FILE DI TRACCIA E DELLO SCRIPT AVZ

Quando si notifica un problema agli specialisti del Servizio di Assistenza tecnica, questi possono richiedere di creare un rapporto con informazioni sul sistema operativo in uso e di inviarlo al Servizio di Assistenza tecnica. Gli specialisti del Servizio di Assistenza tecnica possono inoltre richiedere di creare un *file di traccia*. Il file di traccia consente di monitorare passo per passo il processo di esecuzione dei comandi dell'applicazione e di identificare in quale fase dell'esecuzione dell'applicazione si è verificato un errore.

Una volta analizzati i dati inviati, gli specialisti del Servizio di Assistenza tecnica creano uno script AVZ e lo inviano all'utente. L'esecuzione degli script AVZ consente di analizzare i processi attivi alla ricerca di codice dannoso, eseguire una ricerca del codice dannoso nel sistema, disinfettare o eliminare i file infetti e creare rapporti sui risultati della scansione del sistema.

CREAZIONE DI UN RAPPORTO SULLO STATO DEL SISTEMA

► *Per creare un rapporto sullo stato del sistema:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Assistenza** nella parte superiore della finestra principale per aprire la finestra **Assistenza**, quindi fare click sul collegamento **Strumenti di assistenza**.
3. Nella finestra **Strumenti di assistenza** visualizzata fare click sul pulsante **Crea un rapporto sullo stato del sistema**.

Il rapporto sullo stato del sistema viene creato in formato html e xml e salvato nell'archivio sysinfo.zip. Al termine della raccolta delle informazioni, è possibile visualizzare il rapporto.

► *Per visualizzare il rapporto:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Assistenza** nella parte superiore della finestra principale per aprire la finestra **Assistenza**, quindi fare click sul collegamento **Strumenti di assistenza**.
3. Nella finestra **Strumenti di assistenza** visualizzata fare click sul pulsante **Visualizza**.
4. Aprire l'archivio sysinfo.zip contenente i file del rapporto.

CREAZIONE DI UN FILE DI TRACCIA

► *Per creare il file di traccia:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Assistenza** nella parte superiore della finestra principale per aprire la finestra **Assistenza**, quindi fare click sul collegamento **Strumenti di assistenza**.
3. Nella finestra **Strumenti di assistenza** visualizzata specificare il livello di traccia dall'elenco a discesa nella sezione **Tracce**.
È opportuno richiedere il livello di traccia necessario a uno specialista del Servizio di Assistenza tecnica. In assenza di indicazioni da parte del Servizio di Assistenza tecnica, è consigliabile utilizzare il livello di traccia **500**.
4. Per avviare il processo di creazione di una traccia, fare click sul pulsante **Attiva**.
5. Ricostruire la situazione in cui si è verificato il problema.
6. Per arrestare il processo di creazione della traccia, fare click sul pulsante **Disattiva**.

È quindi possibile passare al caricamento dei risultati della traccia (vedere la sezione "Invio dei file di dati" a pagina [115](#)) sul server di Kaspersky Lab.

INVIO DEI FILE DI DATI

Dopo aver creato i file di traccia e il rapporto sullo stato del sistema, sarà necessario inviarli agli esperti del Servizio di Assistenza tecnica di Kaspersky Lab.

Per caricare i file di dati sul server del Servizio di Assistenza tecnica, sarà necessario fornire un numero di richiesta. Tale numero è disponibile nella Pagina personale del sito Web del Servizio di Assistenza tecnica, se la richiesta è attiva.

► *Per caricare i file di dati sul server del Servizio di Assistenza tecnica:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Assistenza** nella parte superiore della finestra principale per aprire la finestra **Assistenza**, quindi fare click sul collegamento **Strumenti di assistenza**.
3. Nella finestra **Strumenti di assistenza** visualizzata, nella sezione **Azioni**, fare click sul pulsante **Invia informazioni sul sistema al servizio di Assistenza**.
Verrà visualizzata la finestra **Caricamento in corso delle informazioni per il Servizio di Assistenza tecnica**.
4. Selezionare le caselle accanto ai file di traccia da inviare al Servizio di Assistenza tecnica, quindi fare click sul pulsante **Invia**.
Verrà visualizzata la finestra **Numero di richiesta**.
5. Specificare il numero assegnato alla richiesta contattando il Servizio di Assistenza tecnica tramite la Pagina personale, quindi fare click sul pulsante **OK**.

I dati selezionati verranno compressi e inviati al server del Servizio di Assistenza tecnica.

Se per qualsiasi motivo risultasse impossibile contattare il Servizio di Assistenza tecnica, i file di dati possono essere memorizzati nel computer e inviati in seguito dalla Pagina personale.

► *Per salvare i file di dati su disco:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Assistenza** nella parte superiore della finestra principale per aprire la finestra **Assistenza**, quindi fare click sul collegamento **Strumenti di assistenza**.
3. Nella finestra **Strumenti di assistenza** visualizzata, nella sezione **Azioni**, fare click sul pulsante **Invia informazioni sul sistema al servizio di Assistenza**.

Verrà visualizzata la finestra **Caricamento in corso delle informazioni per il Servizio di Assistenza tecnica**.

4. Selezionare le caselle accanto ai file di traccia da inviare al Servizio di Assistenza tecnica, quindi fare click sul pulsante **Invia**.

Verrà visualizzata la finestra **Numero di richiesta**.

5. Fare click sul pulsante **Annulla** e confermare il salvataggio dei file su disco facendo click sul pulsante **Sì** nella finestra visualizzata.

Verrà visualizzata la finestra per il salvataggio dell'archivio.

6. Specificare il nome dell'archivio e confermare il salvataggio.

L'archivio creato verrà inviato al Servizio di Assistenza tecnica dalla Pagina personale.

ESECUZIONE DI UNO SCRIPT CON AVZ

Non è consigliabile modificare il testo dello script AVZ ricevuto dagli esperti di Kaspersky Lab. Se si verificano problemi durante l'esecuzione dello script, contattare il Servizio di Assistenza tecnica (vedere la sezione "Come ottenere assistenza tecnica" a pagina 114).

► *Per eseguire lo script AVZ:*

1. Aprire la finestra principale dell'applicazione.
2. Fare click sul collegamento **Assistenza** nella parte superiore della finestra principale per aprire la finestra **Assistenza**, quindi fare click sul collegamento **Strumenti di assistenza**.
3. Nella finestra **Strumenti di assistenza** visualizzata fare click sul pulsante **Esegui uno script con AVZ**.

Se lo script viene eseguito correttamente, la procedura guidata si chiude. Se si verifica un errore durante l'esecuzione, viene visualizzato un messaggio di errore.

ASSISTENZA TECNICA TELEFONICA

In caso di problemi urgenti, è possibile contattare gli specialisti del Servizio di Assistenza tecnica in lingua russa o internazionale (http://support.kaspersky.com/support/support_local).

Prima di contattare il Servizio di Assistenza tecnica, è necessario raccogliere informazioni (<http://support.kaspersky.com/it/support/details>) sul computer in uso e sulle applicazioni anti-virus installate. Ciò consentirà agli esperti di fornire assistenza più rapidamente.

COME OTTENERE ASSISTENZA TECNICA TRAMITE LA PAGINA PERSONALE

La *Pagina personale* è la sezione personale (<https://my.kaspersky.com/it>) dell'utente nel sito Web del Servizio di Assistenza tecnica.

Per ottenere l'accesso alla Pagina personale, è necessario eseguire la procedura di registrazione nella pagina di registrazione (<https://my.kaspersky.com/it/registration>). Immettere il proprio indirizzo di posta elettronica e una password per l'accesso alla Pagina personale.

Utilizzando la Pagina personale è possibile:

- contattare il Servizio di Assistenza tecnica e Virus Lab;
- contattare il Servizio di Assistenza tecnica senza utilizzare la posta elettronica;
- tenere traccia dello stato delle proprie richieste in tempo reale;
- visualizzare una cronologia dettagliata delle proprie richieste al Servizio di Assistenza tecnica;

Assistenza tecnica tramite e-mail

È possibile inviare una richiesta online al Servizio di Assistenza tecnica in russo, inglese, tedesco, francese, italiano o spagnolo.

Nei campi del modulo di richiesta online è necessario specificare i seguenti dati:

- tipo di richiesta;
- nome e numero di versione dell'applicazione;
- descrizione della richiesta;
- ID cliente e password;
- indirizzo e-mail.

Uno specialista del Servizio di Assistenza tecnica invierà una risposta alla domanda nella Pagina personale dell'utente e all'indirizzo e-mail è specificato nella richiesta online.

Richieste online al Virus Lab

Alcune richieste devono essere inviate al Virus Lab invece che al Servizio di Assistenza tecnica.

È possibile inviare i seguenti tipi di richieste a Virus Lab:

- *Programma dannoso sconosciuto* – si sospetta che un file contenga un virus, ma Kaspersky Anti-Virus non lo identifica come infetto.
Gli specialisti del Virus Lab analizzeranno il codice dannoso inviato. Se rilevano un virus precedentemente sconosciuto, aggiungono al database la descrizione corrispondente, che diventa disponibile durante l'aggiornamento delle applicazioni anti-virus.
- *Falso allarme* – Kaspersky Anti-Virus classifica un file come virus, ma si è certi che non si tratta di un virus.
- *Richiesta della descrizione di un programma dannoso* – si desidera ricevere la descrizione di un virus rilevato da Kaspersky Anti-Virus utilizzando il nome del virus.

È inoltre possibile inviare richieste al Virus Lab dalla pagina del modulo di richiesta (<http://support.kaspersky.com/virlab/helpdesk.html?LANG=it>) senza essere registrati nella Pagina personale. In questa pagina non è necessario specificare il codice di attivazione dell'applicazione.

APPENDICE

In questa sezione vengono fornite informazioni che completano il testo della documentazione.

IN QUESTA SEZIONE:

Utilizzo dell'applicazione dalla riga di comando	118
Elenco delle notifiche di Kaspersky Anti-Virus	127

UTILIZZO DELL'APPLICAZIONE DALLA RIGA DI COMANDO

Kaspersky Anti-Virus può essere utilizzato anche dalla riga di comando. In tal caso, è possibile eseguire le operazioni seguenti:

- attivazione dell'applicazione;
- avvio e arresto dell'applicazione;
- avvio e arresto dei componenti dell'applicazione;
- avvio e arresto di attività;
- acquisizione di informazioni sullo stato corrente dei componenti e sulle relative attività e statistiche;
- avvio e arresto di attività di scansione virus;
- scansione di oggetti selezionati;
- aggiornamento dei database e dei moduli del software, rollback degli aggiornamenti;
- esportazione ed importazione di impostazioni di protezione;
- apertura dei file della Guida utilizzando la sintassi della riga di comando in generale e per singoli comandi.

Sintassi del prompt dei comandi:

```
avp.com <comando> [opzioni]
```

È necessario accedere all'applicazione dalla riga di comando dalla cartella di installazione del programma o specificando il percorso completo di avp.com

Nella tabella che segue sono elencati i comandi utilizzati per controllare l'applicazione e i relativi componenti.

START	Avvia un componente o un'attività.
STOP	Arresta 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	Visualizza lo stato corrente di un componente o un'attività.
STATISTICS	Visualizza le statistiche di un componente o un'attività.
HELP	Visualizza l'elenco dei comandi e informazioni sulla sintassi dei comandi.
SCAN	Esegue la scansione virus degli oggetti.
UPDATE	Avvia 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 di Kaspersky Anti-Virus.

EXIT	Chiude l'applicazione. Il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione.
IMPORT	Importa le impostazioni di protezione dell'applicazione. Il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia di Kaspersky Anti-Virus.
EXPORT	Esporta le impostazioni di protezione dell'applicazione.

Ogni comando richiede un insieme specifico di impostazioni.

IN QUESTA SEZIONE:

Attivazione dell'applicazione	119
Avvio dell'applicazione	119
Arresto dell'applicazione	119
Gestione dei componenti e delle attività dell'applicazione.....	120
Scansione virus.....	121
Aggiornamento dell'applicazione.....	123
Rollback dell'ultimo aggiornamento.....	124
Esportazione delle impostazioni di protezione	124
Importazione delle impostazioni di protezione.....	125
Creazione di un file di traccia	125
Visualizzazione della Guida	126
Codici restituiti della riga di comando	126

ATTIVAZIONE DELL'APPLICAZIONE

È possibile attivare Kaspersky Anti-Virus utilizzando un file chiave.

Sintassi del comando:

```
avp.com ADDKEY <nomefile>
```

Nella tabella seguente sono descritte le impostazioni per l'esecuzione dei comandi.

<nomefile>	Nome del file di chiave dell'applicazione, con estensione *.key.
-------------------------	--

Esempio:

```
avp.com ADDKEY 1AA111A1.key
```

AVVIO DELL'APPLICAZIONE

Sintassi del comando:

```
avp.com
```

ARRESTO DELL'APPLICAZIONE

Sintassi del comando:

```
avp.com EXIT /password=<password>
```

Una descrizione dei parametri è disponibile nella tabella seguente.

<password>	Password dell'applicazione specificata nell'interfaccia.
-------------------------	--

Questo comando non viene accettato senza l'immissione di una password.

GESTIONE DEI COMPONENTI E DELLE ATTIVITÀ DELL'APPLICAZIONE

Sintassi del comando:

```
avp.com <comando> <profilo|nome_attività> [/R[A]:<file_rapporti>]
avp.com STOP <profilo|nome_attività> /password=<password> [/R[A]:<file_rapporti>]
```

Nella tabella seguente sono elencate le descrizioni di comandi e impostazioni.

<comando>	<p>È possibile gestire i componenti e le attività di Kaspersky Anti-Virus dalla riga di comando con i comandi seguenti:</p> <p>START: avvia un'attività o un componente di protezione.</p> <p>STOP: arresta un'attività o un componente di protezione.</p> <p>STATUS: visualizza lo stato corrente di un'attività o di un componente di protezione.</p> <p>STATISTICS: visualizza le statistiche relative a un'attività o a un componente di protezione.</p> <p>Il comando STOP non verrà accettato senza l'immissione di una password.</p>
<profilo nome_attività>	<p>Come valore di <profilo> è possibile specificare qualsiasi componente di protezione di Kaspersky Anti-Virus, modulo di componente, attività di scansione o di aggiornamento su richiesta (i valori standard utilizzati nell'applicazione sono visualizzati nella tabella che segue).</p> <p>Come valore di <nome_attività> è possibile specificare il nome di qualsiasi attività di scansione o di aggiornamento su richiesta.</p>
<password>	<p>Password dell'applicazione specificata nell'interfaccia.</p>
/R[A]:<file_rapporti>	<p>/R:<file_rapporti>: registra solo gli eventi importanti nel rapporto.</p> <p>/RA:<file_rapporti>: registra tutti gli eventi nel rapporto.</p> <p>È possibile indicare un percorso assoluto o relativo. Se l'impostazione non è definita, vengono visualizzati i risultati della scansione e tutti gli eventi.</p>

Nell'impostazione **<profilo>** è necessario specificare uno dei valori disponibili nella tabella seguente.

RTP	<p>Tutti i componenti di protezione.</p> <p>Il comando avp.com START RTP esegue tutti i componenti di protezione se la protezione è stata completamente disabilitata.</p> <p>Se il componente è stato disabilitato tramite il comando STOP dalla riga di comando, non verrà avviato dal comando avp.com START RTP. Per avviarlo, è necessario eseguire il comando avp.com START <profilo> immettendo per <profilo> il nome del componente di protezione specifico, ad esempio avp.com START FM.</p>
pdm	<p>Difesa Proattiva.</p>
FM	<p>Anti-Virus File.</p>
EM	<p>Anti-Virus Posta.</p>

WM	Anti-Virus Web. Valori per i componenti secondari di Anti-Virus Web: httpscan (HTTP) : esamina il traffico HTTP; sc : esamina gli script.
IM	Anti-Virus IM.
Updater	Aggiornamento.
Rollback	Rollback dell'ultimo aggiornamento.
Scan_My_Computer	Scansione.
Scan_Objects	Scansione Personalizzata.
Scan_Quarantine	Scansione della quarantena.
Scan_Startup (STARTUP)	Scansione Personalizzata all'avvio.
Scan_Vulnerabilities (SECURITY)	Scansione Vulnerabilità.

I componenti e le attività avviati dalla riga di comando vengono eseguiti con le impostazioni configurate nell'interfaccia dell'applicazione.

Esempi:

➤ Per abilitare Anti-Virus File, immettere il comando seguente:

```
avp.com START FM
```

➤ Per arrestare una scansione del computer, immettere il comando seguente:

```
avp.com STOP Scan_My_Computer /password=<password>
```

SCANSIONE VIRUS

L'avvio della scansione virus di una determinata area e l'elaborazione degli oggetti dannosi dalla riga di comando generalmente presentano la sintassi seguente:

```
avp.com SCAN [<oggetto esaminato>] [<azione>] [<tipi di file>] [<esclusioni>] [<file di configurazione>] [<impostazioni rapporti>] [<impostazioni avanzate>]
```

Per esaminare gli oggetti, è inoltre possibile utilizzare le attività create nell'applicazione avviando quella desiderata dalla riga di comando. L'attività viene eseguita con le impostazioni specificate nell'interfaccia di Kaspersky Anti-Virus.

Una descrizione dei parametri è disponibile nella tabella seguente.

<oggetto esaminato> : questo parametro fornisce l'elenco di oggetti che vengono esaminati per rilevare eventuale codice dannoso. Può includere diversi valori dell'elenco fornito separati da spazi.	
<file>	Elenco di percorsi dei file e delle cartelle da esaminare. È possibile indicare un percorso assoluto o relativo. Gli elementi dell'elenco devono essere separati da uno spazio. Commenti: <ul style="list-style-type: none"> • se contiene uno spazio, il nome dell'oggetto deve essere incluso tra virgolette; • se viene fatto riferimento a una cartella specifica, verranno esaminati tutti i file in essa contenuti.
/MEMORY	Oggetti RAM.

/STARTUP	Oggetti di avvio.
/MAIL	Caselle di posta.
/REMDRIVES	Tutte le unità rimovibili.
/FIXDRIVES	Tutte le unità interne.
/NETDRIVES	Tutte le unità di rete.
/QUARANTINE	Oggetti in quarantena.
/ALL	Scansione Completa del computer.
/@:<filelist.lst>	<p>Percorso di un file contenente un elenco di oggetti e cataloghi da esaminare. È possibile indicare un percorso assoluto o relativo. Il percorso deve essere specificato senza virgolette anche se contiene spazi.</p> <p>Il file contenente l'elenco di oggetti deve essere in un formato di testo. Ogni oggetto da esaminare deve essere elencato in una riga distinta.</p> <p>È consigliabile specificare percorsi assoluti per gli oggetti da esaminare. Quando si specifica un percorso relativo, questo deve essere specificato relativamente al file eseguibile di un'applicazione, non relativamente al file con l'elenco degli oggetti da esaminare.</p>
<p><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.</p> <p>Se si lavora in modalità automatica, Kaspersky Anti-Virus applica automaticamente l'azione consigliata dagli specialisti di Kaspersky Lab quando vengono rilevati oggetti pericolosi. Le azioni corrispondenti al valore del parametro <azione> vengono ignorate.</p>	
/i0	Nessuna azione sull'oggetto; registrazione delle informazioni nel rapporto.
/i1	Vengono disinfettati gli oggetti infetti; se la disinfezione non riesce, vengono ignorati.
/i2	Vengono disinfettati gli oggetti infetti; se la disinfezione non riesce, vengono ignorati; non vengono eliminati gli oggetti infetti dagli oggetti compositi; vengono eliminati gli oggetti compositi infetti con intestazioni eseguibili (archivi sfx).
/i3	Vengono disinfettati gli oggetti infetti; se la disinfezione non riesce, vengono ignorati; vengono eliminati completamente tutti gli oggetti compositi se è impossibile eliminare i file incorporati infetti.
/i4	Vengono eliminati gli oggetti infetti. Vengono eliminati tutti gli oggetti compositi 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.
<p><tipi di file>: questo parametro definisce i tipi di file che sono sottoposti a scansione virus. Per impostazione predefinita, questo parametro non è specificato e sono sottoposti a scansione solo i file infettabili in base al contenuto.</p>	
/fe	Vengono esaminati solo i file infettabili in base all'estensione.
/fi	Vengono esaminati solo i file infettabili in base al contenuto.
/fa	Vengono esaminati tutti i file.
<p><esclusioni>: questo parametro definisce gli oggetti esclusi dalla scansione. Può includere diversi valori dell'elenco fornito separati da spazi.</p>	
-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:<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 nell'impostazione <dimensione> . Questa impostazione disponibile solo per i file compositi, come ad esempio gli archivi.
<file di configurazione> : definisce il percorso del file di configurazione che contiene le impostazioni di scansione dell'applicazione. Il file di configurazione è in formato testo e contiene l'insieme di parametri della riga di comando per la scansione virus. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia dell'applicazione.	
/C:<nome_file>	Vengono utilizzati i valori delle impostazioni specificati nel file di configurazione <nome_file> .
<impostazioni rapporti> : questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se l'impostazione non è definita, vengono visualizzati i risultati della scansione e tutti gli eventi.	
/R:<file_rapporti>	In questo file vengono registrati solo gli eventi importanti.
/RA:<file_rapporti>	In questo file vengono registrati tutti gli eventi.
<impostazioni avanzate> : impostazioni che definiscono l'utilizzo delle tecnologie di scansione virus.	
/iChecker=<on off>	Viene abilitato/disabilitato l'utilizzo della tecnologia iChecker.
/iSwift=<on off>	Viene abilitato/disabilitato l'utilizzo della tecnologia iSwift.

Esempi:

- ▶ *Avvio di una scansione di memoria, programmi a esecuzione automatica, caselle di posta, directory Documenti e Programmi e file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" "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_settings.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_aggiornamenti>] [/R[A]:<file_rapporti>] [/C:<nome_file>]
```

Una descrizione dei parametri è disponibile nella tabella seguente.

<sorgente_aggiornamenti>	Server HTTP o FTP o cartella di rete per il download degli aggiornamenti. Il valore del parametro può essere nel formato di un percorso completo di una sorgente degli aggiornamenti o un'URL. Se non viene selezionato alcun percorso, sarà utilizzata la sorgente degli aggiornamenti definita nelle impostazioni di aggiornamento dell'applicazione.
/R[A]:<file_rapporti>	<p>/R:<file_rapporti>: registra solo gli eventi importanti nel rapporto.</p> <p>/RA:<file_rapporti>: registra tutti gli eventi nel rapporto.</p> <p>È possibile indicare un percorso assoluto o relativo. Se l'impostazione non è definita, vengono visualizzati i risultati della scansione e tutti gli eventi.</p>
/C:<nome_file>	<p>Percorso del file di configurazione contenente le impostazioni per l'aggiornamento di Kaspersky Anti-Virus.</p> <p>Un file di configurazione è un file in formato testo che contiene un elenco di parametri della riga di comando per un aggiornamento dell'applicazione.</p> <p>È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori delle impostazioni nell'interfaccia dell'applicazione.</p>

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 le impostazioni del file di configurazione updateapp.ini:*

```
avp.com UPDATE /C:updateapp.ini
```

File di configurazione di esempio:

```
"ftp://my_server/kav_updates" /RA:avbases_upd.txt
```

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

Sintassi del comando:

```
avp.com ROLLBACK [/R[A]:<file_rapporti>][/password=<password>]
```

Una descrizione dei parametri è disponibile nella tabella seguente.

/R[A]:<file_rapporti>	<p>/R:<file_rapporti>: registra solo gli eventi importanti nel rapporto.</p> <p>/RA:<file_rapporti>: registra tutti gli eventi nel rapporto.</p> <p>È possibile indicare un percorso assoluto o relativo. Se l'impostazione non è definita, vengono visualizzati i risultati della scansione e tutti gli eventi.</p>
<password>	Password dell'applicazione specificata nell'interfaccia.

Questo comando non viene accettato senza l'immissione di una password.

Esempio:

```
avp.com ROLLBACK /RA:rollback.txt /password=<password>
```

ESPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com EXPORT <profilo> <nomefile>
```

Nella tabella seguente sono descritte le impostazioni per l'esecuzione dei comandi.

<profilo>	Componente o attività di cui si esportano le impostazioni. Per <profilo> è possibile utilizzare qualsiasi valore elencato nella sezione della guida "Gestione dei componenti e delle attività dell'applicazione".
<nomefile>	Percorso del file nel quale verranno esportate le impostazioni di Kaspersky Anti-Virus. È possibile specificare un percorso assoluto o relativo. Se non viene specificato un formato diverso o se non viene specificato alcun formato, il file di configurazione viene salvato in formato binario (.dat) e può essere utilizzato successivamente per importare le impostazioni in altri computer. Il file di configurazione può inoltre essere salvato come file di testo. A questo scopo, specificare l'estensione .txt nel nome del file. Si noti che non è possibile importare le impostazioni di protezione da un file di testo. Tale file può essere utilizzato solo per specificare le impostazioni principali per il funzionamento di Kaspersky Anti-Virus.

Esempio:

```
avp.com EXPORT RTP c:\settings.dat
```

IMPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com IMPORT <nomefile> [/password=<password>]
```

Nella tabella seguente sono descritte le impostazioni per l'esecuzione dei comandi.

<nomefile>	Percorso del file da cui vengono importate le impostazioni di Kaspersky Anti-Virus. È possibile specificare un percorso assoluto o relativo.
<password>	Password di Kaspersky Anti-Virus specificata nell'interfaccia dell'applicazione. I parametri di protezione possono essere importati solo da un file binario.

Questo comando non viene accettato senza l'immissione di una password.

Esempio:

```
avp.com IMPORT c:\settings.dat /password=<password>
```

CREAZIONE DI UN FILE DI TRACCIA

La creazione di un file di traccia può essere necessaria in caso di problemi nel funzionamento di Kaspersky Anti-Virus. Questo consente agli esperti del Servizio di Assistenza tecnica di diagnosticare i problemi più accuratamente.

È consigliabile creare file di traccia solo per individuare un problema specifico. L'abilitazione regolare delle tracce può rallentare il computer ed esaurire lo spazio sul disco rigido.

Sintassi del comando:

```
avp.com TRACE [file] [on|off] [<livello_traccia>]
```

Una descrizione dei parametri è disponibile nella tabella seguente.

[on off]	Abilita/disabilita la creazione del file di traccia.
[file]	Inserisce la traccia in un file.
<livello_traccia>	Questa impostazione può essere compresa tra 0 (livello minimo, solo messaggi critici) e 700 (livello massimo, tutti i messaggi). Quando si contatta l'Assistenza tecnica, un esperto indica il livello di traccia richiesto. Se non viene specificato alcun livello, è consigliabile impostare il valore su 500.

Esempi:

- ◆ Per disabilitare la creazione del file di traccia:

```
avp.com TRACE file off
```

- ◆ Per creare un file di traccia da inviare all'Assistenza tecnica con un livello di traccia massimo pari a 500:

```
avp.com TRACE file on 500
```

VISUALIZZAZIONE DELLA GUIDA

Per visualizzare le informazioni della Guida sulla sintassi della riga di comando, utilizzare il seguente comando:

```
avp.com [ /? | HELP ]
```

Per visualizzare le informazioni della Guida sulla sintassi di uno specifico comando, utilizzare uno dei seguenti comandi:

```
avp.com <comando> /?
```

```
avp.com HELP <comando>
```

CODICI RESTITUITI DELLA RIGA DI COMANDO

In questa sezione sono descritti i codici restituiti della riga di comando (vedere la tabella seguente). 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.
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 VIRUS	
101	Tutti gli oggetti pericolosi sono stati elaborati.
102	Oggetto pericoloso rilevato.

ELENCO DELLE NOTIFICHE DI KASPERSKY ANTI-VIRUS

Questa sezione fornisce informazioni sulle notifiche visualizzate sullo schermo da Kaspersky Anti-Virus.

IN QUESTA SEZIONE:

Notifiche in qualsiasi modalità di protezione.....	127
Notifiche nella modalità di protezione interattiva	131

NOTIFICHE IN QUALSIASI MODALITÀ DI PROTEZIONE

Questa sezione fornisce informazioni sulle notifiche visualizzate sia nella modalità di protezione automatica che in quella interattiva (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)).

IN QUESTA SEZIONE:


Richiesta di esecuzione di una procedura speciale.....	127
Unità rimovibile connessa	128
Rilevamento di un certificato non attendibile	128
Rilevamento di un'applicazione potenzialmente utilizzabile da un intruso per danneggiare i dati o il computer dell'utente	128
Spostamento in quarantena di un file non infetto	129
Rilascio di una nuova versione del prodotto.....	129
Rilascio di un aggiornamento tecnico.....	129
Download dell'aggiornamento tecnico completato	130
Aggiornamento tecnico scaricato non installato	130
Licenza scaduta	130
È consigliabile aggiornare i database prima della scansione	131

RICHIESTA DI ESECUZIONE DI UNA PROCEDURA SPECIALE

Quando viene rilevata una minaccia attualmente attiva nel sistema, ad esempio un processo dannoso nella RAM o negli oggetti di avvio, viene visualizzata una notifica per richiedere l'esecuzione di una speciale procedura avanzata di disinfezione.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo di minaccia e nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei virus di Kaspersky Lab.

Accanto al nome dell'oggetto dannoso viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sull'oggetto. Facendo click sul collegamento www.securelist.com in questa finestra, è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate sulla minaccia rappresentata dall'oggetto.

- Nome e percorso dell'oggetto dannoso.

È possibile selezionare una delle seguenti azioni:

- **Sì, disinfetta e riavvia** – esegue la speciale procedura di disinfezione (opzione consigliata).

Durante la disinfezione, tutte le applicazioni sono bloccate tranne quelle attendibili. Al termine della disinfezione, il sistema operativo verrà riavviato, pertanto è consigliabile salvare le modifiche apportate e chiudere tutte le

applicazioni prima di avviare la disinfezione. Dopo aver riavviato il computer, viene consigliata l'esecuzione di una scansione virus completa.

- **Non eseguire** – l'oggetto o il processo rilevato verrà elaborato in base all'azione selezionata.

Per applicare automaticamente l'azione selezionata ogni volta che si verifica la stessa situazione, selezionare la casella **Applica a tutti gli oggetti**.

UNITÀ RIMOVIBILE CONNESSA

La notifica è visualizzata quando un'unità rimovibile viene connessa al computer.

È possibile selezionare una delle seguenti azioni:

- **Scansione Rapida** – vengono esaminati solo i file memorizzati nell'unità rimovibile che possono rappresentare una potenziale minaccia.
- **Scansione Completa** – vengono esaminati tutti i file memorizzati nell'unità rimovibile.
- **Non eseguire scansione** – non viene eseguita alcuna scansione dell'unità rimovibile.

Per applicare l'azione selezionata a tutte le unità rimovibili connesse successivamente, selezionare la casella **Esegui sempre in questi casi**.

RILEVAMENTO DI UN CERTIFICATO NON ATTENDIBILE

Kaspersky Anti-Virus verifica la protezione della connessione stabilita tramite il protocollo SSL utilizzando un certificato installato. Se viene rilevato un certificato non valido quando si tenta di stabilire la connessione al server, ad esempio se il certificato viene sostituito da un intruso, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- descrizione della minaccia;
- collegamento per la visualizzazione del certificato;
- probabili cause dell'errore;
- URL della risorsa Web.


È possibile selezionare una delle seguenti azioni:

- **Si, accetta il certificato non attendibile** – procede con la connessione alla risorsa Web.
- **Nega certificato**: la connessione al sito Web viene interrotta.

RILEVAMENTO DI UN'APPLICAZIONE POTENZIALMENTE UTILIZZABILE DA UN INTRUSO PER DANNEGGIARE I DATI O IL COMPUTER DELL'UTENTE

Quando viene rilevata un'applicazione che può essere sfruttata da un intruso per danneggiare i dati o il computer dell'utente, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo e nome dell'applicazione potenzialmente utilizzabile da un intruso per danneggiare i dati o il computer dell'utente.
Accanto al nome dell'applicazione viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sull'applicazione.
- ID del processo e nome del file dell'applicazione, con il relativo percorso.
- Collegamento alla finestra del registro di rilevamento dell'applicazione.

È possibile selezionare una delle seguenti azioni:

- **Consenti** – consente l'esecuzione dell'applicazione.
- **Quarantena** – chiude l'applicazione e sposta il file dell'applicazione in Quarantena, dove non costituisce alcuna minaccia per la protezione del computer.

Durante le successive scansioni della quarantena, 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 che all'oggetto venga assegnato lo stato *non infetto* e che quindi possa essere ripristinato.

Lo stato di un file spostato in quarantena può essere modificato su *non infetto* durante una scansione successiva, ma non prima di tre giorni dal suo spostamento in quarantena.

- **Termina applicazione** – interrompe l'esecuzione dell'applicazione.
- **Aggiungi alle esclusioni** – consente all'applicazione di eseguire sempre le azioni specificate in futuro.

SPOSTAMENTO IN QUARANTENA DI UN FILE NON INFETTO

Per impostazione predefinita, Kaspersky Anti-Virus esamina i file in quarantena dopo ogni aggiornamento dei database. Se la scansione di un file in quarantena indica che non è infetto, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- un suggerimento di ripristinare il file in quarantena;
- il nome del file, incluso il percorso della cartella in cui era contenuto prima di essere spostato in quarantena.

È possibile selezionare una delle seguenti azioni:

- **Ripristina** – ripristina il file rimuovendolo dalla quarantena e spostandolo nella cartella in cui era contenuto prima di essere spostato in quarantena.
- **Annulla** – mantiene il file in quarantena.

RILASCIO DI UNA NUOVA VERSIONE DEL PRODOTTO

Quando viene rilasciata una nuova versione di Kaspersky Anti-Virus, che diventa disponibile per il download dai server di Kaspersky Lab, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- un collegamento a una finestra con informazioni dettagliate sulla nuova versione dell'applicazione;
- la dimensione del pacchetto di installazione.

È possibile selezionare una delle seguenti azioni:

- **Si, scarica** – esegue il download del pacchetto di installazione della nuova versione dell'applicazione nella cartella selezionata.
- **No** – annulla il download del pacchetto di installazione.

Se non si desidera visualizzare più la notifica della disponibilità della nuova versione dell'applicazione, selezionare la casella **Non segnalare questo aggiornamento**.

RILASCIO DI UN AGGIORNAMENTO TECNICO

Quando viene rilasciato un aggiornamento tecnico di Kaspersky Anti-Virus, che diventa disponibile per il download dai server di Kaspersky Lab, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- il numero di versione dell'applicazione installata nel computer;
- il numero di versione dell'applicazione dopo l'aggiornamento tecnico;
- un collegamento a una finestra con informazioni dettagliate sull'aggiornamento tecnico;
- la dimensione del file di aggiornamento.

È possibile selezionare una delle seguenti azioni:

- **Si, scarica** – esegue il download del file di aggiornamento nella cartella selezionata.
- **No** – annulla il download dell'aggiornamento. Questa opzione è disponibile se la casella **Non segnalare questo aggiornamento** è selezionata (vedere di seguito).

- **No, ricorda in seguito** – annulla il download e visualizza successivamente un promemoria dell'aggiornamento. Questa opzione è disponibile se la casella **Non segnalare questo aggiornamento** è deselezionata (vedere di seguito).

Se non si desidera visualizzare più la notifica, selezionare la casella **Non segnalare questo aggiornamento**.

DOWNLOAD DELL'AGGIORNAMENTO TECNICO COMPLETATO

Al completamento del download dell'aggiornamento tecnico di Kaspersky Anti-Virus dai server di Kaspersky Lab, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- il numero di versione dell'applicazione dopo l'aggiornamento tecnico;
- un collegamento al file di aggiornamento.

È possibile selezionare una delle seguenti azioni:

- **Sì, installa** – installa l'aggiornamento.

Al termine dell'installazione dell'aggiornamento, è necessario riavviare il sistema operativo.

- **Rimanda installazione** – annulla l'installazione per eseguirla in un secondo momento.

AGGIORNAMENTO TECNICO SCARICATO NON INSTALLATO

Se un aggiornamento tecnico di Kaspersky Anti-Virus è stato scaricato ma non installato nel computer, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- il numero di versione dell'applicazione dopo l'aggiornamento tecnico;
- un collegamento al file di aggiornamento.

È possibile selezionare una delle seguenti azioni:

- **Sì, installa** – installa l'aggiornamento.

Al termine dell'installazione dell'aggiornamento, è necessario riavviare il sistema operativo.

- **Rimanda installazione** – annulla l'installazione per eseguirla in un secondo momento.

Se non si desidera visualizzare più la notifica dell'aggiornamento, selezionare la casella **Non chiedere più fino alla disponibilità della nuova versione**.

LICENZA SCADUTA

Alla scadenza della licenza di prova, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- la durata del periodo di prova;
- informazioni sui risultati dell'esecuzione dell'applicazione (possono includere un collegamento a maggiori dettagli).

È possibile selezionare una delle seguenti azioni:

- **Sì, acquista** – se si seleziona questa opzione, viene aperta una finestra del browser e viene caricata la pagina Web di Compra Online, in cui è possibile acquistare una licenza commerciale.
- **Annulla** – consente di interrompere l'utilizzo dell'applicazione. Se si seleziona questa opzione, le funzioni principali dell'applicazione non sono più disponibili (scansione virus, aggiornamento, protezione in tempo reale e così via).

È CONSIGLIABILE AGGIORNARE I DATABASE PRIMA DELLA SCANSIONE

Se si avviano attività di scansione prima o durante il primo aggiornamento dei database, viene visualizzata una notifica. La notifica suggerisce di aggiornare i database o di attendere il completamento dell'aggiornamento prima di eseguire la scansione.

È possibile selezionare una delle seguenti azioni:

- **Aggiorna i database prima della scansione** – avvia l'aggiornamento dei database, al termine del quale viene avviata automaticamente l'attività di scansione. Questa opzione non è disponibile se l'attività di scansione è stata avviata prima del primo aggiornamento dei database.
- **Avvia la scansione dopo l'aggiornamento** – attende il completamento dell'aggiornamento dei database e avvia l'attività di scansione automaticamente. Questa opzione non è disponibile se l'attività di scansione è stata avviata durante il primo aggiornamento dei database.
- **Avvia la scansione adesso** – avvia l'attività di scansione senza attendere il completamento dell'aggiornamento dei database.

NOTIFICHE NELLA MODALITÀ DI PROTEZIONE INTERATTIVA

Questa sezione fornisce informazioni sulle notifiche visualizzate nella modalità di protezione interattiva (vedere la sezione "Selezione di una modalità di protezione" a pagina [56](#)).

IN QUESTA SEZIONE:

Rilevamento di un oggetto dannoso/sospetto	131
Rilevamento di una vulnerabilità	132
Rilevamento di un'attività pericolosa nel sistema	132
Rollback delle modifiche apportate da un'applicazione potenzialmente utilizzabile da un intruso per danneggiare i dati o il computer dell'utente	133
Rilevamento di un'applicazione dannosa	133
Rilevamento di un'applicazione potenzialmente utilizzabile da un intruso.....	134
Rilevamento di un collegamento sospetto o dannoso	135
Rilevamento di un oggetto pericoloso nel traffico	135
Rilevamento di un tentativo di accedere a un sito Web di phishing.....	135
Rilevamento di un tentativo di accesso al Registro di sistema	136
Impossibile disinfettare l'oggetto	136
Rilevamento di processi nascosti	136


RILEVAMENTO DI UN OGGETTO DANNOSO/SOSPETTO

Durante l'esecuzione di Anti-Virus File, Anti-Virus Posta o di una scansione virus, viene visualizzata una notifica sullo schermo se viene rilevato uno dei seguenti oggetti:

- oggetto dannoso;
- oggetto che contiene il codice di un virus sconosciuto;
- oggetto che contiene il codice modificato di un virus sconosciuto.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo di minaccia e nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei virus di Kaspersky Lab.

Accanto al nome dell'oggetto dannoso viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sull'oggetto. Facendo click sul collegamento www.securelist.com in questa finestra,

è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate sulla minaccia rappresentata dall'oggetto.

- Nome e percorso dell'oggetto dannoso.

È possibile selezionare una delle risposte seguenti all'oggetto:

- **Disinfetta:** viene eseguito un tentativo di disinfezione dell'oggetto dannoso. Questa opzione viene suggerita se la minaccia è nota.

Prima di disinfettare l'oggetto, ne viene creata una copia di backup.

- **Quarantena:** sposta l'oggetto in Quarantena, dove non costituisce alcuna minaccia per il computer. Questa opzione viene suggerita se sia la minaccia che i metodi per la sua disinfezione sono sconosciuti.

Durante le successive scansioni della quarantena, 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 che all'oggetto venga assegnato lo stato *non infetto* e che quindi possa essere ripristinato.

Lo stato di un file spostato in quarantena può essere modificato su *non infetto* durante una scansione successiva, ma non prima di tre giorni dal suo spostamento in quarantena.

- **Elimina:** l'oggetto viene eliminato. Prima di eliminare l'oggetto, ne viene creata una copia di backup.
- **Ignora / Blocca:** viene bloccato l'accesso all'oggetto, senza eseguire alcuna azione; le informazioni vengono registrate in un rapporto.

È possibile tornare all'elaborazione degli 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 tutte le minacce dello stesso tipo rilevate durante la sessione corrente di un componente di protezione o un'attività, selezionare la casella **Applica a tutti gli oggetti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al riavvio di Kaspersky Anti-Virus oppure all'intervallo di tempo dall'inizio di una scansione virus fino al relativo completamento.

Se si è certi che l'oggetto rilevato non sia dannoso, è consigliabile aggiungerlo all'area attendibile per evitare che durante l'utilizzo dell'oggetto il programma rilevi ripetutamente dei falsi positivi.

RILEVAMENTO DI UNA VULNERABILITÀ

Se viene rilevata una vulnerabilità, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della vulnerabilità.
- Il nome della vulnerabilità così come è elencata nell'Enciclopedia dei virus di Kaspersky Lab.
Accanto al nome viene visualizzata l'icona ⓘ. Facendo click sull'icona, viene aperta una finestra con le informazioni sulla vulnerabilità. Facendo click su www.securelist.com nella finestra, è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate sulla vulnerabilità.
- Nome e percorso dell'oggetto vulnerabile.

È possibile selezionare una delle risposte seguenti all'oggetto:

- **Si, correggi** – elimina la vulnerabilità.
- **Ignora** – non esegue alcuna azione sull'oggetto vulnerabile.

RILEVAMENTO DI UN'ATTIVITÀ PERICOLOSA NEL SISTEMA

Quando Difesa Proattiva rileva nel sistema un'attività pericolosa di un'applicazione, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo di minaccia e nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei virus di Kaspersky Lab.

Accanto al nome dell'oggetto dannoso viene visualizzata l'icona ⓘ. Facendo click sull'icona, viene aperta una finestra con le informazioni sull'oggetto. Facendo click sul collegamento www.securelist.com in questa finestra,

è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate sulla minaccia rappresentata dall'oggetto.

- ID del processo e nome del file dell'applicazione, con il relativo percorso.

È possibile selezionare una delle seguenti azioni:

- **Consenti** – consente l'esecuzione dell'applicazione.
- **Quarantena** – chiude l'applicazione e sposta il file dell'applicazione in Quarantena, dove non costituisce alcuna minaccia per la protezione del computer.

Durante le successive scansioni della quarantena, 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 che all'oggetto venga assegnato lo stato *non infetto* e che quindi possa essere ripristinato.

Lo stato di un file spostato in quarantena può essere modificato su *non infetto* durante una scansione successiva, ma non prima di tre giorni dal suo spostamento in quarantena.


- **Termina applicazione** – interrompe l'esecuzione dell'applicazione.
- **Aggiungi alle esclusioni** – consente all'applicazione di eseguire sempre le azioni specificate in futuro.

Se si è certi che il programma rilevato non sia pericoloso, è consigliabile aggiungerlo all'area attendibile per evitare che Kaspersky Anti-Virus generi ripetutamente falsi positivi quando lo rileva.

ROLLBACK DELLE MODIFICHE APPORTATE DA UN'APPLICAZIONE POTENZIALMENTE UTILIZZABILE DA UN INTRUSO PER DANNEGGIARE I DATI O IL COMPUTER DELL'UTENTE

È consigliabile eseguire il rollback (l'annullamento) delle modifiche apportate da un'applicazione potenzialmente utilizzabile da un intruso per danneggiare i dati o il computer dell'utente. Quando un'applicazione di questo tipo termina la propria attività, viene visualizzata una notifica che richiede di eseguire il rollback delle modifiche.

La notifica contiene le seguenti informazioni:

- Richiesta del rollback delle modifiche apportate dall'applicazione potenzialmente utilizzabile da un intruso per danneggiare i dati o il computer dell'utente.
- Tipo e nome dell'applicazione.
Accanto al nome dell'applicazione viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sull'applicazione.
- ID del processo e nome del file dell'applicazione, con il relativo percorso.


È possibile selezionare una delle seguenti azioni:

- **Ignora** – annulla il rollback delle modifiche.
- **Si, esegui il rollback** – esegue il rollback delle modifiche apportate dall'applicazione

RILEVAMENTO DI UN'APPLICAZIONE DANNOSA

Quando Controllo sistema rileva un'applicazione il cui comportamento corrisponde completamente alle attività di un'applicazione dannosa, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo e nome dell'applicazione dannosa.
Accanto al nome dell'applicazione viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sull'applicazione.
- ID del processo e nome del file dell'applicazione, con il relativo percorso.
- Collegamento alla finestra del registro di rilevamento dell'applicazione.

È possibile selezionare una delle seguenti azioni:

- **Consenti** – consente l'esecuzione dell'applicazione.
- **Quarantena** – chiude l'applicazione e sposta il file dell'applicazione in Quarantena, dove non costituisce alcuna minaccia per la protezione del computer.

Durante le successive scansioni della quarantena, 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 che all'oggetto venga assegnato lo stato *non infetto* e che quindi possa essere ripristinato.

Lo stato di un file spostato in quarantena può essere modificato su *non infetto* durante una scansione successiva, ma non prima di tre giorni dal suo spostamento in quarantena.

- **Termina applicazione** – interrompe l'esecuzione dell'applicazione.
- **Aggiungi alle esclusioni** – consente all'applicazione di eseguire sempre le azioni specificate in futuro.

RILEVAMENTO DI UN'APPLICAZIONE POTENZIALMENTE UTILIZZABILE DA UN INTRUSO

Se Anti-Virus File, Anti-Virus Posta o l'attività di scansione virus rileva un'applicazione potenzialmente utilizzabile da un intruso, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo di minaccia e nome dell'oggetto così come è elencato nell'Enciclopedia dei virus di Kaspersky Lab.

Accanto al nome dell'oggetto viene visualizzata l'icona ⓘ. Facendo click sull'icona, viene aperta una finestra con le informazioni sull'oggetto. Facendo click sul collegamento www.securelist.com nella finestra, è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate.

- Nome e percorso del file dell'oggetto.

È possibile selezionare una delle risposte seguenti all'oggetto:

- **Quarantena:** sposta l'oggetto in Quarantena, dove non costituisce alcuna minaccia per il computer. Questa opzione viene suggerita se sia la minaccia che i metodi per la sua disinfezione sono sconosciuti.

Durante le successive scansioni della quarantena, 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 che all'oggetto venga assegnato lo stato *non infetto* e che quindi possa essere ripristinato.

Lo stato di un file spostato in quarantena può essere modificato su *non infetto* durante una scansione successiva, ma non prima di tre giorni dal suo spostamento in quarantena.

- **Elimina:** l'oggetto viene eliminato. Prima di eliminare l'oggetto, ne viene creata una copia di backup.
- **Elimina archivio:** l'archivio protetto da password viene eliminato.
- **Ignora / Blocca:** viene bloccato l'accesso all'oggetto, senza eseguire alcuna azione; le informazioni vengono registrate in un rapporto.

È possibile tornare all'elaborazione degli oggetti ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

- **Aggiungi alle esclusioni:** viene creata una regola di esclusione per questo tipo di minaccia.

Per applicare l'azione selezionata a tutte le minacce dello stesso tipo rilevate durante la sessione corrente di un componente di protezione o un'attività, selezionare la casella **Applica a tutti gli oggetti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al riavvio di Kaspersky Anti-Virus oppure all'intervallo di tempo dall'inizio di una scansione virus fino al relativo completamento.

Se si è certi che l'oggetto rilevato non sia dannoso, è consigliabile aggiungerlo all'area attendibile per evitare che durante l'utilizzo dell'oggetto il programma rilevi ripetutamente dei falsi positivi.

RILEVAMENTO DI UN COLLEGAMENTO SOSPETTO O DANNOSO

Quando Kaspersky Anti-Virus rileva un tentativo di aprire un sito Web con contenuto sospetto o dannoso, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- descrizione della minaccia;
- nome dell'applicazione (browser) utilizzata per il caricamento del sito Web;
- URL del sito Web o della pagina Web con contenuto sospetto o dannoso.

È possibile selezionare una delle seguenti azioni:

- **Consenti:** il download dal sito Web continua.
- **Blocca:** il download dal sito Web viene bloccato.


Per applicare l'azione selezionata a tutti i siti Web con minacce dello stesso tipo rilevate durante la sessione corrente di un componente di protezione, selezionare la casella **Applica a tutti gli oggetti**. La sessione corrente va dal momento in cui il componente viene avviato al momento in cui viene chiuso o Kaspersky Anti-Virus viene riavviato.

RILEVAMENTO DI UN OGGETTO PERICOLOSO NEL TRAFFICO

Quando Anti-Virus Web rileva un oggetto dannoso nel traffico, viene visualizzata una speciale notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia o delle azioni eseguite dall'applicazione.
- Nome dell'applicazione che ha eseguito l'azione.
- Tipo di minaccia e nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei virus di Kaspersky Lab.

Accanto al nome dell'oggetto dannoso viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sull'oggetto. Facendo click sul collegamento www.securelist.com in questa finestra, è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate sulla minaccia rappresentata dall'oggetto.

- Percorso dell'oggetto (URL).

È possibile selezionare una delle seguenti azioni:

- **Consenti:** il download dell'oggetto continua.
- **Blocca:** il download dell'oggetto dalla risorsa Web viene bloccato.

Per applicare l'azione selezionata a tutte le minacce dello stesso tipo rilevate durante la sessione corrente di un componente di protezione o un'attività, selezionare la casella **Applica a tutti gli oggetti**. La sessione corrente va dal momento in cui il componente viene avviato al momento in cui viene chiuso o Kaspersky Anti-Virus viene riavviato.

RILEVAMENTO DI UN TENTATIVO DI ACCEDERE A UN SITO WEB DI PHISHING

Quando Kaspersky Anti-Virus rileva un tentativo di accedere a un sito Web di phishing o potenzialmente tale, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- descrizione della minaccia;
- URL del sito Web.

È possibile selezionare una delle seguenti azioni:

- **Consenti:** il download dal sito Web continua.
- **Blocca:** il download dal sito Web viene bloccato.

Per applicare l'azione selezionata a tutti i siti Web con minacce dello stesso tipo rilevate durante la sessione corrente di Kaspersky Anti-Virus, selezionare la casella **Applica a tutti gli oggetti**. La sessione corrente va dal momento in cui il componente viene avviato al momento in cui viene chiuso o Kaspersky Anti-Virus viene riavviato.

RILEVAMENTO DI UN TENTATIVO DI ACCESSO AL REGISTRO DI SISTEMA

Quando Difesa Proattiva rileva un tentativo di accesso alle chiavi del Registro di sistema, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- la chiave del Registro di sistema alla quale si sta tentando di accedere;
- il nome del file del processo che ha avviato il tentativo di accesso alle chiavi del Registro di sistema e il relativo percorso.

È possibile selezionare una delle seguenti azioni:

- **Consenti:** consente l'esecuzione dell'azione pericolosa una sola volta;
- **Blocca:** l'azione pericolosa viene bloccata una sola volta.

Per applicare l'azione selezionata a ogni tentativo di ottenere l'accesso alle chiavi del Registro di sistema, selezionare la casella **Crea una regola**.


Se si è certi che le attività eseguite dall'applicazione che ha tentato di accedere alle chiavi del Registro di sistema non siano pericolose, aggiungere l'applicazione all'elenco di applicazioni attendibili.

IMPOSSIBILE DISINFETTARE L'OGGETTO

In alcuni casi non è possibile disinfettare un oggetto, ad esempio se il file è talmente danneggiato da rendere impossibile per l'applicazione rimuovere il codice dannoso e ripristinare l'integrità del file. Inoltre, la procedura di disinfezione non può essere eseguita su diversi tipi di oggetti dannosi, ad esempio i Trojan. Se non è possibile disinfettare un oggetto, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo di minaccia e nome dell'oggetto dannoso così come è elencato nell'Enciclopedia dei virus di Kaspersky Lab.

Accanto al nome dell'oggetto dannoso viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sull'oggetto. Facendo click sul collegamento www.securelist.com in questa finestra, è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate sulla minaccia rappresentata dall'oggetto.

- Nome e percorso dell'oggetto dannoso.

È possibile selezionare una delle seguenti azioni:

- **Elimina:** l'oggetto viene eliminato. Prima di eliminare l'oggetto, ne viene creata una copia di backup.
- **Ignora / Blocca:** viene bloccato l'accesso all'oggetto, senza eseguire alcuna azione; le informazioni vengono registrate in un rapporto.

È possibile tornare all'elaborazione degli oggetti ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

- **Aggiungi alle esclusioni:** viene creata una regola di esclusione per questo tipo di minaccia.


Per applicare l'azione selezionata a tutte le minacce dello stesso tipo rilevate durante la sessione corrente di un componente di protezione o un'attività, selezionare la casella **Applica a tutti gli oggetti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al riavvio di Kaspersky Anti-Virus oppure all'intervallo di tempo dall'inizio di una scansione virus fino al relativo completamento.

RILEVAMENTO DI PROCESSI NASCOSTI

Se Difesa Proattiva rileva un processo nascosto nel sistema, viene visualizzata una notifica.

La notifica contiene le seguenti informazioni:

- Descrizione della minaccia.
- Tipo e nome della minaccia, così come è elencata nell'Enciclopedia dei virus di Kaspersky Lab.

Accanto al nome viene visualizzata l'icona . Facendo click sull'icona, viene aperta una finestra con le informazioni sulla minaccia. Facendo click su www.securelist.com nella finestra, è possibile passare al sito Web dell'Enciclopedia dei virus e ottenere informazioni più dettagliate sulla minaccia.

- Nome e percorso del file di processo.

È possibile selezionare una delle seguenti azioni:

- **Quarantena** – chiude il processo e sposta il file del processo in Quarantena, dove non costituisce alcuna minaccia per la protezione del computer.

Durante le successive scansioni della quarantena, 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 che all'oggetto venga assegnato lo stato *non infetto* e che quindi possa essere ripristinato.

Lo stato di un file spostato in quarantena può essere modificato su *non infetto* durante una scansione successiva, ma non prima di tre giorni dal suo spostamento in quarantena.

- **Termina** – interrompe il processo.
- **Consenti** – consente l'esecuzione del processo.

Per applicare l'azione selezionata a tutte le minacce dello stesso tipo rilevate nella sessione corrente di Difesa Proattiva, selezionare la casella **Esegui sempre in questi casi**. La sessione corrente va dal momento in cui il componente viene avviato al momento in cui viene chiuso o Kaspersky Anti-Virus viene riavviato.

Se si è certi che il processo rilevato non sia pericoloso, è consigliabile aggiungerlo all'area attendibile per evitare che Kaspersky Anti-Virus generi ripetutamente falsi positivi quando lo rileva.

GLOSSARIO

A

AGGIORNAMENTI DISPONIBILI

Gruppo di aggiornamenti per i moduli dell'applicazione Kaspersky Lab, inclusi gli aggiornamenti critici accumulati in un determinato periodo di tempo e le modifiche apportate all'architettura dell'applicazione.

AGGIORNAMENTI URGENTI

Aggiornamenti critici dei moduli dell'applicazione Kaspersky Lab.

AGGIORNAMENTO

Procedura di sostituzione/aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky Lab.

AGGIORNAMENTO DEL DATABASE

Una delle funzioni eseguite da un'applicazione Kaspersky Lab che consente di mantenere sempre aggiornata la protezione. I database vengono scaricati nel computer dai server degli aggiornamenti di Kaspersky Lab e sono collegati automaticamente all'applicazione.

ANALISI EURISTICA

Tecnologia progettata per il rilevamento delle minacce che non possono essere identificate utilizzando i database dell'applicazione Kaspersky Lab. Consente di rilevare gli oggetti che potrebbero essere stati infettati da un virus sconosciuto o da una nuova variante 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 Anti-Virus.

ARCHIVIO

File "contenente" uno o più oggetti che possono essere a loro volta archivi.

ATTACCO DI VIRUS

Serie di tentativi intenzionali di infettare un computer con un virus.

ATTIVAZIONE DELL'APPLICAZIONE

Passaggio dell'applicazione alla modalità completamente operativa. L'utente deve disporre di una licenza per attivare l'applicazione.

ATTIVITÀ

Le funzioni eseguite dall'applicazione Kaspersky Lab vengono implementate come attività, ad esempio: Protezione in tempo reale, Scansione Completa, Aggiornamento del database.

B

BLACKLIST DEI FILE CHIAVE

Database contenente informazioni sui file chiave Kaspersky Lab disabilitati. Il contenuto del file della blacklist viene aggiornato insieme ai database del prodotto.

BLOCCO DI UN OGGETTO

Negazione dell'accesso a un oggetto da applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

C**CERTIFICATO DEL SERVER DI AMMINISTRAZIONE**

Certificato che consente di autenticare il Server di amministrazione quando viene connesso alla Console di amministrazione e durante lo scambio di dati con i computer degli utenti. Il certificato del server di amministrazione viene creato durante l'installazione del server di amministrazione ed è memorizzato nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

CONTATORE DEGLI ATTACCHI D VIRUS

Modello in base al quale viene generata una notifica di minaccia di attacco di virus. Il contatore include una combinazione di impostazioni che determinano la soglia di attività del virus, la modalità di diffusione e il testo nei messaggi da inviare.

D**DATABASE**

Database creati dagli esperti di Kaspersky Lab contenenti una descrizione dettagliata di tutte le attuali minacce per la sicurezza dei computer, nonché dei metodi per rilevarle ed eliminarle. I database vengono costantemente aggiornati da Kaspersky Lab al presentarsi di nuove minacce.

DATABASE DI INDIRIZZI WEB DI PHISHING

Elenco di indirizzi Web, definiti come phishing dagli specialisti di Kaspersky Lab. Il database viene aggiornato regolarmente e fa parte dell'applicazione Kaspersky Lab.

DATABASE DI INDIRIZZI WEB SOSPETTI

Elenco di indirizzi Web, il cui contenuto può essere considerato potenzialmente pericoloso. L'elenco viene creato dagli specialisti di Kaspersky Lab. È regolarmente aggiornato e incluso nel pacchetto dell'applicazione 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. Gli oggetti vengono disinfettati utilizzando i record del database. Durante la disinfezione è possibile che parte dei dati vada persa.

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 successivo riavvio del sistema.

DNS (DOMAIN NAME SERVICE)

Sistema distribuito per la conversione del nome di un host (un computer o un altro dispositivo di rete) in un indirizzo IP. DNS funziona in reti TCP/IP. DNS può inoltre memorizzare ed elaborare richieste inverse, determinando il nome di un host in base al relativo indirizzo IP (record PTR). La risoluzione dei nomi DNS viene in genere eseguita da applicazioni di rete, non dagli utenti.

DUMP DELLA MEMORIA

Contenuto della memoria di lavoro di un processo o dell'intera RAM del sistema in un momento specifico.

E**ELENCO DEI SITI WEB PER VERIFICARE**

Elenco di maschere e indirizzi di risorse Web, esaminati obbligatoriamente per verificare la presenza di oggetti dannosi da parte dell'applicazione Kaspersky Lab.

ELENCO DELLE URL BLOCCATE

Elenco di maschere e indirizzi di risorse Web a cui non è possibile accedere a causa del blocco da parte dell'applicazione Kaspersky Lab. Tale elenco viene creato dall'utente durante la configurazione delle impostazioni dell'applicazione.

ELENCO DELLE URL CONSENTITE

Elenco di maschere e indirizzi di risorse Web a cui è possibile accedere senza alcun blocco da parte dell'applicazione Kaspersky Lab. Tale elenco viene creato dall'utente durante la configurazione delle impostazioni dell'applicazione.

ELENCO DI URL ATTENDIBILI

Elenco di maschere e indirizzi di risorse Web, di cui l'utente considera attendibile il contenuto. L'applicazione Kaspersky Lab non sottopone a scansione le pagine Web corrispondenti alle voci dell'elenco per verificare la presenza di oggetti dannosi.

ELIMINAZIONE DI UN OGGETTO

Metodo di elaborazione dell'oggetto che implica la sua eliminazione fisica dalla posizione originaria (disco rigido, cartella, risorsa di rete). È consigliabile 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. È possibile escludere dalla scansione determinati formati di file, utilizzare maschere di file o escludere una determinata area, ad esempio una cartella o un programma, processi di programma o oggetti in base alla classificazione del tipo di minaccia nell'Enciclopedia dei virus. 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 estensione KEY, che rappresenta la "chiave" personale che consente di utilizzare l'applicazione Kaspersky Lab. Un file chiave è incluso nel prodotto acquistato presso i distributori Kaspersky Lab o viene inviato tramite posta elettronica se l'acquisto avviene online.

FILE COMPRESSO

File di archivio contenente un programma di decompressione e istruzioni per la relativa esecuzione per il sistema operativo.

FLUSSI NTFS ALTERNATIVI

Flussi di dati NTFS (flussi di dati alternativi) destinati a contenere attributi aggiuntivi o informazioni sui file.

Ogni file in un file system NTFS è un insieme di flussi. Uno di essi include il contenuto che è possibile visualizzare dopo aver aperto il file, altri flussi (definiti alternativi) sono destinati a contenere metadati e garantire, ad esempio, la compatibilità di NTFS con altri sistemi, come un file system precedente di Macintosh definito HFS (Hierarchical File System). I flussi possono essere creati, eliminati, memorizzati, rinominati e persino eseguiti come un processo.

I flussi alternativi possono essere utilizzati dagli utenti malintenzionati per trasferire dati in segreto o per rubarli da un computer.

G

GATEWAY DUAL-HOMED

Computer dotato di due schede di rete, ciascuna delle quali è collegata a una diversa rete, che trasferisce i dati da una rete all'altra.

I**IMPOSTAZIONI DELL'APPLICAZIONE**

Impostazioni dell'applicazione comuni a tutti i tipi di attività, che regolano il funzionamento dell'applicazione nel suo complesso, ad esempio le impostazioni relative alle prestazioni, ai rapporti e alla memoria di backup.

IMPOSTAZIONI DELLE ATTIVITÀ

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

INSTALLAZIONE TRAMITE UNO SCRIPT DI ACCESSO

Metodo di installazione remota delle applicazioni Kaspersky Lab che consente di assegnare l'avvio dell'attività di installazione remota a uno o più account utente. La registrazione di un utente in un dominio porta a un tentativo di installazione dell'applicazione nel computer client in cui l'utente è registrato. Questo metodo è consigliato per l'installazione delle applicazioni in computer che eseguono i sistemi operativi Microsoft Windows 98 / Me.

INTERCETTATORE

Componente secondario 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.

IP (INTERNET PROTOCOL)

Il protocollo di base per Internet, utilizzato sin dai tempi del suo primo sviluppo nel 1974. Esegue operazioni elementari nella trasmissione di dati da un computer all'altro e rappresenta la base per protocolli di livello superiore come TCP e UDP. Gestisce la connessione e l'elaborazione degli errori. Il ricorso a tecnologie come NAT e il mascheramento consente di nascondere numerose reti private utilizzando un numero limitato di indirizzi IP (o persino un solo indirizzo). In questo modo diventa possibile gestire le richieste della rete Internet in costante espansione attraverso uno spazio degli indirizzi IPv4 relativamente limitato.

K**KASPERSKY SECURITY NETWORK**

Kaspersky Security Network (KSN) è un'infrastruttura di servizi online che consente di accedere alla Knowledge Base di Kaspersky Lab, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati di Kaspersky Security Network assicura una risposta più rapida da parte di Kaspersky Anti-Virus quando vengono rilevati nuovi tipi di minacce, migliora le prestazioni di alcuni componenti di protezione e riduce il rischio di falsi positivi.

L**LICENZA AGGIUNTIVA**

Licenza aggiunta per consentire il funzionamento dell'applicazione Kaspersky Lab ma non attivata. La licenza aggiuntiva viene attivata alla scadenza della licenza attiva.

LICENZA ATTIVA

La licenza attualmente utilizzata per il funzionamento di un'applicazione Kaspersky Lab. La licenza definisce la data di scadenza della funzionalità completa e i criteri della licenza relativi all'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 garantire un livello ottimale di protezione per il computer. Questo livello viene impostato per l'utilizzo per impostazione predefinita.

LIVELLO DI GRAVITÀ DELL'EVENTO

Descrizione dell'evento, registrato durante il funzionamento dell'applicazione Kaspersky Lab. Esistono quattro livelli di gravità:

Evento critico.

Errore funzionale.

Attenzione.

Messaggio informativo.

Eventi dello stesso tipo possono avere livelli di gravità diversi, in base alla situazione in cui si sono verificati.

LIVELLO DI PROTEZIONE

Il livello di protezione viene definito come una configurazione del componente predeterminata.

M

MASCHERA DI FILE

Rappresentazione di un nome file e di un'estensione tramite caratteri jolly. I due caratteri jolly standard utilizzati nelle maschere di file sono * e ?, dove * rappresenta qualsiasi numero di caratteri e ? indica qualsiasi carattere singolo. Utilizzando questi caratteri jolly, è possibile rappresentare qualsiasi file. Si noti che il nome e l'estensione sono sempre separati da un punto.

MESSAGGIO OSCENO

Messaggio di posta elettronica contenente linguaggio offensivo.

MESSAGGIO SOSPETTO

Messaggio che non può essere inequivocabilmente considerato spam, ma che appare sospetto quando viene analizzato, come nel caso di determinati messaggi pubblicitari.

MODELLO DI NOTIFICA

Modello in base al quale viene generata una notifica di oggetti infetti rilevati dalla scansione. Il modello di notifica include una combinazione di impostazioni che regolano la modalità di notifica, la modalità di distribuzione e il testo dei messaggi da inviare.

MODULI DELL'APPLICAZIONE

File inclusi nel pacchetto di installazione di Kaspersky Lab responsabile dell'esecuzione delle attività principali. Un determinato modulo eseguibile corrisponde a ogni tipo di attività eseguita dall'applicazione (protezione in tempo reale, scansione manuale, aggiornamenti). Attraverso l'esecuzione di una scansione completa del computer dalla finestra principale, viene avviata l'esecuzione del modulo di questa attività.

O

OGGETTI DI AVVIO

Il set di programmi necessario per avviare e far funzionare correttamente il sistema operativo e il software installato nel computer. Questi oggetti vengono eseguiti a 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 INFETTO

Oggetto contenente codice dannoso. Il rilevamento di un oggetto contenente codice dannoso avviene quando una sezione del codice dell'oggetto corrisponde in modo preciso a una sezione del codice di una minaccia nota. Kaspersky Lab consiglia di evitare di utilizzare tali oggetti dal momento che possono infettare il computer.

OGGETTO MONITORATO

File trasferito attraverso i protocolli HTTP, FTP o SMTP mediante il firewall e inviato all'applicazione Kaspersky Lab per essere sottoposto a scansione.

OGGETTO OLE

Oggetto allegato o incorporato in un altro file. L'applicazione Kaspersky Lab consente di esaminare gli oggetti OLE per verificare la presenza di eventuali virus. Se ad esempio si inserisce una tabella di Microsoft Office Excel in un documento di Microsoft Office Word, tale tabella viene esaminata come oggetto OLE.

OGGETTO PERICOLOSO

Oggetto contenente un virus. Non è consigliabile accedere a questo tipo di oggetti per evitare di causare un'infezione del computer. Una volta rilevato un oggetto infetto, è consigliabile disinfettarlo tramite una delle applicazioni Kaspersky Lab o eliminarlo se non è possibile eseguire l'operazione.

OGGETTO POTENZIALMENTE INFETTABILE

Oggetto che, a causa della sua struttura o del suo formato, può essere utilizzato dagli intrusi come "contenitore" per memorizzare e distribuire un oggetto dannoso. In genere, si tratta di file eseguibili, ad esempio file con estensione COM, EXE, DLL e così via. Il rischio di penetrazione di codice dannoso in tali file è piuttosto alto.

OGGETTO POTENZIALMENTE INFETTO

Un 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'analizzatore euristico.

OGGETTO SOSPETTO

Un 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. Il periodo di validità della licenza in genere è pari a un anno a partire dalla data di installazione. Allo scadere della licenza, l'applicazione funziona con un numero limitato di funzionalità. Inoltre, non è più possibile aggiornare i database dell'applicazione.

PHISHING

Tipo di frode Internet che consiste nell'invio di messaggi e-mail allo scopo di trafugare informazioni riservate, in genere dati finanziari.

PORTA DI INPUT/OUTPUT

Viene utilizzata nei processori, ad esempio Intel, per lo scambio di dati con i componenti hardware. La porta di input/output è associata a un determinato componente hardware e consente alle applicazioni di effettuare lo scambio di dati.

PORTA DI RETE

Parametro TCP e UDP che determina la destinazione dei pacchetti di dati in formato IP trasmessi a un host o tramite una rete e che rende possibile l'esecuzione di vari programmi in un unico host per ricevere i dati indipendentemente l'uno dall'altro. Ogni programma elabora i dati ricevuti attraverso una determinata porta. Talvolta il programma viene definito "in ascolto" sulla porta.

Per alcuni protocolli di rete comuni, esistono in genere numeri di porta standard (ad esempio i server Web in genere ricevono richieste HTTP sulla porta TCP 80). I programmi possono tuttavia utilizzare qualsiasi protocollo su qualsiasi porta. Valori possibili: da 1 a 65535.

PORTA HARDWARE

Socket in un componente hardware di un computer in cui è possibile collegare un cavo o una spina (porta LPT, porta seriale, porta USB).

PROCESSO ATTENDIBILE

Processo di un'applicazione le cui operazioni non sono monitorate dall'applicazione Kaspersky Lab nella modalità di protezione in tempo reale. In altre parole, nessun oggetto eseguito, aperto o salvato dal processo considerato attendibile viene 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.

L'applicazione intercetta tutti i tentativi di aprire qualsiasi oggetto (lettura, scrittura o esecuzione) ed esegue una scansione di quest'ultimo per verificare la presenza di minacce. Gli oggetti non infetti vengono passati all'utente, quelli contenenti minacce o nei quali si sospetta la presenza di una minaccia vengono elaborati in base alle impostazioni dell'attività e quindi disinfettati, eliminati o messi in quarantena.

PROTOCOLLO

Set di regole chiaramente definite e standardizzate che regolano l'interazione tra un client e un server. I protocolli più conosciuti e i servizi a essi associati includono HTTP (WWW), FTP e NNTP (news).

Q

QUARANTENA

Una 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 dall'area Quarantena o Backup alla cartella in cui era presente inizialmente prima di essere disinfettato, eliminato, messo in quarantena o spostato in una cartella diversa specificata dall'utente.

ROOTKIT

Un'applicazione o un set di applicazioni sviluppate per nascondere le tracce di un intruso o del malware nel sistema.

Nei sistemi basati su Windows, un rootkit in genere è un programma che penetra nel sistema e ne intercetta le funzioni (API Windows). Innanzitutto, l'intercettazione e la modifica delle funzioni API di basso livello consente a un programma di questo tipo di mascherare la propria presenza nel sistema in modo piuttosto sofisticato. Inoltre, un rootkit solitamente nasconde la presenza dei processi, delle cartelle, dei file su disco e delle chiavi di registro descritti nella configurazione del rootkit. Numerosi rootkit installano i propri driver e servizi nel sistema, anch'essi "invisibili".

S

SCANSIONE DEL TRAFFICO

Scansione in tempo reale che utilizza le informazioni contenute nell'ultima versione dei database per gli oggetti trasmessi attraverso tutti i protocolli, ad esempio HTTP, FTP e così via.

SCRIPT

Piccolo programma per computer o un componente indipendente di un programma (funzione) che in genere viene sviluppato per eseguire un'attività specifica di portata ridotta. Viene spesso utilizzato con programmi incorporati in ipertesti. Gli script vengono ad esempio eseguiti quando si aprono determinati siti Web.

Se è abilitata la protezione in tempo reale, l'applicazione tiene traccia dell'avvio degli script, li intercetta e ne esegue la scansione virus. A seconda dei risultati della scansione, è possibile bloccare o consentire l'esecuzione degli script.

SERVER DEGLI AGGIORNAMENTI DI KASPERSKY LAB

Elenco dei server HTTP e FTP di Kaspersky Lab da cui l'applicazione scarica nel computer database e aggiornamenti dei moduli.

SERVER PROXY

Servizio di rete del computer che consente agli utenti di effettuare richieste indirette ad altri servizi di rete. Innanzitutto, un utente si connette a un server proxy e richiede una risorsa, ad esempio un file, che si trova in un altro server. Il server proxy si connette quindi al server specificato e ottiene la risorsa desiderata o restituisce la risorsa dalla relativa cache, qualora il proxy ne preveda una. In alcuni casi, la richiesta di un utente o la risposta di un server può essere modificata dal server proxy per determinati motivi.

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. Contiene informazioni sul file system del disco e un programma di caricamento responsabile dell'avvio del sistema operativo.

Esistono diversi virus che infettano i settori di avvio e che vengono di conseguenza definiti virus di boot. 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.

SOCKS

Protocollo del server proxy che consente di stabilire una connessione point-to-point tra computer nelle reti interne ed esterne.

SOGLIA DI ATTIVITÀ DEI VIRUS

Livello massimo consentito di un tipo specifico di evento in un periodo di tempo limitato che, se superato, viene 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 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 originaria alla cartella Quarantena, in cui viene salvato in forma crittografata, in modo da eliminare il rischio di infezione.

STATO DELLA PROTEZIONE

Stato corrente della protezione che indica il livello di sicurezza del computer.

SUBNET MASK

La subnet mask (nota anche come netmask) e l'indirizzo di rete determinano gli indirizzi dei computer in una rete.

T**TECNOLOGIA ICHECKER**

iChecker è una tecnologia che consente di accelerare la scansione virus escludendo gli oggetti che sono rimasti inalterati dall'ultima scansione, purché i parametri di scansione, ovvero le impostazioni e il database anti-virus, non siano stati modificati. Le informazioni su ogni file vengono archiviate in uno speciale database. Questa tecnologia viene utilizzata nelle modalità di protezione in tempo reale e di scansione manuale.

Si supponga, ad esempio, che a un archivio esaminato dall'applicazione 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, sono state modificate le impostazioni di scansione o è stato aggiornato il database anti-virus, l'archivio viene esaminato nuovamente.

Limitazioni della tecnologia iChecker:

questa tecnologia non rappresenta la scelta ideale per 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).

TRACCE

Esecuzione dell'applicazione in modalità di debug; dopo l'esecuzione di ogni comando, l'applicazione viene arrestata e viene visualizzato il risultato della specifica fase.

V

VIRUS DI AVVIO

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 ZAO

Kaspersky Lab è un'azienda nota a livello internazionale che sviluppa prodotti per la protezione da virus, malware, spam, attacchi di rete e degli hacker e altre minacce.

Nel 2008 Kaspersky Lab è stata classificata tra i primi quattro produttori a livello mondiale di soluzioni software di protezione delle informazioni per gli utenti finali (IDC Worldwide Endpoint Security Revenue by Vendor). Secondo un'indagine COMCON dal titolo "TGI-Russia 2009", Kaspersky Lab è lo sviluppatore preferito di sistemi di protezione tra gli utenti home in Russia.

Kaspersky Lab è stata fondata in Russia nel 1997. Oggi, Kaspersky Lab è un gruppo internazionale con sede centrale a Mosca e cinque divisioni regionali che gestiscono le attività dell'azienda in Russia, Europa occidentale e orientale, Medio Oriente, Africa, America del nord e del sud, Giappone, Cina e altri paesi nella regione Asia-Pacifico. L'azienda impiega più di 2000 specialisti qualificati.

Prodotti. I prodotti Kaspersky Lab offrono funzionalità di protezione per tutti i tipi di sistemi, dagli home computer alle reti aziendali di grandi dimensioni.

La gamma di prodotti personali include applicazioni anti-virus per sistemi desktop, portatili e pocket computer, oltre che per smartphone e altri dispositivi mobili.

L'azienda fornisce applicazioni e servizi per la protezione di workstation, file server e server Web, gateway di posta e firewall. Utilizzate in combinazione con il sistema di gestione centralizzato di Kaspersky Lab, queste soluzioni assicurano una protezione efficace e automatizzata dalle minacce per i computer. I prodotti Kaspersky Lab sono certificati dai più importanti laboratori di testing, sono compatibili con il software di numerosi fornitori di applicazioni per computer e sono ottimizzati per l'esecuzione in numerose piattaforme hardware.

Gli analisti anti-virus di Kaspersky Lab lavorano 24 ore su 24. Ogni giorno identificano migliaia di nuove minacce, creano strumenti per consentirne il rilevamento e la disinfezione e le includono nei database utilizzati dalle applicazioni Kaspersky Lab. *Il database anti-virus di Kaspersky Lab viene aggiornato ogni ora e il database Anti-Spam ogni cinque minuti.*

Tecnologie. Molte delle tecnologie che oggi sono parte integrante dei moderni strumenti anti-virus sono state originariamente sviluppate da Kaspersky Lab. Non è un caso che numerosi altri sviluppatori utilizzino il kernel di Kaspersky Anti-Virus nei propri prodotti, tra cui: SafeNet (Stati Uniti), Alt-N Technologies (Stati Uniti), Blue Coat Systems (Stati Uniti), Check Point Software Technologies (Israele), Clearswift (Regno Unito), CommuniGate Systems (Stati Uniti), Critical Path (Irlanda), D-Link (Taiwan), M86 Security (Stati Uniti), GFI (Malta), IBM (Stati Uniti), Juniper Networks (Stati Uniti), LANDesk (Stati Uniti), Microsoft (Stati Uniti), NETASQ (Francia), NETGEAR (Stati Uniti), Parallels (Russia), SonicWALL (Stati Uniti), WatchGuard Technologies (Stati Uniti) e ZyXEL Communications (Taiwan). Molte delle tecnologie innovative dell'azienda sono coperte da brevetto.

Risultati. Nel corso degli anni, Kaspersky Lab ha ottenuto centinaia di riconoscimenti per il proprio impegno nella lotta contro le minacce per i computer. Ad esempio, nel 2010 Kaspersky Anti-Virus ha ricevuto numerosi importanti riconoscimenti Advanced+ dopo una serie di test svolti da AV-Comparatives, un rinomato laboratorio anti-virus austriaco. Tuttavia, il principale risultato ottenuto da Kaspersky Lab è la fedeltà dei suoi clienti di tutto il mondo. I prodotti e le tecnologie di Kaspersky Lab proteggono più di 300 milioni di utenti e i suoi clienti aziendali sono oltre 200.000.

Sito ufficiale di Kaspersky Lab:

<http://www.kaspersky.it>

Enciclopedia dei virus:

<http://www.securelist.com>

Anti-Virus Lab:

newvirus@kaspersky.com (solo per l'invio di file potenzialmente infetti in formato di archivio)

<http://support.kaspersky.com/virlab/helpdesk.html?LANG=it> (per l'invio di richieste agli analisti anti-virus)

Forum Web di Kaspersky Lab:

<http://forum.kaspersky.com/index.php?showforum=62>

INFORMAZIONI SUL CODICE DI TERZE PARTI

Le informazioni sul codice di terze parti sono contenute in un file denominato legal_notices.txt, disponibile nella cartella di installazione dell'applicazione.

INDICE

A

Abilitazione o disabilitazione della protezione in tempo reale.....	35
Aggiornamento	
da una cartella locale.....	65
impostazioni internazionali.....	65
rollback dell'ultimo aggiornamento.....	67
server proxy.....	67
sorgente degli aggiornamenti.....	64
Ambito di protezione	
Anti-Virus File.....	69
Anti-Virus IM.....	83
Anti-Virus Posta.....	74
Anti-Virus Web.....	82
Analisi euristica	
Anti-Virus File.....	71
Anti-Virus Posta.....	75
Anti-Virus Web.....	81
Anti-Virus File	
ambito di protezione.....	69
analisi euristica.....	71
livello di protezione.....	70
modalità di scansione.....	70
ottimizzazione della scansione.....	72
risposta a una minaccia.....	71
scansione dei file compositi.....	72
sospensione.....	69
tecnologia di scansione.....	71
Anti-Virus IM	
ambito di protezione.....	83
database di indirizzi Web di phishing.....	83
Anti-Virus Posta	
ambito di protezione.....	74
analisi euristica.....	75
filtraggio degli allegati.....	76
livello di protezione.....	78
risposta a una minaccia.....	75
scansione dei file compositi.....	76
Anti-Virus Web	
ambito di protezione.....	82
analisi euristica.....	81
Controllo URL Kaspersky.....	80
database di indirizzi Web di phishing.....	79
livello di protezione.....	78
ottimizzazione della scansione.....	82
risposta a una minaccia.....	79
Area attendibile	
applicazioni attendibili.....	92
regole di esclusione.....	92
Auto-Difesa applicazione.....	95
C	
Cartella di installazione.....	17
Controllo URL Kaspersky	
Anti-Virus Web.....	80
Correzione delle impostazioni del browser Internet.....	101

D

Database di indirizzi Web di phishing	
Anti-Virus IM	83
Anti-Virus Web.....	79
Difesa Proattiva	
elenco di attività pericolose.....	85
gruppo di applicazioni attendibili.....	85
regole per il monitoraggio delle attività pericolose	85
Disinstallazione	
applicazione.....	23

E

EICAR	111
-------------	-----

F

Finestra principale dell'applicazione	29
---	----

I

Icona nell'area di notifica della barra delle applicazioni	27
--	----

L

Licenza	
attivazione dell'applicazione	38
Contratto di licenza con l'utente finale	25
Livello di protezione	
Anti-Virus File	70
Anti-Virus Posta.....	78
Anti-Virus Web.....	78

M

Menu di scelta rapida	28
-----------------------------	----

N

Notifiche	40
disabilitazione	108
disabilitazione del segnale acustico.....	108
invio delle notifiche tramite posta elettronica	108
tipi di notifiche.....	108

P

Pianificazione	
aggiornamento.....	66
scansione virus.....	59
Prestazioni del computer.....	94

Q

Quarantena e Backup	96
---------------------------	----

R

Rapporti	
filtraggio.....	104
ricerca di eventi	104
salvataggio in un file	105
selezione di un componente o di un'attività	103
visualizza	49
Rescue Disk	46
Restrizione dell'accesso all'applicazione.....	56
Rete	
connessioni crittografate.....	88
porte monitorate	90

Rinnovo della licenza	39
Ripristino delle impostazioni predefinite	49
Risposta a una minaccia	
Anti-Virus File	71
Anti-Virus Posta	75
Anti-Virus Web	79
scansione virus	61

S

Scansione	
account	61
avvio automatico di un'attività ignorata	59
azione da eseguire su un oggetto rilevato	61
livello di protezione	58
ottimizzazione della scansione	62
pianificazione	59
scansione dei file composti	61
scansione vulnerabilità	63
tecnologie di scansione	60
tipo di oggetti da esaminare	61

T

Tastiera Virtuale	43
Tracce	
caricamento dei risultati della traccia	115
creazione di un file di traccia	115